符合ISO26262的Simulink建模规范最佳实践

讲 师:马 聪

恒润科技MBD资深咨询工程师

2016-12-7

14:00-15:00 讲师演讲

15:00-15:20 集中答疑

15:20-15:30 问卷抽奖

market_dept@hirain.com

010-64840808-5281

Overview

>>了解建模规范

建模规范是什么
建模规范目的是什么
建模规范谁定的
建模规范应用场景是什么

>>建模规范实例

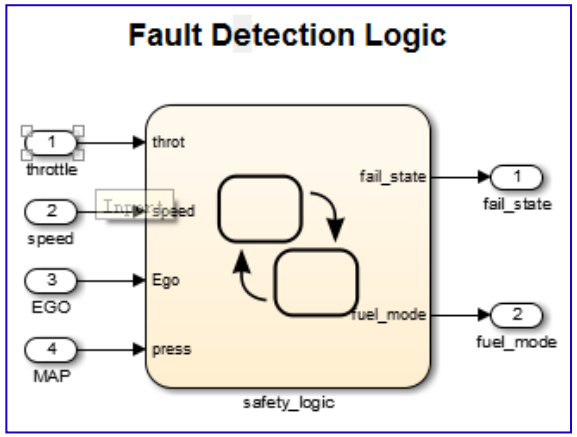
外观和布局
可靠的语言子集
使用样式模板
数据类型(Data Type)

>>ISO26262标准要求

建模规范需要覆盖的规则
（Topics to be covered by modeling guidelines）
如何制定建模规范

建模规范是什么

- 背景：使用Simulink作为软件开发工具
- 缘由：Simulink工具极大的灵活性

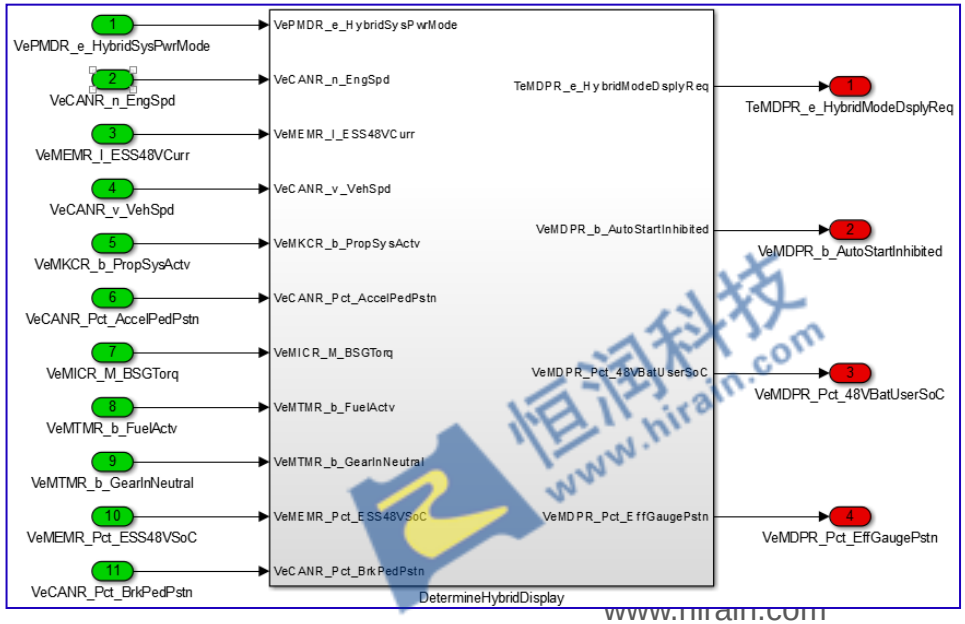


建模规范：

定义规范化的Simulink使用方式

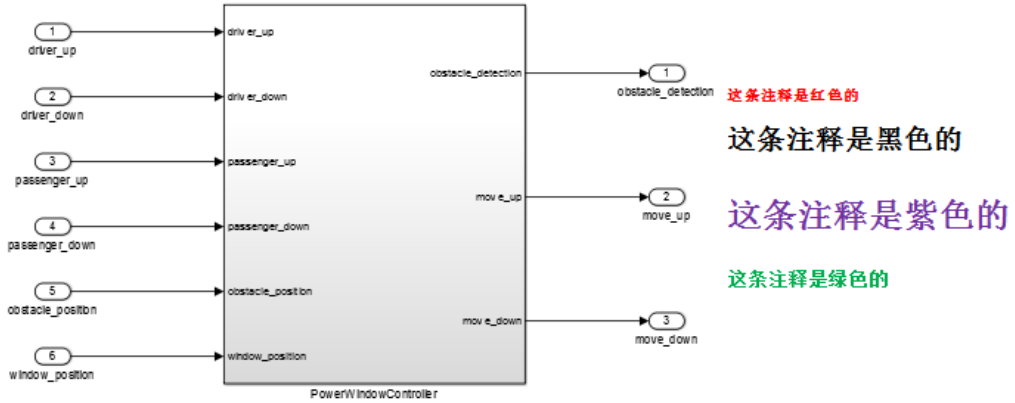
不是法规，是推荐指南

基于专家经验的最佳实践

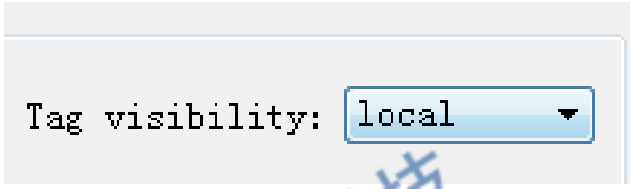


建模规范是什么

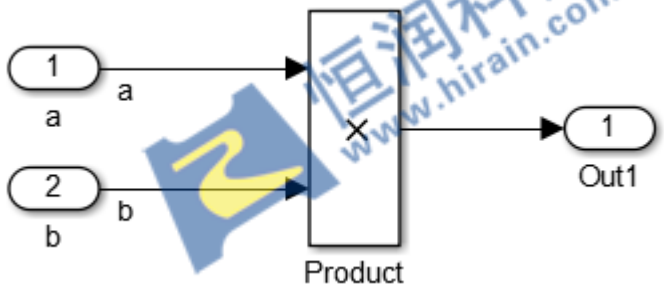
- 所有的文本风格是统一易辨识的



- Goto/From 模块必须设置为Local



- 算术模块（sum/product等）不能使用不一致或不恰当的数据类型；



建模规范目的是什么

- **避免使用易出错的建模方式**
  - 为了增强系统健壮性，从Simulink库中定义验证过的安全子集；
  - 符合理解习惯（比如关系运算模块，常数输入放在第二个输入口）；

- **增加效率和安全性**
  - 保证模型配置的一致性
  - 提高仿真效率的配置
  - 保证代码生成配置的一致性和优化选项的一致性；
  - 避免使用导致效率低下代码的建模模板；

建模规范目的是什么

- **OEM定制，提高OEM和供应商模型交互的可读性、规范性、复用性等**
  - 统一的风格和感官认识
- **ISO26262、IEC61508、DO178C等行业标准要求**

Table 1 — Topics to be covered by modelling and coding guidelines

Topics		ASIL			
		A	B	C	D
1a	Enforcement of low complexity[a]	++	++	++	++
1b	Use of language subsets[b]	++	++	++	++
1c	Enforcement of strong typing[c]	++	++	++	++
1d	Use of defensive implementation techniques	o	+	++	++
1e	Use of established design principles	+	+	+	++
1f	Use of unambiguous graphical representation	+	++	++	++
1g	Use of style guides	+	++	++	++
1h	Use of naming conventions	++	++	++	++

