MATLAB EXPO 2019

基于MathWorks工具链的系统工程：从需求到软件实现

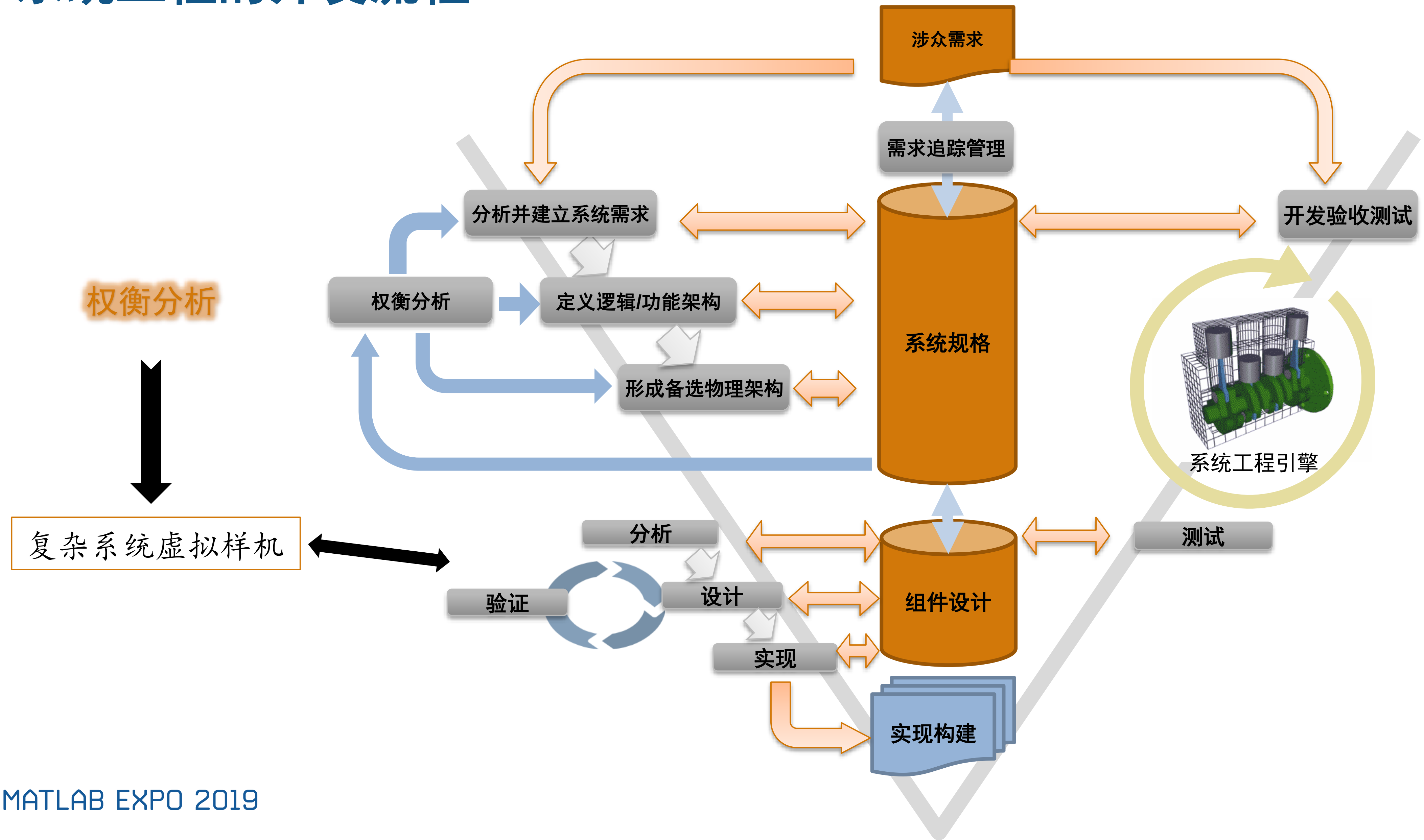
李晨光

内容

- 复杂系统虚拟样机的构建
- 基于事件的动态场景和性能分析
- 面向产品级软件的架构设计和需求管理
- 面向产品级软件的测试验证框架

复杂系统虚拟样机的构建

系统工程的开发流程



权衡分析

复杂系统虚拟样机

涉众需求

需求追踪管理

分析并建立系统需求

权衡分析

定义逻辑/功能架构

形成备选物理架构

系统规格

开发验收测试

系统工程引擎

分析

设计

实现

验证

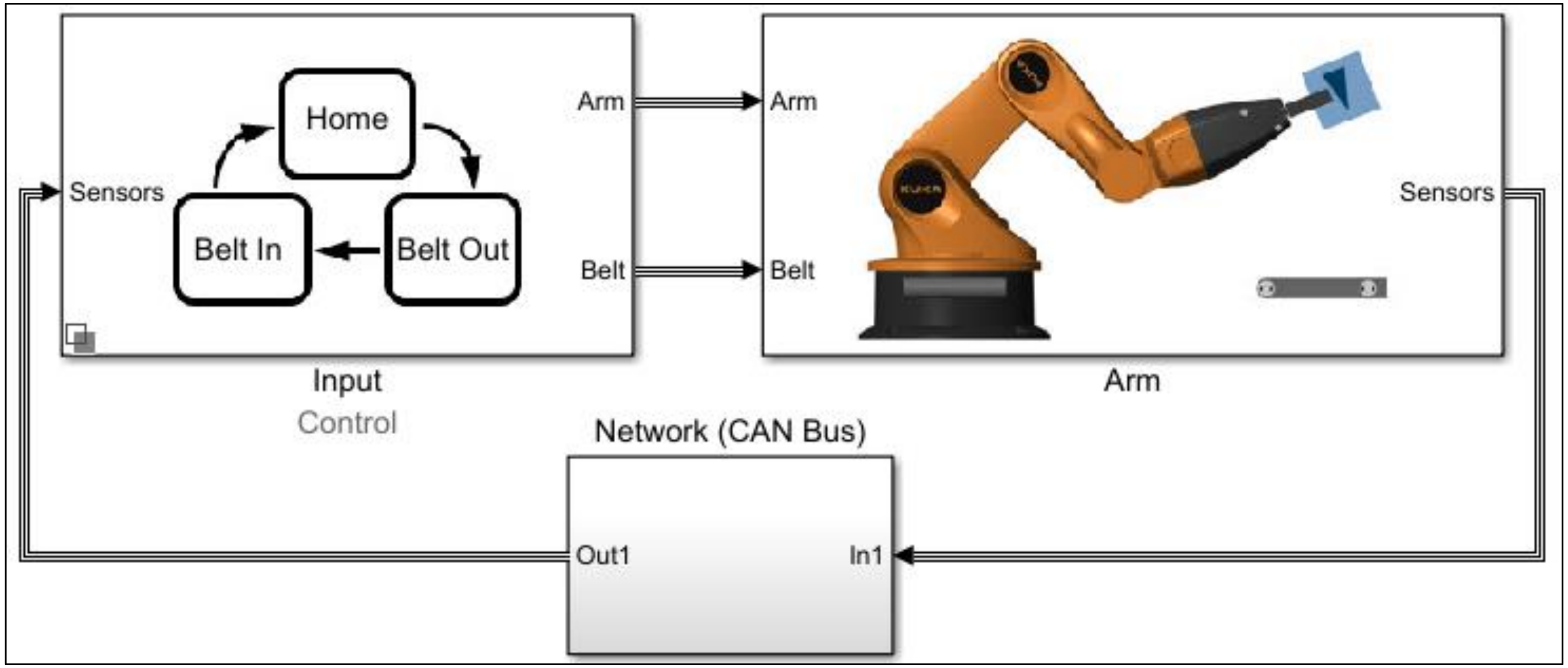
组件设计

测试

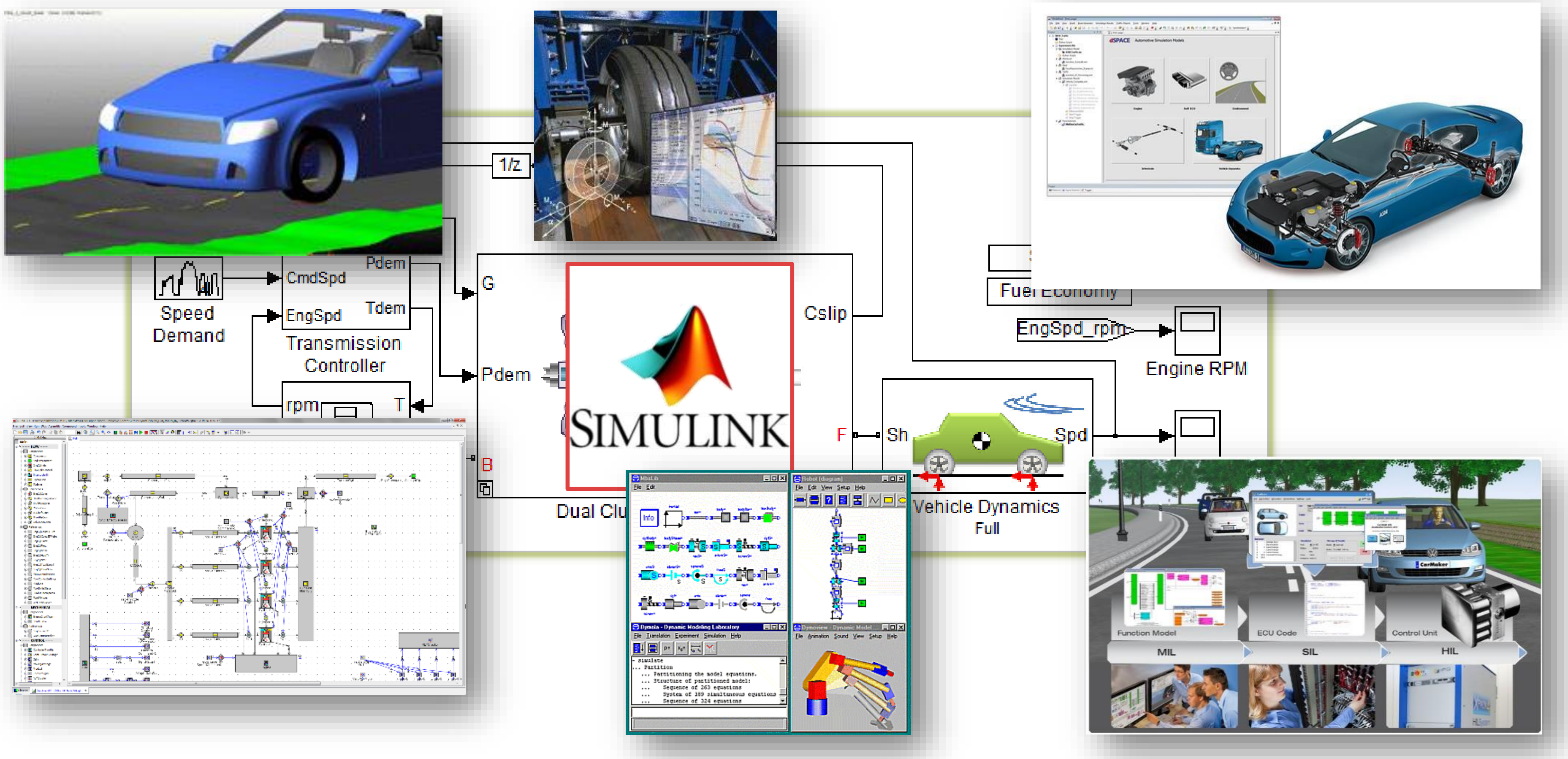
实现构建

虚拟样机示例

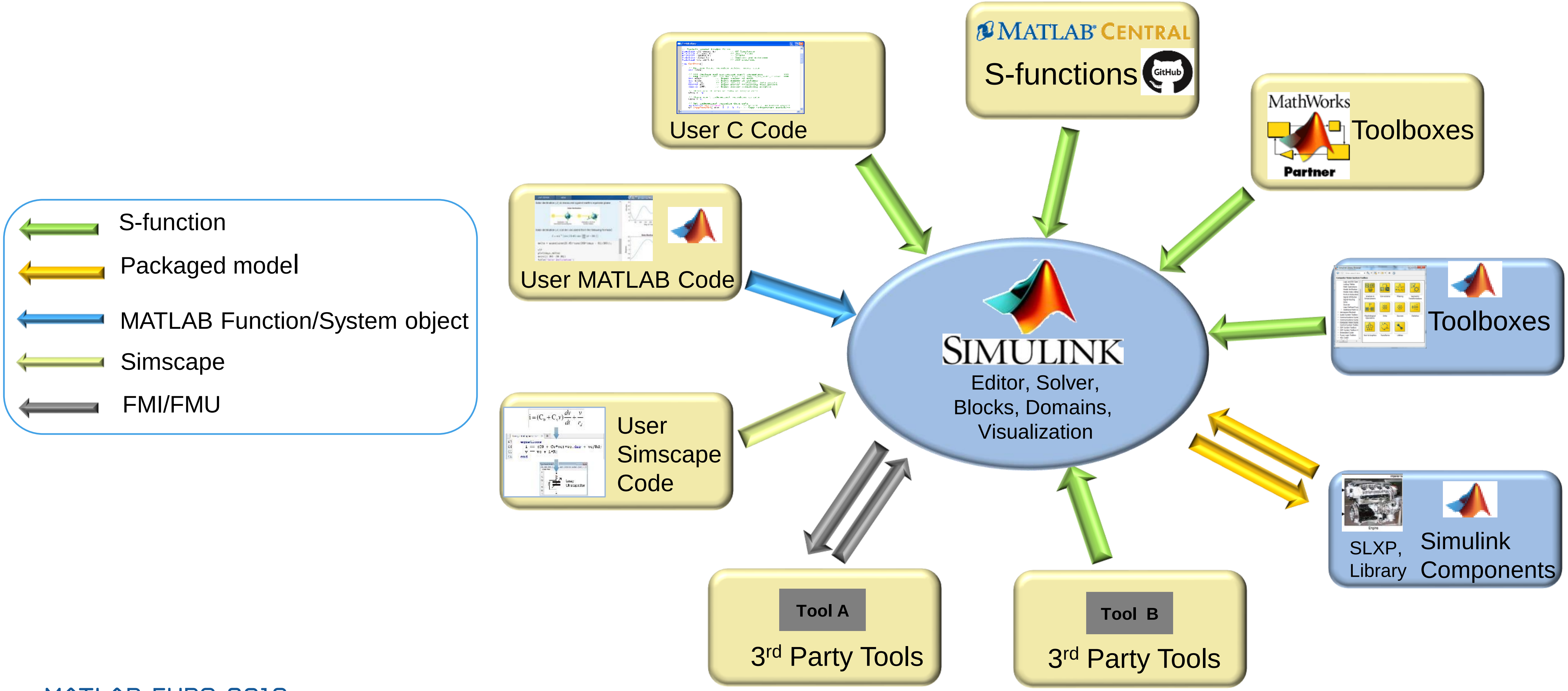
- 控制
  - ✓ 逻辑
  - ✓ 算法
- 本体
  - ✓ 机械
  - ✓ 电力电子
  - ✓ 液压
- 网络
  - ✓ 通信协议



包含第三方工具的虚拟样机模型



Simulink组件建模环境



S-function

Packaged model

MATLAB Function/System object

Simscape

FMI/FMU

User C Code

MATLAB CENTRAL

S-functions

