自动驾驶系统功能安全与预期功能安全研究

刘法旺，李艳文
（工业和信息化部装备工业发展中心，北京 100846）

摘　要： 安全是汽车产业持续健康发展的核心要素。自动驾驶系统依靠大数据、人工智能、计算机视觉、高精地图、高精定位、协同计算等技术，支撑实现环境感知、规划决策和控制执行功能，其功能安全和预期功能安全直接影响整车安全性。针对自动驾驶系统的功能安全和预期功能安全开展研究，对比二者之间的异同。进而，重点对功能安全和预期功能安全的评估要点进行分析，从流程管理、产品开发过程、系统集成验证确认三个方面提出评估要求。最后，从系统工程的角度分析了自动驾驶系统安全面临的主要挑战，并提出研究思考。

关键词： 智能网联汽车；自动驾驶系统；功能安全；预期功能安全；汽车安全完整性等级

中图分类号： U471.2　**文献标识码：** A　**文章编号：** 2095-8412 (2021) 06-062-07

工业技术创新 URL: http://gyjs.cbpt.cnki.net　DOI: 10.14103/j.issn.2095-8412.2021.06.011

引言

安全是发展的前提，发展是安全的保障。当前，全球新一轮科技革命和产业变革正在蓬勃发展，作为产业变革创新的重要载体，智能网联汽车正处于技术快速演进、产业加速布局的商业化前期阶段，推动着汽车产业形态、交通出行模式、能源消费结构和社会运行方式的深刻变化。与此同时，智能网联汽车的系统结构更加复杂，大量应用了大数据、人工智能、协同计算等先进技术，安全问题更加突出。尤其是对于具有自动驾驶功能的智能网联汽车而言，如何采用系统工程的方法[1-2]，系统梳理安全风险、采取减缓措施、开展验证和评价，保障系统达到一定的安全水平，值得深入研究。

为保障自动驾驶安全，联合国世界车辆法规协调论坛审议通过《自动驾驶汽车框架文件》，旨在针对具有L3及更高级别自动驾驶功能的智能网联汽车，确立安全性相关原则，对系统安全、失效保护响应、事件数据记录和自动驾驶数据存储等13项内容进行明确和阐述[3]。此外，欧盟发布《自动驾驶车辆豁免程序指南》[4]、日本发布《自动驾驶安全技术指南》[5]、新加坡发布《自动驾驶技术参考TR68》[6]，均提出自动驾驶安全原则要求。

标准层面，国际标准化组织道路车辆技术委员会（ISO/TC 22）发布ISO 26262-2018《道路车辆 功能安全》，积极推动ISO 21448预期功能安全标准的制定。法规层面，联合国欧洲经济委员会（UNECE）已在R 13制动系统、R 79转向系统、R 131自动紧急制动系统中引入功能安全要求，并在R 157自动车道保持系统中提出功能安全和预期功能安全要求。

自动驾驶系统是指能够持续执行全部动态驾驶任务的硬件和软件所共同组成的系统，是支撑实现车辆自动驾驶的关键，其性能直接影响智能网联汽车自动化和智能化水平，对车辆的安全性、经济性、可用性等具有重要的价值。

本文从分析自动驾驶系统的安全影响因素入手，聚焦对自动驾驶系统的功能安全和预期功能安全进行研究，对比分析二者之间的异同，梳理其验证评估的主要要求，最后总结目前面临的挑战并提出研究思考。

1 自动驾驶系统安全影响因素分析

自动驾驶系统主要用于支撑实现环境感知、规划决策和控制执行等功能[7]。环境感知部分主要获取并处理环境信息，完成对车辆周围环境的感知识别，常见的感知设备包括摄像头、激光雷达、毫米波雷达，以及卫星导航定位系统、惯性导航定位系统等。规划决策部分主要实现两个功能，一是认知理解，根据环境感知收集的信息，对车辆自身实现精准定位以及对周围环境实现准确研判；二是对下一步行动的准确判断和规划，选择合理的路径达到

