·智能网联汽车安全验证与评估专题·

面向安全验证的自动驾驶系统行为能力与场景建模框架*

陈俊涛[1] 陈贞[2] 杨强[3] 刘玉清[4] 贾贝贝[5] 李广友[6]

（1.北京航迹科技有限公司，北京 100080；2.北京镝石数据科技有限公司，北京 100176；3.北京赛目科技股份有限公司，北京 100080；4.重庆长安汽车股份有限公司，重庆 401120；5.北京新能源汽车股份有限公司，北京 100176；6.工业和信息化部装备工业发展中心，北京 100846）

【欢迎引用】陈俊涛，陈贞，杨强，等．面向安全验证的自动驾驶系统行为能力与场景建模框架[J]．汽车文摘，2026(8)：1-15.

【Cite this paper】CHEN J T, CHEN Z, YANG Q, et al. A Framework for Behavioral Competency and Scenario Modeling of Automated Driving Systems for Safety Validation[J]. Automotive Digest (Chinese), 2026(8): 1-15.

【摘要】为应对自动驾驶系统规模化部署与产业化应用进程中的安全验证难题，弥补现有方法在行为能力建模系统性、测试场景语义完整性、设计运行范围的场景覆盖、边界能力验证等方面的短板，基于国际技术法规研究和自动驾驶试点实践，提出一种以“设计运行范围-行为能力-测试场景-验证准则-风险评估”为主线的行为能力与场景建模框架。采用功能-抽象-逻辑-具体场景表达，融合知识驱动、数据驱动与目标导向的建模机制，实现验证路径的结构化和可追溯性。在行为能力建模方面，覆盖标称、危险、失效及边界4类情境，通过目标物-事件-响应分析建立能力、场景与准则的映射关系。在验证层面，明确性能指标与验证准则设定逻辑，支持验证覆盖度与残余风险评估。该框架可为自动驾驶系统安全声明及产品合规性评估提供方法参考。

关键词：自动驾驶系统；设计运行范围；行为能力建模；测试场景建模；安全验证框架

中图分类号：U461.91　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20250153

A Framework for Behavioral Competency and Scenario Modeling of Automated Driving Systems for Safety Validation

Chen Juntao[1], Chen Zhen[2], Yang Qiang[3], Liu Yuqing[4], Jia Beibei[5], Li Guangyou[6]

（1. Beijing Voyager Technology Co., Ltd., Beijing 100080; 2. Beijing Dishi Data Technology Co., Ltd., Beijing 100176; 3. Beijing Saimo Technology Co., Ltd., Beijing 100080; 4. Chongqing Chang'an Automobile Co., Ltd., Chongqing 401120; 5. Beijing Electric Vehicle Co., Ltd., Beijing 100176; 6. Ministry of Industry and Information Technology Equipment Industry Development Center, Beijing 100846）

【Abstract】To address the safety validation challenges faced during the large-scale deployment and industrial application of Automated Driving System (ADS), and to bridge the gaps in existing methods, particularly regarding the systematic behavioral competency modeling, the semantic completeness of test scenarios, the scenario coverage of the Operational Design Domain (ODD), and the validation of boundary capabilities, a framework for behavioral competencies and scenario modeling of ADS is presented. Based on investigations of international technical regulations and automated driving pilot practices, the framework follows the main line of “ODD-behavioral competencies-test scenarios-validation criteria-risk assessment”, adopts a functional, abstract, logical and concrete scenario representation, and integrates knowledge-driven, data-driven, and goal-oriented modeling mechanisms to achieve structured and traceable validation paths. For behavioral competency modeling, it covers 4 scenario types: nominal, critical, failure as well as ODD-boundary, and establishes mappings among competencies, scenarios, as well as validation criteria through object-event-response

*基金项目：新一代人工智能国家科技重大专项（2022ZD0116311）。

通信作者：陈贞（1984—），博士，高级工程师，研究方向为智能网联汽车安全测试与评估方法，chenzhen@dystech.cn。

analysis. At the validation level, the formulation logic of performance metrics and validation criteria is clarified to support the assessment of validation coverage and residual risks. The framework can provide methodological references for ADS safety declarations and product compliance assessment.

Key words: Automated Driving System (ADS), Operational Design Domain (ODD), Behavioral competency modeling, Test scenario modeling, Safety validation framework

0 引言

自动驾驶系统(Automated Driving Systems,ADS)安全验证是其广泛部署与产业化应用的核心挑战之一。传统实车道路测试在覆盖高风险、低概率场景及验证效率方面存在局限性,难以满足ADS在复杂多样的设计运行范围(Operational Design Domain,ODD)下的系统化验证需求。以场景驱动为核心的ADS验证理念已发展出多支柱协同的安全验证框架[1]。该方法强调以ODD为验证边界、以行为能力模型为评价准则、以测试场景集为验证输入,旨在构建具备系统验证覆盖性、结构化映射性和工程可实施性的验证框架,从而提升ADS安全验证的有效性、代表性与可扩展性。联合国欧洲经济委员会世界车辆法规协调论坛(UNECE WP.29)提出的新评估与测试方法[2-4]以及型式批准有关法规(如UN R157[5]、(EU)2022/1426[6]、UN R185[7]),均已确立仿真、场地、道路等多支柱验证体系。

然而,当前工程化部署仍面临3方面挑战:(1)行为能力模型缺乏系统性,难以从需求层自顶向下定义验证目标;(2)测试场景建模方法不统一,可扩展性与语义完整性有待提升;(3)ODD、行为能力与测试场景间缺乏结构化映射机制,导致验证目标不明确、覆盖度难以评估[7-8]。为此,本文结合国际技术法规研究和工程实践,提出一套基于ODD约束、行为能力建模与测试场景构建联动的ADS验证框架。该框架旨在建立可量化的验证覆盖度、可追溯的行为能力判据以及可复用的验证目标,形成从系统能力声明到合规性评估的系统化路径,为ADS安全验证提供方法论参考。

1 自动驾驶系统安全验证框架

1.1 验证体系构建思路

为满足ADS安全验证的工程化要求,本文结合ISO 34502、ISO 34503、IEEE 2846等标准[9-11]、UNECE自动驾驶验证方法[4]、PEGASUS工程实践[12],构建了一个以ODD为核心驱动的ADS安全验证方法框架(图1)。

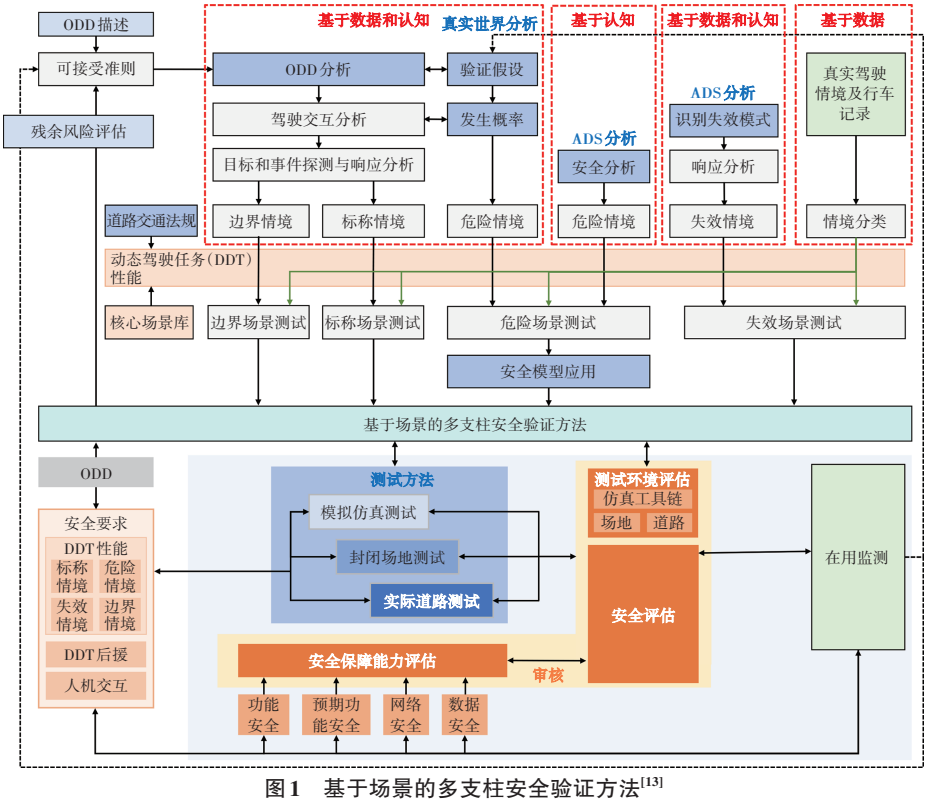


图1 基于场景的多支柱安全验证方法[13]

