



智能网联汽车预期功能安全工作组  
CAICV SOTIF Technical Alliance

# 智能网联汽车预期功能安全 前沿技术研究报告

发布版

2020年12月



版本维护：

版本	修改内容	作者	时间	备注
V1.0	研究内容提纲	清华大学、国汽(北京)智能网联汽车研究院有限公司（国家智能网联汽车创新中心）	2020.05.06	待讨论
V2.0	根据组长单位意见修订	清华大学	2020.06.04	待讨论
V3.0	根据各成员单位意见修订	清华大学、国汽(北京)智能网联汽车研究院有限公司（国家智能网联汽车创新中心）	2020.06.19	待讨论
V4.0	第一次统稿	重庆长安汽车股份有限公司、东风汽车集团有限公司、北京汽车股份有限公司、清华大学苏州汽车研究院、北京航空航天大学	2020.10.10	
V5.0	第二次统稿	清华大学、公安部交通管理科学研究所、中国信息通信研究院、浙江吉利汽车研究院有限公司、泛亚汽车技术中心有限公司、同济大学、电子科技大学、重庆长安汽车股份有限公司、重庆大学、北京理工大学、清华大学苏州汽车研究院、东风汽车集团有限公司、中汽研汽车检验中心（天津）有限公司、北京汽车股份有限公司、上海机动车检测认证技术研究中心有限公司、北京航空航天大学、吉林大学	2020.11.18	
V6.0	内容整体梳理	清华大学、国汽(北京)智能网联汽车研究院有限公司（国家智能网联汽车创新中心）	2020.12.02	



## 目录

第1章 前言	1
1.1 预期功能安全前沿技术研究报告背景	1
1.2 预期功能安全前沿技术研究报告内容	1
1.3 预期功能安全前沿技术研究报告使用范围	1
第2章 国内外智能网联汽车安全相关政策/法规	2
2.1 美国自动驾驶汽车相关法规政策	2
2.1.1 概述	2
2.1.2 特点分析	3
2.1.3 主要内容	4
2.2 日本自动驾驶汽车相关法规政策	9
2.2.1 概述	9
2.2.2 特点分析	10
2.2.3 主要内容	11
2.3 欧洲自动驾驶汽车相关法规政策	20
2.3.1 概述	20
2.3.2 特点分析	21
2.3.3 主要内容	21
2.4 我国自动驾驶汽车相关法规政策	31
第3章 国内外智能网联汽车预期功能安全相关标准	33
3.1 国外智能网联汽车预期功能安全相关标准	33
3.2 国内智能网联汽车预期功能安全相关标准	37
3.3 智能网联汽车预期功能安全标准的发展现状及趋势	39
第4章 国内外智能网联汽车预期功能安全相关技术	40
4.1 感知面临的预期功能安全挑战与发展方向	40
4.1.1 感知系统面临的预期功能安全挑战	40
4.1.2 感知算法的预期功能安全相关研究	42
4.1.3 感知系统未来发展方向	44
4.2 预测相关的预期功能安全技术	44
4.3 决策相关的预期功能安全技术	46



4.4	控制相关的预期功能安全技术.....	48
4.5	人机交互技术现有局限与分析方法.....	49
4.5.1	HMI 交互技术及其局限.....	49
4.5.2	人机交互开发过程.....	51
4.5.3	人机交互分析方法.....	52
4.6	预期功能安全系统分析方法.....	55
4.6.1	故障树分析 (FTA) .....	56
4.6.2	失效模式与影响分析 (FMEA) .....	56
4.6.3	危险与可操作性分析 (HAZOP) .....	57
4.6.4	系统理论过程分析 (STPA) .....	58
4.6.5	不同安全分析方法对比.....	58
第5章	国内外智能网联汽车预期功能安全相关专利.....	65
5.1	国外智能网联汽车预期功能安全相关专利.....	65
5.2	国内智能网联汽车预期功能安全相关专利.....	66
5.3	智能网联汽车预期功能安全专利总结.....	68
第6章	国内外智能网联汽车场景库研究现状.....	71
6.1	国外智能网联汽车场景库研究现状.....	71
6.1.1	PEGASUS.....	71
6.1.2	NHTSA.....	71
6.1.3	Waymo.....	71
6.1.4	福特数据集.....	72
6.1.5	KITTI 数据集.....	72
6.1.6	NuScenes 数据集.....	72
6.1.7	Argoverse 数据集.....	73
6.1.8	Lyft 自动驾驶汽车数据集.....	73
6.1.9	H3D - HRI-US 数据集.....	74
6.1.10	CamVid 数据集.....	75
6.1.11	BDD100K 数据集.....	75
6.1.12	Cityscapes 数据集.....	76
6.1.13	RobotCar 数据集.....	77
6.1.14	rFpro.....	77



6.1.15	Mapillary Vistas 数据集.....	78
6.1.16	Caltech 数据集.....	78
6.1.17	Daimler Urban Segmentation 数据集.....	79
6.2	国内智能网联汽车场景库研究现状.....	79
6.2.1	智能网联汽车驾驶场景数据库.....	79
6.2.2	中国交通事故深入研究 (CIDAS) 数据库.....	80
6.2.3	中国典型驾驶场景库 i-Scenario.....	80
6.2.4	中国智能驾驶全息场景库建设 (“昆仑计划”) .....	80
6.2.5	百度.....	81
6.2.6	自动驾驶场景库“镜”.....	81
6.2.7	公安部交通研究所.....	81
第 7 章	国内外智能网联汽车功能测试评价体系.....	83
7.1	国外智能网联汽车功能测试与评价现状.....	83
7.1.1	虚拟仿真测试.....	83
7.1.2	场地测试.....	85
7.1.3	公开道路测试准入条件与道路测试.....	86
7.1.4	评价体系与可接受风险的测试指标.....	90
7.2	国内智能网联汽车功能测试与评价现状.....	93
7.2.1	虚拟仿真测试.....	93
7.2.2	场地测试.....	95
7.2.3	公开道路测试准入条件现状.....	98
7.2.4	评价体系与可接受风险的测试指标.....	102
7.3	智能网联汽车测试评价发展趋势分析.....	105
7.3.1	虚拟仿真测试发展趋势.....	105
7.3.2	智能网联汽车试验场建设建议.....	106
7.3.3	智能网联汽车测试评价的挑战和目标.....	107
第 8 章	典型 ADAS 系统的 SOTIF 研究现状.....	109
8.1	车道保持系统的预期功能安全研究.....	109
8.2	自动刹车辅助系统的预期功能安全研究.....	109
8.3	自适应巡航系统的预期功能安全研究.....	111
8.4	交通拥堵辅助系统的预期功能安全研究.....	111

8.5 自主泊车系统的预期功能安全研究.....	112
8.5.1 AVP 系统的设计运行域.....	112
8.5.2 AVP 的 SOTIF 相关危害.....	113
8.5.3 识别和评估 AVP 潜在的功能不足和触发条件.....	113
8.5.4 AVP 功能修改以减少 SOTIF 相关风险.....	113
附表 A 预期功能安全相关专利汇总.....	115
附表 B 现有材料提供单位.....	119



## 名词表

名词	缩写	含义
Safety Of The Intended Functionality	SOTIF	预期功能安全
Operation Design Domain	ODD	运行设计域
Dynamic Driving Task	DDT	动态驾驶任务
Edge case		边缘场景
Advanced Driver Assistance System	ADAS	先进驾驶辅助系统
Human Machine Interface	HMI	人机交互
Verification & Validation	V&V	测试与评价
ISO 26262: Road Vehicles - Functional Safety	ISO 26262	道路车辆功能安全-ISO26262 标准
ISO/PAS 21448:2019 Road vehicles - Safety of the Intended Functionality	ISO/PAS 21448	道路车辆预期功能安全-ISO/PAS 21448 标准草案
Federal Motor Vehicle Safety Standards	FMVSS	联邦机动车安全标准（美国）
Convolutional Neural Networks	CNN	卷积神经网络
Fault Detection and Isolation	FDI	故障检测与隔离
Fault Detection and Diagnosis	FDD	故障检测与诊断
Hardware-in-the-Loop	HIL	硬件在环
Adaptive Cruise Control	ACC	自适应巡航系统
National Highway Traffic Safety Administration	NHTSA	美国国家公路交通安全管理局
Robot Operating System	ROS	机器人操作系统
Association for Standardization of Automation and Measuring Systems	ASAM	德国自动化及测量系统标准协会
Cooperative Adaptive Cruise Control	CACC	协同自适应巡航控制
Model-in-the-Loop	MIL	模型在环仿真
Software-in-the-Loop	SIL	软件在环仿真
Intelligent Vehicle Integrated Systems Test Area	i-VISTA	智能汽车集成系统试验区
Intelligent Connected Vehicle Test	ICVT	智能网联汽车用户评价体系
Advanced Driver Assistance System	ADAS	先进驾驶辅助系统
Lane Keeping Assist System	LKA	车道保持系统
Systems Theoretic Process	STPA	系统理论过程分析



Analysis		
Automatic Emergency Brake	AEB	自动刹车辅助系统
Extended-Autonomous Emergency Braking	E-AEB	扩展自动紧急制动
Traffic Jam Assist	TJA	交通拥堵辅助系统
Situational Awareness	SA	情景意识
Automated Valet Parking	AVP	自主代客泊车系统





## 第1章 前言

### 1.1 预期功能安全前沿技术研究报告背景

2020年2月底，国家发展和改革委员会等十一部门联合印发《智能汽车创新发展战略》，明确提出了建设中国标准智能汽车和实现智能汽车强国的战略目标。随着自动驾驶技术的发展与普及，其安全性越来越受到大众的关注。2019年7月，德国宝马联合11家企业（宝马、奥迪、戴姆勒、大众、菲亚特—克斯莱勒、英特尔、英飞凌、安波福、大陆、HERE、百度），共同编写《自动驾驶安全第一白皮书》，旨在促进自动驾驶汽车安全性研发。随自动驾驶系统功能架构趋于完善，国际标准ISO 26262覆盖的故障性风险造成的功能安全问题分析已无法满足高度复杂系统的安全性分析要求。在系统不发生故障的情况下引起的安全风险愈发受到重视，ISO/PAS 21448将此类问题归结为预期功能安全(Safety Of The Intended Functionality, SOTIF)，并给出了其详细定义。标准草案指出进行预期功能安全活动的目标是确保不存在由于影响系统特定行为的性能局限或可合理预见的人为误用所导致的不合理风险。

由于预期功能安全问题是目前自动驾驶汽车商业化发展的最大难题之一，因此中国智能网联汽车产业创新联盟-预期功能安全工作组全体成员单位对预期功能安全前沿技术进行了广泛调研分析，并协作撰写了此报告，以期为我国进一步开展预期功能安全研究工作提供参考。

### 1.2 预期功能安全前沿技术研究报告内容

本报告分别对国内外智能网联汽车预期功能安全相关政策/法规、预期功能安全相关标准、预期功能安全相关技术、预期功能安全相关专利、场景库研究现状、功能测试评价体系、典型ADAS系统的SOTIF研究现状等七个方面进行了详尽的调研、总结与分析。

### 1.3 预期功能安全前沿技术研究报告使用范围

本报告工作重点为调研国内外自动驾驶汽车预期功能安全技术研究现状，旨在为我国开展全面的自动驾驶汽车预期功能安全技术研究提供参考与指导，同时可以为自动驾驶汽车预期功能安全技术研发提供思路。此外，本报告仅对预期功能安全的相关内容进行调研与分析，不包括功能安全与信息安全技术。

## 第2章 国内外智能网联汽车安全相关政策/法规

自动驾驶已成为全球汽车行业发展的热点。美国、日本和欧洲多国在大力发展自动驾驶技术的同时，出台了一系列涉及自动驾驶汽车上路测试和应用管理的政策法规。近期，我国发改委、公安部等11部委联合发布了《智能汽车创新发展战略》。本战略报告系统梳理了5年来（2016至2020年）美、日、欧等国家和地区的自动驾驶汽车上路法规政策，分析政策特点，并提出了相应的启示。

### 2.1 美国自动驾驶汽车相关法规政策

#### 2.1.1 概述

美国政府对待自动驾驶汽车的态度较为开放。2011年，内华达州出台了美国首部自动驾驶地方法案，允许自动驾驶汽车上公共道路开展测试验证。此后，其他各州政府纷纷制定自动驾驶法规。自2012年起，美国至少有41个州提议制修订自动驾驶相关法案。目前已有34个州颁布了自动驾驶法案，已生效的法案共计64个。现阶段各州中开放程度最高、测试车辆最多的地区是加利福尼亚州，该州目前已开放有测试驾驶人的上路测试、无测试驾驶人的上路测试和无人驾驶运营示范等三种许可申请。在上述三种许可的申请中，多数企业仍处在有测试驾驶人的上路测试阶段（累计64家企业获得牌照），仅谷歌旗下Waymo获得无测试驾驶人的上路测试的许可，目前尚无企业获得加州的运营示范许可。

美国采取“联邦-州政府”两级模式管理自动驾驶汽车上路。联邦政府与各州政府划分职责、分工配合，共同推动自动驾驶的有序发展。联邦政府主要通过制订政策指南文件来支持引导自动驾驶上路测试和产业发展，提出安全原则性要求，重点关注确保产业安全发展和消除现有制度对创新的障碍。各州政府主要通过立法等手段管理本地区内自动驾驶汽车上路测试，提出具体要求和实施细则，审核申请材料，定期评估测试车辆的上路资格。《联邦自动驾驶汽车政策》（AV 1.0）提出，联邦政府有意愿从国家层面统一管理全美的自动驾驶汽车。

政策方面，美国交通部（DOT）及下属国家道路交通安全管理局（NHTSA）颁布了多项用于指导自动驾驶汽车发展的政策。2016年颁布了《联邦自动驾驶汽车政策》（AV 1.0），对自动驾驶汽车提出了15项安全评估要求。2017年颁布了《自动驾驶系统2.0：安全愿景》（ADS 2.0），将AV1.0中的15项安全评估要求简化为12项；

2018 年颁布了《未来交通展望：自动驾驶汽车 3.0》(AV 3.0)，明确提出将对自动驾驶汽车的发展给予国家层面的大力支持；今年颁布了《确保美国自动驾驶领先地位：自动驾驶汽车 4.0》(AV 4.0)，强调了政府支持自动驾驶汽车及相关技术开放创新的态度，同时着力提升民众对自动驾驶汽车的认同感。

法规方面，尽管美国现在没有正式通过联邦层面的自动驾驶上路管理法规，但包括《美国通过革命性技术提高安全运输的愿景法案》(S.1885- AV START Act) 等已经形成草案，目前在推动发布过程中。该草案中定义了两种形式的自动驾驶汽车，一种是面向传统驾驶位有人类驾驶人的自动驾驶汽车，另一种是面向通过远程遥控操作的自动驾驶汽车。草案中明确提出人类驾驶人的存在并非必须，且不得以身体残疾为由剥夺残疾人使用和操作自动驾驶汽车的权利。从草案制订的方向来看，未来将有可能允许改变汽车的设计方式，出现如没有方向盘、无制动踏板以及没有驾驶位的自动驾驶汽车。

### 2.1.2 特点分析

通过对美国现有自动驾驶汽车相关法规政策的概述，分析总结美国自动驾驶汽车法规政策有如下的特点：

1、采用两级管理模式。为了明确职责和避免规范不一致，2016 至 2020 年间，美国在联邦层面制定了 4 部自动驾驶汽车发展政策，该系列政策为美国联邦政府用于促进自动驾驶产业发展的指导性政策，明确了美国发展自动驾驶的基本策略。联邦政府的基本立场为不干预自动驾驶技术的路径选择，将关注点置于确保产业安全发展和消除现有制度对创新的障碍。

2、政策法规提供开放宽松的环境。一是自我认证：申请上路许可前，车企自行准备材料证明测试车辆符合各项法规和 FMVSS，无需第三方检测；二是豁免条款：对于不符合 FMVSS 的内容，企业只需提供证明安全性的材料即可申请豁免；三是测试道路：以加州为代表的多数州不指定自动驾驶测试道路，测试车辆根据需要自行选择测试路线。

3、高度开放的政策存在安全隐患。美国政府出台自动驾驶系列政策推动自动驾驶汽车产业的发展，给予汽车企业灵活的发展空间。激进的策略可能在短期内起到效果，但会带来潜在的安全隐患，自动驾驶汽车在测试过程中安全事故频发。以加州为例，目前共有 64 家企业获得上路测试许可，2018 年和 2019 年上路测试的自动

驾驶汽车发生事故数都在 70 起以上。2019 年，亚利桑那州甚至发生自动驾驶汽车致人死亡的事故。大量的交通事故体现出目前自动驾驶技术尚未完全成熟，提升了民众对自动驾驶汽车的不信任度，对产业发展产生消极影响。

### 2.1.3 主要内容

近 5 年来美国自动驾驶汽车相关的法规政策文件发布推进情况如表 2-1 所示。

表 2-1 美国近 5 年自动驾驶汽车相关法规政策汇总表

序号	法规政策名称	发布时间
1	《联邦自动驾驶汽车政策：加速下一代道路安全革命》 (AV 1.0)	2016 年 9 月
2	《自动驾驶系统 2.0：安全愿景》(ADS 2.0)	2017 年 9 月
3	《准备迎接未来交通：自动驾驶汽车 3.0》(AV 3.0)	2018 年 10 月
4	《确保美国自动驾驶领先地位：自动驾驶汽车 4.0》 (AV 4.0)	2020 年 1 月
5	《自动驾驶法案》(H.R.3388-Self Drive Act)	尚未颁布实施
6	《美国通过革命性技术提高安全运输的愿景法案》 (S.1885- AV START Act)	尚未颁布实施

下文对表 2-1 中的政策法规进行简要介绍。

#### 1、《联邦自动驾驶汽车政策：加速下一代道路安全革命》

发布时间：2016 年 9 月。

主要内容：该政策介绍了美国政府对于自动驾驶系统在研发过程中所关注的技术性能期望、联邦与州政府的管理角色、现行的监管模式等，并对未来的监管手段做了一定的畅想，最后对自动驾驶汽车厂商在设计自动驾驶系统的过程中所应该注意的关键点提出了相关要求。具体内容如下：

(1) 提出规范对象，明确测试车辆范围。该政策主要就车辆类型、驾驶方式、安全性要求以及使用途径 4 方面做了说明。首先，车辆类型方面，在公共的道路上用于自动驾驶系统测试与应用的车辆可为轻型、中型、重型车辆。其次，驾驶方式方面，包括装配了自动驾驶系统的车辆和车内具有人类驾驶人且按照人类驾驶人的



指令按照指定路线完成驾驶任务的车辆。另外，安全性要求方面，需要满足 FMVSS（若有不符合的情况出现，每家厂商可申请一定数量的豁免权）。最后，使用途径方面，若车辆不是被厂商、代理商及相关测试驾驶人操作，即可被认定为量产车辆。

（2）明确自动驾驶汽车运行安全研发关键点。厂商在开发过程中应该关注 5 个方面：一是测试数据的记录与分析，车辆在设计开发的初期要考虑加入数据记录与分析的功能；二是功能安全与网络安全，厂商需要保证自动驾驶系统运行过程中的功能安全与联网后的网络安全；三是合理的交互设计，自动驾驶系统需要有良好的用户界面交互设计界面（对行车过程中驾驶安全性的保证）；四是发生事故后的安全保护，自动驾驶汽车应提升发生碰撞事故后的乘员安全系数；五是合理的操作说明书与客户的应用培训。

（3）自动驾驶系统等级评定基本流程。厂商提交自动驾驶汽车产品的设计运行域，内容包括道路种类、地理位置、速度范围、灯光操作及天气条件等。DOT 依据所提交的相关材料结合自动驾驶汽车的基本性能框架，界定该自动驾驶汽车的具体等级。

（4）提出厂商开发自动驾驶系统的基本流程。厂商在进行自动驾驶系统开发过程中，应该明确自动驾驶系统所能适用的具体范围，所研发的车辆应达到目标的有效侦测、意外情况的有效反应、响应能力良好等基本性能。具体流程包括：首先明确自动驾驶系统设计使用的适用范围（目前缺少对自动驾驶系统的具体性能测试和标准）；其次进行目标和意外检测与响应能力的测试；最后开展风险规避能力试验，要求厂商、研发机构应能记录自动驾驶失效后的应急处理过程。上述试验的测试方式可采用仿真测试、封闭场地测试、道路测试等形式。

## 2、《自动驾驶系统 2.0：安全愿景》

发布时间：2017 年 9 月。

主要内容：该政策主要内容为自愿性认证指导，突出了将 AV 1.0 中的 15 项安全规范简化为车辆自动驾驶汽车网络安全、人机界面、耐撞性、消费者的教育和培训，以及碰撞后自动驾驶系统的行为等 12 项主要的安全要素，以及提出相关的自愿性安全自我评估方法。具体内容如下：

（1）自动驾驶系统的自愿性安全评估。NHTSA 提出一种非监管的自动驾驶汽车技术安全评估方法，即自动驾驶系统的自愿性安全评估。目的是为支持汽车行业

和其他主要利益相关者设计、测试及安全部署自动驾驶汽车。评估范围包括系统安全、设计域、目标物检测及响应、应急备份、验证方法、人机界面、车辆网联安全、耐撞性、碰撞后自动驾驶系统行为、数据记录、消费者的教育和培训、法律等 12 项。自愿性安全评估鼓励从事测试和部署的实体公开披露其自动驾驶系统的自愿性安全评估的结果，以展示其实现系统安全的方式方法。

(2) 为州政府提供政策和技术支持。上公共道路测试的自动驾驶汽车受联邦和州政府的管辖。在州政府立法的同时，NHTSA 需向各州提供相应的技术援助。政策中阐明了在监管自动驾驶系统时联邦政府和州政府的职责与定位。具体为 NHTSA 负责管理车辆及车辆设备的安全设计和性能；各州继续负责管理驾驶人和车辆操作。此外，政策还提供了国家公路安全官员的最佳实践，形成了自动驾驶系统在公共道路安全运行的条件及技术框架，包括应用程序和测试权限、登记和所有权、与公共安全官员合作，以及责任和保险等方面的考虑。

### 3、《准备迎接未来交通：自动驾驶汽车 3.0》

发布时间：2018 年 10 月。

主要内容：该政策是 DOT 的地面运输运营管理局首次发布的关于车辆自动化的政策声明。政策整合了制造商、技术研发企业、基础设施运营商、汽车运营商、公交运营商以及各州政府的反馈意见，提出了新的多模式安全引导方法，明确了政策和政府角色，简述了自动驾驶汽车技术的发展。具体内容如下：

(1) 部门及相应职责划分。联邦政府中负责自动驾驶汽车管理的相关部门为 NHTSA、联邦机动车运营安全管理局（FMCSA）、联邦道路管理局（FHWA）和联邦运输管理局（FTA）。职责方面，联邦政府负责管理自动驾驶汽车和自动驾驶装置的安全性能，以及自动驾驶汽车在州际贸易中的应用，其中 NHTSA 的主要职责为指定自动驾驶汽车的联邦安全标准，并处理自动驾驶汽车的安全缺陷。州政府车辆管理部门（DMV）负责驾驶资格的审核与牌照发放、道路规则制定、侵权责任和保险政策制定等。

(2) 自动驾驶汽车实施策略。一是让自动驾驶产业相关者和公众成为解决自动驾驶汽车问题的主导者；二是提供最佳的政策，支持自动驾驶产业相关者更好的理解自动驾驶汽车融入交通后对他们角色和职责的影响；三是通过与自动驾驶产业相关者和标准研究机构开展合作，支持自愿性标准、强制标准和政策的制定；四是以

目标为导向的未来政府决策支持；五是考虑到现有法规对自动驾驶汽车发展和普及带来的挑战，应着手开展法规的更新工作。

(3) 分阶段递进式管理。一是技术开发和早期道路测试阶段，在自动驾驶汽车上路测试前开展完善的工程和安全分析，使用原型自动驾驶系统来了解安全风险并研究应对策略；二是自动驾驶汽车道路试验阶段，本阶段主要在预期的操作环境中建立对成熟软件和硬件的置信度分析，在可预期的条件下，研究分析的关键是系统的故障和测试驾驶人的主观反馈；三是有限制的自动驾驶汽车部署阶段，本阶段主要目的是在预期的运行环境中，研究取得对自动驾驶系统软件和整车的运行信心，测试潜在的安全隐患、收集不同用户和公众的反馈，了解公众的包容度。

#### 4、《确保美国自动驾驶领先地位：自动驾驶汽车 4.0》

发布时间：2020 年 1 月。

主要内容：一是统一标准协同发展：建立从联邦到各州，从政府机构、委员会到相关企业、非盈利组织等在内的技术规范与标准，促进不同组织机构通力合作，并实现相关信息共享；二是统一并简化监管体系：研究简化的监管方式，消除监管障碍，为企业在自动驾驶产业的创新铺平道路。三是提高政策的透明度与一致性：为提升自动驾驶汽车在美国的接受程度，美国政府决定采取透明化的政策方式，用于提升美国公众对自动驾驶汽车的信任度。具体内容如下：

(1) 肯定了自动驾驶汽车的社会及经济效益。该政策提到自动驾驶汽车潜在社会与经济效益包括提高安全性和减少道路交通事故死亡人数；提高全体公民生活、移动出行质量；改善供应链管理等。

(2) 确立了发展的三大原则。一是保护用户及民众。自动驾驶汽车的发展要优先考虑人身安全，同时需关注技术和网络安全，开展隐私及数据安全的保障工作，增强相关政策的机动性与可行性；二是促进市场有序发展。政府方面要保持对待技术态度的中立性，避免过度干预影响技术创新性与企业的创造力，应根据技术发展需求及时更新相关政策；三是积极协调各重点工作。政府应着力制定一致的标准与政策，强化协同、监管等方面的工作，促进自动驾驶汽车与交通运输系统的有效融合，尽快实现自动驾驶汽车的安全运行。

#### 5、《自动驾驶法案》

发布时间：尚未颁布实施。

主要内容：本法案是美国首部旨在确保自动驾驶汽车的安全创新、研发、测试及部署的专门法案草案稿。其目的是明确联邦政府在确保自动驾驶汽车安全方面的职责，推动自动驾驶汽车的测试和部署。具体内容如下：

(1) 明确主管部门。法案中明确了 **NHTSA** 为自动驾驶汽车的主管部门，强调了联邦政府对自动驾驶汽车具有优先监管权。并区分了联邦和州政府在自动驾驶汽车法规制定上的角色，其中 **NHTSA** 的主要职责包括高级自动驾驶汽车的认证、标准和法规制定等。

(2) 落实自动驾驶汽车安全标准。法案草案稿要求自动驾驶汽车生产商或者系统提供商需要向监管部门提交安全评估证明，以证明其自动驾驶汽车在数据、产品、功能等方面采取了足够的安全措施。同时，法案草案稿要求 **NHTSA** 逐步完善包括自动驾驶汽车在内的汽车安全标准或者安全范围，具体项目包括人机交互界面、传感器、感知系统、自动驾驶系统软件和网络安全要求等，并且安全标准和安全范围应该定期审查和更新。

(3) 关注自动驾驶系统网络安全。法案草案稿要求自动驾驶汽车厂商必须制定网络安全计划，具体方案包括如何应对网络攻击、未授权入侵以及规避虚假或者恶意控制指令等安全策略，用以保护关键的控制、系统和程序，并根据环境的变化对此类系统进行定期更新，同时还需制订内部人员的安全培训和管理制度。

(4) 提出通用性豁免条件。法案草案稿提出豁免监管办法，允许汽车制造商第一年的汽车豁免量为 2.5 万辆，第二年为 5 万辆，第三、四年均为 10 万辆。被豁免的自动驾驶汽车无需严格遵守现有的汽车安全标准和相关规定，比如要求汽车具有方向盘和油门踏板等。

(5) 建立自动驾驶汽车顾问委员会。法案草案稿要求 **NHTSA** 建立自动驾驶汽车顾问委员会，成员应当包括来自商业界、学术界的代表，以及独立的研究人员、州和当地机构的代表、安全专家、消费者代表、工程师、劳工组织代表、环境专家、**NHTSA** 代表等。委员会将根据需要设立次级委员会，以开展信息搜集活动、制定技术建议并且向 **NHTSA** 提供建议。次级委员会的成员人数应在 15-30 人。

(6) 强化自动驾驶汽车隐私保护。法案草案稿要求厂商必须制定隐私保护计划，包括对车主以及乘客信息的搜集、保存、使用等方面的保护措施。同时，联邦交易委员会需开展相关研究，确定各隐私信息类型。



(7) 明确自动驾驶系统定义。法案草案稿中将自动驾驶系统定义为可持续实施完全动态驾驶任务的硬件和软件，动态驾驶任务包括横向运动控制、纵向运动控制，主动探测、自主识别、决策分类和执行能力以及对驾驶环境监控等，但不包括路线选择。

#### 6、《美国通过革命性技术提高安全运输的愿景法案》

发布时间：尚未颁布实施。

主要内容：该法案草案稿为美国旨在确保美国在自动驾驶产业中汽车的安全创新、研发、测试及部署的专门法案。目的是明确联邦政府在确保自动驾驶汽车安全方面的职责，推动自动驾驶汽车的测试和部署。具体内容如下：

(1) 承认机器驾驶人。法案草案稿定义了两种类型的自动驾驶汽车，一种是面向传统驾驶位有人类驾驶人的自动驾驶汽车，另一种是面向通过远程遥控方式操作的自动驾驶汽车，同时不得将身体残疾作为自动驾驶汽车的使用和操作许可的制约因素。

(2) 提升豁免车辆数量。该草案稿中允许不满足现行车辆强制性安全标准的自动驾驶汽车也可进行测试或销售，规定一个制造商第1年最多豁免1.5万辆自动驾驶汽车，第2年最多4万辆，第3年最多8万辆，第4年后可豁免超过8万辆。

(3) 成立专业机构。法案草案稿提出设立高度自动驾驶汽车技术委员会，旨在研究制定高度自动驾驶汽车的规则与标准，包括系统安全、自动转向与刹车、防撞方式、关键数据记录、国家与国际标准间的潜在冲突问题等。

(4) 安全评估要求。法案草案稿规定制造商应提交自动驾驶汽车安全评估报告，包括系统安全、数据记录、网络安全、人机交互界面、防碰撞性、自动驾驶汽车能力和限制、碰撞后行为、遵守交通法规以及自动驾驶系统功能等9项。

(5) 网络安全要求。法案草案稿规定除制定网络安全计划外，制造商还可通过与安全研究人员建立一定的联系来减少网络安全的风险。安全研究人员也可通过漏洞披露政策，将其发现的漏洞信息通知制造商，并为其留够时间确认和修复漏洞。

## 2.2 日本自动驾驶汽车相关法规政策

### 2.2.1 概述

为抢占未来汽车产业发展的战略制高点，增强汽车产业竞争力、降低交通事故、

缓解交通拥堵、应对老龄化交通出行问题，日本政府积极布局自动驾驶汽车产业，将其纳入国家发展顶层规划，出台了一系列法规政策文件，推动自动驾驶产业发展应用。日本自动驾驶汽车管理主要涉及内阁官房、经济产业省、国土交通省、警察厅、总务省、内阁府等 6 个政府部门。内阁官房作为牵头单位，负责各部门间的统筹和协调工作，其他政府部门在各自职责范围内推进自动驾驶汽车健康发展。其中，警察厅主要负责法律制修订、道路测试管理规范等制定工作。

目前，日本已出台自动驾驶汽车相关的法律修正案、上路测试规范、指南文件等共 7 项。法律修正案包括《道路交通法》和《道路运输车辆法》等 2 项，主要修改内容为引入自动驾驶系统的定义，并且对自动驾驶系统的使用、测试、维修等内容提出相应的配套规定；上路测试规范包含《关于自动驾驶系统的公共道路测试指南》、《远程自动驾驶系统道路测试许可处理基准》、《自动驾驶的公共道路测试使用许可标准》等 3 项，前两者分别规范了自动驾驶系统控制车辆和远程遥控控制车辆上路测试，第三项规范是前两项的基础上合并修订发布。指南性文件有《自动驾驶汽车安全技术指南》和《自动驾驶相关制度整備大纲》等 2 项，主要阐述自动驾驶汽车的安全技术规范和政府后续立法和监管的方向。

### 2.2.2 特点分析

通过对日本现有自动驾驶汽车相关法规政策的概述，分析总结日本自动驾驶汽车法规政策有如下的特点：

1、从法律定义上接纳自动驾驶。《道路交通法》修正案认可车辆安装具有自动驾驶功能的“自动运行装置”。并在“驾驶”名词定义中，添加使用“自动运行装置”驾驶汽车的情况，允许驾驶人在此情况下分散注意力（如看手机、看视频等行为），从驾驶主体和基本操作行为中全面引入“机器驾驶人”的概念。同时，对自动驾驶汽车进行软硬件具象化描述，通过“二个硬件+一个软件”来实体化自动驾驶汽车的“机器驾驶人”。其中，“二个硬件”指的是自动驾驶系统的载体——“自动运行装置”和用于事件记录的“工作状态记录装置”，“一个软件”是指用于操纵自动驾驶系统的“自动驾驶汽车程序”，配套详尽的更新升级许可制度。以“硬件+软件”的形式对自动驾驶系统细化描述，明确了车辆控制和运行监管的基本车载载体。

2、法规政策总体谨慎。尽管日本为推进自动驾驶汽车落地应用发布了多项法规政策，甚至提出了法律修正案，但是实施细则却非常缜密谨慎。一是规定具体，从

上路前认证到上路后监管都做了明确的规定；二是限制速度，要求上路测试的自动驾驶汽车速度原则上不超过 20 公里/小时；三是软件升级，自动驾驶系统软件升级后需要由警员上车乘坐审核后才能上路；四是循序渐进，要求自动驾驶汽车经过充分的仿真测试和封闭场测试后才可上路测试。

3、人类驾驶者法律义务不清晰。《道路交通安全法》允许 L3 级别自动驾驶汽车的人类驾驶者在确保车况良好、能自主可靠运行的前提下使用手机、观看视频，同时又要求其能够及时意识到车辆异常或紧急情况的发生并及时接管。但是对何时接管、人类驾驶者应当保持何种程度的注意力等关键问题，该法并未给出明确具体的要求。

4、参照传统汽车管理体系制定自动驾驶汽车管理框架。日本《道路运输车辆法》将车辆的自动运行装置纳入传统车辆安全标准要求范围，要求自动运行装置必须符合安全标准，并确保严格按照型号认证、定期检修、年检、问题召回等制度的相关标准来执行，初步形成自动驾驶汽车管理框架。

### 2.2.3 主要内容

近 5 年来日本自动驾驶汽车相关的法规政策文件发布推进情况如表 2-2 所示。

表 2-2 日本近 5 年自动驾驶汽车相关法规政策汇总表

序号	法规政策名称	发布时间
1	《关于自动驾驶系统的公共道路测试指南》	2016 年 5 月
2	《远程自动驾驶系统道路测试许可处理基准》	2017 年 6 月
3	《自动驾驶相关制度整備大纲》	2018 年 3 月
4	《自动驾驶汽车安全技术指南》	2018 年 9 月
5	《道路交通安全法》修正案	2019 年 3 月
6	《道路运输车辆法》修正案	2019 年 5 月
7	《自动驾驶的公共道路测试使用许可标准》（《关于自动驾驶系统的公共道路测试指南》的修订版本）	2019 年 9 月
8	《汽车损害赔偿保障法》、《无线电法》	尚未颁布实施

下面对表 2-2 中日本的自动驾驶相关法规政策进行介绍。

#### 1、《关于自动驾驶系统的公共道路测试指南》

发布时间：2016 年 5 月。

主要内容：该指南明确了驾驶人应当坐在驾驶位上，测试车辆和驾驶人均应符合并遵守现行法律法规，同时明确了测试机构、测试驾驶人资质，测试车辆安全技术要求等。

(1) 对测试过程的要求。一是充分认识公共道路测试的安全隐患，提前确认交通环境，制定相应安全措施；二是采取分阶段测试策略，确认自动驾驶系统功能的安全性，其中第一阶段在实验场地上进行测试验证，第二阶段选择意外交通事故发生可能性较小的公共场地进行测试，第三阶段过渡到复杂交通环境下的道路进行测试；三是对测试驾驶人以及乘坐在测试车辆内的相关人员进行相关培训，包括遇到交通事故、车辆故障等紧急情况下的处置要领的培训，并形成书面材料；四是应对测试汽车进行足额投保，确保具备相应意外事故赔偿能力；五是测试开始前及时向当地警方、市政/交通运输部门报告测试计划，应包括测试时间和地点、测试车辆的自动驾驶功能、拟采取的安全措施等内容。同时提前通过传单和标志等形式向当地居民与道路使用者告知公路测试的时间与地点；六是交通事故发生后，测试机构和测试驾驶人应按照《道路交通安全法》第 72 条的规定，立刻停止驾驶，救援受伤人员，采取道路预警措施，并向警方报告事故情况，同时，测试机构应对事故原因进行调查，在采取纠正措施前，应停止开展同类的道路测试工作。

(2) 对测试驾驶人资质要求。一是持有测试车辆对应类别的驾驶执照，具备多年驾驶经验；二是在封闭场地实际驾驶过测试车辆，熟悉测试车辆的自动驾驶系统原理和特点，娴熟掌握紧急情况下的驾驶操作要领；三是如在测试过程中发生交通事故，驾驶人必须承担《道路交通安全法》规定的驾驶责任和义务；四是测试驾驶人必须乘坐在测试车辆的驾驶位上，并始终观察和监视周围道路交通情况以及车辆状态，在发生系统软/硬件故障等紧急情况时能够进行手动操作，确保驾驶安全且不危害他人；五是在交通量少、视野开阔的路段，允许驾驶人把手放在扶手或膝盖上保持放松姿势，但在视野不开阔或交通量较大的路段，驾驶人应当握住方向盘等操作装置，或把手放在贴近操作装置的位置，以便能够迅速进行操作。

