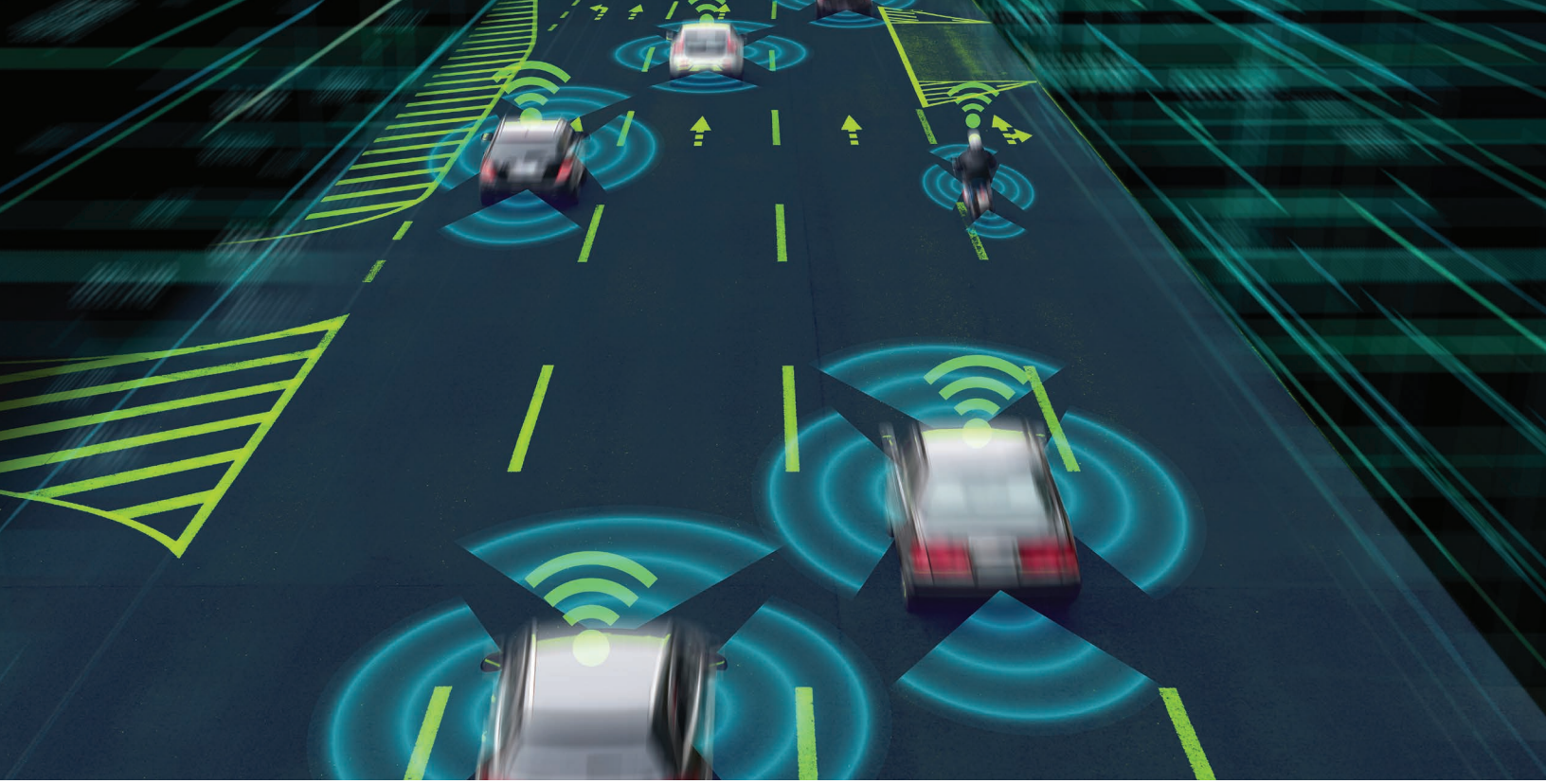

DIGITAL INDUSTRIES SOFTWARE

# 自动驾驶车辆的开发工作流程

**内容摘要**
本文件简要概述了自动驾驶车辆的开发工作流程，这些工作流程符合现行法规和相关标准。自动驾驶车辆是关乎安全的重要系统，由于该系统的定义、设计、开发和部署方式可为安全提供保障，因此从安全的角度来看，在开发过程中遵循明确定义的工作流程至关重要。首先，我们将讨论车辆工程工作流程，考虑到工程对象为自动驾驶车辆，该工作流程将通过运行中监控与报告工作流程继续进行。接下来，在车辆工程工作流程中，我们将重点关注软件开发工作流程。最后，在软件开发工作流程中，我们将深入了解虚拟测试，特别是根据 ISO 21448 和 ISO 34502 等标准进行的基于场景的测试。此外，我们还将讨论虚拟测试的有效性，并重点探讨根据联合国欧洲经济委员会 (UN-ECE) 新评估和测试方法 (NATM) 进行的仿真可信度评估的相关性。

Alexandru Forrai 博士



SIEMENS

# 目录

# 1. 与自动驾驶车辆开发相关的挑战

未来的交通有望使每个人的生活都更加安全和更灵活，并带来积极的经济效益。然而，要将此希望化作现实，特别是当子系统变得更加智能和高度复杂时，就必须测试新车及其架构的每个子系统。

随着复杂性的增加，有必要从根本上改变测试方法并提出新理念，以便在物理和虚拟世界中对车辆进行全面的确认和验证，这一点已在新法规中体现。

为此，联合国欧洲经济委员会 (UN-ECE) 于 2021 年 2 月提出了“自动驾驶的新评估 / 测试方法” (NATM)[1,2]，该框架为自动驾驶系统的安全验证引入了一种多支柱方法（图 1）。

自动驾驶车辆的多支柱安全验证规定了五大认证支柱，它们为安全论证提供了支持。除了众所周知的三大支柱（跟踪测试、真实世界测试和审核）外，该法规还提到了虚拟测试和运行中监控

虚拟测试、跟踪测试和真实世界测试均基于场景，因此我们将在图 1 中看到上述场景目录。在此，我们要强调的是，在虚拟测试、跟踪测试和真实世界测试期间，场景目录均不相同。随着我们从虚拟测试转向真实世界的测试，场景的数量将不断减少，而场景的真实性将不断提升。此外，在虚拟测试和跟踪测试中，我们会遇到更多危急场景，而真实世界的测试中，则很少出现危急场景。

