

## 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

刘法旺<sup>1</sup>, 徐晓庆<sup>2</sup>, 陈贞<sup>3</sup>, 李艳文<sup>1</sup>, 李京泰<sup>1</sup>, 潘鹏<sup>4</sup>, 张晋崇<sup>5</sup>, 张志强<sup>6</sup>

(1. 工业和信息化部装备工业发展中心, 北京 100846; 2. 中国汽车工程研究院股份有限公司, 重庆 401122;  
3. 北京镒石数据科技有限公司, 北京 100176; 4. 襄阳达安汽车检测中心有限公司, 湖北, 襄阳 441004;  
5. 国汽(北京)智能网联汽车研究院有限公司, 北京 100176; 6. 中国汽车技术研究中心有限公司, 天津 300300)

**摘要:** 目前, 针对搭载自动驾驶功能的智能网联汽车, 国内外正在广泛开展特定设计运行条件下的道路测试、示范应用等工作, 其安全测试与评估方法已经成为当前行业研究的热点和难点。从第三方视角出发, 重点针对汽车智能化、网联化面临的主要安全风险, 将智能网联汽车的安全测试与评估分为基础测评和监测调整两个阶段。在基础测评阶段, 综合评估产品对过程保障及测试要求的符合情况; 在监测调整阶段, 基于对车辆实际安全状态的监测, 适时调整安全评估结果。在此基础上, 重点梳理了基于场景的测试、安全评估、监测等测评方法的内在逻辑及原则要求。分别阐述了功能安全、预期功能安全、网络安全和数据安全等过程保障方法及主要要求, 以及模拟仿真、封闭场地、实际道路、网络安全和数据安全、软件升级、数据记录等测试方法及主要要求。提出的方法为特定设计运行条件下, 具有自动驾驶功能的智能网联汽车综合安全评估提供了参考。

**关键词:** 设计运行条件; 自动驾驶功能; 智能网联汽车; 安全测试与评估; 方法

中图分类号: U461.91 文献标志码: A DOI: 10.3969/j.issn.2095-1469.2022.03.01

## Research on Safety Testing and Assessment Methods for Intelligent and Connected Vehicles with Autonomous Driving Functions

LIU Fawang<sup>1</sup>, XU Xiaoqing<sup>2</sup>, CHEN Zhen<sup>3</sup>, LI Yanwen<sup>1</sup>, LI Jingtai<sup>1</sup>, PAN Peng<sup>4</sup>,  
ZHANG Jinchong<sup>5</sup>, ZHANG Zhiqiang<sup>6</sup>

(1. Equipment Industry Development Center, Ministry of Industry and Information Technology, Beijing 100846, China;  
2. China Automotive Engineering Research Institute Co., Ltd., Chongqing 401122, China;  
3. Beijing Dishu Data Technology Co., Ltd., Beijing 100176, China;  
4. Xiangyang Da An Automobile Test Center Co., Ltd., Xiangyang 441004, Hubei, China;  
5. China Intelligent and Connected Vehicles(Beijing)Research Institute Co., Ltd., Beijing 100176, China;  
6. China Automotive Technology and Research Center Co., Ltd., Tianjin 300300, China)

**Abstract:** So far, road testing and demonstration applications for intelligent and connected vehicles (ICVs) with autonomous driving functions have been widely carried out at home and abroad. The challenges in the safety testing and assessment methods for ICVs have attracted great attention of researchers. Initially this paper focuses on the main safety risks in intellectualization and networking of vehicles, and divides the safety test and assessment process into two stages: the basic assessment and monitoring and adjustments. In the

收稿日期:2022-04-06 改稿日期:2022-04-06

网络首发:2022-04-16

参考文献引用格式:

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.  
LIU Fawang, XU Xiaoqing, CHEN Zhen, et al. Research on Safety Testing and Assessment Methods for Intelligent and Connected Vehicles with Autonomous Driving Functions[J]. Chinese Journal of Automotive Engineering, 2022, 12(3): 221-227. (in Chinese)



basic assessment stage, the product is comprehensively assessed for compliance with process assurance and testing requirements. In the stage of monitoring and adjustments, the safety assessment results are adjusted timely based on the vehicle condition monitoring. Then the inherent logic, principles and requirements of scenario-based testing, safety assessment and monitoring are described emphatically. Finally the paper elaborates the methods and the main requirements for process assurance, i.e. the functional safety, the safety of the intended functionality, cyber security and data security, and illustrates the test methods including the simulation/virtual testing, track testing, real-world testing, cyber security and data security testing, data storage testing and software update testing. The method proposed in this paper provides a reference for the comprehensive safety assessment of intelligent and connected vehicles with autonomous driving functions under specific operational design conditions.