GitHub

MathWorks Partner

Toolboxes

User MATLAB Code

SIMULINK

Editor, Solver, Blocks, Domains, Visualization

Toolboxes

User Simscape Code

SLXP, Library

Simulink Components

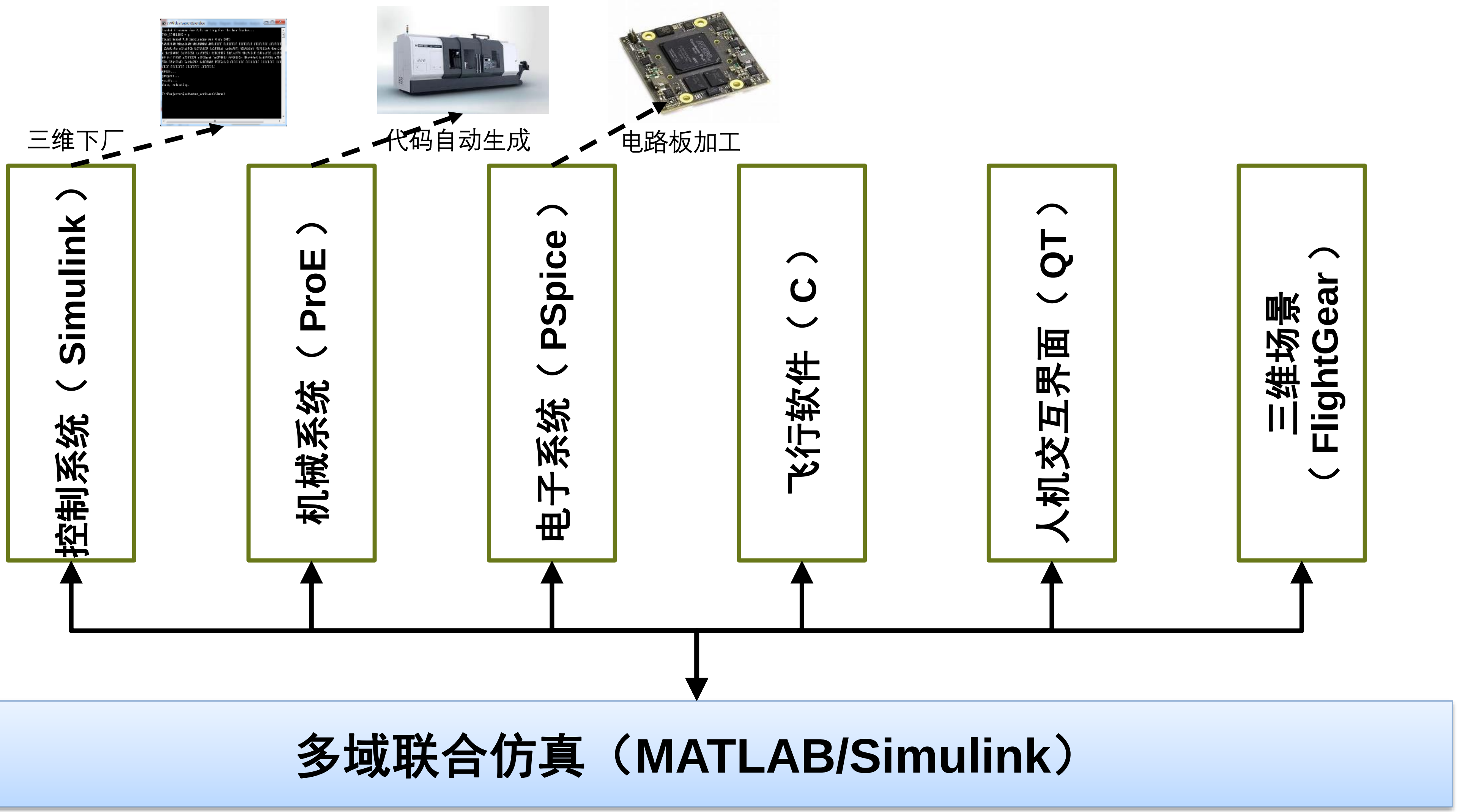
Tool A

3rd Party Tools

Tool B

3rd Party Tools

工具标准化



三维下厂

代码自动生成

电路板加工

控制系统（Simulink）

机械系统（ProE）

电子系统（PSpice）

飞行软件（C）

人机交互界面（QT）

三维场景（FlightGear）

多域联合仿真（MATLAB/Simulink）

基于事件的动态场景和性能分析

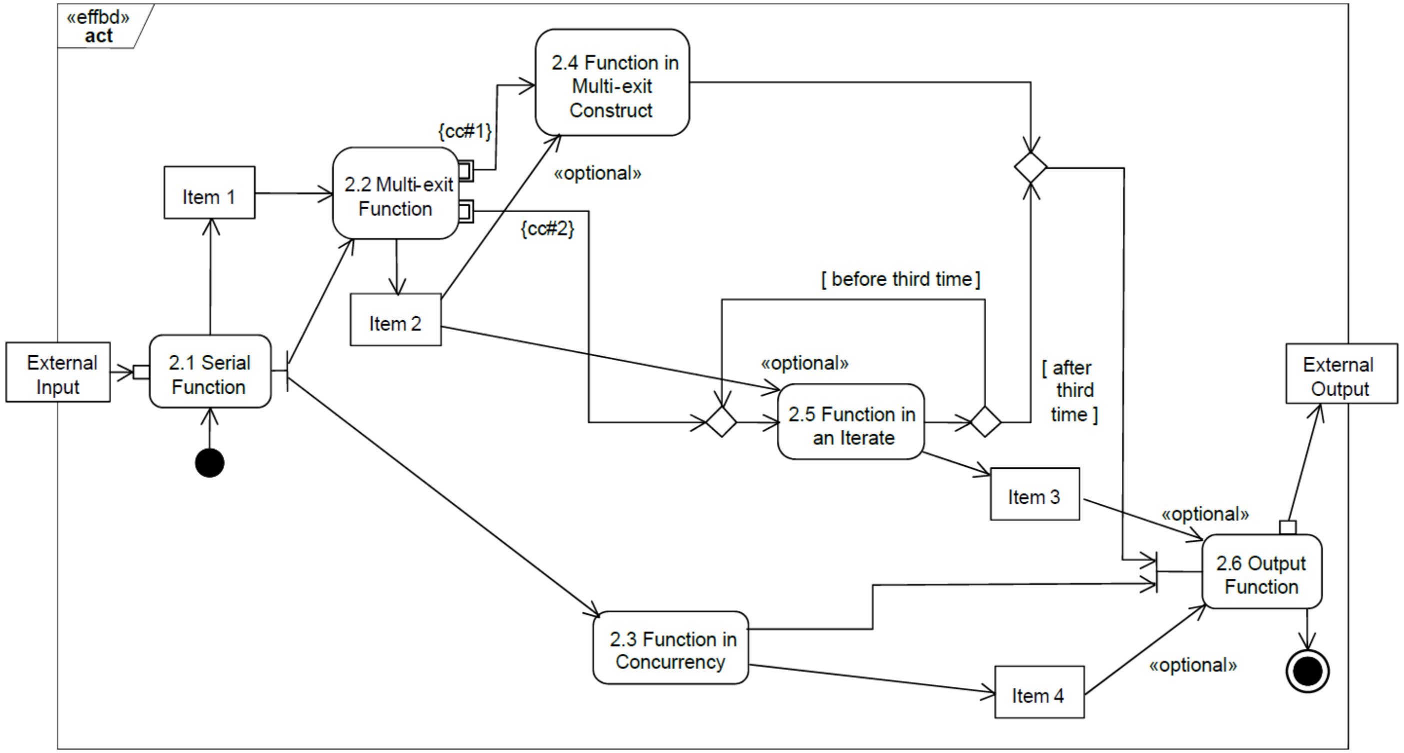
行为模型：基于EFFBD创建场景

INCOSE
International Council on Systems Engineering

SysML EFFBD Profile

OMG SYSTEMS MODELING LANGUAGE SysML™

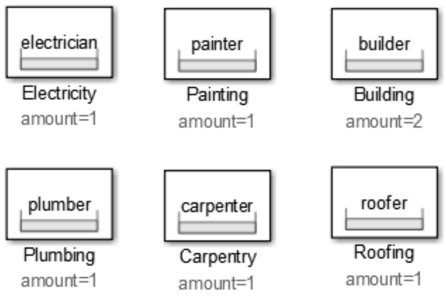
EFFBD - Enhanced Functional Flow Block Diagram