(3) 对测试车辆的安全技术要求。一是测试车辆应符合《道路运输车辆安保基准》规定的安全要求；二是在实验场地内开展充分细致的驾驶测试，确保自动驾驶状态下的测试车辆能够安全行驶；三是车身上标示“正在进行自动驾驶系统测试”的字样；四是安装行驶记录仪和交通事故数据记录仪等装置，用于记录行驶过程中车



辆运行状态和周边交通情况，收集包括车辆运行状态信息在内的各种传感器数据和工作状态；五是自动驾驶系统应确保在发生紧急情况时驾驶人能够进行手动驾驶操作，当自动驾驶系统发生故障或超出自动驾驶功能范围时，测试车辆应留出充裕的时间，通过声音提示驾驶人进入手动驾驶模式；六是在自动驾驶和手动驾驶模式间切换时，应对车辆操作进行恰当的授权，如自动驾驶模式开启或结束时，通过鸣响警示音进行提示；七是测试机构应根据《网络安全基本法》的规定，切实采取网络安全防护措施确保自动驾驶系统安全，防止网络非法入侵；八是自动驾驶系统软件升级后应重新在测试道路上进行测试，确认系统软件安全可靠后，才可进行道路测试。

## 2、《远程自动驾驶系统道路测试许可处理基准》

发布时间：2017 年 6 月。

主要内容：鉴于《日内瓦道路交通国际公约》和日本《道路交通法》规定了“汽车需要有驾驶人驾驶”，而未来全自动驾驶汽车“既无驾驶人又无需掌控方向盘”，日本警察厅为推动远程遥控自动驾驶系统实用化技术的开发，颁布了此基准，将远程监控员定位为远程遥控、承担现行道路交通法规上规定义务和责任的驾驶人。

(1) 审查内容。一是测试机构应对申请的测试道路反复调查，测试时间应避开明显影响公众正常通行的时间段。同时做到能观察和掌握沿线行人突然穿行等实际可能发生的交通事件，确保测试车辆能够安全地在道路上行驶；二是测试场地需选择无线通信稳定的场所进行，一旦通信中断，车辆能够自动平稳安全停止；三是测试车辆正面、侧面和背面应贴有正在试验的标识；四是测试车辆应符合《道路运输车辆安全基准》，远程监控员正确操控所有测试车辆的制动功能。同时，远程监控员可通过电子屏幕及音视频掌握测试车辆周围状况，车辆内部状况以及行驶方向的状况，在必要情况下可与车内人员通话；五是远程监控员应持有与测试车型相符的驾驶执照，清楚知晓作为事实上的车辆驾驶人所承担的义务和法律责任；六是测试机构需要提前向交通，消防部门报备，提交实验车辆的构造，停驶方法等必要信息，确保事故发生时相关部门能及时采取应对措施。

(2) 审查流程。一是测试机构需向测试道路所在行政辖区的警察局提交申请材料；二是收到申请材料后，警察局将指派相关警员进行道路行驶测试。具体方法为由一名远程监控员操作申请许可的测试车辆，该警员亲自乘坐，审查其能否在遵守

交通法规的前提下安全行驶；三是审查合格后，相关部门签发有效期不超过 6 个月的测试道路使用许可文件（具体时限取决于测试道路的交通状况）。

（3）许可实施条件。一是道路测试必须严格按照申请的时间、路段开展；二是只允许许可批准的远程监控员使用其对应的远程遥控自动驾驶汽车进行测试。并且该远程监控员只允许利用远程遥控驾驶系统操纵测试车辆，除非其位于车内。测试期间，远程监控员应始终保持监视状态，其视野以及操作系统应确保不被妨碍；三是远程监控员的驾驶证副本和测试道路使用许可文件副本应放置于测试车辆内；四是测试车辆的行驶速度应低于普遍车辆的安全停车距离对应的速度；五是测试过程中如果发生交通事故，测试机构应及时向警方报警并停止测试，同时将测试车辆记录的视频、音频资料、远程监控员的视频、音频资料和通讯日志等信息递交警方；六是在开展测试前，测试机构应提前向当地居民宣传并说明测试内容；七是测试过程中如果需要增加测试车辆，每增加一辆都应作为新的测试实验重新申请道路测试许可。

### 3、《自动驾驶相关制度整备大纲》

发布时间：2018 年 3 月。

主要内容：为了逐步完善相关政策制度，推动自动驾驶技术进一步发展。该大纲主要从保障综合安全，完善交通规则，明确责任关系三个方面出发，明确了今后政府及相关机构所需研究制定的立法和监管方向。

（1）保障综合安全。一是为应对自动驾驶技术的迭代更新，地区议会，运输服务公司，行政机构以及专家需要协同配合，共同构建灵活有效的安全标准体系；二是针对自动驾驶的私家车和物流服务车辆分别考虑制定自动驾驶汽车安全标准，明确安全要求。包括强制要求安装行驶记录仪，且行驶记录仪应具备记录车辆位置、方向盘操作和自动驾驶系统运行状况等信息的功能。车辆使用期间有必要考虑其所需的维护和管理标准，以及在建立安全标准的基础上更新车辆自动驾驶系统软件的方式。

（2）完善交通规则。针对 L3 级自动驾驶汽车，有限区域中 L4 级自动驾驶汽车。考虑分别对相关的交通法规进行必要的修正，以确保其符合道路交通法规的规范；对于使用自动驾驶汽车的人类驾驶人，重新考虑其作为驾驶人的义务，包括在自动驾驶过程中所允许驾驶以外的活动，以及自动驾驶汽车带来的新义务；考虑自

自动驾驶期间可能违反道路交通安全法规的处罚规则与标准。

(3) 明确责任关系。关于民事责任，考虑自动驾驶汽车在自主行驶时，所发生的事故赔偿责任原则上由车主承担，同时适用于传统机动车交通事故责任强制保险（交强险）的赔付条件，并且充分保障保险公司对汽车制造商的求偿权；若事故由自动驾驶系统缺陷造成，由汽车制造商承担全部责任，同时可能会追究软件开发者的责任；若车辆所有者更新系统并采取了安全举措，仍旧因黑客入侵导致事故，则等效于车辆被盗，经济赔偿由政府救济制度兜底；针对车辆的使用，考虑汽车制造商具有对车主说明与警告的义务，否则也应承担相应责任。关于刑事责任，考虑在自动驾驶汽车市场化后，根据相关的法律制度，明确驾驶人、车内安全人员、远程监控员、服务经营者等各种各样的关系主体的义务。并基于此进行有关刑事责任的讨论。

#### 4、《自动驾驶汽车安全技术指南》

发布时间：2018 年 9 月。

主要内容：该指南针对的是搭载 L3、L4 级自动驾驶系统的乘用车、卡车及公交车，规定了此类汽车所需满足的安全条件，主要内容包括以下 10 项：

(1) 设计运行范围的设定。汽车生产商及使用自动驾驶汽车的移动服务系统供应商，应根据自动驾驶汽车的性能及使用方式确定设计运行范围，对于自动驾驶汽车引发的人身事故进行合理预警并预防其发生。相关内容应包括道路条件（高速公路、普通道路、车道数目等）、地理条件（城市、山区等）、环境条件（天气状况、夜间等）、其他条件（限速、特定道路运行、安全人员乘车与否等）。

(2) 自动驾驶系统的安全性。法规方面，自动驾驶系统应遵守交通法规。系统启动方面，自动驾驶系统的开启条件应限定在设计运行范围内，同时明确了自动驾驶汽车的驾驶人应能控制自动驾驶系统的启动。安全冗余方面，需确保控制系统及传感器有冗余，如果超出设计范围或者发生故障时，L3 级自动驾驶系统应向司机发出警告要求介入，而 L4 级自动驾驶系统应能自动将车辆停到安全的地方。

(3) 遵守安全标准。自动驾驶汽车应能满足已有的自动驾驶相关的道路运输车辆的安全标准，并满足国际标准化组织等机构制定的相关国际标准。

(4) 人机交互界面设计。L3 级自动驾驶汽车的人机界面应能监控司机状态，确保司机随时接管操作，必要时发出警报。当 L4 级自动驾驶汽车的系统确认无法继

续进行自动驾驶时，人机界面应能让司机或乘客事先知道车辆将会自动停车。

(5) 数据记录装置搭载要求。自动驾驶汽车应具备记录自动驾驶系统启动情况、司机注意力集中情况等数据的装置。今后政府还将探讨数据记录装置的具体细节(记录事项、记录时间、保留时间、数据使用目的及个人信息处理等) 以及是否要求强制安装。

(6) 网络安全相关要求。汽车生产商及使用自动驾驶汽车的移动服务系统供应商，应根据国际网络安全的最新规定，在进行车辆的设计和开发时考虑网络安全的相关内容，包括如何应对黑客攻击等。

(7) 用于无人驾驶移动服务的车辆安全性(追加要求)。用于 L4 级无人驾驶移动服务的自动驾驶汽车，应设置摄像头和声音通信设备，便于运行管理中心监控车内状况；应在乘客可轻易触碰到的地方设置紧急停止按钮；紧急状况下停止或遇到事故时，应能自动通报运行管理中心；车辆紧急停止时和运行管理中心的联络，以及紧急状况下的应对情况，应能通过人机界面方便地传递给乘客。

(8) 安全性测试。为了确保能合理预警并预防自动驾驶系统引发的人身事故，汽车生产商及使用自动驾驶汽车的移动服务系统供应商，应适当进行排练、测试、道路试验，事先确保安全。

(9) 确保使用过程安全。为了确保自动驾驶汽车使用过程中的安全，汽车生产商、使用自动驾驶汽车的移动服务系统供应商，以及自动驾驶汽车实际使用者，应对车辆软件进行必要的升级，从而确保安全性。

(10) 向自动驾驶汽车使用者提供告知信息。汽车生产商、经销商以及移动服务系统供应商，应采取措施，让自动驾驶使用者了解一系列信息，包括：系统使用方法、运行设计域(ODD)范围、系统异常时车辆的反应、适当进行软件升级等。

## 5、《道路交通安全法》修正案

发布时间：2019 年 3 月。

主要内容：此次发布的修正案主要在原《道路交通安全法》的基础上，针对自动驾驶汽车特点，提出了与之响应的修订意见，法律修订后将可实现 L3 级的自动驾驶汽车上路行驶，但 L4 级及以上的自动驾驶汽车上路行驶还需进一步完善法律条文。

(1) 新增与变更的相关定义。一是新增“自动运行装置”的定义，在修订案中，自动驾驶系统被定位为“自动运行装置”，具体内容为能替代驾驶者实现关于汽车驾



驶的感知、预测、判断、操作的全部功能的装置。以及具有记录工作状态相关数据的功能的装置；二是修改了关于“驾驶”的定义，添加了使用自动运行装置驾驶汽车的情况。

(2) 规定了“自动运行装置”使用者的义务。包括一是在不满足自动运行装置使用条件时，驾驶者不得使用该自动运行装置驾驶该汽车；二是当驾驶者使用自动运行装置驾驶汽车，并且自动驾驶汽车符合整备得当状态良好、自动运行装置符合使用条件、该车处于即使脱离自动运行装置也能由驾驶者进行可靠操作的状态等三项条件时，对自动运行装置使用者不适用《道路交通安全法》第 71.5.5 项禁止规定（如驾驶期间禁止使用手机，禁止观看视频等）。

(3) 与车辆工作状态记录装置相关的法规制定。一是驾驶者的义务包括驾驶者必须安装工作状态记录装置、驾驶者有保存工作状态记录装置的数据的义务；二是警察具有的权利包括拦停车辆，检查工作状态记录装置的相关文件，检查工作状态记录装置的安装情况，当有必要获取装置中音频视频信息时，有权要求提供等。

## 6、《道路运输车辆法》修正案

发布时间：2019 年 5 月。

主要内容：该法为实现自动驾驶的应用规定了安全标准，针对自动驾驶的修订涵盖以下几个方面：

(1) 将自动运行装置纳入安全标准要求范围。要求必须符合安全标准，确保严格按照型号认证、定期检修、年检、问题召回等制度的相关标准来执行。

(2) 制定自动驾驶汽车程序更新升级许可制度。车辆升级后要获得许可，需同时满足“改造申请者”拥有国土交通省所要求的资质及能力与更新升级后的汽车符合安全标准这两个要求。不被许可的行为包括如果程序更新升级导致车辆不符合安全标准，该行为将会被列入改造通信电路的违法行为中。

(3) 汽车检查电子化。引入了车载式故障诊断装置（OBD）的检查方式。其次规定了应由“独立行政法人汽车技术综合机构”负责技术信息管理。同时，汽车技术综合机构将开发“特定故障代码（DTC）查询应用程序”。并将安装了“特定 DTC 查询应用程序”的“扫描工具”与汽车连接，读取 DTC 后，即可通过互联网与汽车技术综合机构的服务器连接，确定故障类型。

(4) 扩大车辆的检查和整修范围。一是将自动运行装置纳入检修范围，并将“解

体整修”改名为“特定整修”；二是只有得到地方交通局的资质认可的汽车修理商才能对自动运行装置进行维修；三是汽车生产厂商须向汽修商提供用以自动运行装置维修的技术信息。

#### 7、《自动驾驶的公共道路测试使用许可标准》

发布时间：2019 年 9 月。

主要内容：日本警察厅在《关于自动驾驶系统的公共道路测试指南》的基础上重新修订并发布了《自动驾驶的公共道路测试使用许可标准》。该标准将道路测试车辆细分为两类，包括自动驾驶系统控制的车辆以及远程遥控操作的车辆，其共性的要求涵盖以下三个方面：

（1）测试主体要求。一是测试机构必须向交管部门提供为保障安全而必需的相关材料，包括车辆合规文件以及交通事故等特殊事件发生时的应急预案以及联系方式。二是可申请多名测试驾驶人，但每部测试车辆的责任人限于其中一人。三是测试驾驶人必须接受过相关培训，其培训内容包含但不限于以下四点内容：认识到自己一直承担有法律上作为驾驶人的义务以及责任；掌握安全平稳地测试实验车辆的知识以及技能；掌握应对突发情况的相关知识以及技能；测试驾驶人所必须掌握的其他知识以及技能；同时，测试驾驶人须根据实验车辆的种类获得驾驶许可证。四是测试驾驶人在测试过程中必须严格按照下述四个规定执行：始终观察测试车辆周围以及行驶方向的状况，确认测试车辆状态，时刻保持应对紧急情况的状态；确保测试驾驶人在测试车辆行驶时，其视野以及操作不会受到干扰；有乘客时，测试驾驶人以及辅助人员需要确认乘客上下车情况；根据测试车辆的构造、性能、与申请日期以及测试道路情况使测试车辆安全地在公路行驶的其他必要措施。

（2）测试车辆要求。一是满足道路运行车辆的安保基准要求（昭和 26 年运输省第 67 号令）的规定。二是在进行公路测试时，在设想了可能产生的情况以及发生事态的基础上实验，且测试主体已经验证了测试车辆在实际道路中可安全地行驶；计划搭载乘客行驶时，已提前预测可能发生的情况，并采用了可确保乘客安全的措施。三是在实际的测试前，需要警员对车辆进行“公路审查”，即警员搭乘测试车辆，在车辆上路行驶过程中审核其安全性。其审查内容包括三点：在不同时间、不同交通环境、不同交通流量下开展测试；车辆全程自动驾驶，遵守相关法律规定，不得发生交通事故；确认测试驾驶人介入后，可完成测试车辆安全停车操作。

(3) 安全保障措施。一是原则上考虑车辆时速不超过 20 公里。二是车辆的正面、后面以及侧面均须在显著位置贴上“正在进行自动驾驶公路试验”的标识。三是针对测试过程中测试驾驶人急性发病以及车辆断电导致操作无法完成等紧急情况制定了应急预案。其方法涵盖但不限于以下三点：实验车辆可自动并安全地停驶；采用了可迅速地将测试任务转交给其他测试驾驶人的机制；采取了作为测试驾驶人的辅助人员，可按下测试车辆的紧急停驶按键的措施。四是测试车辆必须搭载数据存储设备，除了记录车辆前后方以及车室内状况及车辆状态信息，还需记录测试驾驶人的影像以及声音，与测试车辆相关的传感器收集到的相关信息等各种数据，并妥善保存，将其用于自动驾驶分析以及交通事故时回溯取证。五是发生交通事故时，为使交通，消防部门及时采取应对措施，需要提前向各部门报备，提交实验车辆的构造，停驶方法等必要信息。六是如果由于自动驾驶系统等问题发生交通事故，需要明确事故原因，并在制定防止类似事件发生的措施与预案的基础上，才能申请许可。七是测试主体测试前须和道路相关部门协商沟通，发生事故时迅速联系交管部门；在发生自动驾驶系统安全问题以及行驶中对他人造成不便等特殊事件时，在通报所辖警察部门时，还需上报防止事故再发的对策。

鉴于远程遥控自动驾驶汽车系统的远程操作特性，该许可标准针对性地制定了特别的标准要求，内容涵盖以下四个方面：

(1) 测试主体要求。一是原则上确保在电子通讯技术不会中断的，能满足远程测试车辆安全行驶通信要求的测试道路中进行；二是测试预案中应包含远程遥控自动驾驶系统发生问题，难以进行远程控制时，需安全地停驶并移动测试车辆的应对办法。

(2) 测试车辆要求。一是在通信应答超时的情况下，测试车辆可自动地安全停驶；二是测试车辆内须配备远程监控员的驾驶许可证的复印件；三是仅可使用远程遥控自动驾驶系统对测试车辆进行测试试验（测试驾驶人在车内时除外）。

(3) 道路安全保障措施。一是在限制最高时速 20 公里的同时，需要充分考虑通讯应答时间；二是以申请的最高速度行驶时，远程监控员应根据影像以及声音正确地把握测试车辆周围以及行驶方向的状况；三是计划搭载乘客行驶时，远程监控员可根据影像实时掌握车内情况，必要时可与测试车辆内的乘客通话；四是在远程遥控自动驾驶系统的测试中还应对通信记录进行保存。

(4) 信息安全保障要求。一是在信息安全基本法（平成 26 年法律第 104 号）等的基础上，为了安全地进行公路验证测试，需努力保障信息安全；二是远程监控员离开远程操作设备时，确保他人无法操作测试车辆。

#### 8、正在讨论修订的法律法规

##### (1) 《汽车损害赔偿保障法》

发布时间：正在讨论修改

在自动驾驶中，事故原因和责任关系相较传统车辆更加复杂。因此在发生事故时，相关法律法规有必要完善。根据国土交通省自动驾驶损害赔偿研究组 2018 年 3 月发布的报告，在使用自动驾驶系统期间发生事故情况下的“驾驶者责任”，将维持不变，另外充分保障保险人对汽车制造商的求偿权。

##### (2) 《无线电法》

发布时间：正在讨论修改

为促进包括自动驾驶的 5G 服务顺利应用，该修正案拟将未使用的无线电频段用于 5G，以避免线路拥堵。总务省拟于 2020 年向议会提交修正案。

## 2.3 欧洲自动驾驶汽车相关法规政策

### 2.3.1 概述

欧洲自动驾驶汽车采用“欧盟层面-国家层面”的两层管理模式。欧盟层面中，欧盟主要对欧洲自动驾驶汽车管理提出顶层设计。欧盟委员会成立的智能网联汽车协调小组作为牵头部门，由欧盟汽车行业竞争力与可持续增长高层小组研究宏观发展路线，制定目标。欧盟委员会内，市场与中小企业司负责车辆立法与知识产权；通信司负责协调电信部门；出行与运输司负责交通管理与道路安全；研究与创新司负责研究自动驾驶及其资金支持；气候行动司负责促进行业可持续发展。五大部门各司其职，制定相关政策。国家层面中，英国重视自动驾驶技术与产业的协同发展。英国交通部作为自动驾驶汽车的主要管理部门，配合商务与运输部，互联自动驾驶汽车中心以及法律事务委员会，共同引导自动驾驶产业安全快速发展。德国注重伦理道德引导，联邦政府作为牵头单位，组建智能网联汽车道德委员会，同时协调德国联邦经济和能源部，联邦交通和数字基础设施部在各自职责范围内实施工作。其中，由联邦交通和数字基础设施部负责修订德国《道路交通安全法》。荷兰对自动驾



驶汽车的管理分为国家与地方两个层面，国家层面由国家车辆管理局负责制定标准，统筹协调；地方层面由市政管理部门，封闭测试管理部门，地方道路管理局，地方警察局共同配合，协同管理。

目前，欧洲出台了多项针对自动驾驶汽车上路的法规政策。其中，欧盟层面以顶层设计的指南性文件为主，国家层面聚焦落地的法规规范。欧盟层面来看，欧盟从顶层设计角度出台多项宏观指南性文件，包括《通往自动化出行之路：欧盟未来出行战略》、《自动驾驶汽车的豁免程序指南》和《整车型式认证框架法规》(Regulation (EU) 2019/2144)，对其成员国的自动驾驶汽车产业发展、车型互认和技术标准提出要求。国家层面来看，德国、英国、荷兰等国都根据本国国情制定自动驾驶汽车的上路测试规范，部分国家通过颁布标准和法案等形式对自动驾驶汽车可能涉及的伦理道德和事故赔偿等内容进行规范。

### 2.3.2 特点分析

通过对欧洲现有自动驾驶汽车相关法规政策的概述，总结得到欧洲自动驾驶汽车法规政策有如下的特点：

1、采用两级管理模式。欧盟层面关注顶层设计，规范自动驾驶汽车安全测评，推动欧盟成员国简化涉及自动驾驶汽车的新车型相互认可流程。国家层面各国制定法案允许自动驾驶汽车上路测试，不同国家对测试的要求差异较大。

2、注重伦理道德问题。欧盟层面鼓励成员国根据 2019 年颁布的《欧盟人工智能道德准则》来应对自动驾驶的潜在伦理问题。德国《自动驾驶技术伦理道德标准》明确对人的保护优先于其他利益，并且强调自动驾驶的首要目标是提升所有交通参与者的安全，同时关注弱势群体权益和用户数据隐私。

3、自动驾驶系统尚未取得合法地位。尽管欧洲很多国家已经开展自动驾驶汽车上路测试，但是除德国通过修法明确自动驾驶系统具有驾驶机动车的合法地位外，其它国家尚未赋予自动驾驶系统取代有资质的人类驾驶人的合法性。

### 2.3.3 主要内容

近 5 年来欧洲自动驾驶汽车相关的法规政策文件发布推进情况如表 3 所示。

表 2-3 欧洲近 5 年自动驾驶汽车相关法规政策汇总表

序号	法规政策名称	发布时间
----	--------	------

1	《通往自动化出行之路：欧盟未来出行战略》	2018 年 3 月
2	《自动驾驶汽车认证豁免程序指南》	2017 年 6 月
3	《整车型式认证框架法规》（Regulation （EU） 2019/2144）	2019 年 12 月
4	《道路交通法律修正案》	2017 年 6 月
5	《自动驾驶技术伦理道德标准》	2018 年 5 月
6	《通往无人驾驶之路：自动驾驶汽车测试实践准则》	2015 年 7 月
7	《联网和自动驾驶汽车网络安全关键原则》	2017 年 8 月
8	《自动与电动汽车法案》	2018 年 7 月
9	《例外运输豁免法令》	2015 年 6 月
10	《自动驾驶汽车实验法》	2019 年 7 月
11	《自动驾驶公共道路测试规范》	2017 年 7 月

下面对表 2-3 中欧洲自动驾驶相关的法规政策进行介绍。

#### 1、欧盟《通往自动化出行之路：欧盟未来出行战略》

发布时间：2018 年 3 月。

主要内容：该战略对网联和自动驾驶车辆提出全面的欧盟方案，并确定了用于开发和部署的关键技术，服务基础架构的支持措施。确保欧盟法律和政策框架准备就绪，以支持网联和自动驾驶车辆的安全部署。

#### 2、欧盟《自动驾驶汽车认证豁免程序指南》

发布时间：2019 年 4 月。

主要内容：该指南重点关注 L3 和 L4 级自动驾驶的汽车，实现协调欧盟成员国之间简化涉及自动驾驶汽车的新车型相互认可流程，确保公平竞争和透明度的目的。

（1）对互相认可流程的要求。一是自动驾驶汽车制造商应向欧盟成员国的型式核准机关提出申请；二是该成员国批准在其境内有效的车辆类型后，通过文件通知欧盟机动车技术委员会和其他成员国；三是车辆技术委员会通过一项实施法案决定是否允许该成员国就该类型车辆给予欧共体类型批准（将临时批准转换为欧共体批准）；四是在委员会作出决定之前，其他会员国可自行决定在其领土上是否接受第 2

款所述的临时许可；五是在型式批准机关解释新车型与已获豁免的车型之间区别的简化文件基础上，由委员会提出的另一项决议对已获批豁免的技术范围进一步扩展。

(2) 对安全的要求。一是制造商应向审批机构申报自动驾驶汽车操作设计域的范围，包括道路类型、速度、地理区域、时间等；二是车辆在自动驾驶状态下不得造成能够合理预见和预防的交通事故；三是自动驾驶汽车应遵守交通规则。

(3) 对司机/运营商/乘客互动要求。一是只有满足操作设计域条件时，才能激活自动驾驶模式，应向人员（司机或无司机、乘客或操作控制中心）提供轻松地立即停用或撤销自动模式方法，当即时的系统停用可能危及安全时，系统可能会暂时延迟停止。二是车辆应以明确的方式告知司机（或操作负责人）或乘客系统的操作状态（操作、故障等）。三是司机应了解自动驾驶模式的使用和限制，以及系统可能会为司机启用哪些驾驶以外的任务。四是如果系统的设计目的是在某些情况下要求驾驶人接管，则系统应监视驾驶人是否准备好从系统接管驾驶，通过适当的设计（驾驶人监控系统等）和警告，确保驾驶人可随时响应接收请求，防止驾驶人在操作设计域中出现任何可预见和可预防的误用。五是对于设计为在没有驾驶人的情况下运行的车辆，应提供通信功能，向运行控制中心发送紧急通知。车辆内须设有摄影机及话音通讯装置，以便操作控制中心监察车辆内的情况。

(4) 对驾驶任务的过渡的要求。一是当确定难以继续自动驾驶模式时，系统会要求司机在足够的准备时间内接管车辆；二是自动驾驶汽车须按照适用的交通规则（例如危险灯、刹车灯、转向指示灯）告知其他道路使用者下一步意图。

(5) 对最小风险策略的要求。一是当系统发现难以继续在自动驾驶模式下驾驶时，应能够通过最低风险操作，将自动驾驶汽车转移至最低风险状态；二是只要司机没有接管，系统将保持自动驾驶模式，并将以其他方式转移到最低风险状态。

(6) 对事件数据记录装置的要求。自动驾驶汽车应安装车载装置，记录自动驾驶系统的运作情况及司机的操作情况，以确定谁在事故中操作车辆。需记录的数据包括：自动驾驶系统的运行状态、驾驶人的状态、周围环境信息、车辆的控制信息等。

(7) 对安全评估和测试的要求。自动驾驶汽车及其系统、组件和技术单位应在最大程度上遵守现有欧盟安全法规 2007/46/EC。型式批准机关评估制造商已经对自动化系统的目标建立完善的设计和验证过程，确保车辆不会导致事故且能够提供最

小风险策略。型式批准机关应根据制造商的安全评估报告，对其进行测试、验证和评估，以确定其安全性能。制造商应特别证明其已对自动化系统进行了安全风险分  
析，并将其整合到整体车辆设计和更广泛的交通生态系统中，并提供系统冗余设计  
以应对安全风险。所有设计决策应由制造商作为单个子系统和整个车辆体系结构  
的一部分进行测试、验证和验证。

### 3、欧盟《整车型式认证框架法规》

发布时间：2019 年 12 月

主要内容：该法规对车辆安全技术要求对应的类型、适用技术法规、适用车型  
等做出了清晰的定义。除去车型必须满足的一般安全技术要求，胎压监测系统要求，  
先进车辆技术要求外，对于乘用车、轻型商用车，大巴、卡车、新能源汽车、自动  
驾驶汽车等车型需要额外满足的安全要求也做出了详细的规定。

(1) 一般技术要求。一是制造商应当证明投放市场或服务的所有新车型、新系  
统、组件和独立的技术单元都必须符合法规要求；二是制造商须确保车辆在设计、  
建造及组装时，尽量减少对车辆使用者及其它道路使用者的伤害；三是制造商应确  
保车辆、系统组件和独立的技术都符合技术标准的需求，包括：

- 1) 制动系统、碰撞试验、燃料系统完整性和电气安全；
- 2) 易受影响的道路使用者、视力和能见度；
- 3) 车辆底盘、刹车、轮胎和转向系统；
- 4) 电力系统、车辆照明及防止未经许可的使用；
- 5) 驱动程序和系统行为；
- 6) 车辆的一般构造和特征。

(2) 适用于所有机动车辆类别的先进车辆系统要求。该法规规定了先进车辆系  
统安全技术要求，包括：智能速度辅助、酒精锁安装便利化、驾驶人疲劳和注意力  
警报、驾驶人注意力分散自动警报系统、驾驶人可用性监测系统、事件数据记录系  
统等。

### 4、德国《道路交通法律修正案》

发布时间：2017 年 6 月。

主要内容：将自动驾驶相关概念及规定引入已于 1909 年 6 月 1 日生效的《道路  
交通法》中，规定在特定时间和条件且有驾驶人监督的情况下，高度或全自动化驾



驶系统可接管驾驶人对车辆的控制权。

(1) “高度或全自动化汽车”的定义。高度或全自动化汽车同时具备以下五种特性的技术设备的汽车：

- 1) 可执行自动驾驶功能（包括纵向与横向控制）；
- 2) 能够在高度或全自动化控制驾驶时遵守交通法规；
- 3) 驾驶人可在任何时候手动控制或停止该技术设备；
- 4) 驾驶人可意识到亲自控制汽车的必要性；

5) 能够将驾驶人亲自控制汽车的要求通过可视、可听或者可触及的方式及时呈现给驾驶人。

(2) 对驾驶人责任的要求。在以下情况中，驾驶人有义务立即接管对车辆的控制：一是当高度或全自动化系统要求其接管时；二是当驾驶人意识到或者基于常识应该意识到车辆已不再具备高度或全自动功能的预设运作条件时。

(3) 对事故的赔偿额度的要求。因高度或全自动化汽车的系统故障而导致在事故中人员伤亡的，受害者可获得最高损害赔偿金额为一千万欧元，比目前适用的驾驶事故最高赔偿额高出了一倍。该调整致力于更好地保护与高度或全自动化汽车相关的事故受害者。

(4) 对驾驶数据记录的要求。载有高度或全自动化功能的汽车必须根据通用的国际技术标准来记录汽车在某一时刻究竟由驾驶人控制，还是由高度或全自动化功能控制，即所谓的“黑匣子”记录功能。如果高度或全自动化系统已要求驾驶人接管汽车的控制，或者该系统出现了技术障碍，也将立即生成一条相应的技术状态记录。上述数据应根据主管的道路交通监管部门的要求依法提交，并且该部门有权保存和使用相关数据。但数据的提交应限制在前述部门为实施相应监控目的的必要范围内。此外，数据的保存时效也需满足特定要求，在发生交通事故的情况下需保存三年。

## 5、德国《自动驾驶技术伦理道德标准》

发布时间：2018年5月。

主要内容：由多名科学家与法律专家组成的专家组制定道德准则供汽车行业在研发自动驾驶系统时使用，明确自动驾驶汽车针对事故场景决策的优先级，并要求将这些规则开发到自动驾驶系统中。

- 1) 该准则的第一必要条件是保证自动驾驶系统要比人类驾驶人更安全；

- 2) 人的安全必须优先于其他财产；
- 3) 当自动驾驶汽车发生不可避免的事故时，任何基于年龄，性别，种族，身体属性或任何其他区别因素的歧视判断都是不允许的；
- 4) 在任何驾驶情况下，无论驾驶者是人类还是自动驾驶系统，都必须遵守已经明确的道路法规；
- 5) 为了辨明事故承担责任方，自动驾驶汽车必须配置持续记录和存储行车数据的“黑匣子”；
- 6) 自动驾驶汽车将对所记录的行驶数据保留唯一所有权，其可决定是否由第三方保管或转发；
- 7) 虽然车辆在紧急情况下可能会自动决策，但人类应该在更多道德模棱两可的事件中重新接管车辆的控制权。

#### 6、英国《通往无人驾驶之路：自动驾驶汽车测试实践准则》

发布时间：2017 年 7 月。

主要内容：该准则鼓励和推动此自动驾驶新技术在道路交通中的应用，确保高度/完全自动驾驶汽车在公共道路上测试工作和未来市场应用的安全和规范。

(1) 对道路测试安全的要求。一是测试主体有责任且应当采取所有合理措施，最大限度地减小道路测试带来的潜在风险，不得妨害其他道路使用者的安全。二是测试主体应当确保测试操作符合现有法律，测试车辆应符合英国现行的机动车安全技术标准。三是测试主体应制定详细的测试工作流程，保证测试驾驶人能保持足够警惕，履行职责，不疲劳操作，同时规范测试驾驶人行为。工作流程应设定测试驾驶人每天测试累计时间或每次测试的最长时间。四是测试主体应向当地警方登记备案测试车辆。五是测试主体应当按照机动车保险有关规定，对测试车辆和测试驾驶人进行投保。六是在公共道路上开展测试时，测试机构应与当地应急救援部门、警方和消防部门进行沟通确保在展开调查时能够协同工作。七是在测试过程中如需要交通信号灯等交通基础设施协同测试，应获得相关职能部门（如警方或公路部门）的许可。八是在测试过程中，测试驾驶人应当注意驾驶行为和形象（比如应持续保持正常行驶时的视线方向），避免影响甚至惊吓其他交通参与者。九是测试机构对在测试过程中的测试驾驶人行为和位置数据的收集和分析，应当遵守英国数据保护相关法规，并酌情考虑进行隐私评估。

(2) 对测试车辆的要求。一是测试车辆应当遵照英国道路交通安全法规并符合现行的机动车安全技术标准。对车龄 3 年以上的测试车辆还需通过机动车运行安全性能检验。对申请上公共道路测试的，测试车辆应当先在封闭场地完成测试工作。二是测试机构应当评估测试车辆在公共道路测试的安全性，确保测试车辆不会对其它交通参与者带来危险或影响。三是自动驾驶系统发生故障或失灵时，测试车辆应当以声音警报和视觉警报提示驾驶人。当自动刹车和变向系统失灵时，测试车辆应确保驾驶人依旧能够进行手动刹车和变向。四是测试车辆应当安装行车记录仪，用于采集和存储车辆传感器和控制系统的数 据，至少记录车速、方向、转向、制动、灯光、驾驶模式状态以及可能影响车辆运动的控制命令等信息。测试机构应当向政府提供数据报告，用于确定事故发生时的车辆控制状态。五是测试机构可在测试车辆上安装视频和音频记录系统，但不能替代行车记录仪。六是汽车制造商（设备供应商）应确保自动化控制设备和自动驾驶系统有内置的安全防护，有效防止网络非法入侵。七是自动驾驶/手动驾驶模式间的切换应当快捷简便，切换操作流程应当清晰易懂，手工/自动驾驶模式状态指示应当明确。八是安装和运行在测试车辆上的自动驾驶系统各个版本软件都应当完整归档和记录。要求所有版本软件均经过了广泛的模拟测试，然后进行封闭道路或专用场地测试，最后才能进行公共道路测试。

(3) 对测试驾驶人的资质要求。一是测试驾驶人应持有相应准驾车型的英国驾驶执照或等效资质，具备该车型的多年驾驶经验，且没有任何危险驾驶劣迹或潜在倾向的历史记录。二是测试驾驶人通过了测试机构的专业培训和授权，且已在封闭道路和专用车道上进行了大量测试。同时，测试机构应制定稳妥的风险管理、风险处理和培训流程，而传统的人工操控和自动模式间的切换过程操作是培训重点。三是测试驾驶人应当熟悉并理解自动驾驶系统的功能及其局限性，能够判断何时需要人工接管车辆。测试驾驶人在手动模式和自动驾驶模式下均有责任保证车辆的安全运行。四是不论测试车辆在自动驾驶模式、还是在手工驾驶模式下，必须遵守现行道路交通安全法规（包括禁止使用手提电话、其他手持设备，以及限速、禁停、饮酒和药物限制等要求）。五是如果在公共道路上测试的车辆属于传统汽车加装自动驾驶技术的改装车辆，还应配备辅助人员协助测试驾驶人监控与自动驾驶运行有关的数字信息显示屏或相关信息反馈系统。

## 7、英国《联网和自动驾驶汽车网络安全关键原则》

发布时间：2017 年 8 月。

主要内容：本指南提出 8 项联网和自动驾驶汽车网络安全相关的关键原则，用来指导汽车行业中的设计师、工程师、供应商、企业高级管理人员等从各自的角度确保自动驾驶汽车的网络安全。

(1) 在董事会层面就应该开始重视和管理网络安全问题。一是必须有一个与公司的使命和目标相一致的网络安全计划；二是产品和系统安全的责任由董事会负责；三是加强网络安全意识并开展相关的培训，以确保员工理解其在 ITS/CAV 系统网络安全中所担负的角色和责任；四是开发 ITS/CAV 系统时遵循网络安全设计原则，并将网络安全的所有方面（物理、人员和网络）集成到产品和服务开发过程中。