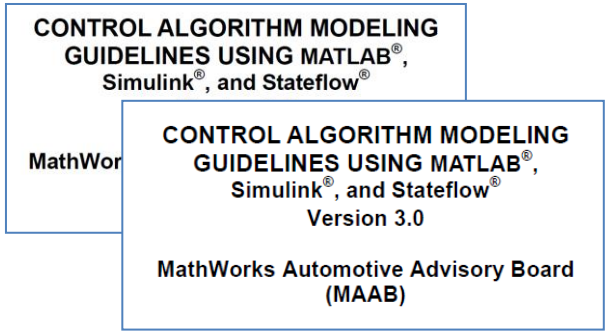
摘自ISO26262-6

建模规范定制：专家经验来自哪里

工具供应商：Mathworks

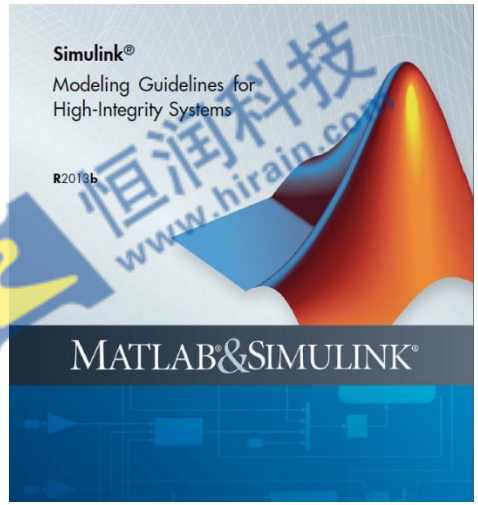
◆ **MAAB (Mathworks Automotive Advisory Board) Ford Daimler AG、Toyota…**

- Control algorithm modeling guidelines using MATLAB, Simulink and Stateflow（2011年 7月 V2.2； 2012年 V3.0 ）
- 主要聚焦于模型可读性和可维护性。



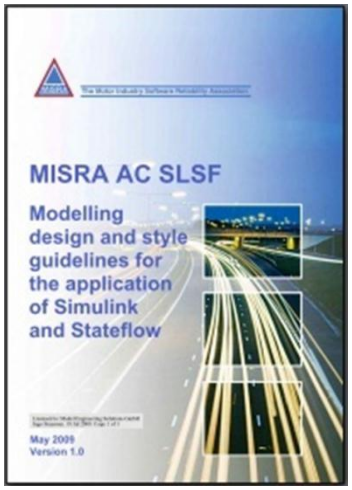
◆ **Mathworks :Modeling Guidelines for High-Integrity Systems**

- 较新的版本无标准文档，集成在Mathworks的 help体系中；
- 聚焦于模块的安全使用、生成代码可靠性安全性等



建模规范定制：专家经验来自哪里

标准协会组织等：MISRA+企业专家

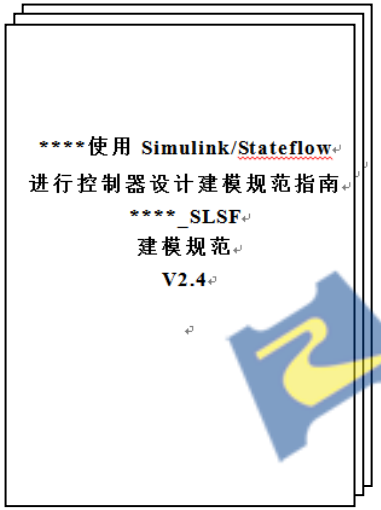


- **MISRA：MISRA_AC_SLSF**

Model design and style for the application of Simulink and Stateflow (2009年5月）

- 聚焦于规范化模型的显示方式、使用方式、模板等
- 期望保证代码精简、可靠

- **企业专家：长期的使用经验总结**
  - 可读性（风格）
  - 便于验证
  - 维护性
  - 仿真效率
  - 代码生成质量



恒润科技 HIRAIN TECHNOLOGIES

建模规范典型应用场景

- **基于模型的软件开发，期望产品通过ISO26262认证**
  - 强制执行
  - 依据不同的ASIL等级，确定建模规范需要考虑的因素，确定项目级建模规范
  - 执行建模规范，并输出对应的检查报告和解释文档；
- **注重产品质量和形象的OEM和供应商**
  - 推荐执行；
  - 模型外观统一、可读性好、维护性强；
- **注重模型到代码质量的OEM和供应商**
  - 推荐执行；
  - 深入研究建模规范代码生成器配置规范；
  - 定制建模模板和代码生成模板