Aligning SysML with Classical Systems Engineering Techniques

住宅建造过程示例– 死锁

有限的资源:



electrician
Electricity
amount=1

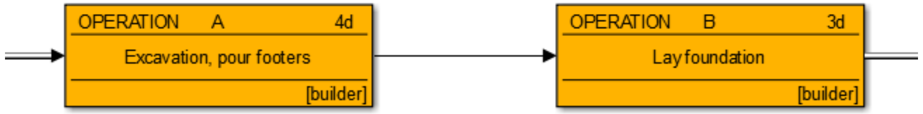
painter
Painting
amount=1

builder
Building
amount=2

plumber
Plumbing
amount=1

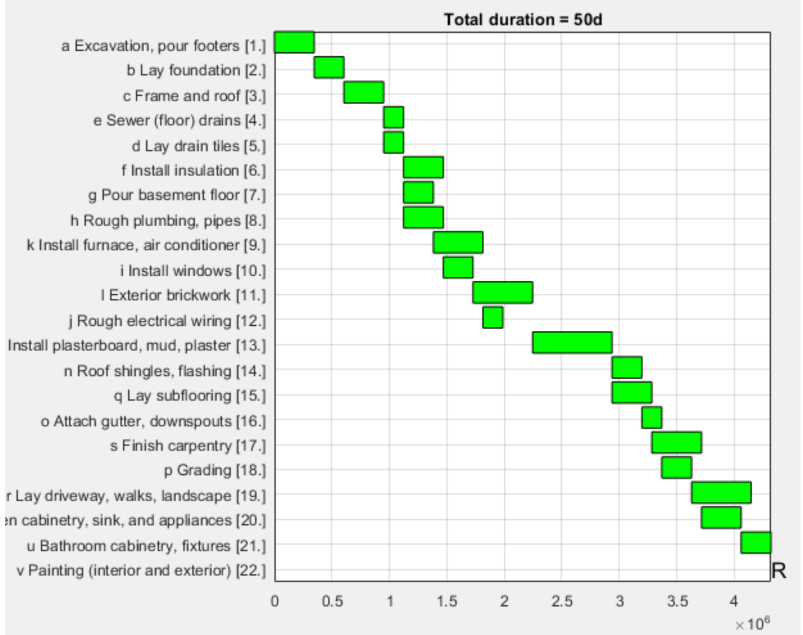
carpenter
Carpentry
amount=1

roofer
Roofing
amount=1

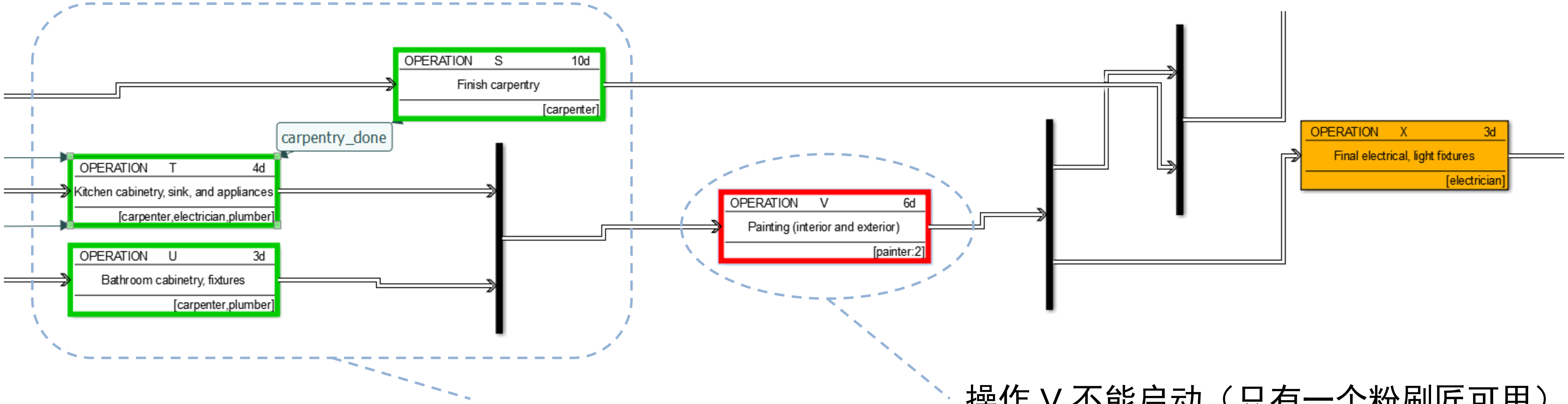


OPERATION A 4d
Excavation, pour footers
[builder]

OPERATION B 3d
Lay foundation
[builder]



定制的动画可以定位死锁:



OPERATION S 10d
Finish carpentry
[carpenter]

carpentry_done

OPERATION T 4d
Kitchen cabinetry, sink, and appliances
[carpenter,electrician,plumber]

OPERATION U 3d
Bathroom cabinetry, fixtures
[carpenter,plumber]

OPERATION V 6d
Painting (interior and exterior)
[painter:2]

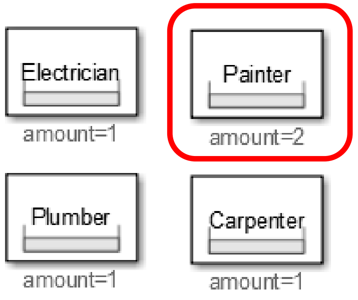
OPERATION X 3d
Final electrical, light fixtures
[electrician]

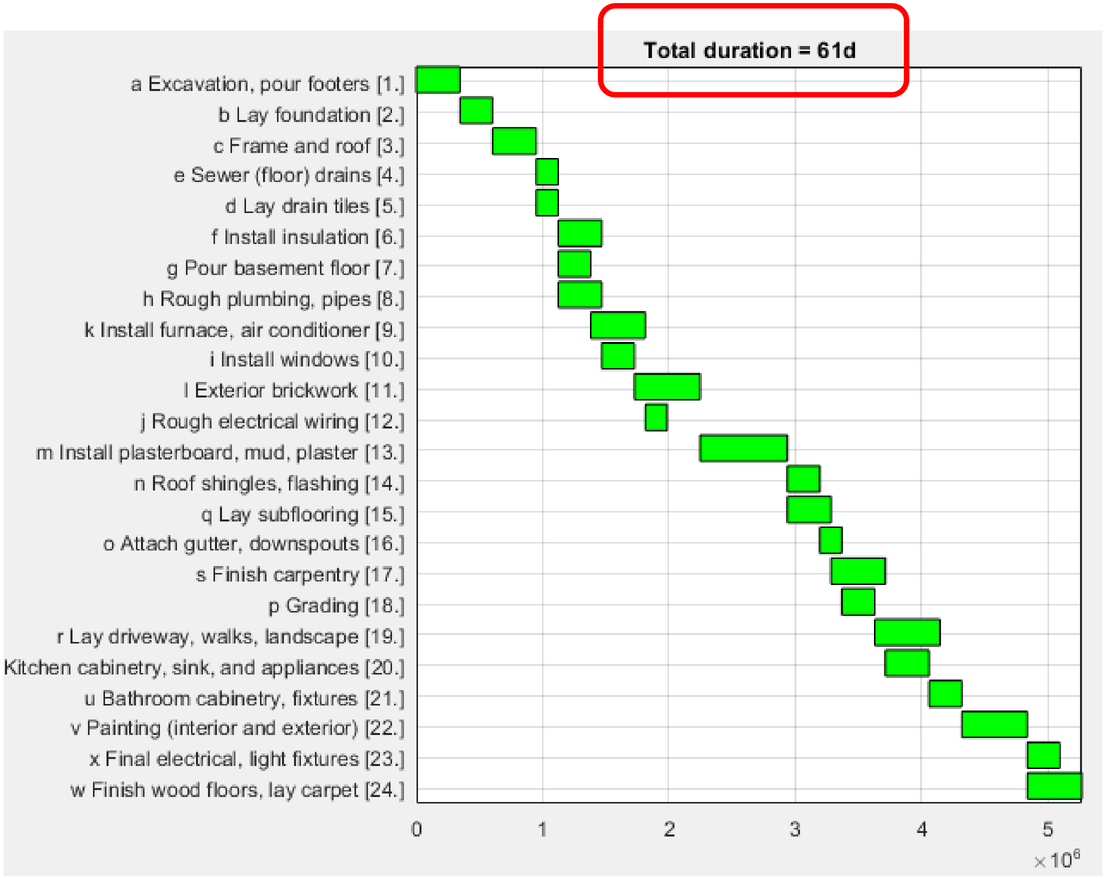
操作 S, T 和 U已完成

操作 V 不能启动（只有一个粉刷匠可用）

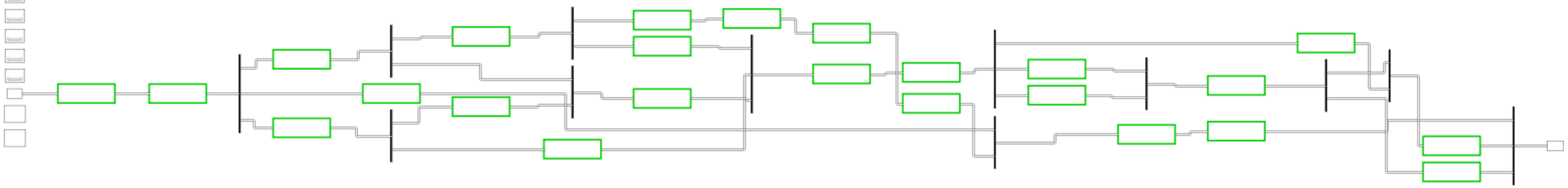
住宅建造过程示例– 仿真

有限的资源:

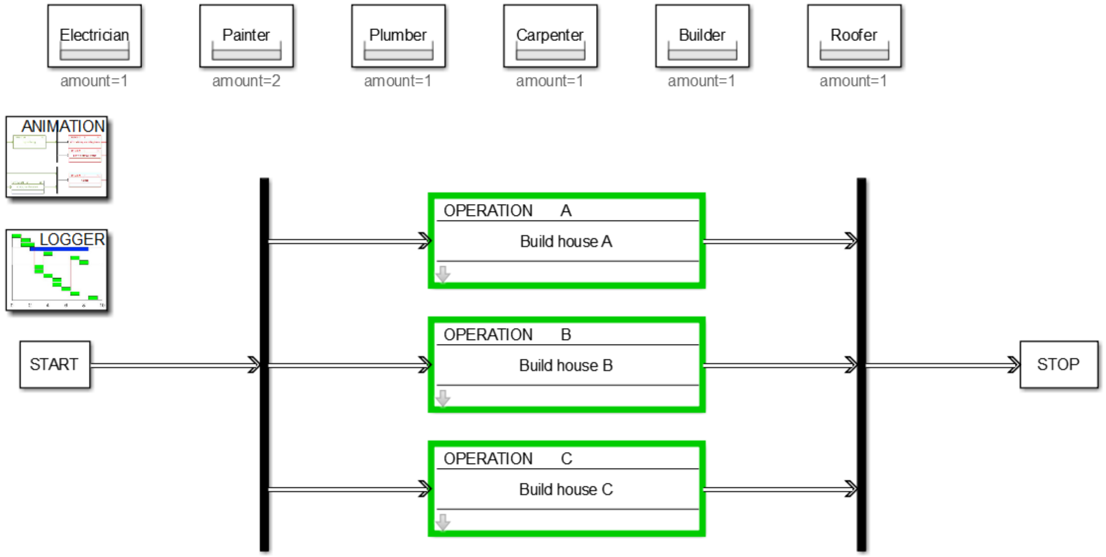


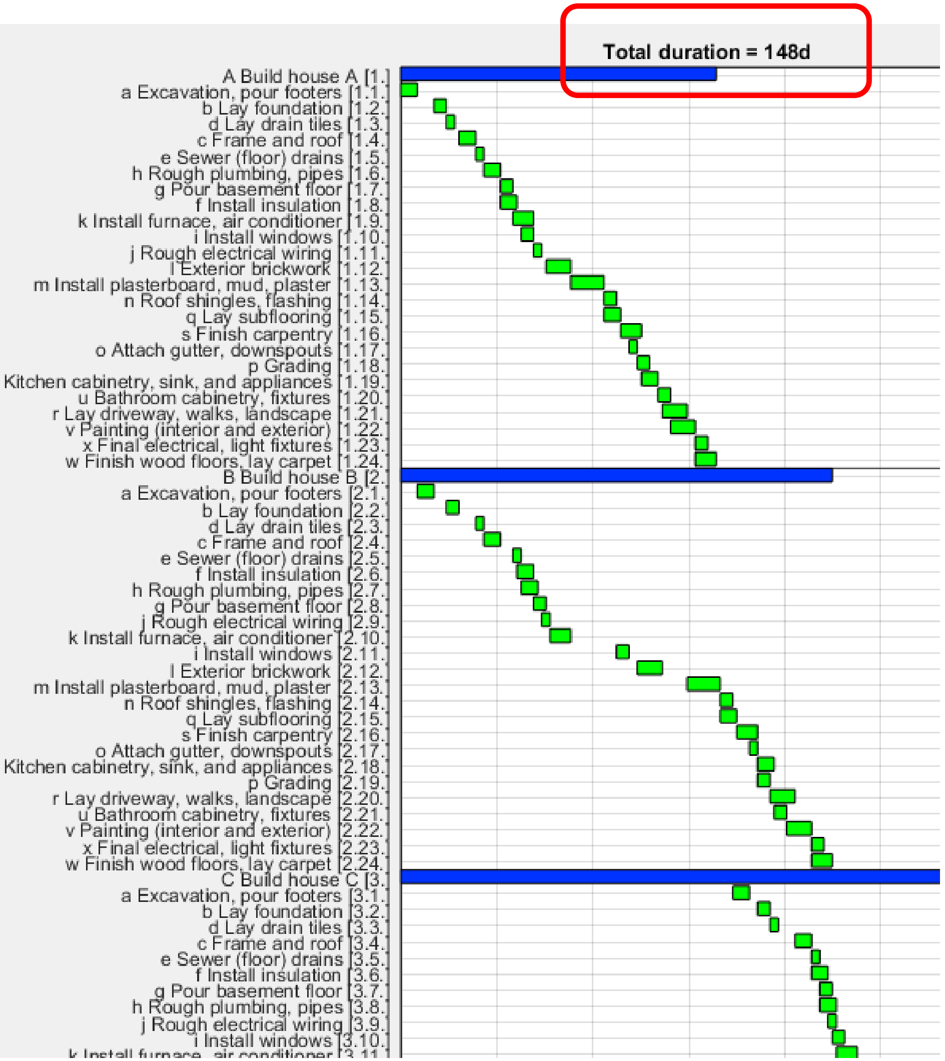


仿真表明建造一栋房子需要61天



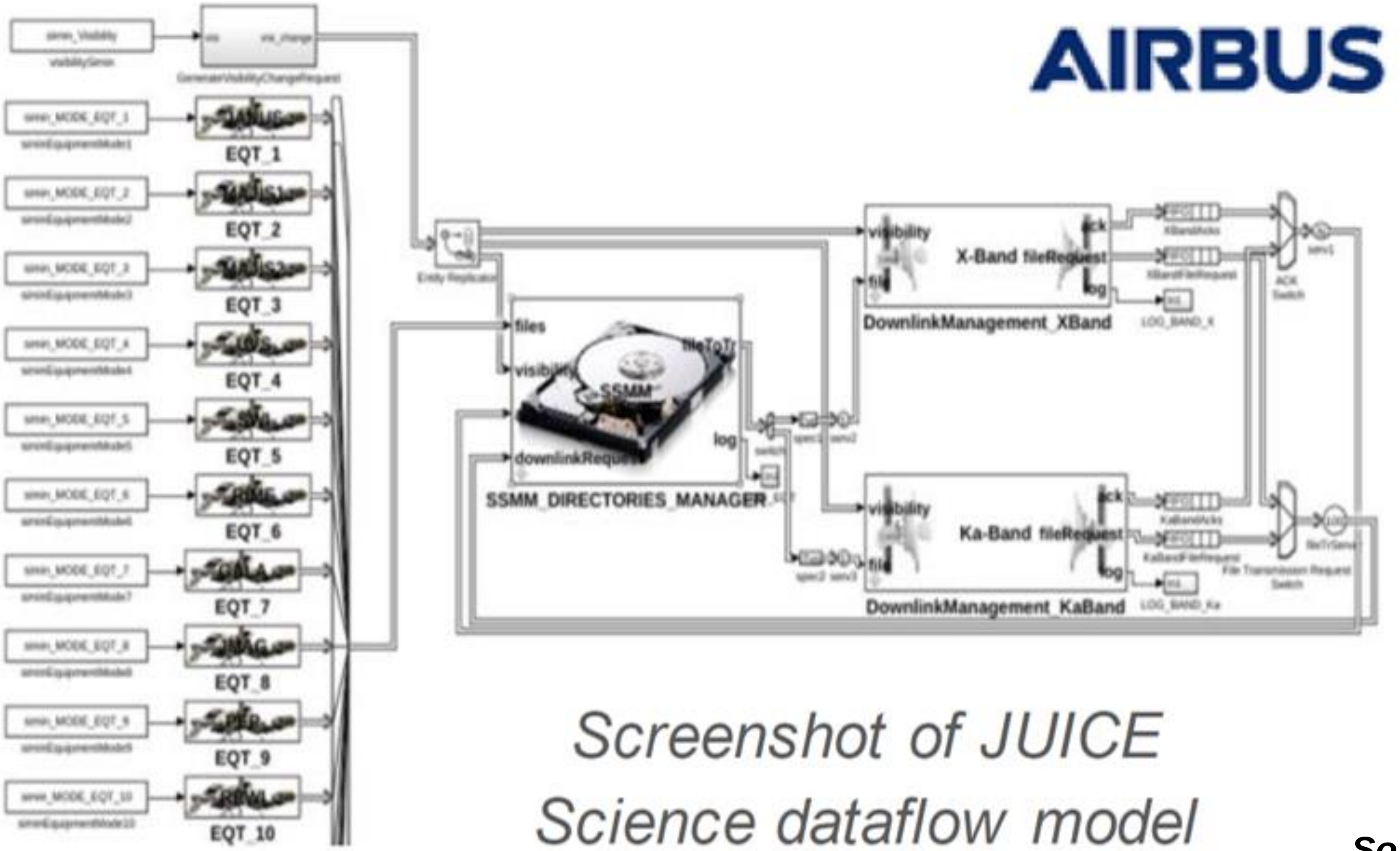
住宅建造过程示例–
同样的资源建造3座房子会是什么情况?





仿真表明建造3栋房子需要148天

数据流模型

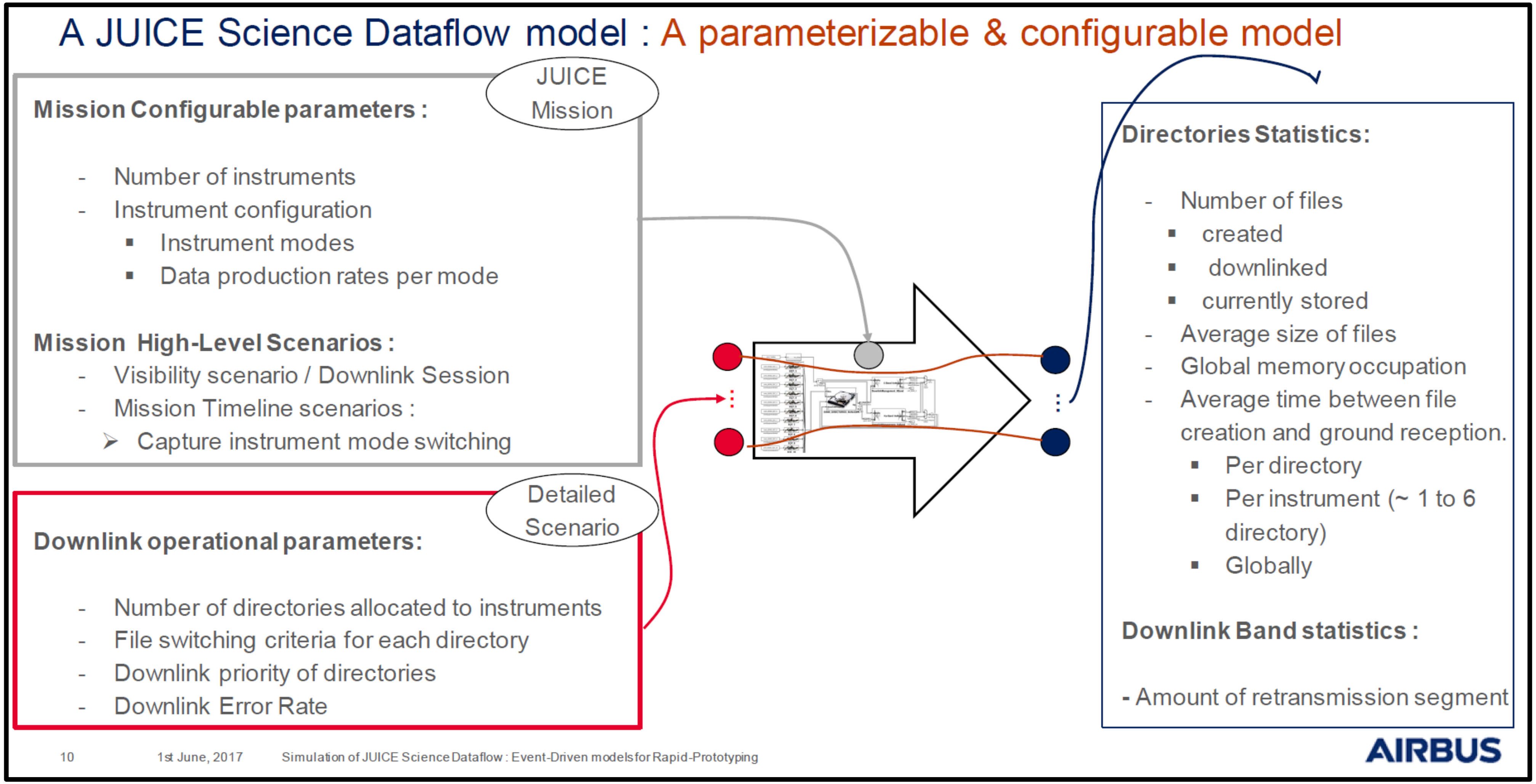


Screenshot of JUICE Science dataflow model

Artist's impression of the JUICE mission.
Credit: ESA/AOES

AIRBUS

Source: Conference DASIA 2017



A JUICE Science Dataflow model : A parameterizable & configurable model

JUICE Mission

Mission Configurable parameters :

- Number of instruments
- Instrument configuration
  - Instrument modes
  - Data production rates per mode

Mission High-Level Scenarios :

- Visibility scenario / Downlink Session
- Mission Timeline scenarios :
  - ➢ Capture instrument mode switching

Detailed Scenario

Downlink operational parameters:

- Number of directories allocated to instruments
- File switching criteria for each directory
- Downlink priority of directories
- Downlink Error Rate

Directories Statistics:

- Number of files
  - created
  - downlinked
  - currently stored
- Average size of files
- Global memory occupation
- Average time between file creation and ground reception.
  - Per directory
  - Per instrument (~ 1 to 6 directory)
  - Globally

Downlink Band statistics :

- Amount of retransmission segment

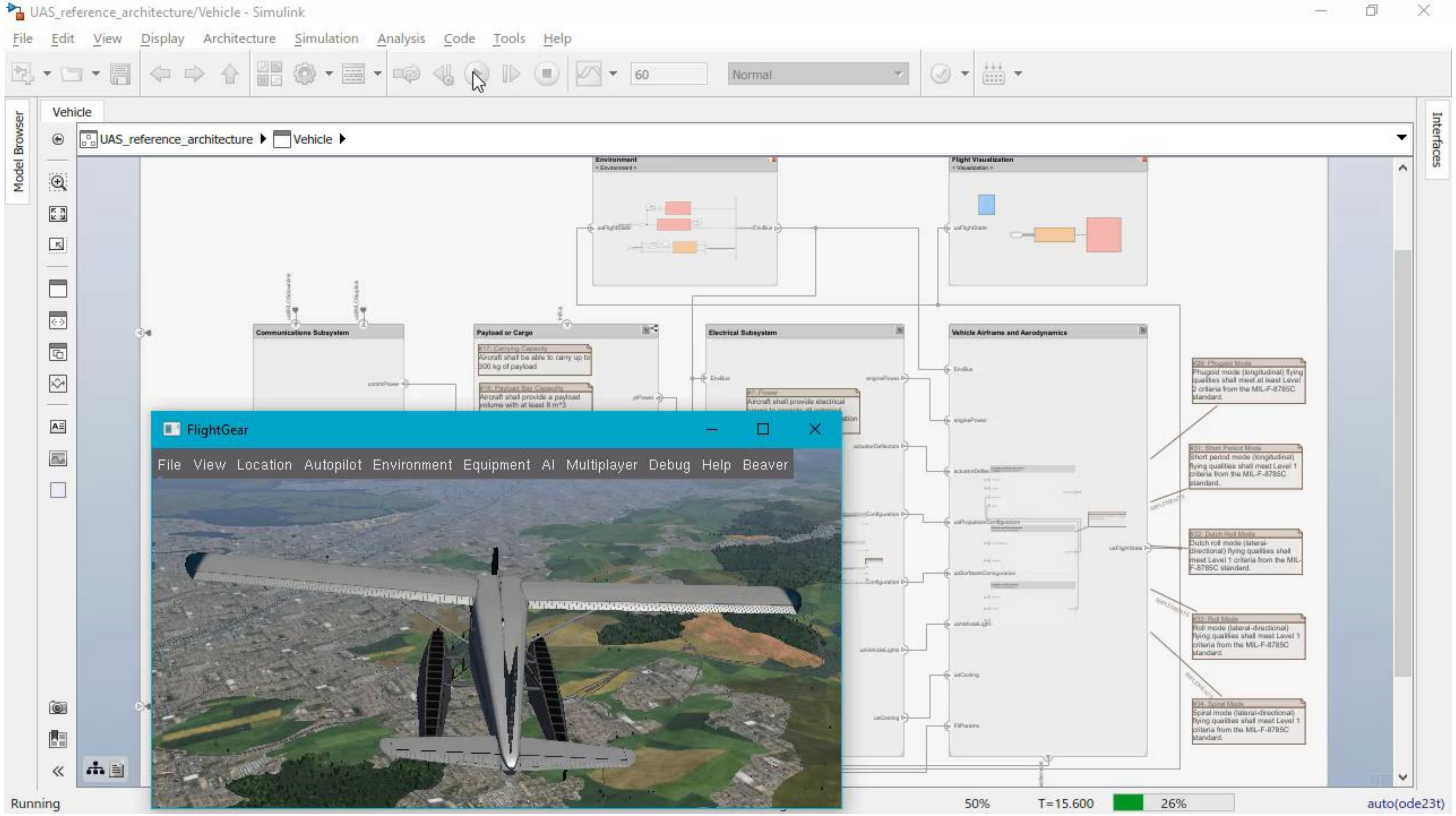
10 1st June, 2017 Simulation of JUICE Science Dataflow : Event-Driven models for Rapid-Prototyping AIRBUS

- “场景可以作为最终产品验证/测试场景的输入”
- “这个快速原型模拟器将有助于定义最终的操作模拟器和程序”
- “场景 : **15 天的任务**(14个可见阶段) → 仿真时间: **< 5 min** ”

Source: Conference DASIA 2017

面向产品级软件的架构设计和需求管理

系统级模型的仿真



#17: Carrying Capacity
Aircraft shall be able to carry up to 300 kg of payload

#18: Payload Bay Capacity
Aircraft shall provide a payload volume with at least 8 m^3

#7: Power
Aircraft shall provide electrical power to operate all onboard ... ation

#29: Phugoid Mode
Phugoid mode (longitudinal) flying qualities shall meet at least Level 2 criteria from the MIL-F-8785C standard.