(2) 包括供应链在内的各公司需提前对安全风险进行评估和管理。一是公司必须对当前相关的安全风险有一定的认识，以便在工程实践中解决安全风险；二是公司与第三方合作，以提高对网络安全风险的认识和解决能力；三是安全风险评估及管理程序已在公司内实施，制定识别、分类、优先处理安全风险（包括来自网络的风险）的适当流程；四是通过设计、规范和采购实践，识别和管理特定于供应链、分包商和服务提供商所存在的安全风险。

(3) 确保网络安全系统在整个周期中都是安全的，确保售后服务和事件响应的及时跟进。一是公司应计划如何在其系统的生命周期内维护网络安全；二是必须有安全策略来应对网络安全风险；三是公司确保系统能够支持数据取证和数据恢复。

(4) 包括承包商、供应商和潜在的第三方在内的所有组织，都应齐心协力提高系统安全性。一是包括供应商和第三方在内的组织必须能够对其流程和产品（物理、人员和网络）提供安全保证，例如独立的验证或认证；二是确定和验证供应链内所有供应品的来源的真实性；三是组织共同规划系统如何安全可靠地与外部设备、连接、服务、操作或控制中心交互；四是组织识别和管理外部依赖关系，当传感器或外部数据的准确性或可用性对自动化功能至关重要时，还必须采用二次测量。

(5) 系统的设计使用了深入防御的方法。一是系统的安全性不依赖于单点故障、模糊的安全性或任何不能被轻易改变的功能；二是安全体系结构采用深度防御和分段技术，寻求通过诸如监视、警报、隔离、信任层/边界和其他安全协议等辅助控制来降低风险；三是必须在整个系统中设置用于跨信任边界中间事务的设计控件。这些包括最小访问原则、单向数据控制、全磁盘加密和最小化共享数据存储；四是远



程和后端系统可能提供对系统的访问，这些系统具有适当级别的保护和监视，以防止未经授权的访问。

(6) 所有软件的整个生命周期都应该得到管理。一是机构采用安全编码实务，按比例管理软件内已知及未知的漏洞所带来的风险；二是必须能够确定所有软件、固件及其配置的状态，包括所有软件组件的版本、修订和配置数据；三是可以安全地更新软件，并在软件损坏时将其恢复到良好状态；四是软件采用开放的设计实践，源代码可以在适当的地方共享并尽可能邀请同行评审的代码。

(7) 保证数据的存储和传输是安全可控的。一是在存储和传输数据时，数据必须足够安全，以便只有预期的接收方或系统功能能够接收或访问数据；二是个人身份数据必须妥善管理；三是用户可以删除系统和连接系统上的敏感数据。

## 8、英国《自动与电动汽车法案》

发布时间：2018 年 7 月。

主要内容：该法案对自动驾驶汽车发生事故后保险理赔和事故责任给出详细的规定。根据法案规定，车辆在自动驾驶状态下发生事故后，根据车辆是否投保，分别由保险公司和车主对事故造成的损失承担赔偿责任。同时，法案还规定了保险人和车主的责任减免条款和追偿制度。

(1) 保险公司承担理赔责任的条件。一是自动驾驶汽车在道路或其他公共场所进行自动驾驶时发生事故；二是车辆在发生事故时已经投保；三是被保险人或其他人因事故而遭受损失。

(2) 车辆所有人对事故承担责任的条件。一是自动驾驶汽车在道路或其他公共场所进行自动驾驶而发生事故；二是在事故发生时车辆未投保；三是《1988 年道路交通安全法》第 143 条（机动车使用者需投保第三者责任险）的规定由于如下原因而不能适用：该车辆由公共机构（如地方当局、警察机构、卫生当局等）所有，或该车辆在从事政府公共服务；四是有人因事故而遭受损失。

(3) 共同过失条款，对保险人或车主所承担的责任进行减免。一是当保险人或车主按照规定对自动驾驶汽车发生的事故承担法律责任，且事故或损害在一定程度上是由受损害方所造成的情况下，根据《法律改革（混合过失）法》（Law Reform (Contributory Negligence) Act），可以在相应程度上减免保险人或车主的责任；二是当事故的发生是完全由于车辆控制者在不适宜的情况下进行自动驾驶所导致时，

则保险公司或车主无需向车辆控制者负法律责任。

(4) 违反规定更改软件、不更新软件造成的事故的保险责任豁免。一是被保险人或者在被保险人同意的情况下对软件做了保险条款所禁止的更改；二是未能安装与安全紧密相关的软件更新，且被保险人明知或应知该软件更新是与安全紧密相关的。根据法案规定，所谓安全紧密相关是指，如果在没有安装软件更新的情况下，对自动驾驶汽车的使用是不安全的，那么，该软件更新就是安全紧密相关的。

(5) 保险公司或车辆所有人的追偿权。根据法案第 5 条规定，在保险公司或车辆所有人依照法律对自动驾驶汽车造成的事故承担责任，且责任程度已经确定的情况下，对事故发生负有责任的第三人需向保险公司或车辆所有人负同等责任。

#### 9、荷兰《例外运输豁免法令》

发布时间：2015 年 6 月。

主要内容：规定了广泛的豁免申请范围，授权国家车辆管理局制定具体要求，相关公司申请道路测试豁免，经过国家车辆管理局审批后，允许自动驾驶汽车在公共道路测试。

(1) 对影响自动驾驶技术发展的条款进行豁免。一是豁免 1994 年《道路交通安全法》第 7 条驾驶人禁止离开事故现场的规定；二是豁免 2000 年《出租车运输法》第五章关于出租车运输相关的规定；三是豁免《道路货物运输法》第 2.11 条，由承运人雇用货车司机进行专业运输。

(2) 针对自动驾驶汽车测试进行了详细的规定。包括测试的目的、测试的路段路线和测试时间段。

#### 10、荷兰《自动驾驶汽车实验法案》

发布时间：2019 年 7 月。

主要内容：该法案规定了严格的自动驾驶汽车公共道路测试豁免审批流程，允许相关企业在特定路段和条件下远程对自动驾驶汽车开展公共道路测试。

(1) 规定了严格的自动驾驶汽车公共道路测试豁免审批流程。荷兰车辆管理局需要向基础设施和环境部长提交一份有关开展自动驾驶汽车公共道路测试的安全评估报告。经过安全评估后，由基础设施和环境部长对自动驾驶汽车开展公共道路测试的豁免进行许可，如果部长认为相关道路测试存在安全风险，则可以撤销豁免。

(2) 法案规定了申请人在申请豁免时提供文件和数据的详细规则。包括以下内

容：

1) 测试目的；

2) 测试的路段路线；

4) 豁免期限；

5) 为了进行实验而应采取确保道路安全、保护道路使用者和乘客、维护道路并保证其可用性、尽可能确保行动自由的安全措施；

6) 控制位置，设备和方法，并监督执行本法律领域任务的独立行政机构。

11、瑞典《自动驾驶公共道路测试规范》

发布时间：2017 年 7 月。

主要内容：对自动驾驶汽车实验法案行许可制；现行交通事故赔偿条款仍然适用于自动驾驶情况；测试单位需确保测试数据采集、保存符合国际相关法规，并且保护个人隐私信息。

## 2.4 我国自动驾驶汽车相关法规政策

### 1、智能汽车创新发展战略

《战略》提出，到 2025 年，我国标准智能汽车的技术创新、产业生态、基础设施、法规标准、产品监管和网络安全体系基本形成。具体包括，实现有条件自动驾驶的智能汽车达到规模化生产，实现高度自动驾驶的智能汽车在特定环境下市场化应用。智能交通系统和智慧城市相关设施建设取得积极进展，车用无线通信网络（LTE-V2X 等）实现区域覆盖，新一代车用无线通信网络（5G-V2X）在部分城市、高速公路逐步开展应用，高精度时空基准服务网络实现全覆盖。

展望 2035 到 2050 年，中国标准智能汽车体系全面建成。

同时，还要重点研发虚拟仿真、软硬件结合仿真、实车道路测试等技术和验证工具，以及多层级测试评价体系。建立健全智能汽车测试评价体系及测试基础数据库。此外，还要开展特定区域智能汽车测试运行及示范应用，验证车辆环境感知准确率、场景定位精度、决策控制合理性、系统容错与故障处理能力，智能汽车基础地图服务能力，“人-车-路-云”系统协同性等。

### 2、交通强国建设纲要

《纲要》提出，加强智能网联汽车（智能汽车、自动驾驶、车路协同）研发，形成自主可控完整的产业链。完善预防控制体系，有效防控系统性风险，建立交通

装备、工程第三方认证制度。强化安全生产事故调查评估。完善网络安全保障体系，增强科技兴安能力，加强交通安全综合治理，切实提高交通安全水平。



### 第3章 国内外智能网联汽车预期功能安全相关标准

自动驾驶汽车既是车辆又是驾驶人，最终实现完全替代驾驶人的机器自主驾驶，因此必须同时担负车辆和驾驶人的各种安全责任。自动驾驶汽车安全贯穿车辆设计、研发、测试、生产、使用、维护等全生命周期，通过设计实现安全，并通过交通场景验证和确认从而改善安全。自动驾驶汽车预期功能安全主要体现在汽车行驶过程中，可避免自动驾驶系统及部件因功能不足或误操作引起的交通安全问题，包括自动驾驶能力，以及适用性和可靠性。针对自动驾驶汽车预期功能安全，国内外已有一些深入研究，并提出了具体要求。本章在此背景下，对国内外智能网联汽车预期功能安全相关标准进行概述和分析，在此基础上，分析智能网联汽车预期功能安全相关标准的发展现状及发展趋势。

#### 3.1 国外智能网联汽车预期功能安全相关标准

表 3-1 总结了当前国外智能网联汽车预期功能安全相关标准情况。

表 3-1 国外智能网联汽车预期功能安全相关标准

标准/法规	名称
ECE 法规	Automated Lane Keeping System (ALKS) 自动车道保持系统的交通干扰临界场景指南
ISO 34501	Road Vehicles - Terms and Definitions of Test Scenarios for Automated Driving Systems 道路车辆-自动驾驶系统测试场景的术语和定义
ISO 34502	Road vehicles - Engineering framework and process of scenario-based safety evaluation 道路车辆-基于场景安全评估的工程框架和过程
ISO 34503	Road vehicles – Taxonomy for Operational Design Domain for Automated Driving Systems 自动驾驶系统的设计运行域分类
ISO 34504	Road vehicles - Scenario categorization and technical realization using standards 道路车辆-场景归类和技术实现应用标准
ISO/NP 34505	Road vehicles- evaluation of Test Scenario

	自动驾驶系统的测试场景评测
ISO/TR 4804	Road vehicles - Safety and cybersecurity for Automated driving systems - Design, verification and validation 道路车辆-自动驾驶系统的安全和网络安全-设计，检验和验证。#基于百度自动驾驶安全第一白皮书
美国交通部	Intelligent Transportation System Joint Program Office – Strategic Plan 2020-2025 智能交通系统战略规划 2020 -2025
UL 4600	Safety for the Evaluation of Autonomous Products 自动驾驶产品安全评价标准
ISO/PAS 21448	Road vehicles — Safety of the intended functionality 道路车辆-预期功能安全
BSI PAS 1880	Developing and accessing control systems for automated vehicles
BSI PAS 1881	Assuring the safety of automated vehicle trials and testing – Specification 确保机动车试验和测试的安全性
BSI PAS 1882	制定中
BSI PAS 1883	The operational design domain (ODD) 运行设计域

下文将针对表 3-1 中的典型相关标准进行阐述。

## 1、UL 4600 《自动驾驶产品安全评估标准》

### (1) UL 4600 的核心内容

UL 4600 关注车辆的智能化演变，制定过程中以驾驶系统没有驾驶人为预期假设。通过要求自动驾驶研发、制造厂商建立安全案例来证明系统的安全性，其类似于自动驾驶系统开发过程中的安全指导书或安全规范。主要用于解决当人类完全从自动驾驶项目操作的执行层面、监督层面撤出后所带来的其它问题。UL 4600 中的安全案例包括目标、论据和证据 3 个要素。遵循最低接受标准、使用反馈、提供提

示、可重复评估、接受不确定性等 5 个关键准则。

## (2) UL 4600 的创新点

和传统标准相比，UL 4600 有两个显著的创新点。一是面向高等级自动驾驶。相较传统标准以人类驾驶人为责任主体的制订思路，UL 4600 抛开人类驾驶人的研究角度，完全以无人驾驶车辆安全需求作为假设开展安全标准的研究制订，侧重于无人人类驾驶人干预的完全自动驾驶安全风险评估。二是通过案例验证安全。UL 4600 不是对安全进行逐条验证，而是通过大量的案例来检验安全性。案例范围涵盖自动驾驶的控制、路径规划、感知、操作、系统周期等方面，并且吸纳其他标准的成熟案例丰富自身。

## 2、ISO/PAS 21448

预期功能安全（SOTIF）是汽车行业的一个新兴概念，全称为 Safety Of The Intended Function，以此概念为核心的标准草案 ISO/PAS 21448 于 2019 年 5 月份发布。

ISO/PAS 21448 旨在为避免因自动驾驶汽车整车及系统的非失效、预期功能局限、合理可预见的误用所引起安全风险，从整车层面、系统层面、软硬件层面及不同系统组件层面如感知、决策、执行提供了针对预期功能的风险识别、分析和设计方法，通过基于对已知不安全场景和未知不安全场景的预期功能安全验证和确认，探测和发现不同层面及系统组件中的功能不足并进行改进，使自动驾驶汽车在预期使用工况下达到合理安全水平。该标准对于不同自动驾驶等级车辆的设计开发具有重要指导意义。

自动驾驶汽车能否安全上路行驶及真正意义上走向量产的关键是能否满足并实现功能安全及 SOTIF 技术要求，同时，也是自动驾驶汽车研发过程中最复杂、最急需突破解决的难点，对于自动驾驶汽车而言，除考虑系统故障引发的安全风险，更应考虑系统功能不足、人机及外界交互等导致的更大安全风险。

## 3、《自动驾驶安全第一白皮书》白皮书

由英特尔、奥迪和大众等 11 家公司组成的团队，共同发布了《自动驾驶安全第一白皮书》的白皮书，作为设计和开发自动驾驶汽车的指南。提出了表 3-2 中的 12 个指导原则，详细说明了自动驾驶汽车在被视为“安全”之前必须具备的能力。

表 3-2 《自动驾驶安全第一白皮书》白皮书 12 个指导原则

1. 设计运行域	自动驾驶系统应考虑运行设计域（Operational Design Domain, ODD）的典型情况，解决可能的风险；当系统超出了设计运行域时，应向驾驶人发出接管请求，并预留足够的时间。
2. 交通行为	自动驾驶汽车的行为不仅需要便于其他交通参与者理解，还需要可预测和管理，且遵守适用的交通法规。
3. 安全层	自动驾驶系统应能识别系统的局限，尤其是不能将控制权安全转移给驾驶人的情况，并采取相应措施将风险降到最低。
4. 安全保护	当提供自动驾驶系统时，应采取错误避免自动驾驶系统受到安全威胁。
5. 安全运行	当与安全相关的功能或系统组件发生故障时（如不可使用），自动驾驶系统应有能力补偿，或将系统转移到安全的状态/地方；当车辆控制权转移到驾驶人时，应确保有足够的时间。
6. 自动驾驶系统移交控制权	当驾驶人没有响应车辆移交控制权的请求时，自动驾驶系统必须采取能够最大限度降低风险的动作，该动作取决于当时的环境和自动驾驶系统的性能。车辆移交控制权的请求应清晰易懂，便于驾驶人操作。
7. 驾驶人主动接管控制权	驾驶人和自动驾驶系统有明确的交互机制，使自动驾驶系统接管和释放控制权。
8. 驾驶人和自动驾驶系统的相互依存关系	系统安全性的整体评估需要考虑自动驾驶系统对驾驶人对驾驶人的影响，包括自动驾驶系统把控制权刚移交到驾驶人手中。
9. 用户责任	为了提高安全性，控制权转给驾驶人时，必须考虑驾驶人的状态（是否处在可接管控制权的状态）。系统能够识别驾驶人的状态，告知相关任务的职责。在自动驾驶状态下也需告知驾驶人安全相关的驾驶情况。

10. 数据记录	车辆应记录与自动驾驶驾驶状态相关的数据，并遵守相关数据隐私的法律。
11. 被动安全	针对自动驾驶汽车特有的碰撞情况，车辆的布局应采取适应的修改。
12. 安全评估	应用验证和确认步骤来确保达到安全目标，实现整体安全的持续改进。

### 3.2 国内智能网联汽车预期功能安全相关标准

国内现有智能网联汽车预期功能安全相关标准如表 3-3 所示。

表 3-3 国内智能网联汽车预期功能安全相关标准

标准/法规	名称
	智能网联汽车道路测试管理规范（试行）
	预期功能安全双层接受准则提案
CAICV	智能网联汽车自动驾驶功能测试规程（试行）
i-VISTA	智能行车辅助试验规程
i-VISTA	智能行车辅助评价规程
i-VISTA	智能泊车辅助试验规程
i-VISTA	智能泊车辅助评价规程

如表 3-3 所示，国内目前针对预期功能安全的相关标准体系还不完善，以下将针对《智能网联汽车道路测试管理规范（试行）》以及由我国提出的预期功能安全双层接受准则提案（即将写入道路车辆预期功能安全标准）进行阐述：

#### 1、《智能网联汽车道路测试管理规范（试行）》

2018 年 4 月，工业和信息化部、公安部、交通运输部联合发布《智能网联汽车道路测试管理规范（试行）》。《管理规范》主要针对在中国境内公共道路上进行的高等级自动驾驶汽车上公共道路测试，从测试主体、驾驶人及测试车辆、测试申请及审核、测试管理、交通违法和事故处理等多个方面进行规范。《管理规范》强调，自动驾驶汽车必须通过 14 项自动驾驶能力检测项方可上公共道路测试。

表 3-4 智能网联汽车自动驾驶功能检测项目



序号	检测项目
1	交通标志和标线的识别及响应
2	交通信号灯的识别及响应*
3	前方车辆（含对向车辆）行驶状态的识别及响应
4	障碍物的识别及响应
5	行人和非机动车的识别及响应*
6	跟车行驶（包括停车和起步）
7	靠路边停车
8	超车
9	并道行驶
10	交叉路口通行*
11	环形路口通行*
12	自动紧急制动
13	人工操作接管
14	联网通讯*

\*注：标注\*的项目为选测项目。

## 2、预期功能安全双层接受准则提案

中国代表团提出量化思想的预期功能安全双层接受准则提案，写入 ISO/PAS 21448 标准草案，包括：

（1）第一层准则：判断自动驾驶行为是否可能引发危害行为事件的度量，即危害行为事件接受准则

（2）第二层准则：在全部行驶里程中，定义总的危害行为事件确认目标，即总体安全风险接受准则

在工信部专项任务支持下（工装函[2016]190号），集行业力量启动可控性国家级研究项目，基于大规模测试建立可控性量化指标库，准确性领先国际现有方法（经验和主观评测），并不断完善，GB 17675、GB 21670 等标准首次写入可控性量化要求。在第一层接受准则的建设中首次提出了“SOTIF 信心度”的度量，建立信心度指标体系，全面衡量自动驾驶安全行为。行业率先将大数据用于可控性研究，采集分析真实测试者“典型”和“极端”工况指标，大数据持续采集，不断提升可控性指标的

准确性和国情代表性。第二层接受准则的建立，假定同等驾驶条件下，与人类驾驶人的安全驾驶能力指标相比，引入自动驾驶后相关指标不变低，则认为自动驾驶系统没有带来明显的不合理风险水平，并基于以上两个接受准则，提出了相应的测试方法实践。

### 3.3 智能网联汽车预期功能安全标准的发展现状及趋势

ISO 26262 的第二次修订已经结束，以更严谨和结构化的方式支持更复杂汽车电子系统。最近发布的 ISO/PAS 21448 标准规定了用于分析、验证和确认非故障情景的开发流程和系统用例。《自动驾驶安全第一白皮书》白皮书将标准拓展至 L3 和 L4 应用。上述标准相互补充，可主要用于定义自动驾驶系统的设计风险，使工程团队设计出各种安全机制并增强自动驾驶系统的预期功能，以降低所识别的风险。

当前，ISO 正组织国际主流车企及供应商开展国际标准道路车辆预期功能安全的研究和制定工作。中华人民共和国工业和信息化部于 2018 年发布了《国家车联网产业标准体系建设指南（智能网联汽车）》以整体性强化顶层系统设计并促进智能网联汽车行业的研究和发展。另外，中国正在密集地制定新的法律规范（2020 年前 30 项新标准，2025 年前 100 项新标准）以适应中国的国情和国际实践。我国在积极参与该国际标准制定的同时，将基于我国实际情况制定适合中国的道路车辆预期功能安全国家标准，进一步增强我国在国际标准制定中的话语权，同时提升我国自动驾驶汽车产业技术安全水平。

## 第4章 国内外智能网联汽车预期功能安全相关技术

预期功能安全是智能网联汽车安全的重要组成部分，主要应对由于自动驾驶功能不足和可合理预见的人为误用造成的危害问题。现有关于智能网联汽车预期功能安全的国际标准草案 ISO/PAS 21448 规范和描述了一个基于迭代的系统分析流程，用于系统识别、分析、减少功能不足造成的危害。与此同时，国内外科研机构和汽车厂商对涉及智能网联汽车关键系统的预期功能安全问题开展了研究。本章分别综述了智能网联汽车感知、环境预测、决策、控制和人机交互面临的预期功能安全挑战与相关技术进展，在此基础上介绍几种预期功能安全相关危害的系统识别与分析方法。

### 4.1 感知面临的预期功能安全挑战与发展方向

自动驾驶的关键技术主要包括感知(Perception)、决策(Planning)和控制(Control)三个方面，其中感知系统以多种传感器捕获的数据以及高清地图的信息作为输入，经过一系列的计算和处理，来预估车辆的状态和实现对车辆周围环境的精确感知，可以为后续决策和控制系统提供必要的信息。然而，依赖复杂传感器和算法工作的感知系统也是预期功能安全问题的重要来源。本节将在介绍感知面临的预期功能安全挑战、感知算法的预期功能安全相关研究的基础上，分析感知系统未来的发展方向。

#### 4.1.1 感知系统面临的预期功能安全挑战

##### (1) 在极端天气（雨、雪和大雾）条件下的感知方面

目前，在一些特殊或者极端恶劣的天气状况下，实现车辆的自动驾驶是非常困难的，因为即使是驾驶人应对此类情况也十分棘手。在雨、雪等恶劣环境下，无论是基于视觉的感知系统还是基于 LiDAR 的感知系统都存在感知困难。大多基于视觉的自动驾驶感知系统都依赖于观测道路标识来辨识道路，然而，薄雪覆盖道路可能会导致这些标识完全消失。此外，即使是模糊、肮脏、磨损或涂漆的道路标记（没有雪况）也会对自动驾驶的感知系统造成不良影响。雪的“沉重感”或密度会影响激光雷达光束的反射效果，产生“幻影障碍（Phantom obstacles）”。这些“幻影障碍”将抑制自动驾驶车辆正确判断环境的能力，并可能导致车辆误停。在多雨或多雾的条件下，会出现类似的不同情况，飞溅的雨水会影响激光雷达的反射效果，雾可能会

遮挡摄像机的视线，从而影响车辆可靠地感知车辆周围环境的能力。

雷达通常在恶劣天气条件下表现良好。但是，由于雷达无法执行稳健的分类和检测道路标记，自动驾驶不能完全依赖雷达来感知，视觉算法的改进是一种潜在的解决方案，因为人类可以只用眼睛进行感知就能在雨雪中安全驾驶。因此，模拟生物视觉的算法有可能在恶劣环境中大幅提高自动驾驶的可靠性。与此同时，相机、激光雷达和雷达传感器等多传感器融合的方法也可以用于检测阴天、晴天、雪、雨和黑暗条件下的行人和车辆，但这些系统仍要改进，以提高准确率和稳定性。此外，基于车联网（V2X）的车辆通讯系统可以协助验证传感器数据的准确性。

### （2）在不利照明条件下的感知方面

镜头光斑（Lens-flares）、大阴影（Large shadows）和其他不利的照明条件也会对感知性能产生不同的影响。例如，视觉系统可能会将大阴影混淆成其他物体的一部分。此外，可能需要在当前感知系统中添加不同的视觉提示（例如尾灯，反射道路标记等）或热成像（远红外）相机，以提高低光条件或夜间的性能。然而，目前大量远红外线摄像机检测和跟踪算法的计算效率不足以实时使用。另外，一些感知系统试图通过依赖环境的先验信息来解决光条件问题，但由于先验信息并非一成不变，如果一个新建设的交通指示灯没有录入先验信息（Priori Information），则自动驾驶车辆遇到它时将会产生问题。

此外，一些方法利用有源传感器，例如 LiDAR，以克服糟糕照明条件。此类传感器不需要外部光线，可以在光线不足和夜间探测障碍物，但激光雷达数据在观察复杂或深度纹理的物体（如灌木丛）时通常会产生噪声，从而阻碍系统的感知。因此，为了更好地解决照明条件问题，可以组合来自多个传感器的数据，以在不良照明条件下获得更好的感知结果，但在这方面仍然存在一些挑战。

### （3）传感器故障和运行状态监控方面

自动驾驶车辆除能稳健地感知环境外，还需能检测和识别传感器故障。例如，驾驶人驾驶传统汽车时，看到发动机故障灯会采取主动停车措施，自动驾驶系统也需能准确检测出感知传感器故障并采取相应措施。通常可以采用基于硬件冗余的方法来解决此问题，即多个相同的传感器交叉验证，从而确定是否有传感器出现故障。然而，上述基于硬件冗余的方法会造成成本上升和增加系统复杂程度等方面的负面影响。因此，基于解析冗余的传感器故障检测与隔离（FDI）方法受到广泛关注。然



而，现有故障检测与分离的方法应用于自动驾驶感知系统仍然具有一些局限性。首先，在基于模型的 FDI 方法中，只有“接近完美”的系统模型才能使该方法有效，但是对于极其复杂的非线性的车辆操纵和不可预测性的周围环境的来讲，“完美”模型的获得并非易事；数据驱动的 FDI 方法依赖大量传感器故障数据对模型进行训练，这样的数据同样难以大量获取；使用基于信号分析的方法来比较传感器度量，以便检测和识别故障或异常传感器是解决该问题的另一种思路，该方法虽然误报率很低，但是漏报率却很高。因此，继续深入适用于自动驾驶感知系统的 FDI 方法研究是目前的主流趋势。

#### （4）驾驶人对于自动驾驶系统功能的正确认知方面

自动驾驶使用者正确理解系统的感知能力及其局限性十分重要，是保证自动驾驶系统正确运行的必要条件之一。然而，公众对于自动驾驶不同级别之间的差异知之甚少，对于不同厂商自动驾驶系统的功能了解程度不够，这将造成驾驶人过度依赖传感器，从而导致严重的后果。研究表明，公众可能无法从自动驾驶的中间阶段（即 Level2 和 Level3 的自动驾驶系统）受益。因为在此等级的自动驾驶系统中，驾驶人可能不会完全理解该阶段自动驾驶自主特征的范围和限制，从而造成事故的发生。例如，此前发生的一些特斯拉事故就是驾驶人盲目信任自动驾驶系统而误操作导致的。此外，驾驶半自动驾驶汽车的驾驶人可能会尝试进行其他的活动，因此在要求接管汽车的控制权时会缺少所需的情景意识。具体讲，在人类驾驶人重新接管汽车控制权时，他们必须立即对周围环境进行判断、确定车辆的位置、根据车辆所处的危险情景决定并施行安全合理的行动方案，但当司机脱离驾驶状态的时间越长，重新介入驾驶所需的时间一般也就越长。因此，驾驶人对于自动驾驶系统功能的正确认知，是确保自动驾驶系统正确运行的必要条件。

#### 4.1.2 感知算法的预期功能安全相关研究

在人工智能技术不断进步的推动下，自动驾驶汽车对周围环境的感知能力得到了飞速发展。但是人工智能带来巨大机遇的同时，也带来了不小的挑战。本轮人工智能的爆发主要是由于深度学习的崛起，深度学习模型在“端到端”模式下、通过标注大量数据来进行误差后向传播而优化参数的学习方法被比喻为一个“黑盒子”，人们很难理解深度学习模型中隐藏层层数、神经元个数、激活函数形式等会对结果产生这样的影响，使得深度学习模型解释性较弱，输出的结果具有一定的不确定性。“黑



盒”问题导致深度学习模型在实际应用过程中，在大多数情况下表现良好，但是在个别情况下的输出的结果却很差，而且难以找到原因，对于自动驾驶来说，往往很差的结果就会导致严重的事故。

针对深度学习模型中的不确定性，目前国内外已经有大量学者开展了相应研究，尝试以不同的方式来度量模型中的不确定性。M.T. Ribeiro 等[1]提出了 LIME，一种新的解释技术，通过学习一个可解释的模型来解释任何分类器的预测，采用局部线性去逼近模型预测，该研究还提出了一种解释模型的方法，通过以非冗余的方式呈现具有代表性的个体预测及其解释，将任务构建为一个子模块优化问题，最后通过解释文本(如随机森林)和图像分类(如神经网络)的不同模型展示该方法的灵活性。D. Erhan 等[2]通过研究网络中单个单元的响应，来更好地理解深度学习模型中特征学习和特征表达的部分，通过测试不同类型数据的输出，进而得到网络中的激活函数对特征的不同表达，以此来观察不同的模型响应，旨在探究何种数据输入才能得到最大化的模型输出。Z. Qi 等[3]等人提出了一个新的解释模块来解释深度学习的预测。将高维的深层网络层非线性地嵌入到低维的解释空间中，利用解释模块提取的少量概念构建原始的深度学习预测。然后将这些概念可视化，以便人类了解深度学习用于决策的高级概念。该研究还将稀疏重建自编码器[4] (Sparse Reconstruction Autoencoder, SRAE)学习嵌入到解释空间。SRAE 的目标是在保持忠实的同时重建部分原有的特征空间。该方法被应用于解释图像分类任务中的 CNN 模型，并引入了一些新的指标来定量地评估解释的性能，而不需要人工参与。实验表明，提出的方法可以更好地解释 CNN 用于预测任务的机制。

近年来，一种新的研究方法以其更少的计算量和更好的解释性受到了相关领域研究学者的广泛关注，即贝叶斯深度学习[5] (Bayesian Deep Learning, BDL)。A. Kendall 等[6]对深度学习中的不确定性进行了分类，分别是偶然不确定性和认知不确定性，并领用贝叶斯深度学习方法对两种不确定性进行建模，以解决计算机视觉中的相关问题。R. McAllister 等[7]针对智能驾驶汽车的安全性，关于其感知系统的不确定性分类对于决策系统的影响做出了讨论，并且提出了贝叶斯深度学习的框架，结合了高度灵活的深度学习架构和贝叶斯方法的优点，讨论了基于对车辆性能的最终影响程度来评估智能车的每个子系统的概率输出的不确定性度量的重要性，发现在整个智能车的系统架构中，位于信息流最底层的子系统往往需要被给予更大的关

注。A. Kendall 等[8]提出了一种基于概率的像素级语义分割的深度学习框架，并将其命名为贝叶斯语义分割。该深度学习预测像素级标签与测量模型的不确定性。通过在测试时使用具有 dropout 的蒙特卡罗抽样来生成像素类标签的后验分布。在数据集上的实验表明，建模的不确定性提高了 2-3% 的分割性能。Yarin 等[9]提出了一个预测不确定性估计的评估框架，专门用于测试在真实的计算机视觉应用中所需的鲁棒性，利用提出的框架，该研究对集成方法和 MC-dropout 进行了全面的比较，结果表明集成方法提供了更可靠的不确定性估计，集成方法的成功归因于其随机初始化的能力，即捕获 DNNs 后验分布中多模态的重要方面。

#### 4.1.3 感知系统未来发展方向

自动驾驶感知系统需要进一步提高准确度和精度，改善感知系统在不利照明和极端恶劣天气条件下的感知能力，未来自动驾驶感知传感器会向感知更加灵敏、精确的方向发展，以增强车辆对复杂城市路况的处理能力与应对各种不利条件、突发状况。例如：通过交叉验证障碍物的位置信息，减少感知系统传感器数据的不确定性；利用好车辆与车辆（V2V）、车辆与基础设施（V2I）之间的通信作为感知补充；开发基于预期功能安全的感知传感器性能缺陷的检测、隔离与诊断方法（FDD）和相应工况下的应对措施，使得智能网联车辆在错误感知时仍能保持安全状态；开发新型、低成本和高精度的感知传感器，通过多传感器融合来减少各个分立传感器缺点的影响，并通过使用传感器的互补性和冗余度来发挥每个传感器的优势，以提高自动驾驶感知系统的准确性、可靠性和确定性；通过对感知系统的深度学习算法的不确定性分析，提高感知算法的可靠性和可解释性等。

#### 4.2 预测相关的预期功能安全技术

在复杂动态交通场景下，利用环境预测技术对自动驾驶车辆周围环境信息进行精准预测是自动驾驶决策的基础，环境预测模型的不确定性也是产生自动驾驶决策预期功能安全问题的根源之一。

现阶段，针对轨迹预测的技术主要包括基于动力学特征的预测方法、基于交互感知的预测方法、基于道路结构特征的预测方法以及基于数据驱动的预测方法。例如，中国科学技术大学的梁华为等[10]采用了动力学、道路结构特征与本体规则相结合的方法进行操作预测。湖南大学的胡满江等[11]采用决策树方法来预测切入场

景中的风险行为。J. Hariyono 等[12]基于行人轮廓、姿势、肢体语言等姿态来预测行人意图。Møgelmoose 等[13]提出一系列基于动力学的预测方法，但是预测精度无法满足自动驾驶安全性要求。采用数据驱动的方式来解决轨迹预测问题是目前的主流方法，该方法的核心思想是将轨迹预测问题转化为回归，即最小化预测轨迹与数据集中的真实轨迹间的误差，西安交通大学的郑南宁等[14]利用 Encoder-Decoder LSTM 方法及场景理解，对十字路口行人轨迹进行了预测，并且达到了较好的效果。

然而，由于驾驶人驾驶策略与行人意图的不确定性，且交通参与者之间的交互作用难以建模，交通参与者的轨迹往往呈现高度非线性。同时，轨迹预测算法输出单一的预测结果无法确保安全，理想的轨迹预测算法应能在每个时间步输出交通参与者的空间位置概率分布，而不仅仅是单一预测结果。此外，轨迹预测算法的预测结果应该是多模态的，因为交通参与者可能采取的行为策略是多种的，因此，预测位置概率分布应与其所采取的策略关联，且预测算法还应该能赋予预测结果相应的置信度，以衡量预测结果的不确定性。

综上所述，目前的环境预测技术仍然不能满足自动驾驶对高精度、快速响应等的要求，因此，研究环境预测模型的不确定性估计方法对于解决预测技术的预期功能安全问题至关重要。目前，研究人员针对经典的时间序列预测模型的不确定性估计已经进行了广泛的研究。例如，A. Kendall 等[15]提出了一种新型贝叶斯深度学习框架，将模型不确定性和固有噪声融入框架内，并将其应用于计算机视觉领域。Y. Gal 等[16]提出在深度神经网络中使用 Dropout 技术以获得模型的不确定性，并通过 MNIST 数据集证明使用 Dropout 技术能够提高模型表现，同时也证明了环境预测模型不确定性估计对于分类问题的重要性。L. Zhu 等[17]基于 LSTM 提出了一种端到端贝叶斯深度模型，进行时间序列预测，并将不确定性融入框架中，用于改善 Uber 极端事件时间的异常检测表现。A. Bhattacharyya 等[18]提出了基于车载摄像头的行人长期轨迹预测方法，针对交通场景中自身存在的不确定性进行了估计与建模。该预测方法首先预测未来车辆里程序列，再利用贝叶斯循环神经网络编码-解码模型预测行人轨迹分布，获取了偶然不确定性与认知不确定性。B. Kim 等[19]为了处理预测轨迹中的不确定性，将高速公路栅格化，通过传感器测量获取周围车辆坐标序列，并将该序列信息其输入至 LSTM 中，预测周围车辆的未来轨迹在道路栅格中的占据概率。M. Hudnell 等[20]基于自动驾驶车辆获取的 2D 图像信息，提出了一种前馈神



神经网络，该网络利用前一时刻使用的目标检测框作为输入，引入了概率形式的 Huber 损失函数，实现了对前方车辆未来时刻位置的准确预测，同时获取了位置的不确定性。

此外，如前所述，驾驶人的驾驶行为具有多模态性，即在相同交通场景下，驾驶人可以采取不同的驾驶策略。例如，当驾驶人以较快的速度接近前车时，驾驶人可能会采取减速，或者换道加速超车等策略，因此，轨迹预测结果应与所驾驶人采取的策略相关联。同时，表征预测结果的不确定性对于车辆后续进行决策规划也至关重要，故必须考虑车辆可能采取的不同轨迹，或者在一定的空间范围内评估预期的碰撞风险，以保障车辆行驶安全性。N. Deo 等[21]针对复杂交通场景中的轨迹预测问题，提出了一种基于 LSTM 的预测模型，该模型可实现对高速公路周围车辆的交互感知运动预测，即根据当前交通环境，预测车辆采取不同驾驶策略的概率分布与预测结果的不确定性程度。M. Mohan 等[22]提出了一种 LSTM 解码编码模型，该模型利用卷积池来学习车辆间的交互作用，能够预测车辆轨迹的多模态分布概率与不确定性。此外，考虑到预测车辆未来状态的分布要求必须能够隐式或者显式地对车辆意图、动力学、交互以及语义环境信息进行建模，J. Hong 等[23]对自动驾驶车辆感知系统提供的 3D 环境信息与高级语义信息（车道、信号灯以及人行横道等）进行了编码，基于深度卷积神经网络理论深度融合环境信息，通过前馈计算学习交通参与者之间及交通参与者与环境之间的交互作用，提出了使用标准监督学习将车辆未来状态建模为不同状态分布的方法，同时以栅格地图占用状态表征预测输出，且每个栅格状态量化了相应状态的概率与不确定性。

