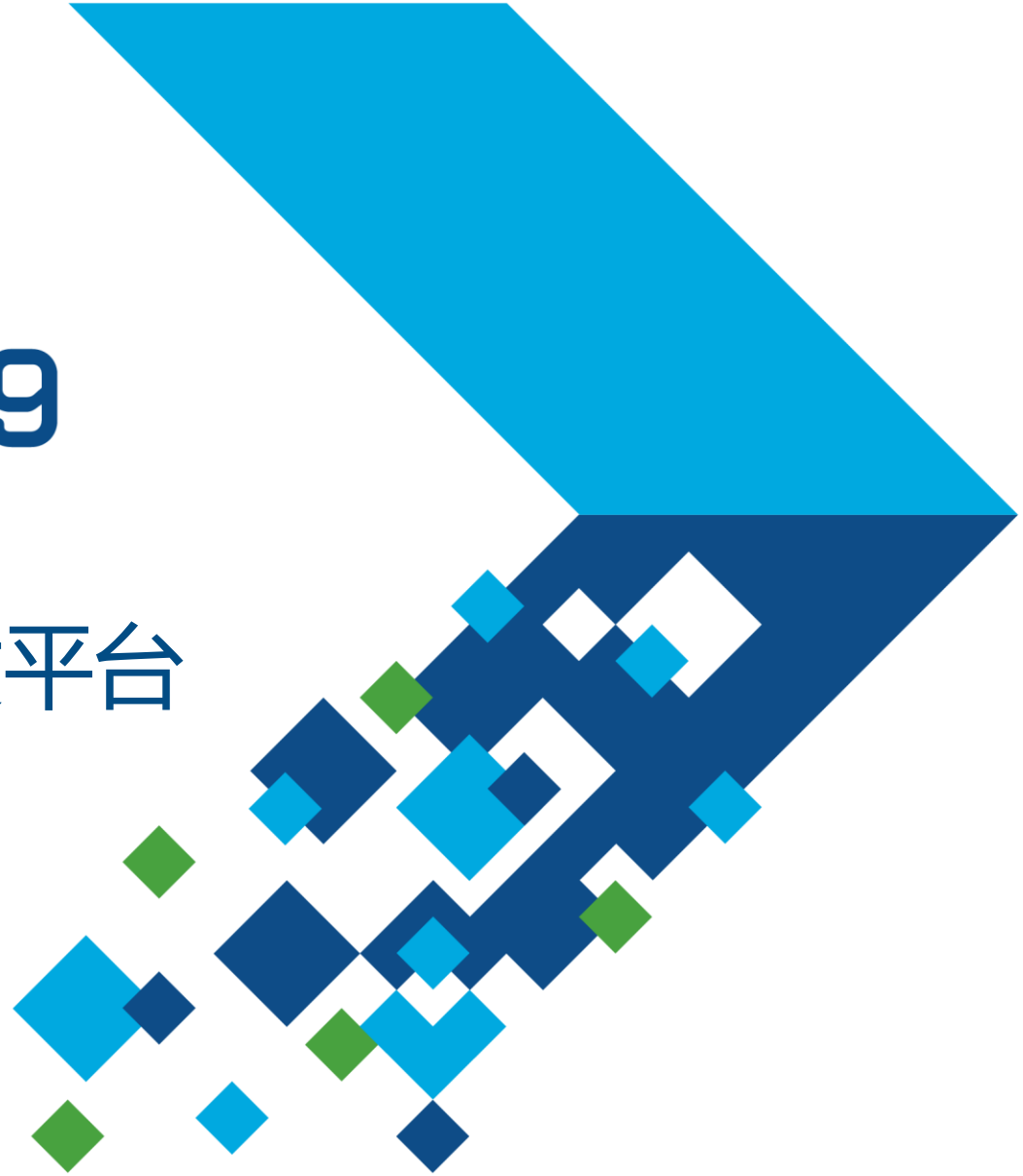
MATLAB EXPO 2019

构建基于模型的机载软件研发平台

苏哲



内容

- 基于模型的研发平台的组成及用户案例
- 构建研发平台的关键技术
- 符合高安全规范的机载软件研发平台

内容

基于模型的研发平台的组成及用户案例

- 构建研发平台的关键技术
- 符合高安全规范的机载软件研发平台

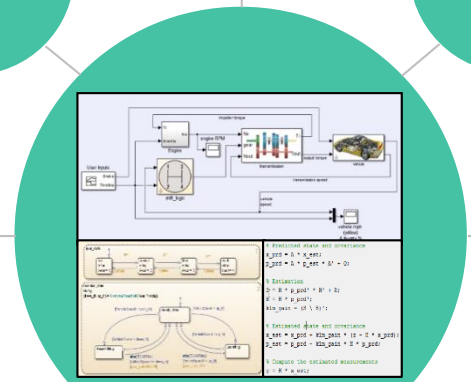
以基于模型设计为核心集成设计开发环境

项目管理
Simulink Project

知识管理
Simulink Check– Model Advisor
Simulink Customized Library

需求管理
Simulink Requirements
– RMI DOORS Integration

数据管理
Simulink Data Dictionary
Simulink Data Inspector



硬件集成
Processor In Loop
Hardware In Loop

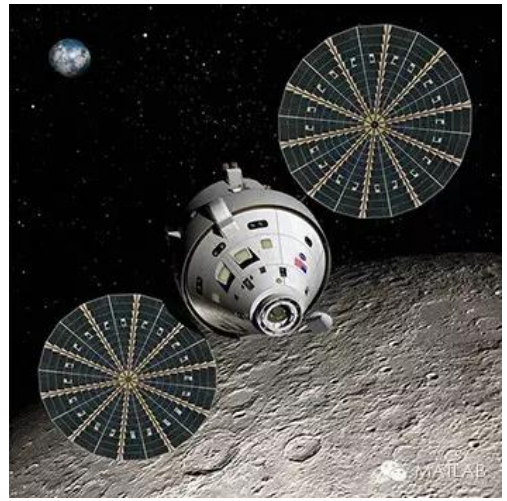
配置管理
Simulink Project
