中国通信标准化协会
China Communications Standards Association

车联网安全标准化白皮书

（2023 年）

中国通信标准化协会

2023年11月

版权说明

前　言

车联网是汽车、电子、信息通信、道路交通运输等行业深度融合的新型产业形态，通过贯通汽车、道路交通运输、云网通信和平台等关键要素，实现“人－车－路－云”数据交互和高效协同，使能综合信息服务、交通治理、安全效能提升、辅助驾驶和自动驾驶等应用，提升交通出行的智能化、网联化和绿色化水平，助力经济社会实现高效、便捷、安全与低碳运转，已成为汽车行业新的发展方向和世界主要国家竞相角逐的产业制高点，也是我国新型工业化进程中的重要推动力量。党的十八大以来，我国车联网产业规模不断壮大，汽车产销量全球第一，建成全球最大 5G 网络，截至 2023 年 5 月，我国车辆装载车联网卡数量超 9840 万张，具备组合驾驶辅助功能（L2）级的乘用车渗透率达到 34.9%。伴随产业快速发展，车联网内涵不断延伸，互联网资产暴露面和安全边界持续扩大，网络安全各类风险加速向车联网领域渗透蔓延，车联网网络安全、数据安全、车辆行驶安全、产业安全等方面风险交织叠加，车联网安全日益成为各方关注焦点。

党中央、国务院高度重视车联网产业发展和安全，相关部门陆续印发《智能汽车创新发展战略》《车联网（智能网联汽车）产业发展行动计划》《关于加强车联网网络安全和数据安全工作的通知》《车联网网络安全和数据安全标准体系建设指南》等政策文件，积极开展车联网安全工作部署。进一步强化车联网安全保障能力建设，不仅需要从监管、技术、行业机制的角度寻求突破，也亟需从标准化维度加

大工作力度，切实发挥标准在车联网安全工作中的基础性、规范性、引领性作用，有效指导和体系化推进相关重点标准研究制定工作。

本白皮书系统梳理了国内外主要国家、地区车联网安全相关发展战略政策，描述了国内外车联网安全标准化现状，针对车联网安全关键要素和重点环节，研究提出车联网安全标准需求和发展方向，给出标准化工作推进建议，旨在呼吁社会各界加强对车联网安全标准化工作的重视程度，共同助力车联网产业高质量安全发展。

本白皮书由中国通信标准化协会（CCSA）网络与数据安全（TC8）车联网安全任务组（TF2）牵头，参与编写单位包括：中国信息通信研究院、天翼物联科技有限公司、广东为辰信息科技有限公司、中国第一汽车集团有限公司、国汽（北京）智能网联汽车研究院有限公司、广州小鹏汽车科技有限公司、北京百度网讯科技有限公司、中信科移动通信技术股份有限公司、三六零数字安全科技集团有限公司、郑州信大捷安信息技术股份有限公司、浙江大学网络空间安全学院、浙江吉利控股集团有限公司。主要参与编写人员：魏亮、谢玮、林美玉、赵爽、张倩、柯皓仁、张宁、杜霖、郭茜、冯开瑞、陈荆花、仇俊华、宋雪冬、杨汶翰、陈鹏、薛宇、闫昭、丁润涛、安景斌、郑德熙、冯世杰、黄丹、韩松庭、徐晖、包施晗、龚伟炜、严敏睿、刘献伦、刘为华、任奎、薛强、卢立、杨坤、潘亮，罗巧玲。

目 录

1. 车联网安全法律政策进展

伴随车联网产业快速发展，车联网网络安全和数据安全事件频发，车联网安全形势不容乐观，对此世界各国都十分重视车联网安全。国际层面以美国、欧盟、英国、日本等国家为代表，陆续出台各项法规政策，强化车联网网络安全、数据安全总体布局。其中，美国加强各方广泛合作，推动技术创新和安全；欧盟则注重隐私保护，对个人数据和非个人数据都提出相应的规范；英国关注网联汽车全生命周期的网络安全，将安全责任拓展到产业链各主体；日本重视数据安全和隐私保护，汽车网络安全方面主要沿用联合国世界车辆法规协调论坛（UN/WP29）制定的规定和要求。国内则从法律法规、国家政策、地方政策等不同层面构建车联网安全保障体系。国家层面顶层设计逐步完善，车联网安全“有法可依”，《网络安全法》《数据安全法》和《个人信息保护法》先后发布实施，初步构建起网络安全和数据安全保障领域的法律体系框架。国务院、工业和信息化部、交通运输部、科学技术部、国家发展改革委、公安部等部委相继出台一系列顶层规划及政策文件，车联网安全发展取得阶段性成效。各级地方政府高度重视网络安全和数据安全的能力建设，密集发布了一系列地方政策对智能网联汽车领域的网络安全和数据安全工作提出了具体要求。

1.1. 国外情况

1.1.1. 美国

美国加强与各利益相关方广泛合作，推动道路运输技术创新和安全，确保美国在自动化领域处于全球领先地位。2021 年 1 月，美国《自动驾驶汽车综合计划》确定了实现自动驾驶系统（ADS）愿景的三个目标：促进合作与透明，为合作伙伴和利益相关者提供技术能力；营造现代化监管环境，开发以安全为中心的框架和工具，以评估自动驾驶系统技术的安全性能；为自动驾驶系统（ADS）的安全集成准备交通系统。美国交通运输部（USDOT）将与利益相关者合作，开展安全评估和整合 ADS 所需的基础研究和示范活动。2021 年 11 月，美国国会正式通过《两党基础设施法》，意在通过建设更好的道路、桥梁和港口、强化各部门信息技术和网络安全、向清洁能源转型以及加强所有其他关键基础设施部门，为实现长期的安全和繁荣奠定基础，推动产业链向北美转移。2022 年 4 月，美国发布《交通战略计划 2022-2026》，意图通过变革性投资使美国基础设施现代化，以提供更安全、更清洁、更出色的交通系统。其中强调要加强运输系统的弹性，以保护其免受网络和其他攻击的破坏。2023 年 5 月，美国《两党基础设施法案》资助的项目批复中包括实时交通信息、公交信号定时系统和无缝公交支

付系统，以提高安全性和交通效率。

1.1.2. 欧盟

欧盟明确车联网网络安全与数据安全基线，更加注重隐私保护，通过行业协作强化整个产业的安全能力。从职能分工来看，欧盟负责出台适用全体成员国的普适性安全法规，各成员国在欧盟法规要求下制定符合国内现状的安全领域法律法规。以网络安全、数据安全法规为通用基本要求，通过汽车产品的型式准入相关法规向车联网安全领域延伸。

2023 年 1 月 13 日，《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS 2 指令）正式取代《网络和信息系统安全指令》（NIS 指令）生效。作为欧盟在安全防护体系的系统性协同指导与网络安全监管方法的法律支撑，NIS 2 指令旨在消除成员国在网络安全要求和措施实施方面的差异。较之 NIS 指令，NIS 2 指令大大扩展了属于其范围的关键实体部门和类型，同时也加强了企业需要遵守的网络安全风险管理要求。如今，NIS 2 指令同《欧盟网络安全法》共同构成了欧盟在网络安全领域的通用上位法。

数据安全领域则是由《欧盟通用数据保护条例》（GDPR）、《数据法案》（DGA）、《数据治理法》等已出台的法规，共同构成数据保护的法律体系。GDPR 作为个人数据保护的主要法规，其立法目的就是保护隐私权并促进该权利的行使。适用于任何收集、处理、管理或存储欧洲公民数据的组织。所以，实质上 GDPR 是一个数据保护的全球标准。但与以往的隐私条例不同，GDPR 对数据处理者也赋予了新的合规要求。从原有的收集和使用数据的拥有者需要对数据保护负责，到现今的数据处理者也将需要直接承担合规风险和义务。同时，GDPR 还提高了数据保护标准，避免数据滥用和数据泄露，其中第 45（3）条的充分性决定条例更是影响、促进了国家间法规框架融合，推动了全球数据治理方式的改变。对于非个人数据的管控上，主要依赖于 2020 年 11 月发布的《数据治理法》与 2022 年的《数据方案》管理受知识产权或商业秘密保护的非个人数据的国际传输。

在汽车产品的安全管理方面，欧盟通过将联合国世界车辆法规协调论坛（UN/WP29）的 R155、R156、R157 三项法规要求强制引入型式批准，结合（EU）2018/858 的整车型式批准和（EU）2019/2144 的零部件型式批准，共同构建起了欧盟车型准入管理的框架体系，将网络安全与数据安全管理要求引入车联网安全领域。

1.1.3. 英国

英国关注网联汽车全生命周期的网络安全，将安全责任拓展到产业链各主体，力图在自动驾驶领域率先颁布监管制度。2022 年 1 月 26 日，英格兰及威尔士法律委员会与苏格兰法律委员会联合发表了一份名为《自动驾驶汽车：联合报

告》的法律改革报告，旨在建立一个更安全的、责任划分更清晰的自动驾驶汽车道路安全运行机制。报告针对目前法规的局限性提出了修改建议，对自动驾驶汽车与有驾驶辅助功能的汽车进行区分，将自动驾驶汽车在行驶各阶段的责任划分得更清楚。

1.1.4. 日本

日本重视数据安全和隐私保护，汽车网络安全方面主要沿用联合国世界车辆法规协调论坛（UN/WP29）制定的规定和要求。2021 年 8 月 3 日，日本个人信息保护委员会（PPC）公布《个人信息保护法》修订案，该法于 2022 年 4 月 1 日正式实施，适用于包括车联网在内的数据安全和隐私保护，是日本个人信息保护的基本框架，在个人信息范围的界定、与第三方的共享、跨境传输等制度方面都独具特色。为加快制定 L4 级自动驾驶法规，近期日本警察厅表示，新版《道路交通法》修正案预定于 2023 年下半年施行，该法案列入了在特定条件下实现完全自动化驾驶的“Level 4”运行许可制度。如果该法开始实施，将意味着日本将允许 L4 级自动驾驶汽车上路。

