TC260-TR-001-2026

网络安全标准化技术研究报告

——智能驾驶网络和数据安全标准化研究

v1.0-202603

全国网络安全标准化技术委员会秘书处

全国网络安全标准化技术委员会网络安全评估标准工作组（WG5）

2026 年 03 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前 言

《网络安全标准化技术研究报告》（以下简称《技术报告》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织编制和发布的技术研究类文件。本文件立足新技术新应用领域网络安全前沿动态，通过系统的技术研究、产业调研、标准分析与综合研判，梳理关键领域网络安全风险与挑战，提出标准化发展趋势及相关工作实施建议，为网络安全国家标准制修订与网络安全保障实施提供前瞻性的技术参考与决策支撑。

声 明

本《技术报告》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《技术报告》的任何部分。凡转载或引用本《技术报告》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

技术支持单位

本《技术报告》得到公安部第三研究所、中国电子技术标准化研究院、湖北大学、北京车网科技发展有限公司、北京云驰未来科技有限公司、华为终端有限公司等单位的技术支持。

主要编写人员：王雪、陈广勇、张海春、郝春亮、杨思佳、王勇、张雨桐、曾剑隽、李哲、宋娟、王楠、于天任、张恒、彭建芬、栾兴霖

目 录

引 言

随着智能驾驶技术的快速演进，汽车正从传统机电控制系统向高度智能化、网联化的综合信息系统转变。人工智能、5G 通信、边缘计算、高精度定位等新一代信息技术的深度融合，使智能驾驶成为推动汽车产业变革和交通体系升级的重要力量。然而，系统智能化程度和车云连接水平的大幅提升，也带来了更复杂的网络安全挑战，网络安全已成为制约智能驾驶规模化落地的关键因素之一。

在此背景下，亟需从标准化角度系统构建面向智能驾驶的网络与数据安全保障体系。一方面，通过统一安全要求与技术框架，有效应对远程攻击、数据泄露、控制劫持等风险；另一方面，通过完善关键环节的技术规范，支撑算法可信、车云协同与通信安全等关键能力建设，为行业监管、标准制定及评估测试工作的开展提供技术支撑。

本研究围绕“智能驾驶网络和数据安全标准体系构建”展开，聚焦感知、决策、执行、通信及运维等关键环节，系统梳理跨车端—通信链路—云平台的安全风险与典型案例，提炼面向实际应用的安全需求；在此基础上，构建涵盖通用安全与基础共性、网络安全、数据安全、人工智能安全及安全管理与能力保障的标准体系框架，为智能驾驶安全体系建设提供基础支撑。

1. 概述

1.1. 研究背景

当前，智能驾驶功能已在量产车型中广泛应用，涵盖自适应巡航控制（Adaptive Cruise Control，ACC）、导航辅助驾驶（Navigate on Autopilot，NOA）、自动紧急制动（Automatic Emergency Braking，AEB）、车道保持辅助（Lane Keeping Assist，LKA）、盲区监测（Blind Spot Detection，BSD）及自动泊车等典型能力。随着系统由单车智能向车云协同持续演进，安全问题由传统车载电子与远程通信风险，进一步扩展至多模态感知数据安全、算法模型安全、V2X 通信安全、OTA 升级安全及运营服务全链条安全，呈现出跨域融合、链路延伸与动态演进等特征。

在此背景下，本报告以具备智能驾驶功能的智能网联汽车及其相关支撑系统为研究对象，重点覆盖 SAE J3016 所定义的 L1—L2/L2+组合驾驶辅助及 L3 及以上自动驾驶。研究范围聚焦“车端—通信链路—云平台—运营管理”全链条中的网络与数据安全问题，重点关注网络安全、数据安全及与其直接相关的算法安全和业务逻辑安全，不涉及功能安全及预期功能安全（SOTIF）的系统性分析。其中，智能驾驶是指智能网联汽车通过融合“智能功能”与“网联功能”，依托环境感知、智能决策、自动控制及与外界的信息交互，执行部分或全部动态驾驶任务。基于上述定义，研究内容既涵盖单

车智能驾驶场景下的系统安全问题，也覆盖车路协同环境中的跨系统安全问题。

基于上述技术发展与安全演进特征，开展智能驾驶网络和数据安全标准化研究，需围绕感知、决策、控制、通信、更新及运营等关键环节，系统识别安全风险，明确安全需求，构建覆盖全链条的标准体系与标准项目布局，以支撑相关技术实施、评估测试及行业监管需求。

1.2. 研究意义

智能驾驶网络和数据安全标准化研究对于促进我国智能网联汽车产业安全、有序、高质量发展具有重要意义。

保障产业安全与用户安全：通过构建系统化的安全标准体系，明确各环节安全要求与防护机制，可有效防范车辆被远程攻击、数据泄露、控制劫持等风险，保障驾驶安全与用户隐私。

推动标准体系完善与技术创新：研究成果将填补现有标准体系在智能驾驶安全领域的空白，推动形成覆盖“端—网—云”全流程的技术标准，为算法可信性验证、V2X 通信安全、车云协同安全提供依据。

支撑监管与测试认证体系建设：通过建立可操作、可评测的安全评估框架和测试方法，为政府部门制定监管政策、认证机构开展安全评估提供技术支撑，促进标准落地实施。

1.3. 研究目标

本研究以“智能驾驶网络和数据安全标准体系构建”为核心目标，围绕研究对象界定、风险识别、需求提炼、体系设计和标准规划五个层面展开，拟实现以下具体目标:

系统梳理智能驾驶安全风险与防护需求：全面识别智能驾驶在感知、决策、执行、通信、运维等环节的网络安全风险点，明确其安全防护需求。

构建标准化框架：围绕感知数据保护、车内网络传输、车端计算与存储安全、智能驾驶算法可信性、V2X 通信安全、入侵检测机制、车云协同安全管理等关键环节，构建覆盖“端、网、云”全流程的网络安全标准框架，推动形成一套具有可操作性、可测评性、可推广性的智能驾驶网络安全标准体系，支撑智能驾驶安全有序发展。

支撑政策制定与产业落地：为国家智能驾驶后续标准制定、测试验证、产业应用和监管落地提供理论支撑与实践指南。

2. 研究思路

本研究坚持“问题导向、体系化设计、可实施落地、可持续演进”的原则，围绕智能驾驶网络和数据安全的核心问题展开系统研究。通过对国内外政策标准、技术架构和安全案例的深入分析，识别智能驾驶在不同层级及不同场景下的网络和数据安全风险与防护需求，形成系统的需求分析与标准化建设框架。

研究的总体思路包括以下四个阶段：

现状研究与问题识别阶段：通过对国内外智能驾驶网络和数据安全相关政策、标准体系及典型实践案例的系统调研，掌握国际标准化趋势与差距，识别我国智能驾驶网络和数据安全在政策、标准、技术和管理层面的主要问题与短板。

需求分析与技术提炼阶段：从智能驾驶典型架构出发，分析其在数据处理、车内通信、算法计算、车云交互及运维管理等环节的安全需求，明确安全防护的重点对象、核心目标和技术要求，提出可量化的安全评估方法。

标准体系框架构建阶段：在充分分析安全需求和风险特征的基础上，构建覆盖“端—网—云”全流程的智能驾驶网络安全标准体系框架，明确标准的分层结构和关键领域，设计标准的总体架构与分类构成。

标准规划与落地实施路径阶段：在标准体系框架构建的基础上，面向各分领域和关键环节，系统开展标准规划，明确标准研制的优先级与布局结构，形成重点标准清单。

3. 技术及产业发展现状

3.1. 技术发展情况

智能驾驶技术正沿着“单车智能持续增强、车路云协同逐步落地”的路径演进。智能驾驶已经形成由感知、计算、通信、云服务和运

营管理共同构成的复杂技术体系，这决定了其安全问题不再是单一部件问题，而是跨域耦合问题。

智能驾驶通过集成 GPS、光学摄像头、激光雷达、超声波雷达、毫米波雷达、TPMS 等多种传感器，实现对周围环境的感知。传感器采集的环境数据、车辆状态数据以及通过 V2X 通信传输的数据，通过车内网络和无线通信方式传输到智能驾驶计算单元，经算法处理后，支持行车决策，如图 3-1 所示。

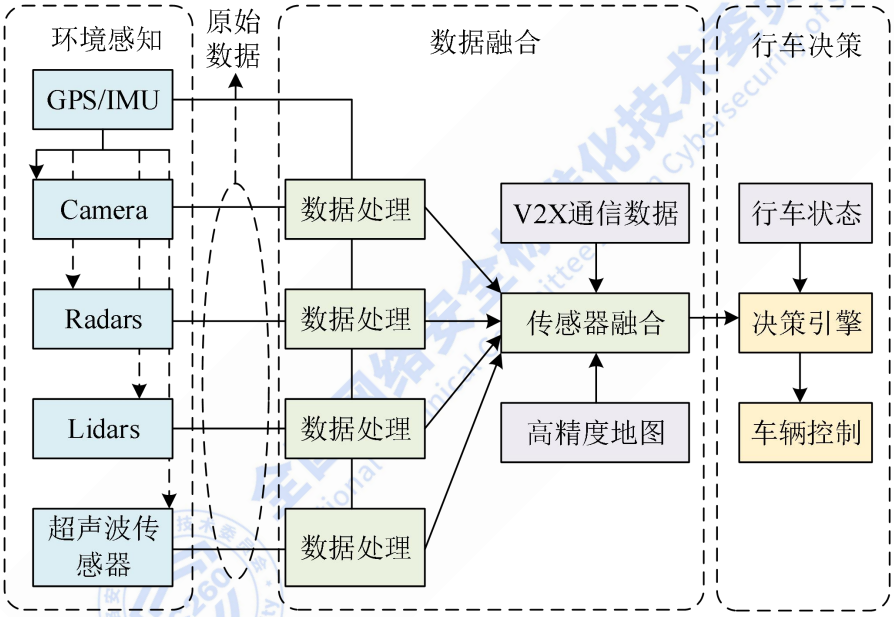

图 3-1 智能驾驶数据融合计算

在智能驾驶的复杂架构中，感知、决策、控制等模块之间相互协作，共同支持智能驾驶功能的实现。根据功能需求，可分为四个层次：感知层、网络层、计算层、应用层，如图 3-2 所示

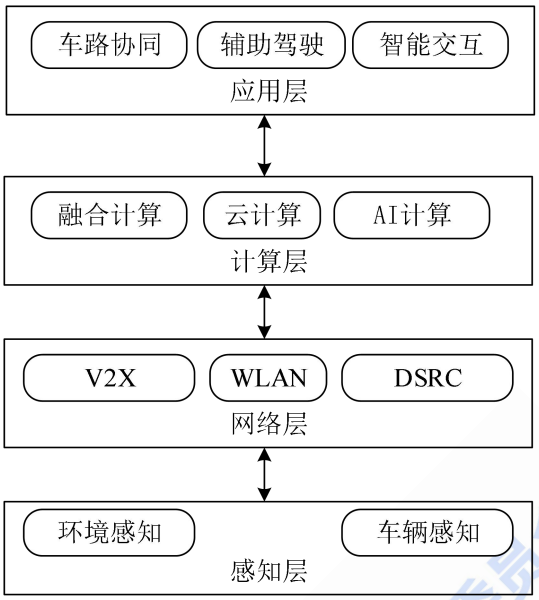

图 3-2 智能驾驶技术架构

感知层：包括加速度传感器、磁性感应、陀螺仪等物理量传感器，摄像头和雷达等视觉传感器，以及其他传感器系统，主要用于感知和获取环境信息。

网络层：确保车载系统和外部网络的通信，如专用短程通信技术（V2X）、车载环境无线接入技术和长期演进技术（LTE 等），实现数据的高效传输。

计算层：计算层是智能驾驶的数据处理与决策支撑核心，负责对多源感知数据进行融合分析，并支撑人—车—路协同运行。通过对海量车辆与环境数据的处理与建模，实现交通要素之间的动态协调，提高整体交通运行效率与安全性。

应用层：应用层面向具体业务场景，提供智能驾驶相关功能与服务。根据服务对象不同，可分为封闭式服务和开放式服务。封闭式服务主要包括自动驾驶、碰撞预警、电子收费等交通安全与效率

相关功能；开放式服务则包括信息娱乐、人机交互等面向用户的增值服务。

在上述架构基础上，智能驾驶逐步形成了以感知、定位、融合、预测、决策与控制为核心的技术体系。感知与定位负责获取车辆及环境状态，是系统的“输入基础”；融合与预测对多源信息进行统一建模并推测交通参与者行为；决策与控制根据环境状态生成驾驶策略并执行操作，是系统实现智能行为的关键。其中，环境感知与行为决策作为智能驾驶的“眼睛”和“大脑”，直接决定系统对外界环境的理解能力和行为选择能力，是当前技术研发与工程落地的核心。

随着人工智能与数据驱动技术的发展，智能驾驶正呈现出以下趋势：

（1）多模态融合感知持续深化

感知技术由单一传感器向多传感器融合发展，结合摄像头、毫米波雷达、激光雷达等多源数据，实现高精度三维环境感知。同时，基于深度学习与 Transformer 结构的算法不断提升系统在复杂场景下的感知精度与鲁棒性，使系统由“看见环境”向“理解环境”演进。

（2）决策规划向智能化与数据驱动演进

传统基于规则的决策方法逐步向数据驱动的智能决策转变，广泛引入强化学习、模仿学习等方法，实现对复杂交通场景中多主体行为的建模与预测，提升决策的灵活性与泛化能力。

（3）系统架构向端到端融合发展

为降低模块间误差累积与系统延迟，智能驾驶逐步由分模块处理向端到端一体化架构演进，通过统一模型实现从感知输入到控制输出的整体优化。

（4）工程化与安全性要求持续提升

随着技术从测试验证向规模化应用推进，系统对算法的实时性、可解释性、安全性及算力适配能力提出更高要求。同时，复杂交通场景下的鲁棒性与安全冗余能力成为关键挑战。

3.2. 产业发展情况

3.2.1. 国际产业发展情况

国际上，智能驾驶产业已从单纯的道路测试和技术展示，逐步转向准入管理、限定场景运营和持续监管并重的发展阶段。以Robotaxi、L2/L2+辅助驾驶和面向特定场景的高等级自动驾驶为代表的应用正在推进，但各国监管部门对安全责任、事件报告、软件更新和远程运营控制的要求也同步趋严。

从产业形态看，国际头部企业一方面持续推进高等级自动驾驶在限定区域内的示范运营，另一方面也在通过召回、停运整改和监管调查等案例暴露出感知鲁棒性、行为边界控制、运营治理和信息披露等方面的不足。这表明智能驾驶竞争已从功能能力竞争，进一步转向安全治理能力竞争。

因此，国际产业发展对标准化工作的直接启示在于：仅有通用

汽车网络安全和软件升级要求并不足以覆盖智能驾驶场景，仍需面向环境感知、车路协同、远程运营和事件处置建立更细化、可验证的标准要求。

3.2.2. 国内产业发展情况

我国智能驾驶产业已形成“量产辅助驾驶快速普及、L3 准入试点稳步推进、特定场景自动驾驶持续探索”的发展格局。监管体系也由前期测试示范逐步转向产品准入、上路通行、运营管理和数据治理并重。

从产品部署看，L2 和 L2+功能已在量产车型中广泛应用，智能驾驶与高精地图、云平台、OTA、车路协同等能力的耦合程度不断提高，安全问题已由传统车载电子安全扩展为跨车端、通信链路、云端平台和运营服务的系统性问题。

从制度演进看，我国已围绕整车信息安全、软件升级、汽车数据处理、准入试点和车路云一体化应用形成较完整的政策基础，但针对智能驾驶特有的环境感知安全、算法与模型管理、协同消息可信、运营服务安全和业务逻辑安全，仍缺乏足够细化的标准支撑。

这意味着后续标准化工作不能停留在通用汽车网络和数据安全要求的简单移植，而应面向智能驾驶的具体对象、具体场景和具体风险建立专门要求。

3.2.3. 地方产业情况

地方层面，北京、上海、深圳、武汉等地已围绕道路测试、示范应用、示范运营和商业化探索形成差异化实践，路侧设施建设、限定区域运营和远程安全员管理等机制不断完善。

这些实践说明，智能驾驶已由研发验证阶段进入与真实交通环境、运营组织和地方监管深度耦合的新阶段。标准化工作不仅要支撑产品研发和准入，也要支撑示范运营、日常监管、事件处置和持续改进。

同时，各地在运营边界、路侧设施能力、远程接管要求和数据治理安排上仍存在差异，客观上也提出了统一技术要求、统一测试方法和统一证据链要求的标准化需求。

4. 安全风险与重大问题分析

4.1. 安全问题及风险分析

如图 4-1 所示，智能驾驶由车端感知硬件、计算平台、车内通信、无线通信、云平台、算法模型与数据服务等多类对象构成，具有跨域融合复杂、链路耦合深、运行环境开放的特征。开展安全分析时，不能仅围绕单一模块罗列漏洞，而应从对象、链路和运行规则三个层面识别风险。

与传统汽车电子系统相比，智能驾驶风险更容易沿“感知输入—融合处理—决策规划—控制执行—远程协同”路径传导放大。任何一

个环节出现篡改、误用、失配或边界控制不当，都可能最终体现为错误决策、异常控制或规模化运营风险。

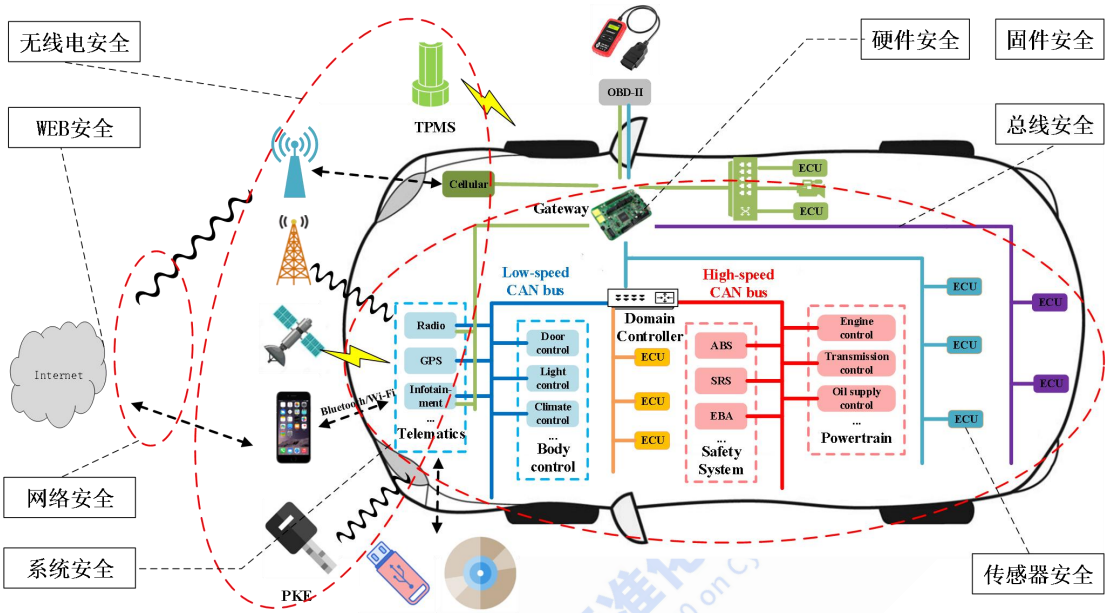

图 4-1 智能驾驶网络安全风险

结合智能驾驶架构和标准化需求，本文将风险重点归纳为硬件、固件、系统、总线、无线电、网络通信、云端、传感器、算法、数据及业务逻辑等类别。各类风险虽表现形式不同，但其共同特点是能够直接影响车辆对环境的判断、对控制命令的执行以及对运行边界的维持。