– SVN/CC Integration

报告生成
MATLAB Report Generator
Simulink Report Generator

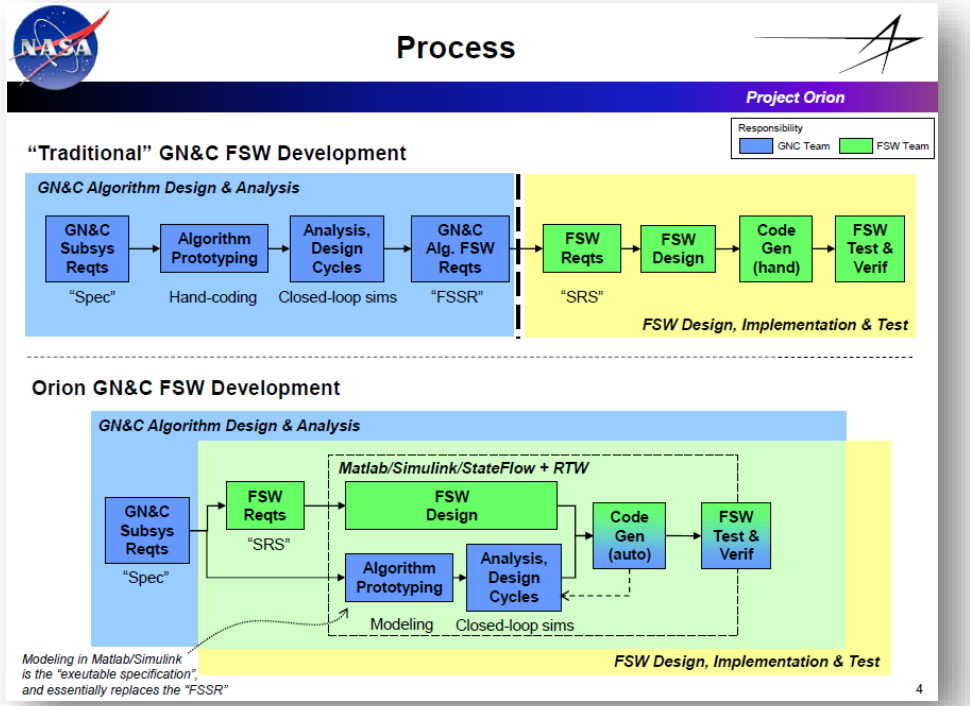
系统架构
System Composer
XML In/Out

基于模型的项目开发平台组成

NASA: 使用基于模型的设计加快NASA GN&C算法开发



- 为新方法奠定基础
  - 制定建模标准，构建风格一致的模型，高效协作。
- 开发和集成GN&C 算法
  - 整个模型由一百多个 Simulink 库模块和组件构成。
- 使用 Embedded Coder 生成代码
- 开创先河
  - 此 GN&C 项目在许多方面为 NASA 开辟了新道路。



西安飞行自动控制研究所：基于模型设计在机载安全关键领域中的应用

- 构建基于模型设计研发平台的关键技术
- 基于模型设计在实际项目中的应用

模型开发环境 —— 核心内容

系统主体框架开发及代码生成

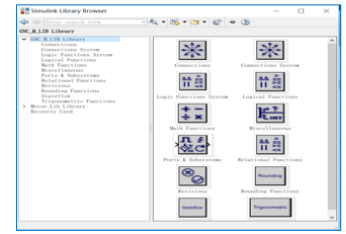
- 完成MDE流程设计与系统功能划分
- 完成主体框架设计与软件界面开发
- 实现了功能应用的独立开发与集成