1.2. 国内情况

1.2.1. 法律法规

国家层面网络和数据安全相关法律法规陆续正式实施，安全工作有法可依。2017 年 6 月 1 日起，《网络安全法》正式实施，明确要求网络运营者（包括整车企业及车辆运营商等）应“履行网络安全保护义务，接受政府和社会的监督，承担社会责任”“依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”等。2021 年 9 月 1 日起，《数据安全法》正式施行，从法律层面清晰定义了数据活动、数据安全，提出国家将对数据实行分类分级保护、开展数据活动必须履行数据安全保护义务承担社会责任等。在明确国家数据安全基本制度体系的基础上，对于重要数据提出了加强安全保护的要求。2021 年 11 月 1 日起，《个人信息保护法》正式施行，对个人信息保护提供更强有力的保障，规定了个人信息的收集、使用、保存和安全保护等方面的具体要求，对下位法规、规章和国家标准形成有效指引。

《网络安全法》《数据安全法》和《个人信息保护法》的先后发布实施，初步构建起网络安全和数据安全保障领域的法律体系框架。

2021 年 7 月 30 日，国务院发布了《关键信息基础设施安全保护条例》，自 2021 年 9 月 1 日生效。目的为保障关键信息基础设施安全，维护网络安全、数据安全，细化和落实《网络安全法》的有关规定。针对汽车行业中可能涉及关键

信息基础设施的运营者，需高度重视组织内网络安全和数据安全合规工作，履行关键信息基础设施运营者的特殊安全保护制度。

2021 年 11 月 14 日，网信办发布了《网络数据安全管理条例（征求意见稿）》，虽然文件中并未明确提及汽车行业，但在智能网联汽车快速发展的背景下，汽车已从孤立的电子信息终端向网联化、智能化的信息节点发展，对数据安全保护的紧迫性也日益凸显。文件中涵盖了数据安全、个人信息保护、数据跨境、网络平台、监督管理等内容，倡导性条款较少，重点在于对三部上位法的落地实施。

上述法律法规，主要是以保障网络安全、防范网络风险、保护数据安全、个人信息安全等为基本考虑，构建智能网联汽车网络安全和数据安全的法律法规体系框架。

1.2.2. 国家政策

自 2015 年以来，国务院、工业和信息化部、交通运输部、科学技术部、国家发展改革委、公安部等部委相继出台一系列顶层规划及政策文件，车联网安全发展取得阶段性成效。出台《汽车产业中长期发展规划》《车联网（智能汽车）产业发展行动计划》《智能汽车创新发展战略》等指导性文件，旨在宏观指导智能网联汽车产业稳步发展，并将智能网联汽车网络安全和数据安全作为一项重要目标和工作重点。

2021 年 7 月，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》，要求压实企业主体责任，加强汽车数据安全、网络安全、软件升级、功能安全和预期功能安全管理，保证产品质量和生产一致性，推动智能网联汽车产业高质量发展。

2021 年 9 月，工业和信息化部发布《关于加强车联网网络安全和数据安全工作的通知》，要求加强车联网网络安全和数据安全工作，建立健全信息安全管理制度，保障车联网系统的稳定安全运行，防范网络攻击和安全事件发生。

2022 年 3 月，工业和信息化部发布《车联网网络安全和数据安全标准体系建设指南》，围绕总体与基础设施、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑六个重点领域和方向，共布局 103 项标准项目，强化标准的体系化推进。

2022 年 10 月，工业和信息化部会同有关部门起草了《道路机动车辆生产准入许可管理条例（征求意见稿）》，为适应当前汽车行业发展的新趋势，文件中强化了汽车网络安全、数据安全及个人信息保护，提出智能网联汽车生产企业应当建立车辆产品网络安全、数据安全、个人信息保护、车联网卡安全管理、软件升级管理制度，完善安全保障机制，落实安全保障措施等内容。

1.2.3. 地方政策

各级地方政府高度重视网络安全和数据安全的能力建设，密集发布了一系列

地方政策对智能网联汽车领域的网络安全和数据安全工作提出了具体要求。

2023 年 5 月 12 日，北京市高级别自动驾驶示范区工作办公室正式发布了《北京市智能网联汽车政策先行区数据安全管理办法（试行）》，填补了国内自动驾驶示范区级数据安全管理的空白。文件中主要包含三个版块内容：一是明确了智能网联汽车产业数据安全管理的关键环节、二是详细梳理了重点数据类型的合规风险、三是创新性构建了示范区数据安全能力建设机制。

2022 年 6 月 30 日，深圳市印发了《深圳经济特区智能网联汽车管理条例》，在该条例中专门设置了“网络安全和数据安全保护”章节，对智能网联汽车涉及的网络安全和数据安全保护问题进行规范。明确规定了相关企业应当依法取得网络关键设备和网络安全专用产品的安全检测认证、依法制定智能网联汽车网络安全事件应急预案，建立网络安全评估和管理机制，制定数据安全管理制度和隐私保护方案并将存储数据的服务器设置在中国境内等。

此外，上海市、长沙市、苏州市等对智能网联汽车的网络安全和数据安全均提出了相关要求，例如《上海市加快智能网联汽车创新发展实施方案》《上海市智能网联汽车测试与应用管理办法》《长沙市智能网联汽车道路测试管理实施细则（试行）V3.0》《苏州市智能车联网发展促进条例》、苏州市《关于促进车联网和智能网联汽车发展的决定（草案）》等。

2. 国外车联网安全标准化进展

国际车联网安全标准化建设稳步推进，加快车联网安全标准化工作的统筹布局。以联合国世界车辆法规协调论、国际标准化组织、国际电信联盟、国际汽车工程师学会、3GPP 组织等为代表的国际组织聚焦各自宗旨和任务，以网络安全、软件升级、V2X 通信安全、自动驾驶安全等为重点方向加快车联网安全标准研制工作。美国、欧盟、英国、日本等国家的权威标准化组织也面向汽车网络安全、车辆通信、数据安全等方面的标准展开标准研制工作，对本国的汽车企业和供应商等主体提出相应的网络安全要求。

2.1. 国际组织

2.1.1. 联合国（UN/WP29）

联合国世界车辆法规协调论坛（The World Forum for the harmonization of vehicle regulations，简称 WP.29）是联合国欧洲经济委员会（UN/ECE）下的永久性工作组，主要负责开展国际范围内汽车技术法规和汽车产品认证的协调工作。其下所设的自动驾驶与网联车辆工作组（GRVA），于 2020 年 6 月，发布了强

制法规 R155（UN Regulation No. 155）与 R156（UN Regulation No. 156），明确提出了汽车网络安全及软件升级要求。

R155 法规要求包含网络安全管理体系认证（CSMS）和车辆网络安全产品型式认证（VTA）。体系认证要求汽车厂商在车辆完整生命周期各个阶段制定网络安全管理流程，并采取对应的控制措施，以确保汽车网络安全风险得到较为全面的识别评估，以及有效的处置。而产品型式认证则侧重对具体车型网络安全缓解措施的审查验证，以确保其与设计方案的一致性和完备性，保障管理体系有效运行。

R156 法规要求包含软件升级管理体系认证（SUMS）和车辆软件升级产品型式认证（VTA），要求汽车厂商对车辆完整的软件升级过程制定管理规范，以充分评估升级对车辆及用户的影响，保障其符合预期的安全执行并实现可追溯。其中，在保护软件包的真实性及完整性、保障升级相关链路安全等部分，则与 R155 存在关联，共同约束汽车厂商实现软件升级网络安全。

除此之外，WP.29 GRVA 还负责其他相关领域的法规和技术标准制定，如自动车道保持系统 ALKS（R157）、转向装置（R79）、自动紧急制动系统 AEBS（R131）、电子稳定控制系统 ECS（R140）、用于 M1 和 N1 车辆的自动紧急制动系统 AEBS（R152）、事件数据记录系统（R160）等。这些法规和正在制定中的驾驶员控制辅助系统（DCAS）、自动驾驶测试方法和评估方法（VMAD）、自动驾驶事件数据记录系统（EDR/DSSAD）等法规，都构成了 WP.29 对自动驾驶和网联车辆的全面监管体系。

2.1.2. 国际标准化组织（ISO）

国际标准化组织（ISO）下设的道路车辆技术委员会（ISO/TC 22 Road vehicles）负责 1968 年维也纳公约中所规定的道路车辆及其装备的兼容性、互换性、安全性和性能评价试验规程（包括仪器的特性）等标准化工作。ISO/TC 22/SC 32 作为其分技术委员会，目前已发布的标准有 ISO/SAE 21434、ISO 24089、ISO/PAS 5112 等。

ISO/SAE 21434 Road vehicles - Cybersecurity engineering（道路车辆 网络安全工程）于 2021 年 8 月发布，规定了道路车辆网络安全风险管理的工程要求，定义了标准的网络安全流程管理框架和网络安全风险管理的通用语言。R155 法规引用其作为对认证机构及技术服务方的人员能力要求，说明其可指导组织开展网络安全策略和流程制定、网络安全风险管理、培养网络安全文化意识等。

ISO 24089:2023 Road vehicles — Software update engineering（道路车辆 软件升级工程）于 2023 年 2 月发布，提供了软件升级的标准要求和建议，可用于指导企业建立规范的软件升级管理、过程监控、测量及改进流程，有效识别软件升级过程中的功能安全和网络安全风险，提升相关方之间的功能安全和网络安全

意识，为汽车厂商满足 R156 提供了参考。

ISO/PAS 5112:2022 Road vehicles — Guidelines for auditing cybersecurity engineering（道路车辆 网络安全工程审核指南）于 2022 年 3 月发布，是 ISO/SAE 21434 相关联的支撑性文件，并且将 ISO 19011 管理体系审核指南扩展到了汽车领域，可用于指导汽车厂商内外部审核的开展。

除上述三个标准外，ISO/TC 22/SC 32 及 33 分技术委员会还发布了 ISO 26262 系列道路车辆功能安全标准、ISO/PAS 21448 预期功能安全、ISO 22735 评估车道保持辅助系统性能的测试方法、ISO 34501 自动驾驶系统测试场景的术语和定义、ISO 34502 基于情景的安全评估的工程框架和过程等相关标准。