**Keywords:** operational design condition; autonomous driving function; intelligent and connected vehicle; safety test and assessment; method

智能网联汽车是汽车产业转型升级的重要战略方向,正处于技术快速演进、产业加速布局的商业化前期阶段。随着搭载自动驾驶功能的智能网联汽车技术及产业的快速发展,功能安全、预期功能安全、网络安全等安全风险更加凸显。安全测试与评估是推动车辆产品量产、保障车辆安全运行的关键环节。然而,搭载自动驾驶功能的智能网联汽车安全测试与评估方法还不成熟,传统的车辆测试验证方法无法覆盖新的安全风险,这也为其规模化安全应用带来了挑战。

针对智能网联汽车的安全管理,国内外行业管理部门均高度重视并持续开展研究,通过制定相关政策、法规、标准等不断完善智能网联汽车安全管理体系,促进智能网联汽车产业生态的迭代优化。联合国世界车辆法规协调论坛自动驾驶工作组(WP.29/GRVA)审议通过了《自动驾驶框架文件》,针对搭载自动驾驶功能的智能网联汽车,明确工作原则、安全愿景以及优先关注的原则性要求,为附属工作组提供工作指导<sup>[1]</sup>。欧盟、美国、日本等国家或组织积极参与联合国法规研讨,并先后颁布了多部智能网联汽车相关政策和法规<sup>[2-15]</sup>,初步建立了对智能网联汽车产品的安全要求框架,明确了各相关管理部门的职责和协同机制,加速智能网联汽车的开发与部署,为搭载自动驾驶功能的智能网联汽车获得型式批准奠定了基础。为助力智能网联汽车的研发测试和示范应用,我国有关部委发布了智能网联汽车相关政策<sup>[16-17]</sup>,明确管理的原则要求及基本框架,引导地方开展智能网联汽车道路测试与

示范应用,为智能网联汽车产业营造了良好的测试和示范应用环境,为搭载自动驾驶功能智能网联汽车的规模化应用管理积累了经验。

对搭载自动驾驶功能的智能网联汽车开展安全测试及评估,是一项复杂的系统工程,面临诸多挑战。例如,智能网联汽车应用场景复杂,无法保障场景覆盖、逻辑覆盖等测试要求;自动驾驶功能依赖人工智能技术,测试验证面临黑箱难题;预期功能安全、数据安全等领域,面临从理论研究到技术实践的落地问题。目前看,很难通过传统的测试方法全面有效地验证智能网联汽车的安全性。

对于智能网联汽车安全测试与评估方法,国内外相关机构都在不断研究探索。联合国自动驾驶验证方法非正式工作组(VMAD IWG)提出一种新的测试评估方法<sup>[18]</sup>,包括场景目录和五类技术手段(模拟仿真测试、封闭场地测试、实际道路测试、审核评估和在用监测报告),逐步获得行业共识,整体框架也在不断完善。我国工业和信息化部也在持续推进智能网联汽车准入管理研究<sup>[19-20]</sup>,逐步明确智能网联汽车产品准入在产品过程保障、测试验证等方面的要求。

参考国内外测试评估方法研究,结合我国智能网联汽车的安全管理需求,本文以搭载3级和4级自动驾驶功能<sup>[21]</sup>的智能网联汽车作为研究对象,重点针对车辆在智能化、网联化背景下面临的功能安全、预期功能安全、网络安全、数据安全等安全风险,从第三方视角出发,研究提出一种系统、可复用、可扩展的安全测试与评估方法,实现对特定