4.1.1. 硬件安全

智能驾驶依赖大量硬件板卡、域控制器、传感器控制单元、执行器控制单元及其配套芯片完成环境感知、数据处理、控制输出等关键功能。硬件安全是智能驾驶可信运行的基础，一旦硬件层遭到篡改、替换、失效或被非法访问，将直接影响感知准确性、控制稳

定性和整车安全。

在智能驾驶场景下，硬件安全重点体现在以下几个方面：一是关键控制板卡和处理芯片的可信性与完整性，需防范未经授权的硬件替换、恶意植入和非法调试；二是存储芯片中固件、密钥、配置参数和日志数据的安全保护，避免敏感信息泄露或被恶意篡改；三是板级调试接口、下载接口和维护接口的访问控制，防止攻击者借助 JTAG、SWD、USB 等接口获取系统控制权限；四是板载总线和片间通信的完整性保护，防止关键控制信号在传输过程中被监听、伪造或干扰。

对于智能驾驶而言，硬件层风险的危害不在于单纯的信息泄露，而在于其可能进一步破坏域控制器可信启动链、影响传感器数据采集结果、干扰执行器控制逻辑，并最终影响车辆的转向、制动、加速、泊车等核心驾驶功能。

4.1.2. 固件安全

固件作为连接底层硬件与上层系统软件的重要中间层，直接决定 ECU、域控制器、传感器模组及执行器单元的功能边界和运行方式。智能驾驶中的固件类型多样，包括基于通用操作系统的复杂固件、基于实时操作系统的嵌入式固件以及面向专用控制任务的轻量级固件，其安全状况对整车智能驾驶功能具有直接影响。

智能驾驶固件安全的主要风险包括：固件中硬编码密钥、口令、证书、接口地址等敏感信息，可能导致身份认证失效和控制链路暴

露；固件升级机制缺乏签名校验、版本校验和回滚保护，可能使恶意固件或错误版本进入关键控制单元；固件中的调试功能、诊断接口或隐藏命令未关闭，可能为非法访问和权限提升提供路径；固件逻辑存在缺陷时，还可能导致传感器驱动异常、控制信号失真、故障处理机制失效等问题。

在智能驾驶场景中，固件安全问题往往并不以单独失陷形式显现，而是通过影响摄像头、雷达、激光雷达、域控制器、制动控制器和转向控制器等关键部件的工作状态，进一步传导至感知融合、规划控制和故障应对环节。因此，固件安全应重点关注可信启动、完整性保护、安全升级和诊断访问控制等能力建设。

4.1.3. 系统安全

当智能驾驶控制平台运行复杂操作系统、中间件、虚拟化环境和容器化服务时，系统安全便成为保障智能驾驶功能稳定运行的核心问题。与传统车载信息娱乐系统不同，智能驾驶对操作系统和运行环境的要求不仅包括一般的信息安全要求，还包括高实时性、高可靠性、高隔离性和可恢复性等要求。

系统安全风险主要体现在：一是系统权限边界不清、账户控制薄弱、服务暴露过多，导致关键服务可能被非法访问；二是调度机制、资源隔离和任务优先级管理不当，可能影响感知、融合、规划、控制等实时任务的稳定执行；三是系统更新、补丁加载和服务热切换过程中缺乏有效校验和变更控制，可能引入兼容性问题和潜在安

全缺陷；四是日志、告警、异常监测和故障恢复机制不足，可能导致故障扩散且难以及时发现和处置。

对于智能驾驶而言，系统安全并不仅仅是防止主机被入侵，更重要的是确保关键任务在异常情况下仍能维持受控运行，保证感知融合链路、决策链路与控制链路的连续性与确定性，防止系统失效进一步演化为行车安全风险。

4.1.4. 总线安全

车内总线承担着 ECU、域控制器、传感器和执行器之间的数据交换与状态同步任务，是智能驾驶实现协同运行的关键基础设施。智能驾驶涉及的总线类型包括 CAN、LIN、FlexRay、MOST 及车载以太网等，不同总线承载的信号既包括感知数据、状态信息，也包括控制指令和诊断命令。

总线安全风险主要包括数据伪造、重放攻击、总线监听、优先级挤占、拒绝服务和协议实现缺陷等。若总线节点缺乏有效身份认证，攻击者可能伪装为合法节点接入车内网络；若总线报文缺乏加密与完整性保护，攻击者可能窃取感知数据、篡改状态信息或伪造控制信号；若总线负载管理和访问控制不足，还可能造成关键报文延迟、丢失或阻塞，影响自动紧急制动、车道保持、自动变道、自动泊车等智能驾驶功能的实时性和准确性。

在智能驾驶场景下，总线安全的核心不是一般的通信保密，而是对控制链中真实性、完整性、时效性的保障。任何对感知输入、

控制输出或系统状态同步的干扰，都可能直接引发错误判断和错误执行，因此总线安全是智能驾驶控制可靠性的基础组成部分。

4.1.5. 无线电安全

无线电系统是车内外信息交互的重要入口。对智能驾驶场景而言，重点风险并非一般消费电子短距无线功能，而是会影响定位、协同感知、远程接入和运营控制的无线链路风险。

从智能驾驶实际应用看，无线电安全应重点关注以下几类风险：一是 GNSS/GPS 等定位信号受干扰或欺骗，导致车辆定位结果偏移，进而影响高等级辅助驾驶、领航辅助和自动驾驶场景中的车道级定位；二是 C-V2X、DSRC、5G 等车外通信链路遭遇伪基站、信号干扰、中间人攻击或虚假消息注入，导致车路协同信息、道路事件信息和远程指令失真；三是无线接入接口管控不足，可能使攻击者通过近距离或远距离链路接近车载系统，扩大攻击面。

与智能驾驶关系不大的通用短距无线应用风险不再展开。本节重点强调，无线电安全问题一旦影响定位、协同感知、远程接入和运营控制，就可能直接改变车辆对道路环境和运行状态的判断，进而影响决策和控制结果。

4.1.6. 网络系统安全

本框架中的网络安全，主要指基于 IP 协议的车云通信、远程诊断、OTA 更新、地图服务、日志回传、运营管理与远程控制相关的

网络通信安全。其关注重点不是传统互联网环境下的通用网络风险本身，而是这些风险如何作用于智能驾驶功能链路。

智能驾驶网络通信面临的主要风险包括：敏感数据在传输过程中遭窃听和泄露，导致车辆状态、运行轨迹、控制策略、诊断信息等被非法获取；通信报文遭篡改、伪造或重放，导致远程命令、地图服务结果、参数配置和策略下发失真；攻击者介入合法通信链路实施中间人攻击，进而劫持车云数据交互过程；边缘节点、车队管理接口或远程服务接口暴露过多，导致非法调用和未授权访问。

对于智能驾驶而言，网络安全风险往往不会停留在信息层面，而是可能进一步作用于控制层。例如错误的地图更新、异常的参数下发、伪造的远程指令和篡改的协同消息，都可能在系统内部被当作合法输入处理，进而影响车辆行为。因此，网络安全应与功能安全、运行边界管理和远程操作控制要求一体考虑。

4.1.7. 云端安全

智能驾驶通常依赖云平台提供高精地图服务、OTA 升级、模型训练与发布、车队运营管理、远程诊断、日志分析、运营调度和车路协同支撑能力。云端平台已成为智能驾驶生态的重要组成部分，其安全状态直接关系到单车能力稳定性以及规模化运营安全。

云端安全风险主要体现在三个方面。其一，平台接入与身份认证机制不足，可能导致车辆、用户、运维人员和第三方服务商访问边界不清，形成越权操作风险；其二，云端模型、参数、策略、地

图和软件制品的管理链路缺乏严格的签名校验、版本控制和发布审计，可能导致错误更新、恶意替换或配置漂移最终影响车端功能；其三，运营平台、调度平台和数据平台的接口安全不足，可能引发远程调度异常、日志泄露、批量配置误下发和车队级联动风险。

云端安全对于智能驾驶的重要性在于其具有集中控制、集中服务、集中更新的特征，一旦云端安全能力不足，风险可能由单点迅速扩展至多车、多区域、多版本系统，形成规模化安全事件。因此，云端安全应重点围绕身份认证、权限控制、发布链路保护、接口治理、运行审计和应急处置展开。

4.1.8. 传感器安全

传感器是智能驾驶感知外部环境和自身状态的前端基础，包括摄像头、毫米波雷达、激光雷达、超声波传感器、GNSS/GPS、IMU等。智能驾驶对传感器数据的高度依赖，使传感器安全成为影响感知可信度和决策正确性的关键因素。

传感器安全风险主要表现为误检、漏检、错检、感知失真和定位偏差。GPS/GNSS信号可能受到干扰和欺骗，导致车辆定位出现偏移；激光雷达可能因虚假回波、信号注入和遮挡干扰产生虚拟障碍物或遗漏真实目标；毫米波雷达可能因特定频率信号干扰、目标伪造和信噪比下降影响障碍识别；超声波传感器可能在近距离场景中受到欺骗和阻塞，影响自动泊车与低速避障；摄像头则可能受逆光、眩光、激光照射、污损、雨雪雾等因素影响，造成交通标志识

别、车道识别和目标检测失败。

与一般车载设备安全不同，传感器安全问题会直接输入智能驾驶感知融合链路。一旦传感器层形成错误观测，后续融合、规划和控制模块即使运行正常，也可能基于错误环境模型做出危险决策。因此，传感器安全分析应强调物理世界干扰、环境鲁棒性、多传感器交叉验证和失效降级机制，而不局限于单一设备的通信安全问题。

4.1.9. 算法安全

在智能驾驶中，算法承担着环境感知、目标识别、轨迹预测、路径规划、行为决策和控制策略生成等核心任务，是连接感知输入与控制输出的关键技术中枢。随着深度学习、强化学习、端到端模型和数据驱动方法的广泛应用，算法安全已成为智能驾驶安全分析的重要内容。

算法安全风险主要包括以下几类：一是训练数据投毒、标注错误和样本偏差，可能导致模型在特定场景下学习错误规则，进而产生系统性误判；二是对抗样本攻击和输入扰动攻击，可能使模型在外观变化极小的情况下输出错误识别结果；三是模型泛化能力不足，在长尾场景、复杂天气、异形目标、施工区域和混合交通环境中出现能力退化；四是模型部署、热更新、参数加载和在线优化过程中缺乏有效校验，可能导致模型版本错误、参数漂移或被恶意篡改。

对智能驾驶而言，算法安全问题的突出特点在于其隐蔽性强、传播链路复杂、验证难度高。算法风险并不一定表现为系统完全失

效，更多情况下表现为局部偏差、特定场景误判和行为选择异常，这类风险更难通过传统故障检测方式发现。因而，智能驾驶算法安全应覆盖训练、验证、部署、运行和更新的全流程管理，并重点关注鲁棒性、可验证性、变更可追溯性和异常检测能力。

4.1.10. 数据安全风险

数据安全风险是智能驾驶安全风险的重要组成部分，其特殊性在于数据不仅承载隐私和合规属性，还直接参与感知训练、地图服务、模型迭代、远程运营和事故追溯。数据一旦被误采、误传、误用或篡改，不仅会导致合规问题，还可能反向作用于车辆行为。

（1）重要数据风险

智能驾驶持续采集道路环境、交通流和车辆运行数据，其中部分数据可能涉及重要区域环境信息、道路运行态势或批量车辆行为信息。一旦采集边界不清、存储控制不足或对外提供缺乏约束，可能引发重要数据泄露和敏感区域信息暴露风险。

尤其是车外视频图像、时空轨迹、路侧协同信息和高频运行日志，在特定场景下既可能包含个人信息，也可能形成高价值的重要数据集合，不能仅按一般业务数据处理。

因此，智能驾驶数据治理应将采集必要性、场景约束、存储边界、对外提供条件和销毁要求纳入统一规则。

（2）个人信息风险

智能驾驶相关个人信息既包括座舱采集的人脸、声纹、驾驶行

为和交互记录，也包括车外画面中的可识别信息以及与远程服务相关的账号、位置和使用偏好。其风险贯穿采集、传输、存储、使用、共享和删除生命周期。

突出问题包括超范围采集、默认全量采集、告知同意不足、敏感信息处理边界不清、权限关闭路径不便捷以及个人信息与运营数据混合使用等。

这类风险不仅损害个人信息权益，也会削弱用户对智能驾驶的信任基础。

（3）云平台数据风险

智能驾驶云平台集中承载日志回传、模型训练、地图服务、运营调度和远程升级等能力，数据安全风险主要体现在分类分级不足、访问控制不严、接口暴露过多、跨域流转失控以及备份恢复与审计能力不足。云端失陷还可能引发多车、多区域的连锁风险。

因此，后续标准化需要同时覆盖数据对象界定、流转规则、接口控制、证据留存和责任划分。

（4）运营服务数据风险

随着智能驾驶从研发测试走向规模化运营，车队调度、远程协助、用户服务、日志回传、事件复盘和持续优化将产生大量运营数据。其风险不再局限于单车数据处理，而是扩展到跨车辆、跨平台、跨区域的数据协同和远程控制安全。

这表明数据安全已成为智能驾驶规模化落地的基础条件之一，

后续应通过专门标准对运营服务、远程控制、车云协同和多主体数据合作等业务场景作出更明确要求。

4.1.11. 业务逻辑安全

智能驾驶业务逻辑安全，是指攻击者或异常输入不必突破传统访问控制边界，而是通过操纵功能启停条件、状态机转换、策略规则、关键参数、远程工作流和跨域协同逻辑，使系统在“形式合法”的调用和输入条件下产生不安全行为的风险。与传统网络攻击相比，业务逻辑安全更贴近智能驾驶真实运行过程，具有较强隐蔽性和复合性。

该类风险主要表现为：运行设计域识别逻辑缺陷导致系统在不适用场景下启用或未及时退出；模式切换和降级策略不完善，导致系统在应当接管、退出、限能或停车时继续运行；关键参数、阈值和策略表缺乏完整性保护和版本一致性管理，导致配置漂移、跨版本不一致和行为异常；车云协同和远程服务中的工作流编排不合理，使低权限主体通过业务流程缺陷实现越权下发、批量配置或异常回滚；异常处置逻辑、冲突仲裁逻辑和故障恢复逻辑不完善，导致系统在复杂场景中频繁抖动、反复降级甚至失控。

业务逻辑安全是智能驾驶标准体系中不可忽视的内容。其关键不在于一般意义上的软件漏洞，而在于系统规则本身是否稳健、边界是否清晰、状态机是否完备、证据链是否可追溯。应将 ODD 约束、模式转换、关键工作流、关键参数一致性和异常仲裁机制纳入标准

化规范。

4.2. 关键案例研究

以下案例不再泛泛罗列行业事件，而是围绕 L2 边界管理、测试运营治理、碰撞后行为控制、可预见误用防范和地图—感知—控制耦合等与标准制定直接相关的问题展开分析，目的在于从事故和召回中提炼出具体的标准化需求。

4.2.1. 特斯拉 Mountain View 事故：L2 系统边界识别与驾驶员监控不足

美国国家运输安全委员会（NTSB）对 2018 年美国加州 Mountain View 事故的结论指出，事故原因包括：Tesla Autopilot 因系统局限将车辆导向高速公路分流区，驾驶员因分心和对部分自动驾驶功能的过度依赖未及时接管；同时，车辆对驾驶员参与度的监测无效，助长了驾驶员的麻痹与不注意。

这一案例对应的标准化启示非常明确。第一，L2 功能必须通过更强的人机界面设计明确责任边界，避免用户将辅助驾驶理解为自动驾驶。第二，驾驶员监控不能停留在是否触碰方向盘的低水平判断，而应提升对持续注意力和接管能力的识别。第三，系统在分流区、事故场景、标线异常区等已知高风险 ODD 边界附近，应采取更保守的行为策略与更强制的告警退出机制。该案本质上是系统能力边界与人因监控不足共同作用的典型实例。

4.2.2. Uber Tempe 致死事故：测试运营治理失效与冗余安全缺失

NTSB 对 2018 年美国亚利桑那州 Tempe 事故的结论认为，直接原因是安全员在测试过程中持续看手机，未监控道路环境和自动驾驶系统运行；同时，Uber ATG 在安全风险评估、测试员管理和抑制自动化 complacency 方面存在明显缺陷，其安全文化不足也是事故的重要促成因素。NTSB 还指出，亚利桑那州交通主管部门对自动驾驶道路测试的监管不足也是促成因素之一。

这一案例说明，智能驾驶标准不能只写算法精度和硬件性能，还必须覆盖测试运营治理要求，包括测试员配置、值守规范、场景准入、运行中监督、事件复盘和退出机制。对于研发测试阶段的 ADS，标准应明确：测试车辆不得以不充分验证的软件替代成熟量产安全冗余；测试组织必须建立风险评估与变更评审机制；道路测试必须具备可审计的监控与问责链路。否则，即使系统技术路线先进，也可能因组织管理失效而发生严重后果。

4.2.3. Cruise 旧金山行人事件：碰撞后行为策略与安全报告合规问题

根据 Cruise 提交给 NHTSA 的召回文件，2023 年 10 月 2 日，一名行人先被旁侧人类驾驶车辆撞击后落入 Cruise 无人车前方。Cruise 车辆初始制动后，其 ADS 将事件错误识别为侧向碰撞，并执行靠边停车动作而非原地保持，导致行人被继续拖拽。Cruise 因此

对相关 ADS 软件发起召回。加州 DMV 随后宣布立即暂停 Cruise 在加州的无人化部署与无安全员测试许可，理由包括车辆对公众运行不安全，以及企业对自动驾驶安全相关信息存在不实陈述。2024 年，NHTSA 又就该事件的事故报告不完整问题与 Cruise 达成同意令，指出 Cruise 在法定时限内提交的报告遗漏了行人被拖拽约 20 英尺的关键细节。

这一案例对标准体系至少提出三项要求。第一，智能驾驶不只要规范碰撞前规避，还必须规范碰撞后行为，包括保持静止、二次伤害避免、故障隔离和人工接管接口。第二，Robotaxi 无人化运营的安全要求不能只看道路表现，还必须纳入事件报告、事实披露、监管接口和证据留存。第三，车端控制逻辑与企业级安全治理应一体纳入评价，否则即使车端技术问题可修复，运营主体的不透明和不合规同样会构成公共安全风险。

4.2.4. 特斯拉 2023—2024 年 Autosteer 召回与后续调查：可预见误用与模式混淆

NHTSA 2023 年召回文件显示，Tesla 共召回约 203.122 万辆配备 Autosteer 的车辆，监管部门认定在某些情况下，Autosteer 的控制措施在显著性和范围上不足以防止驾驶员误用这一 SAE L2 辅助驾驶功能，从而增加碰撞风险。2024 年，NHTSA 又就该召回的补救有效性启动 Recall Query，明确调查重点包括：是否足以解决误用、模式混淆以及系统在非设计环境下被使用的问题。NHTSA 还指出，

在 EA22002 相关工作中，已识别出至少 13 起与可预见误用有关、涉及一人及以上死亡的事故，以及更多严重伤害事故。

这一案例说明，智能驾驶安全问题不能简单归咎于“用户误操作”。当误用具有可预见性、可重复性并与系统设计、人机界面、告警策略、可用场景限制密切相关时，误用本身就应被视为设计缺陷的一部分。因此，在标准条款中应明确要求：系统名称、营销表述、功能可用条件、激活门槛、驾驶员监督机制和退出策略之间必须保持一致；对可预见误用的防范应成为 L2/L3 功能设计验证的强制内容，而不能作为售后教育或用户自担风险处理。

4.2.5. Waymo 2024 低速碰撞电线杆事件：地图—感知—控制耦合缺陷

Waymo 向 NHTSA 提交的 2024 年召回报告显示，2024 年 5 月 21 日，一辆 Waymo 自动驾驶车辆在美国菲尼克斯执行低速靠边停车动作时，与巷道内一根木质电线杆发生碰撞。Waymo 随后启动分析，提出两类缓解措施：一是优化 ADS 对电线杆及类似永久性物体的响应；二是改进地图，使相关物体与可通行区域之间以“硬边界”形式得到更准确表达。

