用于自动驾驶汽车开发、测试与验证的场景

Till Menzel, Gerrit Bagschik and Markus Maurer
Institute of Control Engineering
Technische Universität Braunschweig
Braunschweig, Germany

摘要—

2016 年更新的 ISO 26262 标准，代表了车辆安全的关键电气/电子系统安全指导开发的最新技术，可以应用于高级驾驶辅助系统（ADAS）和自动驾驶系统的开发和验证。标准规定了基于 V 型开发模式的各个阶段所要求的工作内容和输出产品。在 V 型开发模式的各个阶段，均可应用基于场景的方法，来获得相应的工作输出产品。为了完成各个阶段的工作产品，场景必须关注各种方面，如人类可理解的符号或通过状态变量的描述。在应用基于场景的方法时，不同开发阶段对场景细节程度和场景描述方式的需求存在矛盾。本文作者讨论了 ISO 26262 标准中不同阶段对场景描述的要求，提出了满足一致性的场景描述方法，并演示了如何系统建立满足不同阶段需求的场景。

I. 前言

目前市场上已有 SAE 等级 1 和 2 [1] 的驾驶员辅助系统和自动化系统（奥迪交通堵塞试点 [2] 或 Waymo 自动驾驶汽车 [3]）宣布遵循 3 级（有条件自动化）和 4（高度自动化）。引入更高级自动化的挑战是确保这些车辆系统以安全的方式运行。对于驾驶辅助系统，安全证明是通过在测试场地和公共道路上驾驶里程来提供的。但对于更高级别的自动化，基于测试里程的验证的解决方案在经济成本上不可接受。[4]。作为基于距离的验证的替代方案，我们引入了基于场景的方法。其中的关键是有目的的改变和验证自动驾驶汽车的运行场景。因此，必须在开发过程中系统的记录与推演场景，以确保生成可追踪的场景。

ISO 26262 标准是开发安全关键电气/电子车辆系统的指南，因此为功能安全方面的车辆引导系统的开发提供了框架。根据 ISO 26262 标准，可以利用场景来支持开发过程。例如，场景有助于推导需求，开发必要的硬件和软件组件，并在测试过程中证明这些组件的安全性。然而，这些场景的不同应用导致对 ISO 26262 标准的每个开发阶段中的场景表示的不同要求。

本文贡献为基于 V 模型的开发过程中的场景提出了三个抽象级别。通过这种方式，可以在概念阶段的高级抽象中识别场景，并在开发过程中进行详细和具体化。这允许采用结构化方法，从根据 ISO 26262 标准的项目定义开始，然后进行危害分析和风险评估（HARA），最后得到必要的安全验证和验证测试用例。因此，作者基于 Ulbrich 等人 [5] 的定义提出了对“场景”这一术语的扩展定义，并介绍了功能，逻辑和具体场景的抽象级别。

本文组织结构如下：第II节基于选定的相关工作提供了一个简短的动机，这些工作涉及自动驾驶功能的开发过程中的场景，场景的抽象使用级别以及术语场景的现有定义。第 III节推导并分析 ISO 26262 标准开发过程中场景表示和使用的要求。之后，第IV节部分为场景定义了三层抽象，并展示了这些场景表示如何在开发过程中相互转换。最后，第 V节作出一份总结。

II. 相关工作

Ulbrich 等人. [5] 分析跨多个学科的术语场景，并提出自动化车辆领域的一致定义。本文中作者引用的场景定义源自 [5] 中的场景定义。

Go 和 Carroll [7] 指出场景在不同学科中有不同的用途，但用于描述场景的元素在所有情况下都是相似的。因此，可以在几个细节层次和不同形式的符号中描述场景。场景可以用正式，半正式或非正式表示法表达 [7]。这种区别暗示了自动车辆开发过程中多个场景的抽象层级。