该框架以“ODD-行为能力-测试场景-验证准则-结果评估”为主线，体现了从ODD边界定义到验证执行与结果评估的系统闭环逻辑，覆盖标称情境、危险情境、失效情境与边界情境4类运行情境，可以支撑多样化ADS功能在不同ODD下的验证需求。

该方法明确了ODD、ADS行为能力与测试场景间的结构化映射关系。关键步骤包括：(1)明确ODD定义，描述系统运行环境边界；(2)构建ADS行为能力模型，定义其在各类情境下的预期响应；(3)将ODD与行为能力需求转化为可执行的测试场景集合；(4)以测试场景覆盖度与预设验证准则为依据，完成性能验证与风险评估。该框架通过与法规标准对齐的结构化建模，实现了从系统安全目标到具体测试验证的端到端映射。

1.2 设计运行范围建模方法

ODD用于描述ADS能够安全运行的环境边界，是行为能力建模与安全验证的基本前提。ODD要素通常可划分为4个维度：静态道路特征(或静态实体)、环境条件、动态实体以及运行约束条件[9]。

ODD可形式化表示为多维状态空间中的一个子集，用以明确系统功能的运行边界：

$$ODD = \{r, e, d, c | r \in \boldsymbol{R}, e \in \boldsymbol{E}, d \in \boldsymbol{D}, c \in \boldsymbol{C}\} \quad (1)$$

式中：$\boldsymbol{R}$为静态道路特征集合(如道路几何形态、交通设施)，$\boldsymbol{E}$为环境变量集合(如天气、光照等)，$\boldsymbol{D}$为动态实体集合(如其他道路使用者及其运行状态)，$\boldsymbol{C}$为运行约束条件集合(如速度范围、地理围栏等)。

图2展示了不同ADS功能及其ODD配置下，功能需求与行为能力之间的逻辑映射关系，强调了ODD不仅是ADS功能外部运行条件的边界描述，更是行为能力建模与场景生成的关键输入。

1.3 ADS行为能力建模与分类方法

在既定ODD下，ADS应具备完成动态驾驶任务(Dynamic Driving Task，DDT)的行为能力[14]。本文中，行为是指ADS在不同时间尺度下的决策与执行动作。行为能力则是ADS在其ODD内，通过感知、决策、控制、人机交互和冗余管理，实现预期驾驶行为并达成安全目标的能力集合[4]。

为建立结构化的验证空间，覆盖ADS在不同运行情境下的能力需求，本文将ADS行为能力划分为4类，如表1所示。该分类体系为验证目标设定与测试方案设计提供了结构支撑，也是构建测试场景集与生成安全声明的逻辑起点[4]。

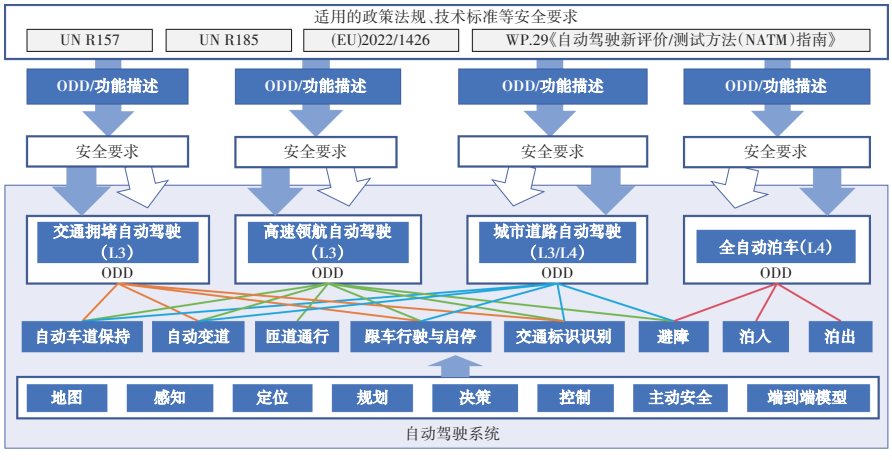


图2 不同ADS功能的ODD配置及技术要求关系[5]

表1 ADS行为能力分类与典型测试场景映射关系

分类	运行情境	定义	行为能力示例	典型测试场景
标称行为能力	正常交通与系统正常	ADS在正常系统状态和正常交通秩序下，应能稳定、合规、可预测地执行动态驾驶任务	变道、让行、保持安全车距、遵守信号灯	常规交叉路口、车道合流、限速区域等
危险应对能力	突发风险或他人违规	ADS在面对有风险的非预期事件，应具备识别与缓解风险的能力	紧急避障、识别违规行为、碰撞规避	行人突然穿行、对向车道违规逆行驶入、能见度骤降等
失效应对能力	故障或系统性能退化	ADS在系统组件故障或性能退化状态下，能识别故障、缓解风险并安全过渡到风险缓解状态(Mitigated Risk Condition，MRC)	故障识别、执行最小风险策略、用户接管提示	传感器失效、控制器异常、动力系统故障、通信中断等
边界应对能力	ODD边界或超出ODD	ADS在ODD边界或超出ODD时，能够识别ODD边界，触发接管请求或执行最小风险策略	ODD识别、接管请求、执行最小风险策略	暴雨、暴雪、大雾、无车道线等

1.3.1　标称行为能力

标称行为能力是ADS在ODD预期交通环境和系统正常状态下，依据道路交通法规及一般安全驾驶原则，稳定、合规、可预测地执行DDT的基础能力。验证中引入“显式化交通通行规则”模型，将人类驾驶的隐性安全原则转化为可验证规则，以提升验证一致性[4]。

1.3.2　危险应对能力

危险应对能力是ADS在面对外部突发风险或非预期事件（如其他道路使用者违规行为、不可预见的环境突变）时，能够识别并采取合理措施以避免或缓解碰撞风险的能力。其建模需界定“可合理预见的风险或非预期事件”，并明确碰撞缓解策略。该能力可参考IEEE 2846的“可合理预见的行为模型”，结合系统理论过程分析（System-Theoretic Process Analysis，STPA）等安全分析方法，识别危险情境[11]。

1.3.3　失效应对能力

失效应对能力是ADS在系统组件发生故障或性能退化时，能够检测、诊断并采取风险缓解措施，安全过渡至最小风险状态的能力。验证通常采用故障注入测试，结合故障树分析、诊断模型与失效传播路径建模，评估ADS对不同失效类型的检测与响应效果，确保残余风险满足功能安全与预期功能安全标准[15]。

1.3.4　边界应对能力

边界应对能力是ADS在接近或超出ODD边界时，能够识别条件变化，触发接管请求或执行最小风险策略的能力。验证需构建接近和超出ODD边界的场景，评估ADS的识别准确性与响应安全性。

以上分类与建模为ADS行为能力提供了系统化框架，为后续的测试场景生成、验证策略设计、验证准则制定与风险评估奠定了逻辑基础。

2　基于ODD的ADS行为能力与测试场景建模方法

2.1　总体框架

为系统性验证ADS功能在其ODD内，以及接近或超出ODD边界时的安全性，需构建以行为能力为核心、测试场景为载体的验证框架。本研究提出的方法框架，融合知识驱动、数据驱动与目标导向机制，总体流程如图3所示，建立从ODD定义、行为能力建模、测试场景建模，到能力-场景映射、验证假设、性能准则设定、覆盖度评估，直至安全声明支撑的闭环路径[16]。其核心理念是围绕“ADS行为能力要求”，构建结构化、可追溯、可量化的验证场景体系，建立可追溯的“能力-场景-准则”验证链条，确保验证过程能够充分支撑系统安全声明的有效性和合规性。该方法包括行为能力建模、测试场景建模、行为能力和测试场景映射、验证假设、性能指标和验证准则设定、验证覆盖度与残余风险评估等步骤[13]。