目的地。控制执行部分在系统做出规划决策以后，替代驾驶员对车辆进行控制，其关键技术包括纵向控制、横向控制等。

根据《自动驾驶汽车框架文件》[3]要求，自动驾驶系统应能自动探测系统失效以及是否满足设计运行条件，并能采取最小风险策略以达到最小风险状态[8-9]。在自动驾驶模式下，车辆应能够遵守道路交通安全法律、法规规定，保障道路交通安全。相比较人工驾驶水平，自动驾驶应具备等同或更高等级的安全性[10-11]。

自动驾驶系统通过高效集成的软硬件，支持实现全部动态驾驶任务。在此背景下，一是传感器、执行器、计算平台、软件、通信等可能会发生系统性失效和随机硬件失效，造成整车危害，即出现功能安全问题；二是由于场景感知、决策算法、人工智能等实现的不充分性、不确定性带来自动驾驶的功能局限，造成非失效风险，影响到整车行驶的安全性，即预期功能安全问题。功能安全和预期功能安全是影响自动驾驶系统行驶安全的关键，需要系统分析可能面临的各类风险，并采取相应的措施将风险降低到可接受的范围。

2 自动驾驶系统功能安全和预期功能安全对比分析

通过对比研究功能安全标准ISO 26262[12]和预期功能安全标准ISO 21448[13]可以发现，二者既有相似之处，但又各有侧重，需要协同推进以保障自动驾驶系统的安全性。

2.1 概念辨析

道路车辆功能安全是指不存在由电子电气系统的功能异常表现引起的危害，而导致不合理的风险[14]。预期功能安全是指不存在由预期功能或其实现的不足引起的危害而导致不合理的风险。在自动驾驶应用场景下，对功能安全和预期功能安全要求也在发生变化[15]。

自动驾驶强化了对系统功能安全的要求。一是在自动驾驶法规层面，提出了更严格的功能安全要求。联合国自动驾驶框架法规文件提出了系统安全、失效保护响应、系统安全验证等原则要求，明确了L3级及以上智能网联汽车的功能安全设计开发和测试验证要求。在针对L3级自动驾驶功能的R 157自动车道保持系统法规中，进一步提出了对过程文档和测试的要求；相比较传统的制动、转向法规，增加了安全管理流程、模拟仿真测试和对评审人员能力的要求。二是在自动驾驶技术层面，提出了更高的功能安全要求。自动驾驶功能日趋复杂，更加依赖电子电气（E/E）系统实现感知、决策和控制，对车辆安全技术的正确性和完整性要求进一步提高。开发过程中，由于自动驾驶系统具有目标和事件探测与响应、最小风险策略、介入请求、人机交互等功能，需要提出更为系统全面的安全目标和功能安全概念需求[16-17]，系统、硬件和软件设计面临更多冗余、异构、监控的要求。

目前，由于性能局限导致的非失效风险增多，对自动驾驶系统预期功能安全提出了新要求。毫米波雷达、激光雷达、摄像头等传感器构成了自动驾驶的感知输入，受光照、恶劣天气等影响，传感器本身没有发生失效，但性能可能会降低，输入出现偏差，导致自动驾驶决策和执行出现问题而引发车辆危害行为，这种由于自动驾驶功能不足导致的非失效风险逐渐增多[18]。传统驾驶模式下，大部分的事故源于人的因素；自动驾驶模式下，自动驾驶系统承担部分或全部动态驾驶任务，产品设计无法预估到所有场景条件，驾驶场景成为影响安全的重要因素，未知的不安全场景对自动驾驶系统提出了挑战。此外，机器学习存在不确定性，也可能造成设计不足，导致非失效风险，危害到自动驾驶的安全性。

2.2 主要异同

功能安全和预期功能安全在侧重点和要求内容上存在较大差别。功能安全主要针对系统性失效和随机硬件失效引起的危害，重点关注的是功能的失效。预期功能安全主要针对因系统功能或其实现的不足导致的危害，而非故障，是对功能安全的有效补充，主要解决因自身设计不足或性能局限在遇到一定的触发条件（如环境干扰或人员误用）时导致的整车行为危害。