#31: Short Period Mode
Short period mode (longitudinal) flying qualities shall meet Level 1 criteria from the MIL-F-8785C standard.

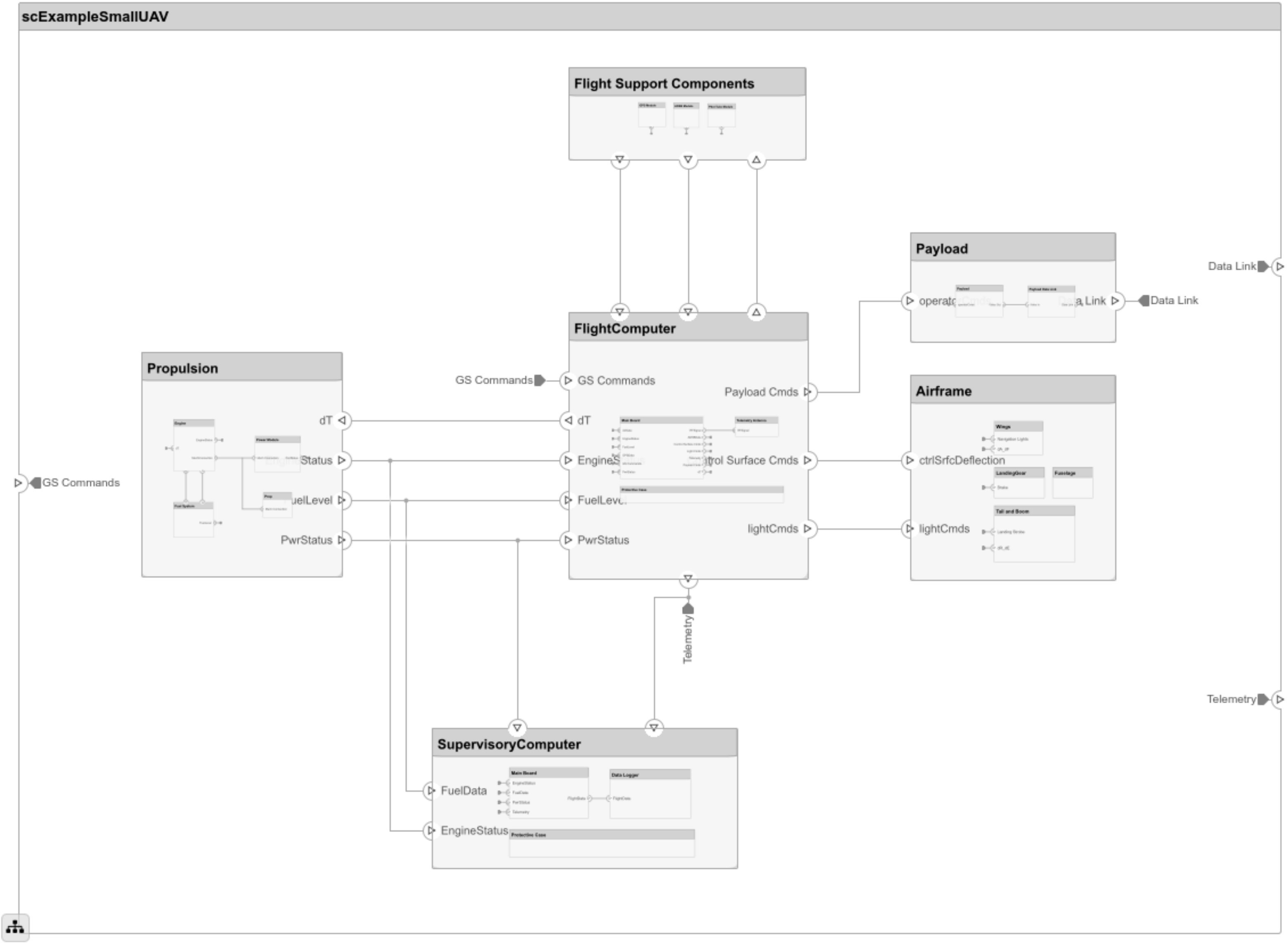
#32: Dutch Roll Mode
Dutch roll mode (lateral-directional) flying qualities shall meet Level 1 criteria from the MIL-F-8785C standard.

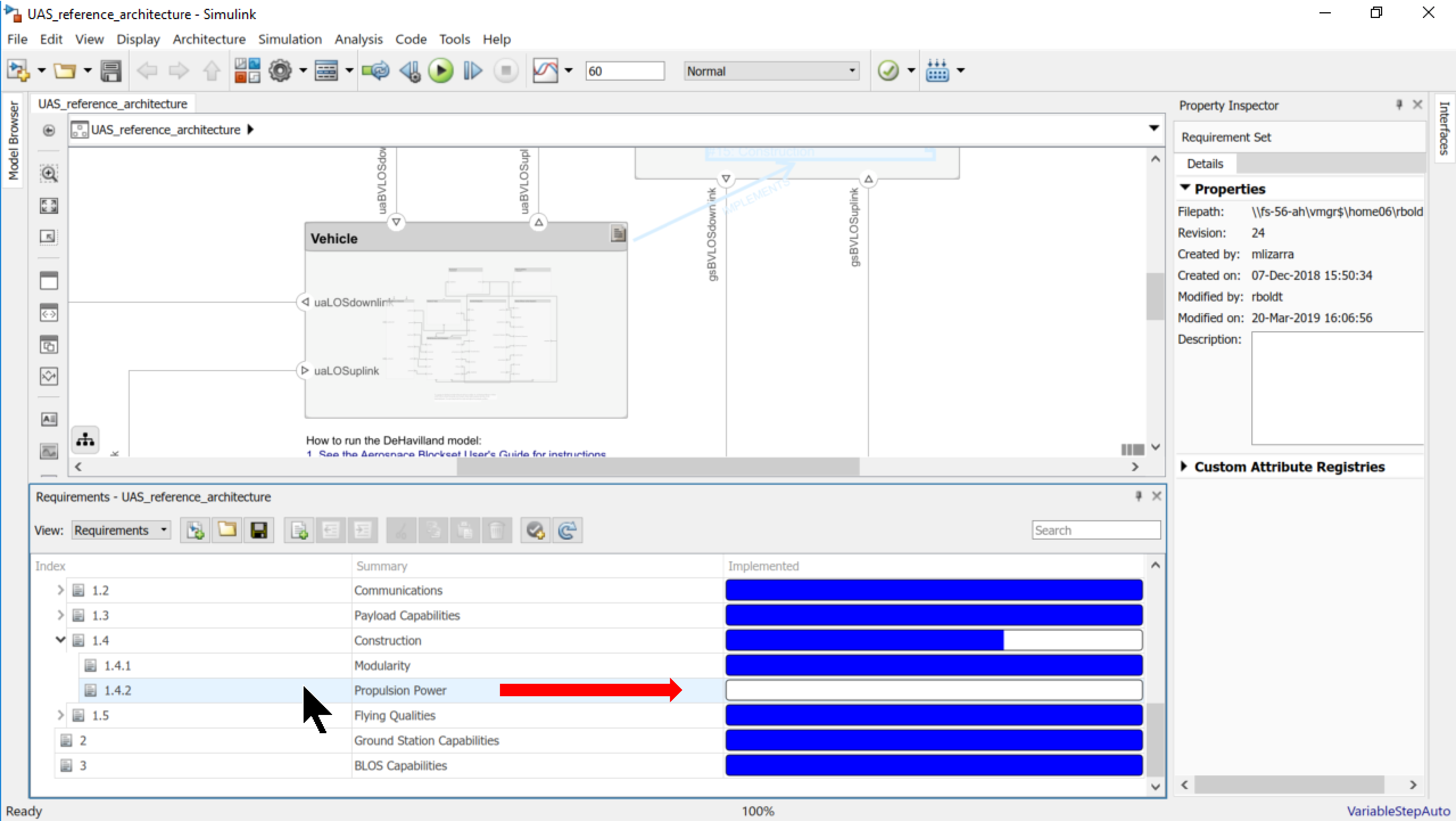
#33: Roll Mode
Roll mode (lateral-directional) flying qualities shall meet Level 1 criteria from the MIL-F-8785C standard.

#34: Spiral Mode
Spiral mode (lateral-directional) flying qualities shall meet Level 1 criteria from the MIL-F-8785C standard.

小型UAV的架构

- 接口
- 需求
- 配置及模板
- 分析





How to run the DeHavilland model:

1. See the Aerospace Blockset User's Guide for instructions

Requirements - UAS_reference_architecture

Index	Summary	Implemented
1.2	Communications	
1.3	Payload Capabilities	
1.4	Construction	
1.4.1	Modularity	
1.4.2	Propulsion Power	
1.5	Flying Qualities	
2	Ground Station Capabilities	
3	BLOS Capabilities	