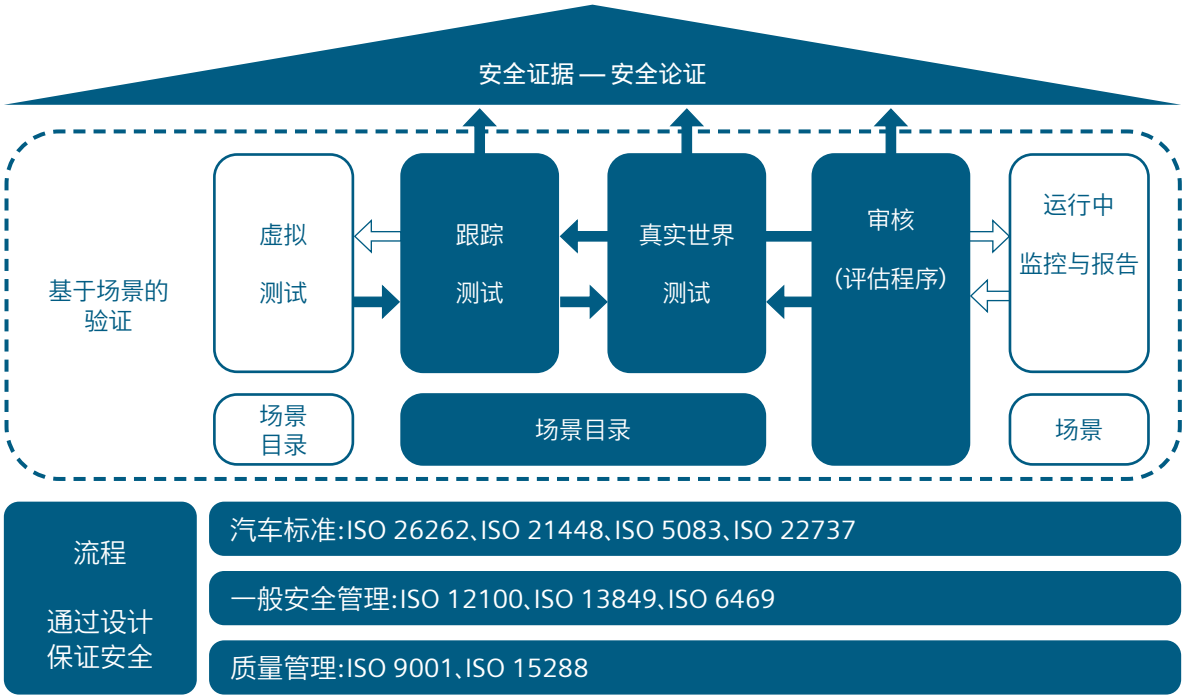


图 1：自动驾驶系统的多支柱安全验证 — UN-ECE NATM。

部署完成后，在监控和报告阶段，相关场景会被记录下来，在场景提取和场景选择完成后，它们会被重新引入虚拟测试、跟踪测试和真实世界测试中。通过对新场景的记录和提取，我们可以发现未知的不安全场景，并持续改进自动驾驶系统。

此外，需要注意的是，根据欧盟立法 [3,4] 和 UN-ECE NATM 进行的自动驾驶车辆认证（参见运行中和监控与报告支柱）完整地引入了持续集成和持续部署工作流程（图 2）。这种持续集成和部署工作流程在软件行业中广为人知（参见 DevOps — 开发和运营）。

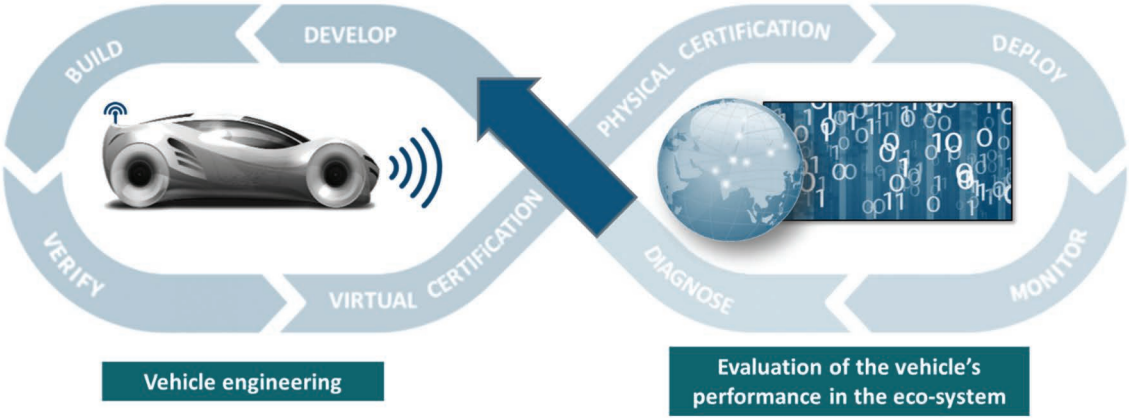


图 2. 按照 UN-ECE NATM 进行的持续集成和持续部署工作流程。

# 2. 车辆工程工作流程

如果我们观察一下工作流程的左侧，便会看到车辆工程工作流程或过程。在本文件中，**工作流程或过程**具有相同的含义，定义为：**为完成任务而需要执行的活动**。

我们观察到，车辆工程工作流程可以通过 ISO 26262[5] 工作流程来进行适当描述，其中系统工程、安全工程、软件工程和硬件工程流程都有单独的过程（图 3）。

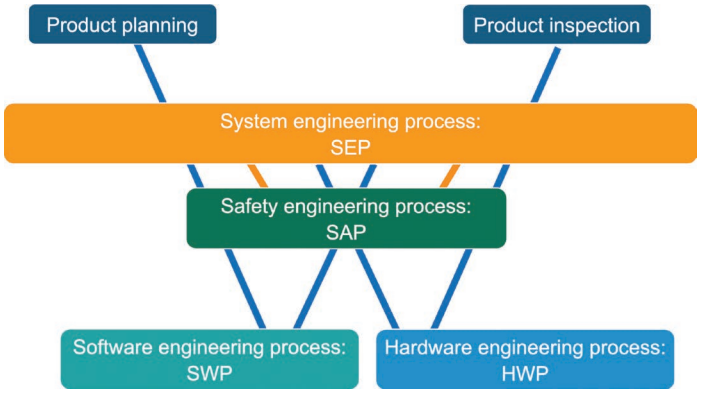


图 3. 符合 ISO 26262 的车辆工程工作流程。

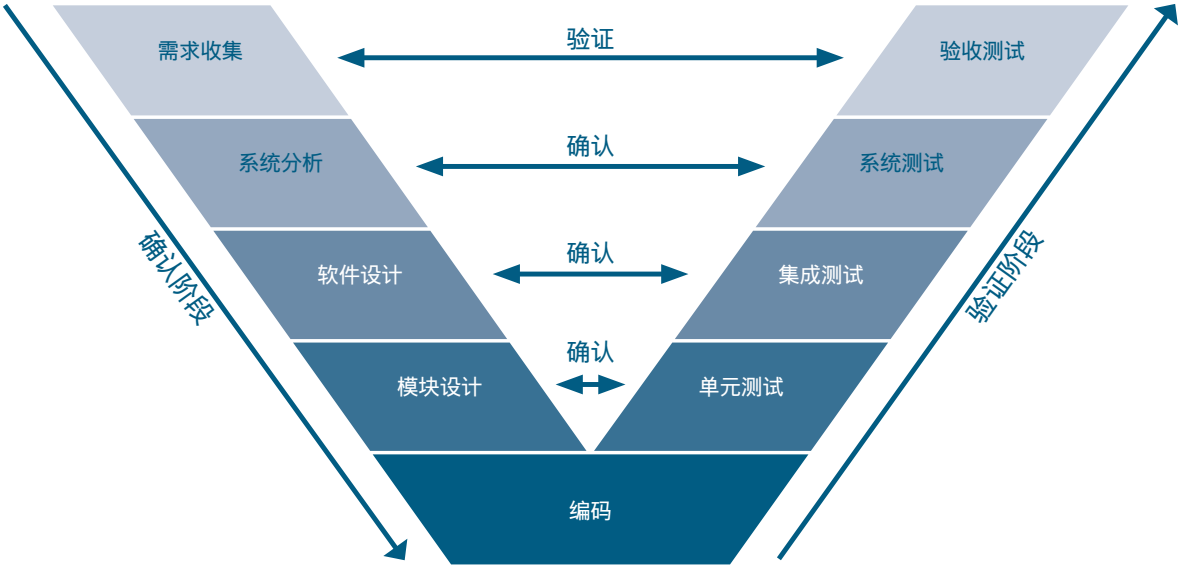


图 4. 符合 ISO 26262 的软件开发工作流程。

由于我们的探讨重点是自动驾驶车辆堆栈的开发，因此我们将主要关注软件开发工作流程。根据 ISO 26262，该工作流程如图 4 所示，而且，对与安全相关的软件开发而言，它是车辆工程工作流程不可或缺的一部分。由于大多数读者都知道软件开发工作流程的每一个步骤，因此我们将不会详细介绍它们。

