白皮书

规避 5 大流程陷阱，顺利实现 ISO 26262 合规

基于模型的设计的实践参考

MathWorks®

简介

ISO® 26262 正在迅速成为汽车安全相关系统研发的事实标准。今天，几乎所有研究安全相关功能的工程师都在采用 ISO 26262。

开发企业可以根据自身的特定流程和目标适当运用这份指南，加快实现 ISO 26262 合规。具体需要考虑的因素包括：

- ISO 26262 标准推荐的功能安全活动
- 具体应用的汽车安全完整性等级 (ASIL)
- 开发流程中会使用的工具

这份白皮书介绍了可能会造成 ISO 26262 合规问题、导致 ISO 26262 评估失败的常见陷阱。同时，这份白皮书还会提供建议，帮助您规避这些陷阱。

ISO 26262 流程陷阱

ISO 26262 标准分为 12 部分，从功能安全需求管理到软件开发流程所必需的属性，方方面面均有涵盖。绝大部分与软件开发相关的要求可见于标准第 6 部分。如果企业计划在开发流程中采用基于模型的设计，则必须确定采用基于模型的设计的具体环节和方式。为了便于完成这项工作，MathWorks® 的 IEC Certification Kit 提供了相应的指南，帮助用户使用 MATLAB® 和 Simulink® 产品建立完善的 ISO 26262-6 合规工作流程。

IEC Certification Kit 可以作为 ISO 26262-6 实施的起点。这一套件通过文档模板和参考工作流程为采用基于模型设计的用户实现 ISO 26262 合规提供指导。

在了解标准的内容后，企业可以采取以下步骤，实施现有流程与 ISO 26262-6 合规流程之间的差距分析：

1. 确定将要开发的电气系统和组件的 ASIL 要求。
2. 确定将要遵循的 ISO 26262-6 标准流程要素。
3. 将选定的流程要素映射到企业现有的开发流程。
4. 分析并理解差距及有待改进之处。
5. 制定流程改进策略和实现计划。

无论开展何种流程转型活动，差距分析都是其中的关键环节。遗憾的是，许多企业在启动 ISO 26262 项目之初低估了项目的严谨性要求。如果抱着“边做边改”的心态开展项目，往往会导致项目延误，或在产品认证期间才发现遗漏了某些重要步骤。

MathWorks 咨询服务部门在基于模型的设计 ISO 26262 差距分析方面有着极为丰富的实践经验。这项服务旨在为开发企业的 ISO 26262-6 合规流程和工具使用方法提供直达实现层级的客

观评估。这项服务不仅可以发现可能出现的流程合规问题，还会提出工具使用建议。这些建议往往不局限于开发流程，还会涵盖建模技巧和工具应用最佳实践。

MathWorks 在与各企业开展合作的过程中发现以下五种常见陷阱：

1. 缺乏针对设计和实现的软件架构策略
2. 没有定义清晰、映射明确的 ISO 26262 合规流程
3. 基本开发环境没有自动化
4. 没有交付物存档策略
5. 未利用供应商提供的工具鉴定套件

1. 缺乏针对设计和实现的软件架构策略

对于功能安全和架构设计团队而言，制定符合产品功能安全目标的策略至关重要。ISO 26262 允许的软件开发方式主要有以下两种：

1. 基于系统要求的最高 ASIL 评级开发所有软件单元和组件。
2. 根据不同的 ASIL 和 QM （质量管控）评级分别采用不同的开发流程。

某些开发企业选择方案 1，原因很简单：一个流程可以用于所有软件单元。这最初看来似乎是一个不错的选择，但在实际应用中，涉及的工作量极为庞大，难以发挥架构设计的简便性优势。因此，很多功能安全和架构设计团队选择方案 2。采用方案 2，企业可将部分定为 ASIL A – D 级的单元视为高评级，对其使用依赖性失效、失效模式与效应分析 (FMEA) 等安全分析方法，并将软件的剩余部分视为 QM 单元。

完成分析后，就需要适当设计电气系统和软件架构，妥善隔离不同等级的 ASIL 和 QM 组件。隔离又称“互不干扰”(Freedom from Interference)，详见 ISO 26262-6:2018 附录 E。为避免不同 ASIL 等级之间发生交互，以致降级或损害其他 ASIL 功能，互不干扰是必要的。附录 E 探讨的主要概念中，有三个值得注关注：