功能安全和预期功能安全均采用V模型开发流程[19]，如图1所示。功能安全在设计阶段包含相关项定义、危害分析与风险评估、功能安全概念、技术概念、软硬件开发，验证确认阶段包含软硬件测试、系统集成验证测试、车辆确认测试。预期功能安全在设计阶段包含规范和设计、危害识别和风险评估、触发事件识别和评估、功能改进，验证确认阶段包含评估已知场景和评估未知场景。

相比较功能安全开发流程，预期功能安全的开发流程更具迭代性。在整体符合V模型流程的基础上，预期功能安全开发流程中各阶段条款要

求又可以表述为图2的迭代开发过程。流程从规范和设计开始（第5条）。对预期功能可能存在的危害行为进行危害识别和风险评估（第6条），以识别潜在危害事件。如果证明这些潜在的危害事件不会导致伤害，则无需改进，并且可以认为预期功能没有不合理的风险。如果证明有可能造成伤害，则对可能触发的危害事件（例如在特定环境条件下对某些对象的错误识别或驾驶员误用）进行分析（第7条）。第6条和第7条阐述了预期功能安全的不同方面。第6条不考虑可能的功能危害预期行为的原因，只考虑其造成的安全后果，重点是评估可能由危害预期行为所引起的危害事件，并明确所要达到的验证和确认目标。第7条阐述了潜在危害行为的原因分析。这些风险在第8条中得到了降低，在第9条、第10条和第11条中得到了验证和确认。最后，考虑验证和确认的结果，评估残余风险是否可接受（第12条），进而判定是否开展运营阶段的活动（第13条）。如果确定风险是不可接受的，则需要进一步改善功能或限制使用案例（第8条）。

3 自动驾驶系统功能安全评估

与传统的道路车辆功能安全相比，人机共驾模式对危害分析和风险评估中的可控性度量提出了新要求。相比较传统道路车辆关注的失效安全系统，失效可运行的安全机制更多在自动驾驶模式下应用。高复杂、高耦合下的自动驾驶系统，安全需求分解、软硬件度量、安全一致性评估等难度显著增加。网络安全与自动驾驶功能安全相互交叉，增加了系统分析的范围。场景的复杂性和功能的多样性，增加了功能安全验证确认的工作量，提高了对自动驾驶残余风险可接受水平的判定难度[20]。

总体来看，自动驾驶系统的功能安全验证评价要求主要包括：

（1）对功能安全流程管理进行评估。规范的功能安全流程管理体系可以避免或减少系统性风险，提高开发效率。功能安全流程管理评估的对象主要包括管理、生产运行和支持过程。功能安全管理要满足整体功能安全管理、概念阶段和系统开发过程的安全管理、生产发布后的安全管理等要求。生产运行要满足响应的功能安全要求，符合生产过程能力评估、控制措施、现场观察说明等规定。支持过程要满足变更管理、配置管理、文档管理、分布式开发接口、安全要求的定义和管理、软件组件鉴定、硬件要素评估等要求。

（2）对产品功能安全开发过程进行评估。主要侧重产品安全，评估对象主要包括概念、系统和软硬件阶段的开发活动。概念阶段的核心要求是危害分析与风险评估、功能安全概念设计；分析整车级危害，确认危害事件的汽车安全完整性