#### 4.3 决策相关的预期功能安全技术

基于丰富的车辆状态、环境感知与预测信息，设计安全、高效的决策规划算法是自动驾驶系统开发和安全行驶的关键，国内外学者对自动驾驶决策算法展开了大量的研究。目前，自动驾驶决策主要分为两类：基于规则的决策方法与基于人工智能的决策方法。

基于规则的决策方法主要包含基于碰撞检测的离散输入空间规划（如 lattice planners[24]）、随机规划（如 RRT[25]）和约束优化与后视距控制[26]等。H. Wang 等 [27]提出将潜在碰撞风险指数、人工势场和模型预测控制器相结合的方法，实现了用于减小事故伤害程度的自动驾驶运动规划。现阶段基于规则的决策技术面临因

交通场景状态纬度高、不确定性强等特点导致决策失效的挑战。

基于人工智能的决策方法能够从历史数据中自主学习、并建立高维决策算法以适应高维、高不确定性的交通场景，有潜力进一步提升自动驾驶决策算法的安全性。强化学习（Reinforcement Learning, RL）无需标签数据，通过与环境的交互来学习最优或接近最优的策略，表现出解决决策问题的潜力[28][29]，因此在自动驾驶决策中得到广泛应用。X. Li 等[30]将强化学习运用到高速动态交通场景的决策算法中，能够处理具有挑战性的高速场景[31]。刘春明[32]提出基于强化学习的车辆高速场景下的自主控制的模型，该模型能够在高速公路上完成普通的驾驶动作，同时也能完成高速车辆汇入等动作。还有研究者结合其他传统算法进行实现，董培方等[33]引入人工势场和环境陷阱搜索结合作为强化学习先验信息，加快了路径规划的收敛速度。Z. Gao 等[34]提出强化 Q 学习的决策方法以提高自动驾驶对复杂环境的适应性。一些研究者结合深度学习与强化学习的优势，如利用深度神经网络非线性逼近映射函数的优势，替代强化学习 Q-learning 中的 Q-table，便于表示连续、复杂的状态动作空间，如 DQN 及其变体[35]。事实上，强化学习由于通过环境交互与策略反馈进行策略迭代，因此需要大量的训练数据，且策略无法解释，相比与传统决策方法，可靠性下降，且由于强化学习生成的策略通常由神经网络存储，存在黑箱问题，因此难以应用在对可靠性要求较高的自动驾驶系统中。国内外学者对基于人工智能的决策算法进行了一定程度可解释性研究。H. Gao 等[36]采用逆强化学习建立了每个驾驶人的奖励函数，并实现了奖励函数的可视化；A. Brown [37]通过梯度提升训练决策树集合，匹配原始强化学习代理性能；D. Hein [38]建立了将基于模型的批量强化学习与遗传编程结合的强化学习遗传编程（genetic programming, GP）方法，从预先存在的默认状态动作轨迹样本中自主学习策略方程式，并证明该方法优于基于 GP 构造符号回归的方法。J. Chen 等[39]引入具有序列隐变量的最大熵强化学习，利用隐空间对复杂城市环境状态空间编码，将隐空间解码为“语义 Birdeye 掩码”来解释动作策略的原因，从一定程度上提高自动驾驶决策的可解释性；T. M. Moldovan 等[40]提出保守 Q-Improvement RL 算法，这是一种利用决策树增强可解释性的新方法，该算法仅在估计的整体策略的未来折现奖励增加足够量时才增加树的大小，能有效控制树大小且具保持较高准确性；。

为进一步提升基于人工智能决策方法的可靠性，国内外学者开始研究将强化学



习决策与基于规则的决策算法相融合,以实现更可靠的安全决策。T. M. Moldovan 等[40]通过利用规则或者经验来调整奖励函数,实现两种策略的混合,以增强策略的安全性,对奖励函数设计的依赖程度非常高,奖励函数设计不合理会导致策略的失效。J. Garcia 等[41]等在强化学习的探索过程中加入风险规避的探索策略,以帮助算法更容易收敛到合理的方向,不过这种调整探索策略的方法最终使用的策略仍然完全依赖强化学习生成的策略。J. Fisac 等[42]根据经验或规则分析当前强化学习策略输出是否安全,进而调整输出动作,以避免发生危险,这种方法使得强化学习无法在边缘场景下使用训练的策略。P. Thomas 等[43]提出一种通过调整策略迭代的方法来提升强化学习的可靠性,这种方法有点在于策略迭代的过程考虑了采样的情况,缺点在于其对置信度的追求导致策略提升速度大幅度降低。

随着自动驾驶决策方法日益复杂,智能车辆的预期功能在某些场景下可能无法达到规范的要求。典型的事件如 2018 年 3 月, Uber 自动驾驶汽车在识别到前方障碍物的情况下,未能采取避障或制动措施,最终与行人发生碰撞致其死亡[44]。因此,与自动驾驶决策相关的预期功能安全问题需要得到进一步的重视。翟强等[45]综述了人工智能算法在智能汽车决策中的应用,从智能算法固有的不确定性的角度讨论了可能的预期功能安全问题,最终提出人机共驾对解决当前智能汽车预期功能安全问题的必要性。不仅如此,人工智能算法应用于自动驾驶决策功能开发的安全问题的考虑,现有研究还分别从架构设计[46]、SIL 和 HIL 测试验证[47]和定性安全论证[48]方面进行研究。C. Wang 等[49]介绍了一种基于仿真评估自动驾驶功能的决策、从而确定其安全水平的方法,该方法同时被特斯拉用于测试新系统及现有系统的新版本[50]。然而,上述基于仿真的方法没有考在实际应用时,其他道路使用者与模拟中的行为可能出现不符合的情况,因此,模拟效果可能具有一定的局限性。X. Zhang 等[51]提出了一种基于预期功能安全概念的安全监视系统,用于自动驾驶感知、决策和控制系统。其中,基于文中提出的用于描述综合不确定程度的“安全熵”概念,来定量评估输入决策的信息,提升系统的安全性。

#### 4.4 控制相关的预期功能安全技术

当自动驾驶上层决策系统选择期望轨迹后,该轨迹将被转化为下层命令用于控制车辆执行系统,包括驱动、制动和转向系统。控制执行功能的预期实施依赖控制算法的正确实现和执行器件的精确执行,然而,现有自动驾驶执行控制功能在特定

场景下仍然存在预期功能安全问题。针对自动驾驶控制执行性能缺陷问题，S. A. Shah 等[52]从功能监控与降级的角度出发，提出了一种基于 E-GAS 的自动驾驶安全三层控制架构 Safe-AV。上述架构中，第一层为基础功能层，包括完备功能和降级功能；第二层为功能监控层，指示当前控制功能的执行情况，输出功能切换信号；第三层为应答机制层，通过应答机制监控系统运行情况。M. Klomp 等[53]针对自动驾驶车辆在实际道路相关场景下运行时，可能出现的控制性能缺陷问题，研究了制动和转向机构的容错控制系统和辅助容错供电系统。进一步讨论了通过差速制动实现冗余转向，弥补转向执行系统性能缺陷的实例。

#### 4.5 人机交互技术现有局限与分析方法

基于现有的自动驾驶技术可以预见，在将来的一段时期内，由自动驾驶系统和人类驾驶人共同驾驶的“半自动”驾驶车辆将占绝大多数。半自动驾驶车辆需要人的干预，哪一方在何时负责车辆驾驶将是一个很难界定的问题。自动驾驶系统如何有效地通知可能正在休息的驾驶人、如何确认驾驶人已经准备好接管驾驶都是亟待解决的问题。

因此，设计合理的人机交互系统具有十分重要的现实意义。本节将归纳介绍现有 HMI 技术，逐一分析局限性，据此介绍人机交互的开发过程和相应的人机交互分析方法。

##### 4.5.1 HMI 交互技术及其局限

根据与车辆交互的空间位置的不同，现有 HMI 可以分为车内交互（iHMI）和车外交互（eHMI）两类，每类又可具体细分。本节将根据上述分类，对现有 HMI 技术进行介绍，并分析 HMI 技术在实际应用中存在的局限性。

iHMI 交互即车内交互，包括触控交互、声控交互、动作交互、眼动交互与智能识别交互等，对上述交互方式的介绍和局限如表 4-1 所示。

表 4-1 iHMI 交互的类型及局限性

iHMI	交互局限
触控交互	对车内触控交互场景基本分成两个类别，一种是基于大屏的屏幕触控，另一种是基于物理按钮触控。基于屏幕的触控的问题，在于需要人眼确认，没有触觉反馈，并且存在“胖手指问题”，在开车

	的过程中因为驾驶人需要监控前方道路，在屏幕上停留的时间较短，容易出现“误触发”，另外的系统反应是否及时也是评价的指标。基于物理触控，不能违背人类驾驶人的习惯。
声控交互	声控车内的声控交互场景主要集中在两个方面：一方面车内人员主动进行声控交互，局限在于背景音嘈杂，或使用方言，发音等问题会出现不操作或误操作的问题。另一方面是车辆对驾驶人的声控提示，要避免提示声不被理解等情况发生。
动作交互	基于视觉的光飞时间，结构光，多角成像技术，局限在于光照较暗、过度曝光或者场景本身缺少纹理的情况下，测量精度低，很难进行特征提取匹配，存在“不触发”或“误触发”的现象。依赖于人机配合程度。
眼动交互	眼动交互的方式有驻留时间触发、平滑追随运动、眨眼、眼势等。局限性在于区分“有意识的运动”和“无意识的运动”存在“不触发”或“误触发”的现象。依赖于人机配合程度。
智能交互	针对未来的脑电、肌电、脉搏、生命探测等技术的研究，内 HMI 会从人主控的主动式向到车/系统主控的被动式方向发展。但是如何解决系统的误识别和漏识别，以及区分哪些是有意识的，哪些是无意识的是非常难的课题。

eHMI 交互即车外交互，包含外部警示、表情、交互、灯条灯带交互、外部设备交互、交通系统交互等，对上述交互方式的介绍和局限如表 4-2 所示。常见的人员误用或误操作包括不被理解、故意不接受、信号不稳定。

表 4-2 eHMI 交互的类型及局限性

eHMI	交互局限
外部警示	通过传统的手段包含喇叭和前车灯，来提示外部交通参与者，存在很大的弊端是，人类存在故意不接受，和非故意不接受。即使警示了也杜绝不了事故的发生。
表情交互	如何让行人知道自动驾驶车是否处于自动驾驶模式中也是

	有必要，无人驾驶与行人的交流非常的困难，所以需要像人类一样的表情交互，示意行人自动驾驶车表达的意思。好处是容易被行人接受，更自然。局限性是表情表达的意思，需要被当地人理解和接受。并且需要获得外部行人的反馈。
灯条灯带交互	除了表情，还可以用灯条灯带，提示行人该车目前的状态以及下一步的行动；局限性在于不太被行人理解真实的意思，还没有形成行业标准。普及比较困难。
外部设备交互	目前通过电子设备（例如蓝牙、NFC 和移动通信等方式）和车端进行通信，比如说用手机遥控汽车泊车功能，局限在于穿透性较差，距离敏感性较强，抗干扰性比较差，有延时等特点，应用场景受限。同时需要注意信号的真实性和连续性。
交通系统交互	针对外部交通系统的交互，主要是采用两种技术，一种是借助视觉深度神经网络检测交通标志及信号灯。另外一种是用无线通讯技术 C-V2X，能够让车-车，车-路，车-人，车-云 实现互联互通，准确及时获取前方道路信息状况，从而提升驾驶安全、保障道路畅通。局限性在于车载终端功能失效，信号拥塞、遮挡或干扰，导航系统的数据精度差等。

#### 4.5.2 人机交互开发过程

典型的开发过程主要包括四个主要过程，分别是用户研究、分析、结构评价和总结评价。其中，上述各个过程中包含的具体内容，如图 4-1 所示。



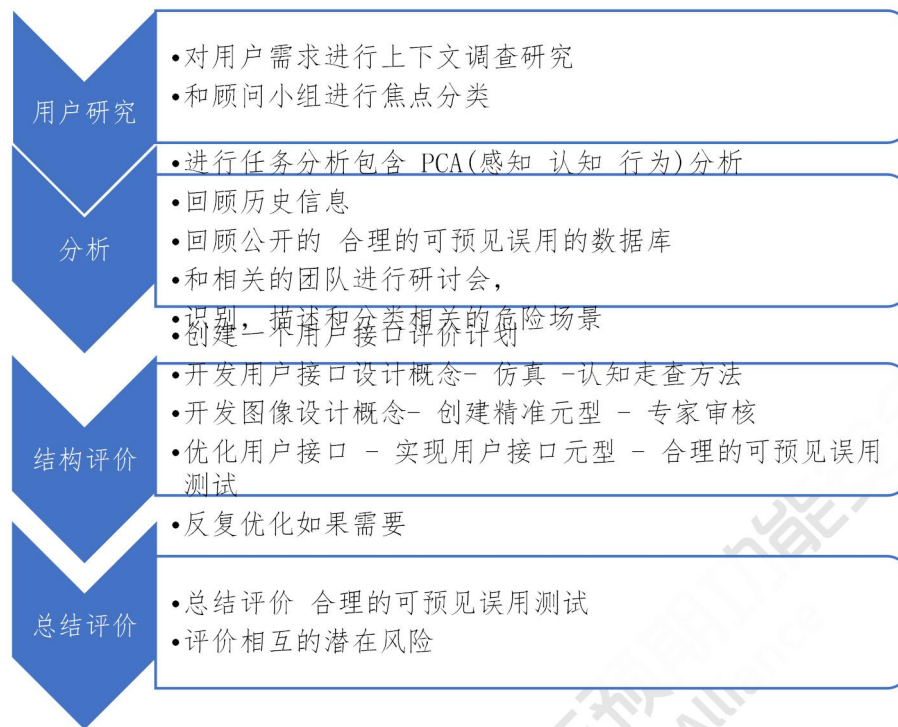


图 4-1 人机交互开发过程

#### 4.5.3 人机交互分析方法

在上节给出的人机交互开发过程中，不同的人机交互开发方法得到应用。表 4-3 中总结了一些典型方法在不同人机交互开发过程中的应用情况，本节将分别对应表中的具体方法，选其典型进行简要的介绍。

表 4-3 典型方法在人机交互开发不同阶段的应用情况

方法	用户研究	分析	设计概念	设计实现	公式化评价	设计完善	最终评价
认知走查	X		X		X		
情景调查	X	X	X				
一天的生活分析	X	X	X				
专家评审			X	X	X	X	X
FMEA&FTA	X	X	X	X	X	X	X
PCA 分析	X	X	X		X		X
仿真	X	X	X	X	X		X
根据标准评审			X	X	X	X	X

任务分析	X	X	X	X	X	X	X
可用性测试	X						
负载评估	X	X	X	X			

### (1) 认知走查法

认知走查涉及研究人员试图确定什么是用户期望,即研究人员通过用户视角逐步审查设计、引导问题专家完成认知审查任务、引导代表性用户完成认知审查任务(有时称为多元化评估)。目的是确定用户是否了解他们为每个用户做了什么。任务,子任务或步骤,以及他们是否了解何时正确或不正确的过程已采取行动。在多元化评估中,研究人员通过以下方式指导用户完成一项任务:根据展示的图纸和模型描述他们如何执行任务。研究人员的工作是通过描述如何将静态用户界面“生动”起来,车辆将响应用户输入。评估可以使用用户界面设计插图,例如图纸(印刷或计算机屏幕上)和控制面板上显示的各种屏幕基于计算机的显示。有时,非功能性硬件模型可以补充图纸使用户对车辆硬件用户有更全面的了解接口。认知演练非常适合初步设计评估,可以产生关于用户界面的令人惊讶的详细有用的见解设计的优势和改进机会。

### (2) 情景调查

了解用户的一种常见而有效的方法是观察他们与之交互感兴趣的项目,并记录视频,以便随后进行分析(图 4-2)。

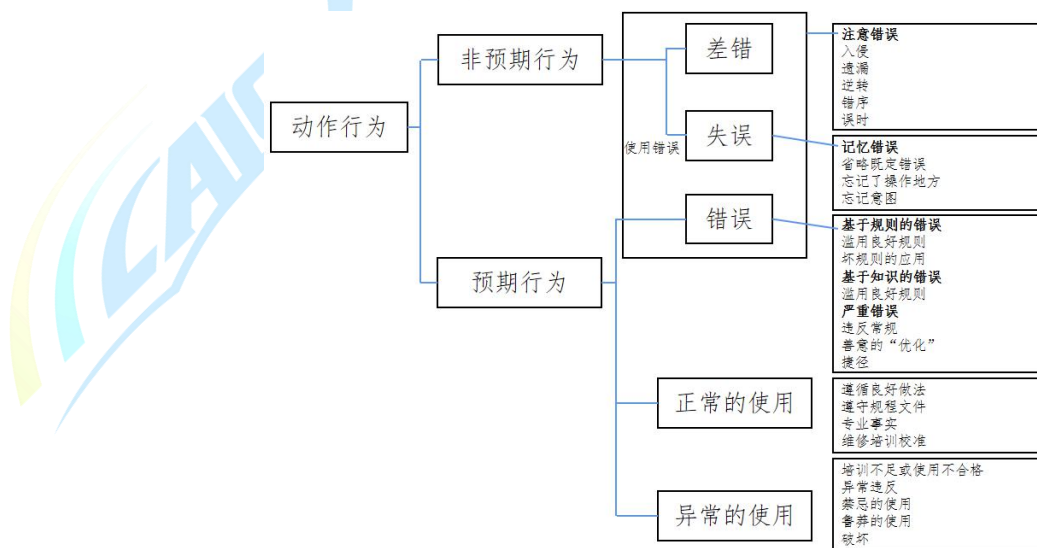


图 4-2 人机交互误操作场景

### (3) “感知”、“认知”和“行为”(PCA)分析

PCA 分析是一种基于任务分析来识别潜在使用错误的方法，该方法建议遵循用户的三个组成部分的交互作用，即“感知”，“认知”和“动作”。为了进行 PCA 分析，可将任务分解为独立的用户交互，即用户感知（示例：听到警告信号，阅读屏幕上文本，感觉到按钮的点击）、认知步骤（示例：召回信息，进行脑力计算，根据知识或规则做出决定）、行动（示例：选择转向控制，按下一个按钮，踩一个控件踏板）。这种分解有助于设计人员了解用户在感知、认知和身体负荷方面的表现。如果用户无法满足这些任务要求之一，则会发生此错误。因此，通过询问以下三个问题，可以识别并轻松发现问题，即“如果用户无法感知 x，该怎么办？”、“如果用户无法解释/处理 y，该怎么办”和“如果用户无法执行动作 z，该怎么办？”。

通过对任务序列中的每个步骤重复上述三个问题，可以初步列出潜在使用问题列表，但并非所有这些使用问题都可能导致使用错误，也并非所有潜在使用错误都与安全相关。使用错误总是会导致系统错误地作为或不作为。ISO/PAS 21448 的附件 E 涉及“认知”，“判断”和“行动”，这等同于 PCA 分析。

### (4) 任务分析法

任务分析的目的是帮助研发人员找到促进或阻碍用户表现的关键因素，以实现期望的结果。认知任务分析着眼于用户的认知过程，例如，用户操作车辆的心理过程，这项技术将使设计师对用户的认知需求有所了解。认知任务分析还可以用于评估车辆的使用方式以及改变用户的想法。

### (5) 用户互动的分类

在半自动驾驶（即 SAE J3016 L3 级或更低）的情况下，驾驶人必须控制车辆：差错 - 旨在点亮转向指示灯却激活了远光灯；失误 - 忘记了自主模式已被停用；错误 - 由于系统反馈不清楚，因此停用了自主模式；异常使用 - 看到了限速标志，但选择了快于限速行驶。

### (6) 可用性测试样本量

考虑选择用于可用性测试样本的大小是很重要的。主要的观点是以样本量的基础，做可用性的公式化评估，并为可用性测试提供合理的测试样本大小的评价。识别使用错误通常需要的样本量由以下公式定义：

$$R = 1 - (1 - p)^n$$

其中， $R$  是观察或检测可用性问题的累积概率， $P$  是单个测试参与者出现可用性问题的概率（或基本可用性缺陷概率），并且  $n$  是评估中测试参与者的数量。

#### （7）改善 SOTIF 可用性的措施

ISO/PAS 21448 第 8 章的活动中有两部分定义了改善架构以及相应功能和系统的更新，即提高传感器性能；提高执行器性能；增强的性能识别和决策算法；改进可测试性。将驾驶权限从系统移交给驾驶人以提高可控性（包括改进人机界面）减少或减轻合理可预见的滥用后果，包括但不限于：（a）改善提供给驾驶人的有关预期功能的信息示例用户手册；（b）改善人机界面；（c）实施监测预警系统。图 4-3 展示了方向盘释放时警告驾驶人的示例。

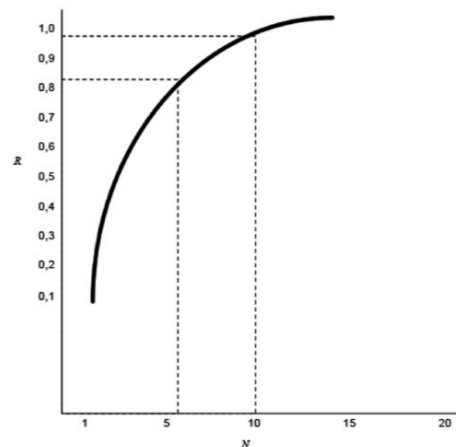


图 4-3 方向盘释放时警告驾驶人的示例

## 4.6 预期功能安全系统分析方法

面向不同领域的安全相关系统，研究人员已提出多种安全分析方法。现有车辆功能安全标准[54]以及预期功能安全标准[55]中即列举了故障树分析(Fault Tree Analysis, FTA)、失效模式及效应分析(Failure Mode and Effect Analysis, FMEA)、危险与可操作性分析(Hazard and Operability Analysis, HAZOP)、系统理论过程分析(Systems-Theoretic Process Analysis, STPA)等方法。在预期功能安全的开发初期，可结合以上一种或多种安全分析方法全面识别所定义的预期功能的相关危害，作为危害评估的输入。上述方法在原理和分析思路上均存在差异性，因而在面对不同分析对象时表现出不同的适用性和有效性，下文将展开介绍每种安全分析方法及其主要应用范围。



#### 4.6.1 故障树分析 (FTA)

故障树分析 (FTA) 是一种基于多米诺骨牌理论的安全分析方法 (图 4-4), 其将事故描述为以特定时间顺序发生的离散事件的结果[56]。该方法由贝尔电话实验室的 Watson 在 1961 年提出, 是一种自上而下的演绎方法[57], 其分析过程以系统级失效状态 (即事故) 作为顶事件, 通过梳理引起顶事件的原因事件并根据其逻辑关系建立故障树图, 从而确定引起失效的基本事件 (即部件故障) [58]。FTA 分析的特点是直观且逻辑性强, 可以用于定性分析, 也可在已知各部件故障率的情况下进行定量分析。该方法主要应用于机电、电气系统的安全及可靠性分析[59][60], 了解系统失效的原因, 也可以结合定量分析对系统潜在风险进行评估, 进而设计降低风险的策略, 或者对已发生的安全事故进行原因分析[61]。该方法也用于对自动化系统的分析, 如飞机自动飞行系统[62]和自动化配电系统[63]等。

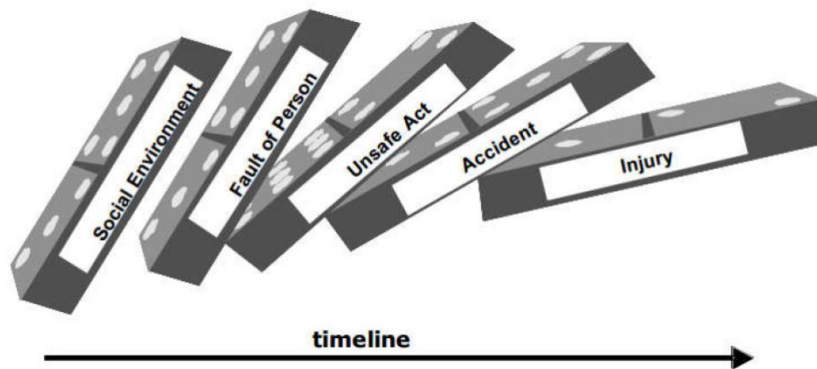


图 4-4 多米诺骨牌理论

#### 4.6.2 失效模式与影响分析 (FMEA)

失效模式与影响分析 (FMEA) 是一种由下而上的归纳式分析方法, 由美国宇航局于 20 世纪 60 年代提出。该方法同样基于多米诺骨牌理论, 通过对产品的子系统、零件以及其构成过程的各个工序逐一进行分析, 找出所有潜在的失效模式, 并分析其可能的后果。其分析过程与 FTA 相反, 从部件具体故障出发, 通过层层分析故障的影响和后果, 从而确定部件故障导致的系统事故[64][65]。FMEA 分析的特点是全面且系统的对所有部件逐一分析。该方法主要应用于设计及生产过程的工序安全性分析[66], 以及设备可能存在的故障及其影响分析[67]。该方法不仅在车辆系统[68]上有诸多应用, 也被应用于车辆柔性部件、制动系统、锂电池系统以及内燃机系统的故障分析, 为面向安全性的设计提供支持[69]-[73]。

FTA 和 FMEA 方法在现有系统安全分析中得到了广泛应用,为了实现更加全面的分析,研究人员常常结合两种方法进行应用,先通过 FMEA 对系统各部件的故障及其影响进行分析,得到部件级失效,然后应用 FTA 从事故开始分析,建立事故与部件级失效的关系,实现自上而下和自下而上方法的合理平衡。多项研究表明[74]-[77]结合以上两种方法的分析对由于具体的软硬件故障导致的系统事故分析具有相当可行性和有效性。

#### 4.6.3 危险与可操作性分析 (HAZOP)

危险与可操作性分析 (HAZOP) 是一种基于经验的结构化分析方法,通过由设计人员和操作人员在内的专家小组系统地辨识各种潜在的偏离设计目的的偏差,分析各偏差发生的原因并评估相应的后果[78]。该方法的核心在于采用经过挑选的关键词表,例如“大于”“小于”“部分”等,来描述每一个潜在的偏离,以识别出所有的故障原因。引导词是 HAZOP 分析的基础,通过其与系统过程的匹配得到系统偏差,并作为后续原因和影响分析的输入[79]。HAZOP 方法已有一套标准化应用导则[80],提供了基本引导词(表 4-4)和与时间和先后顺序相关的引导词表(表 4-5)作为分析的基础。HAZOP 主要应用于化工生产领域,也有研究将其应用于控制系统[81] [82]。

表 4-4 基本引导词及其含义<sup>[80]</sup>

引导词	含义
无, 没有	完全没有达到设计意图
多, 过量	数量上的增加
少, 减量	数量上的减少
伴随	性质上的变化 (增多)
部分	性质上的变化 (减少)
相反	与设计意图逻辑相反
异常	完全替代

表 4-5 与时间和先后顺序相关的引导词及其含义<sup>[80]</sup>

引导词	含义
早	时间上早

晚	时间上晚
先	在顺序上提前
后	在顺序上推后

#### 4.6.4 系统理论过程分析（STPA）

系统理论过程分析（STPA）由 Nancy Leveson 于 2011 年提出[83]，基本分析流程如图 4-5 所示。该方法将安全视为控制问题，当控制系统没有充分处理外部干扰、部件故障或系统部件之间不正常交互时，就会发生危险。STPA 的目标是识别出那些可能导致危险发生的不充分的控制，并且确定相关安全性约束使风险降低到可接受的程度。该方法主要应用于航空航天领域中的自动化系统上，多名研究人员对运载火箭[84]、飞机除冰系统[85]、火/飞/推控制系统[86]、逆推力系统[87]、制动系统等[88]进行了 STPA 分析，通过识别系统不安全控制行为，分析危险状态及潜在原因，进而指导系统设计及优化。STPA 方法中也可以引入人为因素作为不安控制行为的来源，进而应用于轨道交通等涉及人为操作和管理的系统分析中。不同研究应用 STPA 方法对列车、地铁控制系统进行了分析，通过与运行场景、人为错误、管理因素的结合，系统的分析了运行过程中可能的危险来源并提出了安全约束[89-91]。随着自动驾驶技术的推进，STPA 方法也逐步应用到自动驾驶汽车 ADAS 功能（ACC[92]、LKA[93]）以及自动驾驶整车[94]的安全分析中。

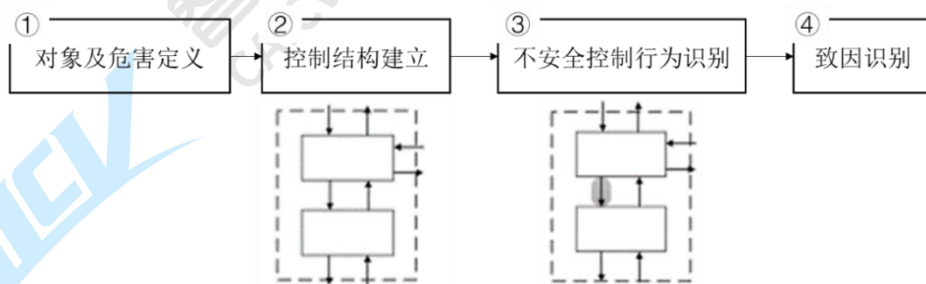


图 4-5 STPA 方法分析流程[93]

#### 4.6.5 不同安全分析方法对比

表 4-6 对比分析了各类危害识别方法的适用范围及存在的问题。FTA 方法以系统级故障作为顶事件，通过自上而下的演绎分析确定系统故障的原因；FMEA 方法则从组件级具体故障出发，通过自下而上的归纳分析确定系统事故。这两种方法在自动驾驶汽车的安全分析方面均表现出一定的局限性，具体为：1) 仅关注系统故障

导致的安全问题，适用于对与外部环境不存在交互的封闭系统安全性分析，在自动驾驶汽车这类与环境发生复杂交互的开放系统的应用中需要对方法做一定程度的扩展；2) 需要具体的系统失效事件或者具体故障类型作为输入，而对于目前的自动驾驶无论是运行事故还是系统内部故障均缺乏充足的数据支持，无法满足基于事故链的安全分析方法的需求。HAZOP 方法中，专家小组基于引导词系统地辨识各种潜在的偏离设计目的的偏差，分析各偏差发生的原因并评估相应的后果。对于自动驾驶这类复杂的软硬件集成系统，仅依赖专家经验和基础引导词的方法难以保证分析结果的全面性和可靠性，因此在该类系统的分析应用中还需要进一步对引导词进行扩充和优化。STPA 方法从控制角度识别系统组件间的不正确交互，进而识别危害，适用于开放系统，在目前研究中是自动驾驶汽车危害识别重点应用的分析方法。然而，STPA 现有分析对象多为 ADAS 系统或功能较为单一的低级别自动驾驶汽车，对于集合多种功能的高等级自动驾驶汽车，应用 STPA 进行危害识别的适用性和有效性还有待研究。

表 4-6 安全分析方法对比

方法	分析过程	适用系统	自动驾驶系统上的应用局限
故障树分析 FTA	基于事故数据 从上而下的演绎分析	封闭系统	不适用于开放系统 缺乏事故数据
失效模式及效应分析 FMEA	基于故障数据 从下而上的归纳分析	封闭系统	不适用于开放系统 缺乏故障数据
危险与可操作性分析 HAZOP	基于引导词 系统偏差分析	开放系统	缺乏适用的引导词 依赖专家经验
系统理论过程分析 STPA	基于系统结构 不安全控制行为分析	开放系统	缺乏面向高等级自动驾驶汽车的应用实践

参考文献：

- [1] Ribeiro M T, Singh S, Guestrin C. " Why should I trust you?" Explaining the predictions of any classifier[C]//Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and



- data mining. 2016: 1135-1144.
- [2] Erhan D, Bengio Y, Courville A, et al. Visualizing higher-layer features of a deep network[J]. University of Montreal, 2009, 1341(3): 1.
- [3] Qi Z, Li F. Learning Explainable Embeddings for Deep Networks[C]//NIPS Workshop on Interpreting, Explaining and Visualizing Deep Learning. Long Beach, CA, December. 2017, 9.
- [4] Ng A. Sparse autoencoder[J]. CS294A Lecture notes, 2011, 72(2011): 1-19.
- [5] Wang H, Yeung D Y. Towards Bayesian deep learning: A framework and some existing methods[J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(12): 3395-3408.
- [6] Kendall A, Gal Y. What uncertainties do we need in bayesian deep learning for computer vision?[C]//Advances in neural information processing systems. 2017: 5574-5584.
- [7] McAllister R, Gal Y, Kendall A, et al. Concrete problems for autonomous vehicle safety: Advantages of bayesian deep learning[C]. International Joint Conferences on Artificial Intelligence, Inc., 2017.
- [8] Kendall A, Badrinarayanan V, Cipolla R. Bayesian segnet: Model uncertainty in deep convolutional encoder-decoder architectures for scene understanding[J]. arXiv preprint arXiv:1511.02680, 2015.
- [9] Gustafsson F K, Danelljan M, Schön T B. Evaluating Scalable Bayesian Deep Learning Methods for Robust Computer Vision[J]. arXiv preprint arXiv:1906.01620, 2019.
- [10] Hu M, Liao Y, Wang W, et al. Decision tree-based maneuver prediction for driver rear-end risk-avoidance behaviors in cut-in scenarios[J]. Journal of advanced transportation, 2017.
- [11] Geng X, Liang H, Yu B, et al. A scenario-adaptive driving behavior prediction approach to urban autonomous driving[J]. Applied Sciences, 2017, 7(4): 426.
- [12] Hariyono J, Jo K H. Detection of pedestrian crossing road: A study on pedestrian pose recognition[J]. Neurocomputing, 2017, 234: 144-153.
- [13] Møgelmoose A, Trivedi M M, Moeslund T B. Trajectory analysis and prediction for improved pedestrian safety: Integrated framework and evaluations[C]//2015 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2015: 330-335.
- [14] Xue P, Liu J, Chen S, et al. Crossing-Road Pedestrian Trajectory Prediction via Encoder-Decoder LSTM[C]//2019 IEEE Intelligent Transportation Systems Conference (ITSC). IEEE, 2019: 2027-2033.
- [15] Kendall A, Gal Y. What uncertainties do we need in bayesian deep learning for computer vision?[C]//Advances in neural information processing systems. 2017: 5574-5584.
- [16] Gal Y, Ghahramani Z. Dropout as a bayesian approximation: Representing model uncertainty in deep learning[C]//international conference on machine learning. 2016: 1050-1059.
- [17] Zhu L, Laptev N. Deep and confident prediction for time series at uber[C]//2017 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2017: 103-110.
- [18] Bhattacharyya A, Fritz M, Schiele B. Long-term on-board prediction of people in traffic scenes under uncertainty[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018: 4194-4202.
- [19] Kim B D, Kang C M, Kim J, et al. Probabilistic vehicle trajectory prediction over occupancy grid map via recurrent neural network[C]//2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2017: 399-404.
- [20] Hudnell M, Price T, Frahm J M. Robust Aleatoric Modeling for Future Vehicle Localization[C]//Proceedings

- of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2019.
- [21] Deo N, Trivedi M M. Multi-modal trajectory prediction of surrounding vehicles with maneuver based lstms[C]//2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018: 1179-1184.
- [22] Deo N, Trivedi M M. Convolutional social pooling for vehicle trajectory prediction[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2018: 1468-1476.
- [23] Hong J, Sapp B, Philbin J. Rules of the road: Predicting driving behavior with a convolutional model of semantic interactions[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2019: 8454-8462.
- [24] Ferguson D, Howard T M, Likhachev M. Motion planning in urban environments[J]. Journal of Field Robotics, 2008, 25(11 - 12): 939-960.
- [25] Karaman S, Frazzoli E. Sampling-based algorithms for optimal motion planning[J]. The international journal of robotics research, 2011, 30(7): 846-894.
- [26] Schwarting W, Alonso-Mora J, Pauli L, et al. Parallel autonomy in automated vehicles: Safe motion generation with minimal intervention[C]//2017 IEEE International Conference on Robotics and Automation (ICRA). IEEE, 2017: 1928-1935.
- [27] Wang H, Huang Y, Khajepour A, et al. Crash mitigation in motion planning for autonomous vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(9): 3313-3323.
- [28] Chen Y F, Everett M, Liu M, et al. Socially aware motion planning with deep reinforcement learning[C]//2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). IEEE, 2017: 1343-1350.
- [29] Gao Z, Sun T, Xiao H. Decision-making method for vehicle longitudinal automatic driving based on reinforcement Q-learning[J]. International Journal of Advanced Robotic Systems, 2019, 16(3): 1729881419853185.
- [30] Li X, Xu X, Zuo L. Reinforcement learning based overtaking decision-making for highway autonomous driving[C]//2015 Sixth International Conference on Intelligent Control and Information Processing (ICICIP). IEEE, 2015: 336-342.
- [31] Xu X, Zuo L, Li X, et al. A reinforcement learning approach to autonomous decision making of intelligent vehicles on highways[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018.
- [32] 刘春明. 基于增强学习和车辆动力学的高速公路自动驾驶研究[D]. 长沙: 国防科技大学, 2014..
- [33] 董培方, 张志安, 梅新虎, 等. 引入势场及陷阱搜索的强化学习路径规划算法[J]. 计算机工程与应用, 2018 (16): 129-134.
- [34] Gao Z, Sun T, Xiao H. Decision-making method for vehicle longitudinal automatic driving based on reinforcement Q-learning[J]. International Journal of Advanced Robotic Systems, 2019, 16(3): 1729881419853185.
- [35] Mnih V, Kavukcuoglu K, Silver D, et al. Human-level control through deep reinforcement learning[J]. nature, 2015, 518(7540): 529-533.
- [36] Gao H, Shi G, Xie G, et al. Car-following method based on inverse reinforcement learning for autonomous vehicle decision-making[J]. International Journal of Advanced Robotic Systems, 2018, 15(6): 1729881418817162.
- [37] Brown A, Petrik M. Interpretable reinforcement learning with ensemble methods[J]. arXiv preprint

- arXiv:1809.06995, 2018.
- [38] Hein D, Udluft S, Runkler T A. Interpretable policies for reinforcement learning by genetic programming[J]. Engineering Applications of Artificial Intelligence, 2018, 76: 158-169.
- [39] Chen J, Li S E, Tomizuka M. Interpretable end-to-end urban autonomous driving with latent deep reinforcement learning[J]. arXiv preprint arXiv:2001.08726, 2020.
- [40] Moldovan T M, Abbeel P. Safe exploration in markov decision processes[J]. arXiv preprint arXiv:1205.4810, 2012.
- [41] Garcia J, Fernández F. A comprehensive survey on safe reinforcement learning[J]. Journal of Machine Learning Research, 2015, 16(1): 1437-1480.
- [42] Fisac J F, Akametalu A K, Zeilinger M N, et al. A general safety framework for learning-based control in uncertain robotic systems[J]. IEEE Transactions on Automatic Control, 2018, 64(7): 2737-2752.
- [43] Thomas P, Theocharous G, Ghavamzadeh M. High confidence policy improvement[C]//International Conference on Machine Learning. 2015: 2380-2388.
- [44] NTSB (2018). National Transportation Safety Board Preliminary Report Highway: HWY18MH010. Retrieved from: <https://www.nts.gov/investigations/AccidentReports/Pages/HWY18MH010-prelim.aspx>.
- [45] 翟强, 程洪, 黄瑞, 等. 智能汽车中人工智能算法应用及其安全综述[J]. 电子科技大学学报, 2020, 49(4): 490-498.
- [46] Willers O, Sudholt S, Raafatnia S, et al. Safety Concerns and Mitigation Approaches Regarding the Use of Deep Learning in Safety-Critical Perception Tasks[J]. arXiv preprint arXiv:2001.08001, 2020.
- [47] Raghupatruni I, Goepfel T, Atak M, et al. Empirical Testing of Automotive Cyber-Physical Systems with Credible Software-in-the-Loop Environments[C]//2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2019: 1-6.
- [48] Gauerhof L, Raafatnia S, Rocco V. Structuring the Safety Argumentation for Deep Neural Network Based Perception in Automotive Applications[C]//Computer Safety, Reliability, and Security: SAFECOMP 2020 Workshops: DECSos 2020, DepDevOps 2020, USDAI 2020, and WAISE 2020, Lisbon, Portugal, September 15, 2020, Proceedings. Springer Nature, 2020, 12235: 383.
- [49] Wang C, Winner H. Overcoming challenges of validation automated driving and identification of critical scenarios[C]//2019 IEEE Intelligent Transportation Systems Conference (ITSC). IEEE, 2019: 2639-2644.
- [50] Riedmaier S, Ponn T, Ludwig D, et al. Survey on Scenario-Based Safety Assessment of Automated Vehicles[J]. IEEE Access, 2020, 8: 87456-87477.
- [51] Zhang X, Zhou M, Shao W, et al. The Architecture of the Intended Safety System for Intelligent Driving[C]//2019 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2019: 1-4.
- [52] Shah S A. Safe-AV: A Fault Tolerant Safety Architecture for Autonomous Vehicles[D]. 2019.
- [53] Klomp M, Jonasson M, Laine L, et al. Trends in vehicle motion control for automated driving on public roads[J]. Vehicle System Dynamics, 2019, 57(7): 1028-1061.
- [54] International Organization for Standardization. Road Vehicles-Functional Safety: ISO 26262-2011[S]. Geneva, Switzerland: ISO, 2011: 11.
- [55] International Organization for Standardization. Road Vehicles-Safety of the Intended Functionality: ISO/PAS 21448-2019 [S]. Geneva, Switzerland: ISO, 2019: 1.
- [56] Ferry Ted S. Modern Accident Investigation and Analysis[M]. New York: Wiley, 1988: 336.