同时，ISO/TC 22 技术委员会还关注与自动驾驶相关标准的制定，如 ISO 34503 道路车辆 用于自动驾驶系统的运营设计领域的分类法、ISO 34504 道路车辆 场景属性和分类、ISO 34505 道路车辆 自动驾驶系统的测试场景－场景评估和测试用例生成、ISO 22733-2 道路车辆 评估自动紧急制动系统性能的试验方法－第 2 部分：汽车对行人、ISO/SAE AWI PAS 8475 道路车辆 网络安全保证级别（CAL) 和针对性攻击可行性（TAF）等相关标准的制定。

2.1.3. 国际电信联盟（ITU）

ITU-T 第 17 研究组（SG17）负责协调所有 ITU-T 研究组的安全相关工作，致力于智能运输系统、物联网、智能电网、智能手机、软件定义网络、网络服务等方面的应用和服务安全。

关于车联网安全相关标准一般在 Intelligent transportation system (ITS) security 部分讨论。其标准号分配范围为 X.1370－X.1389。其中 ITU-T X.1371 定义并描述了联网车辆面临的安全威胁。ITU-T X.1372 为车联网（V2X）通信提供了安全导则，描述了 V2X 通信环境中的威胁，规定了 V2X 通信的安全要求，并描述可能的安全 V2X 通信的实施方案。ITU-T X.1373 在软件更新服务器和有适当安全控制的车辆之间提供了安全软件更新程序。它作为一套最佳实践的标准化功能，可以被车辆制造商和 ITS 相关的产业实际应用。ITU-T X.1374 从对车辆与外部设备间通信接口的威胁和对与车辆通信的外部设备的威胁两个部分分析了对网联车辆的安全威胁。ITU-T X.1374 规定了电信网络环境中可接入车辆的外部接口和外部设备的安全要求，以便根据接入接口的类型，消除已确定的威胁。ITU-T X.1375 则为车载网络（IVNs）的入侵检测系统（IDS）制定了指导方针，主要侧重于检测车载网络中的入侵和恶意活动。ITU-T X.1376 是首个由我国主导的车联网国际标准，其描述了一种针对联网车辆的安全异常行为检测机制，以帮助利益攸关方利用汽车数据来提高车辆安全性。ITU-T X.1377 为联网汽车的入侵防御系统（IPS）制定了指导方针，主要关注对入侵行为的主动响应能力，包括联网汽车入侵防御系统的实施指南和使用案例。

ITU SG17 的车联网安全标准研究工作比较注重实用性，在指导行业实践和产品发展方面具有独特的意义。

2.1.4. 国际汽车工程师学会（SAE）

国际汽车工程师学会（SAE）主要致力于汽车制造业、航空航天等行业的标准化工作，由相关行业的 128,000 多名工程师和相关技术专家组成，其所制定的标准为国际上很多机动车辆技术团体广泛采用。其于 2016 年 1 月发布的 J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems（信息物理汽车系统网络安全指南）是首部针对汽车网络安全而制定的指导性文件，为汽车信息安全提供了全生命周期的保护策略，贯穿于车辆产品设计、研发、生产、运营、服务和退役等各阶段。而随着 ISO/SAE 21434 的发布，SAE J3061 作为其前身，目前已被其代替。

2.1.5. 3GPP

3GPP 组织长期研究移动通信网络演进与发展，其关于 V2X 标准的研制和实施，对车联网 V2X 行业的发展具有基础性的指导意义，也为真正意义的无人驾驶技术发展提供重要支撑。TS33.536 是目前 3GPP 唯一关于 NR-V2X 的安全规范，提供了支持 PC5 单播链路的安全策略。

V2X 技术在 3GPP 的标准发展可以分为三个阶段：第一阶段为 3GPP Release 14 基于 LTE 的 V2X 标准化工作，已于 2017 年 3 月完成。第二阶段为 3GPP Release 15 对 LTE-V2X 的增强标准化工作已于 2018 年 6 月完成。第三阶段为 3GPP Release 16 于 2018 年 6 月启动了 NR-V2X 的研究课题，重点是面向高级 V2X 业务的需求，研究基于 5G NR 的 PC5 接口技术和对 UU 接口的增强。

3GPP Release 16 主要围绕 NR-V2X 的安全需求和安全关键问题，形成了 3GPP TS 33.536 Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services 标准规范。该规范针对 NR-V2X 业务的单播业务场景，定义了基于 PC5 单播模式的安全需求和安全机制，NR-V2X 系统应支持对 PC5 单播用户平面数据和控制面信令的机密性保护、完整性保护和重放保护；NR-V2X 系统应支持为特定的 PC5 单播链路提供配置信令面和用户面的安全策略手段。

2.1.6. 国际电气与电子工程师协会（IEEE）

国际电气与电子工程师协会（IEEE）的标准协会主要从事研究信息技术、通信、电力和能源等多个领域的标准化工作，已在全球吸纳了超过 43 万名会员。其在 2010 年发布的针对智能运输系统应用的标准 IEEE 802.11p（又称 WAVE，Wireless Access in the Vehicular Environment）对传统的无线短距离网络技术加以扩展，实现了车一车之间、车一路之间的网络通讯能力，其最终愿景是建立国家范围的网络，实现车辆与路边接入点或其他车辆之间的通信。该协议标准在很长

一段时间里，被欧美发达国家采用为主流车联网通信技术标准。IEEE 1609 标准就是以该协议为基础的高层标准。在欧洲，IEEE 802.11p 标准还被用作 ITS-G5 标准的基础，支持用于车辆到车辆和车辆到基础设施通信的协议。

2.2. 重点国家地区

2.2.1. 美国

美国基于国家公路交通安全管理局、美国电气和电子工程师协会和美国汽车工程师学会等标准化组织开展车辆通信、数据安全等方面标准研制工作。2016 年 11 月美国国家公路交通安全管理局（NHTSA）制定的一系列标准，如 FMVSS 150-V2V/V2I 等系列，旨在规范车辆间通信的技术规范、数据加密和身份认证等。2019 年 10 月美国电气和电子工程师协会（IEEE）制定的一系列标准，如 IEEE 1609 系列，借鉴了传统 PKI 系统的体系结构，通过证书链实现终端互信，旨在规范车辆间通信加密、身份认证、安全证书、接入安全等。2020 年 4 月美国汽车工程师学会（SAE）制定的一系列标准，如 SAE J2735、SAE J2945.1 等，旨在规范车辆间通信（V2X）的数据格式、数据交换机制、数据加密和身份认证等。

2.2.2. 欧盟

欧盟网络安全领域标准化组织由欧洲网络安全局（ENISA）及欧洲标准化委员会（CEN）、欧洲电工标准化委员会（CENELEC）和欧洲电信标准协会（ETSI）三大标准化机构共同组成，从通用安全技术和个人数据保护等细化维度制定相关标准。其中，ENISA 受《欧盟网络安全法》赋予的职能，在促进成员国网络安全利益相关者与欧盟机构和机构之间的积极合作方面发挥着关键作用。而三大标准化机构则负责具体标准起草，分别为：欧洲标准化委员会（CEN）—主要负责制定工业、商品和服务方面标准；欧洲电工标准化委员会（CENELEC）—主要负责电气和电子领域的标准制定；欧洲电信标准协会（ETSI）—主要负责电信领域的标准制定。

在网络安全领域，联合机构 CEN/CENELEC 通过工作组 JTC 13 网络安全及数据保护工作组制定标准，从通用安全技术、个人数据保护、安全评估标准等维度规范安全要求。已发布标准如《EN 17926：2023》—用以承接《ISO/IEC 27701》的隐私信息管理系统、《EN ISO/IEC 15408-1：2020》—IT 安全评估标准、《EN ISO/IEC 19896-1：2023》—人员能力要求标准等共计 41 项，起草及审批中的标准 21 项。CEN 下属新建工作组 CLC/SC 9XB，负责车辆电气、电子及软件的规范制定，虽尚未开展标准制定工作，但预计将在网联汽车标准研究领域发挥重要作用。ETSI 同样成立了 TC SEC 安全技术委员会，负责提供 ESTI 技术报告及标准，向其他标委提供安全建议与援助。目前标准主要围绕关键基础设施安全要求与规范展开，发布《ETSI TR 103 303》关键基础设施背景下的信通技术保护措

施、《ETSI TR 103 305》有效网络防御的关键安全控制等标准 62 项。德国汽车工业协会（VDA）参考 ISO 27001、ISO 27002 等规范，并参酌法规 GDPR 及汽车产业标准要求为管制项目，提出了 TISAX 信息安全的评估和交换机制。

除此之外，欧盟标委在自动驾驶的标准起草方面也发挥了重要作用，其中 CEN 和 ETSI 正式发布的自动驾驶标准共计 117 项。CEN 主要由其 TC 278 工作组参与起草，主要涉及道路安全、车辆/基础设施/道路使用者之间应用信息通讯技术等智能交通领域标准化；ESTI 则是通过其 ITS 技术委员会，支持跨网络的智慧交通服务应用开发与实施，用以快速响应市场对自动驾驶汽车标准的需求，重点关注信息安全、验证测试等领域。

2.2.3. 英国

英国标准协会（BSI）作为全球权威的标准研发和国际认证评审服务提供商，注册标准涵盖质量、信息安全、电信等几乎所有领域，在车联网安全方面重点关注自动驾驶领域的网络安全。2018 年 12 月，英国标准协会发布自动驾驶技术新网络安全标准，是首个发布此类标准的国家。此标准由英国标准协会与捷豹路虎、福特、宾利等汽车行业领先企业及国家网络安全中心共同合作完成，并获得英国运输部门资金支持。标准内容覆盖评估和管理安全风险、车辆系统生命周期的安全管理、供应链安全管理、软件更新以及车辆系统数据管理等自动驾驶汽车网络安全管理的各个方面。 该网络安全标准有助于提高自动驾驶行业的弹性和准备程度，并帮助英国保持在推进运输技术发展的最前沿。