- 时序和执行
- 内存
- 信息交换

在基于实时操作系统的嵌入式系统中，必须对时序和执行进行深入分析。在软件单元设计和开发期间，应仔细考虑并管理内存和信息交换。根据我们的经验，开发企业通常可以创建概念化设计，却无法将设计转换成 Simulink 中的正确实现。要达成隔离，离不开某些建模方式和模型配置，如模型引用、内存分区和自定义的信息交换方法。MathWorks 在《使用 Simulink 开发 ISO 26262 应用的 11 项最佳实践》中说明了推荐的建模方式和模型配置。

《使用 Simulink 开发 ISO 26262 应用的 11 项最佳实践》中讨论的主题。

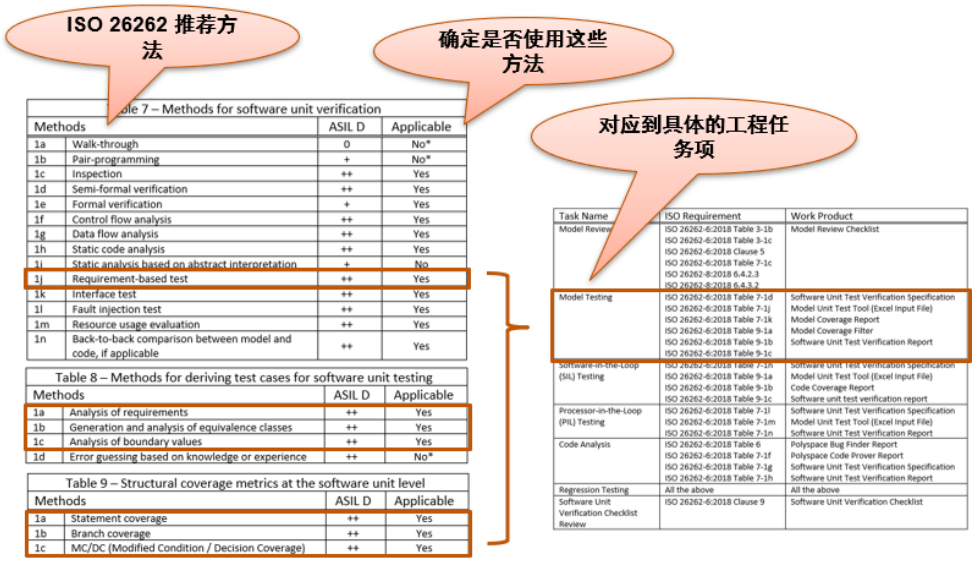
上述白皮书提出了一些最佳实践，可以根据不同的应用需求（包括混合关键性应用）有选择地使用和自定义。由于不具备此类指南，很多企业最终不得不进行大量修改才能实现互不干扰。如果可以在着手开发前解决相关问题，返工和验证活动工作量将显著减少。

2. 没有定义清晰、映射明确的 ISO 26262 合规流程

在汽车行业，多数零部件供应商和 整车厂都会聘请经验丰富的工程师来开发优质软件。然而，如果向这些开发企业索要阐述整个设计和开发流程的清晰文档，多数企业都无法提供。这些企业高度依赖工程师“把事做对”。如果这些开发企业要接受 ISO 26262 合规审计，则可能无法通过。原因在于，工程师们通常专注于具体的设计活动，较少关心设计决策和成果的证据。目前，工作内容的完整性以及合规性仍主要依赖工程师，由他们根据个人经验确定优先级和重要性。为避免此类问题，开发企业必须在前期定义 ISO 26262 合规流程，确保全面执行定义的所有活动，并提供证据证明实际结果与活动目标一致。

MathWorks 还注意到另一大问题：开发企业往往只是基于对 ISO 26262 要求的粗略理解将现有流程文档化。意识到问题时，通常产品已经开发成熟，并且步入评估的最后准备阶段。这种方法往往会导致返工、重新设计，甚至延误生产计划。对于以符合功能安全标准为目标的应用，务必在计划之初就将开发企业的流程映射到实际标准。针对嵌入式软件开发，ISO 26262-6:2018 提供了约 90 项不同的原则和方法，并相应给出了不同的推荐度。开发企业应首先确定将执行哪些 ISO 26262 标准活动，然后将这些活动映射到内部流程，再指定应将哪些交付物存档为相应活动的证明。