但是，我们将澄清一些经常造成混淆的术语。在本文件中，确认、验证、认证和保证的定义 / 描述如下：

- 确认：它是一种确定系统是否满足要求的活动，从以下问题角度考虑："我们是否正确地构建了系统?"
- 验证：评估系统是否满足最终用户需求，从以下问题角度考虑："我们是否构建了正确的系统?"另一方面，模型验证即评估模型在多大程度上代表了现实。
- 保证：对系统按预期运行的合理信心。
- 认证：确定系统是否符合一组条件或标准。

**自动驾驶系统的虚拟测试**

就自动驾驶车辆而言，科学界很早就意识到，从经济、技术和安全的角度来看，仅使用基于里程的覆盖范围进行真实世界测试并不可行。

其中一个主要原因是，在真实世界测试中，与安全相关的事件很少发生。因此，显而易见的是，虚拟测试将在对自动驾驶系统的认证中发挥关键作用。当且仅当仿真可信时，虚拟测试的结果才有助于安全论证。

在软件开发工作流程（图 4）中，虚拟测试在集成测试和系统级测试中进行。基本上，在虚拟测试的情况下，我们使用仿真模型代替一个或多个物理元素。软件 / 汽车行业中著名的虚拟测试方法（考虑基于模型的方法）包括 MiL、SiL、PiL、HiL 等，如图 5 所示。由于它们都是众所周知的测试方法，我们在此处不再详述。

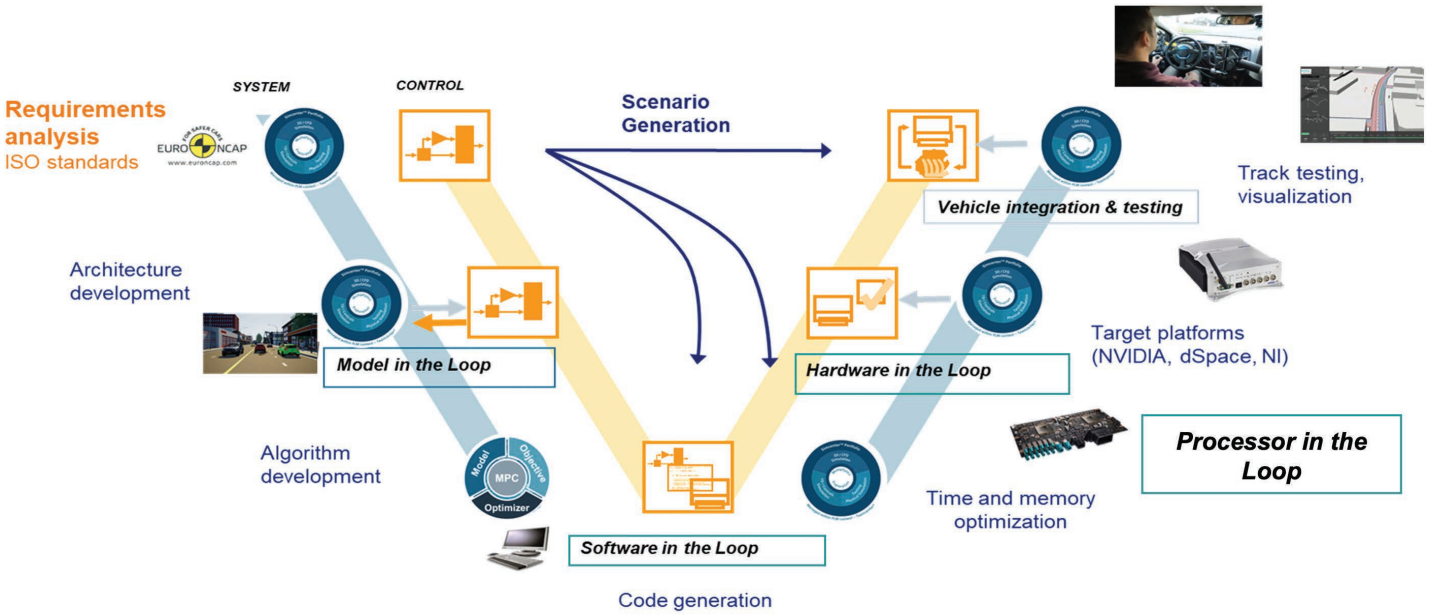


图 5.X 在环软件测试。

我们从“模型在环”开始，通过生成代码转向“软件在环”测试，该测试并非实时执行。在下一步中，如图 6 所示，我们将开始实时执行测试。为此，应该让所使用的模型适应实时运行，并将生成的代码修改为在实时操作系统下运行。如果目标硬件不可用，则可以将其虚拟化，并在 FPGA 平台上运行（硅前“处理器在环”测试）。

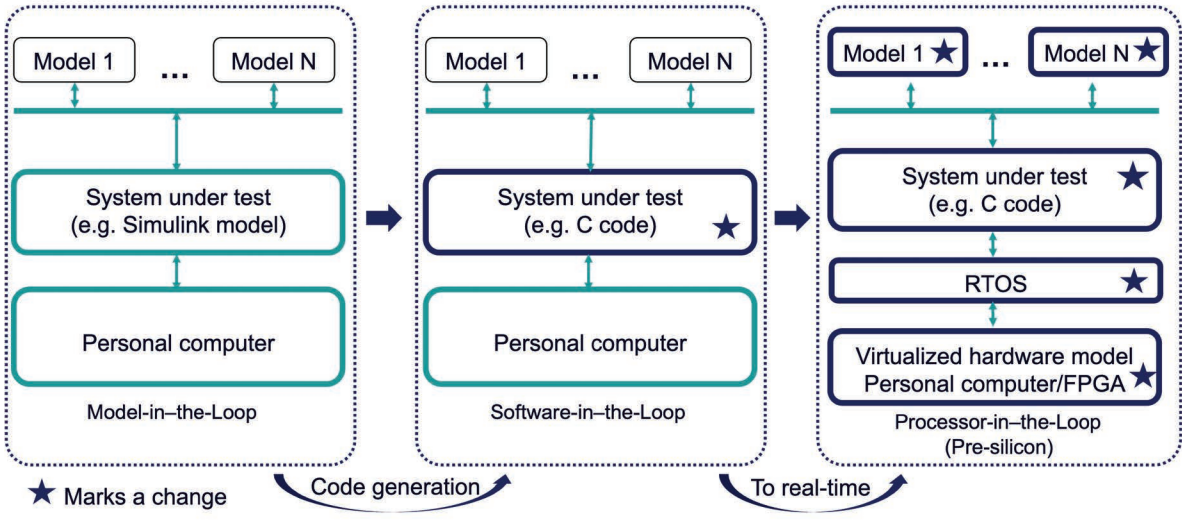


图 6. 从“模型在环”到“处理器在环”。

在图 7 中，我们将展示如何从硅片前“处理器在环”测试向前推进到硅片后“处理器在环”测试。在这种情况下，被测系统可以在评估板上运行。 最后，使用电子控制单元替换评估板，并执行“硬件在环”测试。