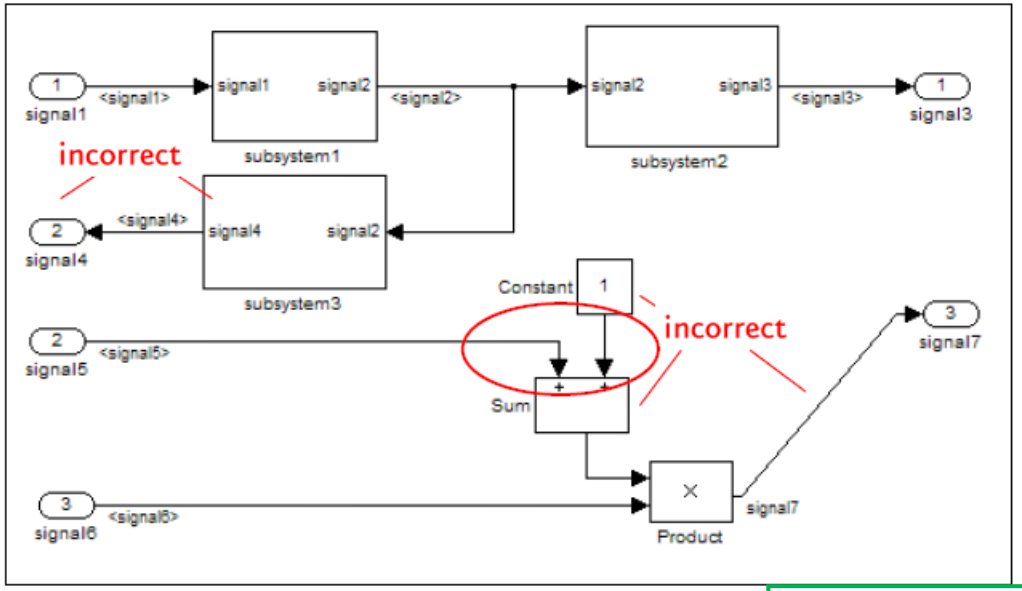
建模规范实例

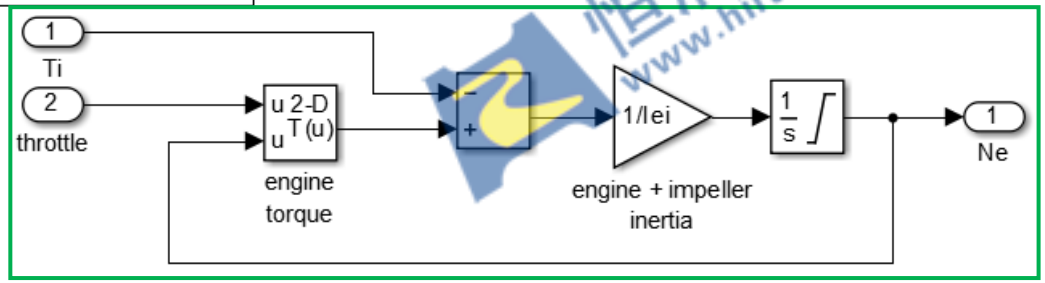
——布局和外观

建模规范实例：布局与外观

◆ 约定信号流方向

- ➢ 信号流整体应从左到右，从上到下，反馈信号除外；
- ➢ 反馈信号流应紧邻的正向信号流下方完成；

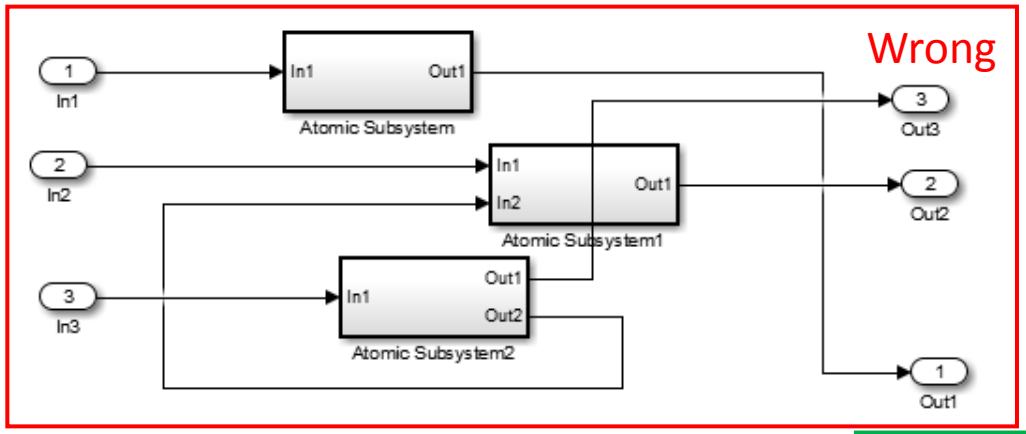


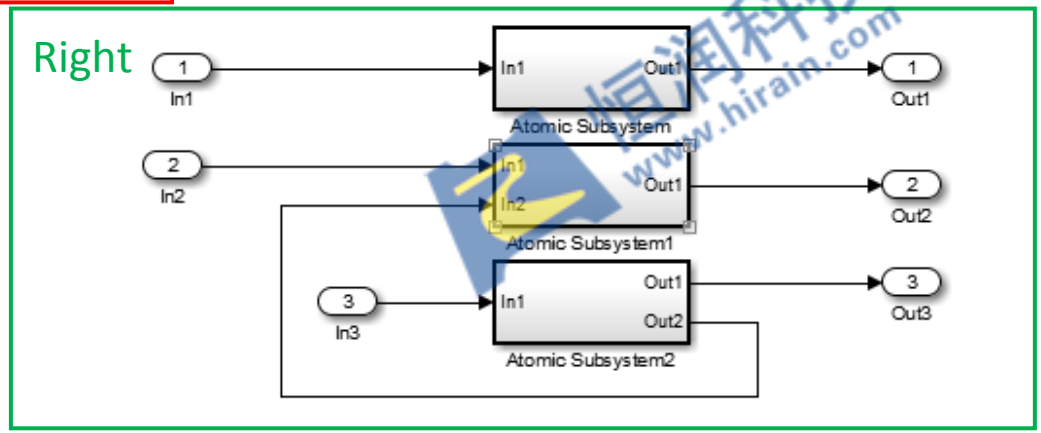


建模规范实例：布局与外观

◆ 约定信号线要求

- 所有信号线必须是水平或竖直的，尽量减少信号线的弯折；
- 信号线不能重叠（与文字、模块）；
- 尽量减小信号线的交叉（虽然经常发生），当与模块位置要求冲突时，遵循（？）规则；



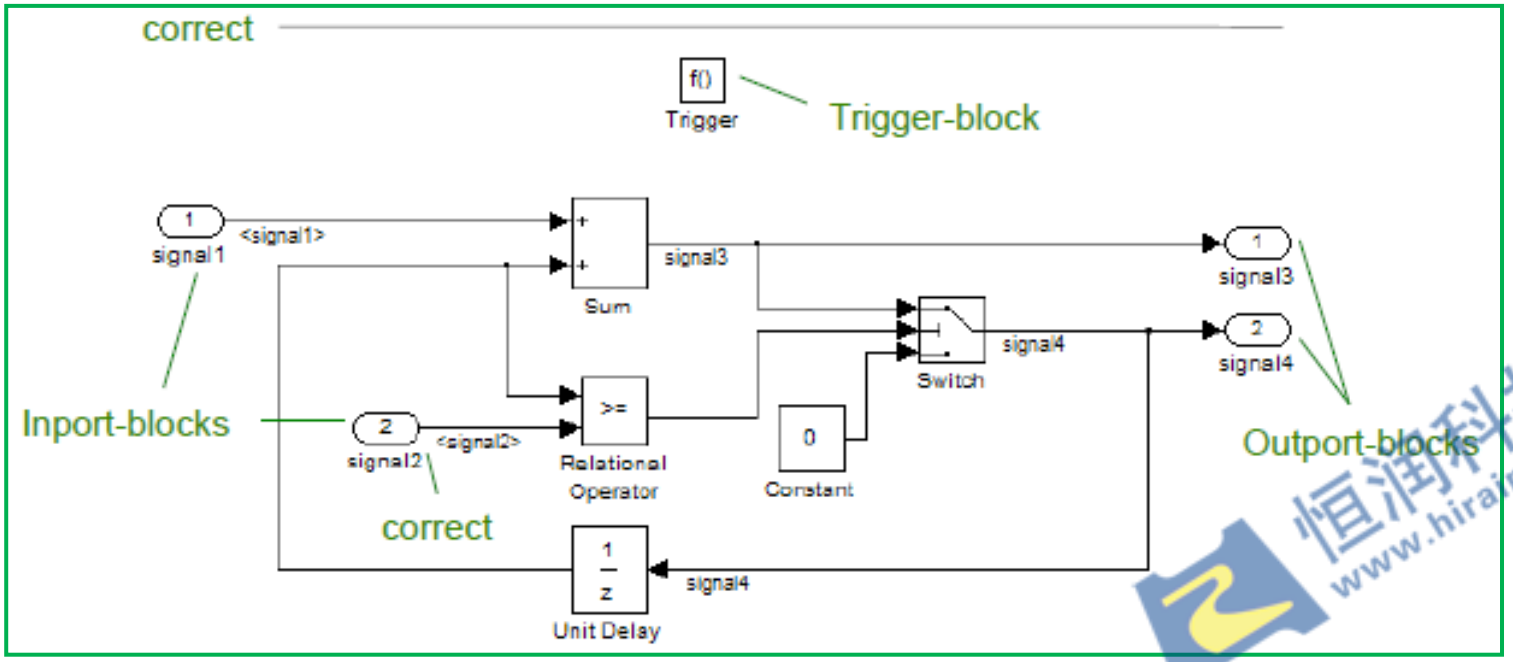


恒润科技
HIRAIN TECHNOLOGIES

建模规范实例：布局与外观

◆ 约定特定模块的位置

- 输入输出端口符合信号流，输入在最左边，输出在最右边，列为整齐的一列；
- Trigger、Enable模块在子系统最上位置（最左上）；
- 常数（constant）模块作为其他模块输入时，不连接第一个端口（除非都是常数）；