在网络安全与数据安全方面，英国也陆续发布多个标准。主要包括车辆设备防盗系统规范程度的安全标准（BS AU 209-2:1998,汽车安全 娱乐和通信用车内设备防盗安全系统规范），安全设备/系统在车辆上的应用指南（BS AU 209-0:1996，汽车安全 汽车安全设备/系统应用指南），车联网服务安全跟踪变化标准（BS ISO 20078-3:2021,道路车辆 扩展的车辆网络服务安全）（BS ISO 20078-3:2021-TC,跟踪变化 道路车辆 扩展的车辆网络服务安全），车辆与外部设备之间的通信、排放标准（BS ISO 15031-7:2013 道路车辆 车辆与排放相关诊断外部设备之间的通信 数据连接安全）等。

2.2.4. 日本

日本工业标准（JIS,Japanese Industrial Standards）由日本工业标准调查会（JISC）组织制定和审议，是日本国家级标准中最重要、最权威的标准之一。在信息技术网络安全方面，JISC 已制定关于信息加密、对使用者操作权限和通信范围实施访问控制管理等相关标准。主要包括信息技术（IT）检索设备安全 第 1 部分：通用要求：JIS C6950-1-2009；信息技术 安全技术 密码模块安全预留要求：JIS X19790-2007; 信息技术 安全技术 IT 安全评估标准 第三部分安全保障要求：JIS X5070-3-2000；信息安全管理规范 JIS Q27002-2006；信息安全管理

系统审查、认证单位要求：JIS Q27006-2008 等。

3. 我国车联网安全标准化现状

我国车联网安全标准化工作稳步推进，已取得积极进展。在标准体系建设方面，早于 2017 年开始，由工业和信息化部联合公安部、交通运输部、国家标准化管理委员会等部委，先后印发《国家车联网产业标准体系建设指南》总体要求、智能网联汽车、信息通信、电子产品与服务、车辆智能管理、智能交通相关等标准体系系列分册，分领域规划网络安全标准项目。2022 年 3 月 7 日，工业和信息化部办公厅印发《车联网网络安全和数据安全标准体系建设指南》，立足当前车联网安全工作实际，明确标准体系建设框架的六大重点领域及方向。在具体标准研制方面，中国通信标准化协会、全国汽车标准化技术委员会、全国信息安全标准化技术委员会等主要标委会均下设专门的工作组，依照标准体系建设方向和要求，加快推进车联网安全标准的研制工作。

3.1. 标准框架

3.1.1. 车联网产业标准体系（1+5分册）

2017 年，《国家车联网产业标准体系建设指南》发布，明确到 2020 年基本建成国家车联网产业标准体系的目标。该指南将标准体系分为智能网联汽车、智能交通、信息通信、车辆智能管理、电子产品与服务五个重点领域，为车联网产业提供标准化支撑。落实该指南开展网络安全标准化工作，是夯实车联网产业健康发展的根基，对提升车联网产业网络安全防护水平具有重要意义。

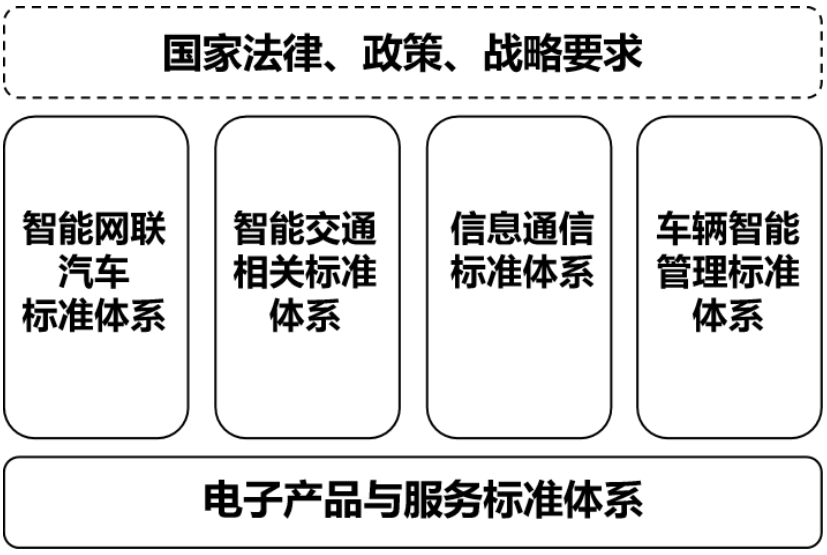

图 1 车联网产业标准体系框架

1、智能网联汽车标准体系

2023 年 7 月，工业和信息化部、国家标准化管理委员会联合修订印发《国家车联网产业标准体系建设指南（智能网联汽车）》（2023 版），是对 2018 版指南的继承、延伸与完善。该指南提出了到 2025 年系统形成能够支撑组合驾驶辅助和自动驾驶通用功能的智能网联汽车标准体系，到 2030 年全面形成能够支撑实现单车智能和网联赋能协同发展的智能网联汽车标准体系的两个建设目标。该指南按技术逻辑架构划分为三个层级，包括基础、通用规范、产品与技术应用等三个部分（如下图所示）。其中，网络安全与数据安全被划定在通用规范标准部分，网络安全标准主要分为安全保障类和安全技术类两个方面，其中，具体包括企业及产品相关的体系管理和审核评估方法、车用数字证书、密码应用等要求。而数据安全标准主要着眼于数据保护和利用的安全性，包括数据通用要求、数据安全管理体系规范、数据安全共享模型和架构等标准。

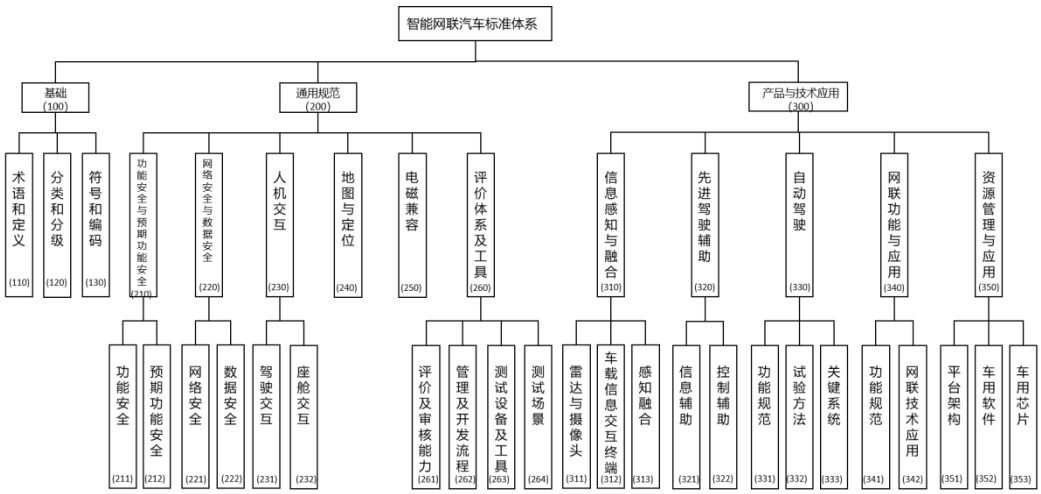

图 2 智能网联汽车标准体系框架

2、智能交通相关标准体系

2021 年，工业和信息化部、交通运输部以及国家标准化管理委员会联合印发《国家车联网产业标准体系建设指南（智能交通相关）》。该指南旨在构建智能交通相关的标准体系，包括智能交通基础标准、服务标准、技术标准和产品标准等，以支持智能交通通用规范核心技术和关键应用。智能交通标准体系包括基础类标准、道路设施标准、车路交互标准、管理与服务标准和网络安全标准 5 部分（如下图所示）。其中网络安全标准包括证书密钥管理、网络安全防护 2 类技术标准。证书密钥管理类标准主要包括车路信息交互所使用的交通行业证书、密钥等相关标准；网络安全防护类标准主要包括路侧设施、计算控制中心等进行信息交互过程中的网络安全防护方法等相关标准确保车联网系统安全。