该案虽然未造成人员伤亡，但对于标准制定很有价值。它表明，智能驾驶的失效并不总是发生在高速、复杂、激烈交互场景中，低速、窄路、靠边停车、固定物识别和可行驶区域边界处理同样可能暴露系统缺陷。标准中应增加对低速精细操作安全的要求，覆盖路

缘、立杆、锥桶、窄通道、背街小巷、非标准化停车带等边缘场景，并要求地图、感知与控制在边界对象处理上的一致性验证。

5. 安全相关政策与标准分析

5.1. 国外标准与政策

国外相关制度可以概括为两类：一类是面向汽车网络安全、软件更新和数据保护的通用制度框架，另一类是面向高等级自动驾驶测试、准入和运营的专门规则。对本报告而言，前者提供安全治理底座，后者揭示智能驾驶场景下新增的监管关注点。

在通用制度层面，UNECER155、UNECE R156、ISO/SAE 21434 以及数据保护、关键信息基础设施和供应链安全相关规则，已经对整车网络安全管理、软件升级、事件响应、数据处理和主体责任提出系统要求。这些规则为我国标准化工作提供了重要参照，但其对象大多仍是通用汽车网络安全和软件更新活动。

在自动驾驶专项治理层面，各国正在将监管重点从“是否允许测试”转向“如何安全运营”。事故报告、远程监控、事件复盘、软件变更管理、运行边界控制和运营主体责任，正成为高等级自动驾驶监管的共同关注点。

这表明，国际规则虽已覆盖汽车网络安全与数据治理的基础制度，但对于智能驾驶特有的环境感知安全、协同消息可信、模型与数据闭环安全、业务逻辑安全以及规模化运营安全，仍缺乏足够细

化、可测试、可抽查的要求。

因此，国际经验对本项目的启示不是简单照搬条文，而是要在现有通用制度基础上，补齐面向智能驾驶对象、场景和运行过程的专门标准。

5.2. 国内政策与标准

国内制度已基本形成“法律法规—部门规章和政策文件—国家标准和行业标准”相衔接的框架。法律层面以《网络安全法》《数据安全法》《个人信息保护法》为总依据；行业治理层面以汽车数据处理、整车准入、道路测试、上路通行试点和车路云应用试点等制度为重点；标准层面则以整车信息安全、软件升级、汽车数据处理和车联网安全相关标准为基础。

现有制度已基本明确企业主体责任、数据分类分级、境内存储、个人信息保护、软件升级管理和测试示范要求，为智能驾驶安全治理奠定了基础。

但从智能驾驶标准化需求看，现有国家标准仍以通用整车信息安全、软件升级和数据处理为主，对环境感知安全、算法模型管理、车路协同可信交互、运营服务数据安全、业务逻辑安全和多主体协同治理等内容覆盖不足，尚难直接支撑后续准入抽测、运营监管和场景化安全评估。

因此，第五章的结论并非“现有制度已经充分”，而是“现有制度已提供底座，但智能驾驶特有风险尚缺少专门标准承接”。这正是本

项目开展需求分析、体系设计和标准规划的必要性所在。

6. 网络安全需求分析

第四章表明，智能驾驶网络安全风险主要集中在环境感知、车内平台、车外通信与协同、云平台与 OTA 以及业务逻辑控制等方面。相应的第六章不再泛化讨论一般信息系统安全，而是围绕这些与智能驾驶直接相关的风险对象提出网络安全需求，并进一步转化为可实施、可测试、可评估的标准化方向，如图 6-1 所示。

图 6-1 智能驾驶网络安全技术框架

6.1. 网络安全技术要求

6.1.1. 环境感知安全技术要求

环境感知系统作为智能驾驶的“感官前端”，承担着对外部动态环境的实时感知、目标检测、物体识别与空间建模等关键任务，是实现安全决策与控制执行的基础支撑环节。该系统高度依赖车载多源传感器的协同运行，包括摄像头、毫米波雷达、激光雷达、超声波雷达、惯性测量单元（IMU）、全球定位系统（GPS）、胎压监测系统（TPMS）等。传感器安全性直接关系到环境感知结果的准确性、完整性与可信性，其一旦遭受攻击或发生故障，可能导致目标误识别、路径误判、行为异常等严重后果，进而引发系统性失控与交通安全事故。

为保障环境感知系统的安全可靠运行，应从传感器层级、数据链路、感知融合、异常检测等方面构建系统化的技术安全要求，具体包括:

（1）传感器身份可信与物理接口安全

所有关键传感器应具备唯一身份认证机制，防止非法设备接入与仿冒替代；硬件接口应配置接口访问控制与异常访问告警机制，防止后装模块植入或总线监听；对传感器固件版本进行完整性校验，防止恶意篡改或固件注入攻击。

（2）感知数据链的完整性与抗篡改保护

传感器采集数据应具备时间戳与序列号机制，确保数据在多传

感器同步场景下的时效性与一致性；数据传输链应实现端到端的完整性校验与链路加密保护，防止中间人攻击与数据劫持；支持数据签名机制以保障感知数据源的可信溯源能力。

（3）抗欺骗与抗干扰能力

摄像头系统应具备对抗图像投影干扰、红外/激光眩光攻击等能力；

毫米波雷达与激光雷达应部署干扰识别与动态频率跳变机制，防范伪造回波与信号覆盖干扰；GPS 应支持 GNSS、IMU、地图多源定位融合机制与欺骗信号识别；胎压监测等传感器应防止无线信号重放与伪造。

（4）多源融合容错机制与可信度评估

在感知系统设计层应引入冗余设计与可信融合机制，如基于传感器可信等级进行加权融合、误差交叉验证等；建立传感器健康状态感知与自动隔离策略，支持在单一传感器退化或失效时进行动态信任重构；引入可信度评分体系，对融合结果进行动态置信度评估并与规划决策模块联动处理。

（5）感知链安全事件检测与响应机制

部署感知行为异常检测模块，识别异常目标出现、轨迹突变、输入分布漂移等现象，提升应对感知层攻击的响应能力；建立感知层攻击特征数据库与响应策略集，支持本地检测与云端协同防御；明确感知层安全事件的分级响应机制，结合系统场景采取“降级运行、

部分功能切换至冗余模式或紧急停车”等响应策略。

6.1.2. 车内网络安全技术要求

车内网络是连接感知、计算、控制和执行模块的关键基础设施，其需求分析应直接对应第四章中的总线安全、系统安全和硬件可信风险。对智能驾驶而言，车内网络安全的核心不是一般保密要求，而是保证关键报文和控制链路的真实性、完整性、时效性与隔离性。

6.1.2.1. 车载 CAN 总线

CAN 总线因其结构简单、实时性高，在制动、转向、动力系统等底层控制与执行模块中广泛应用。但其广播通信、无源认证、缺乏加密等特性使其易受重放攻击、仿冒注入与拒绝服务攻击。核心安全技术要求如下：

（1）节点认证机制：所有 ECU 节点应通过预共享密钥或动态认证机制完成身份验证，防止伪造节点注入非法帧；建议引入基于轻量级算法实现快速认证。

（2）消息认证与完整性保护：为关键控制指令帧添加 MAC 认证字段或基于时间戳的签名机制，防止中间人篡改与帧重放；针对 CAN FD 可利用 64 字节数据段空间嵌入完整性校验字段。

（3）速率限制与流量监控机制：设置 ID 使用频率门限机制，防止攻击者利用高频注入造成总线占用；配置网关层 CAN 帧速率异常检测机制，进行实时入侵告警。

（4）物理隔离与逻辑分区：对动力域、信息娱乐域等不同安全等级域进行物理分区或经由安全网关进行访问控制；实施帧路由白名单机制，限制低安全域访问高安全域数据通道。

6.1.2.2. 车载以太网

车载以太网因其高带宽、强扩展性，被广泛用于感知数据传输、中央融合计算等智能驾驶核心环节，面临 ARP 欺骗、DoS 泛洪、数据嗅探等更多高级威胁。核心安全技术要求如下：

（1）链路加密与身份认证机制：应采用 MACsec 或 IPsec 协议对车载以太网链路进行加密与身份认证，保障数据保密性与完整性；配置设备级密钥协商协议以限制非法设备接入网络。

（2）分段通信隔离与访问控制策略：对不同功能模块之间通过 VLAN 划分进行逻辑隔离；采用访问控制列表机制进行通信路径管控，仅允许授权服务之间的数据流通。

（3）基于行为的入侵检测系统：在网关、交换机或主干节点处部署以太网流量异常检测系统，通过流量特征、时序分析、行为建模等方式识别异常通信行为；支持基于规则与 AI 结合的自适应检测机制。

（4）时间同步完整性保护：智能驾驶高度依赖 PTP 时间同步机制，须防范时间注入攻击与漂移欺骗；引入时间源认证机制与时间戳可信传播验证机制。

（5）远程访问与配置管理安全：所有远程以太网管理接口需部署基于角色的访问控制与多因子认证机制；网络设备配置变更须进行完整性校验与操作日志记录。

6.1.3. 硬件及系统安全要求

6.1.3.1.硬件安全

硬件及系统安全技术要求主要对应第四章中的硬件安全、固件安全和系统安全风险，重点关注可信启动、运行隔离、接口控制、异常恢复和关键任务持续可控。

以下从设备启动、身份认证、执行环境、物理接口、硬件隔离与协同防护等方面，系统总结智能驾驶硬件的安全技术要求。

（1）设备启动安全：硬件平台应支持安全启动机制，即在启动过程中依次验证 Bootloader、操作系统、应用镜像的签名；启动链中每一阶段必须经由硬件级信任根进行签名验证，确保启动组件未被篡改；在验证失败时，系统应进入安全锁定模式，阻止恶意软件加载与执行。

（2）硬件级身份认证与密钥保护：每个硬件模块应具备唯一设备标识符，并支持基于 PKI 的数字证书机制进行认证；私钥、认证凭据、算法模型等安全关键数据应存储于安全模块中，支持硬件加密存储与密钥不可导出机制；支持设备级双向认证机制，确保车内模块与车外平台之间的通信建立于可信链路之上。

（3）可信执行环境：高等级智能驾驶平台应集成 TEE 模块，划分受保护的隔离运行区域用于执行行为决策、路径规划等关键算法；TEE 应具备最小信任基结构清晰、抗侧信道攻击、抗代码注入能力；所有涉及感知数据融合、控制策略生成等关键任务的代码，优先在 TEE 中运行。

（4）硬件接口访问控制与安全配置：所有调试接口默认应处于关闭状态，激活需物理权限验证与加密授权过程；针对通信总线，应配置访问控制策略与白名单机制，限制非授权消息注入；系统支持接口安全审计机制，记录非法访问行为并支持本地/远程响应。

（5）物理防篡改与电源安全保护：敏感硬件区域应具备防篡改封装、防探针访问、防物理旁路读取设计；模块应具备通断电状态监测与电压异常保护机制，防止通过电源干扰实施故障注入攻击；配置电池备份与硬件熔断机制，在非法访问或异常拔插事件发生时，自动擦除密钥并记录事件日志。

6.1.3.2.操作系统安全

操作系统与运行环境是智能驾驶计算平台的基础承载层。相关要求应突出高实时、高可靠和高隔离场景下的运行可信，而不是照搬通用终端操作系统安全要求。

一旦操作系统出现安全缺陷或被恶意利用，攻击者可能获取内核权限、篡改算法进程、控制车辆执行、干扰传感器输入，甚至破

坏整车行为的确定性与可控性。因此，必须构建面向智能驾驶操作系统的系统化安全技术要求体系，以实现运行时的可信、隔离、可控与可恢复。主要安全技术要求如下：

（1）操作系统启动安全：安全启动链支持：操作系统必须处于可信启动链中，确保内核、驱动、服务等启动镜像均经由数字签名验证；操作系统启动过程中应进行完整性校验，防止篡改后的内核加载运行。

（2）内核安全机制：执行空间防写机制，运行期间操作系统内核空间必须只读化，防止攻击者通过代码注入或 ROP 等技术修改内核逻辑；内核运行完整性，所有动态加载模块必须进行签名验证与版本匹配；内核最小化与裁剪机制，应采用精简内核以降低攻击面，仅保留必要功能。

（3）进程与任务隔离机制：运行于 OS 之上的感知、控制、娱乐等各类功能模块应在不同进程空间中运行，防止相互影响；应基于内存空间划分和调度分区，构建如 ARINC 653 或类似的“时空隔离机制”；内存访问控制与权限校验，通过 MMU 配置或虚拟内存机制，确保每个模块只能访问其授权地址空间。

（4）通信与接口安全控制：系统调用访问控制，对 OS 暴露的系统调用接口进行权限控制与访问审计，防止非法调用关键资源；IPC 安全控制机制，对进程间通信设置信任域，防止低权限进程向高权限进程注入数据。设备驱动接口校验机制，防止通过非法接口

配置篡改传感器或执行器行为。

（5）任务调度安全与时间控制：支持调度行为的实时追踪与异常检测，提高系统运行可审计性，异常调度检测与恢复机制，当系统调度出现死锁、长时延等异常行为时，能自动进入故障恢复或降级运行模式。

（6）日志审计与异常检测机制：OS 运行日志应加密存储，防止攻击者伪造或清除痕迹；部署基于行为建模的异常检测模块，如系统调用频率异常、任务调度漂移，识别潜在攻击行为；联动响应机制，支持异常行为与上层功能模块或车载安全控制策略联动，触发控制限制或系统自我修复。

（7）基于可信计算的操作系统运行可信度保障：运行时度量机制，实现操作系统状态的远程验证；操作系统启动与关键模块执行须依赖硬件信任根认证，防止替换执行环境。

6.1.4. 算法安全技术要求

算法安全技术要求主要对应第四章中的算法安全和传感器安全风险。标准化重点应放在输入可信、训练与部署过程可追溯、模型鲁棒性验证、运行中漂移监测以及更新可回退等方面。

为实现智能驾驶的全栈安全保障，必须针对算法本身构建系统性的安全技术要求，从数据、模型、行为、运行、更新等全过程角度强化算法层的鲁棒性、可信性与可控性。核心安全技术要求如下：

（1）算法输入安全与防御对抗样本攻击：感知算法在接收图像、

点云、轨迹等输入前，必须执行输入格式、尺寸、频率与合法性检查。

（2）采用对抗训练、特征平滑、输入模糊滤波等技术提升算法对微小扰动的鲁棒性；对每个输入通道设置置信评分机制，识别感知异常、伪造目标或合成场景干扰。

（3）模型训练安全与防止数据投毒：构建训练数据的签名与哈希校验机制，防止恶意样本注入或标签篡改；采用可信执行环境对训练任务进行隔离，确保中间参数与梯度不被泄露或操控；记录训练样本采集路径、标注者身份与修改历史，实现训练数据全生命周期可追踪。

（4）模型鲁棒性与行为稳定性保障：在部署前通过仿真与测试集进行鲁棒性验证，评估预测误差与退化边界；建立基准场景集，验证模型在不同天气、道路、光照、稀有目标条件下的稳定表现。

（5）模型部署与运行安全：所有算法部署包须通过数字签名认证与哈希校验，防止中间替换或指令注入；模型执行过程中部署行为审计模块，实时监控其计算路径、资源使用与输出变化，识别异常激活或预测漂移；目标识别、碰撞预测等关键控制链路可采用“双模型交叉校验”策略，提升抗单点失效能力。

（6）模型更新与回滚机制：算法模型更新须经加密传输，并进行版本匹配与签名校验；模型发布、安装与卸载过程应具备日志记录与版本追踪能力；在模型更新后出现误判、行为漂移、延迟异常

等情况时，应支持一键回退至上一稳定版本。

6.1.5. 车外网络安全技术要求

车外网络安全技术要求主要对应第四章中的网络系统安全风险，聚焦车云通信、远程诊断、地图服务、日志回传和远程控制链路的身份认证、加密保护、完整性校验和异常会话控制。

（1）通信身份认证与信任机制：车端与云端设备必须建立基于数字证书或对称密钥体系的双向身份认证机制，防止非法接入与中间人伪造通信；所有通信设备如 T-BOX、DCU 必须具备唯一可信硬件 ID 并与数字证书绑定，实现设备身份一一对应；建立通信密钥的自动更新、吊销、备份与恢复机制，防止长期密钥失效或被滥用。

（2）通信加密与数据完整性保护：所有车云通信必须采用 TLS 1.3、IPSec、DTLS 等加密协议实现应用层或传输层的加密保护，保障数据在传输过程中的机密性。

（3）数据完整性校验：所有下发指令、上传数据、地图补丁、算法模型等内容均应附加 MAC 签名或数字签名，用于校验数据是否被篡改。

（4）支持国密算法体系：面向国产安全合规需求，可支持 SM2/SM3/SM4 等国密算法的加解密与认证。

（5）抗重放攻击与会话控制机制：在通信帧中嵌入时间戳与随机数，确保会话唯一性，防止历史消息被重发干扰系统逻辑；所有车云通信会话应通过会话 ID 或令牌进行动态绑定，防止固定凭据被

拦截复用。

（6）远程指令的合法性控制与执行验证：所有来自云端的控制指令如重启系统、升级固件、车辆控制指令等必须进行源签名验证与完整性检查；车端应返回指令执行状态、执行日志、错误码等，形成“指令—响应—日志—验证”闭环机制，防止伪指令生效；云端不同服务角色访问车辆不同控制接口应进行基于角色的访问控制，避免权限滥用。

（7）通信行为审计与异常检测：所有车云通信行为，包括认证事件、数据传输、异常断链、指令执行等应记录至本地或上传云端进行持久化存储，供事后审计使用；在边缘侧部署轻量级安全代理或网关，分析通信流量行为特征，识别重发、伪造、异常流量模式，触发安全策略响应；通信异常应联动车端状态机降级处理，例如“停止数据上传”、“断开远程控制通道”、“进入本地安全模式”等。

6.1.6. 车路协同安全技术要求

车路协同安全技术要求主要对应第四章中的无线电安全和协同链路风险，重点解决协同参与体可信接入、消息真实性验证、抗重放与抗伪造、链路抗干扰以及协同控制边界约束等问题。

（1）通信身份认证与接入控制：车辆、RSU、行人设备、信号机、云平台等通信参与体或国密体系实现身份认证，防止伪造节点参与通信；未经授权的终端设备不得接入协同通信系统。设备注册时应绑定硬件唯一标识并执行行为信誉初始化；路侧 RSU 与车端

V2X 模块启动时需经过可信引导链与证书拉取机制，确保证书、密钥链合法可追溯。

（2）数据保密性与完整性保护：建议在 V2X 通信链路部署对称加密与 MAC 认证或采用 TLS/IPsec 机制对数据进行传输加密与完整性校验；所有核心 V2X 消息需附加数字签名以确保其来源可验证、内容不可篡改；对于包含个人轨迹、身份标识等信息的消息，应进行脱敏处理或采用伪匿名机制保障隐私安全。

（3）抗重放与抗伪造机制：所有 V2X 消息应带有精确时间戳与序列号，结合 GNSS/5G 时钟同步机制防止历史消息重放攻击；设定车端/路侧消息广播频率阈值，对异常频率突增、仿冒消息激增等行为实时报警；利用雷达、摄像头、V2X 等多源融合手段比对识别广播消息与真实物理目标之间的不一致性，提升抗欺骗能力。

（4）通信链路安全与抗干扰保护：V2X 链路中应部署访问控制策略如黑名单过滤、VLAN 隔离、基于信任区域划分，防止跨域访问与非法广播；结合跳频通信、功率调节、冗余链路切换，如 DSRC 与 C-V2X 并存提升系统抗干扰能力；在边缘 RSU 或边缘计算平台部署策略控制器，对 V2X 信息流进行安全转发、QoS 控制与异常链路熔断。