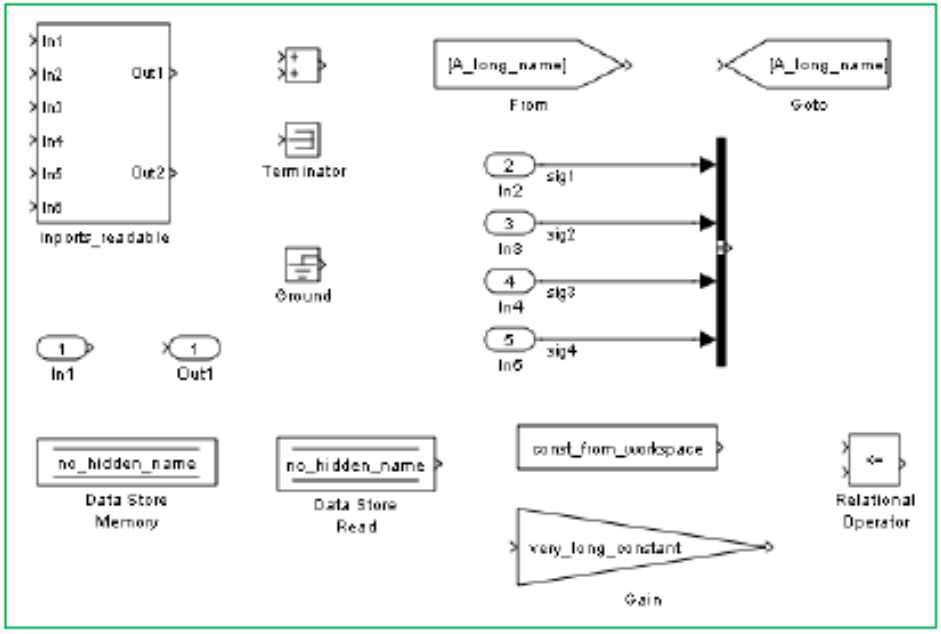


建模规范实例：布局与外观

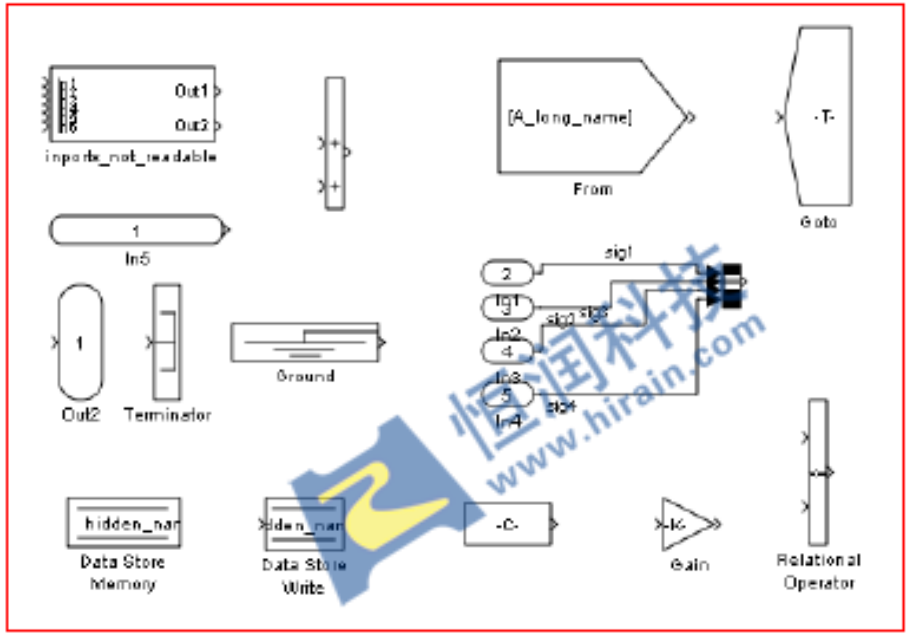
◆ 约定模块属性的清晰性和可见性

- ➢ 模块的端口（名）必须是清晰可见的；
- ➢ 模块外观显示其某项属性的，属性值应当清晰可见；Constant、Gain、From/Goto……
- ➢ 模块大小应当是其默认大小，除非为了实现其他规则；

Right



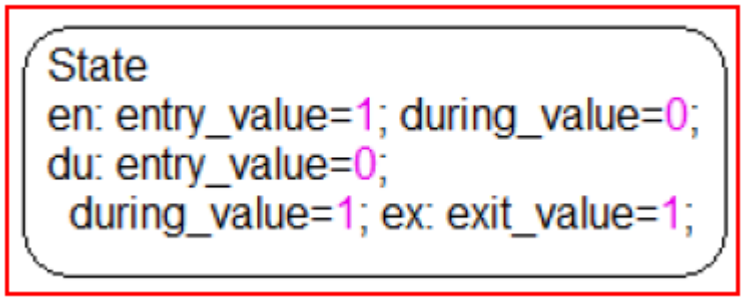
Wrong



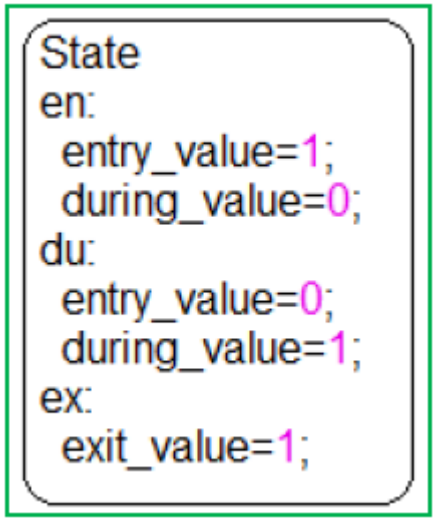
建模规范实例：布局与外观

- **约定Stateflow 中以下命令独立成行；**
  - State关键字：entry(en)、during(du)、exit (ex) ;
  - 所有的动作。
- **约定默认转移位置**
  - 默认转移从state或者junction上方进入；