一些论文提出了利用场景来生成自动驾驶车辆开发过程中的工作产品的方法。Bagschik 等人. [9] 在危

险分析和风险评估的过程步骤中开发了符合 ISO 26262 标准的产生潜在危险情景的程序。该过程利用了交通参与者的抽象描述和自然语言的情景。文章中分析了所有可能的场景元素组合，纳入自动驾驶车辆项目范围内的 SAE L4 [1] 有限用例中功能失效的描述。

Schuldt 等人 [11] 开发基于场景的测试过程，通过使用 4 层模型生成系统测试用例。Bach et al. [12] 提出了一种基于模型的场景描述方式，其具有空间和时间关系，作为 ISO 26262 标准的开发过程中的一般场景描述。该场景描述是针对高速公路上的 ACC 系统的场景原型实现的，并且呈现了结果。

所提到的论文利用具有不同抽象层级的场景来实现车辆引导系统的功能和安全开发。术语“场景”尚未统一定义，这使得难以对场景在开发过程中的作用达成一致的理解。因此，作者将在以下部分中推导并分析有关场景的需求。

III. 基于场景的设计和测试过程

2016 年出版的 ISO 26262 标准展示了车辆引导系统开发过程中的功能安全技术。[1] ISO 26262 标准提出的开发流程如图 1所示。利用场景生成所需工作产品的过程步骤在图中以红色方框标出。场景可以支持 ISO 26262 标准的整个开发过程，从概念阶段到技术产品开发，再到系统验证和测试。因此，必须定义不同流程步骤产生的场景需求。而在整个开发周期中，要求在不同抽象级别上对所用场景有一致性表述。以下部分涉及 ISO 26262 标准定义的开发过程的工作产品，并推导出各流程的场景需求。

A. 概念阶段的场景

在标准第 3 部分的概念阶段，该标准对项目进行了定义，进行了危险分析和风险评估，并引出功能安全概念。

项目定义包括功能定义、系统边界、操作环境、法规需求以及对其他项目的依赖关系的描述。基于这些信息，可以派生出可能的操作场景。Reschka[14] 建议识别安全驾驶状态，并根据操作场景指定名义行为。此过程中的操作场景应以较抽象的方式描述，并以一种易于理解的方式表示。由 ISO 26262 标准定义的下一个使用场景的过程步骤是危害分析和风险评估。危害分析和风险评估包括两个步骤：情景分析和危险识别，以及危险事件的分类。在情况分析中，所有操作情况[2]和导致危险事件的故障行为中的操作模式均需要描述。因此，故障行为可以理解为偏离指定的正常行为。之后，将使用汽车安全完整性等级（ASIL）对危险情景进行评级，其中包括操作情景和故障行为的组合。ASIL 分类的参数是操作场景的暴露程度，可能的严重程度以及危险场景的可控性[3]。为了确定这些参数，危险场景的描述必须包括静止环境（场景）和可以与自动驾驶车辆交互的所有交通参与者。根据现有技术，危险情景的分析由专家进行。因此，必须以自然语言制定危险情景。根据他们的专业领域，人类专家在用于描述场景的术语方面的细节水平各不相同。因此，在危害分析和风险评估的过程步骤中，功能视角的统一词汇表是必要的。此外，为了确保专家之间的共同理解，词汇表中的术语必须以半正式的方式组织。

在 ISO 26262 标准的概念阶段 [C]，场景必须满足以下需求：

C1 人类专家应该能够用自然语言来描述该场景。
C2 场景应以半正式的方式表示。

B. 系统开发阶段的场景

一旦分析了危险场景，就会形成功能安全概念。为了实现功能安全，须提出技术安全需求。与功能需求不同，技术安全需求描述了可量化的条件。例如，保持与其他交通参与者的安全驾驶距离的安全需求通过以米为单位的距离来确定。因此，每个危险场景都必须从半正式的自然语言表述（概念阶段）转换为利用状态量表述（系统开发阶段）的方式。这些状态量的列表是对场景的精确描述，但由于细节水平抽象程度高，人类专家无法直观地处理这些状态量。为了减少场景的数量，可以给定状态量的取值范围，或者可以进一步划分有效/无效的取值范围，即安全/不安全的取值，从而明确系统边界。场景的详细表述确保了能以可验证的方式制定开发项目的需求。方案的详细表述确保了可以以可验证的方式制定对待开发项目的需求。这是 ISO 26262 标准的步骤 4-9 中的安全验证的必要条件。总而言之，场