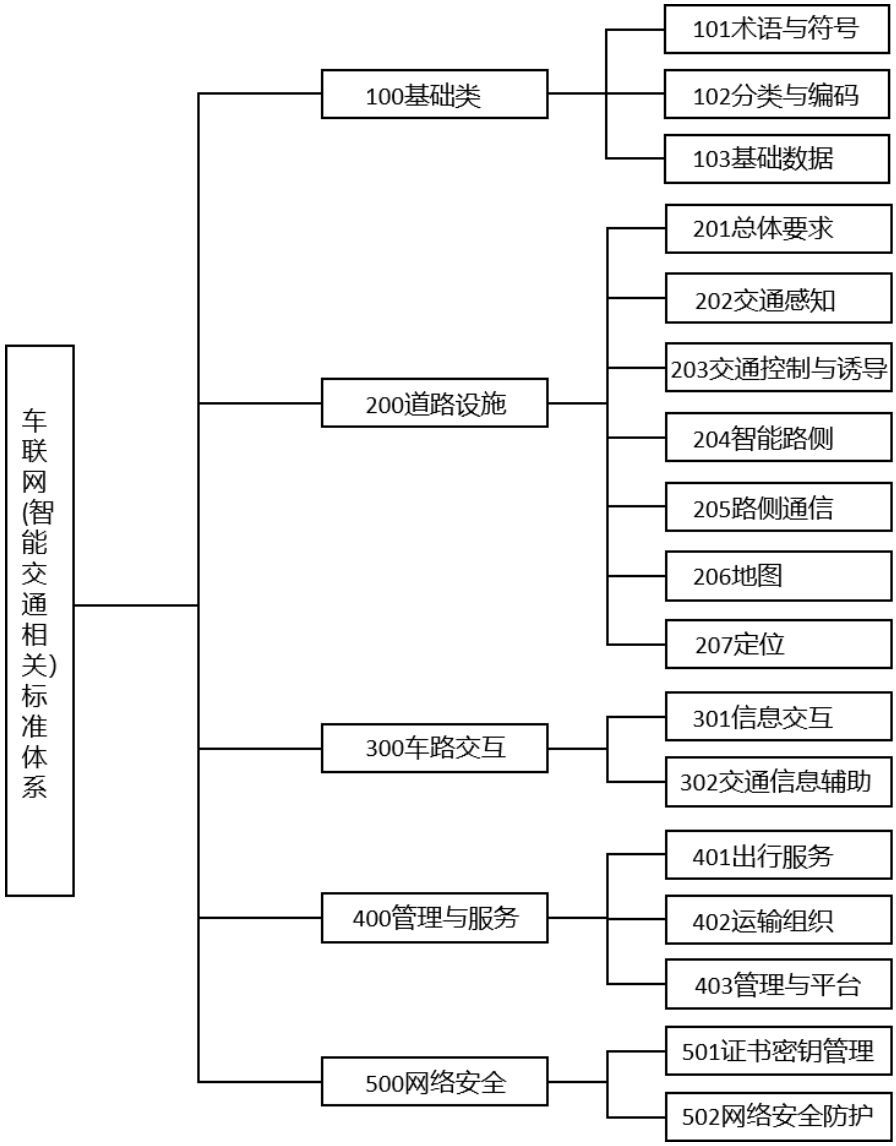

图 3 车联网（智能交通相关）标准体系结构图

3、信息通信标准体系

2018 年，工业和信息化部、国家标准化管理委员会联合印发《国家车联网产业标准体系建设指南（信息通信）》分册。该指南主要针对信息通信领域通用规范、核心技术与关键产品应用，有目的、有计划、有重点地指导车联网产业信息通信领域标准化工作，加快构建包括通信协议、设备、应用服务及安全在内的信息通信标准体系。主要包括基础标准、通信协议和设备、业务与应用、网络与数据安全标准 4 大部分，其中网络与数据安全包括安全体系架构、通信安全、数据安全、网络安全防护、安全监控、应急管理、重要通信、网络信息安全等方面的标准。

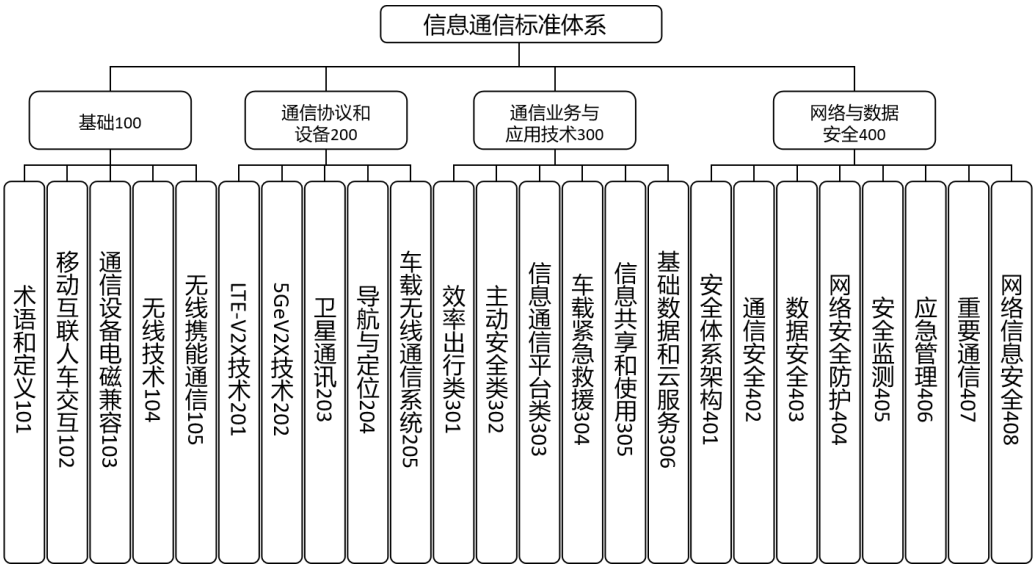

图 4 车联网信息通信标准体系

4、车辆智能管理标准体系

2020 年，工业和信息化部 公安部 国家标准化管理委员会联合印发《国家车联网产业标准体系建设指南（车辆智能管理）》分册。该指南针对车联网环境下的车辆智能管理需求，指导智能网联汽车的登记管理、身份认证与安全、道路运行管理以及车路协同管控与服务等领域的标准化工作。主要包括基础标准、智能网联汽车登记管理、身份认证与安全、智能网联汽车运行管理、车路协同管控与服务标准等 5 部分。其中，身份认证与安全类标准，主要包括智能网联汽车身份与安全、道路交通管理设施身份与安全、身份认证平台及电子证件等 3 类标准。

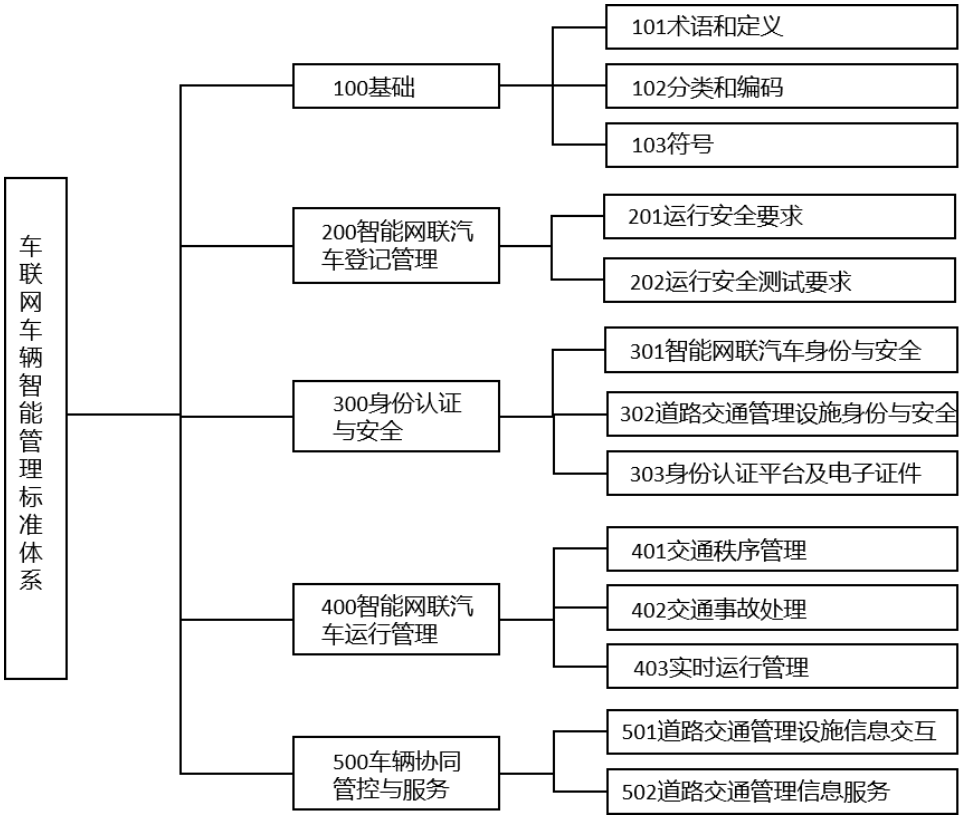

图 5 车辆智能管理标准体系框架图

5、电子产品与服务标准体系

2018 年，工业和信息化部、国家标准化管理委员会联合印发《国家车联网产业标准体系建设指南（电子产品与服务）》分册。该指南包括基础、汽车电子产品、网络设备、服务与平台、网络与信息安全等标准，其中网络与信息安全是贯穿整个体系的共性要求，包括车载系统、终端和服务的安全标准，安全标准主要涉及汽车电子信息安全类标准包括车载系统安全、车载终端安全、移动应用软件和服务运营平台安全等。

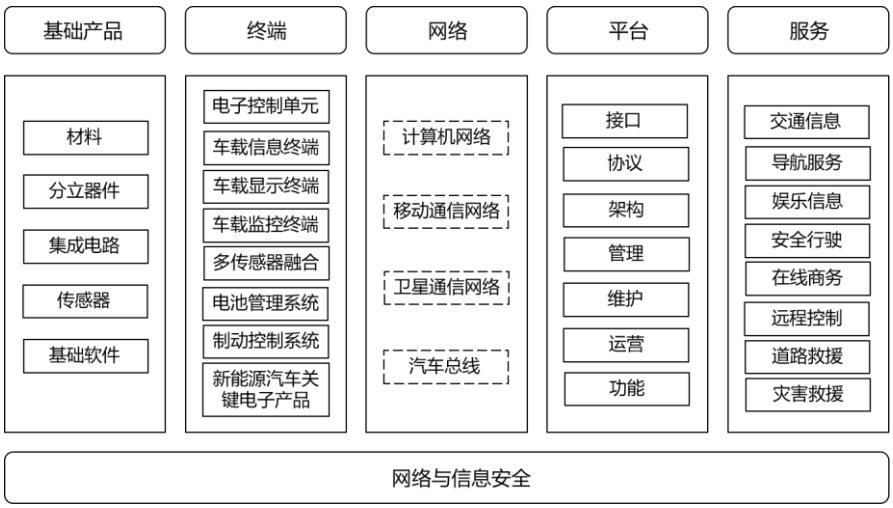

图 6 车联网产业（电子产品和服务）标准体系技术结构图

3.1.2. 车联网网络安全和数据安全标准体系框架

2022 年 3 月 7 日，工业和信息化部办公厅印发《车联网网络安全和数据安全标准体系建设指南》，提出车联网网络安全和数据安全标准体系 2023 年和 2025 年建设目标，明确标准体系建设框架的六大重点领域及方向：总体与基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全和安全保障与支撑，旨在确保车联网环境下的网络和数据安全，为相关行业和企业提供指导和规范。

图 7 车联网网络安全和数据安全标准体系框架图

3.2. 总体与基础共性标准

总体与基础共性部分标准包括术语和定义、总体架构、密码应用等，规范车联网网络安全和数据安全的基本概念、整体架构要求以及密码的通用要求。其中术语和定义标准主要规范车联网网络安全和数据安全的主要概念，为其他标准中的术语和定义提供依据支撑，总体架构标准主要规范车联网网络安全总体架构要