Property Inspector

Requirement Set

Filepath: \\fs-56-ah\vmgr$\home06\rbold

Revision: 24

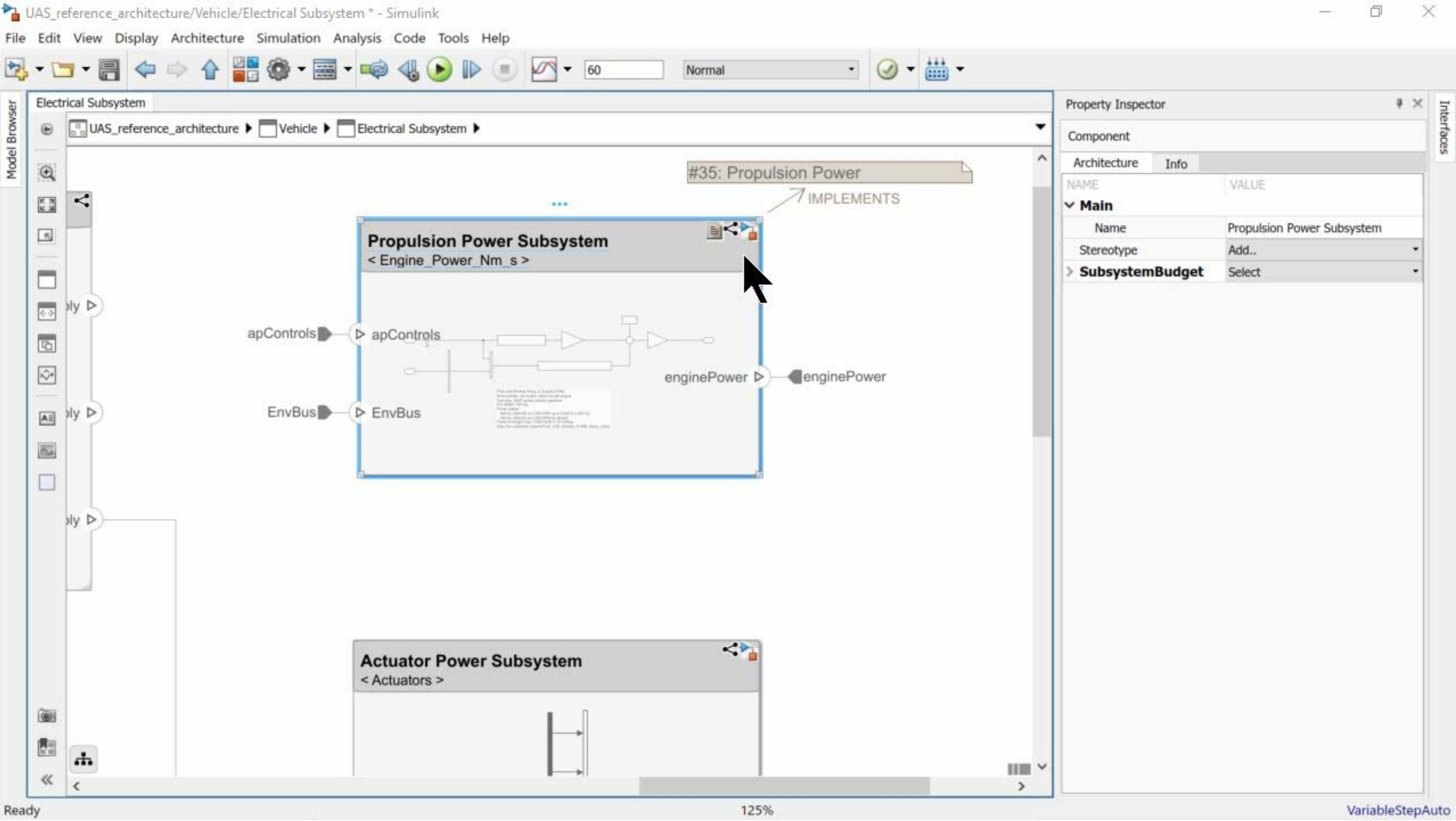
Created by: mlizarra

Created on: 07-Dec-2018 15:50:34

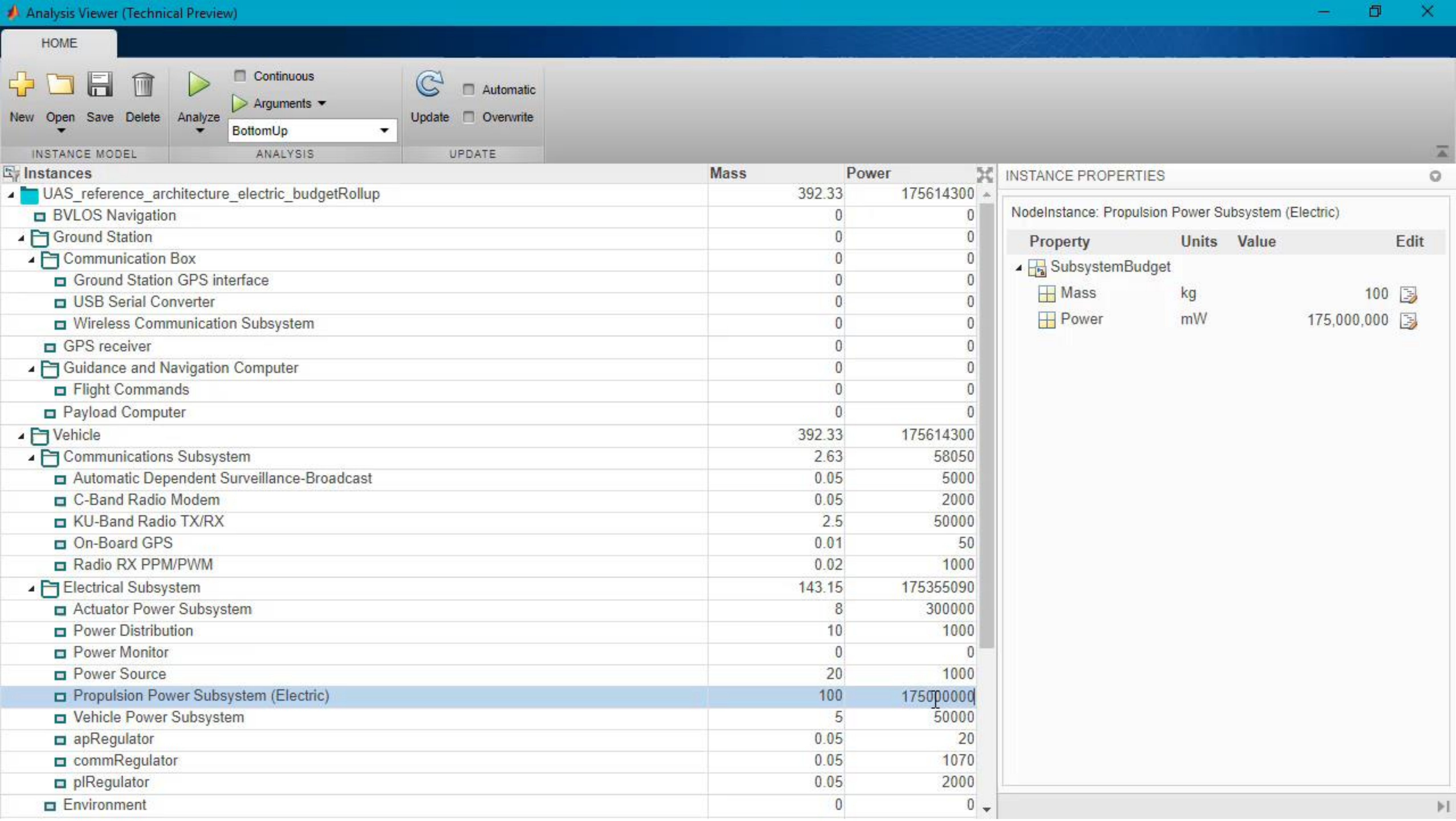
Modified by: rboldt

Modified on: 20-Mar-2019 16:06:56

Description:



NAME	VALUE
Main	
Name	Propulsion Power Subsystem
Stereotype	Add..
SubsystemBudget	Select



Instances	Mass	Power
UAS_reference_architecture_electric_budgetRollup	392.33	175614300
BVLOS Navigation	0	0
Ground Station	0	0
Communication Box	0	0
Ground Station GPS interface	0	0
USB Serial Converter	0	0
Wireless Communication Subsystem	0	0
GPS receiver	0	0
Guidance and Navigation Computer	0	0
Flight Commands	0	0
Payload Computer	0	0
Vehicle	392.33	175614300
Communications Subsystem	2.63	58050
Automatic Dependent Surveillance-Broadcast	0.05	5000
C-Band Radio Modem	0.05	2000
KU-Band Radio TX/RX	2.5	50000
On-Board GPS	0.01	50
Radio RX PPM/PWM	0.02	1000
Electrical Subsystem	143.15	175355090
Actuator Power Subsystem	8	300000
Power Distribution	10	1000
Power Monitor	0	0
Power Source	20	1000
Propulsion Power Subsystem (Electric)	100	175000000
Vehicle Power Subsystem	5	50000
apRegulator	0.05	20
commRegulator	0.05	1070
plRegulator	0.05	2000
Environment	0	0

INSTANCE PROPERTIES

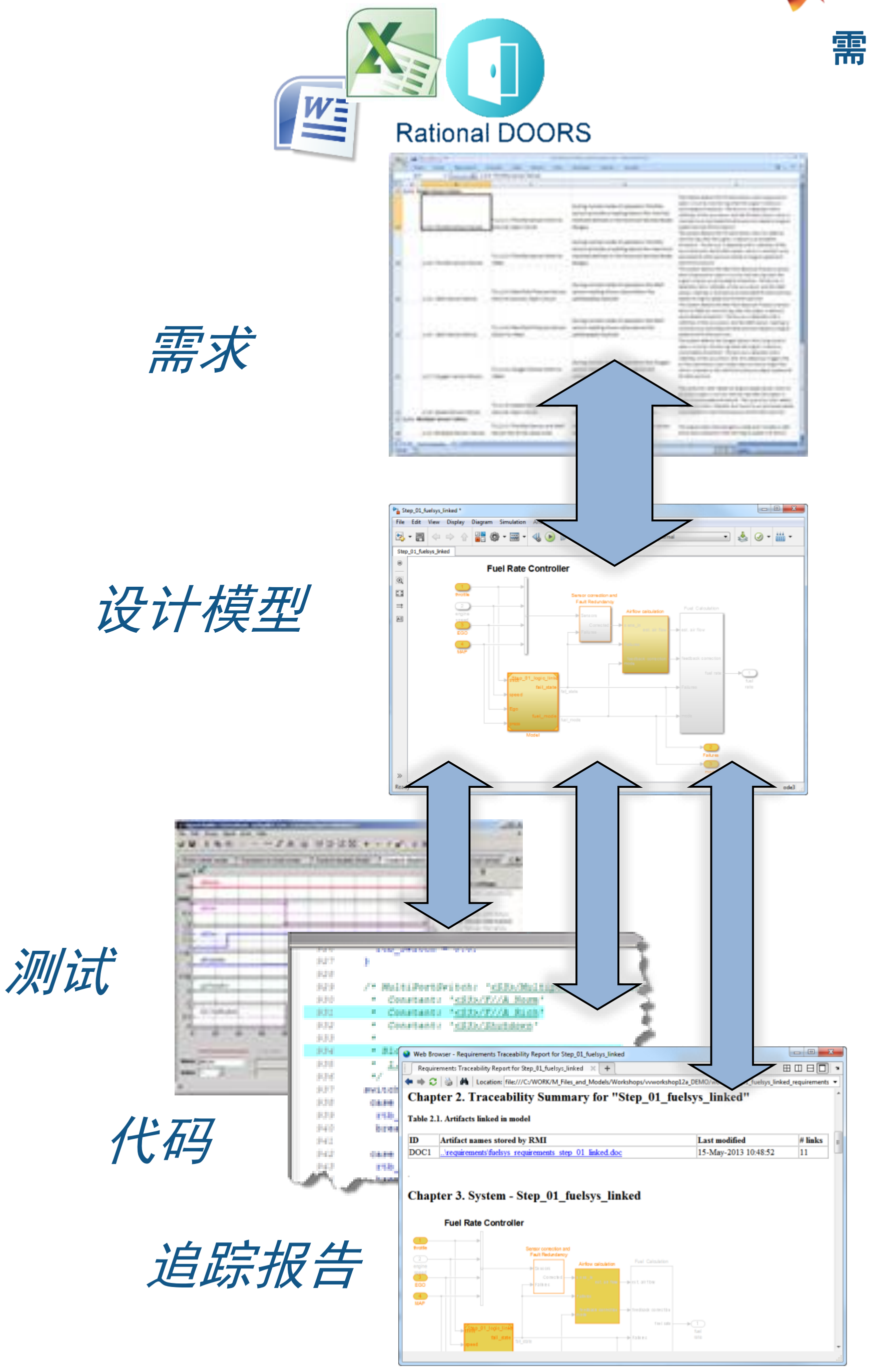
NodeInstance: Propulsion Power Subsystem (Electric)

Property	Units	Value	Edit
SubsystemBudget			
Mass	kg	100	
Power	mW	175,000,000	

面向产品级软件的测试验证框架

验证和确认框架
需求

- 设计工件之间的可追溯性
  - 需求管理接口
  - 在Simulink环境下编辑和同步需求
- 建立链接：
  - 系统需求
  - 设计，接口描述
  - 变更申请
  - 代码
- 标准和认证的报告
  - ISO 26262, IEC 61508, DO-xxx
  - 其它工业标准(CMMI, SPICE, 等等)


Rational DOORS
需求
设计模型
Fuel Rate Controller
测试
代码
追踪报告
Web Browser - Requirements Traceability Report for Step_01_fuelsys_linked
Requirements Traceability Report for Step_01_fuelsys_linked
Location: file:///C:/WORK/M_Files_and_Models/Workshops/vvworkshop12a_DEMO/w... fuelsys_linked_requirements

Chapter 2. Traceability Summary for "Step_01_fuelsys_linked"

Table 2.1. Artifacts linked in model

ID	Artifact names stored by RMI	Last modified	# links
DOC1	..\requirements\fuelsys_requirements_step_01_linked.doc	15-May-2013 10:48:52	11