（5）远程协同控制指令安全：路侧下发的信号控制、避障提示、动态路径等指令需通过权限验证与签名授权，防止指令伪造与越权行为；指令执行须回传状态响应与执行日志，形成“发出—验证—执

行—记录—响应”的闭环控制路径；对车端行为与协同指令预期进行对比分析，识别车辆拒绝指令、误解指令或不当响应等潜在风险。

6.1.7. 云端管理平台安全技术要求

云端管理平台安全技术要求主要对应第四章中的云端安全风险，重点是平台接入控制、数据与制品管理、接口安全、操作审计和批量风险抑制能力。

然而，云端平台因其数据集中、功能复合、接口开放，成为恶意攻击、数据窃取、指令伪造、算法污染等高风险目标。一旦平台安全遭受破坏，将导致大规模车辆服务中断、控制系统失控甚至引发社会性安全事故。因此，必须构建覆盖平台接入、数据安全、访问控制、算法安全、指令下发、系统管理与安全运维的系统化云端管理平台安全技术要求体系。主要安全技术要求如下：

（1）平台接入与身份认证：所有用户、设备、服务、API 访问必须接入基于角色的身份认证系统或零信任架构，支持多因子认证与动态权限分配；所有车端、RSU、边缘节点接入平台前，需完成设备身份注册、数字证书签发与可信认证过程；外部系统调用云端接口必须使用 Token + 时间戳 + 数字签名机制，每次会话具有访问粒度限制与生命周期管理。

（2）数据安全保护机制：各平台应按照自身业务，对数据进行分类分级，识别出如一般数据、敏感数据、重要数据和核心数据，建立数据保护等级策略，并配置对应的加密、访问与审计策略；所

有敏感数据、重要数据和核心数据在传输与存储过程中应采用 AES-256、SM4 等加密机制，支持硬件安全模块加速密钥管理；对用于展示、分析与共享的数据进行脱敏、泛化、模糊化处理，遵循“最小必要原则”传输与使用。

（3）访问控制与操作审计：云平台应对不同角色设定最小权限访问规则，明确可见、可改、可调接口边界；所有用户与系统进行必须记录日志，支持审计追溯；平台应集成安全信息与事件管理系统，分析异常访问模式、账户劫持、权限越权等行为并自动隔离处理。

6.1.8. OTA 安全技术要求

OTA 安全技术要求主要对应第四章中的固件安全、系统安全和云端发布链路风险，重点关注升级来源可信、升级包完整、版本一致、灰度控制、失败回退和模型更新后的运行验证。

（1）OTA 升级链路安全：所有 OTA 通信过程必须使用端到端加密通道，防止中间人攻击、流量监听与敏感信息泄露。建议采用 SM2/SM3/SM4 等国家密码算法体系支持国产密码安全合规；升级服务平台与车端控制器之间应实施双向身份认证，采用证书或基于硬件 ID，如 TPM/eUICC 的设备认证机制，防止非法平台或车辆参与 OTA 操作。

（2）OTA 升级包安全保护：升级包在生成后应采用数字签名机制，车端需在执行升级前进行签名验证与哈希校验，确保数据未

被篡改或篡改可检测；对含有敏感软件、算法模型、系统配置的升级包进行端到端加密传输与加密存储，避免被恶意分析、拦截或篡改；升级包需包含版本号、依赖关系与更新时间戳，车端应拒绝安装已知旧版本或降级风险版本，防止利用历史漏洞的回滚攻击。

（3）升级过程控制与验证：车端升级行为应受到权限控制与策略验证，如仅允许在停车状态、供电稳定、物理安全区域时进行升级。

（4）升级过程应通过多级授权机制（如平台授权与本地安全确认）限制高风险操作；支持 OTA 分批推送、灰度验证与“预发布+回收”机制，避免大规模同步更新导致系统性风险；对高等级安全相关模块升级应增加双重确认与链式验证机制。

（5）可恢复与异常处理机制：设备应支持断点续传、升级失败回退、紧急版本恢复等机制，确保异常中断不导致系统失控；支持冗余分区设计，可在升级失败时快速切换至稳定运行环境。

（6）算法模型与 AI 模块的 OTA 特殊保护要求：对 OTA 下发的算法模型需支持模型结构、参数校验、运行行为、白盒分析机制，防止模型被篡改或功能被劫持；算法更新后应启用运行行为监测与漂移检测机制，验证新模型未引入未知异常；建议 OTA 模型包附带模型可信度标签与性能预期描述，供车端评估是否匹配当前硬件与任务需求。

6.1.9. 业务逻辑安全技术要求

业务逻辑安全技术要求主要对应第四章中的业务逻辑安全风险，重点围绕 ODD 约束、模式转换、驾驶员监督、远程工作流权限、关键参数治理和异常处置规则建立可验证要求。

首先，ODD 约束与功能启用控制是业务逻辑安全设计的基础，应对智能驾驶功能的启用条件、持续运行条件与退出条件进行严格约束与一致性校验。系统应建立可形式化表达的 ODD 判定规则库，覆盖道路类型、车速区间、车道线质量、环境能见度、传感器健康状态、地图/定位可信度等关键要素，并在启用前实施“多源一致性检查+关键条件门控”；系统应具备对 ODD 边界抖动与条件退化应具备快速识别与稳健退出策略，确保在约束不满足时强制降级或退出，避免在不适用场景下维持自动控制。对功能启用还应设置反复启停抑制、异常频繁切换限制与事件审计，防止利用时序触发与边界条件组合实现策略性绕过。

其次，模式状态机完整性与控制权交接安全需得到全面保障。系统应采用明确的模式状态机设计，规定各状态的进入/退出条件、互锁关系与禁止跃迁路径，并对关键转换实施运行时校验与安全断言，防止异常路径导致的控制权错配或功能叠加失控。对于控制权交接过程，应定义“请求—确认—执行—验证”的闭环流程，确保接管/交还控制权具有可验证的触发依据、明确的责任转移点与可追溯的日志证据，并在异常状态下优先进入可预测的安全降级模式。

再者，人机交互与驾驶员监督业务规则是满足 L2/L2+“持续监督”前提的关键约束，应建立以安全优先的提示策略、告警策略与确认机制。系统应禁止将关键安全告警长期静默或被体验策略覆盖，接管请求应具备明确触发阈值、最小告警强度与多通道冗余提示要求，并对驾驶员可接管状态的判定引入多因子一致性校验，防止误判导致的“可接管假象”。同时应规定告警升级、超时处置与最小风险机动触发逻辑，确保在驾驶员未响应或不具备接管能力时系统能够稳定降级并保持可控行为边界。

此外，远程协同与工作流权限编排安全不容忽视。针对车云协同下的功能开关、策略参数、地图/道路信息、诊断与运维指令等远程下发能力，应建立“最小权限+场景约束+双重确认+不可抵赖审计”的业务控制模型，明确谁在何种场景下可对哪些对象执行哪些动作，并对高风险动作设置强制复核与分级授权。系统应对跨域协同信息建立冲突仲裁与一致性校验规则，明确协同数据与本车感知/规划的优先级与置信度管理机制，防止错误协同信息以“高可信”路径进入决策链路并被放大。

最后，策略参数与配置治理及异常处置闭环是业务逻辑安全可持续运行的保障。鉴于大量关键行为由阈值参数、策略表、灰度规则与区域/车型适配配置驱动，系统应对关键配置实施完整性保护、版本一致性校验、变更影响评估与可回滚治理，确保“变更可追溯、执行可验证、回退可恢复”，并避免配置漂移导致的跨批次行为差异

与责任不可追溯。在异常处置方面，应建立稳定的降级与恢复逻辑，规定触发阈值、持续时间、振荡抑制与恢复条件，防止攻击者通过制造输入不一致、依赖服务波动或质量抖动诱导频繁降级/退出，从而形成可用性攻击；同时应要求对关键业务逻辑事件形成证据链日志，为事故复盘、测评认证与监管抽测提供可核查依据。

通过上述业务逻辑安全要求的系统化构建，可将智能驾驶从“链路安全”扩展到“流程与语义安全”，在量产 L2/L2+持续部署与向 L3+演进过程中，形成可操作、可抽测、可认证、可追溯的业务逻辑防护能力，从而有效降低由流程绕过、状态机异常路径、越权编排与配置漂移引发的系统性安全风险。

6.2. 网络安全测试与评估

为支撑准入验证、研发测试和监管抽测，第六章提出的网络安全需求需进一步对应为测试与评估子体系。测试重点应与第四章风险分类保持一致，覆盖硬件、固件、系统、总线、无线电、网络通信、云端、传感器、算法和业务逻辑等对象。

6.2.1. 硬件安全测试子体系

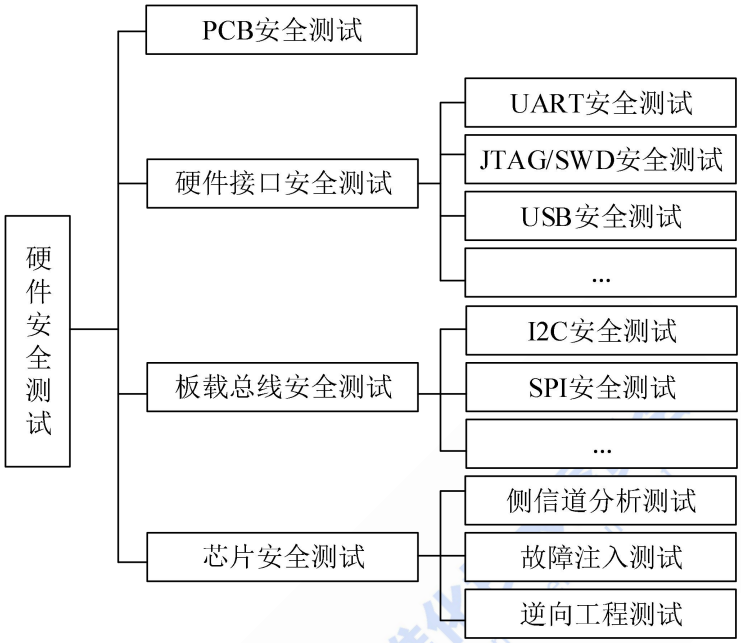

图 6-2 智能网联汽车硬件安全测试子体系

硬件安全测试子体系评估智能网联汽车电子设备硬件板卡的网络安全。如图 6-2 所示，硬件安全测试体系包括 PCB 安全测试、硬件接口安全测试、板载总线安全测试、芯片安全测试。PCB 安全测试评估电子设备 PCB 是否会泄露硬件接口、总线协议、芯片型号等重要信息，攻击者可基于上述信息了解被测系统的硬件构成，为后续攻击奠定基础。

硬件接口测试包括 UART、JTAG、SWD、USB 等协议接口测试，一方面测试人员需要评估硬件接口是否会泄露诸如系统启动日志、系统硬件信息、存储映射信息、系统固件等敏感信息及数据。另一方面，测试人员需要评估硬件接口是否会暴露系统命令行窗口，允许攻击者对被测系统进行调试以获取重要数据或执行恶意命令及程

序。

板载总线安全测试包括 I2C、SPI 等通信协议的安全测试。测试人员应当评估总线上传输数据的机密性、完整性。传输数据如果未加密，攻击者可获取总线传输内容，传输数据如果无完整性校验机制，攻击者可以任意篡改总线数据。

芯片安全测试包括侧信道分析测试、故障注入测试、逆向工程测试。攻击者通过上述测试评估被测系统的关键芯片是否可以抵御功耗分析、电磁分析、时序分析等侧信道攻击；是否具备防止电压故障注入、电磁故障注入、光学故障注入等故障注入攻击的安全机制；是否具备防护逆向拆解的物理防护机制。

6.2.2. 固件安全测试子体系

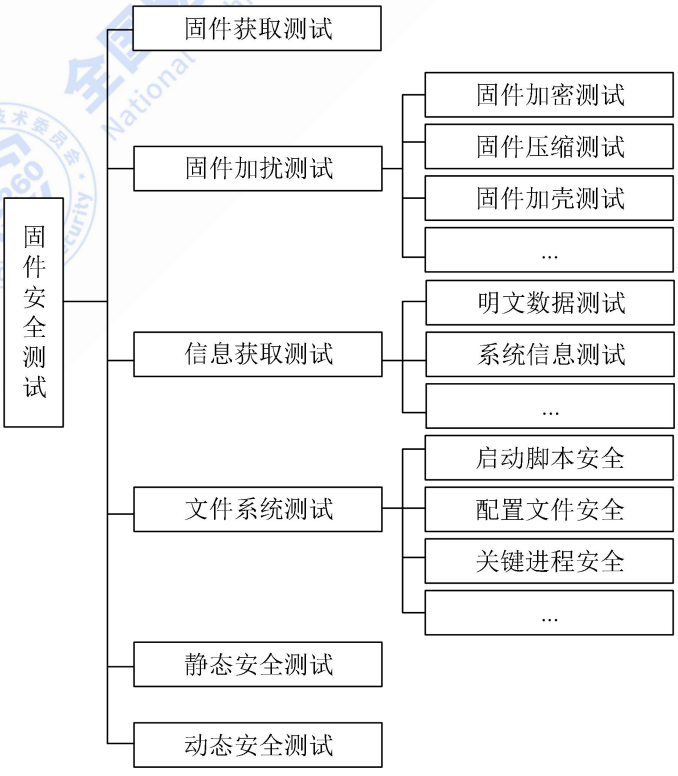

图 6-3 智能网联汽车固件安全测试子体系

固件安全测试子体系评估智能网联汽车 ECU 固件的网络安全风险。如图 6-3 所示，固件安全测试体系包含固件获取测试、固件加扰测试、信息获取测试、文件系统测试、静态安全测试、动态安全测试。固件获取测试评估固件存储的安全性，是否泄露给攻击者。固件获取测试要求测试人员从公共网络、空中下载技术、固件更新应用程序、JTAG、SWD、UART、I2C 和 SPI 等方式尝试获取系统固件。如果测试人员可通过上述方式提取出固件，则固件存在信息泄露的安全风险。

为了增加攻击者逆向分析固件的难度，安全人员通常会对固件进行加扰保护，方式包括固件加密、固件压缩、固件加壳。固件加扰测试需要安全测试人员评估被测系统的固件是否具备此类安全防护机制。通过分析固件的熵值分布可判断固件是否具有加密或者压缩的保护机制。通过逆向分析工具简要分析固件的反汇编代码可判断固件是否存在保护壳。

固件及其中的明文字符串可能泄露具有潜在攻击利用价值的敏感数据。开发人员在编译与链接固件的过程中可能采用格式化的固件组织方式，在发布固件时并未去掉固件中特定格式的文件头以及符号表等关键信息，可泄露被测系统 CPU 架构、固件存储空间分布等关键信息。缺乏安全意识的开发人员可能认证口令、服务器 IP 地址、用户名等敏感数据以明文字符串的方式硬编码在固件中，造成严重的信息泄露事故。

对于存在系统的固件，需要进行文件系统测试。文件系统测试需要测试人员对被测系统固件中的文件系统进行分析，查看其中是否存在关键的启动脚本、配置文件等。相应的文件可泄露系统启动流程、自动开启的进程及服务、系统的配置策略等信息，为后续攻击奠定基础。攻击者甚至可能篡改相应的文件以更改系统启动运行流程以及关键配置。

静态测试中，测试人员将目标固件导入到 IDA Pro 等固件逆向分析工具对固件进行逆向分析。借助工具，测试人员可获得固件中函数的调用逻辑，进而定位到加解密、安全认证等关键函数或者攻击者感兴趣的目标函数。动态分析则需要测试人员利用 QEMU 等仿真工具在仿真环境中运行目标固件，对目标固件进行包括模糊测试在内的动态测试。

6.2.3. 系统安全测试子体系

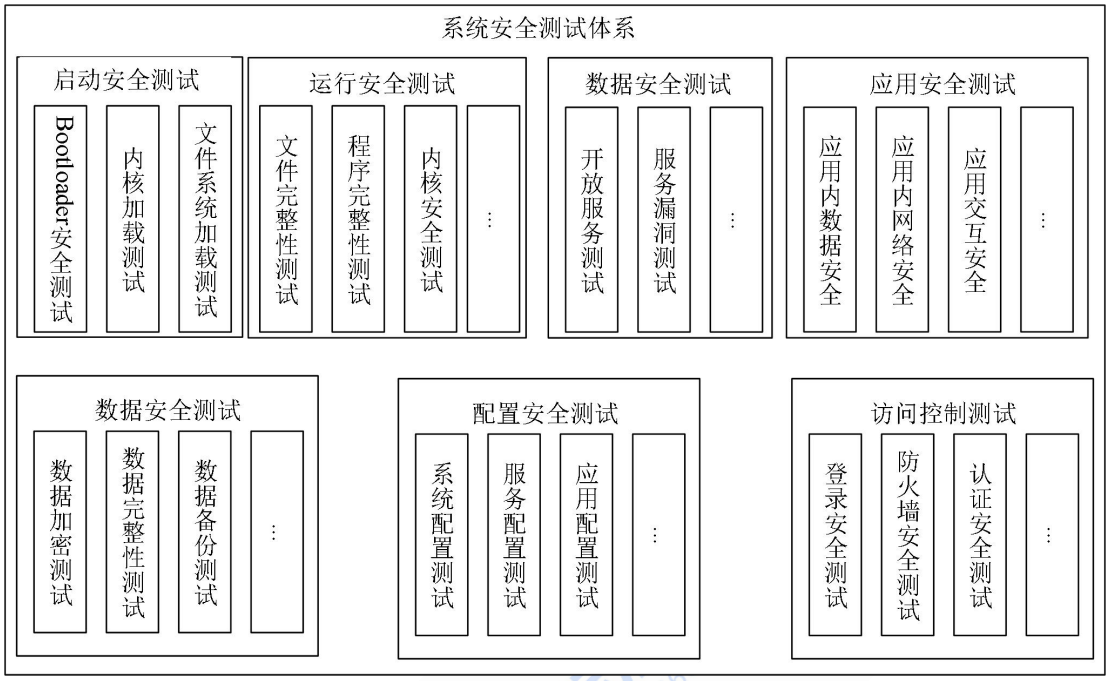

图 6-4 智能网联汽车系统安全测试子体系

系统安全测试子体系评估被测系统操作系统面临的网络安全风险。基于传统互联网领域的网络安全测试经验，本文提出的系统测试体系包括如图 6-4 所示的启动安全测试、运行安全测试、服务安全测试、应用安全测试、数据安全测试、配置安全测试以及访问控制测试。启动安全测试评估系统的启动过程，测试其 Bootloader、内核镜像、文件系统镜像在启动过程中是否存在被替换或恶意篡改的安全风险。运行安全测试用于评估运行过程中是否对关键文件及代码进行了有效的安全度量，防止系统加载了被恶意篡改或替换过的文件及代码，造成信息泄露或权限提升风险。应用安全测试则从数据、网络、服务交互等维度对系统内的应用程序进行安全评估。数据安全测试评估数据在生命周期中是否被安全存储与备份，攻击

者是否可以篡改与解析数据内容。配置安全测试评估安全人员对系统进行了基本的安全配置，如是否关闭了不必要的服务与端口等。访问控制测试从系统登陆、身份认证、防火墙等维度对关键服务及通信的访问控制机制进行评估。