求，明确和界定防护对象、防护方法、防护机制，指导企业体系化开展网络安全防护工作，目前这两个分类的相关标准待制定。

密码应用标准主要规范车联网密码应用要求，明确密码应用通用要求、汽车密码应用、通信密码应用、设备密码应用等要求。目前暂无相关密码国家标准和行业标准的发布，其中国家标准《汽车密码技术要求》、通信行业标准《车联网密码应用通用要求》《车路协同通信密码应用技术要求》《车云通信密码应用基本要求》等标准正加紧编制中。后续还需推动密码算法、密钥管理、密码协议在不同车联网场景、通信、设备和平台等应用的基础标准制定工作。

3.3. 终端和设施网络安全标准

终端和设施网络安全标准主要针对汽车内外包含路侧的设备设施的网络安全提出要求，包括车载设备网络安全、车载网络安全、路侧通信设备网络安全以及网络设施与系统安全等。

车载设备网络安全标准主要规范联网汽车关键智能设备和组件的安全防护与检测要求。目前已发布 GB/T 40857-2021《汽车网关信息安全技术要求及试验方法》和 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》两项国标，已报批《基于移动互联网的数字车钥匙信息安全技术要求》一项通信行业标准。后续应重点推动开展车用安全芯片、车载计算平台、汽车电子控制单元等相关的网络安全标准工作。

车载网络安全标准主要规范整车电子电气架构、总线架构、系统架构等安全防护与检测要求。目前已发布 GB/T 38628-2020《汽车电子系统网络安全指南》、GB/T 40861-2021《汽车信息安全通用技术要求》和 GB/T41578-2022《电动汽车充电系统信息安全技术要求及试验方法》等三项国标。汽车软件升级、整车信息安全、诊断接口信息安全等正在制定中。后续还需推动车载总线系统网络安全、车载以太网网络安全、车载操作系统及应用软件安全等相关标准的制定。

路侧通信设备网络安全标准主要规范联网路侧设备的安全防护设计与实现要求。当前路侧通信设备与计算设备的安全技术要求已在制定中，如《车路协同系统路侧基础设施信息安全技术要求》《路侧采集交通数据脱敏技术要求及测试方法》等。检测与信息服务设备的相关安全标准还待制定。

网络设施与系统安全标准主要规范车联网网络设施与系统的安全防护与检测要求。当前启动了车路协同安全技术架构的通信行业标准的制定，建议后续推动通用的及更多细分领域的车联网网络设施与系统安全标准的制定。

总体而言，车联网终端与设施网络安全标准化程度尚处于启动阶段。同时，随着行业生态发展，在较多的细分项目上涌现了安全标准化诉求，是原先体系建设指南未曾覆盖到的。

后续 2~3 年内，首先应按《车联网网络安全和数据安全标准体系建设指南》的规划，加快相关标准的制定，促进标准体系的初步充实完备。同时，除通信与汽车的标准组织外，鼓励 CCSA、CSAE 等行业联盟组织针对更多细分领域的需求，以团标的形式制定车载终端设备与设施的网络安全标准，以满足更多样灵活的生态需求。

3.4. 网联通信安全标准

网联通信安全标准涵盖车联网通信网络安全和身份认证等相关要求，包括通信安全和身份认证两类标准，规范蜂窝车联网和其他通信技术的安全防护和身份认证方法。

通信安全标准主要规范蜂窝车联网（C-V2X），以及应用于车联网的蜂窝移动通信（4G/5G）、卫星通信、无线射频识别、车内无线局域网、蓝牙低能耗（BLE）、紫蜂（Zigbee）、超宽带（UWB）等安全防护与检测要求。目前，国内已经形成共识使用 PKI（Public Key Infrastructure）公钥体系建立车联网直接通信链路的通信安全体系架构，已发布 YD/T 3750-2020 《车联网无线通信安全技术指南》、YD/T 3737-2020 《基于公众电信网的联网汽车信息安全技术要求》和 YD/T 3594-2019《基于 LTE 的车联网通信安全技术要求》等 3 项通信行业标准。

身份认证标准主要规范车联网数字身份认证相关的证书格式、证书应用和管理、安全认证技术及测试方法等技术要求。目前已发布 GB/T 37376-2019《交通运输 数字证书格式》、YD/T 3957-2021《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》等标准，正加紧编制《基于 LTE 的车联网无线通信技术 安全认证测试方法》《汽车数字证书应用规范》等标准。这些标准规定了国内车联网安全证书体系架构、证书格式和证书申请过程等。

同时，针对车联网网络部署中的两大难点，即如何将不同运营模式下的车载设备进行统一管理的问题，以及如何快速识别出车辆出现的异常情况，如何将异常行为检测与证书撤销进行关联的问题，目前 CCSA 分别制定行标《C-V2X 车联网认证授权系统技术要求》和《C-V2X 车辆异常行为管理技术要求》，来规范车联网设备的认证和授权，管理车辆异常行为。在 C-V2X 直通链路上，因为车联网具有车辆的高移动性、网络拓扑频繁变化等特性，甚至在严重情况下可能危害车辆和行人的道路安全和人身安全。

随着车联网业务的不断发展，联网通信面临拒绝服务、中间人攻击、用户跟踪等多种可能的安全威胁，这些威胁将影响 C-V2X 业务的正常运行。因此，C-V2X 需要轻量化的身份认证和完善访问授权机制以提高通信效率的同时保证安全性，同时，隐私保护也是车联网系统中的重要要求。因此，更需要针对 NR-V2X 安全、隐私保护方向、云边协同的车联网安全技术等制定安全标准。

3.5. 数据安全标准

数据安全标准主要规范智能网联汽车、车联网平台和车载应用服务等的数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护和应用数据安全等方面。通用安全要求标准主要是在采集、共享、传输等生命周期各个环节制定相关标准规范数据处理活动。分类分级标准主要规范车联网数据分类分级保护要求，制定数据分类分级的维度、方法、示例等标准，明确重要数据类型和安全保护要求。数据出境安全标准主要规范车联网行业依法依规落实数据出境安全要求，包括数据出境安全评估要点、评估方法等标准。个人信息保护标准主要规范车联网用户个人信息保护机制及相关技术要求，明确用户敏感数据和个人信息保护的场景、规则、技术方法，包括匿名化、去标识化、数据脱敏、异常行为识别等标准。应用数据安全标准主要规范车联网相关应用所开展的数据采集和处理使用等活动，包括车联网平台、网约车、车载应用程序等数据安全标准。

目前，在通用要求、数据分类分级、个人信息保护方面，已发布 GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》、YD/T 3751-2020 《车联网信息服务 数据安全技术要求》、YD/T 3746-2020《车联网信息服务 用户个人信息保护要求》、T/CSAE 211-2021《智能网联汽车数据共享安全要求》等标准。就如何系统化对车联网领域的数据进行分类和分级管理方面，T/CAAMTB 34-2021《智能网联汽车数据格式与定义》中引入了数据安全等级的定义，在该团队标准中定义的近 200 个数据字段都设置了数据安全等级。

同时，正加紧编制《智能网联汽车 数据通用要求》《智能网联汽车 数据安全管理体系规范》等通用要求标准，《车联网服务平台安全保护要求》《车联网重要数据和核心数据识别规范》《车联网领域数据安全保护要求》等数据分类分级标准，《车联网数据跨境流动安全管理要求》《车联网数据跨境流动安全评估规范》等数据出境安全标准，《基于移动互联网的汽车用户数据应用与保护技术要求》《基于移动互联网的汽车用户数据应用与保护评估方法》等个人信息保护标准，《信息安全技术 网络预约汽车服务数据安全指南》《车联网信息服务 数据安全保护能力评估规范》等应用数据安全标准。

车联网数据安全贯穿于智能网联汽车、通信网络、手机 APP 以及服务平台等之间的各个互联互通过程，数据安全防护目标复杂多样，规模和价值急剧提升，近年来已成为黑客的重点攻击目标，任一过程管理不严或者数据防护不当都会导致被窃取或非法篡改，造成用户数据泄露或损坏，侵犯个人隐私、侵害企业权益。面对以上威胁，更需要从数据分级、数据存储、数据处理和数据上传等多个方面加快制定标准来保障车联网的数据安全。

3.6. 应用服务安全标准

应用服务安全标准规范车联网服务平台和应用程序的安全要求，包括平台安全、应用程序安全和服务安全等方面，确保在典型业务应用场景下的安全性。

平台安全标准主要规范车联网信息服务平台、远程升级（OTA）服务平台、边缘计算平台、电动汽车远程信息服务与管理等安全防护与检测要求。目前已发布 GB/T 40855-2021《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》、YD/T 3752-2020《车联网信息服务平台安全防护技术要求》、T/CCSA 339—2021《车联网网络安全防护定级备案实施指南》、T/CCSA 441-2023《车联网服务平台网络安全防护要求》、T/CCSA 480-2023《车联网在线升级（OTA）安全技术要求与测试方法》。其中，《车联网网络安全防护定级备案实施指南》《车联网服务平台网络安全防护要求》为实施车联网服务平台网络安全防护定级备案及分级防护的指导标准，为企业落实车联网网络安全防护要求提供依据。同时，《车联网网络安全防护定级备案实施指南》《车联网服务平台网络安全防护要求》等团体标准对应的行业标准/国家标准已经完成立项申请，正加紧制定中。同时还需推动车联网远程监控平台网络安全技术要求等标准的立项研制。

应用程序安全标准主要规范车联网应用软件等安全防护与检测要求，目前已发布 T/CCSA 481-2023《车联网应用软件通用安全技术规范》团体标准，对应的行业标准也已经完成立项，正加紧制定中。同时《车载移动应用人机交互安全体验要求和测试方法》也在报批中。

服务安全标准主要规范车联网典型业务服务场景下的安全要求，包括汽车远程诊断、高级辅助驾驶、车路协同等服务安全要求，该部分的标准均有待制定。

总体来看而言，车联网平台安全和应用程序安全方面，已经针对具体业务场景下不同服务等现状进行了较为全面的布局，正加紧编制和预研究，但随着技术的发展和更新，仍需不断完善，填补空白。后续 2~3 年内的标准建设目标，应定位在标准体系的初步充实完备上。按《车联网网络安全和数据安全标准体系建设指南》的规划，加快相关标准的制定，对待制定的标准项目，推动尽快立项制定。