此外，确认和验证针对自动驾驶系统(Automated Driving System，ADS）的虚拟测试为重点，可以根据整体验证策略和基础仿真模型的准确性实现不同的标。其中一些目标包括：

- 为整个系统的安全性提供定性或统计置信度。
- 为特定子系统 / 组件的性能提供定性或统计置信度。

与其所有潜在益处相比，这种方法的局限性在于其模型的固有保真度有限。由于模型只能粗略地反映现实，因此需要仔细评估模型是否充分适合替代真实世界来验证 ADS 的安全性。

基于场景的测试是汽车行业中得到广泛认可的成熟测试方法之一，我们将在下一节简要讨论该测试，并介绍相关的工作流程。

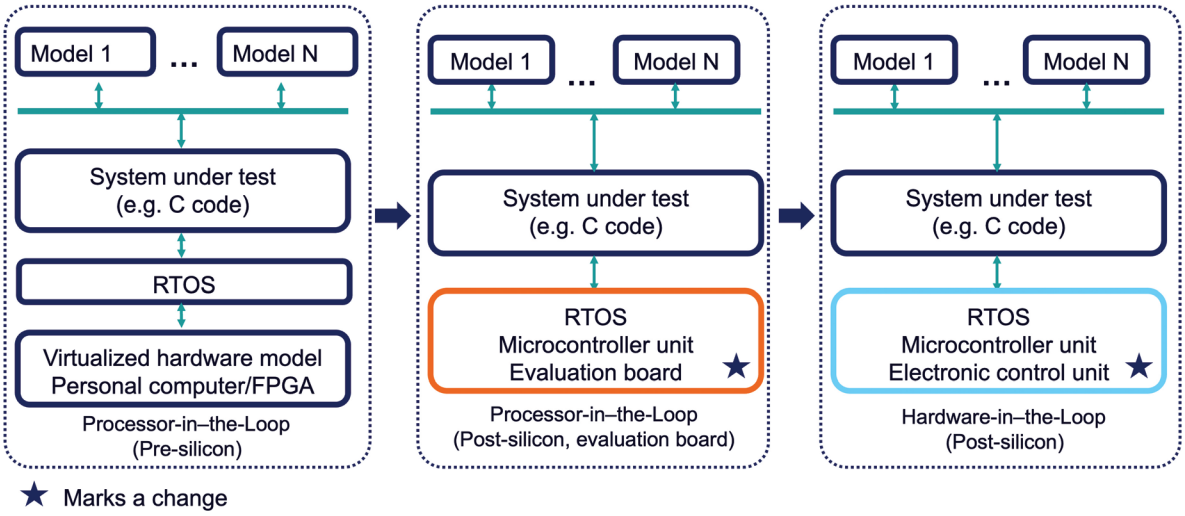


图 7. 从“处理器在环”到“硬件在环”。

# 3. 基于场景的自动驾驶车辆测试和基于场景的测试工作流程

在本节中，我们将首先根据 ISO 21448[6,7] 和 ISO 34502[8] 介绍关键术语和定义，然后说明基于场景的测试工作流程。

**定义：**

**自动驾驶系统 (ADS)**
无论是否局限于特定的运行设计域 (ODD)，都能够共同持续执行整个动态驾驶任务 (DDT) 的硬件和软件。

**被测系统 (SUT)**
通过测试场景进行测试的自动驾驶系统 (ADS)。

**目标车辆**
自主车辆，主车辆，在测试、评估或演示过程中的受试车辆。

**场景**
一系列情景，通常包括自动驾驶系统 (ADS)/ 目标车辆，以及它们在执行动态驾驶任务 (DDT) 过程中的互动。

**情景**
所有实体的快照，包括但不限于自动驾驶系统 (ADS)/ 目标车辆、背景、动态环境以及所有行动者和观察者的自我表征，以及这些实体之间的关系。