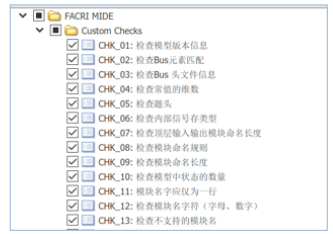
高安全代码生成模型库开发

- 160多个库模块
- 自建部分伺服软件二级模块库

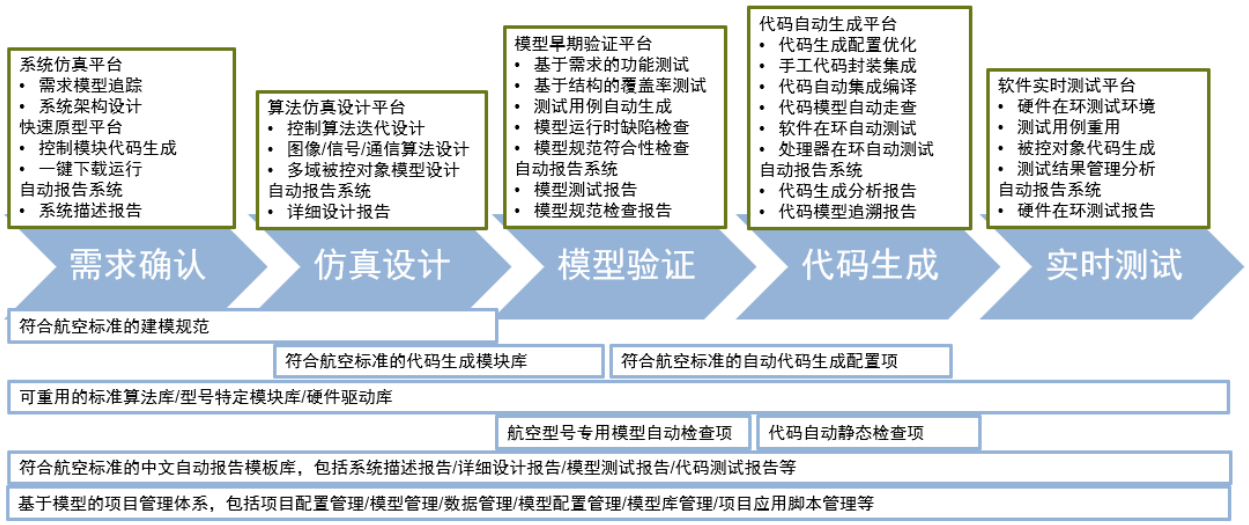
模型设计与代码生成规范建立及自动化检查项开发

- 参考Honeywell/NASA/Mathworks建模规范，构建 FACRI自有建模规范





模型开发环境构建思路与实施



内容

- 基于模型的研发平台的组成及用户案例

构建研发平台的关键技术

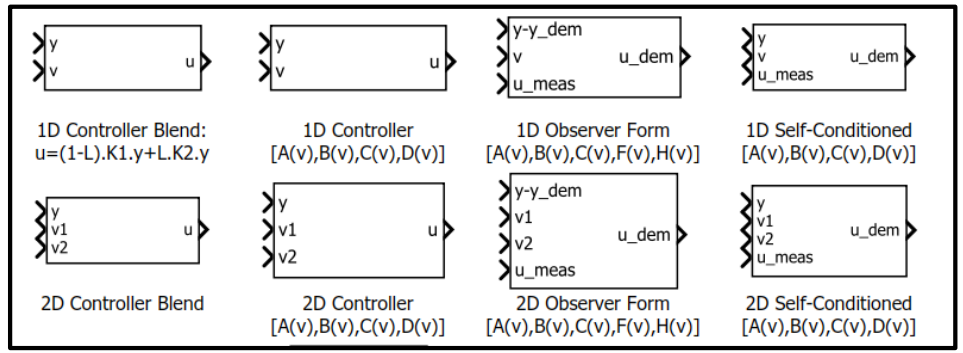
- 符合高安全规范的机载软件研发平台