以下示例文档展示了 ISO 26262-6 的一些表格，以及如何将这些表映射到开发企业的内部流程。



示例：将 ISO 26262 第 6 部分映射到开发企业流程。

差距分析服务可包含此类文档映射工作，有助于反映缺少哪些活动和工作。MathWorks 咨询服务可协助您在维持现有生产计划的同时制定配套的实现计划。这是一个重要步骤，因为当开发企业进入审计流程，这份文档可显示正在开展的 ISO 26262 活动，并可作为功能安全实施计划证据的一部分。这份文档会说明跳过某些活动的原因，以及相应交付物在配置管理系统中的位置。

因此，开发企业有必要针对各项工程活动规划以下三个主要步骤：

- **定义：**创建流程文档，描述开发周期各个阶段需要开展的活动。
- **执行：**贯彻执行这些活动。运用检查清单和设计评审来确保合规性。
- **存档：**确定开发周期各个阶段需要存档的交付物（工作产出物）列表。

在产品开发周期中，越早定义 ISO 26262 合规流程越好。这些任务有助于推动设计决策和实现方法。尽早定义流程也有助于避免评估阶段或生产启动前不必要的返工。

3. 基本开发环境没有自动化

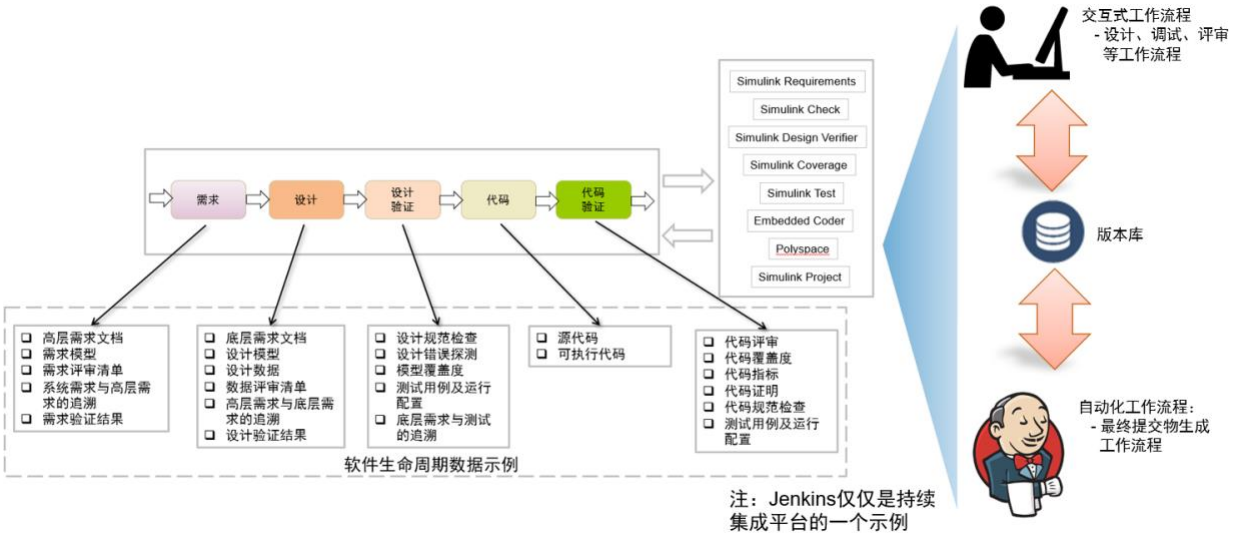
根据我们得到的反馈，首次执行 ISO 26262 项目的开发企业往往发现，规划和执行的严谨性要求远超预期。部分原因在于这些企业对其中某些活动还很陌生，另外，由此增加的任务执行和交付物管理流程也对企业的产能提出了进一步要求。因此，企业应将自动化视为整体 ISO 26262 策略的一部分。必须优化开发流程，确保开发人员能将大部分时间用来创建算法，以及