**实体**
场景中被关注的元素。

**静态实体**
在场景中不会经历状态变化的实体（例如，交通标志就是一个静态实体）。

**动态实体**
在场景中会经历状态变化的实体（例如，交通信号灯是一个动态实体）。

**测试场景**
用于测试和评估自动驾驶系统 (ADS)/ 目标车辆的场景。

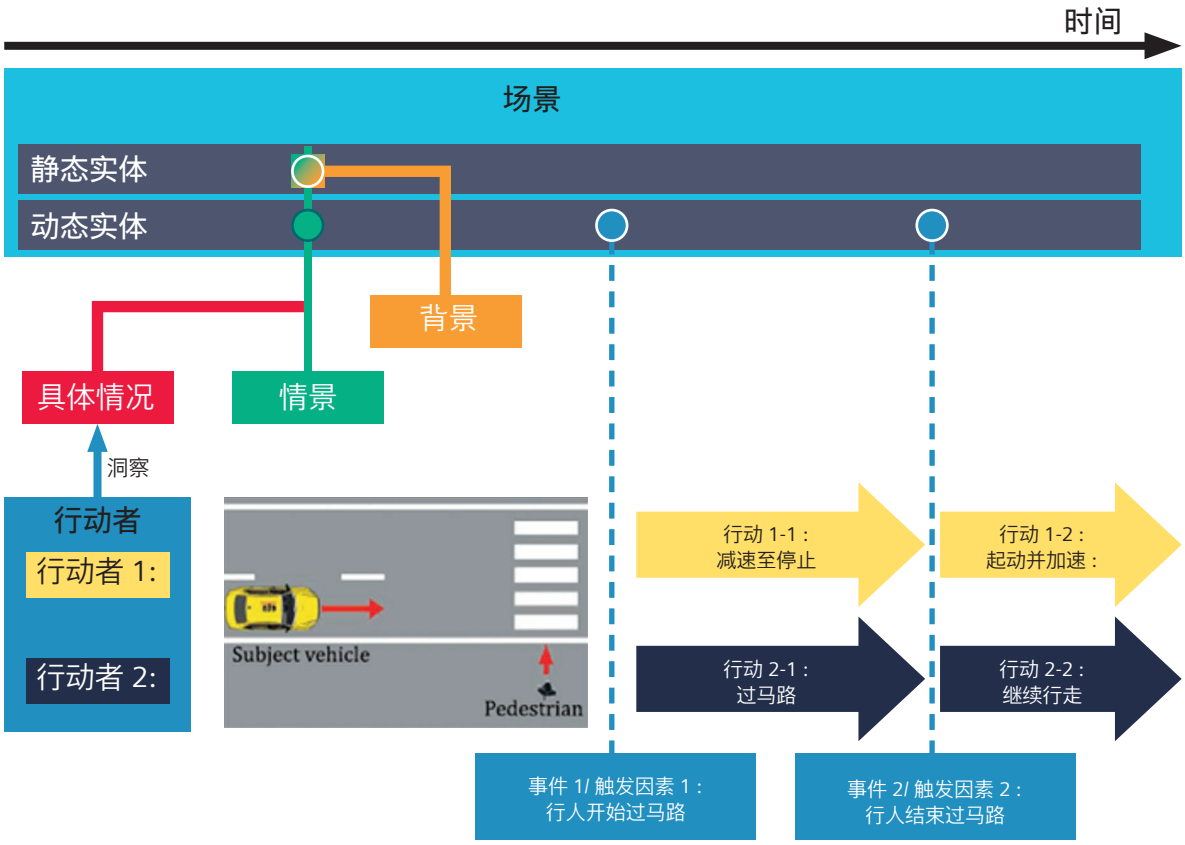


图 8. 符合 ISO 34502 的场景的相关各项之间的关系。

**基于场景的测试**
是一种软件测试活动，它使用测试场景来评估*自动驾驶系统 (ADS)/ 目标车辆*。

上文图 8 说明了场景的各相关术语之间的关系。

在清楚地了解了有关场景和基于场景的测试的概念之后，我们必须能够以不同的方式描述场景，同时考虑抽象程度和细节水平，如图 9 所示。此外，图 10 显示了这些场景在开发过程中的使用方式。

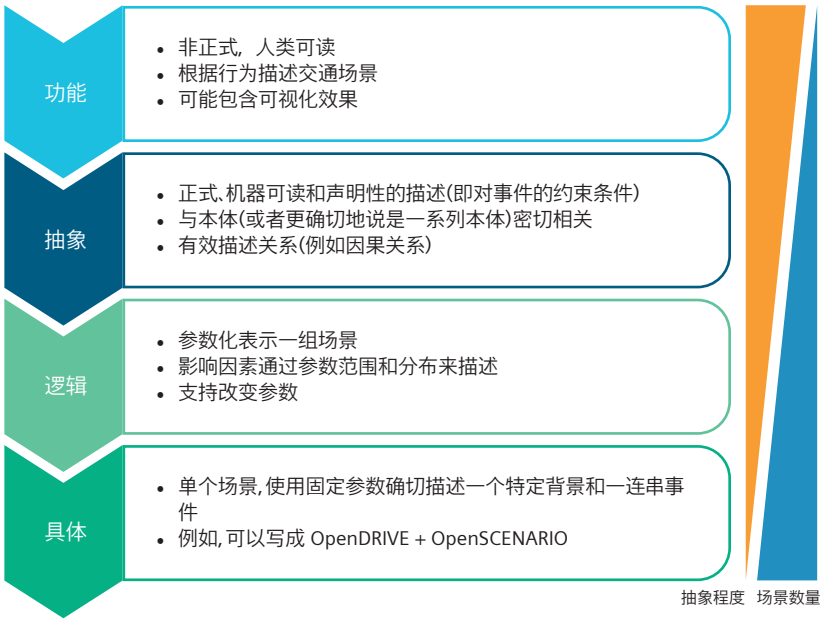


图 9. 符合 ISO 34501 的功能、抽象、逻辑和具体场景之间的关系。

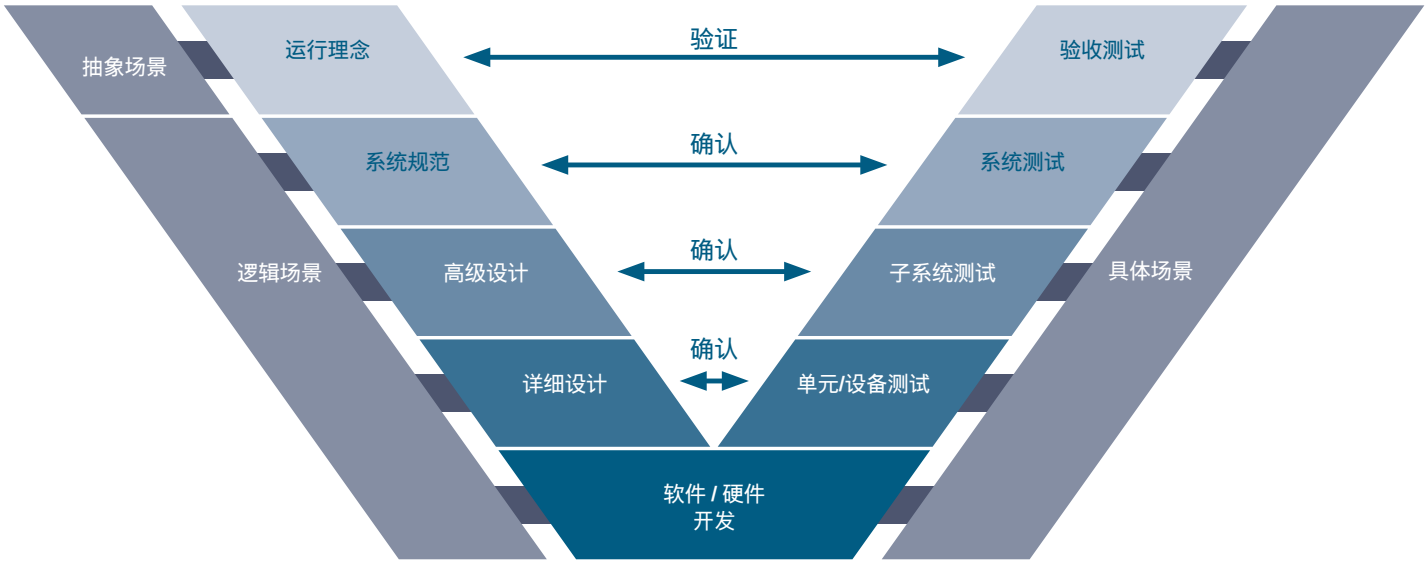


图 10. 开发过程中使用的场景。

ISO 21448 的主要目标之一是在功能有限的情况下对自动驾驶系统进行安全评估。如图 11 所示，ISO 21448 定义了一种渐进式工作流程，即（在场景空间中）逐渐扩大已知和安全场景的区域，减小未知和不安全场景的区域，具体方法是首先发现这些场景，然后采取适当的工程措施确保它们安全。