[1] 车辆引导系统整系统的开发包括额外平行开发流程，其涵盖功能开发等其他方面。

[2] 作者指出，根据 Ulbrich 等人的说法，ISO 26262 标准中使用的术语“操作情况”应该被称为“操作情景”。[5]。

[3] 场景的可控性包括自动驾驶车辆的驾驶员/乘客的可控性以及其他车辆的可控性交通参与者

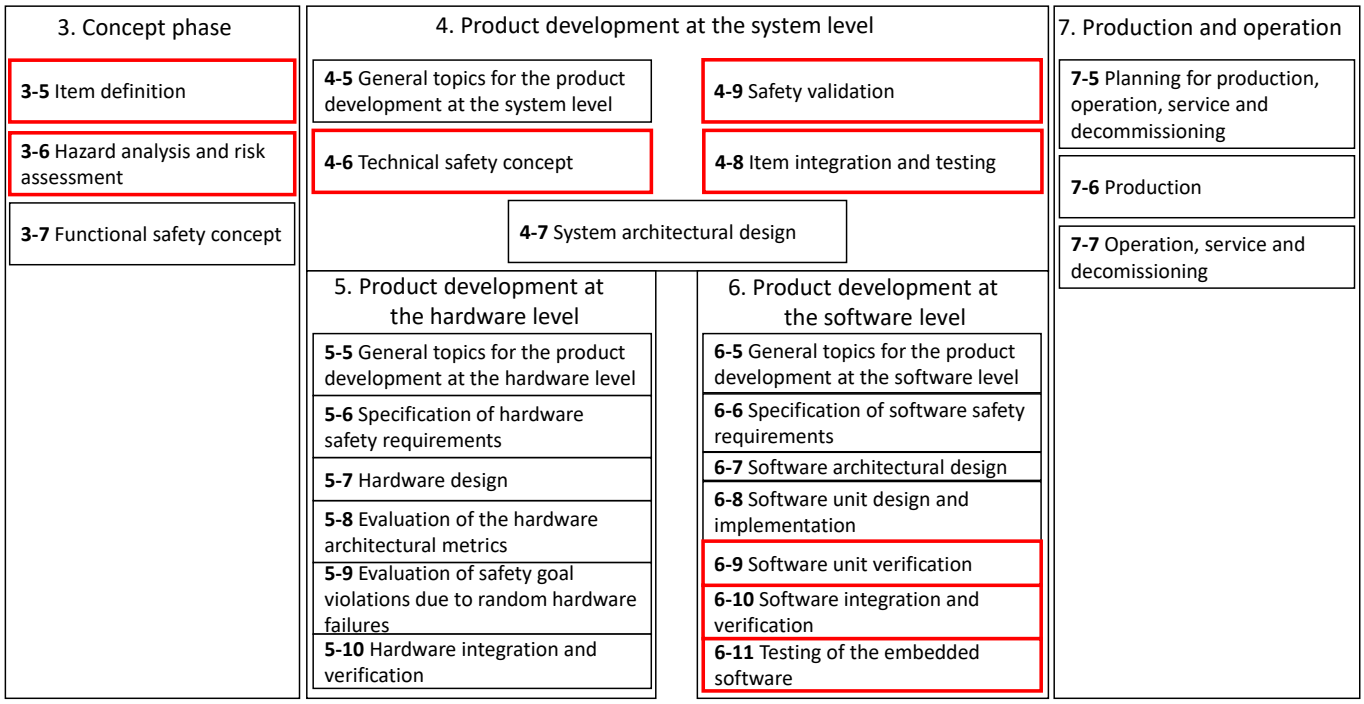

图 1. ISO 26262 标准中提出的开发过程概述。红色显示的流程步骤可以利用方案来生成工作产品。

景必须满足 ISO 26262 标准的系统开发阶段 [S] 中要使用的以下需求：

S1 场景应包括用于场景表示的状态量的参数范围。
S2 场景应为每项参数指定一个标记，以支持自动处理。

C. 测试与验证阶段的场景

在测试阶段，将验证系统是否满足了前述流程中指定的需求。这一过程，验证必须依据标准 [13, part 8, section 9.2]，系统地计划、制定、执行、评估和记录。每个测试用例规范必须独立于测试方法包括以下信息 [13, part 8, section 9.4.2]：

1) 一个独特的标识
2) 要验证的工作产品的引用参考
3) 前提条件和配置[4]
4) 环境条件
5) 输入数据，包括它们的时间顺序
6) 预期的行为，包括可接受的变化

测试用例生成的一个难点在于输入数据的规范性，包括每个参数的时间序列，这些时间序列实质上影响测试对象的行为。同时，由于高度连接的系统，输入数据可能不包含任何不一致[5]，而是代表一致的场景。概念阶段已经给出了系统的操作环境和可能的操作场景，这是为测试用例派生一致的输入数据的基础项目定义中使用的场景由语言表达，并在抽象的详细程度上制定。要在测试用例的范围内使用这些抽象场景，必须详细指定场景并使其具体化。场景的详细规范可以在技术安全需求规范的范围内进行 [13, part 4, section 6]. 技术安全要求描述了项目如何对可能影响安全目标的外部影响做出反应。