对照需求验证算法所需的测试用例。除此以外的各个环节均应实现自动化。要增强 ISO 26262 合规性，业内普遍做法是实现自动化。

要推进自动化，其先决条件在于定义流程，对输入、活动和输出作出清晰定义并加以文档化，如前文所述。值得注意的是，自动化进程包含两方面的工作：

其一，为了帮助用户理解需要完成的任务，应具备一个基于桌面自动化工具的交互式工作流程。为此，一种较为简单的方法是部署一组 API 或 GUI，根据项目需求自动配置工作产出物。其中可以包括模型及代码规范、模型或代码生成配置、报告模板等。

其二，桌面自动化支持的这一整套活动也应该体现在持续集成 (CI) 工作流程中。

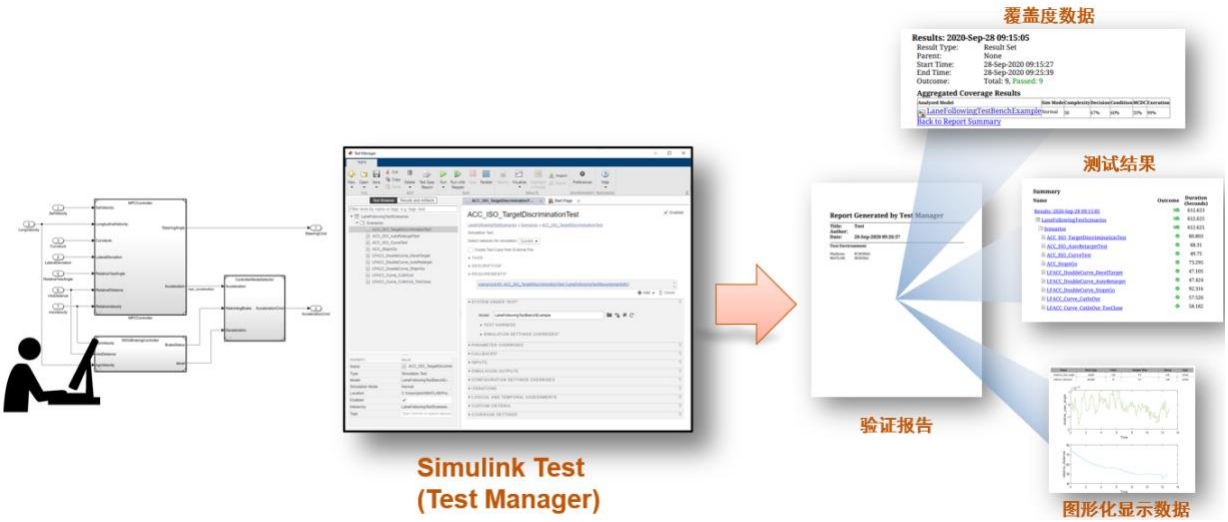


交互式工作流程和自动化工作流程的自动化支持。

在桌面自动化的支持下，用户可在本地 Simulink 环境中与模型交互，同时通过一键式自动化操作简化必要的配置工作。这样，开发人员便可以专注于算法开发，并根据设计规范评审及更新算法。交互式工作流程形成了一道额外保障，确保正确生成最终交付物，并根据定义的规范和指标进行客观验证。

4. 没有交付物存档策略

当企业采用 ISO 26262 工作流程时，至关重要的一点是决定应将哪些交付物存储到配置管理系统。尽管 CI 服务器中有部分流程实现了自动化，或是结果会经过手动检查，但企业仍需将有关这些活动的证明存储到配置管理系统，以保证活动确已完成。为了达成这一目标，每份清单和流程文档均应详细说明应当保存的交付物。



示例：Simulink Test 工作流程及相应的工件。

以上截图是一个验证报告示例，生成的报告可保存至配置管理系统，用于执行测试用例证明。该工件之后可在 ISO 26262 审计中用于评审，如作为版本检查清单的一部分，或是作为某一版本已经完成测试的确认。企业必须制定基线策略，详细说明所用交付物，以及何时会需要重新提交这些交付物。并非所有设计增量或验证报告都是必需的。

在过去的咨询项目中，我们经常发现客户难以得到所有必要的交付物。只有充分理解 ISO 26262 第 6 部分“基于模型的设计工作流程”及相应的 MathWorks 工具链输出，才能获取这方面的信息。这时，MathWorks IEC Certification Kit 就可以很好地发挥作用。该套件根据 ISO 26262-6 中有关主题、原则和方法的表格，在表格内容与适用工具间建立映射。同时，这一套件还包含参考工作流程，可以帮助开发人员将 ISO 26262-6 软件开发工作流程的框架可视化。以下是映射表和参考工作流程示例：