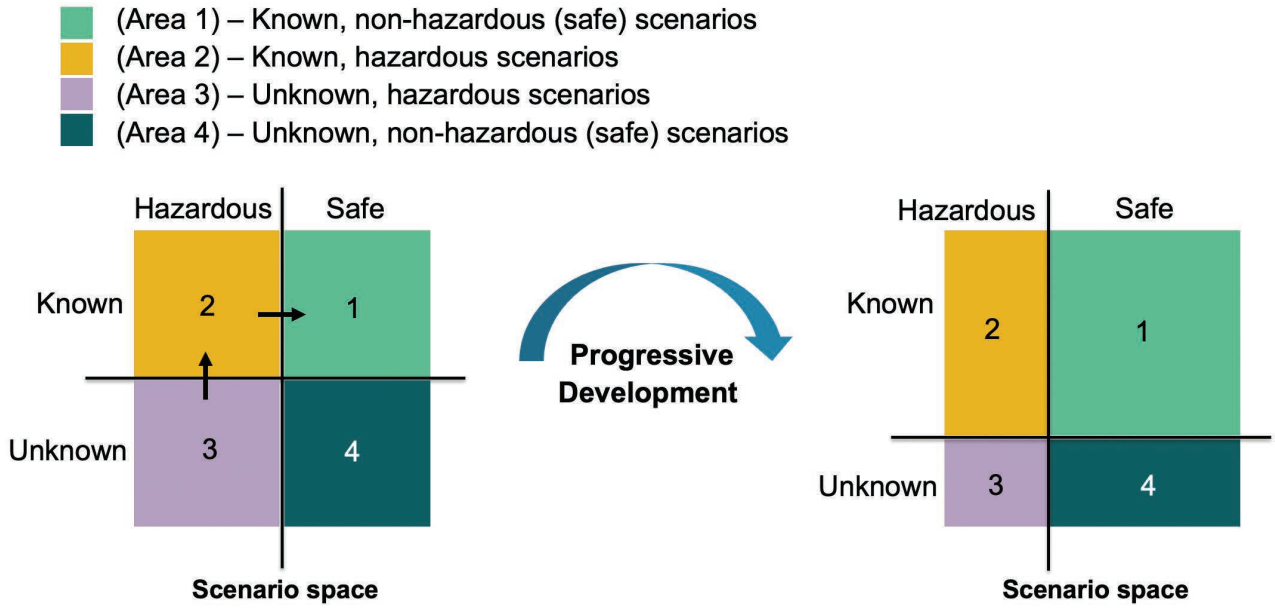


图 11. 符合 ISO 21448 的基于场景的测试工作流程。

图 12 显示了根据 ISO 35402 进行的基于场景的测试的详细工作流程。

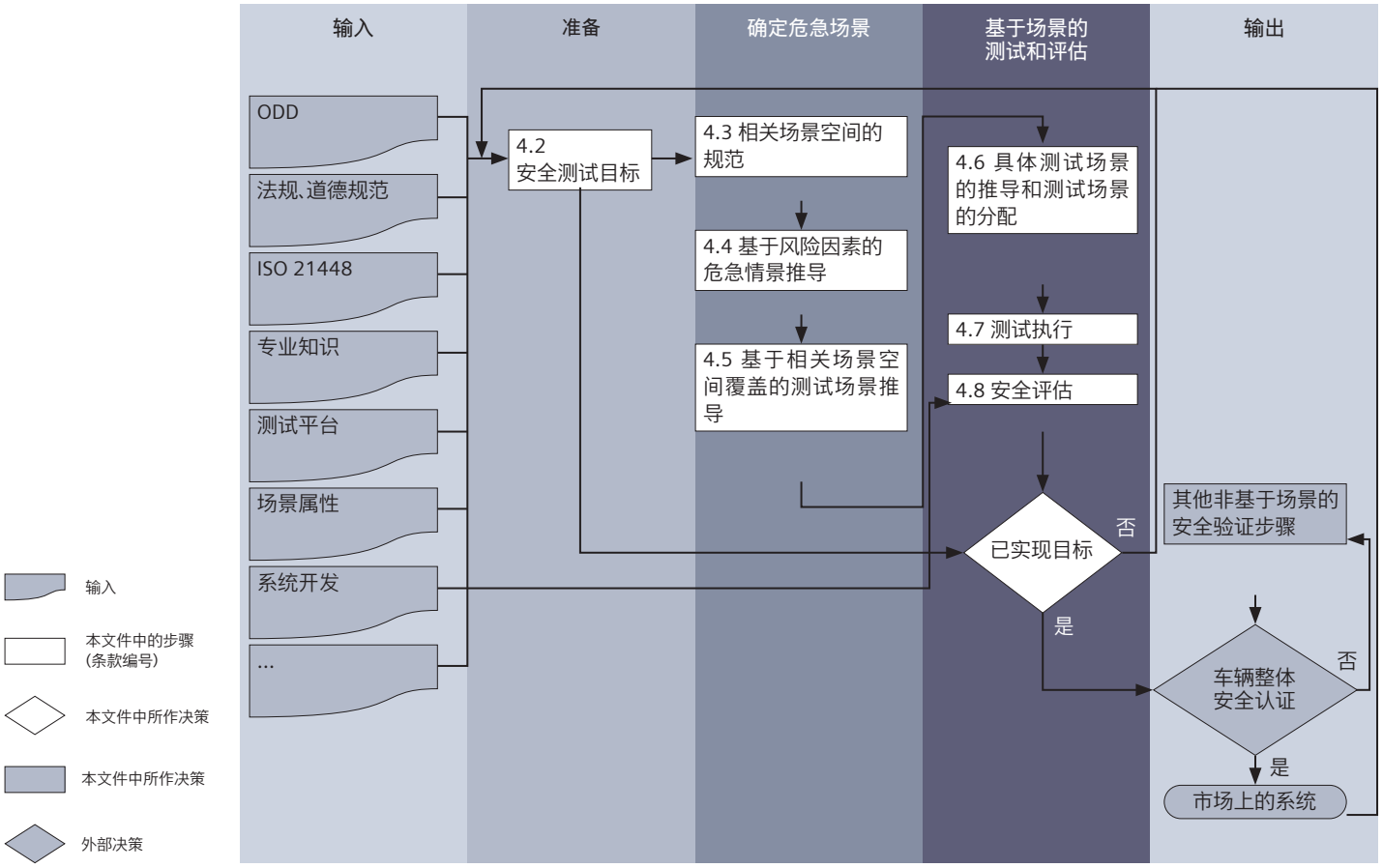


图 12. 符合 ISO 34502 的基于场景的测试和评估工作流程。

这种基于场景的测试工作流程密切相关，并且支持 ISO 21448 中提出的工作流程，下文将对此进行说明。

在图 12 中，第 4.3 项确定了可能导致危险场景的可合理预见风险因素，进一步具体说明 ISO 21448:2022 第 7 条（图 13）的内容。对这些风险因素进行结构化处理以后，可以生成危急场景并将其编译到场景目录中，以便用于测试。因此，本文件中确定风险因素并对其进行结构化处理的方法有助于确保尽可能涵盖 ISO 21448 (SOTIF) 中已知的危险场景。例如，通过考虑运行设计域 (ODD)[9] 的边缘情况，可以推导出此类已知的危险场景，譬如，主车辆夜间行驶在浓雾弥漫的城市道路上，而车辆前方有行人在过马路。

在图 12 中，第 4.5 项确定了需要测试的具体场景及其相应的平台（这也是定义确认和验证策略的重要步骤），有助于处理 ISO 21448:2022 第 9 条（图 13）中所述的问题。

最后，在图 12 中，第 4.3 至 4.8 项有助于处理 ISO 21448:2022 第 10 条和第 11 条（图 13）中所述的问题。通过在安全评估过程中补充已知的危险场景，并改变这些场景的一些特性 / 属性，我们还可以探索未知的危险场景，并*减少未知场景的空间和数量*。