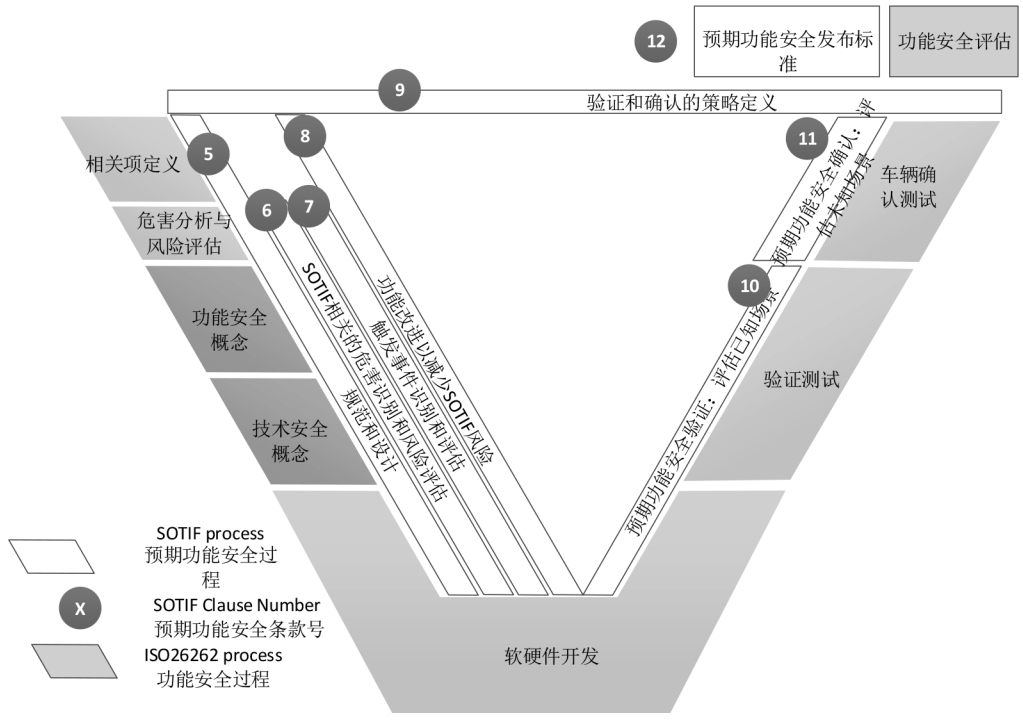

图1 功能安全和预期功能安全开发流程

等级（ASIL），然后通过危害分析和风险评估确定相关项的安全目标，将ASIL等级分配给相应的安全目标，设计功能安全要求，并进行分配。系统阶段的核心要求是进行系统架构设计及分析，提出技术安全要求，分配给软硬件接口。硬件阶段的核心要求是硬件安全要求定义、硬件功能安全指标评估，进行硬件安全设计与实现。软件阶段的核心要求是软件安全要求定义和软件架构设计，进行软件安全设计与实现。

（3）对功能安全系统集成验证确认进行评估。主要侧重对集成验证和确认的评估。集成验证的对象是集成后的自动驾驶系统，目的是提供证据证明系统各个要素正确交互、符合技术和功能安全要求，并为没有可能导致违背安全目标的非预期行为提供足够的置信度水平；测试内容主要包含自动驾驶系统的黑盒测试、仿真测试、边界测试、故障注入、耐久测试等。整车测试的对象是集成了自动驾驶系统的整车，目的是证明集成后整车系统故障造成的非预期风险足够低。确认主要是提供符合整车层面安全目标以及功能安全目标完整性的证据等；是为了证明达成了安全目标，实现了功能安全，并确认自动驾驶系统满足预期的用途，主要基于测试和检查等方式。

4 自动驾驶系统预期功能安全评估

综合来看，自动驾驶系统的预期功能安全验证评价内容主要包括：

（1）对预期功能安全流程管理进行评估。确认满足预期功能安全开发接口管理要求，符合预期功能安全管理职责和角色定义、供应商计划管理等规定。确认预期功能安全开发步骤满足设计定义、危害识别、功能不足识别、功能改进、验证及确认、安全发布、运行维护等要求。