设计运行条件 (Operational Design Condition, ODC) 下搭载自动驾驶功能智能网联汽车的综合安全评估。

## 1 安全测试与评估方法

### 1.1 总体思路

由于具有 ODC 要素组合多样、应用场景复杂、安全问题动态等特点, 仅靠传统测试手段难以实现对搭载自动驾驶功能智能网联汽车安全性的科学全面评估。本方法将智能网联汽车的安全测试与评估分为基础测评和监测调整两个阶段, 即在基础测评阶段综合评估产品对过程保障及测试要求的满足情况, 在监测调整阶段对车辆实际安全状态进行监测, 根据监测结果适时调整评估结果。智能网联汽车安全测试与评估方法的框架, 如图 1 所示。

3 级和 4 级自动驾驶功能是基于 ODC 设计开发的, 汽车生产企业应建立相适应的功能安全、预期功能安全、网络安全、数据安全和软件升级等安全保障能力, 并应在科学规范的产品过程保障要求下开展产品的研发及测试验证。对于搭载自动驾驶功能的智能网联汽车的产品安全要求, 也是基于 ODC 提出的, 主要包含技术要求、过程保障要求和测试要求 3 个方面。其中, 技术要求包含动态驾驶任务执行和后援、人机交互等; 过程保障要求包含功能安全、预期功能安全、网络安全和数据安全等, 重点针对驾驶自动化系统, 应覆盖产品开发过程中要求的软硬件级、系统级和整车级; 测试要求包含模拟仿真、封闭场地、实际道路、网络安全和数据安全、软件升级、数据记录等, 用于支撑整车级产品测试验证和安全评估。

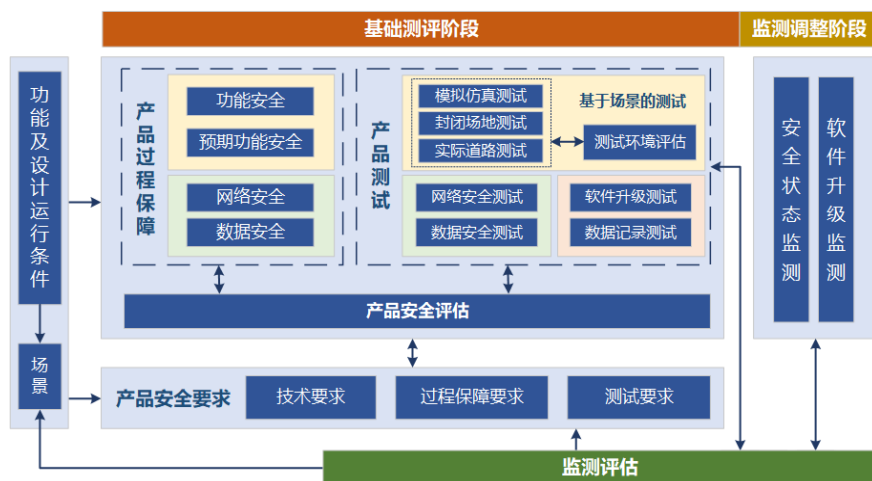


图1 智能网联汽车安全测试与评估方法框架

在基础测评阶段, 应结合汽车生产企业和检验检测机构的差异化功能定位, 综合发挥两者的比较优势, 对智能网联汽车开展基于场景的测试, 以及网络安全和数据安全测试、数据记录测试、软件升级测试等, 测试验证应具备足够的覆盖度。在此基础上, 综合考虑产品对过程保障及测试要求的满足情况, 形成对智能网联汽车产品的综合安全评估结果。

在监测调整阶段, 通过对车辆实际安全状态进行有针对性的监测分析, 适时修正评估结果, 并不断细化完善智能网联汽车安全测试与评估体系。同时, 通过状态监测, 也有利于加强对汽车生产企业

软件升级活动的监督管理, 保障车辆产品持续满足相关安全管理要求及产品生产一致性要求。

### 1.2 基于场景的测试

基于场景的测试方法, 围绕产品安全分析输出的测试场景, 采用模拟仿真、封闭场地和实际道路等测试方法, 测试评估搭载自动驾驶功能智能网联汽车的行驶安全性。模拟仿真、封闭场地和实际道路 3 种测试方法的优缺点, 见表 1。