注意：除了车辆层面外，基于场景的安全评估过程或其部分环节还可以应用于系统、子系统或组件层面。因此，该过程适用于相应的被测 ADS。

图 14 以决策树形式显示了 ISO 21448 放行工作流程。

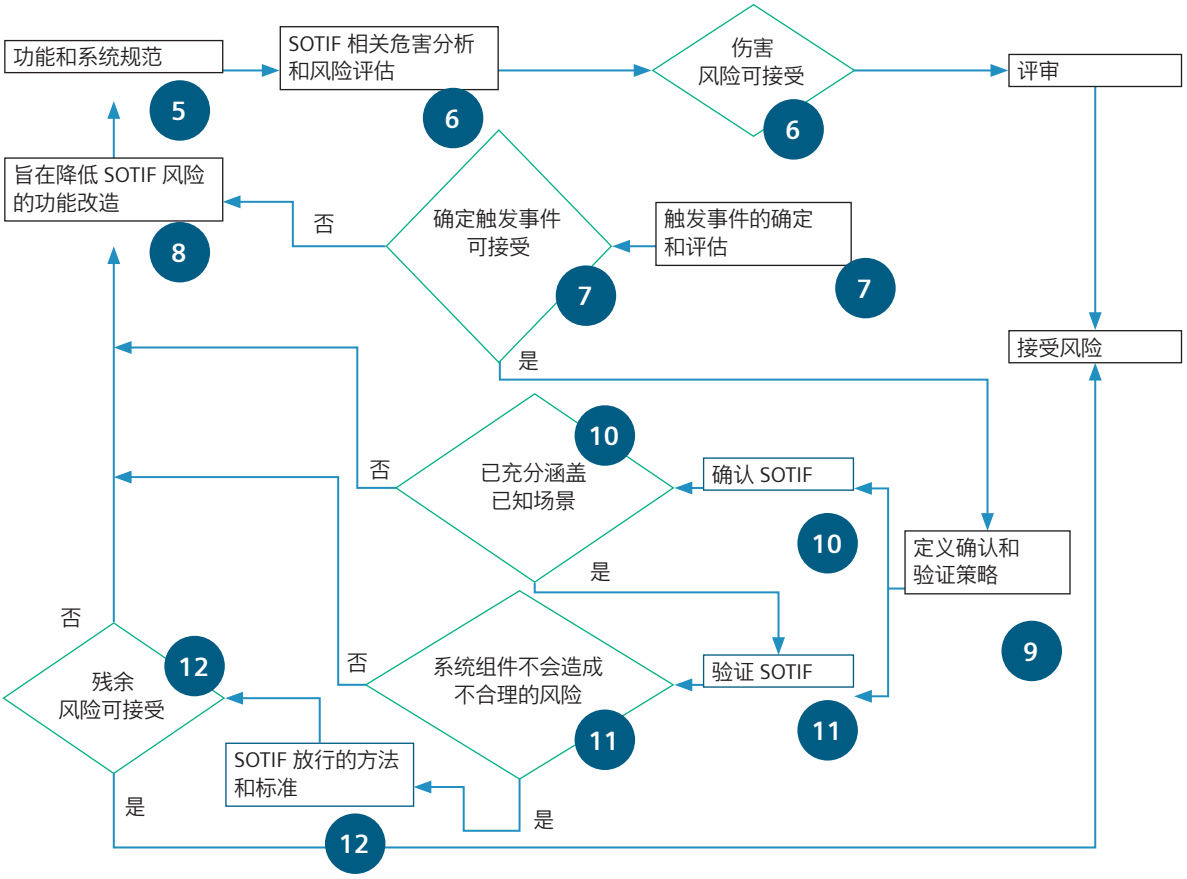


图 13. 符合 ISO 21448 的基于场景的测试工作流程。

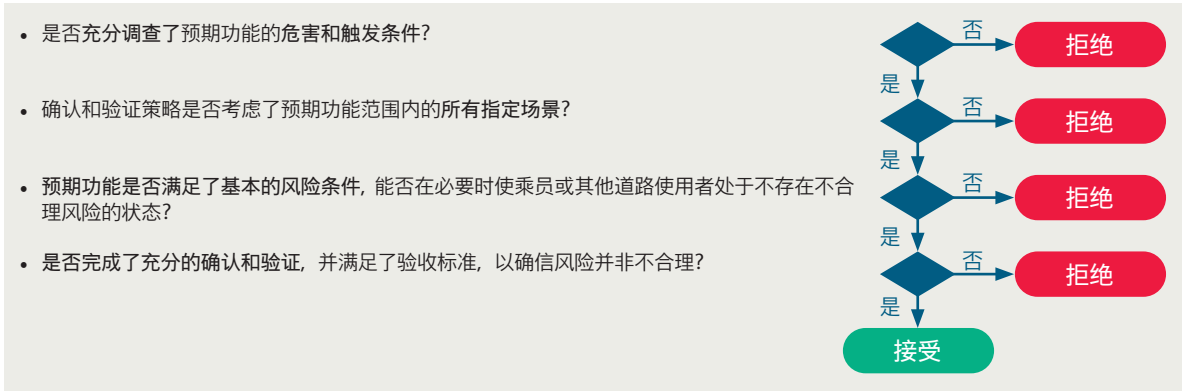


图 14. 基于场景的测试 — ISO 21448 放行工作流程。

到目前为止，我们只讨论了车辆工程工作流程，重点探讨了应用于自动驾驶系统的基于场景的测试工作流程。*运行中监控与报告工作流程虽然相关，但超出了本文件的范围。*

然而，必须注意的是，*持续集成和持续部署软件*工作流程不能一对一地应用于安全相关或安全关键型软件开发。本质区别在于，在 ADS 的安全相关或安全关键型软件开发完成后，即在*车辆工程*工作流程结束时，该软件必须由权威机构（公告机构）认证 / 批准。只有在该软件通过认证后，才能对其进行部署。尽管这个中间步骤（即认证）非常重要，且不能跳过，但它却使*集成和部署*工作变得不连贯。

此外，未经认证的无线 (OTA) 软件更新应仅针对非安全相关软件进行。因此，应将安全相关与非安全相关的硬件和软件分开，如图 15 所示。

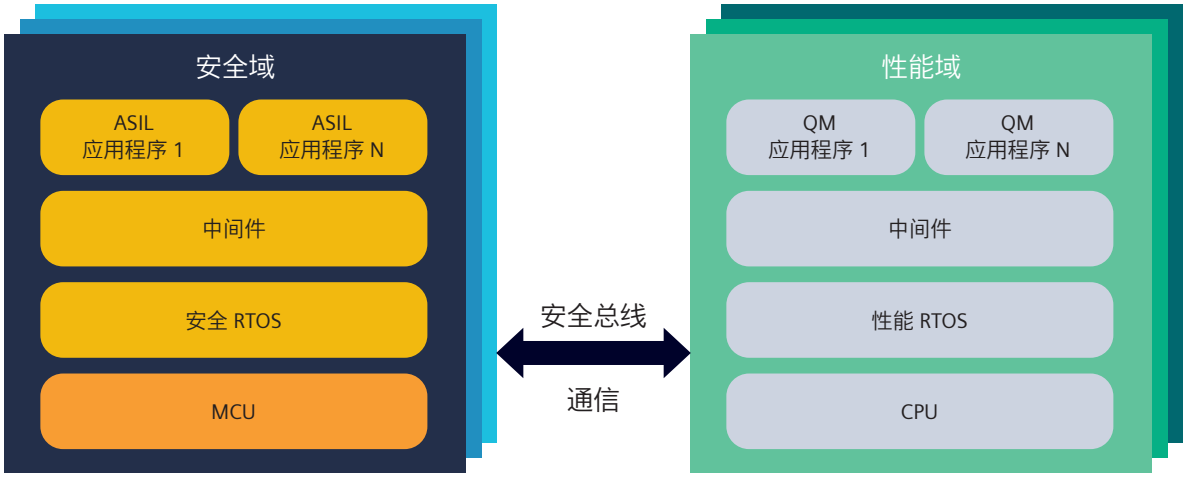


图 15. 安全域和性能域的分离。

# 4. 仿真可信度评估工作流程

在本文件的最后一节中，我们将简要讨论仿真可信度评估[1]。我们已经看到，虚拟测试可以成为认证的一个支柱，这意味着认证过程依赖于虚拟测试的结果。由于虚拟测试依赖于模型，因此在自动驾驶系统的安全验证期间，必须评估模型是否充分适合替代真实世界。