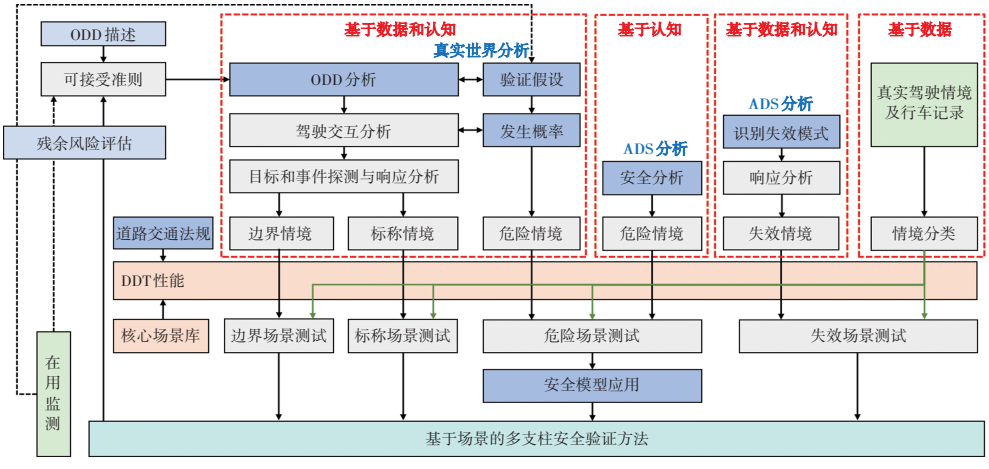


图3　基于行为能力与场景建模的验证方法

2.2　行为能力建模

行为能力建模旨在将ADS的ODD定义、交通交互特征及目标物行为转化为可验证的能力集合。本文基于ODD分析、驾驶交互分析、目标和事件探测与响应（Oject and Event Detection and Response，OEDR）分析等方法[4]，构建结构化、可追溯的行为能力建模流程。

2.2.1　ODD分析：运行边界与能力识别

ODD分析是行为能力建模的起点，其核心任务是从ODD定义出发，确定系统在特定功能下的能力需求。ISO 34503、BSI PAS 1883等为ODD分析提供了结构化指导[9, 17-18]。

基于ODD的4个维度(静态实体、动态实体、环境条件、运行限制条件),可系统化推导出3类核心能力要求:(1)运行合理性:确保系统仅在ODD范围内激活并持续安全运行;(2)边界应对能力:识别并处置ODD边界及超出ODD的运行条件;(3)行为覆盖度:将ODD边界条件映射为具体的能力清单,支撑验证设计。

2.2.2 驾驶交互分析:行为模式推导

驾驶交互分析旨在识别ADS在ODD内与其他道路使用者的互动特征,推导系统应具备的响应能力,具体从以下5个维度展开分析。

(1)静态实体属性:道路、车道与基础设施特征及其对交互逻辑(协作/冲突)的影响。

(2)环境条件属性:天气与光照对ADS运行的潜在交互逻辑影响,包括接管行为和最小风险策略行为。

(3)参与者属性:分析各类道路使用者的类别、静态特征及典型动态行为,与ADS的潜在协作或冲突行为。

(4)行为概率建模:对ODD内其他道路使用者的行为及目标物的状态进行概率建模,区分合理可预见、突发可预见和极低概率3类[19]。

(5)交互语义分类:区分合作、冲突与中立行为,明确其对ADS能力需求的不同作用[20]。

通过驾驶交互分析,确保ADS能力验证聚焦于"合理可预见的场景"[21],避免对极端低概率事件进行过度设计,保证能力建模的工程合理性。

2.2.3 OEDR分析:目标物-事件-响应能力映射

在ODD与驾驶交互分析基础上,通过OEDR分析,将交通对象动态行为与环境演化映射为ADS的行为能力要求,构建"目标物-事件-响应"的能力矩阵,表2为驾驶情境和行为能力建模分析的定性示例。

(1)确定目标物及合理行为。确定ADS可能遇到的目标物类型及其合理可预见行为。

(2)ADS响应动作映射。建立目标物行为与ADS响应的对应关系。

(3)情境归类。根据目标物行为特征及环境状态,将交通情境划分为标称、危险、失效与边界4类,明确各类情境下ADS能力验证重点[4]。

该矩阵形成覆盖从常规到极端情境的全链路"场景-响应能力"映射关系,为ADS性能评价标准制定、测试场景设计以及安全声明的验证闭环提供了直接依据。

2.3 测试场景建模

2.3.1 场景建模目标与覆盖策略

测试场景建模的核心目标是构建一个系统化、覆盖全面的测试场景集合[22],以映射ADS在其ODD内可能面临的各类驾驶情境。测试场景集合的建模遵循以下原则。

(1)覆盖广度。覆盖ODD内所有关键维度,并适当包括ODD边界或外部极端条件。

(2)覆盖深度。考虑关键变量的多值组合与边界变体,重点验证系统在极端条件下的表现能力。

(3)行为相关性。明确关联ADS的感知、决策和控制能力,避免冗余或无关场景。

(4)挑战性。覆盖其他道路使用者的不安全行为,如逆行、突然变道、超速等。

(5)可量化。通过ODD要素覆盖度、功能路径覆盖度等指标评估场景集。

表2 目标物-事件-ADS响应的行为能力映射示例

情境触发源	静态实体	环境条件	典型行为模式	场景分类	ADS响应能力
车辆	直道	雨	前车减速、变道、切入切出、交叉口转弯	标称、危险	跟车、减速、让行、保持车距、紧急制动
	车道变少	雪	对向来车占道、相邻车变道侵入	危险	避让、紧急制动、车道调整
行人	人行横道	雾	人行横道过街、非信号控制区域横穿	标称、危险	让行、减速、紧急制动
	交叉路口	逆光	突然冲出路面、折返横穿	危险	紧急识别并制动或躲避
骑行者	直道	强光	车道内骑行、逆行穿行、并排行驶	标称、危险	跟随、保持距离、减速、避让
动物/静态障碍物	直道/弯道	夜晚	静止或缓慢穿越车道	危险	识别并减速或绕行
道路设施/标识	直道/弯道	晴天/正常照明	限速标志、泊车线、导向标线模糊	标称	遵守交通通行规则、车道保持、降速提示
异常目标物(杂物、落物等)	直道/弯道	晴天/正常照明	路面突然出现物体、掉落物	危险	紧急识别并制动或避障
系统运行边界(接近)	高速公路	光照减弱、雨(由小转大)	车道线识别逐渐恶化、传感器信噪比下降	边界-接近	提前减速,必要时驾驶员接管提示
系统运行边界(超出)	高速公路	大雾/大雪(严重感知受限)	车道线丢失、感知能力显著下降	边界-超出	驾驶员接管请求并执行最小风险策略(如减速靠边泊车)

2.3.2 场景表达分层

为系统地将ADS行为能力映射为可执行测试，通常采用“功能场景–抽象场景–逻辑场景–具体场景”的4层表达结构[16]。各层承担不同建模任务，共同实现从行为意图到可执行测试用例的语义闭环。表3以城市快速路切入场景为例，对比展示了不同层级的场景表示。

表3 自动驾驶系统安全验证中的场景分层表示

场景层级	核心目标与作用	表达方式	城市快速路切入场景	典型参数特征	典型应用环节
功能场景	定义ADS需验证的基本驾驶情境，建立概念层基准	自然语言/语义描述（非形式化）	主车在城市快速路中保持车道行驶，右侧车辆尝试切入	ODD范围、主车行为、目标车行为、环境条件	系统需求分析、ODD边界定义、概念层验证
抽象场景	提供结构化的交互逻辑与因果链关系	状态机、场景图、约束图	主车：中车道，目标车：右后方，行为：切入	行为标签、轨迹类型、相对方位、交互逻辑	场景建模、逻辑模板生成
逻辑场景	定义参数空间，覆盖变量范围与采样机制	参数集合、区间、概率分布	主车速度：[50,80] km/h；切入点纵向距离：[50,100] m	速度区间、能见度范围、目标车加速度区间等	测试用例设计、采样策略生成、参数覆盖度分析
具体场景	形成唯一可执行的测试用例，保障复现性与可比性	参数赋值后的实例化场景	主车速度=60 km/h；切入车速度=50 km/h；光照=7 000 lx	单一数值组合，确定性输入	仿真和实车测试、结果复现与对比

2.3.3 多源融合的场景建模路径

为系统性验证ADS的安全性与鲁棒性，场景建模应覆盖标称、危险、失效及边界情境[16]，并综合利用多源信息，采用知识驱动、数据驱动与目标导向3类方法的协同策略，形成结构化、系统化、分层化的验证场景集[13]。

2.3.3.1 知识驱动方法

知识驱动方法基于专家经验、工程规则、法规标准、功能安全和预期功能安全分析，构建符合设计意图的典型场景与边界场景[23]。典型手段包括：基于开发输入识别关键驾驶情境与典型场景族；通过核心参数扰动组合生成变体场景；结合功能安全和预期功能安全分析，提取与功能失效、性能退化相关的验证场景[15,21]；通过逻辑组装，从简单场景扩展生成复杂场景；对关键参数进行概率建模，生成覆盖标称到危险的场景分布；直接引入或改造法规标准中的场景模板（如UN R157[5]）。