通过这种方式，技术要求还定义了必须确保正在开发系统的功能参数范围。必须在验证过程中测试该参数空间，因此必须考虑该生成测试用例。此外，还必须将场景转换为正式表达，以确保之后测试用例的可执行性及可复现性。场景必须通过不同的测试方法（如模拟或现场测试）定义测试用例执行所需的所有参数。因此，在详细指定场景的步骤中，必须从基于有组织的术语的非正式描述到基于物理系统状态值的形式描述进行转换。为了生成测试用例的输入数据，必须从指定场景的连续参数范围中选择离散参数值。Schuldt [15] 提出使用等价类，边界值分析和组合方法来识别代表性样本。这种方法提供了系统生成的测试用例，但缺乏确

[4]在系统变体的意义上。

[5]这里不一致的意思：故障注入可以在以后用作测试方法。

定有意义的测试覆盖率的方法。为了确定有意义的测试覆盖率，必须考虑测试概念，场景选择和必要的测试方法。在具体步骤中系统地导出，然后正式描述的场景代表被测系统的一致输入数据。因此，派生的场景可以在测试用例的范围内用于验证所实现的系统。总而言之，场景必须满足 ISO 26262 标准的测试阶段 [T] 中要使用的以下要求：

T1 场景应该通过具体的状态值来描述，以确保其可执行性和可复现性。

T2 场景应具备一致性。

T3 场景应该以一种高效的机器可读的方式表示，以确保自动化测试的执行。

D. 对场景需求的分析

表**??**说明了指定的要求与场景描述的矛盾。一方面，需求概念阶段 C1 表示对抽象的语言场景表示的需求，另一方面，需求 S2 和 T3 表示对有效的机器可读场景表示的需求。由于语言表示很难由机器处理，并且人类无法读取大小有效（主要是二进制编码）的数据格式，因此需要不同形式的场景表示。类似地，S1 和 T2 场景需求表示的不同细节程度。一方面，需求 S1 通过状态空间中的参数范围来表述场景。这种表示形式在确定要测试的具体值方面提供了多个自由度。另一方面，需求 T2 要求包括具体参数值来表述需求。这是测试用例可重复执行的必要条件因此，机器可读的场景必须支持两种不同的细节程度。