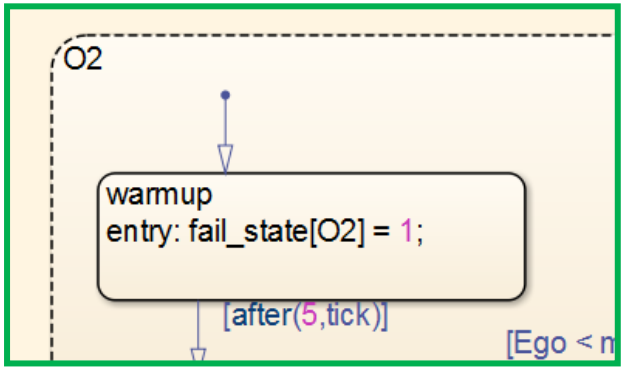
Wrong



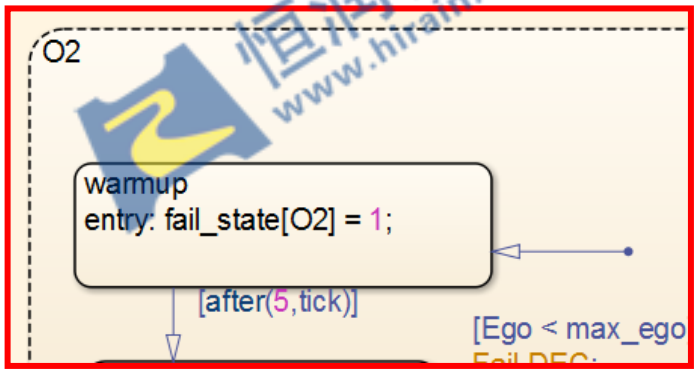
Right



Right

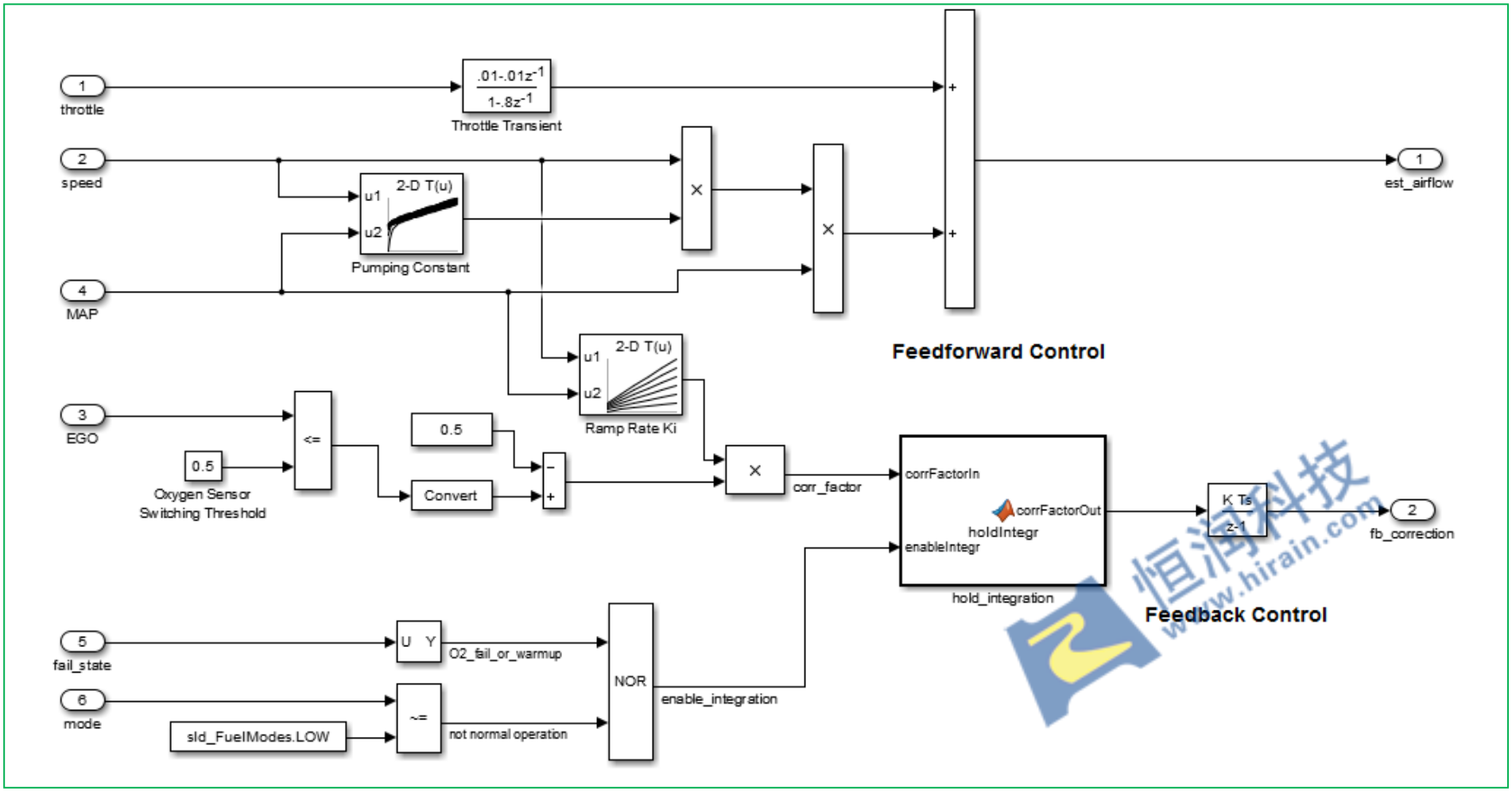


Wrong



建模规范实例：布局与外观

数据流层：模型布局和外观最佳实践

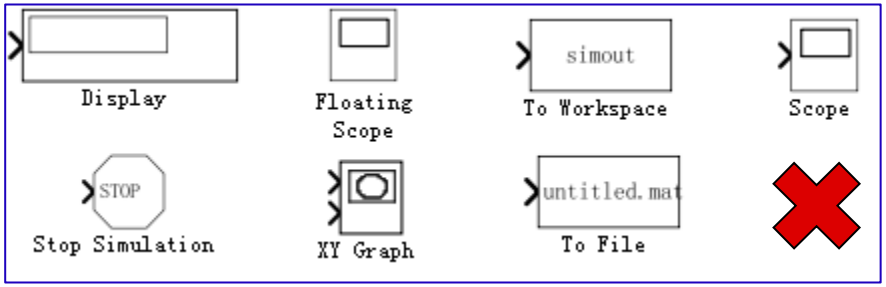


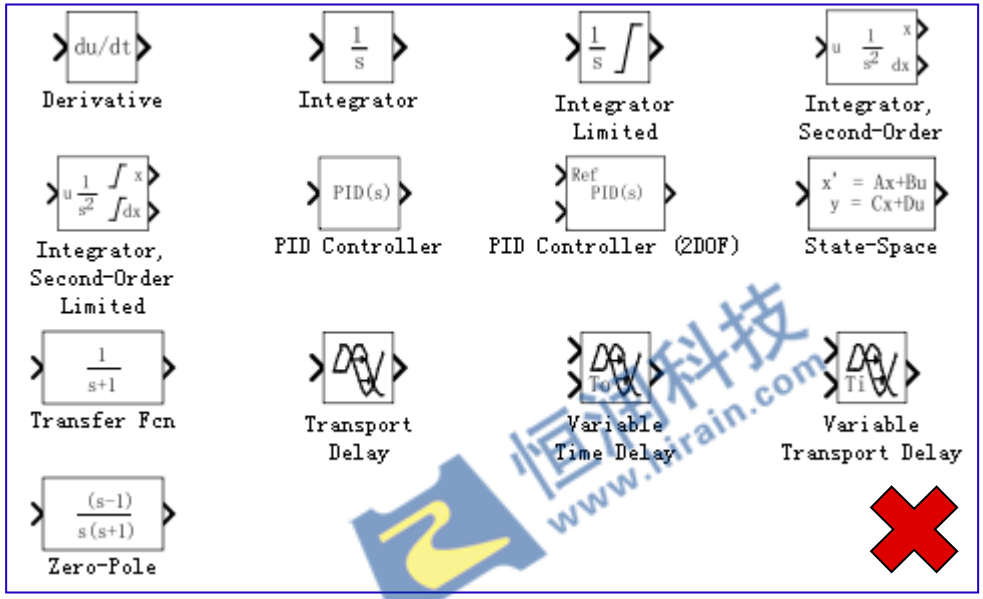
建模规范实例

——可靠的语言子集

建模规范实例：可靠的语言子集

- **约定使用Simulink建模时，允许使用的标准模块库模块；使用验证过的自定义模块；**
  - 控制器模块必须从离散模块库中选取，不能使用连续系统库；
  - Source/Sinks模块库中，约定特定的模块不能使用；
  - 使用自定义库时，验证与评审过的自定义模块（滤波器等）；



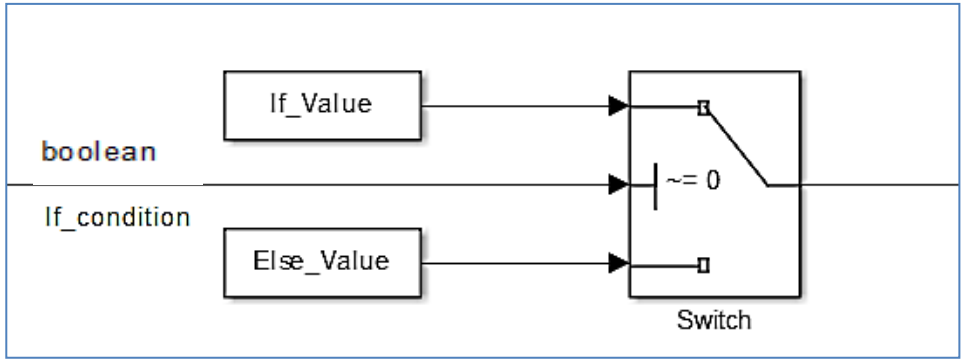


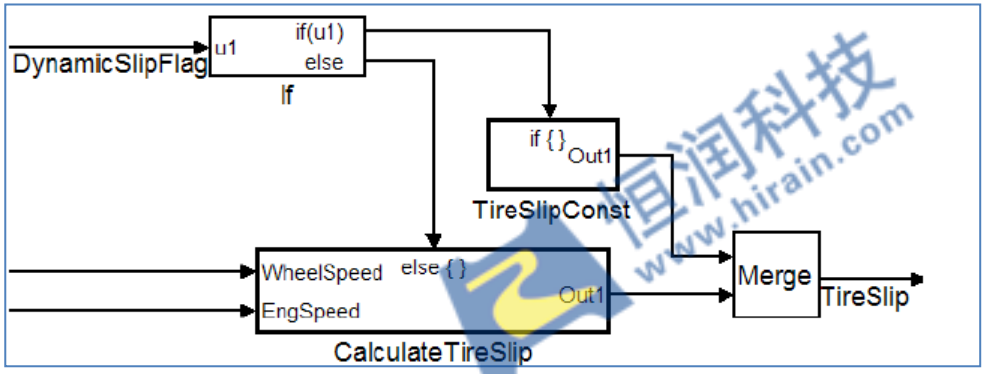
建模规范实例

——使用样式模板

建模规范实例：使用样式模板

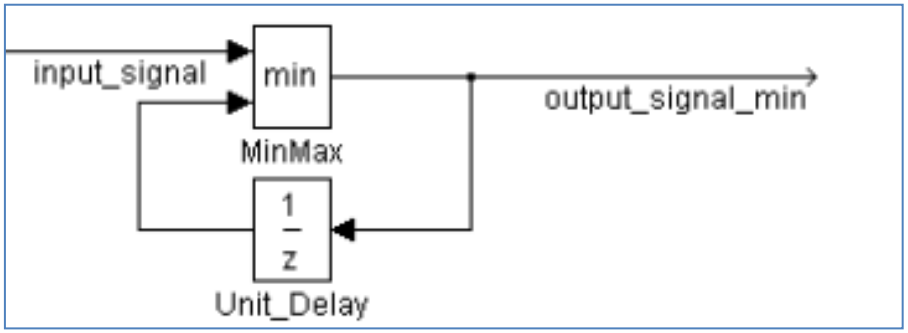
- **使用Switch 与if-then-else的模板：**
  - 使用switch用来分配两个常数；
  - 如果分支包含数据计算、查表、状态保持等复杂运算时，使用 if-then-else模板；