6.2.4. 总线安全测试子体系

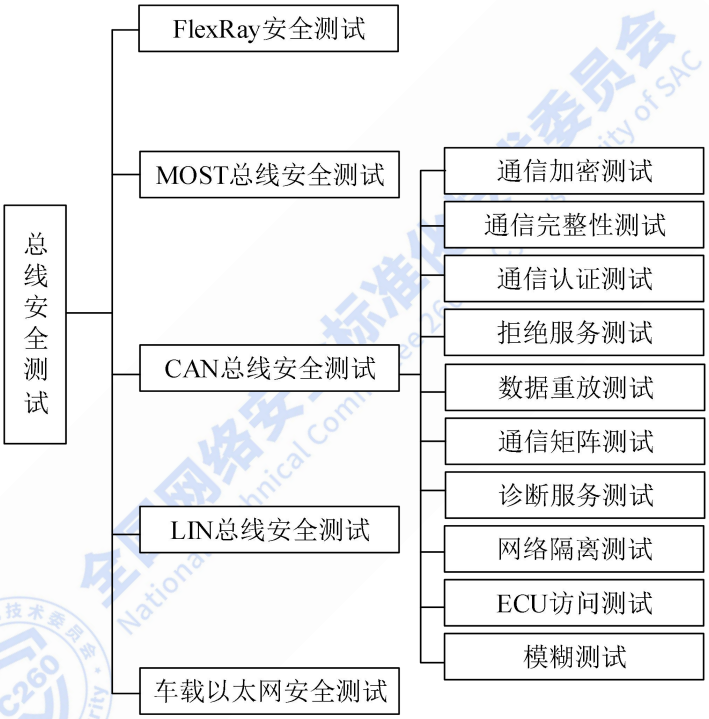

图 6-5 智能网联汽车总线安全测试体系

总线安全测试子体系评估智能网联汽车车载总线网络的安全性。如图 6-5 所示，尽管车载总线网络包含多种总线协议，本文基于车载总线通信的特点提出了覆盖当前车载总线协议的安全测试体系，包含加密测试、完整性校验测试、通信认证测试、拒绝服务测试、重放测试、通信矩阵测试、诊断服务测试、网络隔离测试、ECU 访问测试与模糊测试。

加密测试、完整性校验测试、认证测试、重放测试与拒绝服务测试是总线协议的基本测试项目，用于评估总线协议是否具备保护数据机密性、完整性、可用性、新鲜性、防欺骗性等机制，保证所传输数据的基本安全。此外，汽车制造商在总线数据帧的数据段会采用通信矩阵作为厂商私有协议描述车辆控制指令，通信矩阵测试评估攻击者是否可以轻易获取控制指令内容；网络隔离测试评估安全设计人员是否有效隔离车载网络中的不同总线网络；诊断服务测试评估攻击者获取并利用诊断指令查看、篡改车辆诊断数据的难易程度；ECU 访问测试评估攻击者通过总线网络访问并控制 ECU 节点的难易程度；模糊测试评估总线通信是否存在未知的可利用漏洞。

6.2.5. 无线电安全测试子体系

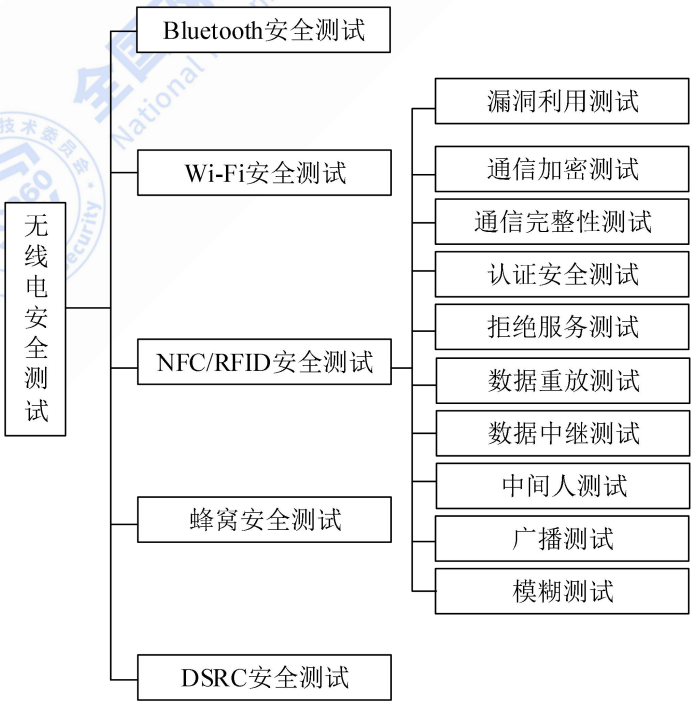

图 6-6 智能网联汽车无线电安全测试体系

无线电测试子体系评估智能网联汽车无线通信系统安全风险。智能网联汽车无线通信协议主要包含 Bluetooth、Wi-Fi、NFC/RFID、蜂窝通信协议以及 DSRC，不同的通信协议采用不同的无线频段传输数据。无线通信协议安全评估遵循如图 6-6 所示的测试体系，包括漏洞利用测试、加密测试、完整性测试、认证测试、数据重放测试、数据中继测试、拒绝服务测试、中间人攻击测试、广播测试与模糊测试。

漏洞利用测试旨在评估被测试系统相关无线通信协议是否存在已知的可利用漏洞，测试人员需要关注相关协议的漏洞披露情况，研究已知的网络安全漏洞并开发漏洞验证测试程序；加密测试、完整性测试、认证测试、重放测试与拒绝服务测试评估被测系统无线电通信协议是否具备保护传输数据机密性、完整性、可用性、防止欺骗性、新鲜性的安全机制；中继测试评估被测系统是否可以抵御无线电通信中继攻击；中间人攻击评估被测系统是否采取了严格的双向认证机制，防止攻击者介入无线通信流程，窃取及篡改通信数据；广播测试评估相关协议的广播机制是否可被用于设备发现等，造成信息泄露。模糊测试用于发现无线电协议的未知恶意漏洞。

6.2.6. 网络安全测试子体系

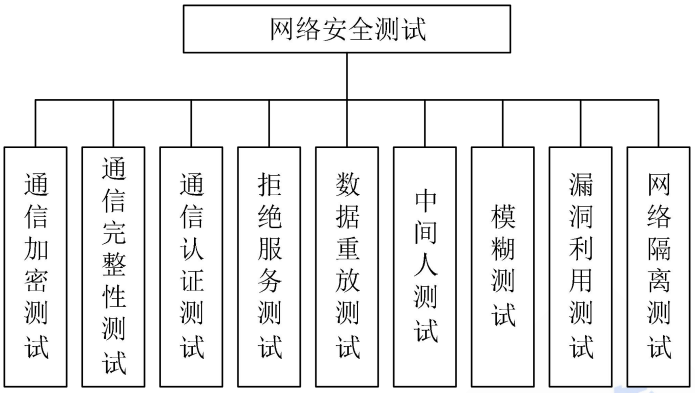

图 6-7 智能网联汽车网络安全测试体系

网络安全测试子体系与无线电通信测试体系有所不同，无线电通信测试体系关注于无线通信协议及其实现的网络安全风险测试，偏重于物理层及链路层，网络安全测试体系则关注在不同物理链路上数据传输安全，偏重于网络层、传输层及应用层。基于传统的网络安全测试经验，如图 6-7 所示的网络安全测试体系包含加密测试、完整性测试、通信认证测试、重放测试、拒绝服务测试、中间人测试、模糊测试、漏洞利用测试、网络隔离测试。网络安全测试体系的测试方法与无线电测试体系相近，只是侧重的通信数据在开放系统互连（Open System Interconnect，OSI）模型中所处的层次不同，在此不再赘述。

6.2.7. 云端安全测试子体系

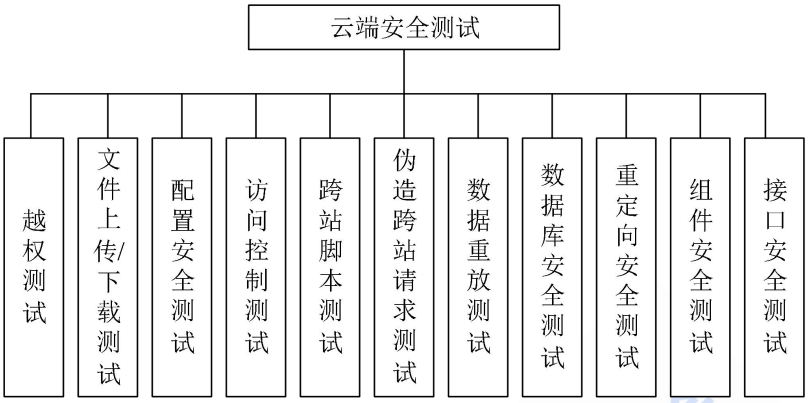

图 6-8 智能网联汽车云端安全测试体系

云端测试子体系评估智能网联汽车云端服务平台网络安全风险。如图 6-8 所示，基于传统互联网领域 Web 安全测试经验，云端测试体系包含越权测试、配置测试等诸多测试项目。越权测试评估 Web 应用程序的权限管理是否正确合理，符合真实的业务需求；文件上传与下载测试评估 Web 应用程序是否正确处理文件格式、大小等，防止恶意代码通过文件上传到云端。；配置安全测试评估安全人员是否安全配置 Web 服务器；访问控制测试评估 Web 服务器是否具备合理的访问控制策略；跨站脚本攻击测试、跨站请求伪造攻击测试、重定向安全测试等测试项评估目标 Web 服务器是否存在相应类型的网络安全漏洞；数据库安全测试评估数据库是否存在数据注入等网络安全风险；数据重放测试评估 Web 应用程序是否可以抵御重放攻击；组件安全与接口安全评估 Web 应用程序采用的接口与组件是否存在网络安全风险。

6.2.8. 传感器安全测试子体系

传感器安全测试子体系评估智能网联汽车传感器的网络安全风险。基于现有攻击方式，本文将传感器分为两类，携带基带数据的传感器及未携带基带数据的传感器。前者包括胎压监测系统、汽车防盗系统、导航定位系统等传感器系统，攻击者通常利用软件无线电工具通过解调、解码等方式监听并精确篡改或伪造此类系统中传输的数据达到欺骗接收系统的目的。后者包括超声传感器、摄像头、激光雷达、毫米波雷达等传感器系统，一般用于测距、环境扫描等场合，攻击者并未精确控制传感器数据，仅仅产生相似的传感器信号以欺骗或者干扰传感器信号接收系统。

如图 6-9 所示，携带基带数据的传感器面临数据明文传输、无完整性校验机制、缺乏认证机制、缺乏消息新鲜性管理机制等基本数据传输风险。此外，本文传感器测试体系还从拒绝服务、信号干扰两个维度评估目标传感器系统的健壮性。未携带基带数据的传感器则可从信号干扰、信号伪造、传感器失效、拒绝服务、信号处理算法安全性等维度进行网络安全评估。

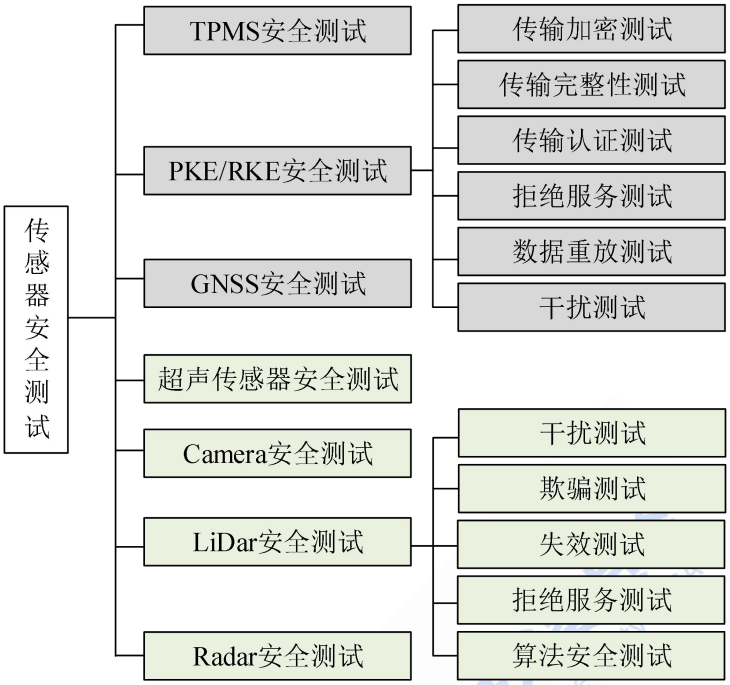

图 6-9 智能网联汽车传感器安全测试体系

6.2.9. 算法安全测试子体系

智能驾驶算法作为智能驾驶的核心决策引擎，其运行过程直接决定车辆的环境感知、路径规划、行为预测与控制执行。由于此类算法普遍依赖深度学习等复杂非线性模型，呈现出“黑箱性强、可解释性差、对抗性脆弱”的特征，因此传统软件安全测试方法难以直接适用，亟需构建专门面向算法本体的安全测试方法体系，以评估其鲁棒性、可靠性、可控性与抗攻击能力。

当前主流的智能驾驶算法安全测试方法主要围绕算法的输入空间敏感性、模型行为一致性、对抗样本脆弱性、模型更新稳定性等关键维度开展。输入空间测试主要通过在感知图像、点云数据、车辆状态等输入上施加微扰或遮挡，评估算法在不同干扰强度与环境

变化下的鲁棒性，并构建退化曲线模型以识别其失效边界；行为一致性测试聚焦于算法面对相似输入时输出稳定性的验证，利用场景构造与模型推理轨迹比较技术，评估模型在行为预测、路径选择等方面的时序稳定性与决策一致性。

针对深度学习模型常见的对抗样本攻击问题，引入对抗测试框架，如基于 FGSM（Fast Gradient Sign Method）、PGD（Projected Gradient Descent）等攻击方法，自动生成扰动样本并评估模型在面对精确攻击时的误判率与响应模式。这类测试有助于识别模型在输入空间中特定“脆弱区域”，指导模型改进与防御机制嵌入。同时，为了提升算法部署的可信性与安全性，测试方法还包括算法版本回滚测试、模型漂移检测与行为偏移评估，通过对比更新前后模型输出差异，识别潜在的安全退化问题。

近年来，随着可解释性技术的发展，基于可视化与特征贡献分析的“白盒测试”方法也逐步被引入智能驾驶算法安全测试体系中，如通过 Grad-CAM、SHAP、LIME 等工具分析模型关注区域与决策路径是否与人类认知逻辑一致，用于检测模型是否受到伪特征驱动或过拟合噪声的影响。

总体而言，智能驾驶算法安全测试方法正逐步形成集黑盒对抗性测试、白盒行为分析、模型一致性评估、部署验证模拟于一体的综合体系。该体系不仅有助于揭示深层次算法安全脆弱性，还能为智能驾驶安全认证、算法更新监管与法规合规提供可量化的技术基

础，成为推动算法可信性标准化与产业应用可持续发展的重要支撑。

6.2.10. 业务逻辑安全检测子体系

业务逻辑安全检测子体系面向智能驾驶“功能启用—模式管理—人机交互—接管降级—远程协同—配置变更—异常处置”的业务流程与状态机层，旨在建立可量化、可复现、可抽测的测试与验证方法体系，以识别并抑制攻击者在不突破传统加密与鉴权边界的情况下，通过操纵业务规则、时序条件与工作流路径触发“形式合法但语义恶意”的不安全行为。由于量产 L1–L2/L2+功能高度依赖多条件门控、复杂状态机与跨域协同编排，其风险暴露往往不体现为单点漏洞，而表现为 ODD 约束不严、状态跃迁异常、告警与接管规则被静默、远程下发缺乏场景约束、配置漂移导致行为偏差以及降级/恢复策略不稳定等逻辑缺陷，传统仅以接口扫描或单元测试为主的方法难以覆盖上述“流程与语义”层面的安全问题，因此亟需构建专门的业务逻辑安全检测体系，以评估系统的可控性、稳定性、抗绕用能力与可追溯性。

当前主流的业务逻辑安全检测方法主要围绕业务规则边界覆盖、状态机完整性验证、时序与组合条件对抗测试、权限与工作流越权验证、配置一致性与变更影响评估、以及异常处置与韧性验证等关键维度开展：其一，ODD 与启用门控检测通过边界值分析、条件抖动注入与多源不一致构造，系统性验证启用/持续/退出规则是否存在可绕过路径，并量化退出延迟与降级触发阈值对风险累积的影响；

其二，模式状态机检测采用状态覆盖与禁止跃迁检查，结合运行时断言与互锁条件核验，识别异常跃迁、功能叠加失控与控制权交接错配，并在关键转换链路上验证“请求—确认—执行—验证”的闭环是否成立；其三，HMI/DMS 逻辑检测通过告警抑制、降噪策略、确认机制与驾驶员可接管判定的对抗性用例生成，评估接管请求触发的充分性、告警升级的可靠性与误判边界，防止关键安全提示被体验策略覆盖；其四，远程协同与工作流检测围绕云端下发的功能开关、策略参数、地图/道路信息与运维指令，开展最小权限、场景约束、双人复核与不可抵赖审计的有效性验证，并通过流程绕过与权限链穿透测试识别越权编排风险；其五，配置与策略治理检测针对阈值表、策略表与灰度规则实施完整性校验、版本一致性巡检与变更影响评估，通过更新前后行为差异对比与回滚测试识别潜在安全退化；其六，异常处置与韧性检测通过依赖服务波动、输入质量退化与冲突信息注入等扰动实验，评估降级/恢复策略的稳定性、振荡抑制能力与最小风险机动（MRM）触发可靠性，并验证关键事件日志与证据链的完备性。

总体而言，业务逻辑安全检测子体系正逐步形成集“规则建模与覆盖验证、状态机与时序对抗测试、工作流越权校验、配置一致性治理、异常处置韧性评估、证据链审计”于一体的综合框架，使智能驾驶的安全验证从组件与链路层延伸至流程与语义层，为量产准入、第三方测评认证与监管抽测提供可量化的技术依据，并支撑智能驾

驶在高频迭代与跨域协同条件下实现可持续的安全运行与可信演进。

7. 数据安全需求分析

智能驾驶数据安全需求并非一般汽车数据安全要求的简单延伸，而是与感知采集、车云协同、远程运营和算法迭代深度耦合。数据一方面关系个人信息、重要数据和商业秘密保护，另一方面又直接影响模型训练、地图服务、远程控制和事故追溯，因此需要围绕智能驾驶特有场景开展专门分析。

结合第四章的数据安全风险，本章重点关注五类与智能驾驶直接相关的数据对象：车外感知数据、座舱与车机个人信息、运营服务数据、云平台集中处理数据以及供应链和多主体流转数据。

其中，车外感知数据和座舱数据分别对应公开空间采集和车内个人信息处理两类高敏感场景；运营服务、云平台和供应链数据则对应智能驾驶规模化部署后最容易形成系统性风险的三类场景。

因此，数据安全标准化的重点不是重复通用原则，而是明确不同对象的数据边界、处理条件、对外提供规则、技术控制要求和评估验证方法。

7.1. 数据安全技术要求

7.1.1. 智能驾驶汽车运营服务数据安全要求

智能驾驶运营服务涉及车辆运行、用户服务、远程协助、日志回传、调度控制和事件复盘等活动，其数据安全要求应覆盖车端、

云端和运营平台协同处理场景。标准应明确运营服务中的数据分类分级、最小必要采集、访问控制、指令留痕、事件追溯和跨主体责任边界。

与一般互联网出行服务不同，智能驾驶运营服务中的数据既具有个人信息属性，也可能直接影响车辆运行状态和公共安全，因此需要将数据安全要求与远程控制安全、事件报告要求和运营治理要求结合考虑。

现有通用标准可提供底线要求，但对远程接管、批量调度、运行日志闭环、车端与云端证据一致性等关键场景覆盖不足，亟需形成面向智能驾驶运营服务的专门要求。

后续标准化可重点围绕运营数据对象界定、控制指令与日志一致性、分角色权限控制、敏感数据共享边界和事件留证机制展开。

7.1.2. 智能驾驶车外画面匿名化处理安全技术要求

车外画面匿名化处理是智能驾驶合规采集和对外提供车外数据的基础要求。该问题与智能驾驶直接相关，因为车外视频图像既是感知训练和验证的重要数据来源，也最容易包含人脸、车牌等个人信息。