IV. 设计和测试过程中的场景术语

正如上一节所述，在 ISO 26262 标准的开发过程中应用场景时，对场景的细节程度的需求是存在矛盾的。在下一节中，作者将为场景建议三个抽象级别，并展示如何在开发过程中将这些抽象级别相互转换。作者将场景划分为三个抽象级别：功能场景（Functional scenarios）、逻辑场景（Logical scenarios）和具体场景（Concrete scenarios），如图2所示。

A. 功能场景

功能场景是场景表述的最抽象级别。在概念阶段，这些场景可用于项目定义、危险分析和风险评估。它们以语言表示，以确保人类专家可以轻松理解现有场景，讨论它们并创建新场景。作者提出了以下定义：

> 功能场景包括语义级别的操作场景。通过语言场景符号来描述域内的实体以及实体间的关系。场景是一致的。用于描述功能场景的术语表应由一般用例或域内专用的术语组成，并且可以具有不同的详细程度。

功能场景的表述包括实体和实体之间的关系，不同场景的描述方式必须是一致的。首先需要制定一个术语表，这个术语表包括不同实体的术语（车辆 A、车辆 B）和这些实体的关系短语（车辆 A 超越车辆 B）。

功能方案所需的详细程度取决于实际开发阶段和正在开发的项目。在词术语表的定义过程中必须考虑这两个方面。例如，高速公路飞行员需要术语表来描述道路几何形状和拓扑结构，与其他交通参与者的交互以及天气状况。相反，停车库行驶需要术语表来描述建筑物的布局，而天气条件可能是无关紧要的。如果使用综合术语表来描述实体和这些实体的关系，则可以从术语表中导出大量场景。对于一致的功能场景泛化，术语表的所有术语必须是不同的。定义域实体的术语来源是，例如，道路交通法规或德国高速公路建设标准等实际标准和指南 [16]。

图3为在高速公路行驶的一个功能场景：一辆轿车和一辆卡车正行驶在右侧车道上，轿车跟随卡车行驶。在这个例子中，道路特征主要描述为横断面布置情况和几何结构特征。根据项目的用例和域，词汇表必须包含用于描述这些特征的附加术语，例如用于布局的“三车道高速公路”，以及用于几何的“直线”或“回旋曲线”。通过从定义的术语表中选择其他术语，可以改变场景。

B. 逻辑场景

基于状态空间变量，逻辑场景是对功能场景的进一步详细描述。那些状态空间变量描述了这些实体的实体和关系。在系统开发阶段，可以利用逻辑场景派生出安全需求。为此，逻辑场景通过正式表示法描述状态空间变量的值范围。作者提出了以下定义：

> 逻辑场景以状态空间呈现操作场景。通过定义状态空间内变量的参数范围，可以表达实体特征和实体间的关系。参数范围可以选择用概率分布来确定。此外，不同参数的关系可以通过相关性或数值条件来确定。逻辑场景应包含该场景的形式标记。

表 I
场景需求的矛盾 (⊥ 矛盾标记)

概念阶段		系统开发阶段		测试阶段
人类专家应能够用自然语言制定该领域的术语。	⊥	场景应包括用于场景表述的状态值的参数范围。	⊥	场景应通过具体的状态值建模，以确保其可重复性并能够使测试方法执行场景。