2.3.3.2 数据驱动方法

数据驱动方法通过分析实际道路运行数据，反映ODD内高风险、复杂、边界场景的实际分布，是构建高可信度场景、确保验证与实际运行环境一致的关键。主要数据源与建模手段包括：事故与碰撞数据，用于提取高危险场景；自然驾驶数据，用于提取典型交互模式，反映常见交通行为的统计规律；交通流模式数据，结合特定ODD的交通特征，从日志数据中分析宏观流量分布与微观交互模式，构建典型场景族；多源感知数据，利用道路基础设施、无人机等采集的感知数据，建模特殊场景（如施工区、临时封路等）；以及在用ADS运行监测平台与事件数据。

数据驱动方法具有高度代表性和时效性，尤其适用于构建真实分布和统计显著的场景库。随着ADS道路运行数据的持续积累，其在高可信度场景建模中的作用将更加突出。

2.3.3.3 目标导向方法

目标导向方法以ADS安全声明为起点，反向推导验证需求以识别覆盖缺口，是建立“验证–声明”闭环的关键。具体实施流程如下：定义安全接受准则，明确系统应当满足的安全目标或边界指标，如最大碰撞概率容许值；识别验证缺口，发现未覆盖或覆盖不足的功能路径、边界条件与交互行为；验证需求反向推导，结合系统架构和STPA、故障树分析（Fault Tree Analysis，FTA）等安全分析方法，推导尚未覆盖或覆盖不足的场景逻辑结构与参数范围[13]；使用形式化语言或工具（如OpenSCENARIO、规则逻辑）将场景转化为可执行用例；以及通过规则驱动构造符合法规及安全要求的场景。

通过对知识驱动、数据驱动与目标导向方法的协同应用，并结合参数抽样、聚类与去重、代表性筛选及标准化表达，可构建结构化、代表性且可追溯的测试场景集。

2.4 行为能力与测试场景映射

为将抽象的行为能力要求转化为可执行、可度量的具体验证任务，本节构建“行为能力–测试场景–安全响应”的映射结构。相较于传统主要依赖海量实车里程累积或基于经验构建离散场景库的验证方法，本方法通过建立从ODD到行为能力再到测试场景的清晰映射链条，实现了验证活动的系统性、可追溯性和目标导向性。通过在抽象、逻辑和具体场景层级建立

对应关系，形成可执行的验证单元，可建立系统化、分层化、可追溯的测试场景集，以覆盖标称、危险、失效及边界4类情境。表4~表7分别展示了4类情境下的映射逻辑与示例。

2.4.1 标称情境下的行为能力与场景映射

标称情境下的行为能力要求ADS在常规、可合理预见的驾驶情境下，稳定、合规地执行动态驾驶任务。传统验证方法常面临将交通法规、安全驾驶原则等定性要求转化为可定量测试参数的困难，导致验证存在主观性和覆盖缺口。本方法通过结构化映射（表4），将遵守规则、安全交互等抽象能力，明确分解为如保持特定横向距离、控制相对速度、执行合规换道等可量化的行为指标，并与包含具体ODD元素、目标物状态和参数范围的测试场景直接挂钩，从而实现了对标称能力客观、系统的验证。

2.4.2 危险情境下的行为能力与场景映射

危险情境下的行为能力是指ADS应对突发或难以提前合理预见的危险事件的能力[4]。与传统依赖事故数据或专家经验的方法相比，本方法通过系统化危害分析，建立了从安全目标到测试场景的可追溯链路。该方法基于后果-危害-不安全控制动作-触发条件-根本原因-行为能力-测试场景的完整追溯链条（以与车外物体碰撞的危险情境为例），如表5所示。参考IEEE 2846等标准[11]，结合STPA、FTA等危害分析方法[21]，系统识别潜在危险源及触发条件，界定ADS在危险情境下的可接受行为边界。当前行业面临的主要挑战在于缺乏统一、可量化的人类驾驶基准模型，导致危险情境验证缺少一致评价指标和普适准则。

2.4.3 失效情境下的行为能力与场景映射

失效情境下的行为能力是指ADS在自身或相关子系统出现故障或性能退化时，仍能维持必要的安全水平，或在失效不可控时进入最小风险状态的能力[4]。如表6所示，本方法通过映射（以感知和定位失效情境为例），将失效类型、具体失效模式、潜在原因与系统应具备的特定安全响应能力及具体测试场景参数系统性地关联起来，使得失效测试成为针对特定安全目标的、有明确通过/失败准则的验证活动。

典型系统失效包括但不限于感知失效、定位与地图失效、决策与规划失效、执行器或控制失效以及人机交互与接管链路失效。针对不同失效模式，ADS的安全要求应包括在可恢复的情况下排除故障并恢复正常运行、在重大故障时采取功能限制或性能降级措施、在关键系统失效时进入最小风险状态以及在全过程中及时且明确地向用户传达故障

表4 标称情境下的行为能力与场景映射关系示例

ODD元素	静态实体	环境条件	驾驶行为	交通通行规则	安全要求	行为能力	测试场景示例
自行车	市区直道	白天	车道行驶	机动车在超越非机动车时，应保持安全距离，不得影响其正常行驶；若需跨越车道线，应提前开启转向灯并确保安全	ADS在识别潜在交通风险时，应采取符合交通安全原则的驾驶调整，特别是控制与自行车的纵向速度差和横向安全距离，以避免危险	ADS能够在识别到与自行车存在潜在冲突风险时，动态调整纵向速度（相对速度≤30 km/h）；ADS在车道内移动，与自行车保持横向安全距离（≥2 m）	一名骑自行车者在市区直道车道边缘（横向距离0.2~1.0 m）以10~20 km/h行驶，ADS车辆以30~50 km/h同向行驶 ADS在超越过程中保持≥2 m横向间距，若空间不足则换道避让，换道动作伴随转向灯提示，减速度≤3 m/s^2
					在考虑安全风险的情况下，ADS应避免对交通流造成不合理干扰	在横向空间不足时，ADS能通过执行换道或减速来完成安全超越	
					ADS应能与其他道路使用者安全交互	在换道时，ADS激活转向信号灯	

表5 危险情境下的行为能力与场景映射关系示例

后果	危害	不安全控制动作	触发场景	根本原因	行为能力	测试场景示例
与车外物体碰撞	ADS未保持与前车的安全距离	制动动作缺失或延迟	前方车辆减速或静止目标出现在行驶轨迹内	目标物未检测或误分类；感知结果模糊；传感器融合错误	ADS应在检测到前车或障碍物存在碰撞风险时，及时触发紧急制动，并在条件允许时执行安全变道避让	环岛场景：前车突然减速至0~10 km/h，ADS车辆以30~40 km/h接近。ADS需在TTC<3 s时触发紧急制动，或安全换道避让以避免碰撞
与车外物体碰撞	风险误判导致未执行必要制动	风险评估错误导致制动未触发	前方车辆缓慢减速或位置识别偏差	目标物轨迹识别错误；自车/物体定位不准确，错误评估为“无碰撞风险”	ADS应在风险评估存在不确定性时采取保守策略（优先减速并保持安全车距，避免依赖单一高不确定性检测结果）	城市直道场景：前车减速至20 km/h，ADS车辆以40 km/h跟随，纵向距离<15 m。ADS需主动减速，保持跟车时距≥2 s

表6　失效情境下的行为能力与场景映射关系示例

失效类型	失效模式	潜在原因	安全要求	行为能力	测试场景示例
感知	无法识别运行环境是否处于ODD边界	未能检测到ODD特征，如大雨/雾	ADS应能够确认并监测其运行环境的ODD条件和边界	ADS应在检测到感知功能失效后，采取最小风险策略（逐步减速并停于合适位置），同时向用户提示失效状态	ADS因感知功能失效而无法确认运行环境是否满足ODD条件。ADS在检测到感知功能失效后，2 s内发出显著告警，并以≤4 m/s²的减速度减速，最终在不危及交通安全的位置（如当前车道、应急车道或安全区域）安全泊车
定位	定位漂移或定位信号丢失	卫星定位信号遮挡、地图匹配失败、传感器融合异常	ADS应能够监控定位精度，当误差超出可接受范围时，采取冗余方案或执行最小风险策略	ADS应在检测到定位功能退化或丧失时，及时启用冗余定位方案（如基于惯导/感知的定位），若无法保证定位精度，则执行最小风险策略	城市峡谷或隧道场景：ADS因卫星信号遮挡导致定位误差>2 m且持续5 s以上。ADS在定位误差超过阈值并持续5 s内，检测并确认定位异常，向用户发出显著告警，并在无法启用有效冗余定位时以≤4 m/s²的减速度减速至安全泊车