标准应明确匿名化处理适用场景、处理时点、处理对象、效果判定和不可逆要求，并区分研发测试、运营服务、事故取证和对外共享等不同数据流转场景。

匿名化处理应以不影响合法必要用途为前提，对可识别个人或

车辆身份的信息进行不可逆处理，处理后数据不应再具备恢复原始身份信息的能力。

标准还应明确处理过程数据、原始缓存数据和导出数据的留存条件与删除要求，避免只对结果数据提出要求而忽视中间过程泄露风险。

对于智能驾驶场景，更应将匿名化效果验证与典型道路场景、光照条件、天气条件和多目标密集场景结合起来，形成可测试的评价方法。

因此，车外画面匿名化处理并不是一般隐私合规附属要求，而是智能驾驶车外数据安全体系中的基础能力之一。

7.1.3. 智能驾驶车外数据停止收集安全技术要求

车外数据停止收集要求主要适用于特定敏感区域、特定任务状态或特定运营场景下的采集边界控制。该要求的重点不是简单追求“全部关闭”，而是在不破坏行车安全的前提下，明确何种场景需要限制采集、由谁触发、如何提示、如何验证以及如何恢复。

因此，本节应聚焦与智能驾驶直接相关的车外摄像头、激光雷达等高敏感采集装置，以及与特定区域数据保护和合规控制有关的状态管理要求，而不扩展到一般车载电子功能。

（1）基本要求

行车安全要求：触发停止收集功能前，系统应显著提示对智能驾驶功能的影响，并结合车速、运行状态和场景条件设置启用约束，

防止因误用导致必要安全能力被错误关闭。

信息安全要求：停止收集状态及其控制指令应具备身份认证、完整性保护和审计留痕能力，防止被恶意远程触发、绕过或篡改。

（2）技术实现要求

开关与状态设计：应设置明确的触发方式和状态标识，保证驾驶人可感知、可确认、可恢复，并能与依赖相关传感器的智能驾驶功能保持联动。

传感器控制要求：进入停止收集状态后，应对相关采集链路实施可验证的关闭或限制措施，并同步向车内提示其对自动泊车、车道保持、环境感知等功能的影响。

状态解除要求：解除停止收集状态应有明确的确认流程，并记录触发时间、触发主体、恢复时间和恢复方式，形成可追溯证据。

状态标识要求：系统应通过车内明显提示和必要的外部提示方式表明车辆处于受限采集状态，避免外部主体和车内驾驶人对当前能力产生误判。

总体而言，该要求服务于特定敏感区域和特定运营场景下的合规控制，是智能驾驶车外数据边界治理的重要补充。

7.1.4. 智能驾驶座舱数据处理安全技术要求

座舱数据处理要求应聚焦与智能驾驶直接相关的车内摄像头、麦克风、生物识别和交互日志等数据对象，重点解决默认收集、超范围使用、跨场景复用和车内外流转边界不清等问题。

现有标准已提出车内处理和默认不收集原则，但对智能驾驶座舱与驾驶辅助、远程服务、驾驶员监测等功能耦合场景下的数据对象界定、留存期限、关闭路径和例外条件，仍需要更细化的规则。

座舱数据安全技术要求应至少覆盖以下方面:

默认设置方面，除法律法规另有规定或用户主动开启外，车内摄像头、麦克风及其他高敏感采集能力应处于默认关闭或最小化采集状态。

对外提供方面，应坚持车内处理优先原则；确需向车外提供的，应明确用途、范围、留存期限和接收对象，并采取加密传输、访问控制和留痕审计措施。

用户控制方面，应提供便捷、明确且不误导的关闭、撤回和删除路径，并确保账户切换、访客模式和恢复出厂设置场景下的权限状态可被正确重置。

因此，座舱数据安全标准的重点不在于重复一般个人信息保护原则，而在于明确智能驾驶场景下车内数据与驾驶功能、运营服务和远程应用之间的边界。

后续可围绕数据对象分类、默认状态、例外条件、提示交互、留存控制和验证方法进一步细化专项标准。

7.1.5. 智能驾驶车机个人信息保护技术要求

车机应用个人信息保护要求应聚焦与智能驾驶直接耦合的应用场景，如导航、远程控车、辅助驾驶配置、用户账户和售后服务等，

而不宜泛化为一般移动应用规范的简单复述。

其核心问题在于：车机应用既是个人信息处理入口，也是部分智能驾驶功能的配置入口和服务入口，一旦存在超范围收集、越权共享或权限管理不当，影响的不仅是隐私，还可能波及车辆服务安全。

因此，后续标准应在通用个人信息保护规则基础上，进一步明确车机应用的最小必要收集边界、敏感权限单独同意、账号与车辆绑定关系、第三方应用接入控制和与驾驶相关功能的权限隔离要求。

（1）基本要求

车端应用在处理个人信息时，应满足国家个人信息保护基本要求，并结合智能驾驶场景对采集必要性、权限边界和账户控制提出更细化规则。

告知同意应与具体功能场景对应，避免通过用户协议、购车合同或默认开启方式替代显著、可理解的前台提示。

保存地点和期限应与业务必要性相匹配，避免长期、模糊或超范围保存。

用户权利接口应便于查阅、复制、删除、撤回授权和关闭功能，并能与车辆账户、访客账户和手机 App 侧权限保持一致。

（2）敏感个人信息处理要求

处理敏感个人信息时，应按照具体功能逐项取得单独同意，不得通过一次性总授权覆盖多项处理活动。

对同意期限、使用目的和第三方共享范围应设置明确边界，不应以提升体验、训练模型等宽泛表述替代具体说明。

（3）个人信息采集安全技术要求

首次启动或首次使用相关功能时，应通过显著方式展示个人信息保护政策和必要提示。

收集敏感个人信息时，应采用单独弹窗或等效方式取得明确授权。

收集范围应限定于实现对应功能所必需的最小范围，不得将与智能驾驶无直接关系的数据作为默认采集项。

总体看，车机应用个人信息保护需要从通用 App 治理进一步延伸到“车机—车辆—云端”协同场景下的专门规则。

7.1.6. 智能驾驶云平台数据安全技术要求

智能驾驶云平台数据安全要求应围绕车辆运行数据、感知数据、日志数据、地图和模型制品、远程控制指令等关键对象展开，重点解决集中存储、跨域流转、批量下发和多角色访问带来的高影响风险。

（1）基本要求

平台应建立与智能驾驶业务相匹配的数据分类分级、最小权限访问、加密存储与传输、接口鉴权、审计留痕和异常处置机制。

对境内存储、对外提供、跨主体共享和模型训练使用等活动，应分别明确审批条件、责任主体和技术控制要求。

（2）账号管理

应对运维、算法、地图、调度、客服、测试和第三方接入等不同角色实施差异化账号管理和权限隔离，避免单一高权限账号覆盖多类敏感操作。

（3）数据流控制

应对车端、云端、边缘节点、第三方平台和外部接口之间的数据流建立可视、可控、可审计的流转规则，防止敏感数据越权共享和失控外发。

跨安全域流转时，应结合数据类别、接收主体、处理目的和留存要求实施校验和阻断策略。

对于兼具训练、运营、运维和监管接口的平台，还应建立环境隔离与数据隔离机制，防止不同用途数据混用。

因此，智能驾驶云平台标准应区别于通用云安全要求，重点补充远程控制、模型发布、地图更新、车队运营和批量风险抑制等场景。

7.1.7. 智能驾驶汽车企业供应链数据安全技术要求

智能驾驶供应链数据安全技术要求应针对整车企业、零部件供应商、算法服务商、云服务商、运营方和第三方应用之间的数据合作场景，重点解决数据边界不清、责任分工不明、接口控制不足和审计证据缺失等问题。

标准化的关键在于将数据合作中的所有权、使用权、管理责任、

共享条件、留存要求和违规责任转化为可执行、可审计的规则，而不是停留在原则性表述。

整车企业应牵头建立供应链数据准入和协同管理要求，将数据分类分级、接口最小化、加密保护、脱敏处理和安全审计纳入合作边界。

对于多主体协同场景，应特别强调日志留存、责任追溯、违规共享发现和退出机制，确保数据安全责任能够真正落地。

因此，供应链数据安全已不是一般商务合作管理问题，而是智能驾驶规模化部署中的基础安全能力之一。

7.2. 数据安全评估与测试

7.2.1. 智能驾驶车外匿名化处理效果评估测试

目前，针对车外画面匿名化处理的算法工具已日趋成熟。包括用于敏感区域检测定位算法和在定位敏感区域后实施完整色块涂抹等局部轮廓化处理的方式。行业内已形成成熟的一站式匿名化处理工具与解决方案，多集成于智能驾驶的车端模块中，确保数据处理在车端完成以保障安全。然而，对于车外画面进行匿名化处理的效果参差不齐，部分工具存在检出率过低问题，从而造成较大的个人信息泄漏风险。

车外画面匿名化处理效果评估与测试，主要针对智能网联汽车在数据采集、处理与传输过程中，对车外画面中所含人脸、车牌等

敏感信息进行局部轮廓化处理效果的验证。旨在确保车辆在向车外传输车外视频图像时，把直接或间接识别自然人身份、车辆身份的信息完全删除或局部轮廓化处理，保障个人信息权益。

依据 TC260-PG-20241A《网络安全标准实践指南——车外画面局部轮廓化处理效果验证指引》，车外画面局部轮廓化处理效果测试需先完成验证准备，由验证方提供功能正常的实车并开放相关接口与权限、明确数据传输相关信息，配合导出待验证样本及提供加密数据解密支持。随后将车辆置于多种典型道路场景，在局部轮廓化处理功能启动状态下开展涵盖不同光照条件的行驶与驻车测试，随车监测并抓取数据形成多组待验证样本。接着将样本导入实验室环境，采用 4 种符合要求的算法与人工抽检相结合的方式验证效果，确保处理后的人脸无法识别、车牌核心信息不可见且无相关信息残留；最后统计两类检测的未通过比例，依据预设标准判定验证通过、未通过或未完成。

7.2.2. 智能驾驶车外数据停止收集安全评估测试

通过研究车外摄像头、激光雷达在数据采集、车内网络传输的流程、方式和特点，提出可实施性强的车外传感器数据收集状态的检测验证方法，确保智能网联汽车关闭车外摄像头、激光雷达装置的行为实现车外数据停止收集，从源头上停止车外数据收集和泄露行为。

车外数据停止收集安全评估测试技术方法主要包含功能性测试

和安全性测试。功能性测试旨在验证摄像头和激光雷达是否处于关闭状态，以及依赖摄像头激光类的智能驾驶功能是否可用。安全性测试主要围绕该停止收集功能是否能抵御网络安全攻击。

（1）功能性测试

➢车外传感设备功能可用性测试

验证一键停止功能开启后，依赖车外摄像头、激光雷达的相关功能是否被禁用。在触发一键停止收集车外数据功能，确认系统进入停止收集状态，依次尝试启动依赖车外摄像头、激光雷达的功能，如自动泊车、车道保持、360 度全景影像等，记录各功能的响应状态及车机提示信息，车机是否弹出明确提示，告知当前处于停止收集车外数据状态，相关功能暂不可用。

➢摄像头关闭状态安全性测试

验证一键停止功能开启后，车外摄像头是否均处于断电状态。触发一键停止功能后，使用设备状态检测仪连接车辆相关检测接口，分别检测车外摄像头的供电状态，持续监测 5 分钟，记录各摄像头供电状态是否稳定。

➢激光雷达关闭状态测试

验证一键停止功能开启后，激光雷达是否处于待机状态，无激光器发光及点云数据输出。在触发一键停止功能后，通过设备状态检测仪检测激光雷达的工作模式，观察激光器发光情况；通过车辆数据接口读取激光雷达数据输出状态，并验证是否有点云数据生成。

（2）安全性测试

➢车辆外围无线接口安全评估

验证车辆外围是否存在可直接访问交互的无线接口，防范无线方式非法接入风险。使用无线接口扫描设备，对车辆外围进行全范围扫描，排查可用无线接口，对扫描发现的无线接口，尝试建立连接并发起访问车辆内部系统的请求，记录扫描结果及连接、访问响应情况。

➢车辆外围有线接口安全评估

验证车辆外围有线接口的接入防护能力，确保未授权接入无法访问内部系统。排查车辆外围可见的有线接口后，使用测试设备直接接入各接口，尝试访问车辆内部系统，使用内部授权账号登录车辆相关管理系统后，再次通过外围有线接口接入测试设备，尝试访问内部系统核心数据；记录两次接入测试的响应结果。

➢车辆外围接口漏洞测试

验证车辆外围接口是否存在可利用提权的高危或严重漏洞。采用渗透测试工具集，对车辆外围所有可识别接口进行全面漏洞扫描。重点检测是否存在权限提升、远程代码执行等可利用的高危或严重漏洞，对发现的漏洞进行验证，评估是否存在实际攻击风险。

（3）车辆内部渗透测试

➢关键代码安全性验证

验证一键停止功能处理流程相关代码的安全性，是否存在开放

外部接口及可利用风险。调取一键停止功能处理流程的相关代码文件，进行代码审计，重点检查代码是否开放外部可调用接口，是否存在逻辑漏洞、权限校验缺失等可被利用的风险点；模拟外部调用尝试，验证代码防护效果。

➢激发信号控制安全性验证

验证一键停止功能激发控制信号的状态验证机制有效性，防范非授权调用。通过专业检测设备监测一键停止功能激发控制信号的传输过程；记录状态验证参数的发送频率，确认是否符合设计要求；模拟非授权控制信号，尝试调用一键停止功能，记录功能响应结果。

7.2.3. 智能驾驶座舱数据处理安全评估测试

目前座舱数据处理原则包括默认不收集和车内处理。默认不收集是指车辆在出厂前应设定为默认不收集座舱数据的状态，数据车内处理是指除 GB/T 41871 中 6.2 所示特例以外，座舱数据应在车内处理，不向车外提供。

座舱数据默认不收集测试主要围绕车机功能查看开展验证，通过将车机恢复初始账号后查看座舱数据的收集权限是否为默认关闭。数据不出车测试主要通过数据抓包技术，查看是否有异常流量传输。相关评估测试方法如下:

（1）总体测试方法

座舱数据不出车的检测方法：在车端进行车辆对外通信数据的抓取和分析。

座舱数据默认不收集的检测方法：在车内进行各项座舱数据收集功能的符合性确认。

（2）座舱数据不出车合规性测试

➢ 传感器数据默认不出车测试

测试各类传感器采集的座舱数据在向车外提供前是否已取得个人信息主体同意。针对摄像头、红外传感器、指纹传感器、传声器，分别设计触发其数据采集的功能场景，如人脸识别、手势控制、指纹解锁、语音助手等，在每一种权限条件下，都将执行相应的功能操作，并在操作过程中同步抓取车辆所有的对外通信网络数据包。随后，将对捕获的数据包进行深度分析，通过识别数据特征码、解析数据格式及检查目标地址等方式，判断其中是否包含对应传感器的原始数据或经过加工处理的衍生数据。此流程旨在通过技术手段实证检验数据外传行为是否严格遵循用户的权限设置。

➢ 远程服务数据提供安全验证

验证为远程查看、云存储等功能向使用者提供数据时，是否满足同意、访问控制及安全措施要求。

首先模拟用户真实操作流程，通过车机系统或配套手机应用程序，在明确知情同意的前提下，授权开启远程查看或云存储功能。功能开启后，随即执行一次具体的远程数据请求，例如通过手机App发起查看车内实时影像的指令，或访问云端已存储的行车视频记录。

在此交互过程中，利用网络抓包工具对车辆与云端服务器之间的所有双向通信数据进行完整捕获。获取通信数据后，将从两个层面进行深度分析：一是检查通信协议，分析传输链路是否采用了有效的加密措施，以评估数据在传输过程中的机密性与完整性是否得到保障；二是模拟安全威胁，尝试使用未经授权的第三方账号或通过技术手段模拟攻击请求，访问同一数据接口，以验证系统的访问控制机制是否能有效识别并拒绝非法的数据访问企图。

（3）座舱数据默认不收集

模拟用户购入新车或执行系统重置操作，观察车辆启动后的首个交互界面。合规的系统应在此时向用户呈现完整的隐私政策与数据收集授权选项，且所有选项均应默认为“关闭”或“拒绝”状态。用户必须进行主动、逐一选择后才能开始收集数据。

在确认默认状态后，评估测试权限控制机制，例如，当用户在设置中明确关闭“位置信息”权限后，导航应用不应再获取到车辆的真实、实时地理位置；关闭麦克风权限应使所有语音交互功能立即失效。

考虑到车辆可能由不同用户驾驶，评估将设计账户切换测试。在主要用户授权某些权限后，当其退出登录切换至“访客模式”时，系统应将所有数据收集权限重置为默认关闭状态，同时，访客自行开启的权限不应影响主用户的既有设置，从而实现权限的完全隔离与独立管理。

对于用户终止数据收集的便利性，评估将查验车辆提供的控制方式。系统应提供至少一种直接、快捷的终止途径，例如用于麦克风的实体物理开关、屏幕上的快捷控制中心按钮或明确的语音指令。一旦用户执行关闭操作，系统应给予即时、明确的反馈，表明数据收集已停止。

最后，针对敏感个人信息的处理，当功能需要收集人脸、声纹或持续地理位置等信息时，系统应弹出独立、专门的授权弹窗进行告知，不应将多项敏感信息捆绑在一起获取同意。在同意期限的设置上，应提供如“本次行程”“七天”“一年”等具体选择，不应出现“始终允许”或“永久”等选项。

7.2.4. 智能驾驶车机应用个人信息保护评估测试

为应对智能座舱应用生态中第三方车端应用 App，包括预装与上架应用等带来的复杂个人信息保护挑战，保障车端应用在处理用户数据遵循“车内处理、默认不收集、知情同意”的核心原则，评估测试方法如下：

（1）隐私政策自动化与深度评估

首先通过自动化解析工具检查车载应用的隐私政策和个人信息保护相关内容是否符合相关法规标准要求，然后再由人工进行一致性风险研判。

利用自动化工具对 App 隐私政策进行结构化解析，检查其是否完整包含法规要求的必备要素，如：处理的个人信息种类、每种信

息收集的具体场景与必要性说明、个人信息保存地点与期限、用户停止收集与删除信息的途径、用户权益事务联系人等。

人工分析隐私政策文本的清晰度、无歧义性，并初步研判其声明范围与 App 功能可能存在的逻辑矛盾。

（2）应用行为深度分析与验证

应用行为分析可通过静态权限与代码分析或动态行为沙箱测试开展。

静态权限与代码分析：解析 App 安装包，评估其声明的系统权限是否与功能必要性强关联，检测代码中是否集成了未声明的第三方 SDK 或存在可疑的数据收集 API 调用。

动态行为沙箱测试：在隔离的测试环境或模拟座舱中运行 App，监控其在各种交互场景下的实际行为。使用网络流量抓包、系统调用 Hook 等技术，捕获其实际收集的数据字段、频率、传输目的地，并与隐私政策声明进行比对，验证是否存在超范围收集、静默收集或向未声明的第三方传输数据的行为。

（3）最小收集原则验证

验证车端应用仅收集实现核心功能所必需的最小范围个人信息与车外数据，是否有超范围收集行为，且未将非必要数据收集作为功能使用前提等。

默认不收集验证：首次安装启动后，验证所有非基础服务所必需的个人信息收集功能是否均处于默认关闭状态。

授权同意流程测试：测试 App 是否在首次使用相关功能时，弹出清晰、独立的授权弹窗，并获得用户的明示同意。验证全局隐私设置中心是否有效，用户能否随时管理各项权限。