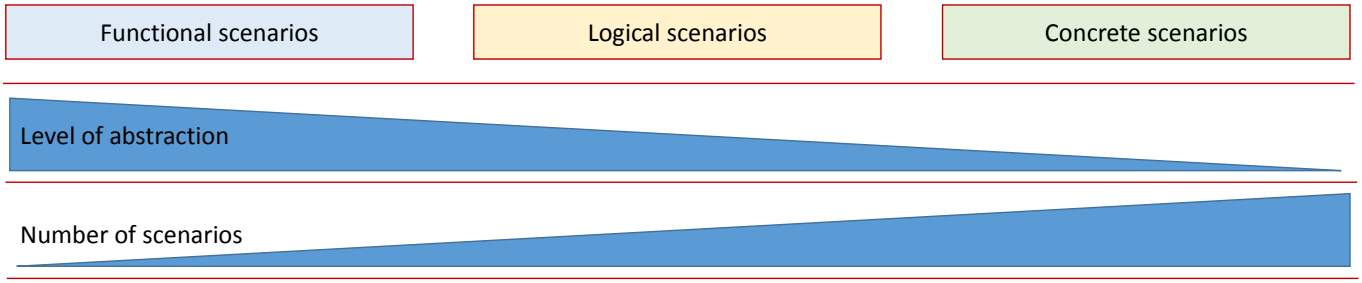

图 2. ISO 26262 标准开发过程中的抽象程度

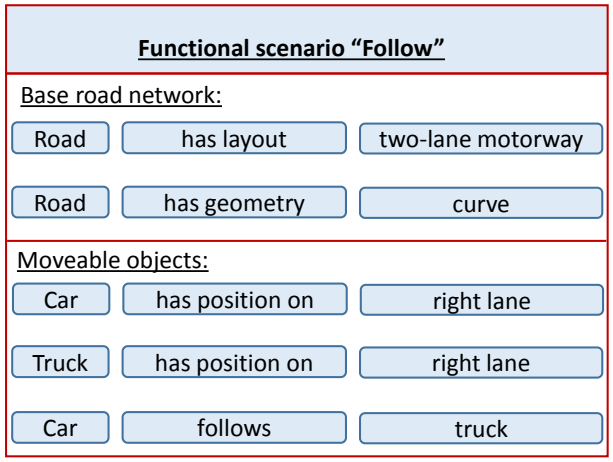

图 3. 在高速公路行驶的一个功能场景：一辆轿车和一辆卡车正行驶在右侧车道上，轿车跟随卡车行驶。

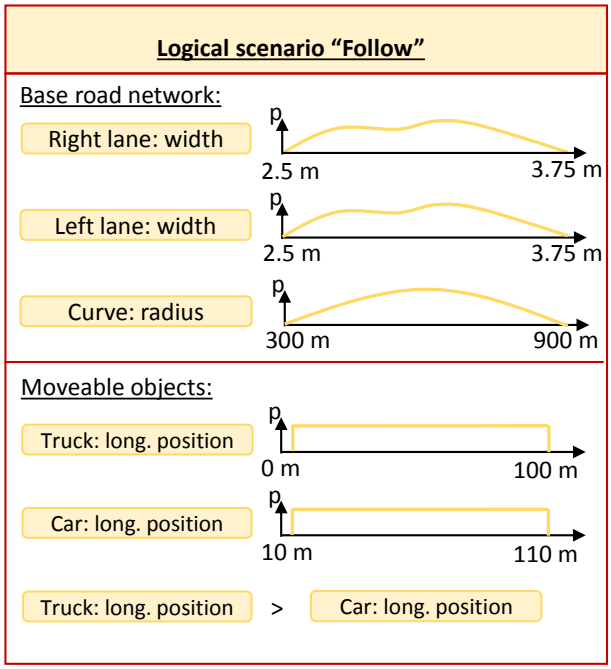

图 4. 逻辑场景的示例。一辆汽车沿着双车道高速公路右侧车道的一辆卡车行驶。

逻辑场景涵盖了提出安全需求所需的所有元素。为了在标准规定的开发过程中逐步规范场景，必须在状态空间中通过形式标记来表述逻辑场景，并从取值范围中确定参数。可以通过概率分布（例如，高斯分布，均匀分布）为每个参数指定范围。参数范围间的关系可以由数值条件或相关函数来指定（例如，超车速度必须大于被超车速度，车道宽度与曲线半径相关）。