- [57] 文伟平, 郭荣华, 孟正, 柏鼎. 信息安全风险评估关键技术研究及实现[J]. 信息安全, 2015(02): 7-14.
- [58] Vaurio J K. Ideas and Developments in Importance Measures and Fault-Tree Techniques for Reliability and Risk Analysis[J]. Reliability Engineering & System Safety, 2010, 95(2):99-107.
- [59] Dutuit Y, Innal F, Rauzy A, et al. Probabilistic Assessments in Relationship with Safety Integrity Levels by Using Fault Trees[J]. Reliability Engineering and System Safety, 2008, 93(12):1867-1876.
- [60] 许荣, 车建国, 杨作宾, 左晓勇. 故障树分析法及其在系统可靠性分析中的应用[J]. 指挥控制与仿真, 2010, 32(01):112-115.
- [61] 丁雨蕾. 重特大交通事故特征及影响因素分析[D]. 东南大学, 2016.
- [62] 王晨. 飞机自动飞行系统故障诊断专家系统设计[D]. 南京航空航天大学, 2015.
- [63] 席禹, 陈波, 郭晓斌, 陈浩敏, 吴鹏. 基于 IEC61850 配电系统自动化可靠性评估[J]. 电力系统保护与控制, 2019, 47(16):129-135.
- [64] Bertsche B. Reliability in Automotive and Mechanical Engineering: Determination of Component and System Reliability[M]. Berlin: Springer Science & Business Media, 2008.
- [65] Tinga T. Principles of Loads and Failure Mechanisms: Applications in Maintenance, Reliability and Design[M]. Berlin: Springer Science & Business Media, 2013.
- [66] 尤筱玥, 雷星晖, 刘虎沉. 基于失效模式与后果分析扩展模型的外包风险分析[J]. 同济大学学报(自然科学版), 2016, 44(02): 309-316.
- [67] 赵津. 采煤机潜在故障预测和可靠性分析[D]. 太原理工大学, 2016.
- [68] Hillenbrand M, Heinz M, Adler N, et al. Failure Mode and Effect Analysis Based on Electric and Electronic Architectures of Vehicles to Support the Safety Lifecycle ISO/DIS 26262[C]//Proceedings of 2010 21st IEEE International Symposium on Rapid System Prototyping. IEEE, 2010: 1-7.
- [69] Renu R, Visotsky D, Knackstedt S, et al. A Knowledge Based FMEA to Support Identification and Management of Vehicle Flexible Component Issues[J]. Procedia Cirp, 2016, 44: 157-162.
- [70] Struss P, Fraracci A. Automated Model-Based FMEA of a Braking System[J]. IFAC Proceedings Volumes, 2012, 45(20): 373-378.
- [71] Schlasza C, Ostertag P, Chrenko D, et al. Review on The Aging Mechanisms in Li-Ion Batteries for Electric Vehicles Based on the FMEA Method[C]//2014 IEEE Transportation Electrification Conference and Expo (ITEC). IEEE, 2014: 1-6.
- [72] Ványi G. Improving the Effectiveness of FMEA Analysis in Automotive—A Case Study[J]. Acta Universitatis Sapientiae, Informatica, 2016, 8(1): 82-95.
- [73] Poprocký R, Galliková J, Stuchlý V, et al. FMEA Analysis of Combustion Engine and Assignment Occurrence Index for Risk Valuation[J]. Diagnostyka, 2017, 18(3): 99-105.
- [74] Held M, Broennimann R. Safe Cell, Safe Battery? Battery Fire Investigation Using FMEA, FTA and Practical Experiments[J]. Microelectronics Reliability, 2016, 64(SEP.):705-710.
- [75] 胡海涛, 高朝晖, 何正友, 袁林. 基于 FTA 和 FMEA 法的地铁牵引供电系统可靠性评估[J]. 铁道学报, 2012, 34(10): 48-54.
- [76] Yu S, Liu J, Yang Q, et al. A comparison of FMEA, AFMEA and FTA[C]//The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety. IEEE, 2011: 954-960.
- [77] Cristea G, Constantinescu D M. A Comparative Critical Study between FMEA and FTA Risk Analysis



- Methods[J]. IOP Conference Series: Materials Science and Engineering, 2017, 252:012046.
- [78] 周广文, 杨霞, 郑世清. 智能化风险及可操作性(HAZOP)分析系统研究进展[J]. 化工进展, 2018, 37(03): 815-821.
- [79] 杜廷召, 田文德, 任伟. 危险与可操作性分析研究[J]. 现代化工, 2010, 30(07): 90-93.
- [80] 中国国家标准化管理委员会, 危险与可操作性分析(HAZOP 分析)应用指南: GB/T 35320-2017[S]. 北京: 中国标准出版社, 2018.
- [81] Hansen K M, Wells L, Maier T. HAZOP Analysis of UML-based Software Architecture Descriptions of Safety-critical Systems[J]. Proceedings of NWUML, 2004: 59-78.
- [82] Do S, Han H. Hazard Identification and Testcase Design Method based on Use Case and HAZOP[J]. Journal of KIISE, 2016, 43(6): 662-667.
- [83] Leveson N. Engineering a Safer World: Systems Thinking Applied to Safety[M]. MIT Press, 2011.
- [84] Ishimatsu T, Leveson N G, Thomas J P, et al. Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis[J]. Journal of Spacecraft and Rockets, 2014, 51(2): 509-522.
- [85] 徐燕, 钟德明, 尹帅. 基于系统理论过程分析的软件安全性分析[J]. 计算机应用, 2013, 33(s2):238-240.
- [86] 胡剑波, 郑磊. 综合火/飞/推控制系统复杂任务的 STAMP 建模和 STPA 分析[J]. 航空工程进展, 2016, 7(3):309-315.
- [87] Hao Wang, Deming Zhong, Yukun Zhao, et al. A System Safety Analysis Method Based on Multiple Category Hazard Factors[C]// International Conference on Dependable Systems and Their Applications. IEEE, 2017.
- [88] Jianbo H, Lei Z, Shukui X. Safety analysis of wheel brake system based on STAMP/STPA and Monte Carlo simulation[J]. Systems Engineering and Electronics, Journal of, 2018, 29(6):1327-1339.
- [89] 闫宏伟. 基于 STAMP 的轨道交通全自动运行系统安全分析研究[D]. 北京交通大学, 2016.
- [90] YAN Fei, TANG Tao, YAN Hongwei. Scenario Based STPA Analysis in Automated Urban Guided Transport System[C]//IEEE. Proceedings of the International Conference on Intelligent Rail Transportation. Birmingham: IEEE, 2016: 425-431.
- [91] Thapaliya A, Kwon G. Reliability and Control Theory: An Integration Approach for Safety Analysis[M]. Advances in Computer Science and Ubiquitous Computing. 2018.
- [92] Abdulkhaleq A, Stefan W. Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain[C]//2013 STAMP Workshop. Cambridge: MIT, 2013.
- [93] Mahajan H S, Bradley T, Pasricha S. Application of Systems Theoretic Process Analysis to A Lane Keeping Assist System[J]. Reliability Engineering & System Safety, 2017, 167:177-183.
- [94] Bagschik G, Stolte T, Maurer M. Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle[J]. Procedia Engineering, 2017, 179:61-71.

## 第5章 国内外智能网联汽车预期功能安全相关专利

预期功能安全是智能网联汽车研发与商业化的关键难题之一。不同于相对成熟的功能安全研究与已经取得一定研究成果的信息安全研究，国内外针对智能网联汽车预期功能安全技术研究及相关专利申请尚处在起步阶段。此外，预期功能安全专注于系统的预期功能局限以及人为误用导致的危害，但是在预期功能安全概念提出之前，业界也开展了类似的研究，这造成相关专利难以明确界定。因此，本章节将同时阐述明确提及预期功能安全的专利和与之内涵紧密相关的专利，以为我国后续预期功能安全研究提供参考。本章节主要包括国外智能网联汽车预期功能安全相关专利、国内智能网联汽车预期功能安全相关专利与智能网联汽车预期功能安全专利总结三部分。

### 5.1 国外智能网联汽车预期功能安全相关专利

国外预期功能安全相关专利主要面向传感器性能局限、决策算法局限和驾驶人误操作。截至2020年10月，共检索到9项国外智能网联汽车预期功能安全发明专利，其中包括4项直接相关的发明专利和5项间接相关的发明专利（详见附表A）。

4项直接相关的发明专利均面向传感器性能局限，包括了1项已授权发明专利与3项未授权发明专利。已授权发明专利（申请号US2019049958A1）公开了一种面向自动驾驶的多传感器关联诊断、传感器融合和深度神经网络（Deep Neural Network, DNN）监测方法及系统。该系统可基于传感器重叠覆盖和性能限制的区域诊断、验证车辆的传感器问题，并利用验证无误后的传感器输出监测传感器融合和深度神经网络的输出。3项未授权的发明专利（申请号US20200231142A1、US20200233418A1、US20200233420A1）分别公开了一种可根据环境条件动态调整传感器有效覆盖坐标的方法和系统、一种用于监测传感器有效覆盖坐标的动态调整与车辆在高精地图中的定位的安全监测系统、以及一种确定自动驾驶车辆安全行驶区域的方法，以确保自动驾驶车辆的安全行驶。

5项间接相关的发明专利包括4项已授权发明专利和1项未授权发明专利。4项已授权发明专利中，2项面向传感器性能局限，1项面向决策算法局限，1项面向驾驶人误操作。

在传感器性能局限方面，已授权发明专利（申请号US20190026597A1）公开了

一种面向自动驾驶汽车的传感器融合系统，该系统利用卷积神经网络(Convolutional Neural Networks, CNN)从多个接口接收传感器检测的交通环境信息，进行道路对象的特征识别。已授权发明专利（申请号 US20170109644A1）公开了一种传感器融合系统，该系统可用于检测和跟踪车辆附近的障碍物。

在决策算法局限方面，已授权发明专利（申请号 US20180229723A1）公开了一种自主车辆决策逻辑优化方法，将传感器数据与安全性相关的用户反馈相关联，并基于行为的不确定性优化决策策略。

在驾驶人误操作方面，已授权发明专利（申请号 US20170101032A1）公开了一种自动驾驶车辆座椅系统，乘客和驾驶人的座椅在自动驾驶模式下会自动缩回并锁定，驾驶人将远离方向盘和脚踏板，防止驾驶人误触碰。

## 5.2 国内智能网联汽车预期功能安全相关专利

国内预期功能安全相关的专利申请尚处于起步阶段，截至 2020 年 10 月，共检索到 59 项公开专利，其中包括 5 项直接相关的发明专利和 54 项间接相关的实用新型及发明专利（详见附表 A）。5 项直接相关的发明专利包括 1 项已授权发明专利与 4 项未授权发明专利。1 项已授权发明专利面向预期功能安全的验证，4 项未授权发明专利中，1 项面向预期功能安全的验证，2 项面向自动驾驶车辆功能算法的研发，1 项面向预期功能安全的危害评估。

在预期功能安全的验证方面，已授权发明专利（申请号 CN201910742725.0）公开了一种自动驾驶算法预期功能安全的验证方法、平台及存储介质，建立了自动驾驶硬件在环测试系统（Hardware-in-the-Loop, HIL），该系统中对 SOTIF 危险场景进行虚拟建模，并对自动驾驶功能算法分别进行 SOTIF 的模型在环和硬件在环验证。发明专利（申请号 CN201910021029.0）提出了一种面向自动驾驶汽车预期功能安全的验证方法及系统，满足了自动驾驶汽车功能开发中对预期功能安全评估的需求，满足量化的、可验证的评估要求，且可操作性强。

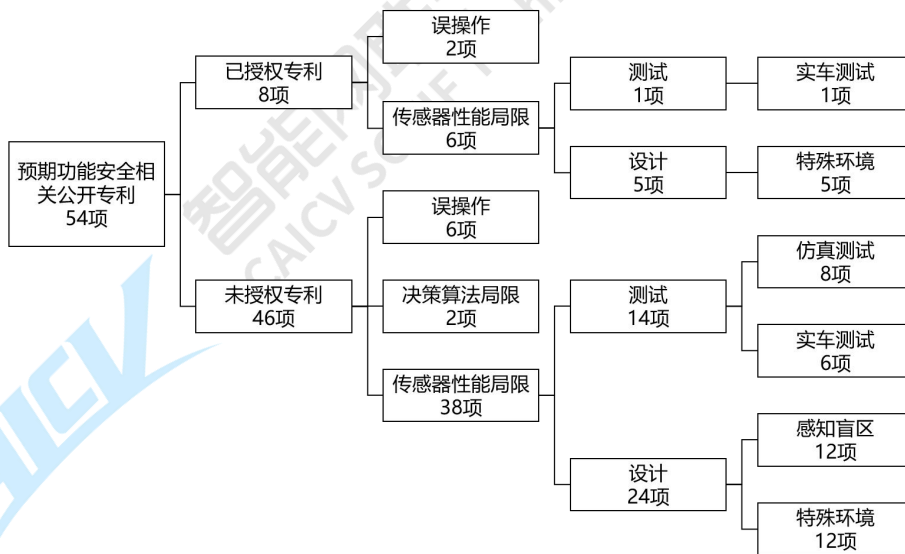
在预期功能安全的危害评估方面，发明专利（申请号 CN201911111961.9）公开了一种基于零日漏洞（Zero-Day）的自动驾驶预期功能安全危害评估方法，将预期功能安全的危害评估和零日漏洞安全评估相结合，提升了 ADAS 和自动驾驶系统的预期功能安全危害检出率。

在自动驾驶车辆的功能算法开发方面，发明专利（申请号 CN201911321150.1）

公开了一种基于预期功能安全的自适应巡航系统（Adaptive Cruise Control, ACC）开发与测试方法，提升了 ACC 的安全性和可靠性，降低了在非故障情况下，由于 ACC 的系统功能不满足预期要求而导致的安全风险。发明专利（申请号 CN201911162457.1）公开了一种基于历史数据的轨迹规划 SOTIF 实现方法，通过聚类边界保证轨迹规划算法的安全性，并对异常数据值进行分析论证，不断扩大已知轨迹的安全范围，提高了智能车行驶安全性。

54 项间接相关的专利中包括 8 项已授权专利和 46 项未授权专利。如图 5-1 所示，上述专利主要面向传感器性能局限、驾驶人误操作和决策算法局限等。8 项已授权专利中，2 项面向驾驶人误操作，6 项面向传感器性能局限，其中面向传感器性能局限的相关专利涉及的特殊环境主要包括雨雪、强/弱光照等。此外，面向传感器性能局限的专利中有 3 项为实用新型专利。

由于预期功能安全问题近几年才受到普遍关注，且专利申请授权过程需一定时间，故目前已授权专利数量仍较少。在 46 项未授权专利中，6 项面向驾驶人误操作，2 项面向决策算法局限，38 项面向传感器性能局限。



在驾驶人误操作方面，共有 2 项已授权发明专利。其中专利（申请号 CN201810457759.0）公开了一种能够防止误操作的自动泊车装置和方法，能够在车辆自动泊车时，对用户执行的操作进行影响等级判断，及时中断自动泊车功能，提升了整车的安全性。专利（申请号 CN201910433733.7）公开了一种基于驾驶人状态



监测系统的车辆智能避险控制方法，能够监测驾驶人的驾驶状态，并在监测到驾驶人无能力继续控制车辆时，通过完备的判断逻辑操控车辆，从而避免车辆失控，提高了行驶安全性。

在传感器性能局限方面，包括 3 项已授权发明专利和 3 项已授权实用新型专利。其中，发明专利（申请号 CN202010193642.3）公开了一种夜间车辆检测方法、装置及系统，能够在夜间，特别在目标车辆能见度非常低的远距离处，检测目标车辆并精确测量其与自车的距离，克服了目前视觉解决方案的局限性，提升了夜间车辆检测的鲁棒性、准确性与快速性。发明专利（申请号 CN201510171979.3）公开了一种基于亮度递减验证的夜间车辆尾灯提取方法，适用于基于图像的夜间车辆检测系统，其具备良好的尾灯形态适应性和颜色适应性，提高了基于尾灯的夜间车辆检测方法的检测率和鲁棒性。发明专利（申请号 CN201611056477.7）公开了一种自动驾驶车辆通过视觉干扰区的能力测试方法及测试场，同时保证了测试的相对真实性与测试安全性，并针对车辆经过视觉干扰区的能力评价方法进行标准化，使测试结果更加权威可靠。实用新型专利（申请号 CN201821180725.3）公开了一种自动驾驶车辆底部智能照明光源装置，解决了现有自动驾驶车辆在亮度条件差时不能识别地面标志、标线或地面状态的问题。实用新型专利（申请号 CN201721550308.9）提出了一种面向自动驾驶车辆的夜视辨识装置，在不同光照环境下，可有效满足对车外环境进行监控识别作业的需求，提高了自动驾驶车辆在不同光照条件下运行的安全性和可靠性。实用新型专利（申请号 CN201921446143.X）公开了一种汽车外置感知传感器清洗装置，实现了自动清洗外置感知传感器，可有效保证外置感知传感器的正常工作，提高了自动驾驶的安全性。

### 5.3 智能网联汽车预期功能安全专利总结

如前所述，目前共检索到与预期功能安全直接、间接相关的国内专利共计 59 项，所有专利申请时间的分布情况如图 5-2 所示。从总体上看，专利申请数呈增长趋势，且数量在 2019 年突增，达 33 项之多。



图 5-2 预期功能安全国内相关专利申请时间（样本 N=59）

从专利申请数量上看，在 59 项专利中，申请数量位于前五的研究单位如图 5-3 所示，依次为北京百度网讯科技有限公司、同济大学、吉林大学、浙江吉利控股集团有限公司与特路（北京）科技有限公司。其中，北京百度网讯科技有限公司在测试、设计方面均有专利申请，同济大学和吉林大学的专利主要面向测试，浙江吉利控股集团有限公司的专利主要面向误操作和感知盲区，特路（北京）科技有限公司的专利均为测试场地及方法。

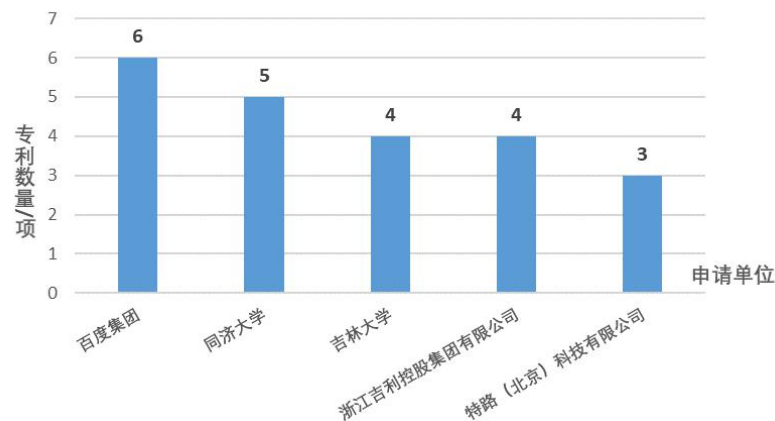


图 5-3 专利申请数 TOP5 排名

从研究单位性质看，59 项专利中，企业申请专利占 41 项，约占总数的 70%，其余 18 项是高校申请的专利，如图 5-4 所示。此外，调研发现：企业更注重预期功能安全相关的研究和专利申请，且大多面向设计技术，高校申请的专利则主要面向测试。

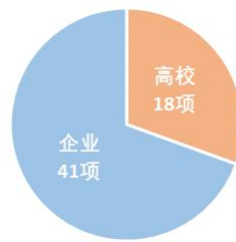


图 5-4 预期功能安全国内相关专利数量分布（样本 N=59）

综上所述，在数量上，国内相关专利的申请数量总体呈增长趋势，预期功能安全相关专利的申请逐渐受到重视。在内容上，国内外的设计相关的专利大多面向传感器性能局限，主要针对感知盲区和特殊环境下的传感器性能局限。针对决策算法局限，目前的相关专利多以测试为主。针对误操作，相关的专利申请数量较少，且各专利的研究角度差异较大，没有统一的研究方向。此外，目前仍缺少面向执行器功能局限的相关专利。在申请单位上，相比于国内高校，企业更注重预期功能安全相关的研究和专利申请。

在未来，预期功能安全的相关专利将会得到进一步重视。在申请数量方面，预计将保持近两年的增长趋势，更多的公开专利也将得到授权。在研究内容方面，包括执行器功能局限、驾驶人误操作等研究将受到更广泛的关注，将形成更完善的研究体系。在研究单位方面，企业和高校之间将加强合作交流，以更好地推动符合预期功能安全的智能网联汽车在中国落地。因此，预计将有更多的预期功能安全相关专利转化为实际的技术，将在智能网联汽车上得到实际应用，进一步促进智能网联汽车的发展。

## 第6章 国内外智能网联汽车场景库研究现状

智能网联汽车在实际商业化运行之前，需要对其安全性能进行充分验证。随着自动驾驶的“场景化”趋势愈发明显，场景库对于测试、验证自动驾驶汽车的安全性至关重要。然而，针对预期功能安全的场景库建设尚在研究阶段，因此，本章节将阐述当前智能网联汽车的场景库研究现状，以为我国面向预期功能安全的场景库建设提供参考。本章节主要分为国外智能网联汽车场景库研究现状与国内智能网联汽车场景库研究现状两个部分，将以国内外发布数据集或标准所依托的项目（单位）展开介绍。

### 6.1 国外智能网联汽车场景库研究现状

#### 6.1.1 PEGASUS

PEGASUS 项目由德国汽车行业相关企业和研究机构共同发起，以制定的自动驾驶车辆的一系列测试标准为目的，根据自动驾驶产品开发在概念阶段、系统开发阶段与测试阶段对场景的需求差异，分别提出了相应的功能场景、逻辑场景和具体场景概念。此外，针对场景的格式进行了规范，提出了 OpenScenario 场景格式标准，这一标准得到了国际研究人员的广泛认可。

#### 6.1.2 NHTSA

美国国家公路交通安全管理局（National Highway Traffic Safety Administration, NHTSA）主要由车辆安全研究室和行为安全研究室组成，车辆安全研究室的主要任务是制定战略、计划与实施研究，以不断减少碰撞、死亡和伤害为目标，行为安全研究办公室主要关注司机、乘客、行人和摩托车驾驶人的行为和态度，并基于此来制定、完善政策，以阻止不安全行为发生。NHTSA 为解决上述安全问题，建立了如下数据系统：（1）碰撞调查取样系统（CRSS）；（2）死亡率分析报告系统（FARS）；（3）碰撞调查取样系统（CISS）；（4）特殊碰撞调查（SCI）；（5）非交通监控（NTS）；（6）碰撞伤害研究和工程网络（CIREN）。

#### 6.1.3 Waymo

2019 年 8 月，Waymo 首次公开了 Waymo Open Dataset 数据集，该数据集包含了 Waymo 在亚利桑那州凤凰城、华盛顿柯克兰、加州山景城和旧金山行驶数百万英里所收集的数据，而且涵盖了白天夜晚、黎明黄昏、晴天雨天等不同天气情况及不



同道路环境。2020年3月，Waymo再次公开了Waymo Open Dataset数据集的扩展版本，增加了800个片段。

此外，美国Waymo公司还研发了Carcraft仿真软件，可利用从真实场景中收集到的驾驶数据对无人驾驶车辆性能进行测试、改进。同时，它还可以通过参数模糊化等技术生成大量的衍生测试场景，以快速重复测试一些在现实世界中发生概率较低但十分关键的场景。基于Carcraft无人驾驶车辆可以针对某一关键场景进行多次训练，如对交通信号进行一些改变，添加额外的行人等，以提升系统性能。目前，每天有25000辆虚拟无人驾驶车辆在模拟器中行驶，里程可达八百万英里以上。

#### 6.1.4 福特数据集

2020年3月，福特公司发布了其最新版无人驾驶数据集，包含2017至2018年间的自动驾驶车队路测数据，涵盖了机场、高速公路、市中心、大学校园和郊区等多种驾驶场景。数据采集设备主要包括4个激光雷达传感器、6个1300万像素相机，1个500万像素相机与一组惯性测量单元。所采集的数据包括3D地面反射率地图、3D点云地图、六自由度真实姿态和局部姿态等信息，数据均以Rosbag格式存储，可以使用开源机器人操作系统（Robot Operating System，ROS）进行可视化、修改与应用。

#### 6.1.5 KITTI 数据集

KITTI数据集由德国卡尔斯鲁厄理工学院和丰田美国技术研究院共同参与构建，用于评测面向自动驾驶场景的计算机视觉算法，主要包括评价目标检测、目标跟踪、路面分割等计算机视觉技术在车载环境下的性能。KITTI数据集包含市区、乡村与高速公路等场景下采集的真实图像数据，每张图像中多达15辆车和30个行人，还有不同程度的遮挡。在KITTI数据集中，目标检测包括车辆检测、行人检测、自行车检测三个单项，目标追踪包括车辆追踪、行人追踪等两个单项，道路分割包括Urban Unmarked、Urban Marked、Urban Multiple Marked三个场景及前三个场景的平均值Urban Road四个单项。

#### 6.1.6 NuScenes 数据集

2019年4月，安波福正式发布了数据集nuScenes，该数据集包含从波士顿和新加坡收集的多个场景信息。该数据集特点如下：（1）全套传感器（1个激光雷达、5

个雷达、6 个摄像头、IMU、GPS); (2) 1000 个场景, 每个场景 20 秒; (3) 1400000 摄像机图像; (4) 390000 次激光雷达扫描; (5) 两个不同的城市: 波士顿和新加坡; (6) 左侧与右侧交通; (7) 详细地图信息; (8) 23 个对象类手动标注 140 万个 3D 边界框; (9) 属性: 可见度、活动度和姿势等; (10) 1.1 亿激光雷达点手动注释 32 类。



图 6-1 nuScenes 数据集

#### 6.1.7 Argoverse 数据集

2019 年 6 月, 美国福特公司旗下的 Argo AI 发布了自动驾驶精选数据和高精度地图。Argo AI 发布的 Argoverse 数据集是第一个公开包含高精度地图数据的数据集, 该数据集包含了匹兹堡和迈阿密地区的 290 公里车道地图, 如位置、连接、交通信号、海拔等信息。

#### 6.1.8 Lyft 自动驾驶汽车数据集

2019 年 7 月, Lyft 发布了其自动驾驶汽车数据集, 该数据集以 nuScenes 格式(安波福研发)存储, 包含 55000 个由人工标记的 3D 注释交通代理框架, 7 个摄像头与 3 个激光雷达的比特流数据、1 个可供驾驶使用的地面地图以及 1 个空间语义高精度地图。高精度地图中包括 4000 多条巷段、196 条人行横道、60 个停车标志、54 个停车区域、8 个减速带、11 个缓冲带等。

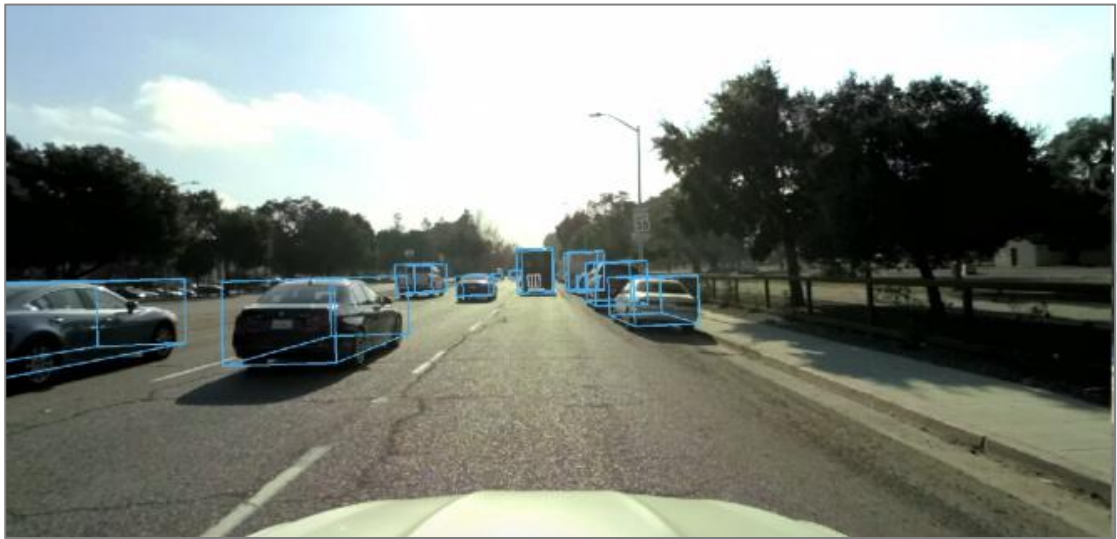


图 6-2 Lyft 数据集

#### 6.1.9 H3D - HRI-US 数据集

2019 年 3 月，日本本田研究所发布了面向无人驾驶的 H3D 数据集，该数据集是一个面向大规模全环绕 3D 多目标检测和跟踪的数据集。H3D 数据集包括以下内容：（1）全 360 度激光雷达数据集；（2）160 个拥挤且高度互动的交通场景；（3）1071302 个 3D 边界框标签；（4）8 种常见的交通参与者类别；（5）基于最先进的 3D 检测和跟踪算法。

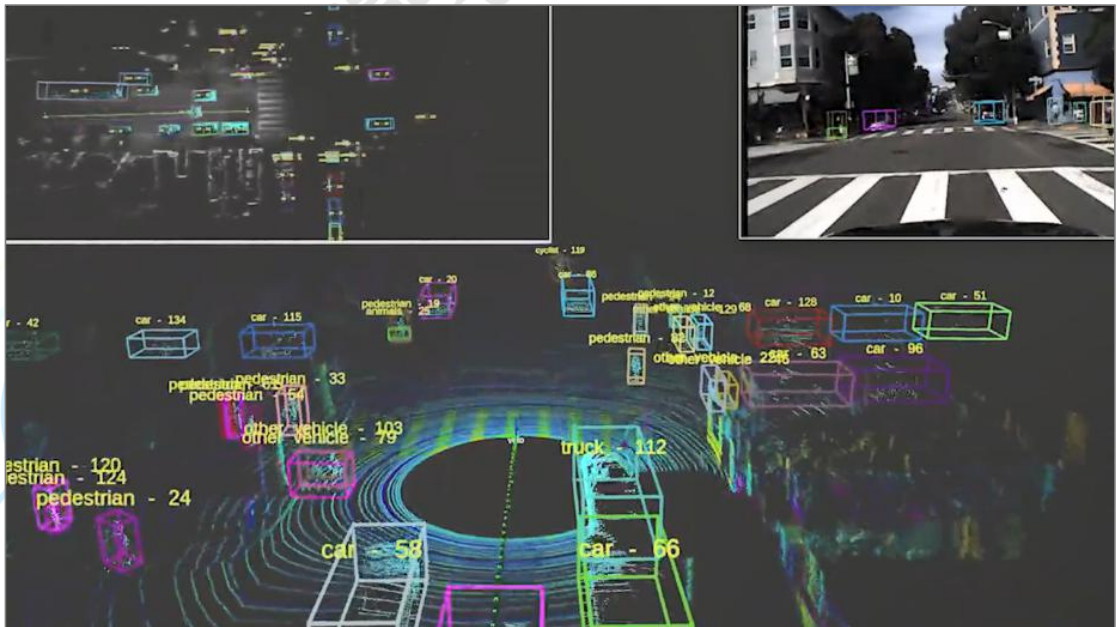


图 6-3 H3D - HRI-US 数据集



#### 6.1.10 CamVid 数据集

英国剑桥大学发布的 CamVid 数据集是一个具有对象类语义标签的视频集合，该数据集提供基础事实标签，并将每个像素与 32 个基本语义类相关联。该数据集提供时长超过十分钟的高质量 30Hz 的画面，相应的语义标记图像为 1Hz，部分为 15Hz，解决了算法测试对实验数据的需求，可定量评估算法。