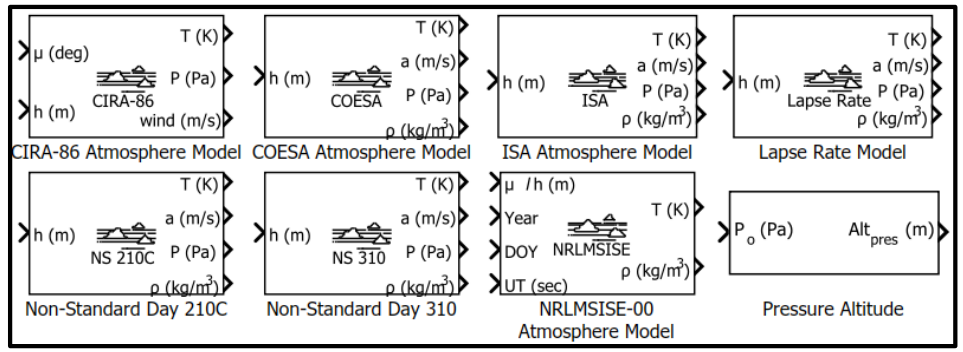
构建研发平台的关键技术

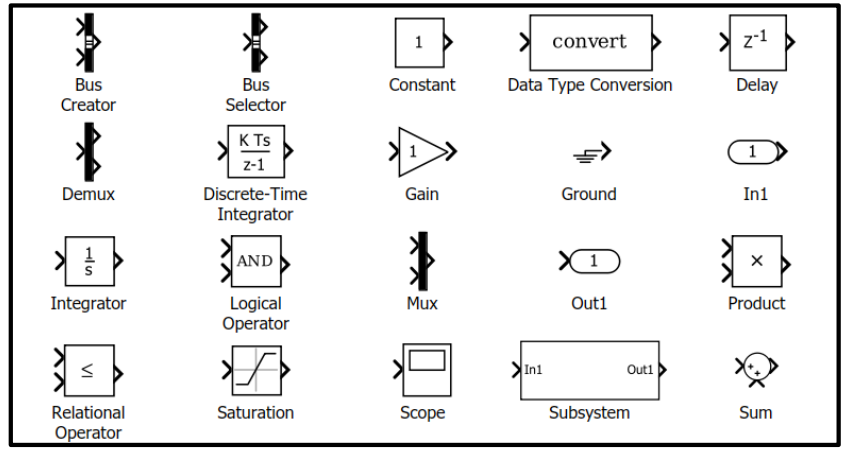
- 构建模型库
- 定制建模规范
- 规范设计流程

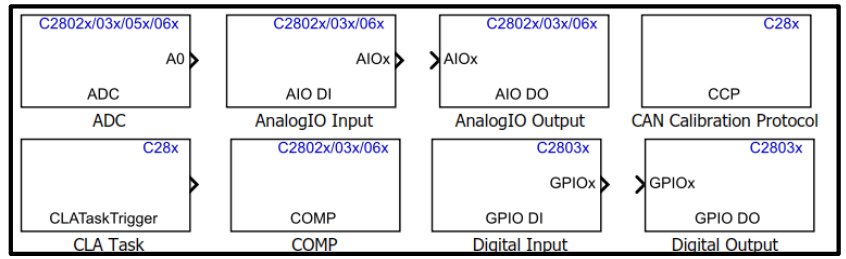
模型库

- 基础库
- 算法模型库
- 本体/环境模型库
- 硬件驱动模型库





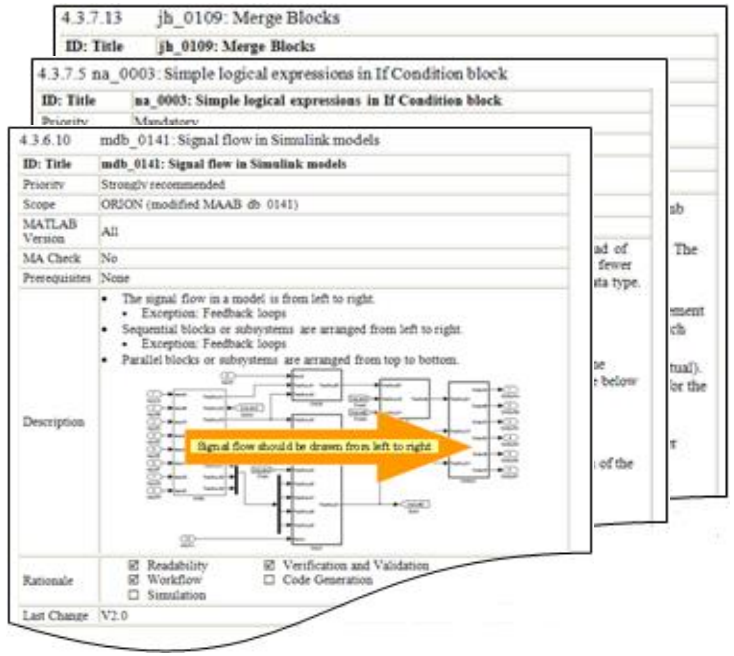


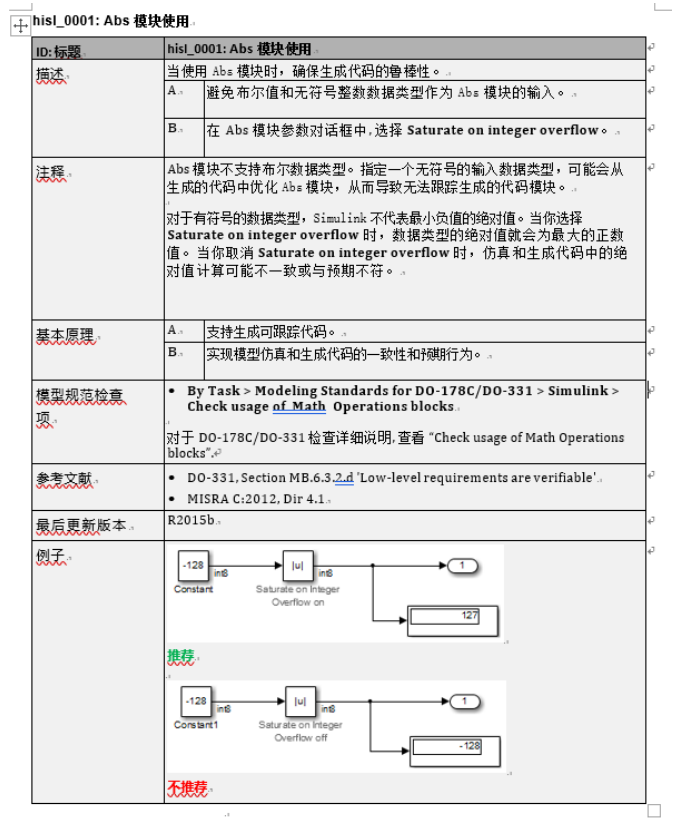


验证过的　　可复用的　　可维护的