图4显示了从图3所示的功能场景中衍生出的逻辑场景。通过从语言表述到状态空间的转换以及描述参数的场景的规范，功能场景被转换为逻辑场景。因此，功能场景术语表中的每一项都必须分配一个描述该术语的参数。在这个例子中，两条车道都是通过车道宽度来描述的，几何结构是由一个半径来表示的，车辆由其纵向位置来描述，并要求卡车纵向位置大于轿车。本文作者选择了一组简化的参数。在实际应用中，可能需要多

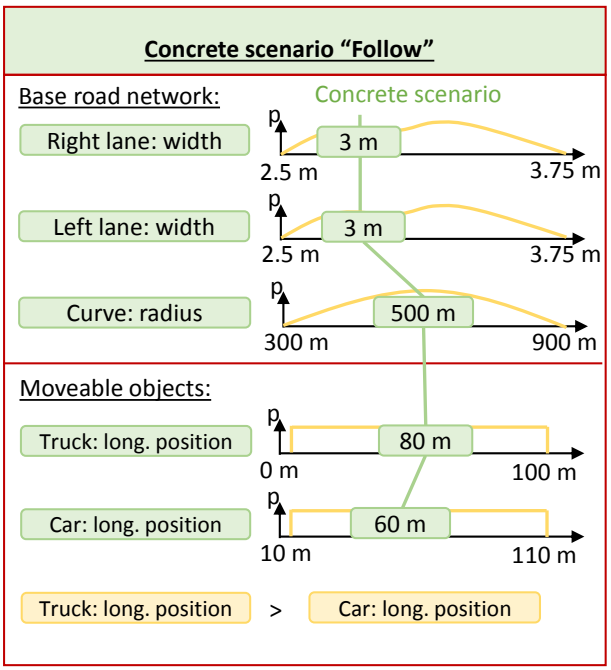

图 5. 具体场景示例。一辆汽车沿着双车道高速公路右侧车道的一辆卡车行驶。

个参数来描述单个术语，例如，一辆卡车可以通过规定其尺寸、重量和发动机功率来定义。

另外，对于图 4中的示例的每个参数，指定了值范围和参数实际出现的概率分布。该信息有助于在系统开发阶段制定技术要求，并为在测试阶段系统生成具体方案提供基础。

C. 具体场景

具体场景由某个确定的参数值来表示状态空间中实体和实体间关系每个逻辑场景都可以通过从参数范围中选择具体值来转换为具体场景。具体场景可以作为测试用例的基础。作者提出了以下定义：

> 具体场景以状态空间详细描述了操作场景。通过确定状态空间中每个参数的具体值来明确描述实体和实体间的关系。

对于每一个具有连续取值范围的逻辑场景，都可以派生出任意数量的具体场景。例如，通过为每个参数选择无穷小的采样步长，可以实现无限数量的具体场景。为保证生成具体场景的效率，应选择有代表性的离散值进行组合。必须强调的是，只有具体场景可以直接转化为测试用例。

图5为一个具体的场景，该场景由图4中所示的逻辑场景衍生。对于每个参数，已经选择了在定义的值范围内的具体值，同时满足了关于参数的指定条件。要将具体场景转换成测试用例，需要增加被测对象的预期行为表现，以及对相关测试设施的需求 [5]。而被测对象的预期行为则可以从操作场景、逻辑场景或项目定义中导出。

V. 结论与展望

本文分析了基于场景的方法在依据 ISO 26262 标准开发自动驾驶系统过程中的可行性。作者分析了可以使用场景来生成工作输出产品的各个工作阶段，并明确了不同阶段对场景描述的需求，阐述了场景描述需求在细节程度上存在的差异。在此基础上，作者定义了场景的三个抽象级别，以满足上文阐述的场景需求。此外，作者给出了每个抽象级别的定义，并说明了如何使用场景的抽象级别来生成 ISO 26262 标准中定义的不同阶段的工作产品。未来，需要新的方法和工具来生成功能场景，并将这些功能场景转换为 ISO 26262 标准开发过程中的具体场景。除了这一贡献之外，还提交了 2018 年 IEEE 智能车辆研讨会的配套文稿，其中提供了基于知识的方法，用于创建各种各样的功能场景。因此，场景的现有数据格式可以集成到建议的抽象级别中。之后，可以针对自动驾驶车辆的测试概念，开发用于场景规范和场景具体化的新方法和工具。

参考文献

[1] Society of Automotive Engineers (SAE), “J3016 - Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems,” Society of Automotive Engineers (SAE), 2016.