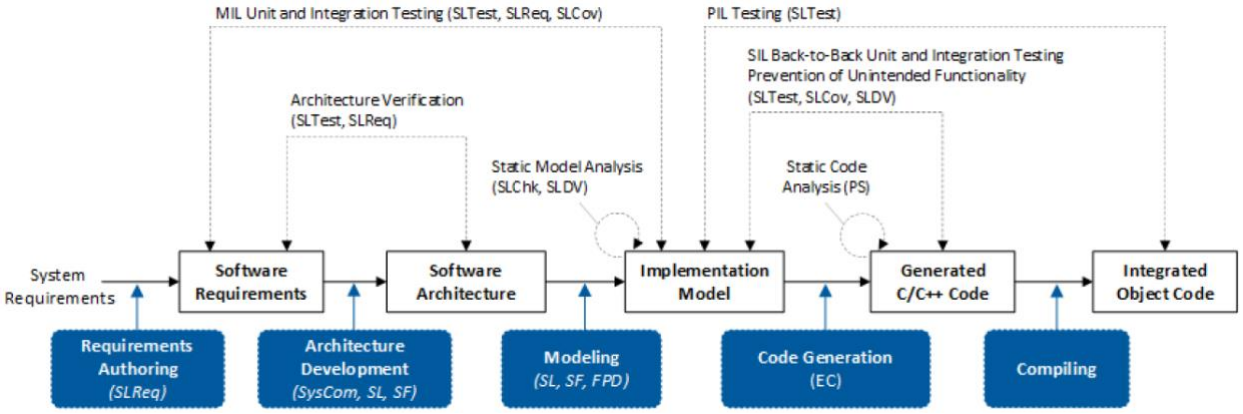
Table 9 — Structural Coverage Metrics at the Software Unit Level

Methods		ASIL A	ASIL B	ASIL C	ASIL D	Applicable Model-Based Design Tools and Processes	Comments
1a	Statement coverage	++	++	+	+	Simulink Coverage – Model coverage analysis Simulink Coverage – Code coverage analysis	During model testing, Simulink Coverage can collect execution coverage at the model level. During SIL and PIL execution, Simulink Coverage can measure the statement coverage of the generated code.
1b	Branch coverage	+	++	++	++	Simulink Coverage – Model coverage analysis Simulink Coverage – Code coverage analysis Simulink Design Verifier – Test case generation	During model testing, Simulink Coverage can collect decision coverage (also known as branch coverage) at the model level. During SIL and PIL execution, Simulink Coverage can measure the decision coverage of the generated code. Simulink Design Verifier can generate test cases that satisfy decision coverage at the model level.
1c	MC/DC (Modified Condition/Decision Coverage)	+	+	+	++	Simulink Coverage – Model coverage analysis Simulink Coverage – Code coverage analysis Simulink Design Verifier – Test case generation	During model testing, Simulink Coverage verification can collect MC/DC coverage at the model level. During SIL and PIL execution, Simulink Coverage can measure MC/DC coverage of the generated code. Simulink Design Verifier can be used to generate test cases that satisfy MC/DC coverage at the model level.