（2）对产品预期功能安全开发过程进行评估。对于自动驾驶功能和系统的定义，评估是否提供了足以启动预期功能安全相关活动信息的证据，并在每次迭代预期功能安全相关活动后进行更新。评估预期功能安全后续开发过程是否满足相关要求。其中，在整车层面进行预期功能安全危害分析与风险评估，可通过应用ISO 26262-3中指定的方法来实现；不同之处在于，在分析与预期功能安全相关的危害时，没有针对危害事件确定ASIL等级的过程。采用适当的分析方法识别功能不足和触发条件，其中通过识别环境条件和可预见的误用可以确定可能触发系统潜在危害行为的系统边界。通过已识别措施迭代更新规范和设计，避免、降低或减轻预期功能安全相关风险；改进措施主要有系统改进、功能限制、考虑接管权限、减少误用等。

（3）对预期功能安全验证确认进行评估。主要包括三个方面。一是验证确认策略的定义要满足相关要求，要考虑对已知和未知危害场景的评估、产生证据的流程、必要的证据等。二是确认实施的已知危害场景评估符合相关要求。其中，传感器验证的目的是证明传感器在预期使用下的功能性能、时序、精度及鲁棒性的正确性；决策算法验证的目的是在需要时，其可作出反应以及避免非预期行为；执行器验证的目的是验证其在决策算法中预期使用和可合理预见误用的安全表

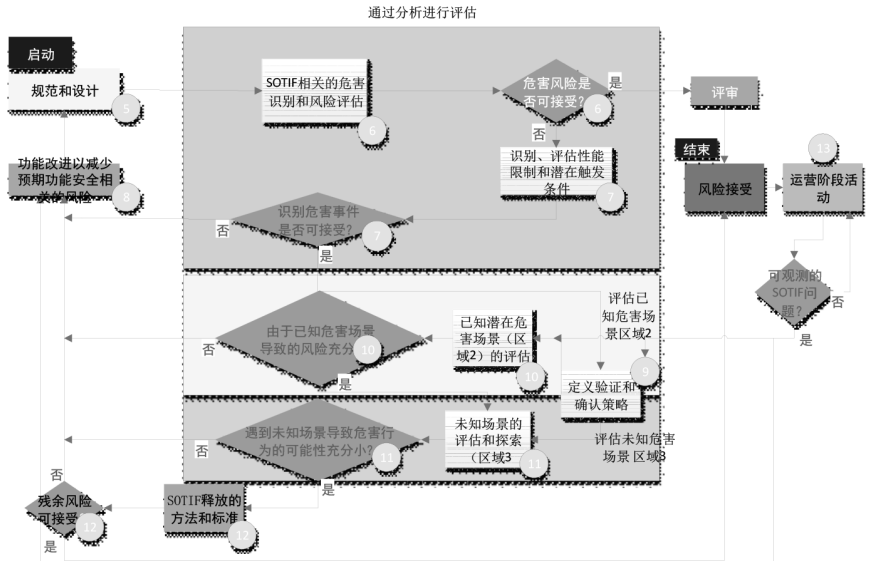

图2 预期功能安全迭代开发过程

现。三是确认实施的未知危害场景评估符合相关技术要求。其中，未知危害场景评估用到的方法主要包括信噪比衰减的鲁棒性确认、随机输入测试、可合理预见的误用测试等[21]。

5 安全保障面临的挑战

基于上述研究，对搭载L3级及以上自动驾驶功能的智能网联汽车，驾驶权部分或全部发生转移，功能安全和预期功能安全风险更加突出，测试、验证、评价自动驾驶的安全性更加困难。另一方面，随着V2X技术的普及应用，周边车辆、基础设施等协同工作，甚至参与感知、决策和控制，网络安全风险也更加凸显。同时，智能网汽车可以采集车辆数据、用户数据、位置数据等信息，并可能将其发送到云端，又会带来智能网联汽车数据安全、个人信息保护问题[22]。

随着汽车智能化、网联化发展，汽车、电子信息、通信等领域不断融合，自动驾驶安全的内涵和外延正在发生变化，功能安全、预期功能安全、网络安全、数据安全等问题相互交织。其中，网络安全是指汽车的电子电气系统、组件和功能被保护，使其资产不受威胁的状态。数据安全是指通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力。