（4）第三方应用个人信息处理合规性专项检测

对车端应用集成的第三方应用收集、使用、传输、存储个人信息的全流程进行专项核查，验证其是否符合相关法规要求，是否遵循最小必要原则、履行告知同意义务且保障用户权益。

合同与协议审查：评估车企/平台方与 App 开发商签署的《数据安全协议》。验证协议是否明确约定了双方数据保护责任、禁止超范围处理、用户权益响应机制、数据删除义务、是否允许向境外提供、对分包商的约束等，并核对附件中约定的传输字段列表与实际检测发现是否一致。

7.2.5. 智能驾驶云平台数据安全评估测试

依据 GB/T 34942—2025《网络安全技术 云计算服务安全能力评估方法》，智能驾驶云平台数据安全测试核心围绕三大板块展开，形成覆盖技术、管理、合规的全维度评估体系。一是数据全生命周期安全能力测试，聚焦智能驾驶场景下海量感知数据、车控数据等的安全管控，核查数据传输环节的链路加密与完整性保障效果，验证存储阶段的加密防护、访问权限管控及备份恢复能力，同时评估数据处理、删除等环节的安全合规性，确保数据全流程不泄露、不篡改。二是系统与技术架构安全测试，重点验证云平台网络边界防

护，如防火墙、入侵检测系统的有效性，虚拟环境隔离安全性，以及智能驾驶相关 API 接口的安全防护能力；同时核查身份认证与权限管理体系，包括多因素认证、最小权限落实等是否符合标准要求，筑牢技术安全底座。三是安全管理与合规性测试，评估云平台安全管理体系的完整性，包括配置管理、维护管理、应急响应机制，如数据泄露处置、灾备演练等的有效性；验证安全审计日志的完整性与可追溯性，确保智能驾驶数据分类分级管理、个人信息保护等符合相关法规要求，同时核查云服务商安全资质及供应链安全责任界定的落实情况。具体测试方法如下：

一是数据全生命周期安全能力测试。数据传输环节，通过抓包分析、模拟攻击等方式，验证智能驾驶感知数据、车控数据等传输时是否采用符合标准的加密协议，核查数据传输过程中的完整性校验机制是否有效，防止数据被篡改或窃听；数据存储环节，检查云平台是否对不同等级的智能驾驶数据实施分类加密存储，通过权限测试验证不同角色对存储数据的访问控制效果，同时开展备份恢复测试，模拟数据丢失场景验证备份数据的可用性、完整性及恢复时效性；在数据处理与删除环节，通过审计日志核查数据处理流程的合规性，采用技术检测手段验证数据删除后是否存在残留，确保符合不可恢复要求。

二是系统与技术架构安全测试。网络边界防护测试方面，采用端口扫描、渗透测试等方式，验证云平台防火墙、入侵检测/防御系

统对外部攻击的拦截效果，核查网络访问控制策略是否精准适配智能驾驶数据传输需求；虚拟环境隔离测试，通过跨虚拟机攻击模拟、资源隔离检测等手段，验证不同租户、不同业务模块的虚拟环境是否有效隔离，防止数据交叉泄露；API 接口安全测试，针对智能驾驶相关 API 接口，开展未授权访问、接口滥用、参数篡改等测试，验证接口的身份认证、权限校验及输入输出过滤机制；身份认证与权限管理测试，核查多因素认证机制的落地效果，通过模拟超权操作、权限变更流程测试，验证最小权限原则的落实情况及权限管理的规范性。

三是安全管理与合规性测试。安全管理体系测试，通过查阅制度文件、访谈相关人员、现场核查等方式，评估云平台配置管理、维护管理、人员安全管理等制度的完整性与执行效果；应急响应测试，采用桌面推演、实战演练等方式，验证数据泄露、系统瘫痪等突发场景下应急处置流程的合理性与有效性，核查灾备方案的可行性；安全审计测试，检查审计日志对智能驾驶数据全流程操作的记录完整性，验证日志的不可篡改特性及追溯能力；合规性验证，对照相关法规及标准要求，核查数据分类分级管理、个人信息保护等措施的落实情况，通过查阅资质文件、合同条款等，验证云服务商安全资质及供应链安全责任界定的合规性。

7.2.6. 智能驾驶汽车企业供应链数据安全评估测试

针对智能驾驶汽车数据合作权责不明确这一核心安全痛点，评

估需围绕权责条款有效性、权责履行一致性两大重点展开，确保权责划分落地到数据全生命周期管理中。

（1）权责条款规范性审查

该环节聚焦合作协议与制度文件，评估权责划分的明确性与合规性，是评估的基础前提。首先需梳理供应链各合作主体的权责文本，包括整车厂与供应商、第三方服务商签订的合作合同、数据安全协议、保密协议等，核查文本中是否清晰界定数据所有权、使用权、管理权的归属，是否明确各主体在数据采集、传输、存储、共享、处理、销毁全流程的具体义务，例如供应商的数据采集权限边界、整车厂的数据监管责任、第三方服务商的数据脱敏义务等。

其次要对照相关法律法规要求，审查权责条款是否覆盖数据分类分级、敏感数据特殊保护、跨境数据传输审批、数据泄露应急处置等合规要求，是否明确数据泄露、违规共享等场景下的责任归属与追责机制，防范“权责模糊”“责任推诿”的条款漏洞。同时需核验权责条款的可操作性，避免出现“原则性要求多、具体措施少”的问题，例如明确数据传输加密的技术标准、数据存储的权限管控要求、数据销毁的流程规范等，确保权责条款能直接指导实际操作。

（2）权责履行一致性核验

该环节通过对“文本要求”和“实际操作”的比对分析，评估权责条款的落地执行情况，是评估的核心环节。一方面需开展流程穿透式核查，选取供应链典型数据流转场景，跟踪数据全生命周期流转

路径，核验各主体是否严格按照权责条款履行义务。例如核查供应商是否存在越权采集数据的行为、数据传输是否采用协议约定的加密方式、第三方服务商是否落实数据脱敏要求等，同时调取数据操作日志、访问记录、审计报告等凭证，验证权责履行的真实性。

另一方面需开展主体能力匹配度评估，针对中小供应商、第三方服务商等安全能力薄弱的主体，核查其是否具备履行权责条款的技术条件与管理能力，例如是否配备数据安全防护设备、是否建立数据安全管理制度、是否开展员工数据安全培训等，评估权责条款与主体能力的适配性，避免出现“权责要求过高、主体无力履行”的悬空问题。此外，还需通过访谈与问卷调研，收集供应链各主体的反馈意见，了解权责条款在执行过程中存在的痛点与障碍，为后续优化提供依据。

8. 标准体系框架设计

8.1. 设计原则

标准体系设计应遵循四项原则：一是聚焦智能驾驶特有风险，不与通用汽车网络和数据安全标准简单重复；二是坚持对象清晰、场景清晰和证据清晰，确保标准可实施、可测试、可抽查；三是与现有法律法规和通用标准有效衔接，在其基础上补充智能驾驶专项要求；四是兼顾当前量产辅助驾驶与后续更高等级自动驾驶需求，形成可演进的体系结构。

据此，标准体系不宜按传统信息系统方式做泛化铺陈，而应围绕智能驾驶在车端、通信链路、云端平台、运营服务和算法模型方面新增的风险对象进行分类布局。

8.2. 总体框架

结合第五章标准分析和第六、七章需求分析，本文构建的标准体系并非替代现有整车信息安全、软件升级和汽车数据处理标准，而是在现有制度底座上，补齐智能驾驶特有风险的标准空白。体系重点覆盖术语与对象界定、专项技术要求、测试评估方法、运营治理要求和持续改进机制。

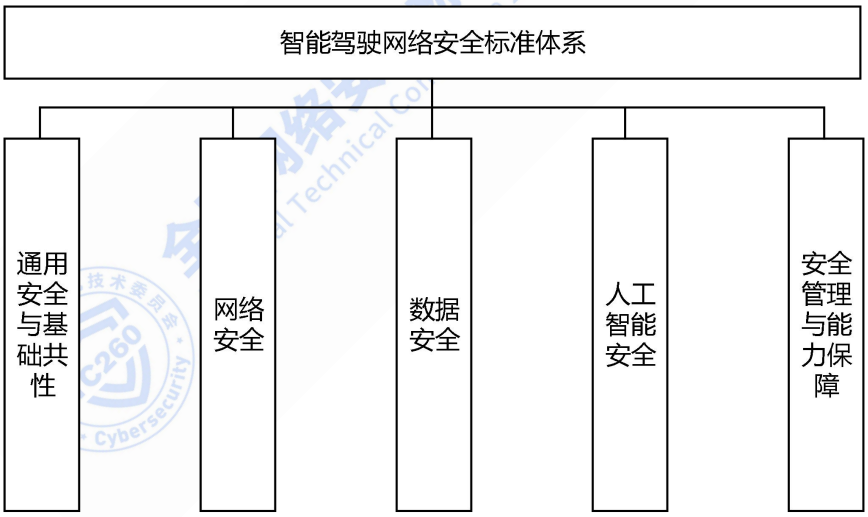

图 8-1 智能驾驶网络安全标准体系

因此，本体系划分为“通用安全与基础共性、网络安全、数据安全、人工智能安全、安全管理与能力保障”五个子类，如图 8-1 所示。其中，通用类负责边界定义和统一框架，其余四类分别承接智能驾驶新增的技术和治理需求。

8.3. 标准构成

8.3.1. 通用安全与基础共性标准

通用安全与基础共性标准用于解决智能驾驶标准化中的共性问题，包括术语定义、对象分类、系统架构、风险分析方法、证据链要求和跨域协同基本框架。

与现有通用汽车信息安全标准相比，该类标准的增量价值不在于重复整车基本要求，而在于为环境感知、车路协同、云平台、算法模型和运营服务等对象建立统一的抽象与接口，避免后续专项标准对象不一致、口径不统一。

如表 8-1 所示，现有通用基础标准已覆盖信息安全工程方法、整车通用要求、软件升级与部分供应链安全能力，但对智能驾驶特有的跨域协同框架和对象边界仍缺乏专门支撑，因此需要新增或细化相关基础标准。

表 8-1 通用安全与基础共性标准

序号	标准名称	性质	进展
1	汽车信息安全通用技术要求	GB/T	发布
2	汽车整车信息安全技术要求	GB	发布
3	汽车软件升级通用技术要求	GB	发布
4	道路车辆 信息安全工程	GB/T	发布
5	道路车辆 信息安全工程审核指南	GB/Z	下达计划
6	道路车辆 网络安全验证和确认	GB/T	启动立项
7	道路车辆 网络安全保障等级和目标攻击可行性	GB/T	预研阶段
8	智能网联汽车 供应链网络安全技术规范	GB/T	预研阶段

8.3.2. 网络安全标准

网络安全标准用于承接第四章和第六章识别出的车端、通信链路和云端平台风险，重点覆盖环境感知链路、车内网络、车端系统、车云通信、车路协同、云平台、OTA 和业务逻辑控制等对象。

与现有汽车网络安全标准相比，本类标准的重点不是重复通用整车安全管理要求，而是补充智能驾驶特有的对象和场景要求，特别是感知链可信、协同消息可信、远程控制边界、模型与参数发布链保护以及运行逻辑一致性控制。

基础支撑方向应包括硬件可信、固件可信、关键接口保护和发布链保护等内容，为车端系统安全奠定基础。

车端系统与组件方向应覆盖车内总线、车载以太网、操作系统、中间件、传感器接口和关键执行链路安全。

网络与通信方向应覆盖车云通信、无线接入、协同消息认证、抗重放与抗干扰、时间同步保护和会话控制。

远程服务与运维方向应重点覆盖 OTA、远程诊断、地图和模型更新、批量下发和失败回退。

多主体协同方向应重点覆盖车路协同、边缘节点、运营平台和多角色权限边界。

总体上，本类标准应形成从车端可信、链路可信到云端可信、流程可信的完整网络安全框架。

如表 8-2 所示，现有和在研标准已覆盖部分车内网络、云平台

和 OTA 要求，但对智能驾驶环境感知安全、车路协同安全和业务逻辑安全仍明显不足。

表 8-2 网络安全标准

序号	标准名称	性质	进展
1	电动汽车远程服务与管理系统信息安全技术要求及试验方法	GB/T	发布
2	车载信息交互系统信息安全技术要求及试验方法	GB/T	发布
3	汽车网关信息安全技术要求及试验方法	GB/T	发布
4	电动汽车充电系统信息安全技术要求及试验方法	GB/T	发布
5	汽车信息安全应急响应管理规范	GB/T	发布
6	汽车诊断接口信息安全技术要求及试验方法	GB/T	发布
7	基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求	GB/T	发布
8	道路车辆 软件升级工程	GB/T	下达计划
9	汽车软件识别码	GB/T	申请立项
10	汽车网络安全入侵检测技术要求及实验方法	GB/T	完成立项
11	汽车安全漏洞分类分级评价	GB/T	征求意见
12	汽车密码应用技术要求	GB	起草中
13	汽车数字证书应用规范	GB/T	申请立项
14	车路协同系统智能路侧协同控制设备技术要求和测试方法	GB/T	发布

后续应优先补齐智能驾驶专项对象和场景化测试方法，使网络安全标准能够直接支撑准入抽测和运营监管。

8.3.3. 数据安全标准

数据安全标准用于承接第四章和第七章识别出的车外感知数据、座舱与车机个人信息、运营服务数据、云平台集中处理数据以及供应链流转数据风险。

与现有汽车数据处理和个人信息保护标准相比，本类标准的核心增量在于：面向智能驾驶车外感知和运营场景细化数据对象边界；面向车云协同和远程服务明确对外提供条件；面向多主体流转建立

责任和审计要求。

本类标准可进一步细分为车外感知数据安全、座舱与车机个人信息保护、运营服务数据安全、云平台数据安全和供应链数据安全等方向。

通用要求应明确数据对象分类、采集必要性、留存期限、删除规则和对外提供条件。

分类分级要求应结合智能驾驶时空连续、多模态采集和批量运营特点，细化重要数据识别方法。

对跨境和对外提供场景，应建立与智能驾驶业务匹配的评估要点和控制要求。

个人信息保护方向应突出车外画面匿名化、座舱默认不收集、敏感信息单独同意和账户权限一致性。

应用与运营数据方向应覆盖远程控车、运营平台、车机应用和第三方服务接入场景。

如表 8-3 所示，现有标准已覆盖部分汽车数据通用要求和个人信息保护内容，但对运营服务数据、车路云一体化场景的数据边界以及多主体协同流转要求仍缺少细化标准。

表 8-3 数据安全标准

序号	标准名称	性质	进展
1	工业互联网数据安全保护要求	YD/T	发布
2	电信网和互联网数据安全通用要求	YD/T	发布
3	车联网信息服务 用户个人信息保护要求	YD/T	发布
4	车联网信息服务数据安全技术要求	YD/T	发布
5	信息安全技术 个人信息安全规范	GB/T	发布
6	信息安全技术 个人信息去标识化指南	GB/T	发布

序号	标准名称	性质	进展
7	信息安全技术 个人信息安全影响评估指南	GB/T	发布
8	信息安全技术　汽车数据处理安全要求	GB/T	发布
9	智能网联汽车 自动驾驶数据记录系统	GB	发布
10	智能网联汽车数据通用要求	GB/T	发布
11	信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求	GB/T	发布
12	数据安全技术敏感个人信息处理安全要求	GB/T	发布
13	信息安全技术重要数据处理安全要求	GB/T	征求意见
14	信息安全技术基于个人信息的自动化决策安全要求	GB/T	发布
15	数据安全技术 个人信息跨境处理活动安全认证要求	GB/T	发布
16	信息安全技术数据安全风险评估方法	GB/T	征求意见
17	数据安全技术 数据分类分级规则	GB/T	发布
18	数据安全技术 个人信息保护合规审计要求	GB/T	征求意见
19	智能网联汽车时空数据传感系统安全基本要求	GB	发布
20	信息安全技术 网络数据处理安全要求	GB/T	发布
21	车联网信息服务 数据安全保护能力评估规范	YD/T	发布

因此，数据安全标准体系需要从“通用合规要求”进一步深化到“智能驾驶专项对象和场景要求”。

8.3.4. 人工智能安全标准

人工智能安全标准用于承接感知模型、预测模型、决策模型和相关数据闭环风险。其目标不是泛化讨论 AI 伦理，而是解决智能驾驶模型在开放道路环境中的鲁棒性、可验证性、可追溯性和运行中可控性问题。

从内容上看，应覆盖训练数据治理、模型构建与评测、部署保护、运行监测、异常处置和 OTA 更新控制等环节，并与车端系统安全、数据安全和运营治理要求衔接。

与现有通用人工智能安全标准相比，智能驾驶场景更强调物理

世界攻击、时延约束、失效降级、跨模态一致性验证以及模型变更对整车行为的影响评估。

当前已有标准多集中于通用 AI 风险管理、数据标注和服务安全，对智能驾驶场景仍存在以下不足:

一是行业特异性不足，难以直接映射到感知、融合、预测、决策和控制链路。

二是缺乏面向物理世界攻击、长尾场景和极端工况的鲁棒性测试规范。

三是模型在线监测、异常处置和回退机制尚未形成统一要求。

四是评测基线、指标体系和数据集要求不统一，难以支撑跨车型、跨供应链的一致比较。

五是第三方模型、算子和工具链的供应链安全控制不足。

因此，人工智能安全标准应以车载场景为牵引，形成从数据、模型到运行和更新的专项要求，如表 8-4 所示。

表 8-4 人工智能安全标准

序号	标准名称	性质	进展
1	信息安全技术生成式人工智能预训练和优化训练数据安全规范	GB/T	发布
2	信息安全技术生成式人工智能人工标注安全规范	GB/T	发布
3	信息安全技术生成式人工智能服务安全基本要求	GB/T	发布
4	生成式人工智能技术应用社会影响 服务提供者合规管理指南	GB/T	发布
5	生成式人工智能技术应用社会影响 评估指南	GB/T	发布
6	网络安全技术 人工智能计算平台安全框架	GB/T	发布
7	人工智能 风险管理能力评估	GB/T	发布
8	网络安全技术 人工智能生成合成内容标识方法	GB/T	发布
9	车用人工智能技术应用指南	——	计划
10	车用人工智能平台架构指南	——	计划

序号	标准名称	性质	进展
11	人工智能 隐私计算通用框架	——	计划

8.3.5. 安全管理与能力保障

安全管理与能力保障标准用于承接组织治理、研发安全、运营安全、供应链管理、事件响应和合规审计等要求，是前述技术标准能够真正落地实施的保障层。

与现有管理类标准相比，如表 8-5 所示，智能驾驶管理标准需要更强调车端、云端、路侧和运营组织之间的协同责任，以及模型、地图、远程控制和数据流转等新型对象的治理要求。

研发安全管理应把威胁分析、对象识别、测试验证、模型变更评估和发布审查嵌入研发流程。

运营安全管理应覆盖日志采集、异常检测、漏洞修复、配置管理、批量风险控制和事件处置闭环。

供应链安全管理应覆盖硬件、软件、模型、数据和云服务等多类外部资源，建立准入、审计、退出和通报机制。

合规审计与持续改进应强调证据链、量化指标和第三方评估能力，使标准从原则要求转化为可验证要求。

现有管理类标准已经提供基本框架，但在智能驾驶场景下仍存在顶层衔接不足、工程化细则不足、模型治理覆盖不足和运营闭环不足等问题。

因此，安全管理与能力保障类标准应作为后续体系建设的重要

组成部分，与专项技术标准同步推进。

表 8-5 安全管理与能力保障标准

序号	标准名称	性质	进展
1	工业和信息化领域数据安全事件应急预案	通知	发布
2	关于进一步加强智能网联汽车准入、召回及软件在线 升级管理的通知（征求意见稿）	通知	发布
3	工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见	通知	发布
4	汽车企业数据安全管理体系要求	团标	发布
5	汽车安全漏洞分类分级评价	GB/T	征求意见
6	道路车辆 信息安全工程	GB/T	发布
7	汽车数据安全管理若干规定	通知	发布