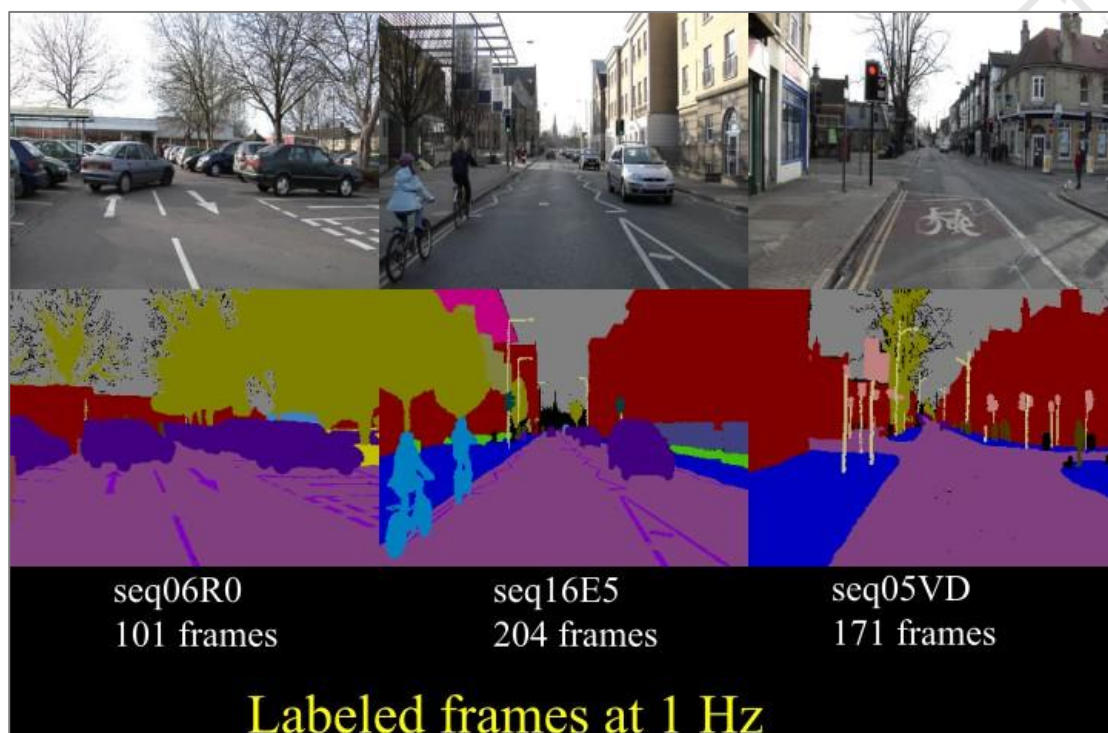


图 6-4 CamVid 数据集

#### 6.1.11 BDD100K 数据集

2018 年，美国加州大学伯克利分校 AI 实验室 (BAIR) 发布了数据集 BDD100K，该数据集由 100000 个视频组成，每个视频大约 40 秒，分辨率为 720p，每秒 30 帧。这些视频同时提供由手机记录的 GPS/IMU 信息，可以显示粗略的驾驶轨迹。这些数据在美国不同的地方采集，涵盖了不同的天气条件（包括晴天、阴天及雨天等）以及白天和晚上的不同时间段，采用 2D 边框注释了 100,000 张图片（包括公交车、交通灯、交通标志、人、自行车、卡车、摩托车、轿车及火车等）。



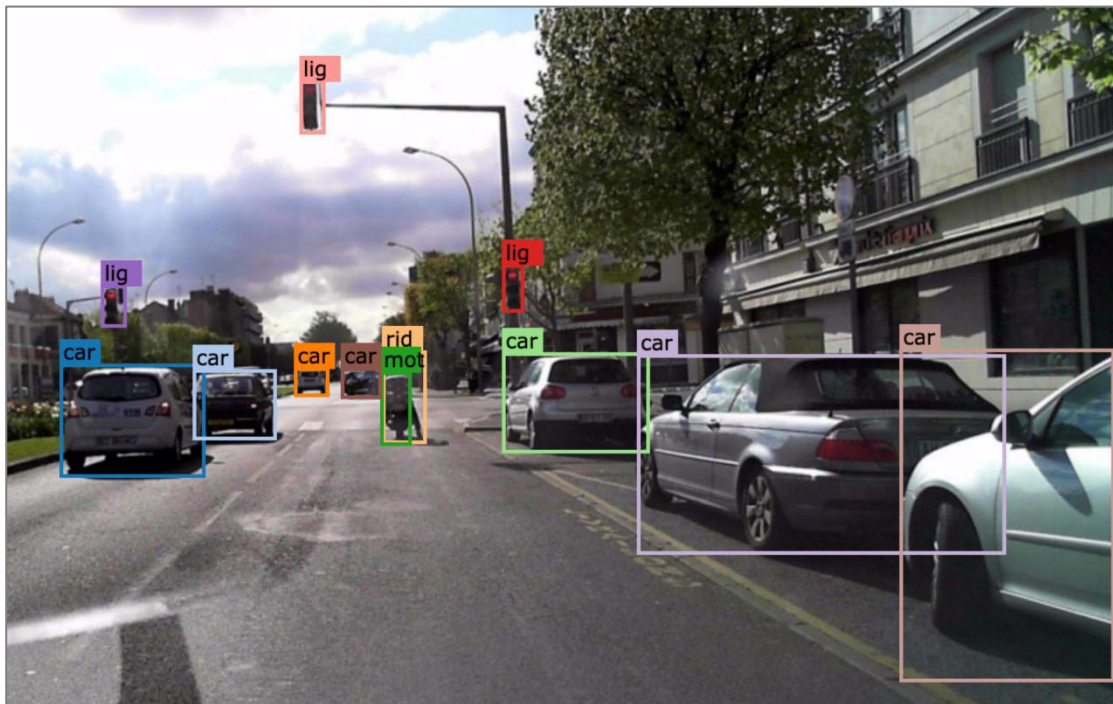


图 6-5 BDD100K 数据集

#### 6.1.12 Cityscapes 数据集

2015 年，德国奔驰公司发布了 Cityscapes 评测数据集，该数据集是目前机器视觉领域最具权威性和专业性的图像分割数据集之一。Cityscapes 评测数据集共分为像素级分割和实例分割两个子任务，其中实例分割的难度要更大，这也是计算机视觉领域最具挑战的任务之一。在 Cityscapes 实例分割任务所对应的数据集中，包含了 5000 张精细标注的图像和 20000 张粗略标注的图像，涵盖了 50 个城市的不同场景、不同背景、不同街景，以及 30 类包括地面、建筑、交通标志、自然、天空、人和车辆等的物体标注。

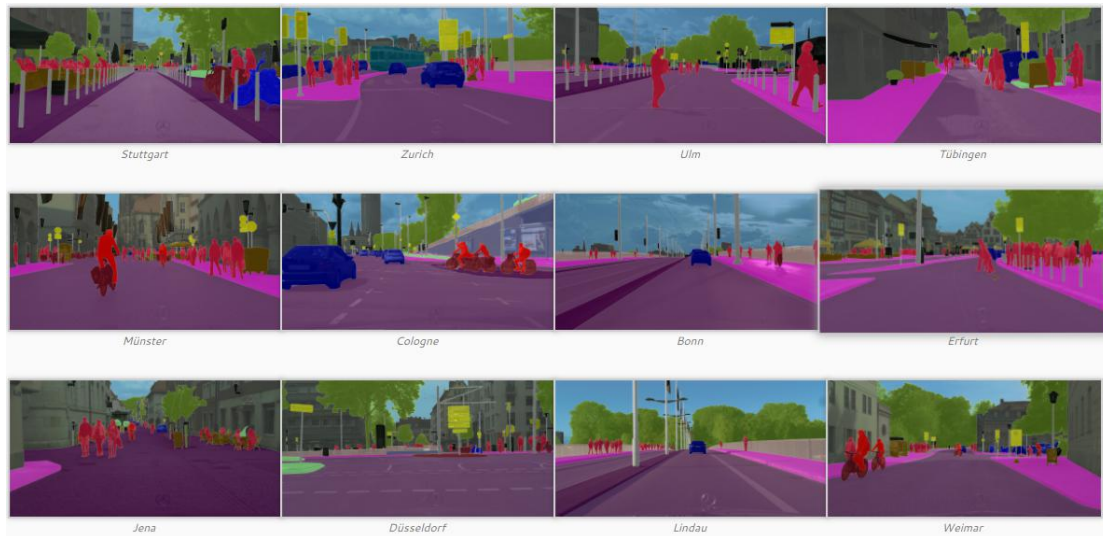


图 6-6 Cityscapes 数据集

### 6.1.13 RobotCar 数据集

2016 年,英国牛津大学发布了 RobotCar 数据集,该数据集记录了 2014 年 4 月至 2015 年 12 月间, RobotCar 平台(日产 LEAF 自动驾驶汽车)每周在牛津市中心运行 10 公里路线产生的数据,里程总计约 1010 公里驾驶。该数据集包含超过 2000 万张由六台车载相机拍摄的图片、激光测距信息、GPS 和惯性导航收集的地貌信息,总容量约为 23.15TB,涵盖了所有天气情况(包括雨雪,夜间,直射阳光等)。值得注意的是,在数据集采集的过程中,尽管车辆重复运行在同一区域,但这一地区的道路和建筑等环境信息出现了很大改变,因此基于此数据集,研究人员可以探究在现实动态城市环境中,自动驾驶车辆如何进行定位和地图映射。

### 6.1.14 rFpro

英国驾驶模拟公司 rFpro 发布了用于训练、研发自动驾驶汽车的仿真平台,可利用数字环境准确地映射真实世界,使汽车制造商能够在任何可想象的情况下测试其系统的性能。该平台的一个关键特点是“以非常高的精度,精确复制现实世界的测试环境”,使得自动驾驶车辆的各种传感器能够产生真实反应,其测试结果也就具有可靠性。在一项为期 3 年的项目中, rFpro 公司利用高精度扫描技术将大量真实道路转换为模拟测试场景,并最终创建了一个“模拟测试库”,用户可在库中选择各种不同的模拟测试场景,可精确控制从“天气”到“行人”等各种环境变量的输入。

### 6.1.15 Mapillary Vistas 数据集

Mapillary Vistas 数据集是一个新颖的大规模街道级图像数据集，其主要特点如下：（1）25,000 张高分辨率图像；（2）152 个目标类别；（3）100 个实例-特别注释的类别；（4）覆盖全球六大洲；（5）不同的天气、季节、时间、照相机和视点的变化。

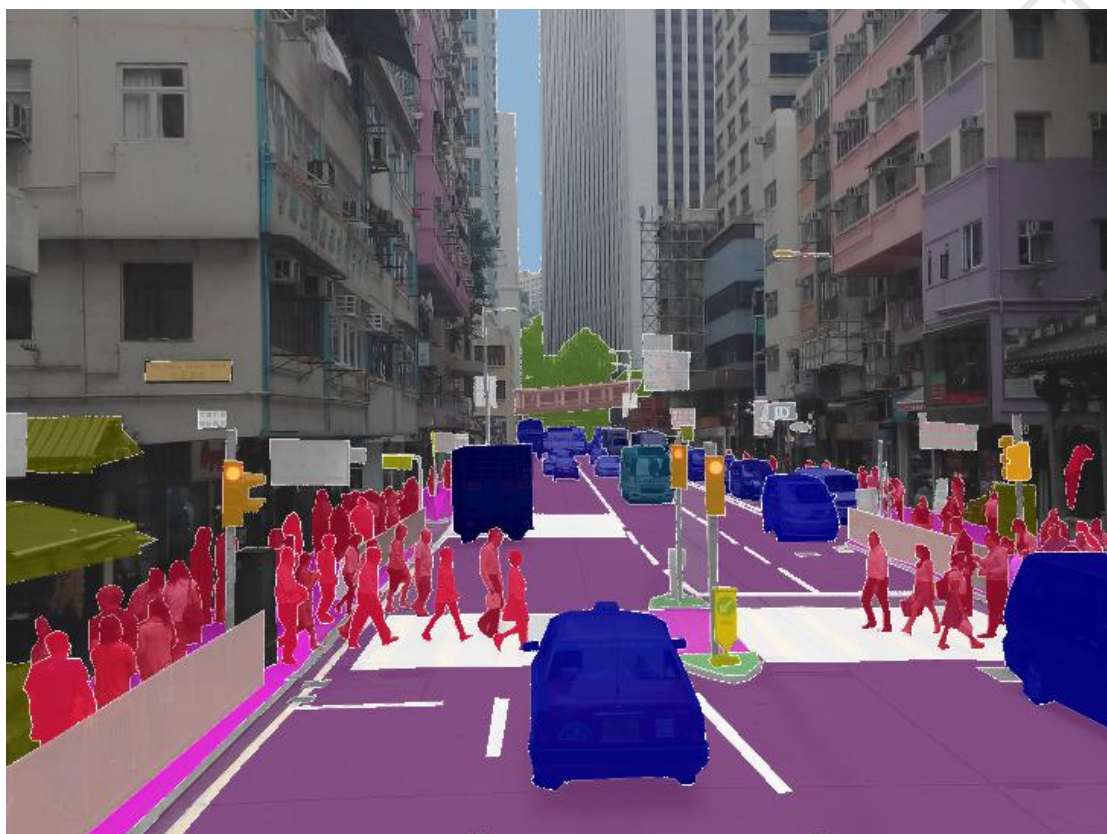


图 6-7 Mapillary Vistas 数据集

### 6.1.16 Caltech 数据集

美国加州理工学院发布了行人数据集 Caltech，包含大约 10 小时、分辨率为 640×480、30Hz 的视频，这些视频由一辆在城市环境中正常行驶的车辆采集，并对大约 250,000 个帧，共计 350,000 个边界框和 2300 个独特的行人进行了注释，包括边界框和详细遮挡标签之间的时间对应关系。





图 6-8 Caltech 数据集

### 6.1.17 Daimler Urban Segmentation 数据集

德国戴姆勒集团发布了 Daimler Urban Segmentation 数据集，该数据集由 5000 个经过校正的立体图像对组成，分辨率为 1024×440、500 帧，视频序列中的每 10 帧就带有 5 类的像素级语义类注释：地面，建筑，车辆，行人，天空。

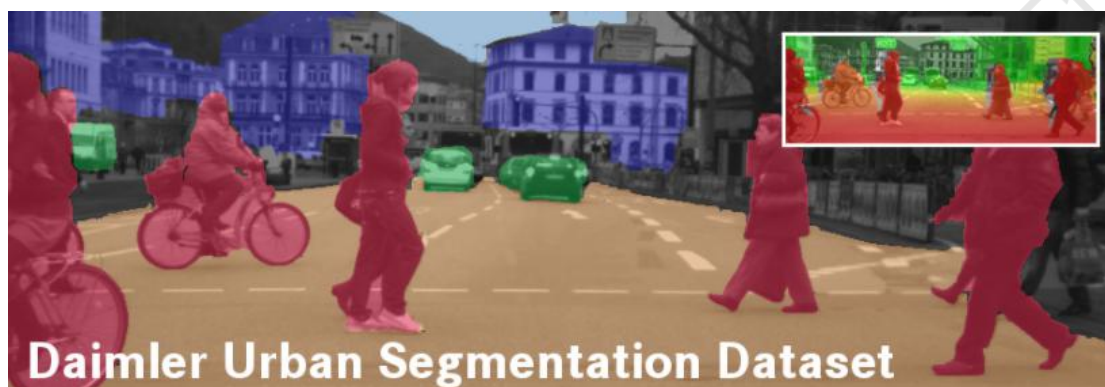


图 6-9 Daimler Urban Segmentation 数据集

## 6.2 国内智能网联汽车场景库研究现状

### 6.2.1 智能网联汽车驾驶场景数据库

2015 年，中汽数据（天津）有限公司（以下简称：中汽数据）开始开展中国智能网联汽车驾驶场景数据库研究及应用工作。中汽数据基于高精度场景数据采集平台（设备包括：多线激光雷达、固态激光雷达、毫米波雷达、视觉感知传感器和 GPS 惯性导航系统），采集了国内大量的场景数据（其中高速、城市快速路里程 50 余万公里、城市道路 10 万公里、城市停车场 2000 多个，数据体量近 1PB），采集范围涵盖全国大部分地区（东北、华北、华中、华东、华南、西南、西北），环境条件包括晴天、雨天、雪天、雾霾等。基于真实采集数据、符合 ISO/CNCAP/ENCAP/SAE 及 GB 等国内外标准法规数据、CIDAS 实车事故记录数据及危险场景数据，构建了面向 L3 级以下功能测试的测试场景库，共计 26 种。根据不同数据来源，场景库类型可分为：（1）标准法规仿真场景；（2）危险工况仿真场景；（3）自然驾驶仿真场景；（4）参数重组仿真场景。

此外，考虑到在实际研发过程中，各整车厂、供应商以及仿真工具商使用的数据格式标准不一，德国自动化及测量系统标准协会（Association for Standardisation of



Automation and Measuring Systems, ASAM) 推出了仿真领域的 OpenX 系列标准, 并获得了全球的关注。相应地, 国内 CASAM 工作组由中国汽车技术研究中心(数据资源中心)联合 ASAM 共同成立, 旨在组织中国企业开展 OpenScenario 等场景标准研究工作, 支撑 ISO/TC22/SC33/WG9 自动驾驶测试场景标准撰写工作, 并推动中国标准场景与国际化接轨。

### 6.2.2 中国交通事故深入研究(CIDAS)数据库

2011 年 7 月 15, 中国汽车技术研究中心联合国内外多家知名汽车企业启动了中国交通事故深入研究项目(以下简称: CIDAS), 旨在通过对中国道路交通事故的深入调查、分析和研究, 为中国乃至国际汽车行业提供基础数据支持和技术服务。CIDAS 项目成果已在相关汽车安全标准的制定与修订、车辆主被动安全技术研究, C-NCAP 测试评价等多个方面得到了广泛应用。

CIDAS 项目每年采集 800 起符合标准的交通事故(即至少一人受伤、至少一辆四轮车参与), 采用现场调查及监控视频、无人机回勘等方式, 调查区域包括长春、北京、威海、宁波、成都、佛山、黔西南、长沙等区域, 涵盖了平原、丘陵、盆地、高原等多种地形, 以及城市道路、高速公路、乡村道路、山区道路等不同道路类型。目前, CIDAS 数据库共计记录 5200 余起事故, 拥有 31 张数据表, 3027 项数据项。

### 6.2.3 中国典型驾驶场景库 i-Scenario

2019 年 12 月, 中国汽车工程研究院股份有限公司(以下简称: 中国汽研)发布了具备中国驾驶场景特征的虚拟仿真场景库: i-Scenario。参考德国 Pegasus 项目的场景分类体系及 ASAM 推出的 OpenDRIVE 和 OpenScenario 仿真格式, 构建了涵盖标准法规、人工经验数据、中国交通事故数据和自然驾驶数据四大数据源, 可应用于 MIL、SIL、HIL 等虚拟仿真系统。该场景库包含了数百例标准法规场景、3000 例经验式场景、5 万例功能场景和 150 例事故场景。

### 6.2.4 中国智能驾驶全息场景库建设(“昆仑计划”)

2017 年 6 月, 中国智能驾驶全息场景库建设项目(以下简称: “昆仑计划”)在国家智能网联汽车(上海)试点示范区启动。“昆仑计划”的目标是建设一个面向全行业的、加速智能网联汽车研发、测试和标准制定的中国道路驾驶场景库。该场景库涵盖了中国道路交通事故深度研究数据、超 50 万公里自然驾驶数据、人机共驾数

据以及道路交通流与路侧数据，可为智能汽车虚拟仿真加速测试平台、智能汽车人工智能训练平台、Vehil 测试平台、驾驶模拟集群测试平台、智能网联测试园区以及全息开放道路测试区提供核心场景支撑。

场景库的数据采集需求包括正常、危险和事故驾驶三种类型。此外，为增加智能网联汽车应对不同环境的能力，同时也考虑了一些实际交通不存在的场景。目前上海示范区可支持以下六类的数据：（1）事故场景数据；（2）自然驾驶场景数据；（3）驾驶模拟器场景数据；（4）路侧交通流/V2X 测试场景数据；（5）国内外标准规范场景；（6）自动重构场景。

#### 6.2.5 百度

2019 年 3 月，百度公开了一种基于真实数据构建仿真场景的方法，利用传感器扫描得到的街景图与真实轨迹，自动生成逼真图像和仿真移动模式，并发布了基于该技术的 ApolloCar3D 和 TrafficPredict 数据集。ApolloCar3D 数据集包括超过六万车辆的实例，配有高质量的三维 CAD 模型和语义关键点。TrafficPredict 是一个运动物体的轨迹数据集，包括时间戳，车辆 ID，类别，位置，速度，朝向等信息，轨迹总长度达到 1000 多公里。

#### 6.2.6 自动驾驶场景库“镜”

2019 年，清华大学苏州汽车研究院发布了自动驾驶场景库“镜”。“镜”场景库主要包含以下几个部分：（1）运用机器视觉、深度学习等技术，基于上帝视角提取的大规模交通流轨迹数据集 Mirror-Traffic；（2）面向 L2 及以下的标准法规测试场景；（3）面向 L3 及以上的高速公路和城市道路的驾驶场景；（4）边缘场景；（5）泊车场景；（6）自动驾驶物流车场景等。

#### 6.2.7 公安部交通研究所

参考国内交通情况及国外测试基地管理模式，公安部交通研究所初步设计了我国自动驾驶能力测试场景方案。目前，测试环境已形成以封闭场地为点、以半开放道路为线、以全开放道路为面的测试布局。其中，封闭场地占地 200 亩，拥有公路、城市道路、高速公路、环道、多功能、室内等六大测试区；半开放道路环境拥有 10 千米测试道路、146 个视频全程监控点和 9 个信控路口。自动驾驶能力测试方案包含封闭、半开放、开放、高速、虚拟 5 种测试环境，2 个测试评价库（测试场景库



和评价规则库), 以及 1 个自动驾驶能力测试评价平台。

#### 参考文献:

- [1] [https://m.sohu.com/a/232555924\\_297649](https://m.sohu.com/a/232555924_297649)
- [2] <https://www.auto-testing.net/news/show-96278.html>
- [3] [https://blog.csdn.net/weixin\\_41361987/article/details/79991047](https://blog.csdn.net/weixin_41361987/article/details/79991047)
- [4] <http://shujujishi.com/dataset/8264fbc0-a53d-4df4-84e4-63a3d86c5c5b.html>
- [5] [https://blog.csdn.net/qz\\_39337332/article/details/105335457](https://blog.csdn.net/qz_39337332/article/details/105335457)
- [6] [https://www.sohu.com/a/117578595\\_465975](https://www.sohu.com/a/117578595_465975) [https://www.sohu.com/a/359543655\\_717788](https://www.sohu.com/a/359543655_717788)
- [7] <http://www.cheyun.com/content/18087>
- [8] [https://zhuanlan.zhihu.com/p/61023298?from\\_voters\\_page=true](https://zhuanlan.zhihu.com/p/61023298?from_voters_page=true)
- [9] <https://link.zhihu.com/?target=https%3A//usa.honda-ri.com/hdd/introduction/h3d>
- [10] <https://www.nuscenes.org/>
- [11] <https://usa.honda-ri.com/h3d>
- [12] <https://www.mapillary.com/dataset/vistas?pKey=xyW6a0ZmrJtjLw2iJ71Oqg&lat=20&lng=0&z=1.5>
- [13] [http://www.vision.caltech.edu/Image\\_Datasets/CaltechPedestrians/](http://www.vision.caltech.edu/Image_Datasets/CaltechPedestrians/)
- [14] <https://robotcar-dataset.robots.ox.ac.uk/>
- [15] <http://www.51hitech.com/about/news-detail?id=330>
- [16] <https://bair.berkeley.edu/blog/2018/05/30/bdd/>
- [17] <https://bdd-data.berkeley.edu/>
- [18] <https://xw.qq.com/cmsid/20190402A0E8C600?f=dc>
- [19] <http://news.xinhua08.com/a/20180914/1777780.shtml>
- [20] 中国电动汽车百人会智能网联研究院, 全球自动驾驶发展动态 (2020.03.23-2020.03.29)

## 第 7 章 国内外智能网联汽车功能测试评价体系

由于面向预期功能安全的测试评价体系尚在建设中，因此，本章节将针对国内外智能网联汽车功能测试评价体系进行阐述。与传统汽车相比，智能网联汽车有其特殊性，需要根据智能网联汽车的特点有针对性地对其开展测试和评价，以降低汽车行驶的安全性为前提，全面评价智能网联汽车的各项性能，确定智能网联汽车测试和评价的目标。将智能网联汽车测试评价方法与汽车整车的产品开发过程进一步融合，按照产品开发过程 V 模型，在产品开发的阶段使用合适的测评方法，可以建立指导产品开发的测试评价体系。在这个测试评价体系中要充分考虑场景的重要性，确保各阶段测试所涵盖的场景有一定的代表性，能够反映实际驾驶环境的真实情况，要建立场景生成、使用、优化的闭环控制系统，以此不断推进场景的丰富程度。本章节主要包括国外智能网联汽车功能测试与评价现状、国内智能网联汽车功能测试与评价现状及智能网联汽车测试评价发展趋势分析三个部分，为我国预期功能安全测试评价体系建设提供参考。

### 7.1 国外智能网联汽车功能测试与评价现状

#### 7.1.1 虚拟仿真测试

随着人工智能技术的发展，面对传统汽车所存在的“交通拥堵、环境污染、事故频发、能源短缺”等问题，自动驾驶汽车为其提供了新的解决途径。对于提高自动驾驶汽车研发效率、健全技术标准和法律法规、推进相关产业创新发展而言，建立科学完善的测试评价体系是至关重要的。为确保自动驾驶汽车上路的安全性，美国于 2016 年出台了《自动驾驶法案》，首次对自动驾驶汽车的生产、测试和部署进行监管。然而，汽车系统的复杂性，以及多变的天气、复杂的交通环境、多样的驾驶任务和动态的行驶状态等因素为自动驾驶汽车的测试增加了难度。因此，虚拟测试成为了自动驾驶汽车测试评价的一种重要技术手段。

目前，自动驾驶汽车虚拟测试方式主要包括 3 种。第一种是模型在环测试，模型在环测试的关键在于建模的精度与计算效率。在车辆动力学建模方面，Dieter 等对车辆动力学建模与仿真进行了系统的总结，除了基于理论的车辆动力学建模方法之外，还有许多其他建模方法，例如：基于系统辨识的建模方法、基于数据驱动的建模方法、面向对象的建模方法等。Sundaravadivelu 等在 AVL-CRUISE 中搭建虚拟



测试环境，并与 CarMaker 进行联合仿真，对车辆动力学模型进行测试验证。Hossain 等基于 Unity3D 跨平台游戏引擎搭建了自动驾驶虚拟测试环境，测试了传感器感知状态与车辆的动力学特性。此外，美国 Waymo 公司开发了 CarCraft 自动驾驶虚拟测试平台，如图 7-1 所示。Waymo 已经研发出多个完整的虚拟城市，并且在 2018 年的 8 月，宣布其自动驾驶汽车在公共道路上的行驶里程达到了 900 万公里，模拟仿真测试里程超过 50 亿英里。

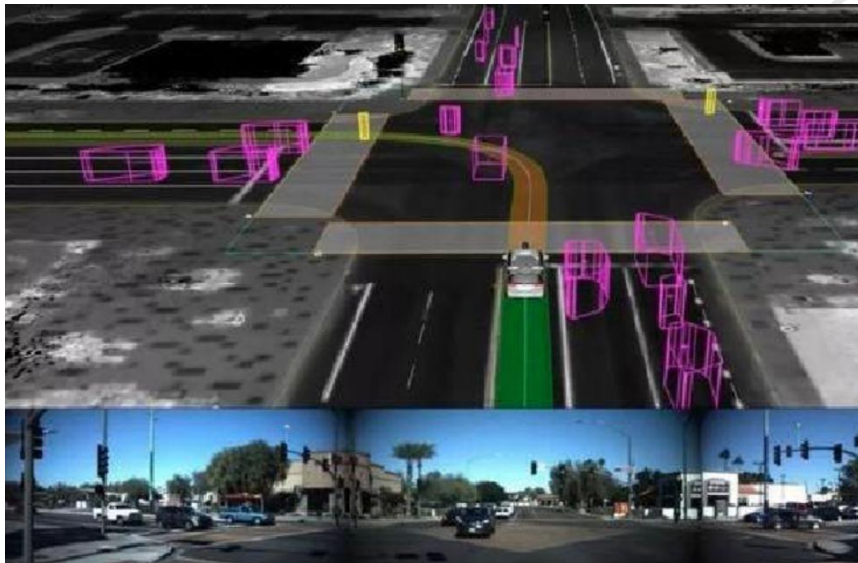


图 7-1 CarCraft 开发软件

其次是硬件在环测试。硬件在环测试主要包括环境感知系统在环测试、决策规划系统在环测试与控制执行系统在环测试等，其测试要求包括：持续测试、组合测试、扩展性测试。Hao 等搭建的雷达在环试验台通过模拟电波暗室内的射频环境，准确地生成了带宽雷达目标回波，并得到了带宽雷达目标散射中心的高分辨率距离分布。Ma 等提出一种 V2V 环境下面向智能网联汽车应用的 HIL 测试系统，并将协同自适应巡航控制（Cooperative Adaptive Cruise Control, CACC）作为用例进行了测试。该系统集成了一台智能网联汽车、DSRC 设备和一个交通模拟程序，通过仿真实时效仿雷达传感器和 DSRC 通信的真实性能，验证多种感知条件对 CACC 系统队列稳定性的影响，为测试 CACC 应用程序提供了一种经济有效的方法。Hager 等提出了雷达、摄像头、V2X 等多源传感融合系统在环的试验框架，通过闭环测试得到其感知数据及车辆 CAN 总线数据，其提出的基于 dSPACE 的测试方案还可实现传感器数据流的实时修改，并可直接将数据注入 ECU 之中进行交互测试。Drolia 等

通过模型模拟车辆的加速、横摆、驱动力等参数，实现车辆牵引力控制、巡航控制等控制器在环测试。We 等将实时仿真技术应用到控制器在环的试验测试中，其可以在系统开发的早期阶段验证功能的正确性以及实时性。

最后是车辆在环测试。车辆在环测试是将整车嵌入到虚拟测试环境中进行测试，通过模拟场景来测试整车性能，主要包括封闭场地车辆在环和转毂平台车辆在环。此类测试的关键在于将车辆信息传递给模拟环境以及将模拟环境中产生的传感器信息传递给车辆控制器。Tamas 等开发了一种基于开源交通流量模拟器 SOMU 的仿真测试环境，可模拟测试车辆周围的道路环境、其他交通参与者等环境，通过 CAN 总线实现测试车辆与仿真软件之间的数据连接，实现了在现实空旷环境中的车辆在环测试。

### 7.1.2 场地测试

道路测试是开展智能网联汽车技术研发和应用不可或缺的重要环节之一。确保车辆在各种道路交通状况和使用场景下都能够安全、可靠、高效的运行，需要对其功能进行大量的测试验证，这需经历复杂的演化过程。因此，智能网联汽车在正式进入市场之前，必须要在真实交通环境中进行充分地测试，全面验证自动驾驶功能。

在自动驾驶测试评价体系中，依托封闭测试开展自动驾驶功能、安全性验证工作愈发重要。因此，模拟尽可能多的交通场景，不断积累测试数据，将为自动驾驶汽车技术迭代提供有力支撑。能够满足封闭测试需求的自动驾驶测试场也将扮演重要角色，目前全球范围内正加速布局测试场的建设，接下来，本节将分别对各国的建设情况展开介绍。

美国：2015 年 7 月，全球首个自动驾驶封闭测试区 M-City 正式开园并引发广泛关注，之后世界各国开始竞相开展自动驾驶测试场的建设。2016 年 11 月，美国交通部公布“自动驾驶试验场试点计划”，并于 2017 年 1 月 19 日确立了 10 家自动驾驶试点试验场。美国交通部指定的这 10 家自动驾驶试点试验场分布于 9 个州，分别位于美国的东北部、东部、东南部、北部、中西部、南部、西部、西南部，满足了美国交通部希望的地区发展平衡的要求。这些试验场具有差异化的气候条件和地貌特征，使得自动驾驶汽车可以在更加丰富的条件下开展测试。

英国：英国政府计划投资 1 亿英镑用于建设网联与自动驾驶汽车测试设施，并于 2017 年 3 月 30 日宣布启动第一阶段投资竞标。该计划的目标是沿伯明翰和伦敦

之间的 M40 走廊，建设网联与自动驾驶汽车先进技术集群，同时将基于英国现有的部分网联与自动驾驶汽车测试中心，在英国汽车产业核心区域（包括西米德兰兹郡的考文垂、伯明翰、米尔顿凯恩斯，以及牛津和伦敦）集中建设测试设施集群。

德国和法国：2017 年 2 月 8 日，德国交通部在柏林宣布，德国和法国计划在两国之间的一段跨境公路上测试自动驾驶汽车。这一路段长约 70 公里，从德国西部萨尔兰州的梅尔齐希（Merzig）延伸至法国东部的梅斯（Metz）。两地之间相距约 1 小时车程，以实现在真实的跨境交通中测试自动驾驶与网联汽车技术。

日本：2016 年 2 月 12 日，日本经济产业省制造产业局汽车课正式公布“无人驾驶评价据点整備”项目，并征集承接单位，该项目最终由筑波市茨城县的日本机动车研究所（JARI）承接，并于 2016 年开始建设。自动驾驶汽车测试场 J-Town 于 2017 年 4 月面向日本国内企业和研究机构开放测试，企业、研究机构均可付费使用所需的道路进行测试。

韩国：2016 年 8 月，韩国政府宣布开放一个约 36 万平方米的场地(K-City)供自动驾驶车辆进行性能测试。2018 年 12 月，韩国交通部表示 K-City 已建成，可测试基于 5G 移动网络的自动驾驶汽车。

瑞典：AstaZero 是位于瑞典哥德堡附近的大型测试区域，于 2014 年 8 月完成一期建设并投入使用，占地约 200 万平方米，基于传统汽车试验场的改造升级，可为自动驾驶汽车提供完整的测试环境与条件，它的主要投资和使用方是汽车厂商沃尔沃。

新加坡：2014 年 8 月，新加坡陆路交通局和新加坡科技研究局合作发起了新加坡自动驾驶汽车计划，并成立了新加坡自动驾驶汽车动议委员会，用于监管自动驾驶汽车的研究和测试。从 2015 年 1 月开始在纬壹科技城开放了近 5 公里的路段，提供给符合要求的无人驾驶汽车测试使用。

### 7.1.3 公开道路测试准入条件与道路测试

#### 一、公开道路测试准入条件

国外对公开道路测试准入条件主要包括两方面：

##### （1）技术要求

该类要求包括自动驾驶汽车的车辆标准、必要的驾驶切换系统、行驶情况记录系统及特定的安全功能标准。具体包括：

车辆标准：美国内华达州、加州法规均要求拟进行测试的自动驾驶汽车必须满足相应的安全标准、技术性能标准等。

自动驾驶和人为驾驶的切换系统：美国内华达州、加州以及新加坡的法规均要求自动驾驶汽车必须装有方便操作员重新控制自动驾驶汽车的驾驶模式切换系统。

行驶状况的记录系统：美国加州以及新加坡的法规要求自动驾驶汽车应装有记录系统，以捕捉和储存数据。其中，加州的法规特别要求该记录系统能够至少捕捉和存储交通事故发生前 30 秒的传感器数据，且该数据为只读数据，须保留 3 年。内华达州法规要求车辆须装有显示自动驾驶系统运行状况的视觉指示器。

安全功能：美国加州、内华达州以及新加坡的法规均要求自动驾驶汽车应装有在自动驾驶系统出现故障时提醒驾驶人接管汽车的警告装置。其中，加州法规还要求自动驾驶汽车应具备自动驾驶模式是否开启的车内提示装置以及驾驶人能自如地开启和关闭自动驾驶模式的功能等。

## （2）自动驾驶汽车测试的事先计划

有些国家要求测试者在进行公开路试之前必须先制定全面的事先计划。具体讲，测试者应提前向相应的主管部门（如内华达州、加州为机动车管理局、密歇根州为州务卿）提出申请，公开路试必须在获得批准之后方可进行。澳大利亚的法规要求测试者在进行自动驾驶公开路试之前必须先与当地相关的道路交通主管部门进行沟通，以确认是否需要申请许可或者豁免。如需要申请许可或者豁免，申请者应提供测试的细节（包括测试地点、测试所使用的技术等），以便监管部门了解测试可能会发生的交通风险，并评估测试者相应的应对措施、测试对于基础设施和网络的要求、与公众及其他利益相关者的关系（可能涉及与应急服务部门之间的安排）、在测试中可能进行的调整 and 改变（测试者可能在测试中更新软件或升级硬件）等。

## 二、道路测试

目前，欧洲、美国、日本等国家都加快了智能网联汽车的产业布局，加快推动了自动驾驶相关法案制定，相继出台示范运行和道路测试管理规范。

### （1）美国

美国内华达州于 2011 年 3 月率先进行了道路测试立法、发放测试牌照，美国联邦交通部于 2016 年 9 月发布了《美国自动驾驶汽车政策指南》、2017 年 9 月发布《自动驾驶系统 2.0：安全愿景》，美国众议院 2017 年 7 月通过了《自动驾驶法案》，加



州 2018 年 2 月修改无人驾驶测试法规，允许无驾驶人员情况下进行智能网联汽车道路测试。

美国各州的智能网联汽车道路测试主要执行申请制，同时也有考试制。例如，加利福尼亚州规定申请企业只需要提供车辆以及司机的基本信息、车辆保险证明、公司证书即可，申请费仅为 3600 美元，申请成功即可向政府备案后在所有类型的路段上开展不配备安全驾驶人测试。内华达州的智能网联汽车道路测试执行考试制，首先，提供 10000 英里（16090 km）的封闭测试场测试证明，其次，通过封闭测试场考试，政府人员随车进行打分，考核成功后只能在特定路段开展无配备安全驾驶人测试。

目前，美国已经允许载人测试，并已开展无人驾驶出租车的运营。例如，2017 年 Waymo 在亚利桑那州凤凰城开始示范运营无人驾驶出租车，但对乘客、线路等有一定的限制。2019 年，Waymo 在加州获得无人驾驶出租车运营许可。