或失效信息。

2.4.4　边界情境下的行为能力与场景映射

边界情境下的行为能力是指ADS在运行接近或超出ODD边界时，仍能维持基本安全水平，或在必要时通过最小风险策略过渡至最小风险状态[4]。典型边界情境包括大雨、大雾、大雪、车道线丢失等低能见度或低附着力环境。

ADS安全要求包括对ODD边界及超出边界情境的识别，包括对ODD边界及超出边界情境的识别，触发显著告警，及时向用户传达接管请求，并执行最小风险策略以避免碰撞。表7为边界情境下的行为能力与场景映射关系示例。

表7　边界情境下的行为能力与场景映射关系示例

ODD要素	属性	潜在原因	安全要求	行为能力	测试场景示例
天气	大雨、大雾、大雪	环境条件恶化（如能见度不足、路面附着系数降低），导致超出ODD边界	ADS应具备识别ODD边界并触发安全响应的能力	ADS应在识别超出ODD边界时，触发显著告警，并通过最小风险策略逐步减速至安全泊车（如当前车道或应急区域）	在大雾天气下，能见度低于50 m，ADS无法持续识别车道线 ADS在检测到不符合ODD条件时，应在2 s内向用户发出显著告警，并以≤4 m/s²的减速度减速，最终在不影响交通安全的位置（如当前车道、应急区域或路侧安全带）安全泊车

通过建立行为能力与测试场景的映射链条，本方法实现了验证过程的3项核心提升：（1）验证目标明确，每个测试场景均直接服务于特定行为能力的验证；（2）逻辑链条完整，形成了从安全需求到测试结果的追溯闭环；（3）验证效率优化，能系统性地覆盖高风险、低概率的长尾场景。

2.5　验证假设

2.5.1　验证假设作用与分类

验证假设定义了系统运行环境、道路使用者行为模型、ADS功能边界等前提条件，为场景建模与性能评估提供逻辑基础[4]。验证假设需明确、合理且可验证，可通过试验、数据采集及理论建模加以确认，确保测试结果的有效性和可推广性。

根据作用与内容，验证假设主要分为以下3类：

（1）系统能力假设：ADS具备对指定类型目标物的探测、识别与响应能力。

（2）行为模型假设：道路使用者行为符合合理概率模型或统计边界。例如，行人闯红灯的概率应基于当地交通数据建模；车辆在高速公路上并线的平均车间距具体数值因车速和交通密度而异[5]。

（3）环境边界假设：系统仅在定义的ODD内运行，并能识别ODD边界。

2.5.2　假设建模方法与验证

合理的验证假设可通过经验知识、法规标准、数据驱动分析及形式化建模方法建立，具体包括：

（1）经验与法规基础：参考如ISO 26262[15]、ISO 21448[21]、IEEE 2846[11]等标准中的行为模型假设、风险分类及安全策略。

（2）数据驱动分析：基于自然驾驶数据、事故数据库及交通行为统计数据进行建模，推导驾驶行为概率分布。

（3）形式化建模：采用时序逻辑、状态机或模型检查等技术，定义道路使用者行为边界及潜在事件链模型。

开发阶段通过测试日志分析、场景回放与对比实验，验证开发人员对场景和行为能力的初始假设是否成立，确保其在ADS性能评估中有效。

2.5.3　假设的管理与追踪

在实际验证流程中，验证假设需以明确、可追溯

方式进行记录和系统化管理。ADS性能评估应针对每项假设制定验证任务，确保：

（1）可验证性：每项假设具备可度量指标或验证路径，例如“系统在小雨天气下识别精度误差<5%”。

（2）一致性与覆盖度：假设间无逻辑冲突，覆盖所有关键能力和运行边界的触发条件。

假设管理体系与场景建模、能力验证任务联动，形成可追溯验证链，避免验证结果错误外推至超出假设边界的运行情境。

2.5.4　地域差异与定制化挑战

由于道路交通法规、驾驶风格与行为文化存在显著差异，ADS验证假设应支持区域化配置与差异化参数设定。一是行为模型本地化，如车辆并线行为等模型应基于当地统计分布调整。二是基础设施适配，如考虑交通标线清晰度、信号系统完备性等。验证体系应支持跨区域部署时的动态调整，以测试场景的现实相关性、可移植性及结论可推广性。

2.6　性能指标与验证准则设计

性能指标与验证准则是连接ADS行为能力、安全目标与验证结果的关键桥梁。本研究通过结构化方法，将定性安全要求转化为可量化、可验证的具体指标，以提升验证结果的客观性、可比性与可追溯性。本节围绕交通通行规则编码、安全模型构建、失效与风险评估等方面，构建可实施、可追溯且可验证的性能评价与判定机制。

2.6.1　交通通行规则编码

现有交通通行规则主要面向人类驾驶员，未明确界定ADS行为的安全边界与判定条件。为满足“在标称驾驶情境下，ADS预期行为应遵循所在国家或地区道路交通法规”的安全要求，并支撑自动化验证执行，本文提出将自然语言法规转化为结构化、可验证的ADS行为准则。

交通通行规则通常可分解为3类核心要素：运行条件（ODD与车辆状态）、行为规范（明示条款）、隐含假设（基于人类认知的预设）。规则编码的关键在于将隐含假设显性化，并将模糊表述转化为可量化指标，形成适用于ADS验证的规则表达形式，即：ODD+行为能力+驾驶决策[13]。

以《中华人民共和国道路交通安全法》第四十七条为例[24]，其结构化编码过程包括以下步骤。

（1）术语识别与词汇表构建。从法规条款中提取与运行条件和行为能力相关的关键术语，并建立标准化词汇表（表8），作为规则形式化与逻辑建模的基础。

表8　交通通行规则关键术语和词汇构建示例

术语	词汇	含义
ODD	人行横道	有标线或标志的人行过街设施
	行人正在通过	行人已进入人行横道或表现出明确的过街意图
	无交通信号灯道路	无红绿灯、标志标线或交警指挥的道路（如胡同、小区内部路）
	行人横过道路	行人以垂直或斜向路径穿越车行道
行为能力	减速行驶	降低车速至可随时泊车的安全范围
	泊车让行	降低车速至0 m/s，直至行人离开
	避让	横向偏移或泊车避免与行人冲突

（2）模糊术语量化转换。对依赖人类认知的模糊表述进行参数化定义，将法规要求转化为可计算、可判定的指标条件（表9）。该过程使交通规则具备自动化验证所需的形式化基础。

表9　模糊术语及其量化转换方案示例

术语	量化转换方案
减速行驶	速度≤20 km/h或$v\leq\sqrt{2ad}$（其中a=3 m/s²，d为行人距离）
行人正在通过	行人速度>0.5 m/s
	运动方向与人行横道线夹角∈[30°, 150°]
	行人进入以车辆为中心、半径50 m的检测区域
泊车让行	减速度1.5~3 m/s²，直至车速v=0 m/s
	泊车位置与行人的距离≥1.5 m
	让行持续条件：泊车维持至行人完全离开车辆所在车道或相邻车道，横向距离>2 m
避让	横向偏移≥0.5 m或泊车等待
	响应时间≤1.5 s

（3）逻辑抽象与函数定义。定义布尔或数值函数，用于描述规则触发条件与系统状态（表10），为规则嵌入测试系统提供逻辑组件。

表10　逻辑表达式示例

函数	输出类型	含义
isEgo(x)	布尔值	x为自动驾驶车辆
isPedestrian(y)	布尔值	y为行人
isCrossing(y)	布尔值	y正在通过人行横道，且满足步骤（2）中“行人正在通过”的量化条件
isAtCrosswalk(y)	布尔值	y位于人行横道区域内
hasNoTrafficSignal()	布尔值	当前道路无交通信号灯
calcSafeDistance(v)	距离/m	安全距离$d=v\times1.5+v^2/(2a)$（v为自车速，a=3 m/s²）
isStopped(x)	布尔值	自车速度为0 m/s且持续时间≥1.0 s
getLateralDist(x,y)	距离/m	自车与行人的横向距离

（4）规则编码生成。通过逻辑运算符和变量声明，将规则条件与行为约束组合，形成可嵌入测试系统的判定规则，实现对ADS行为的“通过/未通过”判定（表11）。

通过上述编码过程，每条交通通行规则可映射至ADS的感知、规划与控制链路，明确触发条件、预期响应及判定标准，从而显著提升测试的合规性和可追溯性。需要指出的是，交通通行规则主要适用于标称情境，在风险或边界情境下仍需引入安全模型进行补充评估。