9. 标准体系规划建议

标准规划应紧扣第五章识别出的制度空白和第六、七章提炼的需求，遵循“先补短板、后促协同；先建可测要求、后扩展评价体系”的思路。规划目标不是简单增加标准数量，而是形成与现有标准体系分工清晰、与智能驾驶专项需求对应明确的项目布局。

9.1. 通用安全与基础共性标准

优先建议补充智能驾驶对象界定、系统架构、风险分析方法和证据链要求等基础标准。与现有通用汽车信息安全标准相比，该类项目主要解决智能驾驶专项标准之间对象和口径不一致的问题，为后续专项标准提供统一框架。

表 9-1 通用安全与基础共性标准

序号	标准名称	制修订建议	标准定位
1	网络安全技术 智能驾驶系统安全框架	制定	围绕智能网联汽车智能驾驶系统在感知、决策与执行控制中面临的网络安全威胁，构建可指导行业主体实施安

序号	标准名称	制修订建议	标准定位
			全防护的系统化安全框架。

9.2. 网络安全标准

网络安全方向建议优先布局与现有体系差异最明显、且最直接影响准入和运营安全的项目，包括智能驾驶环境感知安全要求、车路协同安全要求、业务逻辑安全要求、智能驾驶网络安全测试方法和风险评估方法等，如表 9-2 所示。上述项目将补齐现有标准对感知链、协同链和运行逻辑关注不足的问题。

表 9-2 网络安全标准

序号	标准名称	制修订建议	标准定位
1	智能驾驶系统网络安全测试技术要求	制定	指导开展智能驾驶系统网络安全测试
2	智能驾驶系统网络安全风险评估方法	制定	指导智能驾驶汽车网络安全风险评估活动，标准化风险评估流程

9.3. 数据安全标准

数据安全方向建议围绕智能驾驶运营服务数据安全、车外感知数据处理与匿名化、特定场景下车外数据采集边界控制、智能驾驶云平台数据安全以及供应链数据安全协同要求等内容开展规划，如表 9-3 所示。与现有汽车数据标准相比，这些项目更强调智能驾驶专项对象、远程服务场景和多主体流转规则。

表 9-3 数据安全标准

序号	标准名称	制修订建议	标准定位
1	智能网联汽车数据跨境评估指南	制定	指导汽车在数据出海前，开展评估工作，识别潜在的安全风险。
2	车路云一体化数据可信交互技术要求	制定	定义车路云一体化场景下，数据可信交互的基本要求，约束各业务场景下的数据传输和共享的处理活动，明确身份认证、完整性校验、可信计算与隐私保护等技术要求，支撑智能网联交通的数据安全与可信运行。
3	自动驾驶汽车服务座舱隐私保护要求	制定	编制自动驾驶汽车服务座舱隐私保护要求，明确自动驾驶车辆在示范运营过程中对车内和车辆运营企业的数据安全要求。
4	车路云一体化 数据分类分级指南	制定	指导车路云一体化场景下，多场景数据分类分级，标准化车路云场景下的数据分类分级方法，为数据共享提供理论基础。
5	车端应用个人信息保护安全要求	制定	针对车机端场景特殊性与数据风险差异化，明确个人信息全生命周期合规边界、强化敏感信息分级保护与用户授权知情权保障的专项标准，是衔接通用个人信息保护规范与智能网联汽车产业需求。
6	智能驾驶服务云平台数据安全要求	制定	针对智能驾驶服务云平台特有的数据安全风险提出安全要求和方法措施。
7	智能驾驶供应链数据安全要求	制定	针对智能驾驶的数据流通、使用等数据合作情况，识别相应的安全风险和防范措施。

9.4. 人工智能安全标准

人工智能安全方向建议围绕车载感知与决策模型鲁棒性测试、模型部署与更新安全、模型运行监测与异常处置、第三方模型供应链安全等方向布局，如表 9-3 所示。其与现有通用 AI 标准的区别在于，聚焦车载场景、物理世界攻击和整车行为影响评估。

表 9-4 人工智能安全标准

序号	标准名称	制修订建议	标准定位
1	车用人工智能鲁棒性与对抗安全测试方法	制定	旨在建立统一的 AI 安全测试框架，规范物理与数字对抗样本生成、扰动注入、传感器欺骗与环境干扰试验方法，明确测试场景、分级指标与通过判定标准，实现 AI 模型抗攻击能力的可验证性。
2	车用人工智能在线监测与异常处置规范	制定	制定智能驾驶 AI 系统的在线安全运行标准，定义模型漂移监测、输入异常检测、预测偏差识别的技术方法与响应策略，构建“检测—隔离—回滚—恢复”的闭环防御机制。
3	车用人工智能模型与参数保护技术要求	制定	规范模型资产在部署与运行阶段的安全防护，要求参数加密、签名验证、密钥管理、访问审计和反窃取机制，确保 AI 模型的保密性与完整性，防止恶意替换与逆向攻击。
4	车用人工智能开发安全与 OTA 安全管理规范	制定	针对 AI 模型的全生命周期更新与维护，规范安全 CI/CD 流水线设计、模型版本控制、变更风险评估（SIA for AI）与灰度发布策略，确保模型更新过程的安全可控与可追溯。
5	车用人工智能安全评估与合规认证体系	制定	建立可量化的 AI 安全评估基线与分级认证体系，涵盖鲁棒性、可解释性、隐私保护、社会影响与伦理约束等维度，支撑监管部门与企业的第三方合规评估与对标

9.5. 安全管理与能力保障

安全管理与能力保障方向建议围绕智能驾驶研发安全管理、运营安全管理、供应链安全管理、事件报告与通报、能力成熟度评估等项目推进，如表 9-5 所示。其与现有管理类标准的区别在于，更强调车端—云端—运营平台协同和模型、地图、远程控制等新型对

象治理。

表 9-5 安全管理与能力保障标准

序号	标准名称	制修订建议	标准定位
1	自动驾驶汽车运营服务安全要求	制定	本标准拟明确自动驾驶汽车运营服务的主要风险以及相应的安全管理要求。适用于自动驾驶汽车运营服务提供者安全开展运营服务，规范网络安全水平和数据处理活动。
2	智能驾驶安全能力成熟度模型	制定	构建面向组织、流程、技术、度量、改进的成熟度分级与评估量表，作为准入与年度复评辅助依据。
3	智能驾驶软件物料清单管理规范	制定	统一 SBOM、Model-SBOM 字段（组件、算子、训练语料、编译链、已知缺陷）、签名与通报机制，明确准入审核、变更复评与召回联动要求。

附录 A 相关政策法规清单（国际/国内）

表一 智能驾驶网络安全相关政策法规

序号	名称	时间	性质	地区
1	中华人民共和国网络安全法	2017	法律	中国
2	中华人民共和国数据安全法	2021	法律	中国
3	中华人民共和国个人信息保护法	2021	法律	中国
4	汽车数据安全管理若干规定（试行）	2022	指导文件	中国
5	关于加强智能网联汽车生产企业及产品准入管理的意见	2023	指导文件	中国
6	UN Regulation No. 155 - Cyber security and cyber security management system	2020	法规	UNECE
7	UN Regulation No. 156 - Software update and software update management system	2021	法规	UNECE
8	General Data Protection Regulation	2025	法规	欧盟
9	网络和信息系统安全指令	2023	法规	欧盟
10	数据法案	2025	法案	欧盟
11	网络弹性法案	2023	法案	欧盟
12	数据保护及数字信息（第 2 号）法案	2023	法案	英国
13	自动驾驶法	2021	法案	德国
14	自动驾驶汽车安全技术指南	2018	政策	日本
15	为交通运输的未来做好准备-自动汽车 3.0	2020	政策	美国

附录 B 已发布及在研的标准（国际/国内）

表二 智能驾驶网络和数据安全相关标准

序号	标准名称	标准类型	标准性质	对应国外标准
1	GB 44495—2024 汽车整车信息安全技术要求	GB	发布	UN R155
2	GB 44496—2024 汽车软件升级通用技术要求	GB	发布	UN R156
3	GB 44497—2024 智能网联汽车 自动驾驶数据记录系统	GB	发布	——
4	GB/T 40861—2021 汽车信息安全通用技术要求	GB/T	发布	——
5	GB/T 40856—2021 车载信息交互系统信息安全技术要求及试验方法	GB/T	发布	——
6	GB/T 40857—2021 汽车网关信息安全技术要求及试验方法	GB/T	发布	——
7	GB/T 41578—2022 电动汽车充电系统信息安全技术要求及试验方法	GB/T	发布	——
8	GB/T 44774—2024 汽车信息安全应急响应管理规范	GB/T	发布	——
9	GB/T 44778—2024 汽车诊断接口信息安全技术要求及试验方法	GB/T	发布	——
10	GB/T 44417—2024 车路协同系统智能路侧协同控制设备技术要求和测试方法	GB/T	发布	——
11	GB/T 35273—2020 信息安全技术 个人信息安全规范	GB/T	发布	——
12	GB/T 37964—2019 信息安全技术 个人信息去标识化指南	GB/T	发布	——
13	GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南	GB/T	发布	——
14	GB/T 41871—2022 信息安全技术　汽车数据处理安全要求	GB/T	发布	——
15	GB/T 44464—2024 智能网联汽车数据通用要求	GB/T	发布	——
16	GB/T 43435—2023 信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求	GB/T	发布	——
17	GB/T 45574—2025 数据安全技术敏感个人信息处理安全要求	GB/T	发布	——

序号	标准名称	标准类型	标准性质	对应国外标准
18	GB/T 45392—2025 信息安全技术 基于个人信息的自动化决策安全要求	GB/T	发布	——
19	GB/T 46068—2025 数据安全技术 个人信息跨境处理活动安全认证要求	GB/T	发布	——
20	GB/T 43697—2024 数据安全技术 数据分类分级规则	GB/T	发布	——
21	GB/T 41479—2022 信息安全技术 网络数据处理安全要求	GB/T	发布	——
22	GB/T 45652—2025 信息安全技术 生成式人工智能预训练和优化训练数据安全规范	GB/T	发布	——
23	GB/T 45674—2025 信息安全技术 生成式人工智能数据标注安全规范	GB/T	发布	——
24	GB/T 45654—2025 信息安全技术 生成式人工智能服务安全基本要求	GB/T	发布	——
25	GB T 46800—2025 生成式人工智能技术应用社会影响 评估指南	GB/T	发布	——
26	GB/T 45958—2025 网络安全技术 人工智能计算平台安全框架	GB/T	发布	——
27	GB/T 46347—2025 人工智能 风险管理能力评估	GB/T	发布	——
28	GB 45438—2025 网络安全技术 人工智能生成合成内容标识方法	GB	发布	——
29	GB/T 46194—2025 道路车辆 信息安全工程	GB/T	发布	——
30	GB/T 45112—2024 基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求	GB/T	发布	——
31	道路车辆 网络安全验证和确认	GB/T	启动立项	ISO 8477
32	汽车密码应用技术要求	GB	起草中	——
33	汽车软件识别码	GB/T	申请立项	——
34	汽车数字证书应用规范	GB/T	申请立项	——
35	汽车网络安全入侵检测技术要求及实验方法	GB/T	完成立项	——
36	道路车辆 信息安全工程审核指南	GB/Z	下达计划	ISO/PAS 5112
37	道路车辆 软件升级工程	GB/T	下达计划	——
38	道路车辆 网络安全保障等级和目标攻击可	GB/T	预研阶	ISO 8475

序号	标准名称	标准类型	标准性质	对应国外标准
	行性		段	
39	智能网联汽车 供应链网络安全技术规范	GB/T	预研阶段	——
40	汽车安全漏洞分类分级评价	GB/T	征求意见	——
41	信息安全技术重要数据处理安全要求	GB/T	征求意见	——
42	信息安全技术数据安全风险评估方法	GB/T	征求意见	——
43	数据安全技术 个人信息保护合规审计要求	GB/T	征求意见	——
44	汽车安全漏洞分类分级评价	GB/T	征求意见	——
45	车联网信息服务 数据安全保护能力评估规范	YD/T	制定中	——
46	YD/T 3865—2021 工业互联网数据安全保护要求	YD/T	发布	——
47	YD/T 3802—2020 电信网和互联网数据安全通用要求	YD/T	发布	——
48	YD/T 3746—2020 车联网信息服务 用户个人信息保护要求	YD/T	发布	——
49	YD/T 3751—2020 车联网信息服务数据安全技术要求	YD/T	发布	——
50	T/CAMMTB 189—2024 汽车企业数据安全管理体系要求	团标	发布	——
51	工业和信息化领域数据安全事件应急预案	通知	发布	——
52	关于进一步加强智能网联汽车准入、召回及软件在线 升级管理的通知（征求意见稿）	通知	发布	——
53	工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见	通知	发布	——
54	YD/T 4981—2024 工业领域重要数据识别指南	YD/T	发布	——
55	YD/T 4982—2024 工业企业数据安全防护要求	YD/T	发布	——
56	YD/T 6415—2025 工业领域数据安全风险评估规范	YD/T	发布	——
57	智能网联汽车时空数据传感系统安全基本要求	GB	报批	——

序号	标准名称	标准类型	标准性质	对应国外标准
58	智能网联汽车时空数据安全处理基本要求	GB	报批	——
59	汽车数据安全管理若干规定	通知	发布	——
60	车用人工智能技术应用指南	——	计划	——
61	车用人工智能平台架构指南	——	计划	——
62	人工智能 隐私计算通用框架	——	计划	——

缩略语

缩略语	英文全称	中文释义
ACC	Adaptive Cruise Control	自适应巡航控制
NOA	Navigate on Autopilot	导航辅助驾驶
AEB	Automatic Emergency Braking	自动紧急制动
LKA	Lane Keeping Assist	车道保持辅助系统
BSD	Blind Spot Detection	盲区监视系统
V2X	Vehicle-to-Everything	车联网通信
GPS	Global Positioning System	全球定位系统
IMU	Inertial Measurement Unit	惯性测量单元
TPMS	Tire-pressure monitoring system	胎压监测系统
ODD	Operational Design Domain	运行设计域
ECU	Electronic Control Unit	电子控制单元
CAN	Controller Area Network	控制单元区域网络
LIN	Local Interconnect Network	局部连接网络
MOST	Media Oriented Systems Transport	面向媒体的系统传输
JTAG	Joint Test Action Group	联合测试工作组
SWD	Serial Wire Debug	串行线调试
USB	Universal Serial Bus	通用串行总线
GNSS	Global Navigation Satellite System	全球导航卫星系统
C-V2X	Cellular Vehicle to Everything	蜂窝车联网
DSRC	Dedicated Short Range Communications	专用短程通信
OTA	Over-The-Air	空中下载技术/远程软件升级
API	Application Programming Interface	应用程序接口
T-BOX	Telematics BOX	车载通信终端
DCU	Domain Control Unit	智能驾驶域控制器
PKI	Public Key Infrastructure	公钥基础设施
TEE	Trusted Execution Environment	可信执行环境
MMU	Memory Management Unit	内存管理单元
TLS	Transport Layer Security	传输层安全协议
IPSec	Internet Protocol Security	互联网协议安全
DTLS	Datagram Transport Layer Security	数据报传输层安全协议
MAC	Message Authentication Code	消息认证码
RSU	Road Side Unit	路侧单元
VLAN	Virtual Local Area Network	虚拟局域网
MACsec	Media Access Control Security	媒体访问控制安全协议
PTP	Precision Time Protocol	精确时间协议
ARP	Address Resolution Protocol	地址解析协议
DoS	Denial of Service	拒绝服务

缩略语	英文全称	中文释义
SBOM	Software Bill of Materials	软件物料清单
CI/CD	Continuous Integration/Continuous Deployment	持续集成/持续部署
SDK	Software Development Kit	软件开发工具包
SOTIF	Safety Of The Intended Functionality	预期功能安全
FGSM	Fast Gradient Sign Method	快速梯度符号法
PGD	Projected Gradient Descent	投影梯度下降
OSI	Open System Interconnect	开放系统互连
UART	Universal Asynchronous Receiver/Transmitter	通用异步收发传输器
I2C	Inter-Integrated Circuit	集成电路总线
SPI	Serial Peripheral Interface	串行外设接口
PCB	Printed Circuit Board	印刷电路板
NFC	Near Field Communication	近场通信
RFID	Radio Frequency Identification	射频识别
MRM	Minimal Risk Maneuver	最小风险机动
HMI	Human Machine Interface	人机界面
DMS	Driver Monitoring System	驾驶员监控系统
TPM	Trusted Platform Module	可信平台模块
eUICC	embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
Grad-CAM	Gradient-weighted Class Activation Mapping	可视化与特征贡献分析工具
SHAP	shapley Additive Explanation	模型事后解释的方法
LIME	Local Interpretable Model-agnostic Explanations	模型无关的局部可解析性算法
5G	5th Generation Mobile Communication Technology	第五代移动通信技术
SAE	SAE International	国际自动机工程师学会
ADS	Automated Driving System	自动驾驶系统
SIA	Safety Impact Analysis	安全影响评估
ROP	Return-Oriented Programming	返回导向编程
IPC	Inter-Process Communication	进程间通信
QoS	Quality of Service	服务质量

参考文献

[1] 中华人民共和国网络安全法[L].2025-10-28.

[2] 中华人民共和国数据安全法[L].2021-06-10.

[3] 中华人民共和国个人信息保护法[L].2021-08-20.

[4] 全国信息安全标准化技术委员会(SAC/TC 260).信息安全技术 网络安全等级保护基本要求:GB/T 22239-2019[S].中国标准出版社,2019.

[5] 全国信息安全标准化技术委员会(SAC/TC 260).信息安全技术 网络安全等级保护安全设计技术要求:GB/T 25070-2019[S].中国标准出版社,2019.

[6] 孙航,张路,季国田.智能网联汽车标准体系及重点标准研究与展望[J].汽车安全与节能学报,2024,15(06):795-812.

[7] 中国汽车技术研究中心有限公司. 2025 年车用人工智能标准体系研究报告[EB/OL]. (2025-07-14) [2025-10-28]. https://www.catarc.org.cn/prod-api/preview/ntcas/resources/file/2025/07/14/697699211202629.pdf.

[8] 工业和信息化部, 国家标准化管理委员会. 国家车联网产业标准体系建设指南（智能网联汽车）（2023 版）[EB/OL]. (2023-07-27) [2025-10-28]. https://www.gov.cn/zhengce/zhengceku/202307/P020230727459713380334.pdf.

[9] 张骁,陈海龙,杨思佳,等.自动驾驶网络安全政策与标准化研究[J].中国信息安全,2024,(02):26-29.

[10] 汽车数据安全管理若干规定(试行)[L].2021-08-16.

[11] 工业和信息化部关于印发《车联网(智能网联汽车)产业发展行动计划》的通知[L].2018-12-25.

[12] 工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见[L].2021-07-30.

[13] 工业和信息化部、公安部、交通运输部关于印发《智能网联汽车道路测试与示范应用管理规范(试行)》的通知[L].2021-07-27.

[14] On-Road Automated Driving (ORAD) Committee. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles[M]. SAE international, 2021.

[15] ISO/SAE. ISO/SAE 21434:2021 Road vehicles—Cybersecurity engineering[S]. Geneva: International Organization for Standardization, 2021.

[16] ISO. ISO 26262:2018 Road vehicles—Functional safety[S]. Geneva: International Organization for Standardization, 2018.

[17] UNECE. UN Regulation No. 155: Uniform provisions concerning the approval of motor vehicles with regard to cyber security and cyber security management system[S]. Geneva: United Nations Economic Commission for Europe, 2020.

[18] UNECE. UN Regulation No. 156: Uniform provisions concerning the approval of motor vehicles with regard to software update and software update management system[S]. Geneva: United Nations Economic Commission for Europe, 2020.