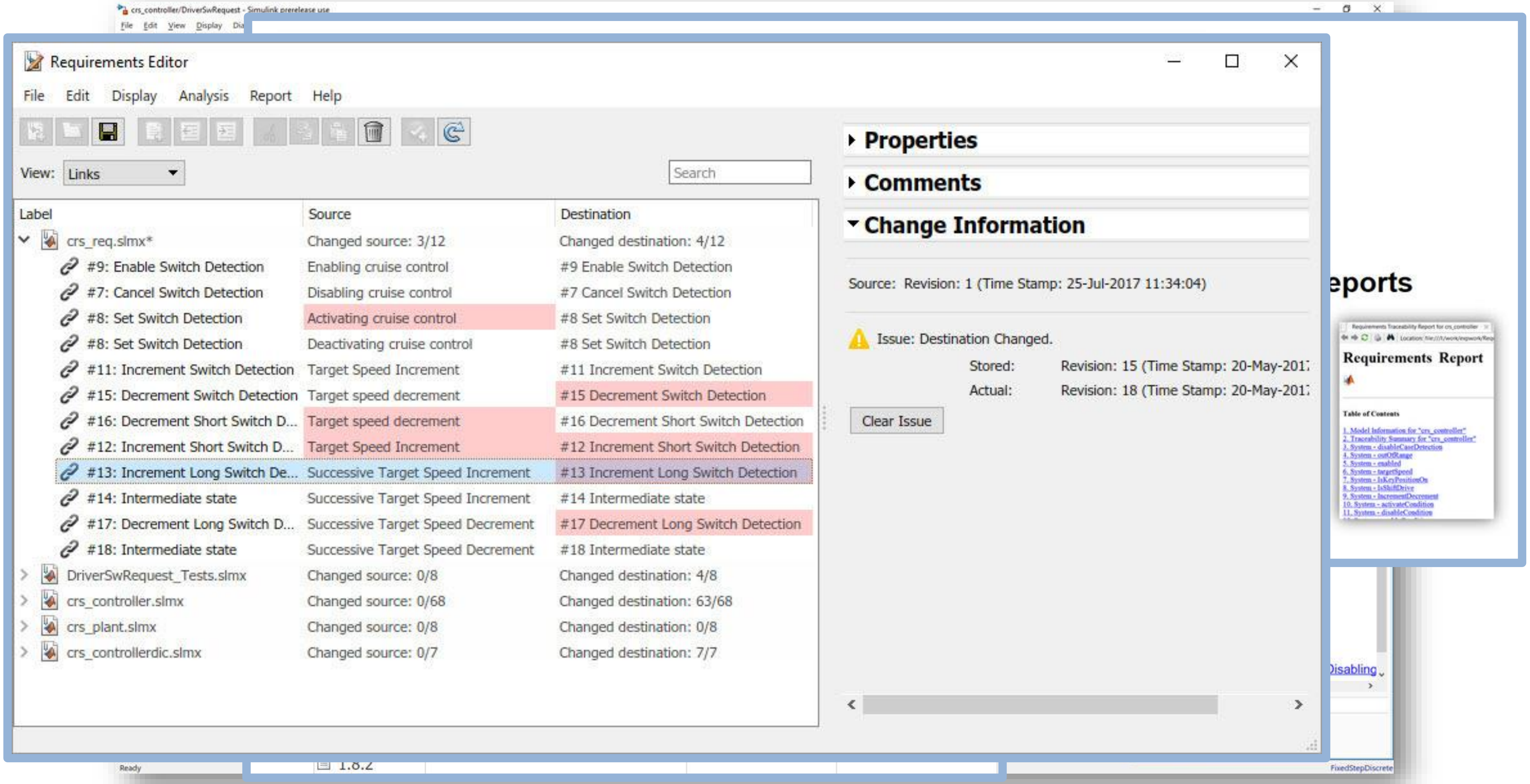
Chapter 3. System - Step_01_fuelsys_linked

Fuel Rate Controller

验证和确认框架

验证和确认框架

需求



Label	Source	Destination
crs_req.slmx*	Changed source: 3/12	Changed destination: 4/12
#9: Enable Switch Detection	Enabling cruise control	#9 Enable Switch Detection
#7: Cancel Switch Detection	Disabling cruise control	#7 Cancel Switch Detection
#8: Set Switch Detection	Activating cruise control	#8 Set Switch Detection
#8: Set Switch Detection	Deactivating cruise control	#8 Set Switch Detection
#11: Increment Switch Detection	Target Speed Increment	#11 Increment Switch Detection
#15: Decrement Switch Detection	Target speed decrement	#15 Decrement Switch Detection
#16: Decrement Short Switch D...	Target speed decrement	#16 Decrement Short Switch Detection
#12: Increment Short Switch D...	Target Speed Increment	#12 Increment Short Switch Detection
#13: Increment Long Switch De...	Successive Target Speed Increment	#13 Increment Long Switch Detection
#14: Intermediate state	Successive Target Speed Increment	#14 Intermediate state
#17: Decrement Long Switch D...	Successive Target Speed Decrement	#17 Decrement Long Switch Detection
#18: Intermediate state	Successive Target Speed Decrement	#18 Intermediate state
DriverSwRequest_Tests.slmx	Changed source: 0/8	Changed destination: 4/8
crs_controller.slmx	Changed source: 0/68	Changed destination: 63/68
crs_plant.slmx	Changed source: 0/8	Changed destination: 0/8
crs_controllerdic.slmx	Changed source: 0/7	Changed destination: 7/7

Source: Revision: 1 (Time Stamp: 25-Jul-2017 11:34:04)

Issue: Destination Changed.

Stored: Revision: 15 (Time Stamp: 20-May-201

Actual: Revision: 18 (Time Stamp: 20-May-201

Requirements Traceability Report for crs_controller

Location: file:///I:/work/reqwork/Req

Requirements Report

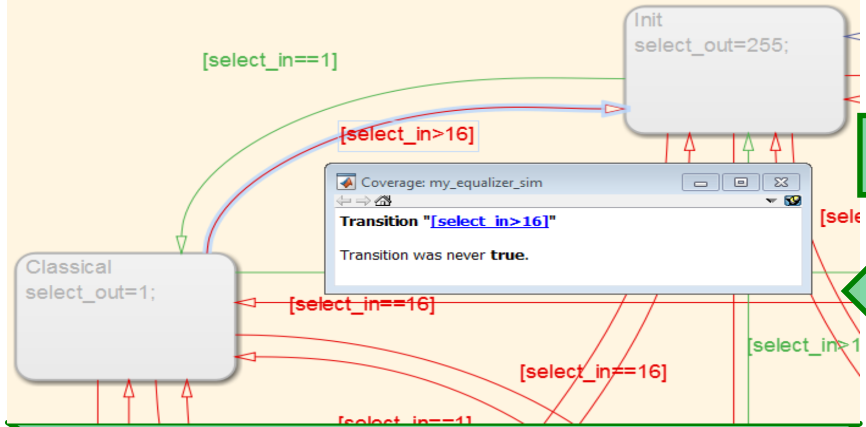
Table of Contents

1. Model Information for "crs_controller"
2. Traceability Summary for "crs_controller"
3. System - disableCaseDetection
4. System - outOfRange
5. System - enabled
6. System - targetSpeed
7. System - IsKeyPositionOn
8. System - IsShiftDrive
9. System - IncrementDecrement
10. System - activateCondition
11. System - disableCondition

验证和确认框架

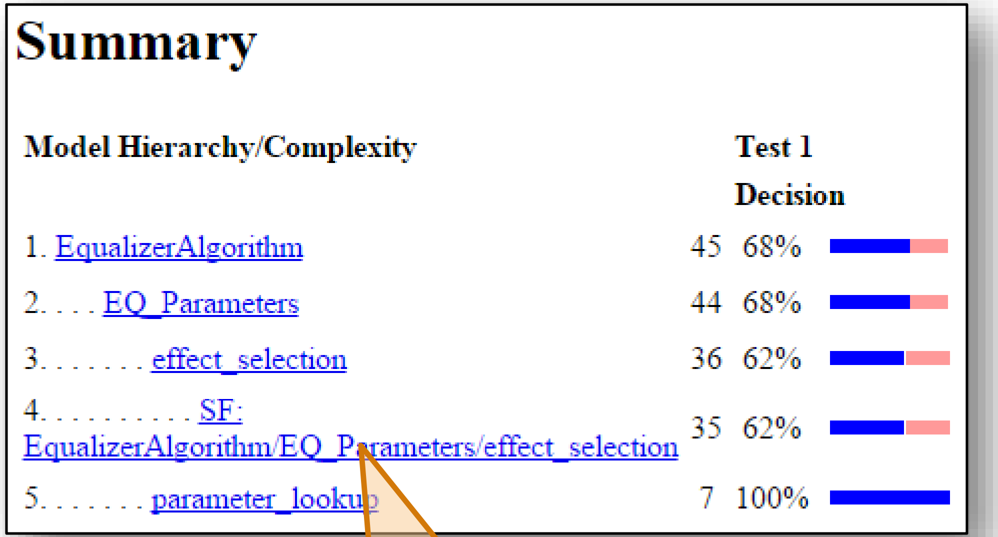
验证和确认框架

模型和代码覆盖分析



Transition "[select_in>16]"

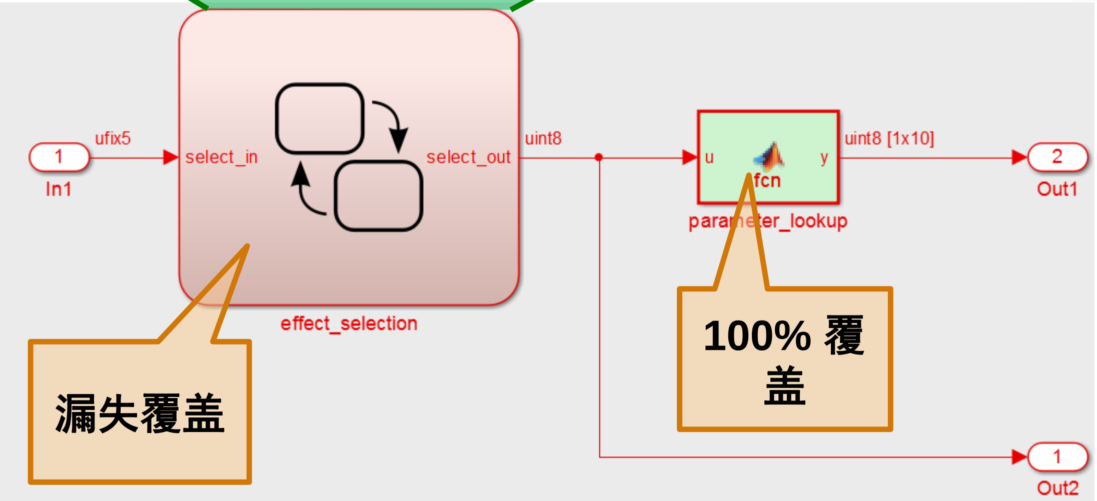
Transition was never true.



Summary

Model Hierarchy/Complexity		Test 1 Decision
1. EqualizerAlgorithm	45	68%
2. . . . EQ_Parameters	44	68%
3. . . . . . . effect_selection	36	62%
4. . . . . SF: EqualizerAlgorithm/EQ_Parameters/effect_selection	35	62%
5. . . . . . . parameter_lookup	7	100%

自动收集和生成测试覆盖报告



漏失覆盖

100% 覆盖

验证和确认框架

验证和确认框架

使用形式化方法识别设计错误

设计错误检测

- **发现**死逻辑和设计缺陷

测试用例生成

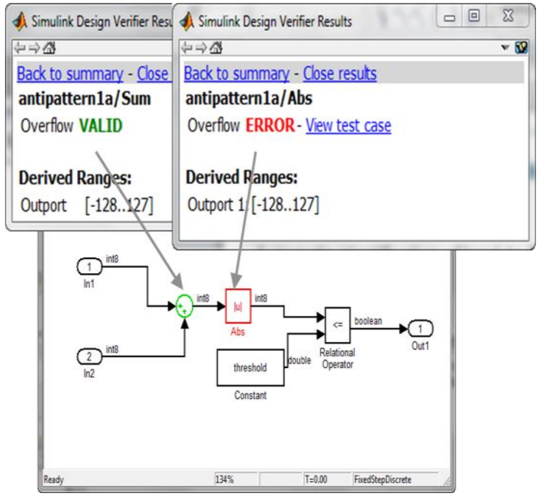
- **自动**生成用于完成覆盖分析的测试用例

需求证明

- **证明**正式设计符合需求

模型切片

- **简化**模型以隔离行为


Simulink Design Verifier Resu

Back to summary - Close

antipattern1a/Sum

Overflow VALID

Derived Ranges:

Outport [-128..127]