2.6.2　安全模型与风险评估指标

在高风险情境或交通通行规则不足以确保碰撞避免时，仅依赖规则符合性难以全面评价ADS行为的安全性与合理性。为此，本文引入安全模型对系统风险规避能力进行量化，其核心作用在于明确碰撞风险可接受边界，从而判定何时应当采取规避动作，何时可通过风险缓解满足安全要求[4-5]。

在ADS验证中，安全模型主要承担3类任务：（1）碰撞风险分类，区分可通过系统响应消除的风险与在合理范围内可接受的残余风险；（2）系统响应评估，衡量感知、决策与控制执行链路在风险情境下的响应及时性与有效性；（3）在交通规则与安全要求发生冲突时，提供优先级决策依据。基于典型安全模型，如责任敏感安全（Responsibility-Sensitive Safety，RSS）[25]、最后转向点（Last Point to Steer，LPTS）[26]、安全区（Safety Zone）[26]、模糊安全（Fuzzy Safety）[5]等，可建立安全模型、性能指标及验证准则的映射关系（表12）。

验证流程可归纳为3个步骤：（1）由安全模型推导关键性能指标，并设定安全阈值。（2）在自动化测试过程中实时计算安全距离、响应时间、潜在碰撞速度等指标，并动态评估风险水平。（3）将安全性能指标嵌入测试判定逻辑，作为测试通过与否的直接依据。

2.6.3　失效场景下的风险评估

当ADS出现功能异常或部件故障时，需重点评估其容错能力与最小风险策略的执行效果。在此类场景下，需要结合风险评估方法对系统安全性进行综合判定，主要包括：（1）基于ISO 26262的风险等级评估模型[15]；（2）基于计算实验的概率估计方法，用于估计失效条件下的碰撞概率分布；（3）通过风险空间覆盖度，衡量测试场景集合对潜在风险的代表性；（4）融合交通规则符合性、安全模型判定结果与风险等级评估，形成联合判定准则。

最终，通过验证ADS在功能或部件失效条件下的行为响应及风险演化过程，并判定其残余风险是否满足合理可行最低限度（As Low As Reasonably Practicable，ALARP）原则，实现对失效场景安全性的验证闭环。

表11　规则编码示例

规则内容	规则编码	解释
机动车行经人行横道时，应当减速行驶	$\forall x$: isEgo(x)/\isNearCrosswalk() →setSpeed(x,min(v, 20))	只要接近人行横道，无论是否有行人，自车x速度不得超过20 km/h
遇行人正在通过人行横道，应当泊车让行	$\forall x,y$: isEgo(x)/\isPedestrian(y)/\isCrossing(y)/\isAtCrosswalk(y) →mustStop(x)/\maintainStopUntil(getLateralDist(x,y)>2)	当自车x检测到行人y正在人行横道上通行时，应当完全泊车；维持泊车状态直至与行人的横向距离>2 m
机动车行经没有交通信号灯的道路时，遇行人横穿车道，应当避让	$\forall x,y$: isEgo(x)/\isPedestrian(y)/\hasNoTrafficSignal()/\isCrossingRoad(y) →(calcLateralOffset(y)≥0.5m\/executeFullStop(x))	若行人y横穿车道，自车x需横向偏移≥0.5 m或完全泊车；选择逻辑由安全距离决定：若TTC<2.5 s则触发泊车

表12　典型安全模型、性能指标与验证准则映射

安全模型	主要方法	典型性能指标	验证准则	适用场景与优势
RSS	定义纵向与横向安全距离，基于责任假设计算安全空间	纵向和横向安全距离、最小缓冲空间	纵向和横向安全距离应不低于阈值	交互不确定、责任界定不明场景：提供安全缓冲
LPTS	计算最后可转向时间点，量化纵向碰撞缓解能力	最后可转向时间点、纵向碰撞缓解能力	纵向极限工况下，系统应有效避免碰撞	纵向碰撞极限工况：提供纵向极限工况下避免碰撞的基线能力，提供风险边界
Safety Zone	基于预设安全空间阈值并结合潜在碰撞速度计算风险缓解能力	安全空间阈值、潜在碰撞速度、风险缓解能力	横穿场景下，系统风险应低于阈值	弱势道路使用者横穿场景：针对弱势道路使用者，量化系统风险水平
Fuzzy Safety	将风险从二值判定转化为连续等级，结合时间裕度、速度差、感知置信度等不确定因素	时间裕度、速度差、感知置信度、动态风险等级	风险等级应处于可接受范围内	高不确定性、复杂交互场景：提供连续风险分级，支持动态风险评估

2.7 验证覆盖度与残余风险评估

验证覆盖度与残余风险评估共同构成支持ADS安全声明的核心机制[4]。为构建从场景覆盖到风险收敛的完整闭环，包括3方面：(1)建立行为能力-测试场景的映射关系，用于识别验证空白区域；(2)基于参考行为模型(交通通行规则编码、安全模型)，界定合理性边界；(3)在验证过程中通过场景扩展与样本迭代，推动残余风险逐渐收敛至可接受水平。

2.7.1 验证覆盖度的定义与评价

验证覆盖度衡量测试场景在整个ODD中的代表性与完整性。本文通过构建行为能力与测试场景映射矩阵，明确每项能力的验证情况，识别潜在的验证空白区域，确保测试涵盖ADS运行中可能遇到的标称、危险、失效与边界场景组合，避免样本选择偏差导致验证不充分或系统性能被高估。

2.7.2 残余风险的可信性评估

当测试覆盖度达到一定水平后，需要评估系统在未覆盖情境中的安全表现是否可信。结合安全模型中定义的性能指标，残余风险的评估应结合场景扩展与测试迭代，而非简化为单一概率值，而是通过场景扩展与测试迭代逐步收敛，形成充分的验证证据。核心机制包括：(1)可接受风险定义：基于参考行为模型界定事故是否“可避免”，划分可接受与不可接受的行为边界。(2)参考行为-场景映射矩阵：将规范性行为模型应用于不同场景组合，检验系统表现是否落入“合理驾驶行为”集合。(3)验证迭代机制：通过新场景扩展或更高保真度测试补充证据，直至残余风险收敛并趋近于可接受范围。

2.7.3 多支柱测试方法的场景适配性

验证覆盖度不仅取决于场景设计，也与测试方法选择有关。仿真测试支持参数空间扩展与极端工况探索，适用于ADS系统全生命周期的安全验证。场地测试，对经过仿真测试验证，需要实车进一步验证确认的区间，在可控环境下，重复验证特定的安全关键工况。道路测试，验证系统在真实交通流中适应性与规则遵守。具体应用时，根据场景复杂性、测试目标和资源约束，选择最适合的测试方式，并在不同方法之间形成互补。

2.7.4 数据采样与处理技术

为提升验证覆盖度与场景代表性，可采用系统化的数据采样与处理方法：

(1)参数采样。通过随机或分层采样方式选择参数值，避免测试过程因过度依赖有限场景集而产生过拟合效应。

(2)最大化样本多样性。覆盖长尾场景，确保最大化场景差异性。

(3)数据处理流程。包括数据预处理与清洗、标准化格式转换、手工与自动化数据标注、场景因子提取与分类、数据聚类与概率分布估计等[27]。支持构建验证场景要素与概率分布特性。

通过抽样技术与场景参数扰动机制生成测试集，并在多支柱测试中协同进行，逐步收敛至可信的残余风险水平。

3 评测场景集构建实践

3.1 单一场景构建

以高速公路前车切出场景为例，构建如图4所示的测试场景。在场景构建过程中，系统性地考虑目标物及事件探测与响应能力的影响因素；同时关注主车在横向与纵向运动中的安全性及紧急避撞策略的执行能力，涉及关键运动参数。

基于功能场景要素和逻辑场景参数，并结合安全要求分析，该功能场景重点关注ODD和车辆行为。逻辑场景参数的取值范围综合考虑道路设计标准、限速要求及场景合理性，如表13所示。