建模规范 / 建模指南

- 软件模型规范
- 需求模型规范
- 对象/环境模型规范
- 已有知识的积累

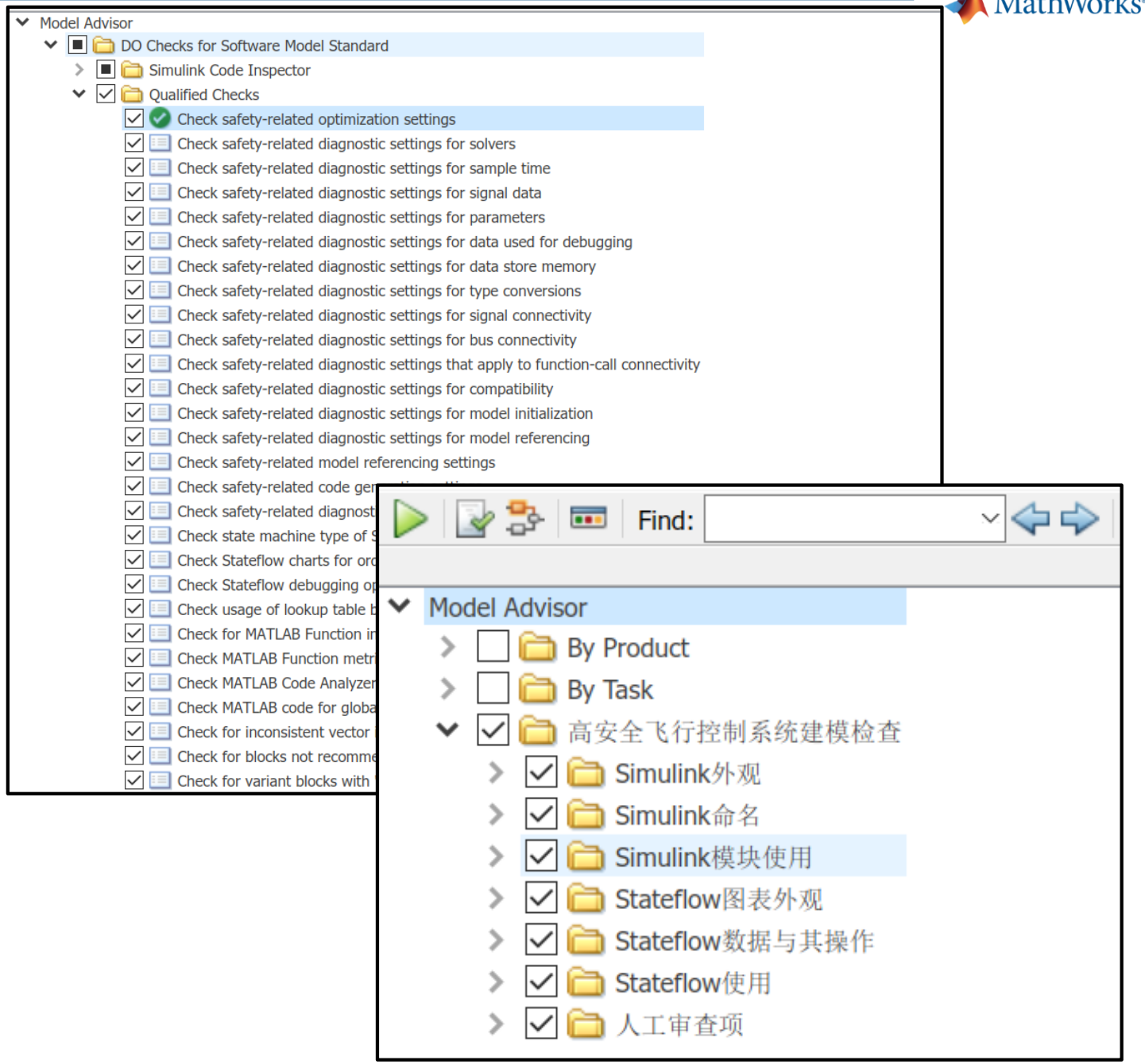




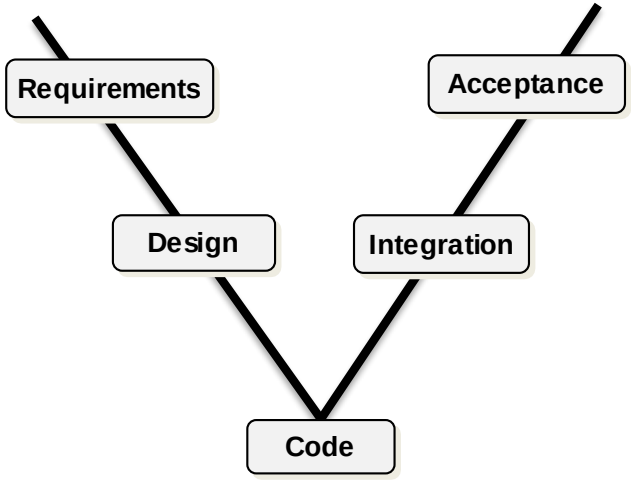
可读性 效率 可追溯性 代码生成

自动化检查项

- Simulink Check
- 配置已有检查内容
- 定制开发新的检查项



规范设计流程

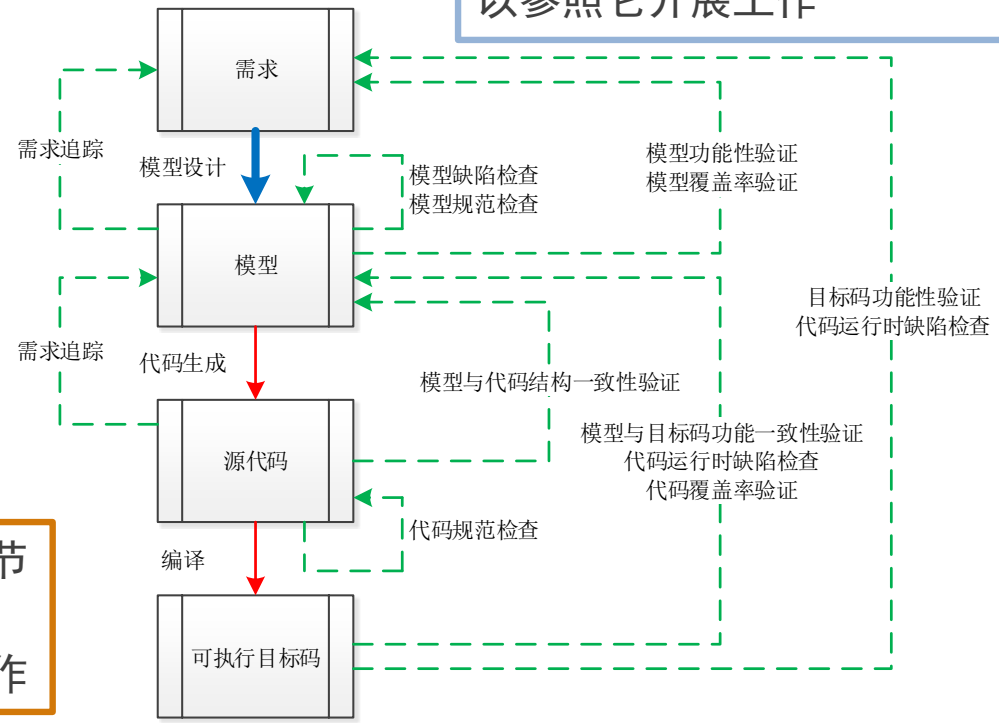


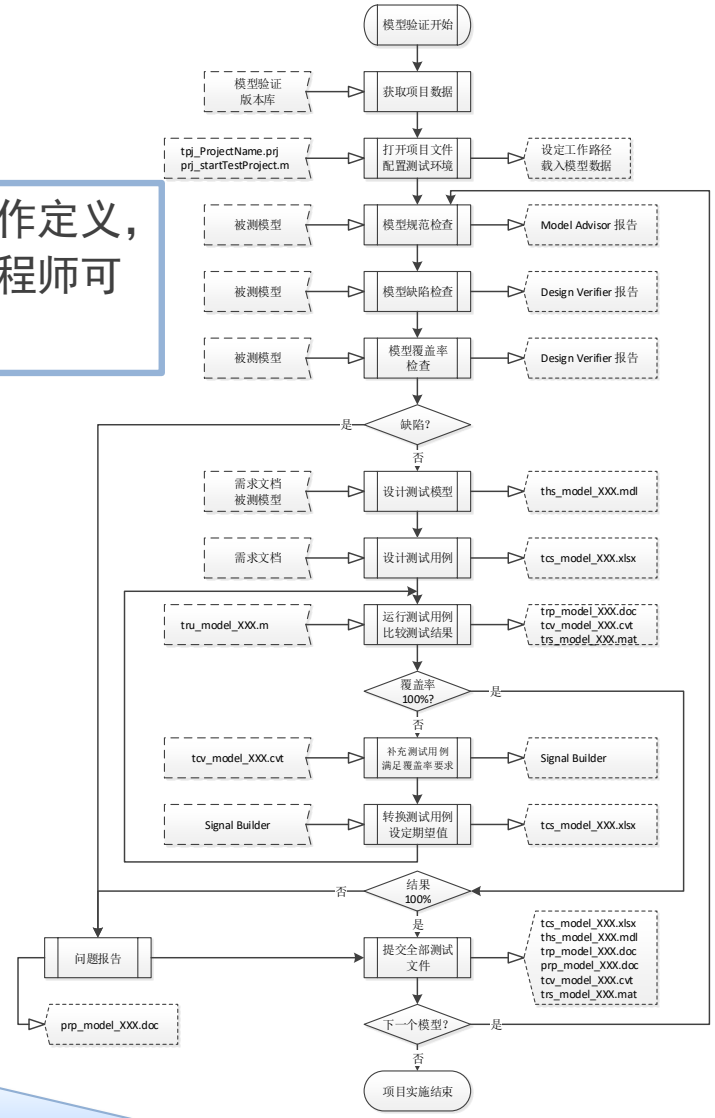
“V”流程