目前有相关研究在开展[23-24]，然而从系统工程的角度来看，如何保障智能网联汽车整车，尤其是自动驾驶系统的安全，还面临以下两个方面的主要挑战：

一是缺乏系统的顶层设计。车辆功能安全、预期功能安全、网络安全、数据安全等问题相互交叠，各领域安全理论进一步交叉，自动驾驶系统的安全问题更加复杂，需要从系统工程角度出发，加强顶层设计，保障安全解决方案的系统性、完整性和实用性。

二是缺少经验和数据的积累。ISO26262 功能安全和ISO 21448 预期功能安全均偏重方法论，在实际应用中面临如何量化以切实有效保障安全的难题。为了确保自动驾驶系统的安全性，单纯依靠提高测试累积里程无法满足要求，亟需建立科学合理的安全量化接受准则。

6 结论和展望

本文结合国际上自动驾驶相关法规、标准等进展，对自动驾驶系统安全的影响因素进行了分析，聚焦研究自动驾驶系统的功能安全和预期功能安全。功能安全侧重关注功能失效，预期功能安全侧重关注功能实现不足和性能局限；功能安全和预期功能安全均符合V模型开发流程，预期功能安全开发过程更具迭代性。在此基础上，对自动驾驶系统功能安全和预期功能安全的评估要点进行研究，从流程管理、产品开发过程、系统集成验证确认三个方面梳理了评估的主要要求。最后，对功能安全、预期功能安全、网络安全、数据安全进行了整体思考，提出整车尤其是自动驾驶系统的安全面临缺乏顶层设计、缺少经验和数据积累两大挑战。

后续拟采用系统工程的方法，加强对功能安全、预期功能安全、网络安全、数据安全等问题的研究梳理，提出系统性验证评估体系，并推动试点加强经验和数据的积累，保障安全和发展的平衡，促进产业健康可持续发展。

参考文献

[1] Hommes V E, Qi D. Assessment of Safety Standards for Automotive Electronic Control Systems [S/OL]. http://ntl.bts.gov/lib/59000/59300/59359/812285_ElectronicsReliabilityReport.pdf. 2016.

[2] ISO/TC 22. ISO/TR 4804 Road Vehicles—Safety and security for automated driving systems—Design, verification and validation methods [S/OL]. https://www.iso.org/obp/ui/#iso:std:iso:tr:4804:ed-1:v1:en. 2020-12.

[3] UNECE. Framework document on automated/autonomous vehicles (level 3 and higher): ECE/TRANS.WP.29/2019/34 [S/OL]. 2019-06-25.

[4] EU. Guidelines on the exemption procedure for the the EU approval of automated vehicles [EB/OL]. https://ec.europa.eu/newsroom/growth/item-detail.cfm?item_id=648900. 2019-4-9.

[5] MLIT, Japan. Guideline regarding Safety Technology for Automated Vehicles in Japan[R/OL]. https://unece.org/DAM/trans/doc/2018/wp29grva/GRVA-01-34.pdf. 2018-09.

[6] Singapore Standards Council. TR68: Autonomous Vehicles Technical Reference [EB/OL]. 2019-1-8.

[7] 余贵珍, 周彬, 王阳, 等. 自动驾驶系统设计及应用[M]. 北京: 清华大学出版社, 2019: 1-10.

[8] Joshi A, Whalen M, Heimdahl M. Model-based safety analysis final report [R]. 2006.

[9] Kulas R A, Rieland H, Pechauer J. A System Safety Perspective into Chevy Bolt's One Pedal Driving[C]// WCX SAE World Congress Experience. 2019.

[10] ISO/TC 22. Road Vehicles—Safety and security for automated driving systems—Design, verification and validation methods: ISO/TR 4804:2020 [S/OL]. https://www.iso.org/obp/ui/#iso:std:iso:tr:4804:ed-1:v1:en. 2020-12.

[11] UNECE. Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System: ECE/TRANS/WP.29/2020/81[S/OL]. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grsg/GRSG-118-05e.pdf. 2020-07-17.