鉴于此，应评估图 16 所示仿真模型和仿真环境的可信度，以确定结果与实际性能相比的可转移性和可靠性。尽管可以使用其他工具，但图 16 中仍提到了虚拟测试期间可以使用的西门子工具。

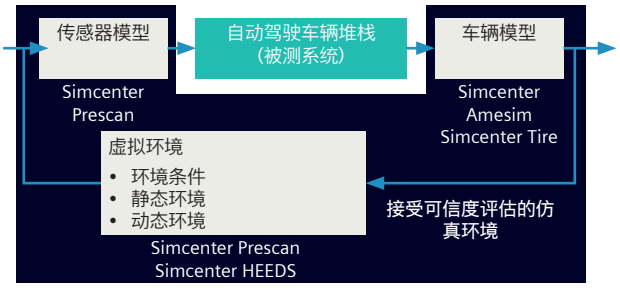


图 16. 接受可信度评估的仿真环境。

除了仿真模型和仿真环境外，可信度评估还扩展到涵盖模型和仿真管理。所有这些方面都体现在图 17 中，该示意图代表了根据 NATM[1] 进行仿真可信度评估的工作流程。

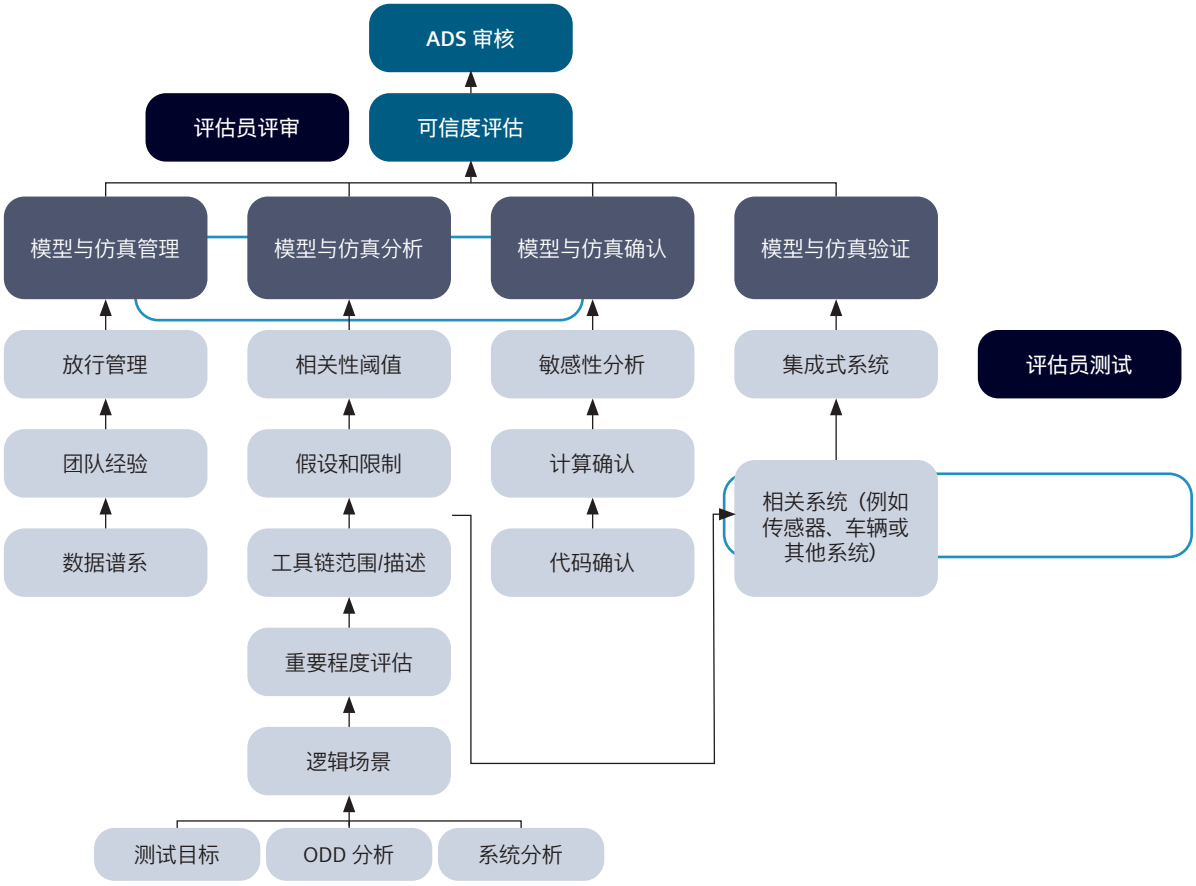


图 17. 用于仿真可信度评估的可行工作流程。

## 参考文献


1. 联合国欧洲经济委员会（United nations economic commission for Europe，UN-ECE）《自动驾驶的新评估 / 测试方法》(NATM)，unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-58.pdf，2023 年 11 月查阅。

2. UN-ECE 关于自动驾驶系统安全要求的指南和建议 WP.29-187-10e.pdf (unece.org)，2023 年 11 月查阅。

3. 欧洲议会和理事会第 (EU) 2019/2144 号欧盟法规，eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R2144&from=EN，2023 年 11 月查阅。

4. EU-2022/1426 — 第 (EU) 2022/1426 号委员会实施条例，出版办公室 (europa.eu)，2023 年 11 月查阅。

5. ISO 26262《道路车辆 — 功能安全》，2018 年第二版。

6. ISO 21448《道路车辆 — 预期功能安全》，2022 年第一版。

7. ISO 22737《用于预定路线的低速自动驾驶 (LSAD) 系统》，2021 年第一版。

8. ISO 34502《道路车辆 — 自动驾驶系统的测试场景 — 基于场景的安全评估框架》，2022 年 11 月第一版。

9. BSI 1883《自动驾驶系统 (ADS) 的运行设计域 (ODD) 分类法 — 规范》，2020 年第一版。

**Siemens Digital Industries Software**

美洲：1 800 498 5351

欧洲、中东及非洲地区：00 800 70002222

亚太地区：001 800 03061910

如需其他地区电话号码，请单击此处。

**Siemens Digital Industries Software** 通过 Siemens Xcelerator 数字商业平台的软件、硬件和服务，帮助各规模企业实现数字化转型。西门子全栈式工业软件和全面的数字孪生可助力企业优化设计、工程与制造流程，将创新想法变为可持续的产品，从芯片到系统，从产品到制造，跨越所有行业，创造数字价值。Siemens Digital Industries Software – Accelerating transformation。

**siemens.com/software**



85809-D2-ZH 2/24 LOC