ISO26262 推荐的活动

IEC Certification Kit 推荐的实施方法

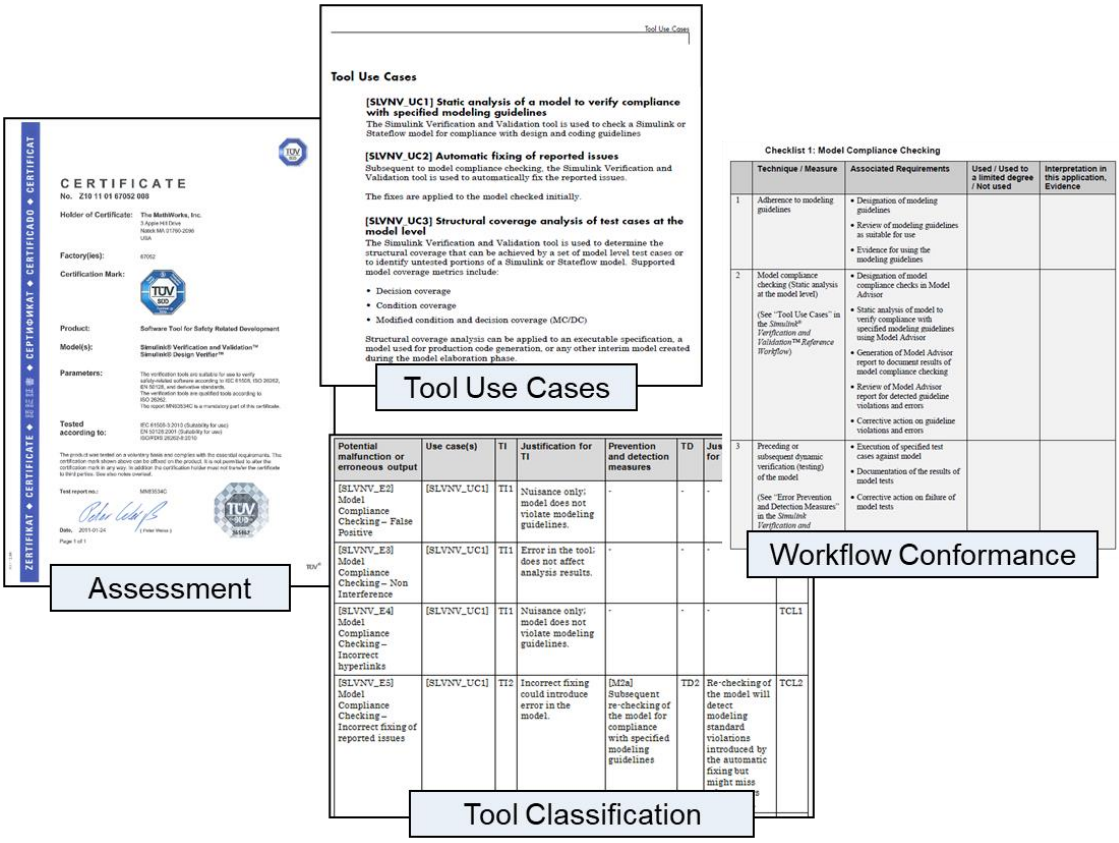
示例：ISO 26262-6:2018 表 9 工具映射



IEC Certification Kit 参考工作流程。

5. 未利用供应商提供的工具鉴定套件

ISO 26262-8:2018 探讨了开发 ISO 26262 合规应用期间所采用的支持流程。同时，该部分还探讨了“工具鉴定”这一重要概念，在汽车行业，这还是一个比较新的概念。倘若缺少工具鉴定流程，自动化工具很可能将错误引入最终产品。如果在开发 ASIL 评级应用时使用了某个工具，则需根据工具置信度 (TCL) 对该工具分级，而后按必要步骤证明该工具可以安全使用。这原本是一项颇为繁琐的工作。幸运的是，许多工具供应商都提供了工具认证套件，使这项工作大为简化。MathWorks 同样推出了工具认证套件。



IEC Certification Kit 预鉴定工件样本。

以上截图是 MathWorks IEC Certification Kit 文档示例。该套件提供每个工具的分级分析，分析基于工具的用例、潜在误动作以及错误检测和预防方法。如果工具的分级不是 TCL 1，则还会提供其他材料，如针对工具开发流程的独立评估，以及通过测试用例开展的软件工具确认。

在 MathWorks 的 ISO 26262 差距分析中，我们发现不少客户忽视了这类认证套件的存在，由此导致了许多重复劳动。经评审发现，大部分工具鉴定工作存在交付物缺失和/或分析失误、合理解释不当的情况。评估期间，所有这些因素都可能会引发不必要的返工。

小结

我们分享了在近期 ISO 26262 项目中发现的一系列常见陷阱。希望这些信息能帮助其他汽车工程团队实现 ISO 26262 合规。我们认为，规避这些陷阱的关键在于规划、流程定义、软件架构、报告/存档、自动化和工具鉴定。

联系信息

我们期待聆听您的见解和反馈。

Zhihui Li, zli@mathworks.com

了解更多

ISO 26262 流程部署咨询服务 – 咨询服务概述

MATLAB 和 Simulink 中的 ISO 26262 支持 - 资源