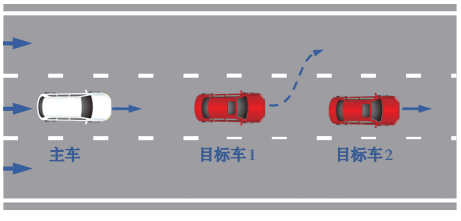


图4 “前车切出”场景示意

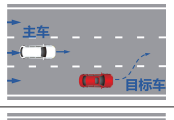
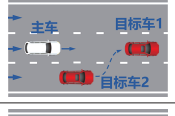
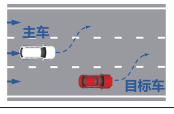
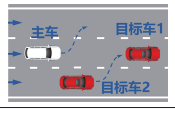
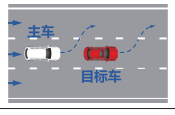
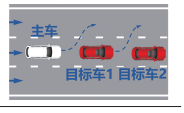
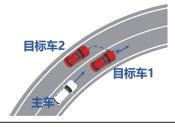
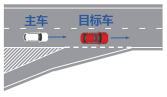
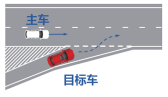
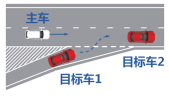
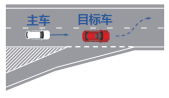
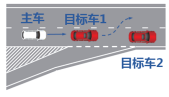
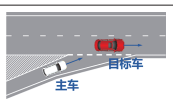
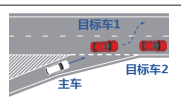
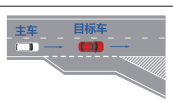
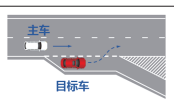
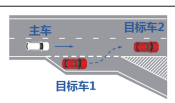
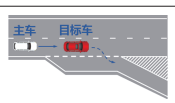
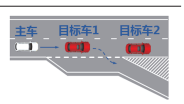
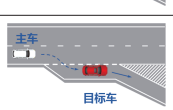
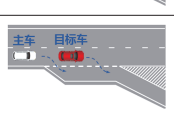
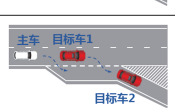
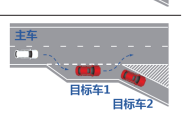
3.2 评测场景集构建

基于ADS评测场景集构建要求，本文以高速公路和城市快速路应用场景为例展示评测场景集构建实践(表14)。动态驾驶任务功能场景应确保车辆在横纵向运动中安全，能够对目标物及交通事件进行及时响应并执行紧急避撞策略，同时遵守交通通行规则。通过组合目标物、道路、主车及目标物行为等要素，可构建不同道路类型下的主车与目标物交互场景，以验证动态驾驶任务的安全性。对于超出ODD而无法继续执行动态驾驶任务的情况，车辆需具备请求用户接管或执行最小风险策略的能力。基于用户主动干预或误操作的场景，可验证人机交互安全性；在车辆或系统失效的情况下，需确保能够检测失效并采取适当响应。通过参数定义和取值范围控制，可满足不同安全要求的测试目的。

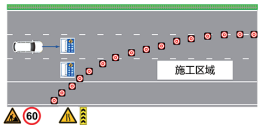
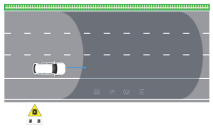
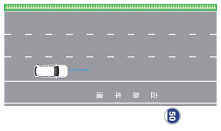
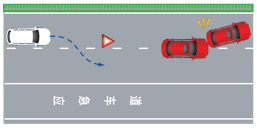
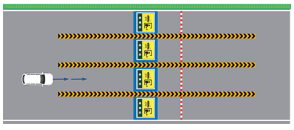
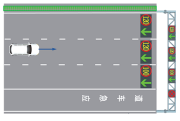
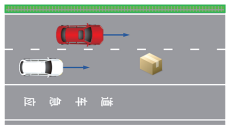
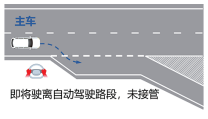
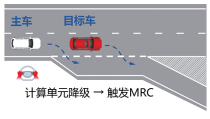
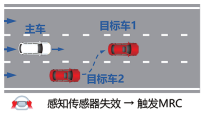
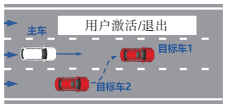
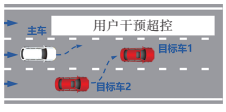
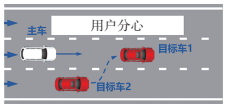
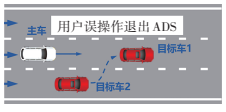
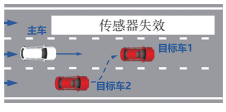
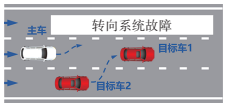
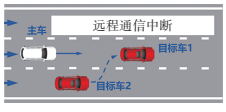
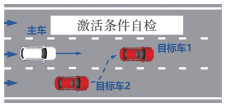
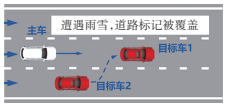
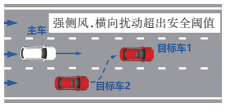
表 13　L3 级自动驾驶系统的“前车切出”场景要素示例

功能场景要素				逻辑场景参数及范围分布
设计运行条件	ODD	道路	高速公路	坡度：[−10°，10°]，弯道半径：[150，300，500] m 同向车道数：[2≤α≤5，α 取正整数]，本车所在车道：[1−α，取正整数，沿主车行驶方向从左至右进行编号] 车道宽度：[3.25，4] m，路面摩擦因数：[0.6，0.8]
		道路设施	道路标线	道路标线：[白虚，白实，黄虚，黄实，双白虚，双白实，白色虚实，黄色虚实，双黄虚，双黄实]
		目标物	汽车	类型：[载客汽车、载货汽车、专用作业车]
		与天气相关的环境条件	晴天	光照：[1 000，100 000] lx 能见度：[200，3 000] m
		数字信息	位置信息	[有，无]位置信号：北斗
	车辆状态	运动状态	运行速度	速度范围：0~120 km/h
		依赖条件	有	通信正常、高精度地图有效
	驾乘人员状态	驾驶员状态	可用	未分心/未闭眼、坐在驾驶座位、系安全带
		乘员	正常	系安全带、坐在座位
行为	主车	主车预期动作	车道保持	初始速度：50~100 km/h
	目标物	目标物初始状态	与主车同车道、主车前方、同向行驶	目标车 1 与主车初始纵向间距：50~100 m 目标车 2 与主车初始纵向间距：120~150 m
		目标物动作	目标车 1：切出 目标车 2：车道保持	目标车 1 初始速度：40~80 km/h 目标车 1 切出方向：向左切出、向右切出 目标车 1 切出动作持续时间：2~15 s 目标车 2 初始速度：10~30 km/h

表 14　高速公路和城市快速路下的测试场景集

场景大类	场景分类	测试场景示例（功能场景级别）							
		道路几何	自车行为	交互行为					
				前车减速	目标车切入	有前车−目标车切入	目标车切出	前车切出后有前车	
基础 DDT 场景	与动态 ORU 交互	直道	巡航						
			变道						
		弯道	巡航						
			变道						
		匝道入口	巡航						
			变道						
		匝道出口	巡航						
			变道						

续表

场景大类	场景分类	测试场景示例(功能场景级别)				
基础DDT场景	与静态基础设施交互	 车道线缺失/模糊	 施工区	 隧道	 限速标志	
		 事故现场	 收费站	 可变信息标志	 临时性障碍物	
叠加场景	DDT后援	 +超出ODD边界接管	 +超出ODD边界未接管	 +算力不足降级	 +传感器失效	……
	人机交互	 +用户激活/退出	 +用户干预(转向/制动)	 +用户闭眼/分心	 +用户误操作	……
	系统内部状态	 +传感器失效	 +执行器故障	 +通信故障	 +激活条件自检	……
	外部环境状态	 +弱光照条件	 +暴雨	 +雨雪	 +强侧风	……

注:ORU(Other Road User)为其他道路使用者。

4 方法对比与优势分析

从方法论、验证逻辑、覆盖性、效率等维度,本文框架与当前主流方法对比情况如表15所示。本文核心特点在于通过建立“ODD-行为能力-测试场景”的结构化映射链路,将验证从基于经验和统计的活动转变为目标明确、逻辑清晰、过程可控的工程过程。

表15 本文验证框架与现行主流方法的系统性对比[28-29]

对比维度	里程累积法	离散场景库法	本文框架
方法论基础	基于里程统计的归纳验证	基于场景枚举的经验验证	基于ODD与行为能力结构化映射的演绎-归纳协同验证
验证目标关联性	测试场景与安全目标关联性弱,验证充分性难以论证	场景与安全目标映射关系模糊,覆盖度评估主观性强	建立能力-场景-准则可追溯链条,验证目标明确且可量化
场景覆盖完备性	长尾场景覆盖效率低,验证充分性难以证明	场景选择依赖经验,存在系统性覆盖盲区	通过ODD与行为能力结构化映射,实现系统性场景覆盖
验证效率	需海量里程积累,成本高	场景库规模膨胀快,管理复杂度高	针对性生成高风险场景,效率高
工程可扩展性	新功能需重新累积里程,扩展性差	新场景需重新收集标注,扩展性一般	模块化设计支持快速适配新ODD与功能,扩展性好
合规性支撑	难以提供结构化证据链	可提供部分合规证据,但系统性不足	与国内外法规标准自然对齐
残余风险评估	依赖统计推断,风险评估可信度低	仅评估已测场景风险	系统化评估残余风险