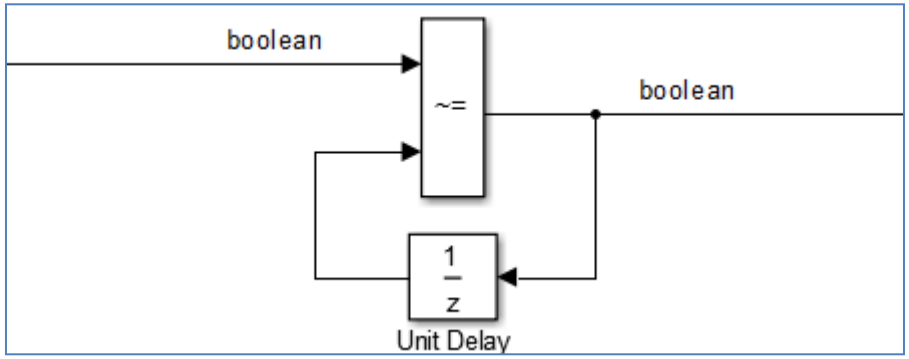


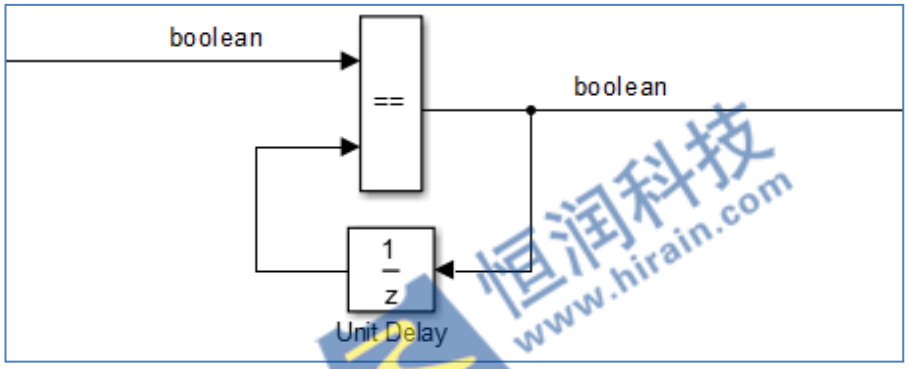


建模规范实例：使用样式模板

- **Simulink向量信号特定属性的获取模板：**
  - 使用下面的模板来获取已经过去的信号属性：





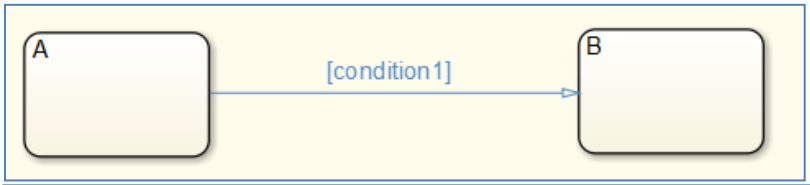


建模规范实例：使用样式模板

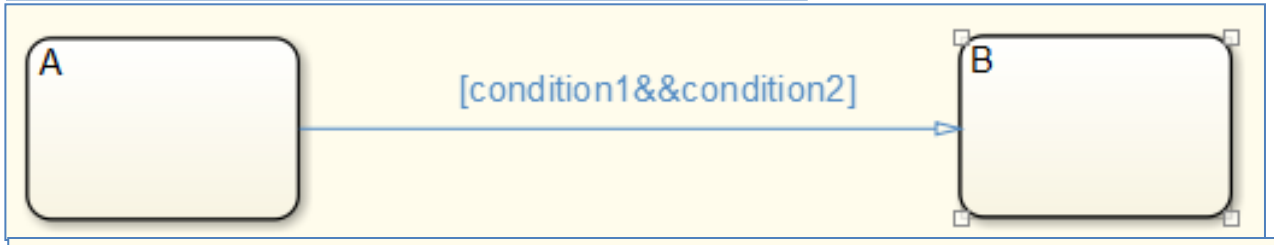
◆ multiple Transition conditions/ Actions使用模板