3 种测试方法各有侧重, 实际测试中需要遵循一定的逻辑关系, 实现三者优势互补。基于自动驾驶功能的 ODC, 构建充分合理的场景数据集, 通过



表1 基于场景的测试方法优缺点对比

| 测试方法 | 保真度 | 成本 | 效率 | 可复制性 | 安全性 | 场景覆盖度 |
|------|-----|----|----|------|-----|-------|
| 模拟仿真 | 低   | 低  | 高  | 高    | 高   | 高     |
| 封闭场地 | 中   | 高  | 低  | 中    | 中   | 低     |
| 实际道路 | 高   | 中  | 中  | 低    | 低   | 中     |

模拟仿真测试,初步评估智能网联汽车的行驶安全性并验证ODC边界,识别出危险场景;通过封闭场地测试,基于选定的典型场景,验证智能网联汽车的功能;通过实际道路测试,基于足够的测试里程及测试场景要素覆盖,评估智能网联汽车应对实际交通的安全性和可靠性,并将实际道路中有价值的新场景更新到场景数据集中。

在实际测试过程中,需评估自动驾驶功能及ODC、测试项目以及测试环境(软件、硬件、车辆、驾驶员、道路环境等),综合研究制定测试策略,通常按照模拟仿真测试、封闭场地测试、实际道路测试的顺序依次开展测试工作,但也可以针对特定的安全测试需求进行调整和补充。

### 1.3 安全评估

智能网联汽车安全评估是实现车辆产品安全管理的关键支撑,主要采用系统工程方法,开展产品过程保障、测试验证等审核工作。安全评估应充分考虑产品开发过程中对功能安全、预期功能安全、网络安全和数据安全等过程保障要求的满足情况,同时应保障产品测试验证策略具备足够的覆盖度。测试验证应充分考虑汽车生产企业为满足产品过程保障要求开展的研发测试,以及必要的检验检测结果。

安全评估在考虑产品满足各类测试要求的基础上,还应综合考虑不同测试方法的优缺点,实现不同测试方法之间的相互补充,提高安全评估的科学性、针对性和有效性。

### 1.4 监测评估

监测评估可以分为基础测评和监测调整两个阶段。基础测评阶段主要针对计划量产的研发测试车辆,支撑对车辆开展综合性安全评估。监测调整阶段则是针对已投入使用的车辆,主要发挥3个方面的作用。一是基于监测结果,及时发现前期安全评估

结果与车辆实际安全状态之间的偏差,适时调整评估结果;二是基于车辆运行数据的反馈分析,有效支撑对产品安全要求、测试与评估方法等管理体系的评估与调整;三是车辆实际使用过程中可能会遇到新的有价值场景,可用于更新和完善场景数据集。

## 2 过程保障及测试方法

### 2.1 功能安全过程保障

功能安全定义为不存在由电子电气系统的功能异常行为引起的危害而导致不合理的风险<sup>[22]</sup>。对于搭载自动驾驶功能的智能网联汽车,驾驶权可能发生转移,功能安全风险更加突出。

为保障智能网联汽车达到一定的功能安全水平,需要对智能网联汽车,尤其是自动驾驶系统,提出功能安全保障要求。一是设计方面,要满足失效识别、危害分析和风险评估、安全分析等要求;二是验证方面,要满足功能安全集成测试和确认要求;三是开发接口方面,要保障系统、硬件和软件各层级满足整车功能安全要求。功能安全过程保障侧重对产品开发过程提出要求,核心是保障智能网联汽车安全运行的鲁棒性。

### 2.2 预期功能安全过程保障

预期功能安全定义为不存在因设计不足、性能局限或人员误用引起的危害而导致不合理的风险<sup>[23]</sup>。对于搭载自动驾驶功能的智能网联汽车,由于场景的复杂性、性能局限导致的非失效风险增多,预期功能安全的重要性更加凸显。