Simulink Design Verifier Results

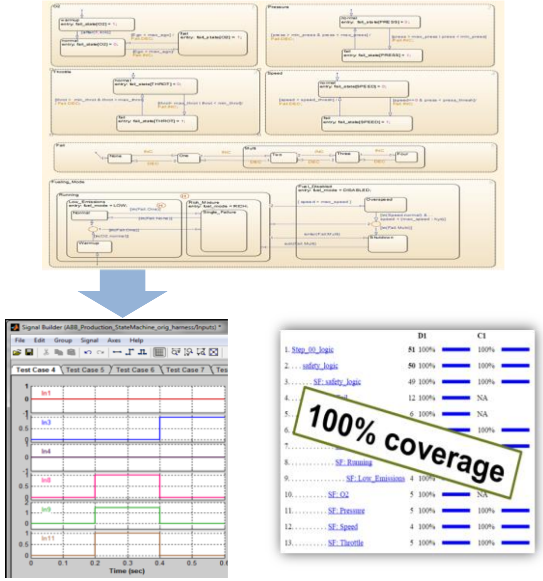
Back to summary - Close results

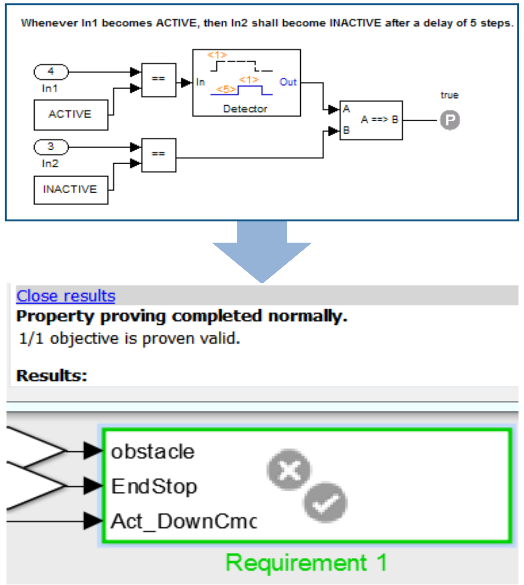
antipattern1a/Abs

Overflow ERROR - View test case

Derived Ranges:

Outport 1 [-128..127]



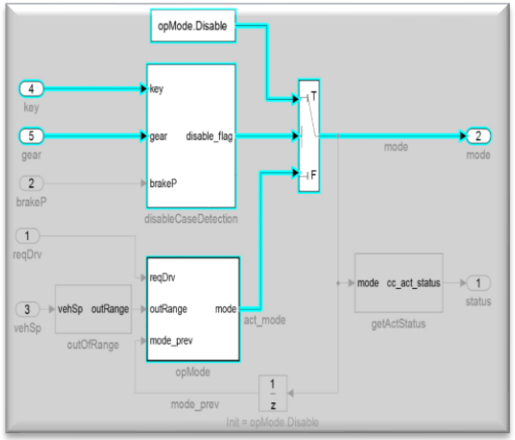

Whenever In1 becomes ACTIVE, then In2 shall become INACTIVE after a delay of 5 steps.

Close results

Property proving completed normally.

1/1 objective is proven valid.

Results:



验证和确认框架

验证和确认框架

为模型和生成的代码编写、执行和管理基于仿真的测试

Test Harnesses（测试套件）

- **隔离**待测系统
- **同步**变更

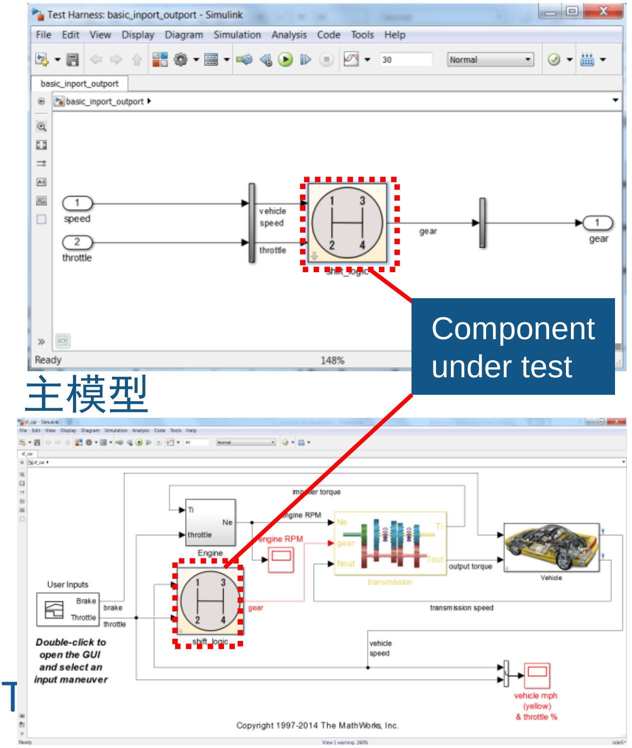
测试序列

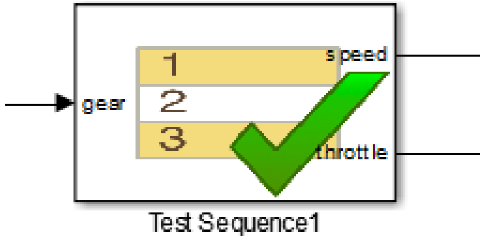
- **编写**动态输入和柔性评估

测试管理

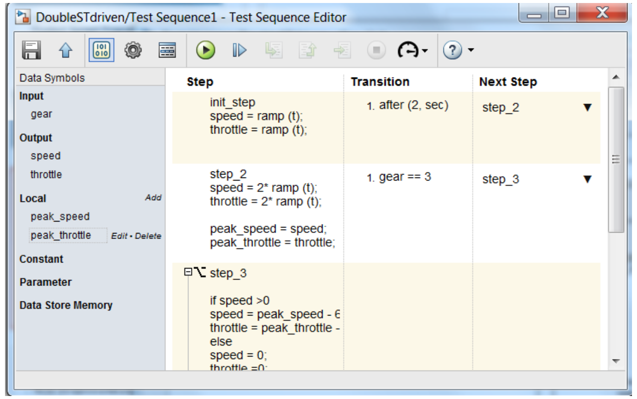
- **创建测试（基于模板）**
- **管理**创建、执行、报告

Test Harness


Test Harness: basic_inport_outport - Simulink
File Edit View Display Diagram Simulation Analysis Code Tools Help
Normal
basic_inport_outport
speed
throttle
vehicle speed
gear
shift_logic
Ready
148%
Component under test
主模型
Engine
Ti
Ne
impeller torque
engine RPM
transmission
output torque
Vehicle
User Inputs
Brake
Throttle
brake
throttle
transmission speed
vehicle speed
Double-click to open the GUI and select an input maneuver
vehicle mph (yellow) & throttle %
Copyright 1997-2014 The MathWorks, Inc.



Test Sequence1



DoubleSTdriven/Test Sequence1 - Test Sequence Editor

Data Symbols

Input
gear

Output
speed
throttle

Local *Add*
peak_speed
peak_throttle *Edit • Delete*

Constant

Parameter

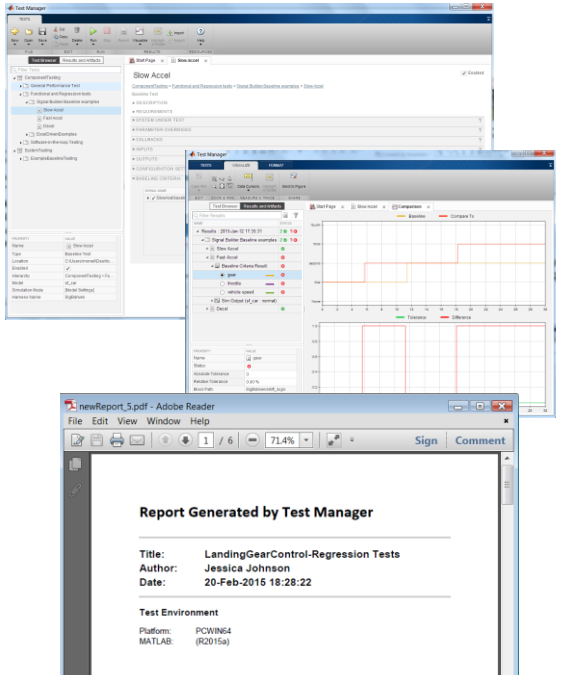
Data Store Memory

Step	Transition	Next Step

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

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

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



Report Generated by Test Manager

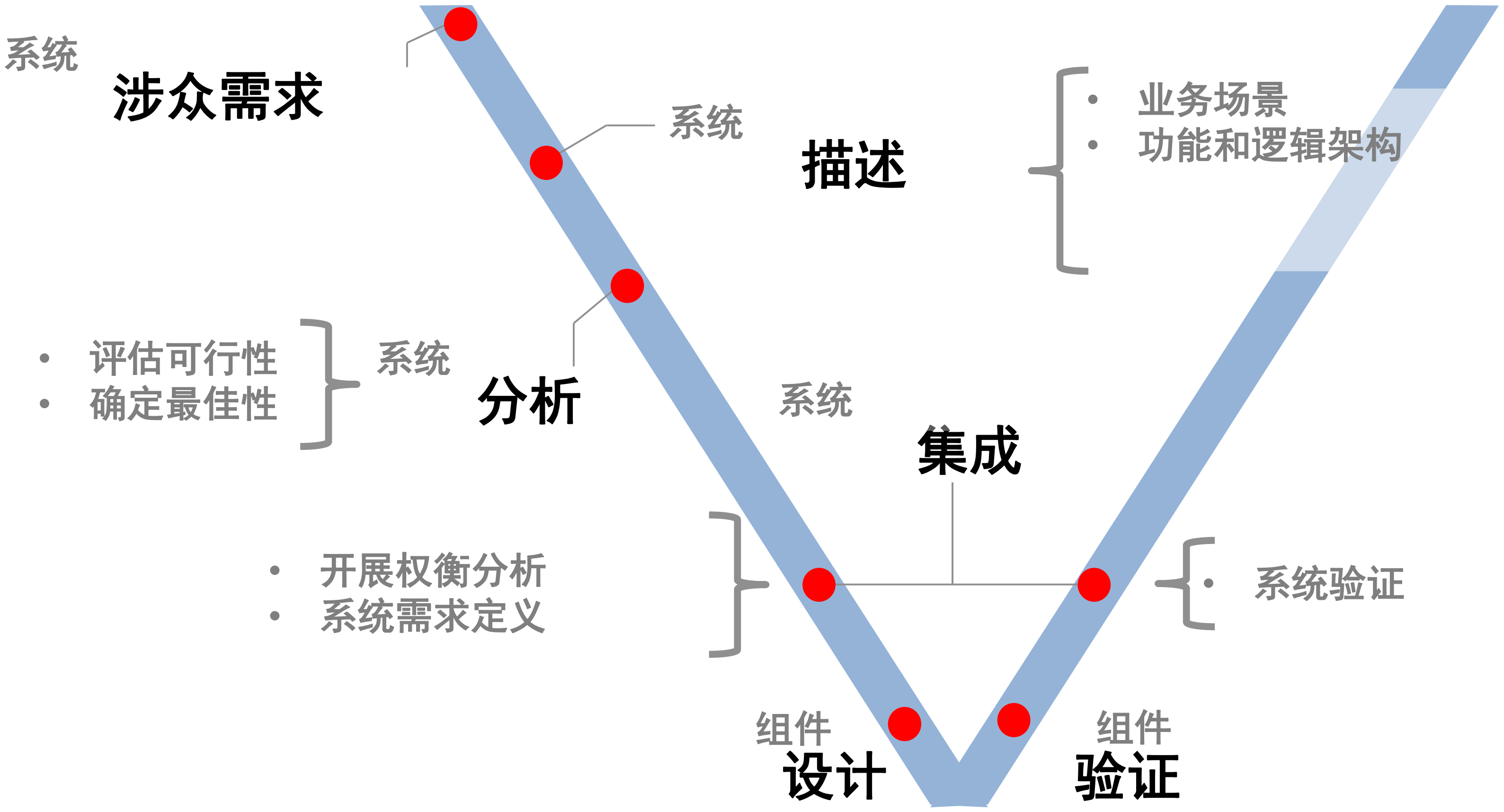
Title: LandingGearControl-Regression Tests
Author: Jessica Johnson
Date: 20-Feb-2015 18:28:22

Test Environment

Platform: PCWIN64
MATLAB: (R2015a)

验证和确认框架

谢谢


系统
涉众需求
系统
描述
业务场景
功能和逻辑架构
评估可行性
确定最佳性
系统
分析
系统
集成
开展权衡分析
系统需求定义
系统验证
组件
设计
组件
验证