[2] “TechDay piloted driving – The traffic jam pilot in the new Audi A8,” 2017, accessed: 01–15–2018. [Online]. Available: https://www.audi-mediacenter.com/en/techday-piloted-driving-the-traffic-jam-pilot-in-the-new-audi-a8-9276

[3] “Waymo is first to put fully self-driving cars on US roads without a safety driver,” 2017, accessed: 01–15–2018. [Online]. Available: https://www.theverge.com/2017/11/7/16615290/waymo-self-driving-safety-driver-chandler-autonomous

[4] W. Wachenfeld and H. Winner, “The Release of Autonomous Vehicles,” in *Autonomous Driving*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg, Germany: Springer Berlin Heidelberg, 2016, pp. 425–449.

[5] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, “Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving,” in *2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC)*, Las Palmas, Spain, 2015, pp. 982–988.

[6] G. Bagschik, T. Menzel, A. Reschka, and M. Maurer, "Szenarien Entwicklung, Absicherung und Test von automatisierten Fahrfunktionen - English title: Scenarios for Development, Test and Validation of Automated Vehicles," in *11. Workshop Fahrerassistenz und automatisiertes Fahren FAS 2017*, Walting, Germany, 2017.

[7] K. Go and J. M. Carroll, "The Blind Men and the Elephant: Views of Scenario-based System Design," *Interactions*, vol. 11, no. 6, pp. 44–53, 2004.

[8] C. Bergenhem, R. Johansson, A. Söderberg, J. Nilsson, J. Tryggvesson, M. Törngren, and S. Ursing, "How to Reach Complete Safety Requirement Refinement for Autonomous Vehicles," in *CARS 2015-Critical Automotive applications: Robustness & Safety*, Paris, France, 2015.

[9] G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, "Identification of Potential Hazardous Events for an Unmanned Protective Vehicle," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, Gothenburg, Sweden, 2016, pp. 691–697.

[10] T. Stolte, A. Reschka, G. Bagschik, and M. Maurer, "Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC)*, Las Palmas, Spain, 2015, pp. 672–677.

[11] F. Schuldt, F. Saust, B. Lichte, M. Maurer, and S. Scholz, "Effiziente systematische Testgenerierung für Fahrerassistenzsysteme in virtuellen Umgebungen - English title: Efficient systematic test case generation for automated driving functions in virtual driving environments," in *AAET - Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme Transportmittel*, Braunschweig, Germany, 2013, pp. 114 – 134.

[12] J. Bach, S. Otten, and E. Sax, "Model based scenario specification for development and test of automated driving functions," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, Gothenborg, Sweden, 2016, pp. 1149–1155.

[13] ISO, *26262 – Road vehicles – Functional Safety*, 2016.

[14] A. Reschka, "Fertigkeiten- und Fähigkeitengraphen als Grundlage für den sicheren Betrieb von automatisierten Fahrzeugen in städtischer Umgebung - English title: Skills and ability graphs as basis for safe operation of automated vehicles in urban environments," Ph.D. dissertation, Technische Universität Braunschweig, 2017.

[15] F. Schuldt, "Ein Beitrag für den methodischen Test von automatisierten Fahrfunktionen mit Hilfe von virtuellen Umgebungen - English title: Towards testing of automated driving functions in virtual driving environments," Ph.D. dissertation, Technische Universität Braunschweig, 2017.

[16] *Richtlinie für die Anlage von Autobahnen - English title: Guidelines for Constructing Motorways*, Forschungsgesellschaft für Straßen und Verkehrswesen Std., 2009.