为保障智能网联汽车达到一定的预期功能安全水平,需要对智能网联汽车,尤其是自动驾驶系统,提出预期功能安全保障要求。一是开发过程方面,提出规范设计、功能不足和触发条件的识别评估、功能改进等迭代设计要求;二是验证确认方面,要满足已知危害场景和未知危害场景验证确认要求;三是开发接口要求方面,要保障零部件符合对应的预期功能安全设计开发、验证、确认等规定。预期功能安全过程保障的核心是通过迭代开发、验证确认等方式,满足对已知和未知风险的合理控制,保障智能网联汽车安全。

### 2.3 网络安全和数据安全过程保障

网络安全是指通过采取必要措施,使汽车的电子电气系统、组件和功能免受网络威胁,确保车辆及其功能处于被保护的状态<sup>[24]</sup>。数据安全是指通过采取必要措施,确保数据处于有效保护和合法利用的状态,以及具备保障持续安全状态的能力<sup>[25]</sup>。

按照网络安全和数据安全管理要求,针对汽车产品概念、开发、生产、运维和报废5个阶段,汽车生产企业应有针对性地建立管理体系,规范产品的开发流程并指导产品开发。同时,企业应落实管理体系要求,保障产品满足相应的网络安全和数据安全管理要求。

### 2.4 模拟仿真测试

模拟仿真测试是指以实际采集、计算推理等建模的方式将搭载自动驾驶功能智能网联汽车及其应用场景进行数字化还原,建立尽可能接近真实世界的车辆和环境仿真模型,通过对车辆在仿真环境中的运行分析,评估计算ODC内的失效概率,以达到对智能网联汽车进行有效测试的目的。对于模拟仿真测试,应说明测试过程中所涉及的测试方法、通过条件等,并确保模拟仿真测试结果的可追溯性。

模拟仿真测试可用于评估智能网联汽车在多样化场景和复杂条件下的功能及性能,对全面评估智能网联汽车的安全性具有重要作用,与实车测试等共同构建形成完备的测试评估体系。模拟仿真测试场景应至少包括充分、合理的标称场景、危险场景和边缘场景<sup>[26]</sup>,以支撑验证智能网联汽车是否满足安全要求。同时,应使用高置信度的模拟仿真测试工具链,在仿真环境中评估智能网联汽车是否满足安全要求,尤其是针对危险场景及边缘场景下功能实现的安全验证。

### 2.5 封闭场地测试

封闭场地测试是指在封闭场地内开展的针对搭载自动驾驶功能智能网联汽车的实车测试,用于验证车辆在典型场景下的功能和性能。封闭场地测试具有交通参与者与目标物可控、场景可复现等特点,测试过程中可以确保测试环境、设备、方法及

流程的一致性,能够有效保证测试结果的准确性和可追溯性。

封闭场地测试应充分结合车辆自动驾驶功能及ODC,提出封闭场地测试的典型场景,以及对应的测试方法和通过条件,搭建封闭场地测试场景,有针对性地开展相应测试工作,同时验证模拟仿真测试结果。

### 2.6 实际道路测试

实际道路测试是指在公开道路上开展的针对搭载自动驾驶功能智能网联汽车的实车测试。实际道路测试应在车辆通过了充分的模拟仿真和封闭场地测试后开展,可以测试车辆在真实交通环境中的行为表现,同时可以用于验证模拟仿真和封闭场地测试结果。基于测试里程、测试场景要素等,验证车辆应对真实交通环境的能力。

实际道路测试应选取与ODC相匹配的道路开展测试。在实际道路测试过程中,被测车辆应在ODC下持续执行动态驾驶任务;应遵守道路交通通行规则;应对测试车辆进行监测和对测试过程进行记录,确保测试结果的可追溯性。

### 2.7 网络安全和数据安全测试

网络安全和数据安全测试,重点针对车辆已经实施的网络安全和数据安全技术或者风险处置措施,验证与车辆安全目标的匹配情况,主要用于确认产品网络安全和数据安全达到规定要求。

网络安全测试重点保障产品网络安全管理目标的落实,以整车为试验对象,从车辆的外部连接接口、通信信道、数据代码安全等层面开展。数据安全测试侧重于保障数据处理活动的安全性,主要针对车辆数据丢失、数据泄漏的威胁以及关键数据非法盗取、破坏、越权访问的威胁。