5 结束语

结合当前行业实践，本文构建以“ODD-行为能力-测试场景-验证准则-风险评估”为主线的ADS验证方法。该方法通过系统化构建能力-场景映射关系与覆盖度评估机制，实现验证目标可溯源、验证范围可界定与测试场景可生成，并引入风险评估机制以支撑验证完整性与风险容忍度量化。

本文提出的框架为自动驾驶系统的安全验证提供了一种系统化的解决方案，为安全声明、产品合规性提升及验证体系构建提供参考。未来工作将聚焦方法适用性验证、工具链开发、标准适配等，支撑高可信度仿真与实车测试的融合应用。

参 考 文 献

[1] 刘法旺, 徐晓庆, 陈贞, 等. 搭载自动驾驶功能的智能网联汽车安全测试与评估方法研究[J]. 汽车工程学报, 2022, 12(3): 221-227.

[2] United Nations Economic Commission for Europe. Framework Document on Automated/Autonomous Vehicles: WP.29/2019/34/Rev.1[R]. Geneva: UNECE, 2019.

[3] United Nations Economic Commission for Europe. New Assessment/Test Method for Automated Driving (NATM)-Master Document[R]. Geneva: UNECE, 2021.

[4] United Nations Economic Commission for Europe. Guidelines and Recommendations for Automated Driving System Safety Requirements, Assessments and Test Methods[R]. Geneva: UNECE, 2024.

[5] United Nations Economic Commission for Europe. UN Regulation No. 157: Uniform Provisions Concerning the Approval of Vehicles with Regard to Automated Lane Keeping Systems[S]. Geneva: United Nations, 2021.

[6] European Commission. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 Laying Down Rules for the Application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles[S]. Brussels: European Commission, 2022.

[7] United Nations Economic Commission for Europe. UN Regulation No. 185: Uniform Provisions Concerning the Approval of Motor Vehicles with Regard to Their Automated Driving Systems[S]. Geneva: United Nations, 2026.

[8] The ADS Informal Working Groups. Big Picture: High-Level Overview(ADS-12-41)[C]// Proceedings of ADS IWG 12th Session, 2025.

[9] International Organization for Standardization. Road Vehicles-Test Scenarios for Automated Driving Systems-Specification for Operational Design Domain: ISO 34503:2023[S]. Switzerland: ISO, 2023.

[10] International Organization for Standardization. Road Vehicles-Test Scenarios for Automated Driving Systems-Scenario Based Safety Evaluation Framework: ISO 34502:2022[S]. Switzerland: ISO, 2022.

[11] Institute of Electrical and Electronics Engineers. IEEE Standard for Assumptions in Safety-Related Models for Automated Driving Systems: IEEE 2846-2022[S]. New York: IEEE, 2022.

[12] PEGASUS Project. The PEGASUS Method[EB/OL]. (2019-02-14) [2025-12-25]. https://www. pegasusprojekt. de/en/pegasus-method.

[13] The ADS Informal Working Groups. ODD-Based Behavioral Competencies and Scenario Identification Approach[C]// Proceedings of ADS IWG 12th Session. Helsinki: 2025.

[14] 国家市场监督管理总局, 国家标准化管理委员会. 汽车驾驶自动化分级: GB/T 40429—2021[S]. 北京: 中国标准出版社, 2021.

[15] International Organization for Standardization. Road Vehicles-Functional Safety: ISO 26262:2018[S]. Switzerland: ISO, 2018.

[16] The ADS Informal Working Groups. Proposal for a New United Nations Regulation on Uniform Provisions Concerning the Approval of Motor Vehicles with Regard to Their Automated Driving Systems[EB/OL]. (2025-11-11) [2025-12-25]. https://wiki. unece. org/spaces/trans/pages/310575388/ADS+16th+Session.

[17] International Organization for Standardization. Road Vehicles-Test Scenarios for Automated Driving Systems-Vocabulary: ISO 34501:2022[S]. Switzerland: ISO, 2022.

[18] British Standards Institution. Operational Design Domain-Implementation of BS ISO 34503:2023-Guide: BSI PAS 1883:2025[S]. London: BSI, 2025.

[19] SAJJAD M, OMAR Y, MEHRDAD D, et al. Deep Learning-based Vehicle Behaviour Prediction for Autonomous Driving Applications: a Review[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(1): 33-47.

[20] CHANG C, ZHANG J, GE J, et al. VistaScenario: Interaction Scenario Engineering for Vehicles with Intelligent Systems for Transport Automation[J]. IEEE

Transactions on Intelligent Vehicles, 2024, 9(3): 2803-2819.

[21] International Organization for Standardization. Road Vehicles-Safety of the Intended Functionality: ISO 21448: 2022[S]. Switzerland: ISO, 2022.

[22] 工业和信息化部, 公安部, 住房和城乡建设部, 等. 智能网联汽车准入和上路通行试点实施指南(试行)[EB/OL]. (2023-11-17) [2025-12-25]. https://www. gov. cn/zhengce/zhengceku/202311/P020231111746586573 4883. pdf.

[23] European Commission. Regulation (EU) 2019/2144 of the European Parliament and of the Council as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles[S]. Brussels: European Commission, 2022.

[24] 全国人民代表大会常务委员会. 中华人民共和国道路交通安全法[M]. 北京: 法律出版社, 2021.

[25] SHASHUA A, SHALEV-SHWARTZ S, SHAMMAH S. Implementing the RSS Model on NHTSA Pre-Crash ScenarIOS[R/OL]. Mobileye, (2018)[2025-08-25]. https://static.mobileye.com/website/corporate/rss/rss_on_nhtsa.pdf.

[26] The FRAV Informal Working Groups. Draft text for Safety Models annex(FRAV-42-04) [C]// Proceedings of FRAV 42nd Session, 2023.

[27] ELGHARBAWY M, SCHWARZHAUPT A, FREY M, et al. Ontology-based Adaptive Testing for Automated Driving Functions Using Data Mining Techniques[J]. Transportation Research Part F: Traffic Psychology and Behaviour, 2019, 66: 234-251.

[28] KOOPMAN P, WAGNER M. Challenges in Autonomous Vehicle Testing and Validation[J]. SAE International Journal of Transportation Safety, 2016, 4(1): 15-24.

[29] MENZEL T, BAGSCHIK G, MAURER M. Scenarios for Development, Test and Validation of Automated vehicles[C]// Proceedings of the IEEE Intelligent Vehicles Symposium, 2018: 1821-1827.

（责任编辑　**梵玲**）

《汽车工程师》征稿启事

《汽车工程师》于1974年创刊，是由中国第一汽车集团有限公司主管、中国第一汽车股份有限公司主办的国内外公开发行的汽车应用技术类学术期刊，为RCCSE中国准核心学术期刊、CACJ中国应用型扩展期刊，被哥白尼精选数据库、EBSCO学术数据库、欧洲学术出版中心(EuroPub)数据库、J-Gate数据库收录。

《汽车工程师》以报道汽车产品设计领域的技术研究成果为主，专注于技术开发与应用层面的创新成果，提供汽车设计创新解决方案。《汽车工程师》将把握电动化、智能化、网联化、共享化的汽车技术主流发展趋势，努力吸收优质稿源，为我国汽车工程技术创新能力提升贡献力量。重点征稿方向包括：锂离子电池与新体系电池、动力电池热管理与热失控、燃料电池及其关键零部件、车用电机及其控制器、自动驾驶汽车环境感知与感知融合、自动驾驶汽车定位与建图、自动驾驶汽车测试、人工驾驶-无人驾驶车辆混行条件下的自动驾驶控制、智能线控底盘、一体化底盘、功能安全和预期功能安全。

热忱欢迎汽车行业的专家学者不吝赐稿，反映国家重点扶持项目、自然科学基金项目和其他重点项目等研究成果的稿件将优先发表，我们期待与您共同践行“把论文写在祖国大地上”的指示精神，为强大中国汽车工业作贡献！

本刊使用协同采编系统处理稿件，请登陆期刊网站注册后投稿，投稿要求见本刊网站中“下载中心”栏目的作者指南，网址：http://tjqc.cbpt.cnki.net。

《汽车工程师》编辑部