3.7. 安全保障支撑标准

安全保障与支撑标准涵盖安全风险评估、安全监测与应急管理和安全能力评估等方面，为车联网网络安全管理和支撑提供相关的安全要求和准则。

风险评估标准方面，目前，正加快编制《车联网网络安全风险评估规范》《车联网网络安全风险分类分级指南》《车联网密码应用安全评估要求》等行业标准。

安全监测与应急管理标准方面，在研国标共有 7 项，包括《车联网网络安全

异常行为检测机制》《汽车信息安全应急响应管理规范》《道路车辆 信息安全工程》《道路车辆 信息安全工程审核指南》《汽车网络安全入侵检测技术规范》《汽车安全漏洞分类分级规范》《车联网安全管理接口规范》等。其中《车联网安全管理接口规范》为企业平台和国家平台的安全对接提供规范依据。同时，在研通信行业标准包括《车联网安全管理平台通用技术要求》《车联网卡实名登记系统技术要求》《车联网网络安全能力成熟度模型》《车联网网络安全风险分类分级指南》等，其中《车联网安全态势感知系统与监管平台接口技术要求》行标报批稿已公示结束，现进入正式发布流程。

建议加快风险评估和安全监测与应急管理标准研制步伐促使标准尽快发布实施，特别是推动《车联网安全管理接口规范》《汽车安全漏洞分类分级规范》《车联网网络安全风险分类分级指南》等重点标准的研制和发布，完善车联网网络安全保障能力。同时，加快车联网卡实名制管理、车联网风险评估、车联网安全能力评估等方面的标准，为实现车联网终端与设施网络安全、网联通信安全、应用服务安全、数据安全提供保障与支撑基础。

4. 工作建议

4.1. 立足强化风险应对提升标准研判能力

随着汽车电动化、网联化、智能化交融发展，车辆开放连接逐渐增多，“车、路、云、网”数据交互日益频繁，车联网网络安全、数据安全、车辆行驶安全、产业安全等方面风险交织叠加，非法控车、恶意调度、产线入侵、数据泄露等网络安全新威胁不断涌现，车联网安全形势日趋严峻复杂。在车联网安全产业发展的关键期，面对挑战，应积极开展风险分析和应对工作，坚持问题导向、需求导向、目标导向，及时提炼并总结车联网安全风险趋势和特点，不断优化重点标准研制方向，积极推进已有标准的修订完善和亟需标准的立项研制，进一步提升车联网安全标准的引领性、及时性、有效性，指导企业夯实安全防护能力，发挥标准保障车联网产业安全发展的重要作用。

4.2. 持续夯实标准体系建设和迭代更新

应建立车联网安全标准协调推进工作机制，统筹协调各标准委员会车联网安全标准立项、技术归口等工作，加大产学研用资源凝聚力度，广泛吸纳相关单位参与，加强标准化工作对网络安全技术在车联网领域深入应用的支撑力度。紧密结合国内外车联网安全技术和产业发展新动态、新趋势，持续提炼梳理车联网安

全标准新需求，启动面向未来的前瞻性标准预研。加强对标准实施情况的监督和评估，及时识别标准实施中暴露的问题，并在现有标准体系的基础上迭代更新，保障车联网安全标准对车联网产业高质量安全发展的持续推动作用。

4.3. 加强标准宣传推广和符合性评估

应充分发挥政府部门、产业组织引导作用，建立完善、高效的标准宣贯及培训机制，及时开展车联网安全标准体系和重点标准的宣讲、培训和推广，向相关企业和机构解读标准和评估方法，帮助产业各方深刻理解车联网安全标准化的发展现状和未来规划并落实标准要求。应针对终端与设施网络安全、网联通信安全、数据安全、应用服务安全等领域重点标准开展试验验证和试点示范，汇聚优秀应用案例。以此为基础建立并不断完善标准符合性评估体系，制定明确的评估指南和实施细则，完善认证程序，研发高效、方便的评估工具，培育车联网安全标准符合性评估、测试、咨询能力。

4.4. 加大标准化人才培养力度

应建立标准化人才培养体系，制定培养计划和培养方案，开展课程学习、研讨会、实践培训等多种教育培训方式。高校、科研机构、企业等应加强协作，联合建立标准化人才培养基地，打造标准化教育和培训中心。建立标准化人才评价机制，制定评价标准和方法，开展标准化人才评估和认证，为企业和市场提供高层次标准化人才。建立标准化人才激励机制，在职称晋升、薪资待遇、荣誉表彰等方面给予侧重支持，为标准人才加强职业发展和成长空间。加强国际标准化人才的培养和引进，提升参与国际标准化工作的能力。

4.5. 深度参与车联网安全国际标准化工作

积极参与国际标准化组织（ISO）、国际电信联盟（ITU）、国际电工技术委员会（IEC）、联合国世界车辆法规协调论坛（WP.29）等相关国际标准化组织的标准制定工作。依托我国智能网联汽车产业整体优势及标准体系建设成果，深度参与国际标准的研究和编写，牵头起草重点国际标准与法规，提升我国标准成果的国际转化率和影响力。全面、深入参与国际标准法规的交流与协调，依托汽车产业对话机制与标准化合作框架，加强与国际主要汽车产业国家、地区及“一带一路”沿线国家的交流合作。

附件一：国际车联网安全标准清单

序号	组织	名称	发布时间
1	ISO/SAE	21434 ROAD VEHICLES-CYBERSECURITY ENGINEERING 道路车辆-网络安全工程	2021.8.31
2	SAE	Cybersecurity for Commercial Vehicles	2018.08.28
3	ISO	TR 4804-Road vehicles-Safety and cybersecurity for automated driving systems-Design, verification and validation	2020.12.01
4	SAE	EPR2020013-Unsettled Topics Concerning Airworthiness Cybersecurity Regulation	2020.8.31
5	SAE	EPR2020026 - Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity	2020.12.10
6	SAE	J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	2016.01.01
7	NEMA	NEMA TS 10-Connected Vehicle Infrastructure-Roadside Equipment	2020.01.01
8	DS	DS/ISO/TR 23786-Road vehicles-Solutions for remote access to vehicle-Criteria for risk assessment	2019.09.19
9	ISO	ISO TR 23786 - Road vehicles-Solutions for remote access to vehicle-Criteria for risk assessment	2019.09.01
10	NEMA	NEMA TS 8－智能交通系统 （ITS） 的网络和物理安全	2018.01.01
11	UNECE WP.29	UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system	2020.6
12	UNECE WP.29	UN Regulation No. 156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system	2020.6
13	UNECE WP.29	UN Regulation No. 157 Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems	2020.6
14	ISO/SAE	ISO/SAE 21434-2021 Road vehicles-Cybersecurity engineering	2021.8
15	SAE	SAE J3061 Cybersecurity Guidebook for Cyber-Physical	2021.12

		Vehicle Systems	
16	ISO/PAS	ISO/PAS 5112:2022 Road vehicles- Guidelines for auditing cybersecurity engineering	2022.3
17	ISO	ISO 24089:2023 Road vehicles-Software update engineering	2023.2
18	ITU-T	ITU-T X.1371 Security threats to connected vehicles	2022.05.29
19	ITU-T	ITU-T X.1372 Security guidelines for vehicle-to-everything (V2X) communication	2020.03.26
20	ITU-T	ITU-T X.1373 Secure software update capability for intelligent transportation system communication devices	2017.03.30
21	ITU-T	ITU-T X.1374 Security requirements for external interfaces and devices with vehicle access capability	2020.10.29
22	ITU-T	ITU-T X.1375 Guidelines for an intrusion detection system for in-vehicle networks	2020.10.29
23	ITU-T	ITU-T X.1376 Security-related misbehaviour detection mechanism using big data for connected vehicles	2021.01.07
24	ITU-T	ITU-T X.1377 Guidelines for an intrusion prevention system for connected vehicles	2022.10.14
25	3GPP	22.885 study on LTE support for Vehicle to Everything(V2X) services	2015.12.21
26	3GPP	36.785 Vehicle-to-Vehicle(V2V) services based on LTE sidelink; User Equipment(UE) radio transmission and reception	2016.10.12
27	3GPP	36.786 Vehicle-to-Everything(V2X) services based on LTE ; User Equipment(UE) radio transmission and reception	2017.3.31
28	3GPP	36.885 Study on LTE-based V2X services	2016.6.20
29	3GPP	22.185 service requirement for V2X services	2022.4.1
30	3GPP	37.885 study on evaluation methodology of new vehicle-to-Everything V2X use cases for LTE and NR Rel15	2019.6.24
31	3GPP	23.303 Proximity-based services (ProSe)	2023.6.21
32	3GPP	22.186 Enhancement of 3GPP support for V2X scenarios	2022.4.1
33	3GPP	22.886 study on enhancement of 3GPP support for 5G V2X services	2018.12.21
34	3GPP	38.885 Study on NR Vehicle-to-Everything (V2X)	2019.3.28