### 2.8 数据记录测试

搭载自动驾驶功能的智能网联汽车应具备事件数据等关键数据的记录功能,并能存储记录自动驾驶功能激活期间的车辆实时工作状态。存储记录的数据可用于自动驾驶相关的事故重建与分析、责任主体判定、功能优化升级等。

目前,智能网联汽车数据记录功能主要通过汽

车事件数据记录系统 (Events Data Recorder, EDR) 和自动驾驶数据记录系统 (Data Storage System for Autonomous Driving Vehicle, DSSAD) 实现。EDR测试应包含对碰撞事件、数据记录、记录功能、数据提取等的测试<sup>[27]</sup>, DSSAD测试应包含对记录元素种类、触发验证机制、数据存储机制、数据安全读取机制等的测试。

## 2.9 软件升级测试

软件升级是指将某版本的软件程序或配置参数更新到另一个版本的过程, 软件是指电子控制系统中由数字数据和指令组成的部分。智能网联汽车软件升级日益频繁, 部分软件会影响车辆的功能和性能, 进而带来车辆行驶安全风险。

为保障软件升级过程的安全性及可靠性, 汽车生产企业应针对软件升级建立管理体系, 提升车辆安全保障能力。此外, 还应针对车辆软件升级进行必要的测试验证工作, 至少包括升级包的真实性和完整性、车辆安全、升级失败处理等测试。

## 参考文献 (References)

- [1] Representatives of China, European Union, Japan and the United States of America. Proposal for Amendments to ECE/TRANS/WP. 29/2019/34 Framework Document on Automated/Autonomous Vehicles (Levels 3 and Higher) [Z]. United Nations: UN/WP.29, 2019.
- [2] National Highway Traffic Safety Administration. Preliminary Statement of Policy Concerning Automated Vehicles [Z]. USA, 2013.
- [3] National Highway Traffic Safety Administration. Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety [Z]. USA, 2016.
- [4] National Highway Traffic Safety Administration. Automated Driving Systems: A Vision for Safety 2.0 [Z]. USA, 2017.
- [5] National Highway Traffic Safety Administration. Preparing for the Future of Transportation: Automated Vehicles 3.0 [Z]. USA, 2018.
- [6] National Highway Traffic Safety Administration. Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 [Z]. USA, 2020.
- [7] National Highway Traffic Safety Administration. Automated Vehicles Comprehensive Plan [Z]. USA, 2021.
- [8] European Commission. Guidelines on the Exemption Procedure for the EU Approval of Automated Vehicles [Z]. 2019.
- [9] United Nations Economic Commission for Europe. Vienna Convention for Road Traffic [Z]. 2016.
- [10] German Ethics Commission on Automated and Connected Driving. The German Ethics Code for Automated and Connected Driving [Z]. Germany, 2017.
- [11] German Bundestag. Road Traffic Law [Z]. Germany: German Bundestag, 2017.
- [12] 日本警察厅. 自动驾驶汽车道路测试指南 [Z]. 日本: 2016.  
National Police Agency. Guidelines for Road Testing of Automated Driving Vehicle [Z]. Japan, 2016. (in Chinese)
- [13] 日本警察厅. 远程自动驾驶系统道路测试许可处理基准 [Z]. 日本, 2017.  
National Police Agency. Road Test Permission Processing Standard for Remote Automatic Driving System [Z]. Japan, 2017. (in Chinese)
- [14] 日本国土交通省. 自动驾驶汽车安全技术指南 [Z]. 日本: 2018.  
Ministry of Land, Infrastructure, Transport and Tourism.