解决了设计过程中主要环节定义，但没有具体的实现，工程师无法参照它开展工作

“微”流程

解决了设计过程中的实现操作定义，每个操作都是可执行的，工程师可以参照它开展工作





内容

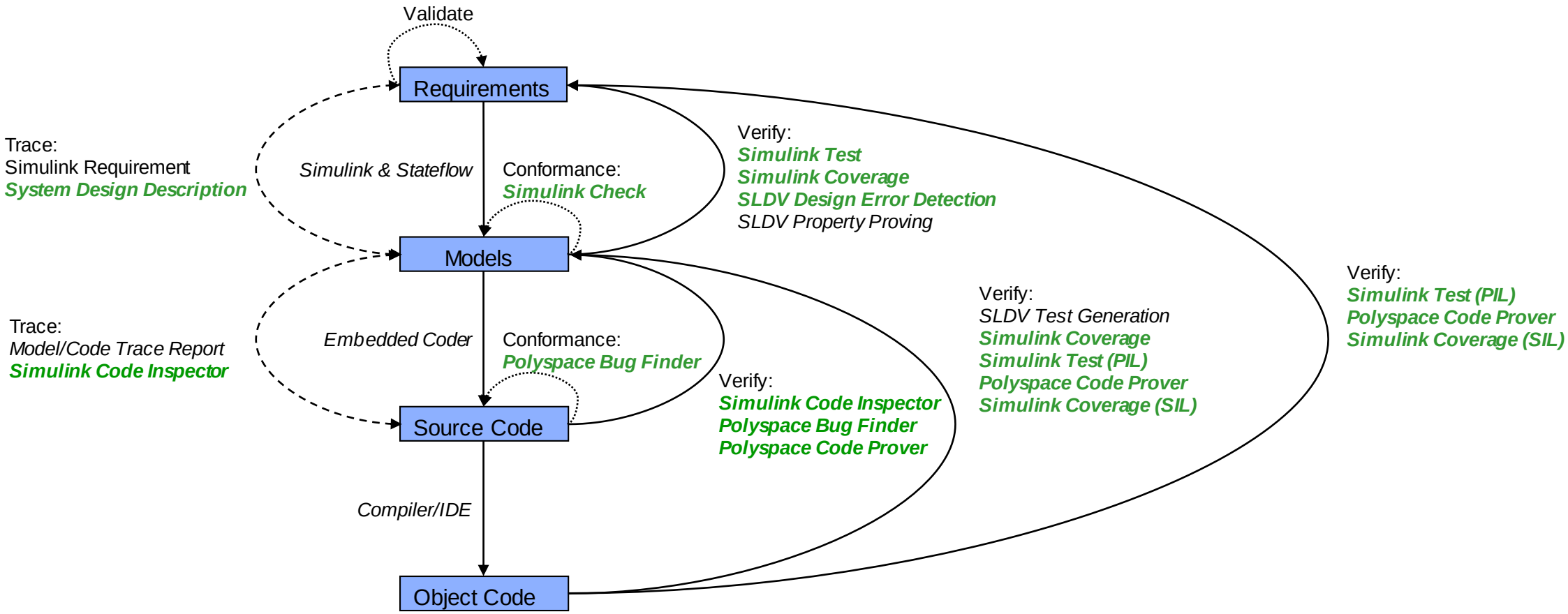
- 基于模型的研发平台的组成及用户案例
- 构建研发平台的关键技术

符合高安全规范的机载软件研发平台

符合高安全规范的研发平台

- Simulink工具对DO-178C/DO-331的支持
- DO Qualification Kit (for DO-178)

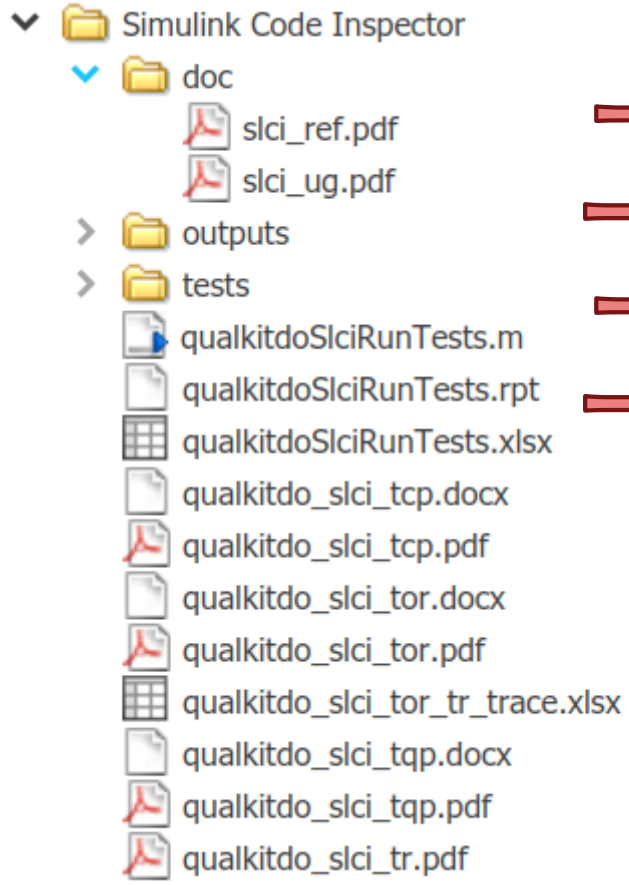
Simulink工具对DO-178C/DO-331的支持



Generated Evidence

DO Qualification Kit (for DO-178)

- Simulink Check (TQL-5)
  - DO-178C/DO-331 模型规范检查
- Simulink Coverage (TQL-5)
  - 模型/代码覆盖度
- Polyspace (TQL-4)
  - Polyspace Bug Finder
  - Polyspace Code Prover
- Simulink Report Generator (TQL-5)
  - 系统设计描述报告
  - Simulink XML 差异对比报告
- Simulink Code Inspector (TQL-4/TQL-5)
  - 代码模型一致性检查和追溯报告
- Simulink Test (TQL-5)
  - 仿真和测试结果
- Simulink Design Verifier (TQL-5)
  - 模型死逻辑检查



工具鉴定计划

工具操作要求

测试用例

期望结果

总结

- 构建基于模型设计平台用户案例
  - NASA的案例
  - FACRI的案例
- 构建研发平台的关键技术
  - 模型库
  - 建模规范
  - 设计流程
- 符合高安全规范的机载软件研发平台
  - Simulink工具对DO-178C的支持
  - DO-KIT认证支持包

谢谢