附件二：国内车联网安全标准清单

序号	标准名称	标准号/计划号	状态
100 总体与基础共性			
101 术语和定义			
1	车联网网络安全通用术语和定义		待制定
102 总体架构			
2	车联网网络安全总体架构		待制定
103 密码应用			
3	车联网密码应用通用要求	2023-0701T-YD	制定中
4	汽车密码技术要求	GB	制定中
5	车路协同通信密码应用技术要求	2023-0694T-YD	制定中
6	车云通信密码应用基本要求	H-202204243894	制定中
7	车联网通信设备密码应用技术要求		待制定
8	车联网服务平台密码应用基本要求		待制定
200 终端与设施网络安全			
201 车载设备网络安全			
9	汽车网关信息安全技术要求及试验方法	GB/T 40857-2021	已发布
10	车载信息交互系统信息安全技术要求及试验方法	GB/T 40856-2021	已发布
11	汽车芯片信息安全技术规范	GB/T	制定中
12	车载可插卸物联网设备安全防护及检测要求	H-202207294262	制定中
13	智能网联汽车环境智能感知算法安全评测规范	2022-1491T-YD	制定中
14	基于移动互联网的数字车钥匙信息安全技术要求	2019-1022T-YD	已报批
15	V2X 车载通信单元基于通用引导架构的安全证书管理功能技术要求	H-202303076217	制定中
16	汽车电子控制单元网络安全防护技术要求		待制定
17	汽车安全芯片技术要求及试验方法	QC/T	制定中
18	车载计算平台网络安全技术要求		待制定
19	智能网联汽车车载端信息安全技术要求	T/CSAE 101—2018	修订中
20	智能网联汽车车载端信息安全测试规程	T/CSAE 252—2022	已发布
21	智能网联汽车人机交互安全测试评价规程	T/ITS 0221-2022	制定中
202 车载网络安全			
22	汽车电子系统网络安全指南	GB/T 38628-2020	已发布
23	汽车信息安全通用技术要求	GB/T 40861-2021	已发布
24	电动汽车充电系统信息安全技术要求及试验方法	GB/T 41578-2022	已发布
25	汽车软件升级通用技术要求	20214423-Q-339	制定中
26	汽车整车信息安全技术要求	20214422-Q-339	制定中
27	道路车辆-信息安全工程	20230389-T-339	制定中
28	汽车诊断接口信息安全技术要求及试验方法	20211169-T-339	制定中
29	基于公众电信网的车载远程通信终端网络安全技术要求	2021-1065T-YD	制定中
30	汽车网络安全域及防护层级化定义		待制定

31	车载总线系统网络安全技术要求		待制定
32	车载以太网网络安全技术要求		待制定
33	车载操作系统及应用软件安全防护要求		待制定
34	汽车电子外部接口网络安全技术要求		待制定
203 路侧通信设备网络安全			
35	车联网设备安全技术要求及检测方法 路侧无线通信设备	H-202211305485	制定中
36	车联网设备安全技术要求及检测方法 路侧计算设备	H-202211305483	制定中
37	面向车联网应用的算力网络安全指南	H-202304076460	制定中
38	车联网网络关键设备安全技术及检测要求 路侧检测与信息服务设备		待制定
204 网络设施与系统安全			
39	智能网联汽车时空数据传感系统安全检测基本要求	20230947-Q-334	制定中
40	面向车路协同的车云互联安全技术要求	H-202303136232	制定中
41	车联网网络设施与系统安全防护要求		待制定
42	车联网网络设施与系统安全检测要求		待制定
300 网联通信安全			
301 通信安全			
43	车联网无线通信安全技术指南	YD/T3750-2020	已发布
44	基于公众电信网的联网汽车信息安全技术要求	YD/T3737-2020	已发布
45	基于 LTE 的车联网通信安全技术要求	YD/T3594-2019	已发布
46	基于 NR-V2X 的车联网无线通信安全技术要求	H-202204243899	制定中
47	车联网网络安全接入技术要求		待制定
48	面向车联网的卫星通信安全技术要求		待制定
49	车联网汽车短程通信接口安全技术规范		待制定
302 身份认证			
50	交通运输 数字证书格式	GB/T 37376-2019	修订中
51	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	YD/T 3957-2021	已发布
52	车联网数字证书应用接口规范	2023-0705T-YD	制定中
53	基于 PKI 的车联网应用服务安全认证体系框架	2023-0714T-YD	制定中
54	智能网联汽车数字身份及认证通用规范	20221429-T-312	制定中
55	基于 LTE 的车联网无线通信技术 安全认证测试方法	2019-0022T-YD	制定中
56	汽车数字证书应用规范	GB/T	制定中
57	C-V2X 车联网认证授权系统技术要求	2021-0580T-YD	制定中
58	车联网服务 V2X 安全证书应用接口规范		待制定
59	车联网 V2X 密钥管理系统技术规范		待制定
60	电子驾驶证安全技术要求		待制定
61	车联网关键部件轻量级安全认证通用技术要求		待制定
62	面向车路协同的通信证书管理技术规范	T/ITS 0127-2020	已发布
400 数据安全			
401 通用要求			
63	信息安全技术 汽车数据处理安全要求	GB/T 41871-2022	已发布

64	智能网联汽车数据通用要求	20213606-T-339	制定中
65	智能网联汽车数据安全管理体系规范	GB/T	制定中
66	智能网联汽车数据安全共享模型与规范		待制定
67	智能网联汽车数据安全共享参考架构		待制定
68	智能网联汽车数据安全要求		待制定
69	智能网联汽车时空数据安全处理基本要求	20230949-Q-334	制定中
70	智能网联汽车数据保护密码应用技术要求		待制定
71	车联网数据安全保护能力参考框架	2023-0702T-YD	制定中
72	车联网安全监测数据采集技术要求及测试方法	H-202112273507	制定中
402 分类分级			
73	车联网信息服务 数据安全技术要求	YD/T 3751-2020	已发布
74	车联网服务平台重要数据记录系统技术规范		待制定
403 数据出境安全			
75	车联网数据跨境流动安全管理要求	2023-0704T-YD	制定中
76	车联网数据出境流动安全评估规范	2023-0703T-YD	制定中
77	车联网数据跨境流动安全评估规范		待制定
404 个人信息保护			
78	车联网信息服务 用户个人信息保护要求	YD/T 3746-2020	已发布
79	基于移动互联网的汽车用户数据应用与保护技术要求	2018-0182T-YD	制定中
80	基于移动互联网的汽车用户数据应用与保护评估方法	2018-0183T-YD	制定中
81	车联网个人信息安全保护要求及测评方法	2023-0696T-YD	制定中
82	车联网用户个人信息合规检测要求		待制定
405 应用数据安全			
83	信息安全技术 网络预约汽车服务数据安全要求	GB/T 42017-2022	制定中
84	网络预约出租汽车服务平台数据安全防护要求	2017-0938T-YD	制定中
85	车联网信息服务 数据安全保护能力评估规范	2020-1317T-YD	制定中
86	车联网数据和个人信息脱敏实施规范	H-202303086223	制定中
87	车联网应用服务 数据脱敏实施方法		待制定
500 应用服务安全			
501 平台安全			
88	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 40855-2021	已发布
89	车联网信息服务平台安全防护技术要求	YD/T 3752-2020	已发布
90	车联网密码应用安全监测平台技术要求	2023-0699T-YD	制定中
91	车联网信息服务平台安全防护检测要求	2021-0192T-YD	制定中
92	车联网在线升级（OTA）安全技术要求与测试方法	T/CCSA 480-2023	已发布
93	车联网安全态势感知平台技术要求	2021-0944T-YD	制定中
94	车联网服务平台通信安全保障技术要求		待制定
95	车联网网络安全防护定级备案实施指南	T/CCSA 339—2021	已发布
96	车联网网络安全防护定级备案实施要求	H-202106102110	制定中
97	车联网服务平台网络安全防护要求	T/CCSA 441—2023	已发布

98	车联网服务平台网络安全防护要求	G-202106100081	制定中
99	车联网服务平台安全接入技术要求	H-202204083808	制定中
100	车联网远程监控平台网络安全技术要求		待制定
502 应用程序安全			
101	车联网应用软件通用安全技术规范	T/CCSA 481-2023	已发布
102	车联网应用软件安全技术规范	2023-0713T-YD	制定中
103	车载移动应用人机交互安全体验要求和测试方法	2020-1863T-YD	制定中
503 服务安全			
104	车联网服务平台与车载终端交互安全技术要求		待制定
105	车联网汽车远程诊断服务网络安全技术要求		待制定
106	车联网高级辅助驾驶系统与远程平台交互网络安全技术要求		待制定
107	车联网车路协同服务网络安全技术规范		待制定
600 安全保障与支撑			
601 风险评估			
108	车联网网络安全风险评估规范	2023-0707T-YD	制定中
109	车联网网络安全风险分类分级指南	2023-0706T-YD	制定中
110	车联网密码应用安全评估要求	H-202207294268	制定中
602 安全监测与应急管理			
111	汽车信息安全应急响应管理规范	20213611-T-339	制定中
112	车联网安全管理接口规范	G-202106090080	制定中
113	车联网安全管理平台通用技术要求	2023-0695T-YD	制定中
114	车联网密码应用安全监测平台通用技术要求	2023-0700T-YD	制定中
115	车联网网络安全异常行为检测机制	20221740-T-339	制定中
116	C-V2X 车辆异常行为管理技术要求	2021-0187T-YD	制定中
117	汽车网络安全入侵检测技术规范	GB/T	制定中
118	车联网安全态势感知平台技术要求	2021-0944T-YD	制定中
119	车联网安全态势感知平台与监管平台接口技术要求	2021-1053T-YD	制定中
120	车联网网络安全信息共享要求		待制定
121	车联网网络安全应急管理要求		待制定
122	车联网系统安全漏洞分类分级指南	2023-0712T-YD	制定中
123	车联网卡实名登记系统技术要求	2023-0698T-YD	制定中
124	车联网卡实名登记及人像比对技术要求		待制定
125	车联网卡实名登记及人像比对测试规范		待制定
126	车联网业务 HI 接口总体技术要求		待制定
127	车联网业务 HI 接口技术实施要求		待制定
128	车联网业务 HI 接口测试方法		待制定
129	车联网网络安全能力成熟度模型	2023-0709T-YD	制定中
130	车联网网络安全能力成熟度评价准则	2023-0711T-YD	制定中
131	车联网网络安全能力成熟度评估实施方法	2023-0710T-YD	制定中
132	车联网网络安全服务机构能力认定准则	2023-0708T-YD	制定中
133	车联网供应链网络安全风险管理准则	2023-0697T-YD	制定中
134	道路车辆 信息安全工程审核指南		待制定

135	车联网网络安全 设计文档分类与定义		待制定
136	车联网网络安全防护要求	T/TIAA 015-2019	已发布

注：所有“待制定”状态的标准为工业和信息化部在 2022 年 2 月发布的《车联网网络安全和数据安全标准体系建设指南》中的“车联网网络安全和数据安全相关标准项目明细”。