➢ 依照下面的模板来使用 多条件转移模板；

- **单一条件**



- **不大于三个简单条件（条件中无逻辑运算）**



- **多于3个简单条件或复杂条件（条件中有逻辑运算）**

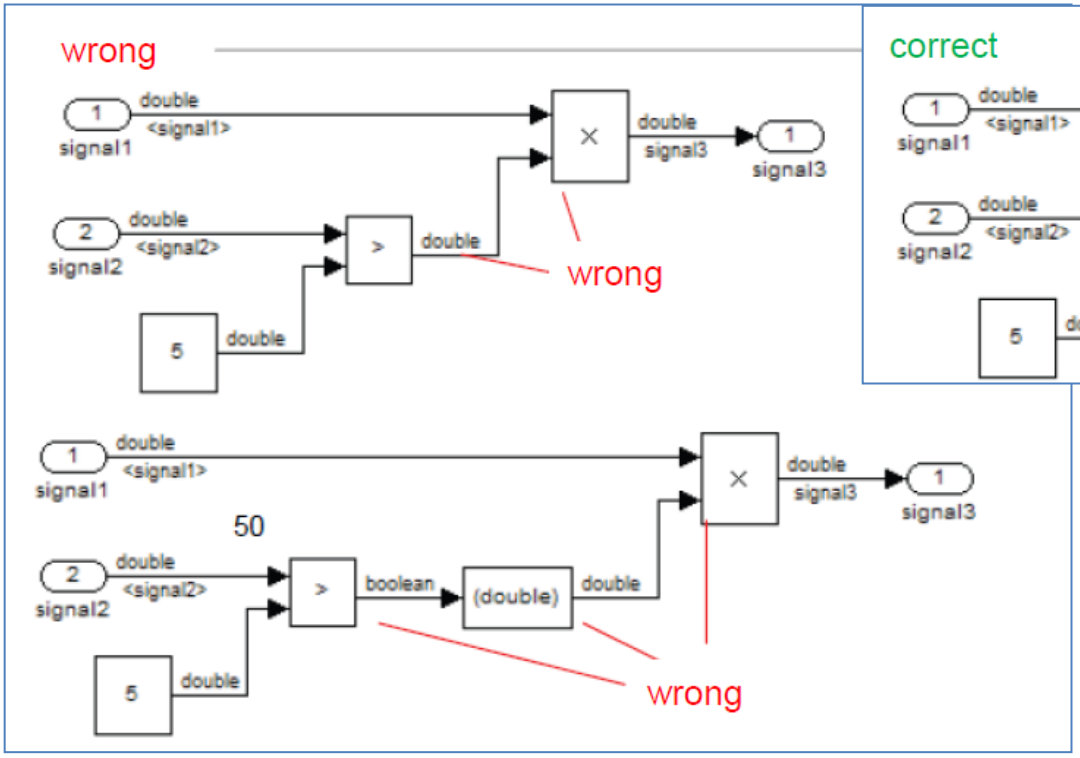
建模规范实例

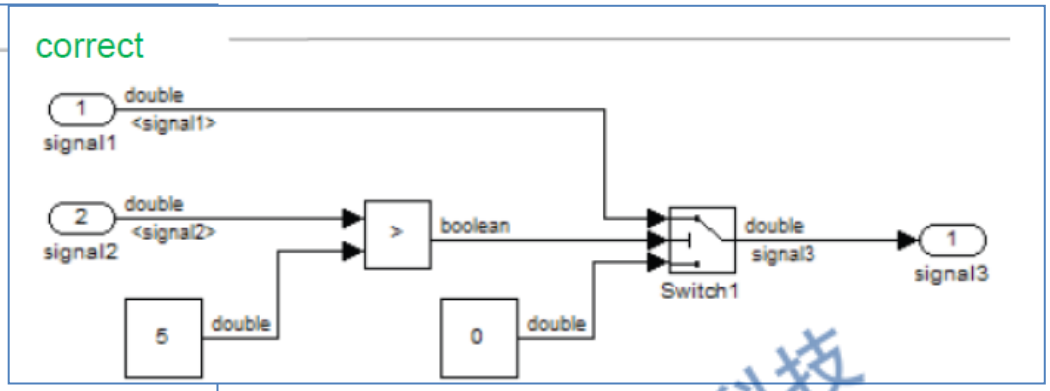
——数据类型

建模规范实例：数据类型

◆ 数值运算模块与逻辑运算模块数据类型

- ➢ 在配置中勾选：将逻辑信号以布尔类型进行实现
- ➢ 逻辑运算模块输入量必须是布尔类型；
- ➢ 数值运算不能对逻辑变量进行操作；



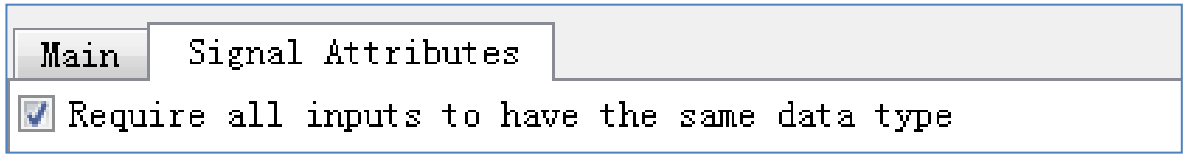


建模规范实例：数据类型

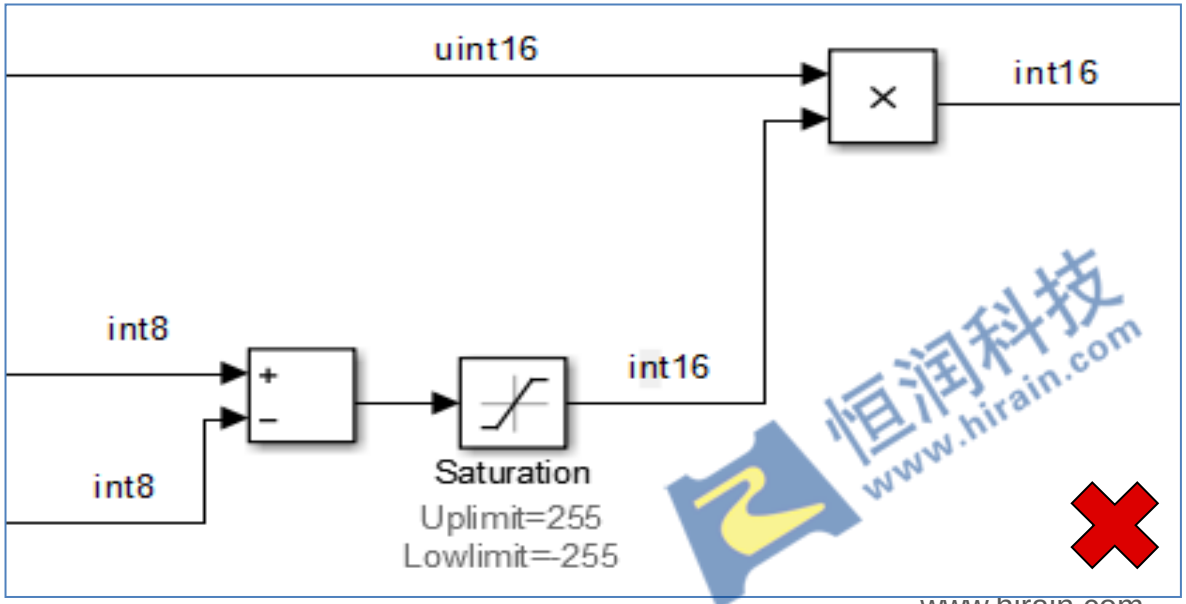
◆ 算术运算模块变量类型一致性

- ➢ 算术模块输入变量类型应当是一致的；
- ➢ 输出数据类型应当包含所有输出的可能；

• **勾选输入类型相同**



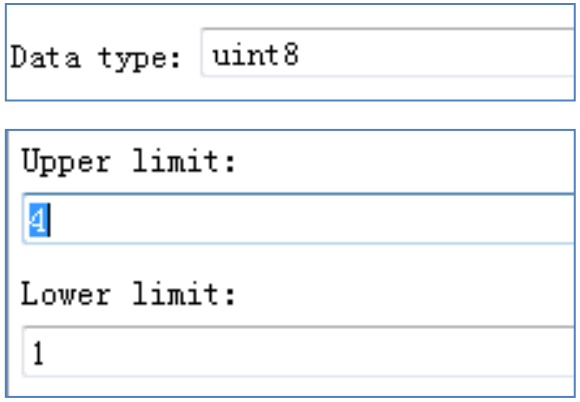
• **合理的数据类型定义**

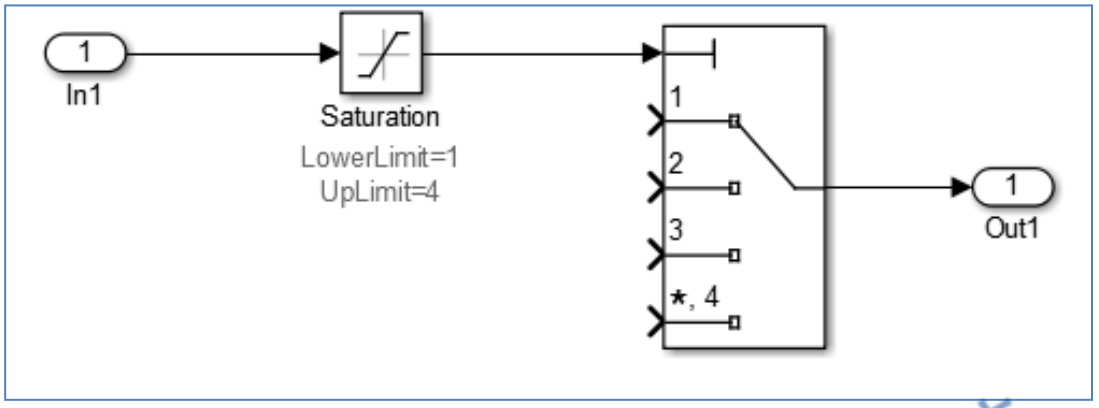


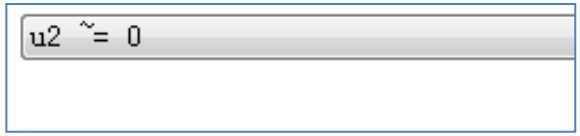
建模规范实例：数据类型

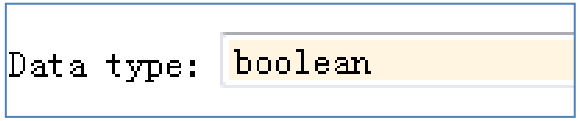
◆ 控制信号的数据类型

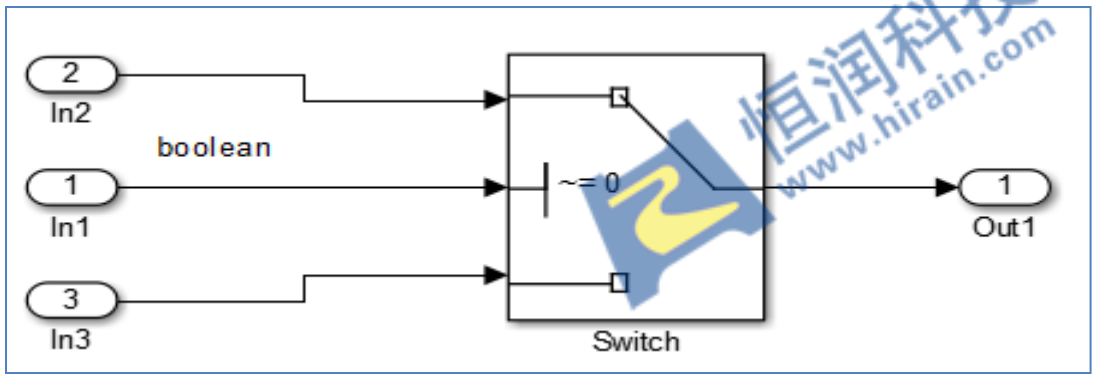
- 至少是离散的数据类型（建议unsigned integer）
- 定义其数据范围（推荐）











ISO26262标准建模规范要求

——设计准确性保证手段之一

ISO26262标准建模规范要求

摘自ISO26262-6　5.4.6—5.4.7

5.4.6 The criteria that shall be considered when selecting a suitable modelling or programming language are:

a) an unambiguous definition;

EXAMPLE Syntax and semantics of the language.

b) the support for embedded real time software and runtime error handling; and

c) the support for modularity, abstraction and structured constructs.