美国大部分州规定测试车辆必须配备测试数据记录装置，并在当地机动车管理局登记车辆基本信息，如加州要求测试主体登记车辆的基本信息并安装测试数据记录装置。部分州持相对开放的态度，对车辆几乎无要求，如亚利桑那州规定测试企业在州机动车管理局登记即可。密歇根州规定测试主体在本州登记，同时车辆合法即可，数据由测试主体自行核验，测试主体每年提交测试报告即可。

## （2）欧洲

2015 年 7 月，英国发布无人驾驶汽车路测指南《无人驾驶汽车发展路径：测试实践准则》，分别从测试主体、测试车辆及测试驾驶人三方面确定相应标准。2017 年 5 月，德国通过了关于自动驾驶汽车的首部法律《德国交通案》，允许驾驶者在双手离开方向盘或视线离开道路情况下进行道路测试。德国、英国和荷兰均按申请制进行智能网联汽车道路测试，测试主体只需要将相关材料提交当地主管部门即可，但是英国规定必须在封闭场地进行充分的测试。在道路测试中，德国和英国对车辆的要求如表 7-1 所示。此外，德国和英国在开展道路测试时已覆盖国内全部道路类型，但需要在特定道路上开展配备安全驾驶人测试，荷兰众议院颁布的《自动驾驶测试法（草案）》允许在特定路段开展不配备安全驾驶人的测试。德国的智能网联汽车道路载人测试需要相关技术专家给出指导性意见即可，英国和荷兰则无特殊要求。欧洲的德国、英国都要求测试车辆安装数据记录装置，并将数据上报主管部门。

表 7-1 欧洲智能网联汽车道路测试对车辆的要求

地区/国家	道路测试对车辆的要求
德国	<ul style="list-style-type: none"> <li>①车辆必须通过TüV的认证；</li> <li>②测试主体必须为测试车辆购买保险；</li> <li>③车辆必须配备数据记录装置；</li> <li>④车辆由持有运营许可的汽车生产商生产；</li> <li>⑤车辆需符合《德国道路车辆登记和许可条例》对机动车准入的限制，不符合的车辆需要向州提出豁免，联邦各州可以自由的添加条款作为豁免条件。</li> </ul>
英国	<ul style="list-style-type: none"> <li>①测试车辆符合机动车安全标准，车龄超过3年的需要通过机动车运行安全验；</li> <li>②在封闭测试场内完成基本的测试工作，验证自动驾驶系统的稳定性；</li> <li>③测试机构应当充分评估测试车辆在公开道路测试的安全性；</li> <li>④自动驾驶系统应确保在发生紧急情况时向安全驾驶人发出警报并可以随时切换到手动驾驶模式；</li> <li>⑤测试车辆要安装行车记录仪，记录测试数据；</li> <li>⑥自动化控制设备和自动驾驶系统应内置安全防护，防止非法网络入侵；</li> <li>⑦自动驾驶系统各个版本都应该完整归档和记录，所有软件版本需在封闭场地测试后方可在公开道路测试。</li> </ul>

### (3) 日本

2016年5月，日本发布了《关于自动驾驶系统的公道实证实验的方针》，同月颁布了《自动驾驶汽车道路测试指南》，并于2017年秋季开始在高速公路、一般公路上对自动驾驶系统进行大规模测试试验。

《自动驾驶汽车道路测试指南》规定测试主体在向主管机构提交测试申请并上报测试计划后，即可在所有区域开展自动驾驶道路测试，驾驶位可不再配备安全驾驶人，但在测试过程中副驾驶位上仍然需要配备测试驾驶人。该项指南和《远程自动驾驶系统道路测试许可处理基准》都未在载人测试方面提出禁止规定。然而，日本对测试车辆的要求较为严格，具体如表 7-2 所示，并且日本政府规定可进行道路测试的企业需要向警方、市政、交通部门提交测试数据。

表 7-2 日本智能网联汽车道路测试对车辆的要求

地区/国家	道路测试对车辆的要求
日本	<ul style="list-style-type: none"> <li>①符合《道路运输车辆安保基准》对安全的要求；</li> <li>②在实验场地内开展充分细致的测试，确保自动驾驶状态下的测试车辆能够安全行驶；</li> <li>③车身上标示“正在进行自动驾驶系统测试”的字样；</li> <li>④安装行驶记录仪和交通事故数据记录仪等装置；</li> <li>⑤当自动驾驶和手动驾驶模式间切换时，应对车辆操作进行恰当的授权，如自动驾驶模式开启或结束时，通过鸣响警示音进行提示；</li> <li>⑥自动驾驶系统应确保在发生紧急情况时驾驶人能够进行手动驾驶操作；</li> <li>⑦测试机构应根据《网络安全基本法》的规定，切实采取网络安全防护措施确保自动驾驶系统安全，防止网络非法入侵；</li> <li>⑧自动驾驶系统软件升级（包括已通过道路测试确认安全性的自动驾驶系统上的新增功能）应重新在封闭道路上进行测试，确认系统软件安全可靠后，才可进行道路测试。</li> </ul>

此外，法国于 2014 年 2 月公布了自动驾驶发展路线图，向全球汽车厂商开放道路进行自动驾驶汽车测试。联合国于 2016 年 3 月正式修订《维也纳道路交通公约》，允许自动驾驶技术应用到交通运输中。世界车辆法规协调论坛（WP29）也在制定自动驾驶技术相关的技术法规，以推动道路测试规范。

#### 7.1.4 评价体系与可接受风险的测试指标

##### 一、评价体系

完善的测试评价体系是支撑智能网联汽车自动驾驶技术研发的必备条件。目前，国内外面向智能网联汽车的安全测试都还处于探索阶段，标准和体系的制定都在进行中，尚未形成一套完整成熟的测试评价体系。大多数国家仅通过颁布相关法规政策、制定部分功能标准体系来进行自动驾驶技术的测试评价，且测试评价的内容不尽相同，主要分为：基本的功能与性能、预期功能安全性、信息网络安全、决策能力与安全意识以及车路协同与通信技术五个部分。国外自动驾驶 ADAS 功能测试标

准体系的当前进展如表 7-3 所示。

表 7-3 国外ADAS测试标准体系

地区/国家	道路测试对车辆的要求
美国	<p>2011: FCW/LDW</p> <p>2012: AEBS/FCW/LDW/BUA/BSD</p> <p>2015: BUA (SUVs &amp; Vans强制要求)</p> <p>2020: 期望自动驾驶</p>
欧盟	<p>2013: AEBS/LDW (强制要求 N2,N3,M2,M3 类新型车辆)</p> <p>2014-2017: FCW/AEBS/LDW/BSD(ENCAP Star-Rating)</p> <p>2020: 期望自动驾驶</p>
日本	<p>2013: AEBS/LDW 强制要求高于 3.5t 的新卡车 (防撞)</p> <p>2020: 期望自动驾驶</p>

美国方面，诸如 Waymo、福特、通用、优步等企业率先搭建智能驾驶测试车队，以不同的方式尝试开展商业化应用的运营服务。在大规模进入市场之前，智能驾驶汽车需要在实际场景中进行长时间的测试，不断验证系统、功能的可行性、安全性及稳定性。

欧洲 AdaptIVe 评价方法主要从四个维度展开，即技术评价、性能评价、交通流评价和对安全性与交通环境影响评价。具体地，技术评价包括对自动驾驶功能、性能的评价。用户相关评价包括驾驶人与车辆的交互、驾驶任务切换及用户满意度评价。交通流评价包括自动驾驶汽车与交通流的融洽度评价，其他交通参与者满意度评价。安全性和交通环境影响评价是指对自动驾驶汽车渗透进道路交通后道路交通安全性及交通效率、能耗的影响进行评价，具体评价方法如图 7-2 所示。



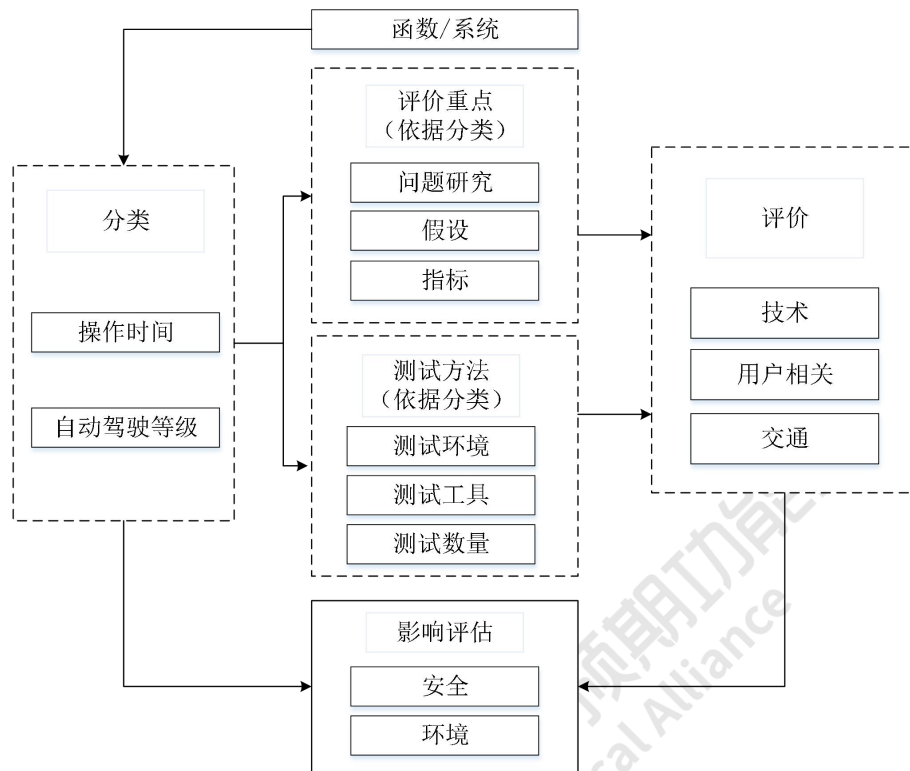


图 7-2 AdaptIVe 评价方法

## 二、可接受风险的测试指标

美国对道路测试的风险控制主要通过自动驾驶政策指南，鼓励汽车厂商自愿遵守，认可和支持由相关组织协会制定自动驾驶技术的自愿性标准，作为能有效加快自动驾驶技术推广应用的非强制性手段。

美国在自动驾驶政策指南中，针对自动驾驶系统安全的设计和验证提出了较为详细的要求，即应以自动驾驶系统不存在不合理的安全性风险为目标，并基于系统工程方法进行鲁棒性设计和验证过程。该过程不仅应该包含当车辆在电力、电子、机械失效或者软件错误时维持安全状态的功能，还应该描述处理自动驾驶系统失效的冗余性设计和安全策略。例如，Waymo 的系统安全计划涉及 5 个不同的安全领域，包括行为安全、功能安全、碰撞安全、操作安全和非碰撞安全。英伟达将多样性和冗余设计应用到每个解决方案中，以实现最高级别的计算，从传感器到处理器再到算法，确保发生故障时永远不会只有一条安全防线。

自动驾驶车辆的测试安全与其运行设计域（Operational Design Domain, ODD）密切相关。道路测试中，车辆如遇到超出 ODD 的情况，则发生事故的风险将急剧提高。美国的自动驾驶政策指南要求：应该鉴定并记录每一个自动驾驶系统的 ODD，

并应使用包括以下信息来定义自动驾驶系统的性能，即可安全运行的道路类型、地理范围、速度范围、系统的操作环境(天气，白天和夜间等)。例如，Waymo 的适用范围就涵盖了地理位置、道路类型、速度范围、天气、时间、国家和地方性交通法律法规。对自动驾驶汽车系统性能测试，美国自动驾驶政策指南要求测试车辆在正常操作时的性能、在防撞情况下的性能以及与 ODD 有关的退出自动驾驶策略的性能。这种对测试过程中风险的控制措施可在一定程度上降低路测时的风险。

## 7.2 国内智能网联汽车功能测试与评价现状

国内各汽车制造商在整车开发过程中逐步建立了功能测试团队，现已具备相应的测试能力，可从网络测试、节点功能测试、系统集成测试、整车测试等四个维度，利用 SIL、HIL、MIL、随机测试等测试方法对汽车的功能设计进行充分验证和测试。然而，随着智能驾驶和智能网联技术的不断发展，应用于车辆的控制器数量剧增，功能愈发复杂。此外，新型网络、新型传感器、功能安全、信息安全等新技术的引入也对整车厂的测试能力和测试方法提出了新的要求。因此，各大汽车制造商正着力于研究新的测试方法、建立相应测试场景，以满足智能网联汽车的应用测试需求。

### 7.2.1 虚拟仿真测试

为实现车辆的智能控制，大量的电子控制单元（Electronic Control Unit，ECU）被嵌入到智能网联汽车中，对 ECU 的测试工作已成为了 ECU 开发过程中的关键环节。据统计，在 ECU 的开发周期中，ECU 软硬件的研发工作量只占整个开发周期工作量的 30%~40%，剩余 60%~70%的工作量都是用于测试 ECU 的软硬件性能。在 ECU 的软硬件测试过程中，硬件测试工作相对规范、简单，然而由于汽车自身的复杂性与特殊性，软件的测试过程相对困难。为解决车用 ECU 测试问题，研究人员提出了以下三种与车用 ECU 开发过程相关的仿真测试方法，即模型在环仿真测试方法(Model-in-the-Loop，MIL)，硬件在环仿真测试方法(Hardware-in-the-Loop，HIL)和软件在环仿真测试方法(Software-in-the-Loop，SIL)，这些仿真测试方法以车辆的动力学模型为基础，可应用于 ECU 研发过程中的不同阶段，完成不同的功能测试。

由于具有测试场景丰富、计算速度快、测试效率高、资源消耗低、可重复性好、可嵌入车辆研发的各个环节等特点，虚拟测试受到了各汽车制造商与研究机构的广泛关注。例如，美国 Waymo 公司与中国百度公司等均建立了相应的自动驾驶模拟系

统，并开展了大量的虚拟测试。

在模型在环测试方面，2015 年成立的 51VR 科技公司自主研发了自动驾驶仿真平台、虚拟驾驶仿真平台，如图 7-3 所示。该自动驾驶仿真平台的功能覆盖了道路环境搭建、智能交通流、传感器及动力学仿真，可以方便地接入自动驾驶感知和决策系统。此外，同济大学团队基于 PreScan 测试平台，对其所提出的自动紧急制动系统进行了充分测试验证，同时对紧急制动过程中的相关参数进行了探究。吉林大学自主研制了 PanoSim 虚拟测试软件平台，并基于该平台对驾驶人驾驶习性进行了聚类分析，提出了考虑不同驾驶习惯的 ADAS 控制策略，进行了算法仿真验证。



图 7-3 51VR 自动驾驶仿真平台

在硬件在环测试方面，环境感知系统在环测试主要包括相机在环测试、雷达在环测试、V2X 在环测试以及多源传感融合系统在环测试等。吉林大学针对 V2X 测试，研发了一种结合虚拟环境和真实环境的端到端测试系统，此系统可以承担整个协议栈的测试任务。决策规划系统在环是指将真实的车辆控制器放入虚拟的整车环境中，通过仿真模型来模拟受控对象的状态，并通过 CAN 接口、I/O 接口等将车辆控制器与仿真模型进行连接。西安交通大学提出一种新型 HIL 仿真平台，该平台实现了运动学模型、虚拟传感器和各种仿真场景的柔性构建，并开发了硬件 ECU 接口，平台可利用 HIL 仿真对自动驾驶车辆场景感知、路径规划、决策及控制算法进行闭环测试与评价，可将测试算法快速迁移到真实自动驾驶汽车上。控制执行系统在环测试主要包括制动系统在环测试、转向系统在环测试、驱动系统在环测试等。吉林大学提出一种电子液压制动与电子机械制动相结合的制动控制系统，并基于

dSPACE Autobox 和 CarSim 搭建了硬件在环平台进行测试与算法验证。

在车辆在环测试方面，中国科学院大学基于 APC 理论，搭建了与实际交通平行执行的自动驾驶汽车测试验证平台，对自动驾驶汽车的环境感知、动态认知规划、智能决策等功能进行了验证。长安大学团队研发了一种整车在环仿真的自动驾驶汽车室内快速测试平台，该平台实现了试验台、虚拟仿真场景和自动驾驶汽车之间的深度融合，可在各种虚拟交通场景下测试自动驾驶汽车轨迹规划、轨迹跟踪及执行器控制性能，大幅缩短了自动驾驶汽车的研发周期，提高了测试效率。

### 7.2.2 场地测试

场地测试包括普通道路、专用试验场、专用道路等测试。车辆在批量生产之前需进行高温高湿、高寒高原等道路测试，以及交通部专用场地测试。智能驾驶技术引入后，需进一步开展全国主要交通道路的路试和数据采集，以验证车辆的安全性，丰富的测试环境能够满足智能网联汽车在不同条件下的测试需求，为各测试示范区测试数据共享后的数据多样化与全面性提供基础条件。

2018 年 4 月，工信部、公安部、交通部联合发布了《智能网联汽车道路测试管理规范（试行）》，其中规定了道路测试需要遵守的基本原则，为智能网联汽车的道路测试提供指导，同年 12 月，工信部发布了《车联网（智能网联汽车）产业发展行动计划》。

国内智能网联汽车测试示范区包括封闭测试区和开放道路测试两部分。封闭测试区中有工信部等部委支持推进的国家级测试示范区，主要分布在东北、华北以及沿海等汽车产业发达的地区，具有差异化的气候条件和地貌特征，形成区域性互补。在开放道路测试上，北京、上海、天津、重庆、广州、武汉、长春、深圳、杭州、无锡、长沙、保定、济南、平潭、肇庆等多座城市出台了道路测试管理规范，划定了具体道路开放区域。

目前已建成的测试示范区基本覆盖了城市道路、乡村道路等多种道路场景，具备较为完善的场景设施和智能网联设备，部分测试区已经搭载了 5G 通讯设备，信号可覆盖全封闭测试区。上海、长春、北京、长沙等测试区积极同高校和企业合作，现已具备一定的科研能力，参与了智能网联汽车的改装和开发，融合了研究和测试工作。接下来，本节将对国内的一些代表性示范区展开介绍。

国家智能汽车与智慧交通（京冀）示范区：该示范区是为落实工业和信息化部、





北京市人民政府、河北省人民政府签订的“基于宽带移动互联网的智能汽车与智慧交通应用示范部省合作协议”而设立，于2016年1月18日签署了合作框架协议，由北京智能车联产业创新中心运营。北京智能车联产业创新中心是由千方科技主导，联合国内十多家相关的企业、高校，在北京经信委、经济技术开发区管委会指导下共同成立的公司，同时该公司也是北京自动驾驶车辆道路测试的第三方服务机构，负责北京市自动驾驶车辆测试申请、现场审核、日常监管等工作。2018年2月，北京市采纳全国首个自动驾驶能力测评团体标准《自动驾驶车辆道路测试能力评估内容与方法 T/CMAX 116-01-2018》作为北京市自动驾驶车辆道路测试前能力评估的依据，并发布了《北京市自动驾驶车辆道路测试能力评估内容与方法（试行）》，实现了从标准到政策的落地。

国家智能汽车与智慧交通（河北）示范区：该示范区是由工业和信息化部指导，长城汽车具体实施建设和运营的国家级智能汽车与智慧交通应用示范项目。示范区一期工程为封闭测试区，位于长城汽车徐水试验场内，占地13.4万平方米，总投资6000余万元人民币。测试区新建了长度5公里的测试道路，该测试道路主要由十字路口、五岔路口、环岛及特殊路面等组成，充分模拟了城市及城郊交通工况。未来，示范区二期、三期工程将结合长城汽车徐水大王店产业新城的交通设施、通信基础设施情况，开展包括智能驾驶、智慧路网、新能源汽车、共享出行等在内的多个应用示范，构建新的出行方式。2018年3月30日，长城汽车与中国移动、华为联合开发的基于5G的自动远程驾驶技术在长城汽车徐水试验场通过测试，WEY VV7在搭载了基于5G技术的智能控制系统后，在主驾驶位无人操控的情况下，可以完成起步、加速、刹车、转向等动作。

国家智能网联汽车（上海）试点示范区：该示范区于2015年6月获工信部批准建设，2016年6月在上海安亭投入运营，是工信部批准的首个智能网联汽车示范区，该示范区由上海市智能网联汽车创新中心运营管理。2018年3月1日，上海发放首批智能网联汽车开放道路测试牌照。4年来，测试区已累计为国内外近百家企业提供了超过1300天次、1万小时的测试服务。截至2020年6月，上海嘉定可用于智能网联汽车测试的开放道路已达53.6公里，覆盖面积达65平方公里。示范区涵盖了不同类型、不同等级的道路，测试场景达1580个，覆盖工业区、商业区、交通枢纽、住宅区等多个场景。此外，现有的开放测试道路已经实现了5G信号全覆盖、



高精度地图采集，同时建设了车路协同应用系统、全息道路感知系统、安全监管监控平台等一批服务于智能交通的基础设施。目前，上海共有包括上汽、宝马在内的 20 家车企获得了 78 张智能网联汽车测试牌照，先途智能、新石器等一批智能网联专用车，已在特定区域内实现无人清扫、移动无人零售、无人配送等一系列功能。

智能汽车集成系统试验区（Intelligent Vehicle Integrated Systems Test Area, i-VISTA）：该示范区是国家工信部及重庆市政府共筹、共建的具有国际领先水平的智能汽车和智慧交通应用示范工程及产品工程化公共服务平台，该试验区运营主体是中国汽车工程研究院股份有限公司。截至 2019 年 11 月，i-VISTA 已建成 5G 封闭试验区、5G 可控全网联模拟城市乡村高速试验示范区和覆盖全国 85% 以上道路环境的复杂开放道路，能为标准法规研究、前沿技术测试验证、关键技术融合应用、多场景产业化示范探索等提供丰富的测试环境，助力智能网联汽车和智慧交通产业的健康发展。

国家智能网联汽车（长沙）测试区：该示范区从 2016 年 6 月开始规划建设，于 2018 年 6 月 12 日正式对外开放。2018 年 11 月 28 日，工业和信息化部向湖南湘江新区智能系统测试区授牌，测试区运营主体是湖南湘江智能科技创新中心有限公司。该公司作为智能网联汽车产业生态运营商，依托智能系统测试区为平台，以 15 平方公里的人工智能科技园为载体，在基础层、技术层、应用层与产业链企业进行研发测试示范、技术标准共建、场景应用拓展、技术成果转化、产业项目落地等方面合作。

国家智能网联汽车应用（北方）示范区：2018 年 7 月，该示范区由国家工信部、吉林省政府、中国一汽共同启动并投入运营。示范区封闭场地面积达 35 万平方米，封闭道路里程 3 公里，具有 6 大类，共计 99 个测试场景，通过行驶场地和驾驶情景的组合可以扩展到 300 余个场景，智慧交通设施共有 4 大类，共计 100 余个，实现了高精地图和 5G 信号的全覆盖。

国家智能交通综合测试基地（无锡）：2017 年 8 月，工业和信息化部、公安部和江苏省人民政府签订了“共建国家智能交通综合测试基地协议”，同年 9 月举行了揭牌仪式。该测试基地位于无锡市滨湖区，规划总面积达 208 亩，分为公路测试区、多功能测试区、城市街区、环道测试区和高速测试区等，涵盖多种类型道路、隔离设施、减速设施、车道线、临时障碍物、交通信号、交通标志等。2018 年 9 月，国

家智能交通综合测试基地自动驾驶公共道路测试环境正式开放，上汽、奥迪作为首批车企获得测试牌照。

**浙江 5G 车联网应用示范区：**2015 年 9 月，工信部与浙江省人民政府签订了《关于基于宽带移动互联网的智能汽车、智慧交通应用示范合作框架协议》，明确浙江成为中国首个开展部省合作推进 5G 车联网应用示范的省份，以云栖小镇为核心的(杭州)西湖区、以乌镇为核心的(嘉兴)桐乡市作为 5G 车联网的示范试点。2016 年初，两个示范试点的实施方案通过专家评审，并开始开工建设。

**武汉智能网联汽车示范区：**2016 年 11 月，工信部与湖北省政府在武汉签订合作框架协议，批准建设智能网联汽车和智慧交通应用示范城市，示范区落户武汉开发区。该示范区规划总面积达 90 平方公里，包含封闭测试场地及开放测试示范区，示范道路总长 159 公里，其中测试道路总长 68.3 公里，交通路口共计 152 个，涵盖了居民区、商业区、物流区、旅游风景区以及工业区。2019 年 9 月，国家智能网联汽车（武汉）测试示范区正式揭牌，百度、海梁科技、深兰科技拿到全球首张自动驾驶商用牌照。

**广州智能网联汽车与智慧交通应用示范区：**2018 年 3 月 30 日，广州市正式启动基于宽带移动互联网的智能网联汽车与智慧交通应用示范区项目，该项目选址花都区 and 韶关新丰县，占地面积分别为 1900 亩和 8600 亩，两个测试区预计总投资 46 亿元，建成后预计可实现 400 台车/日的测试容量。

**中德合作智能网联汽车车联网四川试验基地：**2017 年 11 月 27 日，成都经开区正式获得工信部批准承建四川试验基地，这是全国唯一的国家级中德智能网联汽车试验基地。该试验基地涵盖智能网联汽车、车联网标准及测试验证等内容，预计整体投资 300 亿元，主要包括四个部分，即 1.2 平方公里的封闭测试区，5 平方公里的半开放体验区，50 平方公里的综合示范区，200 平方公里的智慧交通生态圈。

### 7.2.3 公开道路测试准入条件现状

本小结针对现有的公开道路测试准入条件与道路测试细则进行调研，包括该细则的总则及测试准备条件及要求。其中测试准入条件及要求又包括测试前车辆管理、测试过程安全管理等。

### 7.2.3.1 总则

(一) 为推动预期功能安全在公共道路的测试的发展和应用，规范自动驾驶车辆的公共道路测试车辆状态的准入测试条件，依据《智能网联汽车道路测试管理规范（试行）》、《XXX 自动驾驶道路测试管理实施细则（试行）》，特制定本实施细则。

(二) 自动驾驶技术车辆开展道路实车测试，应遵守本实施办法。

(三) XXX 负责本实施细则的统一监督和管理。

(四) 自动驾驶：指车辆通过人工智能、视觉计算、雷达、监控装置和全球定位系统协同合作，可以在无人主动的操作下，自动安全进行操作。

(五) 自动驾驶道路测试：指在所有在测试场/公共道路等实施的自动驾驶开发测试，包括功能测试、性能测试、可靠性测试、适应性测试等各类测试。

(六) 自动驾驶车辆：指在符合《机动车运行安全技术条件》(GB7258)的机动车上装配自动驾驶功能的车辆。

(七) 自动驾驶数据记录装置：指安装在自动驾驶测试车上，能全过程实时持续记录测试时的传感相关数据（周边环境、车辆运行、车辆操作）的记录装置。

(八) 预期功能安全：是为了规避那些因系统设计不足、功能限制及人员的误用导致潜在危险行为发生的不合理风险。

### 7.2.3.2 测试准入条件及要求

#### 一、测试前车辆管理

##### 1、测试车辆状态要求

(1) 应符合国家上路行驶相关法律法规。

(2) 应满足各公司测试车外出测试手续的管理规定。

(3) 测试车辆应具备常规机动车辆行驶的基本技术要求。

(4) 应满足紧急情况一键关闭自动驾驶功能的要求，测试驾驶人能够在自动驾驶系统出现故障或发出警告提醒时，要有立刻按下应急开关，切断控制器电源。

(5) 在开展测试前，由测试安全员对测试车辆的技术状态进行检查确认并签字确认。

(6) 测试车辆应稳定识别绝大部分车道线（虚线、实线、双黄线、鱼骨线、黄白线）及运动、静止车辆（大车、小车、非机动车）。

(7) 测试车辆自动驾驶激活后，横向和纵向控制性能需达到要求，横向控制在



稳定跟车时，车辆能够对中行驶，纵向控制能随前车加速及减速及稳定跟车。

## 2、测试团队要求

(1) 测试团队由测试负责人、测试安全员、测试驾驶人、测试工程师等组成。

(2) 所有测试人员在试验前应充分学习了解试验规程，熟知试验内容及操作方法。

(3) 所有测试人员在试验前应进行培训，充分理解本次测试项目，充分理解故障注入测试的故障注入方法和故障恢复手段及故障注入后的预期表现，对于部分不易操作的测试场景，做好数据采集，后期分析得出结论。

(4) 测试负责人，负责对整个测试方案、测试计划、测试过程进行总体管理，是测试安全的直接管理人。

(5) 测试安全员，负责梳理测试风险及措施，应急预案，测试过程中的安全保障，是测试的安全检查和监督责任人。

(6) 测试驾驶人，必须满足以下方面要求：

1) 必须拥有各测试试验单位规定的驾驶资质，并在测试实施时确保有效；并符合各单位驾驶资质管理办法；测试驾驶人如为外租驾驶人，需符合各公司外租驾驶人相关规定。测试驾驶人必须熟练掌握道路交通安全法规、驾驶理论、交通安全心理学等安全驾驶知识；并充分了解自动驾驶系统技术体系、自动驾驶测试车辆结构及自动驾驶测试系统等相关知识。

2) 测试驾驶人需经过自动驾驶实车训练和考核，训练证明材料应包括测试驾驶人对系统异常的判断能力和在危险场景条件下接管测试车辆的测试实例。充分理解测试后的整车预期表现，并能做出正确判断，能准确判断系统异常条件下接管测试车辆的能力。

## 3、测试场地要求

(1) 公共道路/区域（如 APA 适应性）测试前，需要提前评估该道路/区域的车流量、人流量，采取流量从低到高层层递进的原则安排测试。

(2) 进行低照度、大雾天、中到大雨天气等特殊场景试验，应制订专项试验规范和安全防范措施。

## 4、测试安全审批

(1) 测试负责人需要制定自动驾驶道路测试安全审批表，审批表内容包括：测

试基本信息、测试车辆信息、测试人员信息、安全风险评估及应对举措、以及审批意见。

(2) 测试车辆基本信息参考该测试车辆准入检查结果，填写控制器版本、车辆常规状态检查结果、自动驾驶系统功能检查结果（功能激活关闭、故障报警、应急按钮、数据记录）、自动驾驶样件/设备检查结果等。

## 二、测试过程安全管理

### 1、基本要求

(1) 测试负责人、测试驾驶人及随行测试人员必须遵守国家 and 地方交通法律法规。

(2) 需严格按照试验规范及操作规定进行操作，严禁违章操作，违章指挥，违反劳动纪律。

(3) 测试工作必须严格按照测试审批表定义的时段、区域开展测试；不得超区域超时段进行测试。

(4) 测试过程中，严禁擅自变更测试审批表相关信息，如需变更，由测试安全员提出并重新进行测试审批，审批通过后方可实施。

### 2、车辆状态检查

(1) 每日行车前，测试安全员需对临时牌照、消防器材、基本车况、安全设施等进行检查，确保车况良好及相关设施齐备。

(2) 每次测试前，测试安全员需要检查自动驾驶功能是否正常、零部件状态是否正常、数据记录设备是否可以正常采集。

(3) 禁止在测试过程中对车辆自动驾驶系统的硬件、软件状态进行变更。

### 3、测试应急防护

(1) 测试过程中，原则上主驾必须全程配备测试驾驶人；若测试场景需要安全员离开主驾，车辆必须具备遥控制动功能，由其他测试人员负责应急处理。

(2) 指定区域重复多次测试时，必须有测试人员在车下进行安全警戒，避免社会人员或车辆侵入试验区域带来安全风险，如有非试验人员或移动物体进入试验区域时，警戒人员立即通知驾驶人接管车辆并暂停试验。

(3) 泊车测试时，必须有试验人员协助驾驶人观察车辆与障碍物之间的安全距离，并及时提醒驾驶人，确保安全试验。

(4) 如与其它测试共用试验场时,应在直线加速道与定圆广场交点路旁设置观察哨并配备对讲机。

#### 4、事故处理

(1) 测试中如有异常安全风险事件出现(未发生事故),需要立即暂停测试,并重新进行测试安全风险及应对措施分析。经测试安全员申请、测试负责人确认,报测试对应安全审批人员确认后方可继续开展测试。

(2) 测试车辆在进行道路测试过程中发生交通事故,测试驾驶人应立即停止测试,并立即报公安交通管理部门,按照国家道路交通安全法律法规的要求进行处理。

(3) 交通事故发生后,由测试负责人将记录数据在4小时内进行上报公司安全部门。

(4) 自动驾驶测试车辆在发生事故后,待测试车辆及人员提供交通事故处理完结的相关证明,并重新进行安全审批,经处所领导审批通过后方可恢复测试。

(5) 测试人员存在违反事故处理相关规定的,将取消其测试资格,并按公司相关规定进行考核。

### 7.2.4 评价体系与可接受风险的测试指标

#### 7.2.4.1 评价体系

由于国内自动驾驶汽车相关技术发展起步较晚,因此目前尚未形成一套成熟的体系来对自动驾驶汽车进行测试评价。评价体系需要能充分有效地验证车辆在复杂驾驶场景下能否满足预期用途的要求。充分性是指测试和评价体系能够充分体现用户的使用要求,能够充分反应实际驾驶环境的各种场景、工况。有效性是指所使用的测试评价方法确实有效,一是能够满足智能网联汽车开发周期的需求,二是所使用的方法能够有效地验证智能驾驶性能的优劣,能够有效评价车辆的系统的一致性和可靠性。

为了满足智能网联汽车测试和评价的充分性和有效性要求,必须要有合适的验证方法。验证智能网联汽车性能最有效的方法就是道路测试,即让汽车在实际复杂场景工况下进行实车测试,但是考虑到成本代价,也有很多企业机构进行虚拟平台仿真测试或者在数字孪生环境下进行集成测试。例如,上汽通用汽车有限公司广德分公司为了在规定的时间内完成智能网联汽车的测试和评价,对驾驶场景组成的三大要素“人、车、环境”进行研究,考虑将其中的部分或全部要素进行模拟或虚拟,

以便进行模拟测试和仿真测试，从而大大缩短测试和评价的周期。

2019 年，网上车市联合上海交通大学在上海正式发布了智能网联汽车用户评价体系（Intelligent Connected Vehicle Test, ICVT），从更专业、更客观的角度对车辆做出的评价，让消费者可以更为直观地了解车辆在智能网联方面的性能表现。ICVT 这一评价体系的特点如下：（1）基于功能及消费者的使用需求；（2）将主观评价进行细分量化，形成科学的计算公式，变为客观的、可量化的评价标准；（3）标准具有实时性，根据技术发展、市场需求等情况动态调整，使消费者需求和体验的主观需求转变为客观标准；（4）是消费者和厂家的高效沟通互动工具。

智车科技从智能网联汽车网络安全角度入手，基于对相关网络安全技术指标的梳理分析，并结合科学的赋权方法，构建起各测评对象与测试用例的权重体系，以直观的评分方式对汽车网络安全评测结果加以表述，使用户能够迅速获得对车辆网络安全水平的准确认知。如图 7-4 所示，该公司设计了一套从测试用例到关键零部件、云管端系统，直至整车系统的评价方法。

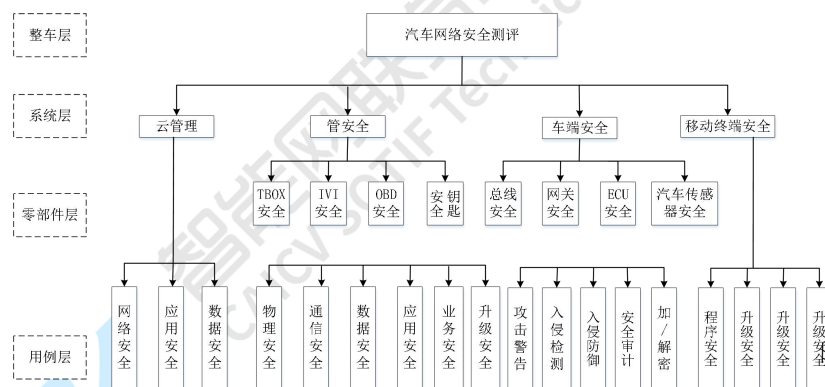


图 7-4 智能网联汽车网络安全（分层）评价体系

上海机动车检测认证技术研究中心有限公司从安全性、高效性和舒适性三个方面出发，对智能网联汽车的自动驾驶功能测试评价面临的挑战进行了分析，提出了一个持续、灵活的自动驾驶功能测试评价系统框架。该框架以数据库为基础，通过筛选逻辑确定虚拟测试、场地测试和公共道路测试之间的场景比例关系，三种测试方法之间相互补充，能够对自动驾驶功能进行更全面的评价，并且数据基础、筛选逻辑以及测试方法都是持续灵活、不断迭代的。测试评价指标涵盖多空间、多时间维度，不仅可以评价自动驾驶功能单场景单次的测试性能表现，也可以评价多车、长周期内的性能表现，具体测试评价体系如图 7-5 所示。