[12] ISO/TC 22/SC 32. Road vehicles—Functional safety: ISO 26262-2018 [S/OL]. https://www.iso.org/standard/68383.html. 2018-12.

[13] ISO/TC 22/SC 32. Road vehicles—Safety of the Intended Functionality: ISO DIS 21448 [S/OL]. https://www.iso.org/standard/70939.html. 2020-01.

[14] 道路车辆功能安全 第一部分：术语：GB/T 34590.1-2017[S].

[15] Ballingall S, Sarvi M, Sweatman P. Safety Assurance Concepts for Automated Driving Systems[J]. SAE International Journal of Advances and Current Practices in Mobility, 2020, 2: 1528-1537.

[16] Salay R, Queiroz R, Czarnecki K. An Analysis of ISO 26262: Using Machine Learning Safely in Automotive Software[J]. arXiv:1709.02435v1. 2017.

[17] Cassel A, Bergenhem C, Christensen O M, et al. On perception safety requirements and multi sensor systems for automated driving systems[J]. SAE International Journal of Advances and Current Practices in Mobility, 2020, 2: 3035-3043.

[18] Lafuente I, Tobar M, Luján C, et al. Challenges in the Regulatory Framework of Automated Driving[R]. SAE Technical Paper, 2019.

[19] Macher G, Schmittner C, Dobaj J, et al. An integrated view on automotive spice, functional safety and cyber-security[J]. SAE Technical Papers, 2020 (2020-01-0145).

[20] Wishart J, Como S, Elli M, et al. Driving safety performance assessment metrics for ads-equipped vehicles[J]. SAE International Journal of Advances and Current Practices in Mobility, 2020, 2: 2881-2899.

[21] Feng S, Feng Y, Yan X, et al. Safety assessment of highly automated driving systems in test tracks: A new framework[J]. Accident Analysis & Prevention, 2020, 144: 105664.

[22] 刘法旺, 李艳文, 李国俊, 等. 欧美日智能网联汽车准入管理研究及启示[J]. 汽车文摘, 2021, (5): 1-7.

[23] 毛向阳, 尚世亮, 崔海峰. 自动驾驶汽车安全影响因素分析与应对措施研究[J]. 上海汽车, 2018(1): 33-37.

[24] Riccardo Mariani. An Overview of Autonomous Vehicles Safety[C]// 2018 IEEE International Reliability Physics Symposium (IRPS).

作者简介：

刘法旺（1981—），男，河南商城人，博士，高级工程师。主要研究方向：智能网联汽车安全。
E-mail: liufawang@eidc.org.cn

李艳文（1978—），通信作者，男，山东临沂人，博士，高级工程师。主要研究方向：智能网联汽车功能安全和预期功能安全。
E-mail: liyanwen@eidc.org.cn

（收稿日期：2021-05-11）

Research on Functional Safety and Safety of the Intended Functionality for Automated Driving System

LIU Fa-wang, LI Yan-wen
(*Ministry of Industry and Information Technology Equipment Industy Development Center, Beijing 100846, China*)

Abstract: Safety is the core element of sustainable and healthy development of the automobile industry. Automated driving system relies on technologies such as big data, artificial intelligence, computer vision, high-precision map, high-precision positioning, collaboration computing, etc. to support the realization of environment perception, planning and control. Its Functional Safety and Safety of the Intended Functionality (SOTIF) directly affect the safety performance of automated driving vehicle. Firstly, the similarities and differences between Functional Safety and SOTIF of the automated driving system are compared. Then, the key points of assessment for Functional Safety and SOTIF are analyzed, and the assessment requirements are put forward from three aspects, including process management, product development process and system integration verification and validation. Finally, from the perspective of system engineering, the main challenges faced by the safety and cybersecurity of automated driving system are analyzed, and the research thinking is put forward.

Key words: Intelligent and Connected Vehicle (ICV); Automated Driving System; Functional Safety; Safety of the Intended Functionality (SOTIF); Automotive Safety Integration Level (ASIL)