## 3 结语

本文从第三方视角出发, 参考国内外测评方法研究, 结合我国智能网联汽车安全管理需要, 针对特定 ODC 下搭载自动驾驶功能的智能网联汽车面临的主要安全风险, 研究提出了一种安全测试与评估方法。该方法从基础测评和监测调整两个阶段, 分别基于车辆研发测试过程中对过程保障和测试要求的满足情况, 以及车辆实际使用过程中安全状态的监测情况, 有针对性地开展安全综合评估。此外, 还对功能安全、预期功能安全、网络安全和数据安全等过程保障方法及主要要求, 以及模拟仿真、封闭场地、实际道路、网络安全和数据安全、软件升级、数据记录等测试验证方法及主要要求, 分别进行了阐述。

本文对搭载自动驾驶功能的智能网联汽车安全测试与评估方法进行了初步探索, 致力于为智能网联汽车的安全管理提供方法参考。



- Guidelines for Safety Technology of Automated Driving Vehicle [Z]. Japan, 2018. (in Chinese)
- [15] 日本警察厅. 道路交通法修正案 [Z]. 日本, 2019. National Police Agency. Road Traffic Law (Amendment) [Z]. Japan, 2019. (in Chinese)
- [16] 工业和信息化部. 智能网联汽车道路测试管理规范(试行)[Z]. 北京, 2018. Ministry of Industry and Information Technology. Management Specification for Road Testing of Intelligent and Connected Vehicles (for Trial Implementation) [Z]. Beijing, 2018. (in Chinese)
- [17] 工业和信息化部. 智能网联汽车道路测试与示范应用管理规范(试行)[Z]. 北京, 2021. Ministry of Industry and Information Technology. Management Specification for Road Testing and Demonstration Application of Intelligent and Connected Vehicles (for Trial Implementation)[Z]. Beijing, 2021. (in Chinese)
- [18] Working Party on Automated/Autonomous and Connected Vehicles. Proposal for a second iteration of the New Assessment/Test Method for Automated Driving - Master Document [Informal Document] [Z]. United Nations, 2022.
- [19] 工业和信息化部. 智能网联汽车生产企业及产品准入管理指南(试行)(征求意见稿)[Z]. 北京, 2021. Ministry of Industry and Information Technology. Guidelines for the Manufacturers and Products Access Management of Intelligent and Connected Vehicle (for Trial Implementation) (Draft for Comments) [Z]. Beijing, 2021. (in Chinese)
- [20] 工业和信息化部. 关于加强智能网联汽车生产企业及产品准入管理的意见 [Z]. 北京, 2021. Ministry of Industry and Information Technology. Opinions on Strengthening the Manufacturers and Products Access Management of Intelligent and Connected Vehicle [Z]. Beijing, 2021. (in Chinese)
- [21] GB/T 40429—2021. 汽车驾驶自动化分级 [S]. 北京: 全国汽车标准化技术委员会, 2021. GB/T 40429—2021. Taxonomy of Driving Automation for Vehicles [S]. Beijing: National Technical Committee of Auto Standardization, 2021. (in Chinese)
- [22] ISO 26262: 2018. Road Vehicles—Functional Safety [S]. Switzerland: International Organization for Standardization, 2018.
- [23] ISO/FDIS 21448: 2021. Road Vehicles—Safety of the Intended Functionality [S]. Switzerland: International Organization for Standardization, 2021.
- [24] ISO/SAE 21434: 2021. Road Vehicles—Cybersecurity Engineering [S]. Switzerland/USA: International Organization for Standardization/Society of Automotive Engineers, 2021.
- [25] 全国人民代表大会常务委员会. 中华人民共和国数据安全法 [Z]. 北京, 2021. The National People's Congress of the People's Republic of China. Data Security Law of the People's Republic of China. China [Z]. Beijing, 2021.
- [26] European Commission. Annexes to the Commission Implementing Regulation 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 Motor Vehicles with Regard to their Automated Driving System (ADS), Version 7.2 [Z]. 2021.
- [27] GB 39732—2020. 汽车事件数据记录系统 [S]. 北京: 全国汽车标准化技术委员会, 2020. GB 39732—2020. Vehicle Event Data Recorder System [S]. Beijing: National Technical Committee of Auto Standardization, 2020. (in Chinese)

## 作者简介



刘法旺 (1981-), 男, 河南信阳人, 博士, 高级工程师, 主要研究方向为智能网联汽车安全。

Tel: 010-68209373

E-mail: liufawang@eidc.org.cn

## 通信作者



徐晓庆 (1990-), 男, 山东临沂人, 博士, 高级技术专家, 主要研究方向为智能网联汽车安全测试与评估方法。

Tel: 18518551871

E-mail: xuxiaoqing@caeri.com.cn