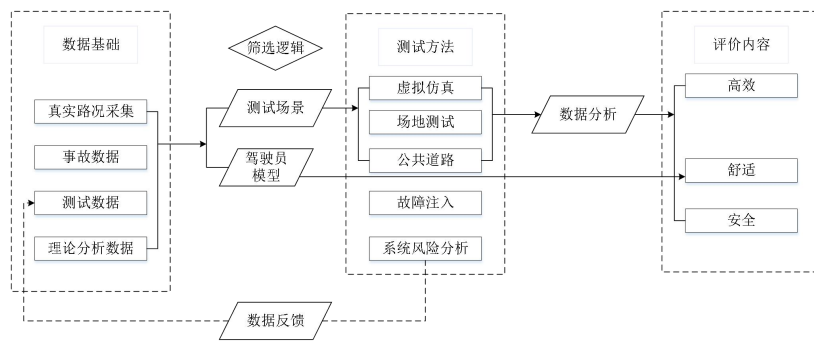


图 7-5 自动驾驶汽车评价体系

中国汽车工程研究院智能汽车测试评价中心的甘海云认为智能网联汽车的 ADAS 系统在国内处于导入期，大部分自主品牌 ADAS 产品处于研发阶段。智能网联汽车需建立 DSRC 通信环境、智能路侧设施、后台交通协调管理中心，可开展 DSRC 通信符合性测试，支持 ADAS、车车/车路/车人协同功能验证和性能试验，能够对 ADAS 车辆在环 VeHIL、ADAS 场地、ADAS 开发、ADAS 法规等进行测试评价试验，能对车联网通信容量、车联网信号可靠性和通信延迟、车联网信息安全保护机制等进行测试评价。此外，该公司提出的对汽车操控安全性指数、舒适性指数和驾驶性指数的测试评价规程中有完整的评分体系，可作为智能网联汽车评价体系研究的基础。

目前，我国共计 7 个省市发布了智能网联汽车自动驾驶功能道路测试的指导文件，主要针对需要申请道路测试的主体进行有针对性的封闭测试，以通过相应实车试验的测试评价。此外，高校、科研院所等也从不同角度、不同维度对智能网联汽车的相关性能展开测试评价体系研究，有效地推动了智能网联汽车相关技术的快速、有效发展。

#### 7.2.4.2 可接受风险的测试指标

2019 年 6 月 28 日，北京市交通委发布了自动驾驶测试道路管理办法，办法明确自动驾驶路测道路须先进行风险评估后才能够按程序许可允许自动驾驶车辆上路。同时，应在地图上对自动驾驶路测区域进行标注，方便市民识别，在遇到交通管制等特殊情况，应采取相应措施保障自动驾驶车辆安全。此外，办法还明确需对拟开放的测试道路的规划背景、交通现状、存在问题、防控措施、社会影响和群众满意度等方面须进行风险评估，该管理办法在一定程度上降低了自动驾驶汽车路测过程中的测试风险。

自北京出台《智能网联汽车自动驾驶功能测试规程》后，上海、重庆等地先后规划智能网联汽车道路测试路段并颁发道路测试号牌，实现了智能网联汽车上路测试，但各地的具体测试要求有所不同，测试指标的评价标准也有所差异。当道路交通事故发生时，主要通过对测试主体、测试驾驶人、测试车辆进行严格规范以对道路测试的风险进行控制评估，从而保证在路测过程中需完成的测试指标风险是可接受的。

### 7.3 智能网联汽车测试评价发展趋势分析

#### 7.3.1 虚拟仿真测试发展趋势

计算机仿真与虚拟测试技术在智能网联汽车研发过程中将扮演愈发重要的角色。具备信息高度共享化的智能网联汽车与车联网技术从根本上组成了一个信息物理系统，仿真技术也需在信息模型与物理模型两个维度进行综合仿真。因此，从模型到软件，软件到硬件，部件到系统，需要不断深入地从各层级构建智能网联汽车的知识模型，构建完整的知识技术体系。交通系统是人-车-路相互作用的系统，自动驾驶系统仿真技术的重点发展方向是提供接近真实的复杂动态环境，尤其对机动车，非机动车，行人等交通参与者的高度动态交互行为，对天气与天光变化的仿真，并把上述动态交通要素按照不同的复杂程度进行重新组合。

由于智能网联汽车将在一个漫长的周期内逐步替代传统汽车，这必然形成传统汽车与智能网联汽车混行的局面，因此，人机交互研究将成为仿真技术研究的一个重要方向。智慧交通与车联网技术能够实现自动驾驶汽车与数字智能化道路的有机融合，交通系统下的车辆行为研究也是仿真技术的另一发展方向。此外，需要对智能网联汽车进行更多维度的测试与评价，首先可以对车辆驾驶的自治性进行评价，对车辆本身在一定外界条件下的行驶能力进行测试评价。其次，可以对车辆参与交通的协调性做出测试与评定，根据其他的交通参与者的行为方式选择自身用何种行为进行交互性回应。这些测试与评价都需要仿真技术提供更高维度的虚拟场景与评价体系。

未来，智能网联仿真技术会始终服务于法律法规。通过仿真评估交通事故的法律责任，帮助监管和管理交通行为，对交通规则进行技术评估。智能网联仿真技术将服务于产品认证，通过仿真方法提供一个科学而全面的产品测试和审查方法。智

能网联仿真技术还将协助建立一个全国范围的通用型数据库，其包含智能网联汽车工作的典型工况和边缘案例，数据信息可与其他国家和地区共享，帮助行业进行跨地区的交叉认证，最终提升自动驾驶系统的技术普适性。

### 7.3.2 智能网联汽车试验场建设建议

鉴于目前我国智能网联汽车研发多集中在 SAE L3 级的自动驾驶层面，因此，从时效性和实用性的角度考虑，专用试验场的建设应遵循“两步走”原则。从短期来看，智能网联汽车的测试和评估还将集中在 SAE L3 级，尤其是对 ADAS 等自动驾驶系统子功能、子模块的验证，试验场在这一阶段承担的角色是提供一个封闭受控、满足标准化和部分非标准化驾驶辅助系统测试场景的环境。从长远来看，我国在智能网联汽车领域的研发将趋向于更高级别的自动驾驶，预计在十年内部分机构有能力开发出完全智能网联汽车。因此，为满足最新科研成果的测试需求，专用试验场在后续建设过程中应逐步丰富场景，提升环境复杂度，以满足 SAE L3 级及以上自动驾驶系统的测试需求。借鉴国外已有成熟的智能网联汽车试验场建设经验，从测试环境和测试设施的角度，对国内智能网联汽车试验场建设提出以下建议：

(1) 道路环境方面。国外现有的试车场路面一般由铺装路面与非铺装路面组成，少数场地由于面积限制只提供铺装路面。基于 SAE L3 级及以下的自动驾驶和 ADAS 系统测试需求，我国试验场建设在第一阶段可以暂时只规划建设有铺装路面的高速道路和城市道路，以满足驾驶辅助系统测试需求。后续在场地面积等条件允许的情况下，应采取铺装路面与非铺装路面相结合的方式建设，通过道路形态的多样性来测试复杂多变的道路特征对高度智能化车辆行驶过程的影响。

(2) 配套基础设施。为降低改造成本，提升设施利用率和使用周期，我国的试验场建设应遵循柔性化理念，早期提供一定的基础设施支持，并为未来丰富场景预留空间。

(3) 辅助测试设备。我国试验场除引入假人、自行车、气球车等其它道路参与者，还应针对中国特有的道路情况，如电动自行车这一交通参与者，自行研发相应的模拟测试设备，评价智能网联汽车对中国路况的适应程度。此外，天气也是影响智能网联汽车表现的一个重要因素，考虑到天气模拟器的建设运营维护成本较大，该类设施可以在第二阶段加入试验场，但应在前期预留相应接口和空间，不作为主要功能建设，待场地运行平稳、资金充裕后，可以在改扩建过程中逐渐加入相关设

施。

(4) 网联功能测试。我国试验场应支持欧美目前主流的 V2X 通讯设备, 如 DSRC 等。从数据传输与储存的角度考虑, 应在整个试车场区域实现无线网络和 5G 网络全覆盖, 并对专有网络进行加密, 保证测试信息安全。为了保证精确定位, 测试场地应布置差分 GPS 基站, 同时也应能支持应用北斗导航系统。

### 7.3.3 智能网联汽车测试评价的挑战和目标

智能网联汽车是一种极其复杂的系统, 所处的实际驾驶环境要素繁多、复杂多变, 其测试和评价体系研发还面临着许多不确定性与困难:

(1) 多种新型传感器的组成, 包括视频传感器、雷达传感器、激光雷达传感器、超声波传感器、车对车 V2V 通讯、车对道路设施 V2I 通讯、GPS 传感器、高精地图等, 不少传感器还带有数据分析处理智能子系统, 测试和评价必须充分考虑到这些特点, 并有效开展针对性的测试和评价。

(2) 考虑到这些新型传感器本身还存在一些弱点, 传感器数据融合对于构建车辆外部的整体环境非常必要, 对于测试来说, 需要考虑所有传感器的数据同步性, 数据的不同步会造成数据融合算法的错误。

(3) 智能网联汽车所处的驾驶环境复杂, 除了道路设施外, 交通参与要素如车辆、行人也是需要重点考虑的内容, 此外, 有人驾驶的车辆还面临更多的不确定性, 他们会根据智能驾驶车辆做出自己的判断, 从而改变行车的控制方式, 如经过十字路口有的驾驶人可能会快速地制动而有的可能会缓慢制动, 因此, 对于驾驶人不同的驾驶行为也需要在测试和评价时进行充分考虑。

(4) 天气等因素会严重影响智能网联车辆的传感器性能, 如雨、雪、雾、光照、温度等, 因此, 车辆的测试需要在不同的天气环境下进行。

综上所述, 上述挑战是在进行测试评价体系建设时必须完成的, 最终目标是能够充分有效地验证车辆在复杂的驾驶场景下具备的功能是否满足预期用途要求。在推进智能网联汽车发展的过程中, 必须始终将用户和公共社会的安全性放在首位, 为了做到这点必须深入研究智能网联汽车的测试和评价技术, 确保测试评价的充分性和有效性。具体讲, 可以从智能网联汽车的技术特点入手, 从场景数据、测试方法、评价准则等方面进行研究, 从而建立起一套完整的测试评价体系, 指导测试和评价工作的积极有效开展。在这一体系建设过程中, 将面临很多其他挑战, 例如,





场景库的建设尚处于起步阶段，相关数据还很不完善，需要国内整个汽车行业的通力合作。近年来，我国各地相继推出了测试示范区，国家也正式发布了智能网联汽车测试管理办法，部分车企已经获得测试牌照并开展了相关测试，这些积极的变化是将智能网联汽车推向市场的有益尝试，相信在整个汽车行业的共同努力下，智能网联汽车的测试和评价也将逐步完善。

智能网联汽车预期功能安全工作组  
CAICV SOTIF Technical Alliance



## 第 8 章 典型 ADAS 系统的 SOTIF 研究现状

本章节将针对当前一些典型的先进驾驶辅助系统（Advanced Driver Assistance System, ADAS）的预期功能安全研究现状展开介绍，主要包括车道保持系统的预期功能安全研究、自动刹车辅助系统的预期功能安全研究、自适应巡航系统的预期功能安全研究、交通拥堵辅助系统的预期功能安全研究与自主泊车系统的预期功能安全研究等五部分内容。

### 8.1 车道保持系统的预期功能安全研究

车道保持系统（Lane Keeping Assist System, LKA）一般通过环境传感器识别本车相对于车道中央的位置，辅助驾驶人保持在车道内行驶。最常使用的环境传感器通常是相机，但是相机比较容易受到周围环境的影响，尽管相机本身并没有出现故障，但由于外界环境影响的因素也难以对车道线进行识别，从而引发事故。为解决这些由于功能限制或误用而导致的事故，对 LKA 系统进行预期功能安全研究十分必要。

2017 年，H. Mahajan 等[1]应用系统理论过程分析方法（Systems Theoretic Process Analysis, STPA）对 LKA 系统进行了安全分析，归纳可能导致的事故、危险，建立了分层控制结构图，基于结构图分析不安全控制行为，并根据不安全控制行为分析影响因素，并制定了相应的安全要求与安全约束。在分析过程中，研究人员将驾驶人与 LKA 控制器均作为系统的控制器，同时考虑了驾驶人与控制器的交互问题。STPA 方法是在 LKA 系统概念开发阶段执行的，它基于系统交互作用而不仅仅是故障事件来考虑危险、因果因素。

2018 年，上海泛亚汽车技术中心有限公司的尚世亮[2]等人在满足 SOTIF 开发需求的前提下，开发了一种自动化测试系统，并进行了硬件在环以及实车的自动化测试，最终以 LKA 系统作为示例进行了 SOTIF 测试。在此研究中，设定的环境为：当在驾驶人正常状况下进行转弯行为时，通过 CAN 总线将  $1\text{N}\cdot\text{m}$  的 LKA 转向命令反向注入到 EPS 系统中，用以模拟非预期的 LKA 功能，通过车辆转向盘扭矩的表现得出，LKA 功能的扭矩上限为  $4\text{N}\cdot\text{m}$ ，并且该实验验证了该上限的安全性。

### 8.2 自动刹车辅助系统的预期功能安全研究

自动刹车辅助系统（Automatic Emergency Brake, AEB）能够及时发现前方的潜

在碰撞，从而避免事故发生或减轻事故伤害。2020年3月19日，由于自动紧急制动系统存在故障，沃尔沃汽车宣布召回了全球范围内的74万辆汽车，共涉及9款在售车型。尽管这些车型出自于CMA平台，并且完全满足功能安全要求的开发，但依旧出现了大规模的由于电子电器系统问题而导致的召回事件。这次召回的原因是AEB系统在一些场景下无法有效的识别物体，如将汽车排气管附近的红色飘带识别为路障等，从而导致AEB系统无法正常工作。通常AEB系统探测物体会根据毫米波雷达与摄像头的信息融合，但是由于多普勒效应，毫米波雷达对于静态物体的识别并不准确，摄像头在外界环境恶劣的情况下，例如雨、雪、雾天等，探测度也会降低，因此对AEB系统进行预期功能安全研究十分有必要。

在安全分析中，可以使用STPA方法自上而下地分析，明确AEB系统的设计要求[3]。S. Sharma等[4]应用STPA方法针对SAE L4级别自动驾驶汽车的AEB系统进行了安全分析。STPA方法通过使用自上而下的系统安全性分析方法得到了可能发生的危险与不安全控制行为，定义了高级安全约束，并通过不安全控制行为分析可能因素和情景，明确安全约束，并最终明确技术安全要求。STPA方法为情景分析提供了一种结构化方法，但这种方法与ISO标准集成的效果会更佳，在执行预期功能安全与功能安全分析时十分有效。ISO/PAS 21448附录[5]针对AEB系统可接受的误报率进行了定义与验证，对AEB的预期功能安全分析方法进行了阐述，主要流程包括：系统失效划分、实施SOTIF HARA、交通统计学分析、定义测试场景。随着自动驾驶系统的自动化程度与整合度不断提高，ODD具有复杂化、动态化、多而广的变化趋势，对自动驾驶功能进行单独测试（如在车-车临界碰撞场景中测试AEB）难以保证上路后的操作安全性[6]。

一种客观的规则集的引入有利于提高HARA的可靠性，S. Khastgir [7]通过参数化HARA，使评价过程更加客观，提出的方法被认为可用于AEB的危害评估。J. Sini等[8]人以TTC为指标，制定了因误用AEB造成的对可控性的影响的分类规则。S. M. Kim等[9]通过实际驾驶测试计算行人和车辆出现在主车前的频率，建立模糊模型量化ASIL评级指标。H. Martin等[10]介绍了工作流的过渡结果，以识别不同传感器的性能局限性，并通过考虑一些传感器技术得出扩展自动紧急制动（Extended-Autonomous Emergency Braking, E-AEB）用例的触发事件。该研究重点关注E-AEB的环境感知，即雷达和相机的传感技术。研究人员认为对于每个传感器

都需要在适用 SOTIF 之前验证功能的局限性，并分析研究触发事件，为了克服这些局限性要定义功能以改进系统，提出了一种基于系统的 HAZOP 方法，以识别触发可能的事件的工作流程。在更高的自动化级别上，不需要监视驱动程序，为了实现这种对安全至关重要的功能，必须采用新颖的传感器技术来感知环境。尽管这些传感器技术仍然有一些局限性，但是为进行功能集成，必须在开发周期中确定并改善这些传感器的局限性。当前 AEB 系统的 SOTIF 评价正在由定性分析向客观、量化的评价方式转化，以提高评价方式的实用性。

### 8.3 自适应巡航系统的预期功能安全研究

自适应巡航控制系统（Adaptive Cruise Control, ACC）是一种 SAE L2 级别的辅助驾驶系统，通过雷达传感器监测与前方汽车车距，通过轮速传感器采集车速信号，基于前方车距信息调节自身车速以实现跟车行驶。类似地，ACC 系统在运行的过程中会存在外界环境干扰导致功能受限、人为误用或组件交互行为引起的故障等情况，因此对 ACC 系统的预期功能安全研究尤为重要。

德国斯图加特大学的 Abdulkhaleq 等应用 STPA 方法对 ACC 系统进行了详尽的安全分析，提出了软件安全校验方法和模型检测方法，并最终将其融合成一种基于 STPA 方法的软件集成系统的综合安全工程方法[11][12]。首先，研究人员假定了在几种事件发生时，应保持车辆速度，确定了软件级别的目标，并确定可能导致事故和相应的软件级危险，然后明确了设计要求与安全约束，并建立了安全控制结构图。在此控制结构中，研究人员考虑了驾驶人与速度控制软件控制器的交互行为，建立了过程模型，并基于安全控制结构图分析了不安全控制行为以及可能导致的危险，分析了可能导致不安全控制行为的原因。此外，研究人员根据安全需求建立了形式化描述，利用符号模型验证器进行了验证，验证结果显示根据安全分析提出的安全需求可以满足 ACC 系统的安全要求。Abdulkhaleq 等在另一项研究中[13]对 ACC 系统的过程模型进行了补充，通过对 ACC 系统进行详尽的安全分析，并对提出的安全需求进行软件级的验证，为 ACC 系统的预期功能安全研究提供了参考。

### 8.4 交通拥堵辅助系统的预期功能安全研究

交通拥堵辅助（Traffic Jam Assist, TJA）系统是在车道居中控制和自适应巡航控制（ACC）系统基础上进一步发展而来的智能驾驶辅助系统，与 ACC 系统不同，



TJA 系统不仅进行纵向控制，在某些情景下可进行横纵双向控制，即增加了转向控制功能。TJA 系统不仅可根据检测到的车道线完成对中行驶，在摄像头等传感器被遮挡时依然能根据探测到的前车行驶轨迹做跟随行驶，可在交通拥堵时提供驾驶辅助，减轻驾驶人疲劳程度。TJA 系统的计算输入为车道线标志位置和前方车辆的位置以及其运动情况。

运行设计域（Operational Design Domain, ODD）规定车辆在拥堵的交通流中需要以较低的速度（低于 65 公里/小时）行驶，TJA 系统启动后将控制车辆的转向、加速和刹车，以保持车辆在交通流中的位置，此时，驾驶员可以短暂的脱离对车辆的操控控制，但仍需要保持警惕适时干预以维持行驶安全，即为有条件的自动驾驶。H.E. Monkhouse [14]等对 TJA 系统评估表明，TJA 系统在前车跟随、道路危险处理等任务中的操纵水平有限，如何保证驾驶人拥有足够的情景意识（Situational Awareness, SA）以及如何度量驾驶人的响应是保证 TJA 系统安全性的关键所在。

## 8.5 自主泊车系统的预期功能安全研究

自主代客泊车系统(Automated Valet Parking, AVP)可实现封闭区域内指定地点到停车位之间这一特定区域内完全自主的车辆自动驾驶，是 SAE L4 级自动驾驶系统中最可能率先取得商业化的系统。AVP 系统的安全性测试及验证受到了广泛关注，测试的关键之处在于如何通过安全分析方法明确安全需求，并根据安全需求生成相应的测试场景。A. Reschka 等[15]提出了无驾驶人监督的自动驾驶车辆安全概念，H. Esen 等[16]提出了基于 AVP 安全需求的自动测试系统，V. Schönmann 等[17]将车系统分解为若干可控的功能场景，并依据 ISO2626 的 ASIL 评价体系给出了代客泊车系统的分级安全需求。系统、有效的安全分析方法及高效、全面的测试场景生成手段是 AVP 系统 SOTIF 测试亟待解决的问题。

本节将以 SAE L4 级别的全自主泊车 AVP 系统为例说明泊车系统的预期功能安全研究。

### 8.5.1 AVP 系统的设计运行域

AVPS 是 SAE L4 级别的自主泊车系统，可实现一定范围区间内的代客泊车与代客取车，包含低速自动驾驶行车、自主寻找车位、自动泊车入库及自动泊车出库等，在特定区域的自动驾驶可以处理的场景包括：巡线行驶、跟人行驶、跟车行驶、路

口通行、上下坡、避让障碍物、等待让行、寻找车库、Park in、Park out 等。

### 8.5.2 AVP 的 SOTIF 相关危害

在低速（小于 15KM/H）的车速下，基于 SAE J2980 标准，车辆之间低速碰撞的严重度 S 可取 S0，此处不再考虑车辆之间碰撞的场景，定义 SOTIF 相关的危害为车辆对人员造成的伤害，即车辆对行人的碰撞或碾压。考虑可控性 C 时，需要综合考虑车辆本车的控制能力和人员可躲避车辆碰撞的能力。

### 8.5.3 识别和评估 AVP 潜在的功能不足和触发条件

由于是无人驾驶与监控，此处不再考虑人员对车辆的误用，此处主要考虑系统设计的不足及性能限制。针对系统的设计不足，主要考虑系统对 ODD 内的场景覆盖程度，即系统对 ODD 内的所有场景是否都有正确的逻辑响应，对 ODD 边缘的场景系统是否有提前的响应处理的机制，对 ODD 范围外的场景系统是否有相应安全应对策略。因此，系统需要对使用场景进行合理详细的划分，确保系统对场景的覆盖度到达一个合理的范围。

针对性能限制，此处主要考虑感知模块性能、执行模块是否满足设计需求及 AI 算法的逻辑是否合理正确性。以感知模块为例，需要从感知传感器类型及其性能指标、传感器固有的缺陷，结合场景的 ODD 指标来挖掘系统可能无法应对的危害场景。例如，从摄像头与雷达数据融合判别行人并将数据发送给 AVPS 控制器，到 AVPS 控制器请求制动系统制动和制动系统液压结构实际执行制动，这一过程所需的时间为 1.5s。假如奔跑的儿童从车辆感知视野盲区横向切入到车辆前方只有 0.5s，显然现有系统的性能无法满足实际需求。评估系统对危害事件的可接受性时，可以参考参数严重度 S 和可控性 C。对于上述危害事件，在低速（小于 15KM/H）时，对儿童造成碰撞或者碾压后可能造成致命伤害，这对于 SOTIF 而言，是不可接受的。

### 8.5.4 AVP 功能修改以减少 SOTIF 相关风险

针对已知的危害，可通过对功能进行改进、限制或者降级来减少与 SOTIF 相关的风险。就上述例子而言，考虑对功能进行改进，可通过仿真或模拟，测算当横向目标以一定速度切入时所能接受的反应时间，然后合理分配给感知-决策-执行系统。此外，还可以从提高传感器识别行人效率、算法决策效率、以及减少制动系统进行制动时的机械动作时间，来设计合理的时间分配。针对改进措施，就执行器来说，

可以在 AVPS 系统开启前, 使控制制动系统进入到预夹紧状态, 以确保制动系统在接收到制动命令时可以在第一时间生效, 以缩减机械结构执行的时间。

#### 参考文献

- [1] Haneet, Singh, Mahajan, et al. Application of systems theoretic process analysis to a lane keeping assist system[J]. Reliability Engineering & System Safety, 2017.
- [2] 尚世亮, 崔海峰, 郭梦鸽, 等. 自动化测试在 SOTIF 开发中的应用[J]. 汽车技术, 2018, 000(011):23-26.
- [3] Sharma S. CONSIDERING SAFETY AND SECURITY IN AV FUNCTIONS[D]. University of Waterloo, 2019.
- [4] Sharma S, Flores A, Hobbs C, et al. Safety and Security Analysis of AEB for L4 Autonomous Vehicle Using STPA[C]//Workshop on Autonomous Systems Design (ASD 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.
- [5] ISO/PAS 21448, Road Vehicles - Safety of The Intended Functionality[S]. 2019.01.
- [6] Elrofai H, Paardekooper J P, de Gelder E, et al. Scenario-based safety validation of connected and automated driving[J]. Netherlands Organization for Applied Scientific Research, TNO, Tech. Rep, 2018.
- [7] Khastgir S, Birrell S, Dhadyalla G, et al. Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems[J]. Safety Science, 2017, 99: 166-177.
- [8] Sini J, Violante M. A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment[J]. Microelectronics Reliability, 2020, 109: 113661.
- [9] min Kim S, Do G, Ahn J, et al. Quantitative ASIL Estimation Using Fuzzy Set Theory[J]. International Journal of Automotive Technology, 2020, 21(5): 1177-1184.
- [10] Martin H, Winkler B, Grubmüller S, et al. Identification of performance limitations of sensing technologies for automated driving[C]//2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2019: 1-6.
- [11] A. Abdulkhaleq, S. Wagner, Integrated safety analysis using systems-theoretic process analysis and software model checking, Computer Safety, Reliability, and Security Volume 9337 of the series Lecture Notes in Computer Science, 2015, pp. 121-134.
- [12] Abdulkhaleq A, Wagner S, Leveson N. A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA[J]. Procedia Engineering, 2015, 128(2015):2-11.
- [13] A. Abdulkhaleq, S. Wagner, A software safety verification method based on system-theoretic process analysis, Computer Safety, Reliability, and Security Volume 8696 of the series Lecture Notes in Computer Science, 2014, pp. 401-412.
- [14] Monkhouse H E, Habli I, McDermid J. An Enhanced Vehicle Control Model for Assessing Highly Automated Driving Safety[J]. Reliability Engineering & System Safety, 2020: 107061.
- [15] Reschka A. Safety concept for autonomous vehicles[M]//Autonomous Driving. Springer, Berlin, Heidelberg, 2016: 473-496.
- [16] Esen H, Kneissl M, Molin A, et al. Validation of Automated Valet Parking[M]//Validation and Verification of Automated Systems. Springer, Cham, 2020: 207-220.
- [17] Schönemann V, Winner H, Glock T, et al. Fault Tree-based Derivation of Safety Requirements for Automated Driving on the Example of cooperative Valet Parking[C]//26th International Technical Conference on The Enhanced Safety of Vehicles (ESV). 2019, 9: 2019.

附表 A 预期功能安全相关专利汇总

序号	国家	专利名称	申请日	申请人	申请号
1	US	Method and system for multiple sensor correlation diagnostic and sensor fusion/DNN monitor for autonomous driving application	2017.08.08	NIO USA INC	US2019049958A1
2	US	Fail-operational architecture with functional safety monitors for automated driving system	2019.01.18	Baidu USA LLC	US20200231142A1
3	US	Method to dynamically determine vehicle effective sensor coverage for autonomous driving application	2019.01.18	Baidu USA LLC	US20200233418A1
4	US	Method to define safe drivable area for automated driving system	2019.01.19	Baidu USA LLC	US20200233420A1
5	US	Seat system for autonomous vehicles	2016.10.04	Volvo Car Corp	US20170101032A1
6	US	Evaluating risk factors of proposed vehicle maneuvers using external and internal data	2018.09.24	Intel Corp	US20190047559A1
7	US	Feedback-based control model generation for an autonomous vehicle	2017.02.15	Ford Global Technologies LLC	US20180229723A1
8	US	Probabilistic inference using weighted-integrals-and-sums-by-hashing for object tracking	2015.10.19	Ford Global Technologies LLC	US20170109644A1
9	US	Deeply integrated fusion architecture for automated driving systems	2017-07-24	GM Global Technology Operations LLC	US20190026597A1
10	CN	一种能够防误操作的自动泊车装置和方法	2018.05.14	吉利汽车研究院（宁波）有限公司； 浙江吉利控股集团有限公司	CN201810457759.0
11	CN	车辆的控制方法	2020.01.03	北京汽车集团有限公司； 北京汽车研究总院有限公司	CN202010008269.X
12	CN	基于驾驶人状态监测系统的车辆智能避险控制方法	2019.05.23	河南德力新能源汽车有限公司	CN201910433733.7
13	CN	车道保持控制系统及车道保持控制方法、车辆	2019.08.07	浙江吉利汽车研究院有限公司； 浙江吉利控股集团有限公司	CN201910726416.4
14	CN	一种无踏板自动驾驶车辆起步方法及装置	2019.06.18	吉林大学青岛汽车研究院	CN201910523928.0
15	CN	用于辅助驾驶人预防性驾驶的方法和系统	2019.06.03	沃尔沃汽车公司	CN201910477089.3
16	CN	一种带安全保护功能的智能驾驶系统	2016.03.02	上海航盛实业有限公司	CN201610119201.2
17	CN	一种用于车辆在环测试的传感器测试环境舱及测试方法	2019.11.08	同济大学	CN201911089013.X



序号	国家	专利名称	申请日	申请人	申请号
18	CN	基于硬件在环的自动驾驶智能汽车电磁兼容性测试平台	2019.12.18	长春汽车检测中心有限责任公司 宝马（中国）服务有限公司	CN201911324234.0
19	CN	故障注入测试方法、装置、系统及存储介质	2020.03.31	北京百度网讯科技有限公司	CN202010242677.1
20	CN	基于感知缺陷的自动驾驶测试场景的评价方法	2019.03.27	清华大学苏州汽车研究院（吴江）	CN201910236167.0
21	CN	一种用于自动驾驶汽车边缘测试的测试方法	2019.05.28	同济大学	CN201910453465.5
22	CN	一种自动驾驶测试场景的构建方法及其难度系数计算方法	2019.07.02	吉林大学	CN201910589116.6
23	CN	一种基于室内交通场景模拟传感器建模和验证装置及方法	2019.10.28	苏州智行众维智能科技有限公司	CN201911027717.4
24	CN	一种针对失效样本的自动驾驶视觉感知测试方法和装置	2019.10.09	武汉光庭信息技术股份有限公司	CN201910955518.3
25	CN	基于 V2I 的智能驾驶汽车传感器盲区安全控制方法及系统	2019.07.30	同济大学	CN201910692453.8
26	CN	自动驾驶车辆通过信号干扰区的能力的测试方法及测试场	2016.11.25	特路（北京）科技有限公司	CN201611056475.8
27	CN	一种无人车无信号灯环岛通行能力测试系统及测试方法	2020.01.22	长安大学	CN202010075003.7
28	CN	用于自动驾驶车辆逆光测试场及测试方法	2020.04.21	特路（北京）科技有限公司	CN202010319344.4
29	CN	一种用于智能网联汽车的电磁抗扰性能测试系统及方法	2019.12.12	中国汽车工程研究院股份有限公司;重庆凯瑞质量检测认证中心有限责任公司	CN201911276936.6
30	CN	坡道驾驶性能测试方法、装置及存储介质	2018.12.26	北京百度网讯科技有限公司	CN201811600249.0
31	CN	自动驾驶车辆通过视觉干扰区的能力的测试方法及测试场	2016.11.25	特路（北京）科技有限公司	CN201611056477.7
32	CN	车辆盲区信息的采集方法及装置	2018.12.05	汉能移动能源控股集团有限公司	CN201811484100.0
33	CN	一种车辆的盲区目标追踪方法	2019.08.13	浙江吉利汽车研究院有限公司;浙江吉利控股集团有限公司	CN201910744498.5
34	CN	一种基于熵权法的传感器共享最优节点选择方法	2019.12.16	桂林电子科技大学	CN201911291694.8
35	CN	基于车载盲区视觉场景分析控制转向扭矩的车道辅助方法	2019.08.29	浙江零跑科技有限公司	CN201910811032.2
36	CN	汽车路面标识盲区自动驾驶系统	2019.03.18	重庆睿驰智能科技有限公司	CN201910202558.0
37	CN	车载传感器的位姿调整方法、装置、设备和介质	2019.10.31	北京百度网讯科技有限公司	CN201911051040.8
38	CN	一种自动驾驶汽车环境感知的预测方法、装置及系统	2020.02.26	公安部交通管理科学研究所	CN202010120372.3
39	CN	一种商用车盲区障碍物检测方法及其装置	2020.03.16	东软睿驰汽车技术(沈阳)有限公司	CN202010181598.4
40	CN	一种弯道视野盲区消除系统及其方	2020.01.20	创驱（上海）新能源科技	CN202010065062.6



序号	国家	专利名称	申请日	申请人	申请号
		法		有限公司	
41	CN	基于单目识别的视野盲区避障方法及装置	2020.05.28	东软睿驰汽车技术(沈阳)有限公司	CN202010472961.8
42	CN	视觉盲区检测方法及装置	2019.08.16	北京百度网讯科技有限公司	CN201910758493.8
43	CN	一种盲区自动驾驶控制方法及系统	2019.08.21	浙江吉利汽车研究院有限公司;浙江吉利控股集团有限公司	CN201910773866.9
44	CN	夜间车辆检测方法、装置及系统	2020.03.19	南京兆岳智能科技有限公司	CN202010193642.3
45	CN	一种便于智能车辆驾驶的图像去雨方法	2019.08.26	电子科技大学	CN201910791277.3
46	CN	雨雾场景下的车辆感知系统及方法	2019.08.06	阿尔法巴人工智能(深圳)有限公司	CN201910719990.7
47	CN	一种基于域迁移的非结构化道路检测方法	2019.04.25	吉林大学	CN201910341103.7
48	CN	一种基于深度预测编码网络的夜视图像的场景预测方法	2018.04.10	东华大学	CN201810316986.1
49	CN	一种感知天气状况的方法及系统	2019.09.27	驭势科技(北京)有限公司	CN201910927454.6
50	CN	自动驾驶车辆雨天行驶安全保障系统及方法	2019.12.30	广州赛特智能科技有限公司	CN201911396433.2
51	CN	汽车外置感知传感器清洗装置及汽车	2019.09.02	北京新能源汽车技术创新中心有限公司	CN201921446143.X
52	CN	一种在自动驾驶系统中进行雨刷控制的方法和装置	2017.09.05	百度在线网络技术(北京)有限公司	CN201710792882.3
53	CN	一种基于亮度递减验证的夜间车辆尾灯提取方法	2015.04.13	杭州电子科技大学	CN201510171979.3
54	CN	一种基于高精度地图的汽车大灯转向随动控制系统及方法	2018.12.21	东风汽车集团有限公司	CN201811572970.3
55	CN	一种夜间无人车障碍物检测系统与方法	2020.03.12	武汉理工大学	CN202010169003.3
56	CN	一种自动驾驶汽车用夜视辨识装置	2017.11.17	南京视莱尔汽车电子有限公司	CN201721550308.9
57	CN	一种自动驾驶车辆底部智能照明光源	2018.07.25	一汽解放汽车有限公司	CN201821180725.3
58	CN	自动驾驶天气环境认知的方法、系统、计算机可读存储介质及车辆	2019.10.23	重庆长安汽车股份有限公司	CN201911009632.3
59	CN	集成的摄像机、环境光检测及雨传感器组件	2016.08.31	德尔福技术有限公司	CN201610786992.4
60	CN	激光雷达保护罩及激光雷达	2019.10.29	北京百度网讯科技有限公司	CN201911040346.3
61	CN	一种基于历史数据的轨迹规划的SOTIF的实现方法	2019.11.25	吉林大学	CN201911162457.1
62	CN	基于零日漏洞的自动驾驶预期功能安全危害评估方法	2019.11.14	华东师范大学; 上海工业控制安全创新科技有限公司	CN201911111961.9
63	CN	一种用于自动驾驶汽车预期功能安全的验证方法及系统	2019.01.09	同济大学	CN201910021029.0
64	CN	一种基于预期功能安全的自适应巡航开发与测试方法	2019.12.20	吉林大学	CN201911321150.1



序号	国家	专利名称	申请日	申请人	申请号
65	CN	自动驾驶算法预期功能安全的验证方法、平台及存储介质	2019.08.12	安徽江淮汽车集团股份有限公司	CN201910742725.0
66	CN	一种自动驾驶车辆速度控制多目标优化的跟驰算法	2018.12.26	同济大学	CN201811600366.7
67	CN	车辆驾驶系统及方法	2017.06.14	深圳市车米云图科技有限公司	CN201710454280.7
68	CN	一种安全辅助驾驶系统及控制方法	2018.07.06	联合汽车电子有限公司	CN201810739118.4



附表 B 现有材料提供单位

现有材料提供单位

章节	现有材料提供单位
第 1 章：前言	清华大学
第 2 章：国内外智能网联汽车预期功能安全相关政策/法规	公安部交通管理科学研究所
第 3 章：国内外智能网联汽车预期功能安全相关标准	中国信息通信研究院、公安部交通管理科学研究所、浙江吉利汽车研究院有限公司、泛亚汽车技术中心有限公司
第 4 章：国内外智能网联汽车预期功能安全相关技术	清华大学、同济大学、电子科技大学、浙江吉利汽车研究院有限公司、重庆长安汽车股份有限公司、重庆大学、北京理工大学
第 5 章：国内外智能网联汽车预期功能安全相关专利	同济大学、清华大学苏州汽车研究院
第 6 章：国内外智能网联汽车场景库研究现状	东风汽车集团有限公司、清华大学苏州汽车研究院、中汽研汽车检验中心（天津）有限公司
第 7 章：国内外智能网联汽车功能测试评价体系	清华大学苏州汽车研究院、北京汽车股份有限公司、重庆长安汽车股份有限公司、上海机动车检测认证技术研究中心有限公司
第 8 章：典型 ADAS 系统的 SOTIF 研究现状	北京航空航天大学、吉林大学、北京汽车股份有限公司、重庆长安汽车股份有限公司、上海测迅汽车科技有限公司