Criteria that are not sufficiently addressed by the language itself shall be covered by the corresponding guidelines, or by the development environment.

5.4.7 To support the correctness of the design and implementation, the design and coding guidelines for the modelling, or programming languages, shall address the topics listed in Table 1.

NOTE 1 Coding guidelines are usually different for different programming languages.

NOTE 2 Coding guidelines can be different for model-based development.

NOTE 3 Existing coding guidelines can be modified for a specific item development.

EXAMPLE MISRA C[3] and MISRA AC AGC[4] are coding guidelines for the programming language C.

语言本身不能体现的条件，用语言的使用规范来补充！！

保证设计正确的方法之一！！

基于模型方式的编码规则可能（可以）不同！！

ISO26262标准建模规范要求

摘自ISO26262-6 Table 1

Table 1 — Topics to be covered by modelling and coding guidelines

Topics			ASIL			
			A	B	C	D
1a	Enforcement of low complexity[a]	复杂度计算方法+结果	++	++	++	++
1b	Use of language subsets[b]	定制可用的模块库/编码方式	++	++	++	++
1c	Enforcement of strong typing[c]	数据类型定义与使用方式	++	++	++	++
1d	Use of defensive implementation techniques	错误预防的设计方法	o	+	++	++
1e	Use of established design principles	使用确定的设计方法	+	+	+	++
1f	Use of unambiguous graphical representation	不使用难以理解的设计方法	+	++	++	++
1g	Use of style guides	特定算法的设计模板	+	++	++	++
1h	Use of naming conventions	项目特定的命名方式	++	++	++	++

[a] An appropriate compromise of this topic with other methods in this part of ISO 26262 may be required.

[b] The objectives of method 1b are

- Exclusion of ambiguously defined language constructs which may be interpreted differently by different modellers, programmers, code generators or compilers.
- Exclusion of language constructs which from experience easily lead to mistakes, for example assignments in conditions or identical naming of local and global variables.
- Exclusion of language constructs which could result in unhandled run-time errors.

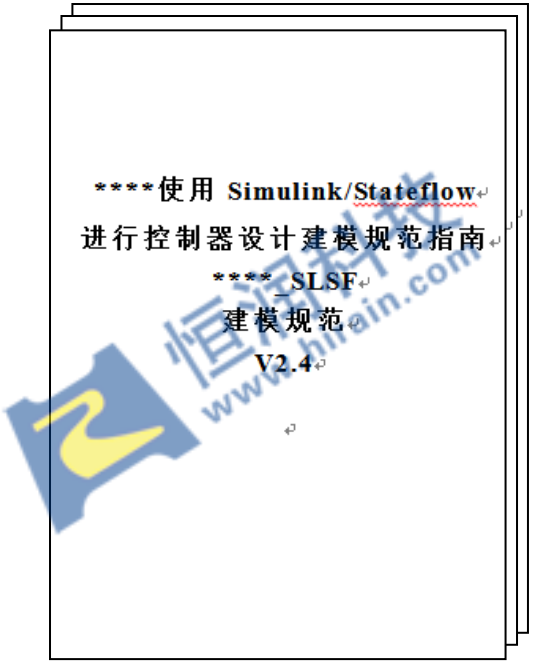
[c] The objective of method 1c is to impose principles of strong typing where these are not inherent in the language.

制定建模规范

- 可读性好：清晰、易读、风格；
- 高效的工作流：维护、变更、复用、可裁剪；
- 高效的仿真效率：快速、便于分析；
- 便捷的验证性能：测试、集成；
- 高效的代码生成：代码质量、安全性等；

- 建模规范——布局和外观
- 建模规范——可靠的语言子集
- 建模规范——使用样式模板
- 建模规范——数据类型
- 建模规范——……

- 企业目前的开发现状（技术水平，研究内容）
- ISO26262对建模和编码的风格指南
- 编码标准要求：MISRA C：2012
- 参考并裁剪目前国内外已有的建模规范指南
- 企业专家经验的不断丰富



恒润科技
HIRAIN TECHNOLOGIES

Conclusion

>>了解建模规范

建模规范是什么
建模规范目的是什么
建模规范谁定的
建模规范应用场景是什么

>>建模规范实例

外观和布局
可靠的语言子集
使用样式模板
数据类型(Data Type)

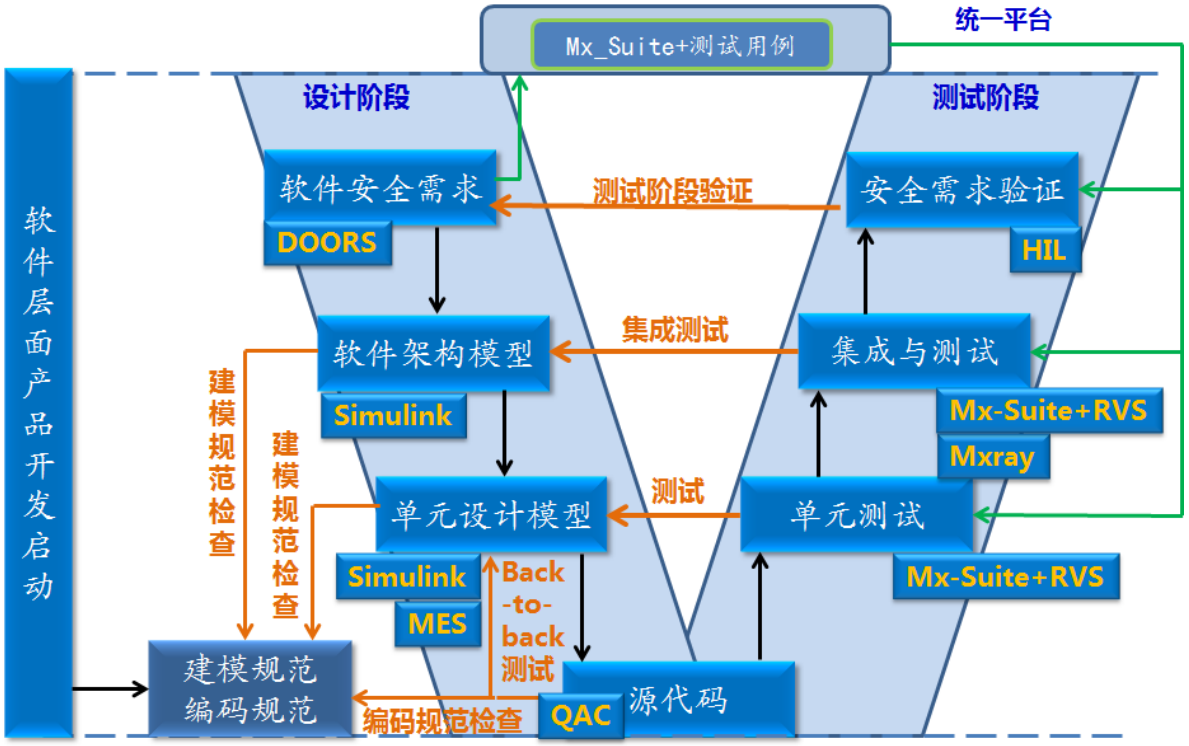
>>ISO26262标准要求

建模规范需要覆盖的规则
（Topics to be covered by modeling guidelines）
如何制定建模规范

打个广告：培训及咨询服务

◆ 基于模型开发培训

- 基础工具使用培训
- 建模规范培训
- 模型测试与验证培训
- 代码生成高级培训



◆符合ISO26262软件开发与测试咨询服务

- 系统需求
- 系统架构模型+单元需求
- 基于需求+建模规范建模
- 建模规范检查
- 模型静态作错误检查
- 模型测试
- 自动生成代码
- 代码规范检查
- 代码/模型背靠背测试
- 模型集成和集成模型质量评估

打个广告：功能安全软件开发工具链