《智能网联汽车网络安全技术要求》（送审稿）

编制说明

一、项目背景

目前我国智能网联汽车产业进程走在世界前列，得到政策大力支持。从2010年以车载信息娱乐服务为核心的“车联网”概念的萌芽，到2016年以行车安全为核心的智能网联技术路线的提出，再到2017LTE-V2X标准的确定开启商业化进程，从2020年开始5G逐步替代LTE实现更高级别的自动驾驶，至今，智能网联汽车产业经历了10余年摸索，产业路径逐渐清晰，产业前景渐明。

在国家政策层面，从国家安全战略的层面强调加快提升网络安全、数据安全、人工智能安全等领域的治理能力。《国家综合立体交通规划纲要》和《增强制造业核心竞争力三年行动计划》提出推进智能网联汽车应用、推动关键技术产业化的基调，智慧城市基础设施与智能网联汽车协同发展试点工作的开展，落实了智能网联汽车的落地示范和应用，新能源汽车产业发展规划明确提出了打造网络安全保障体系的要求，智能汽车创新发展战略提出了完善安全管理联动机制、提升网络安全防护能力、加强数据安全监督管理等具体要求，智能网联汽车产业发展行动计划也提出了对信息安全的要求，对智能网联汽车生产企业及产品准入管理强调了数据安全管理能力和网络安全保障能力的要求，智能网联汽车道路测试与示范应用管理规范对网络安全保障能力和风险评估做了要求。

在智能网联汽车相关标准体系方面，国家有关部门出台了智能网联汽车产业标准体系建设指南，分别从总体要求、信息通信、电子产品和服务、车辆智能管理、智能交通相关、智能网联汽车等角度提出标准化体系。

在智能网联汽车网络安全政策方面，2021 年开始，工信部开始注重加强车联网（智能网联汽车）网络安全管理，计划落实安全主体责任，全面加强安全保护。网信办开始加强对汽车数据安全的管理，标准方面车联网（智能网联汽车）网络安全标准体系建设指南也将出台。

此外，在地方级政策方面，当前，各省市及地区都在推进汽车产业“数字化、智能化、网联化”发展，产业借助政府政策营造市场氛围、创造市场需求。目前，深圳市智能车路协同管控设计与实践已取得良好实践成效。深圳作为智能网联汽车的示范城市之一，为促进和加快智能网联汽车产业的发展，目前已公布《深圳

经济特区智能网联汽车管理条例》，须结合智能网联汽车网络安全发展前景，参考产业落地实践经验，重点解决智能网联汽车网络安全方面的问题，建立《深圳市智能网联汽车网络安全标准（框架）》等标准文件。

然而，针对智能网联汽车的网络安全管理、建设的法规及标准有所缺失。当前，智能网联汽车的网络安全问题不容忽视。在网络安全领域，随着汽车智能化、网联化发展，遭受网络攻击、网络侵入的风险将会大幅增加。此外，由于汽车处于高速行驶状态，并且正在逐步成为构建智能交通、智慧城市的关键要素，以及存贮消纳能源的重要载体，其网络安全风险更大。统计显示，2020 年全球针对智能网联汽车的攻击达到 280 余万次。

面对日益严峻的智能网联汽车网络安全形势，需要通过建立完善的智能网联汽车网络安全标准。通过建立完善的智能网联汽车网络安全技术要求，让智能网络汽车生产、运营、使用、监管单位有标可循、有技可依。推进加快智能网联汽车网络安全防护体系建设，推动智能网联汽车网络安全风险评估与应急响应机制、智能网联汽车网络安全监测预警、关键设备及平台网络安全能力测评等相关配套平台落地实践,提升智能网联汽车产业网络安全防护能力，推动深圳市智能网联汽车网络安全管理水平，提升整体技术水平、竞争力以及智能网联汽车在深圳市的落地保障。

二、工作简况

1、任务来源

本标准由深圳市市场监督管理局于2022年4月28日批准立项，立项名称为《智能网联汽车网络安全技术要求》。

本标准由深圳市政务服务数据管理局提出并归口。

2、主要起草过程

2021 年 11 月 18 日，成立标准编制工作组，启动标准研究及编制工作，明确标准需求、时间表、成果要求等。

2021 年 12 月至 2022 年 1 月，开展市场调研。调研深圳市智能网联汽车监管部门、汽车制造企业、智能网联汽车相关研究机构、相关平台等产业链上下游，了解深圳市智能网联汽车推广落地情况，信息系统及网络现状，安全需求形成调研报告，给出标准工作规划。

2022 年 1 月至 2 月，标准预研。调研国际国内关于智能网联汽车、自动驾

驶、汽车终端网络安全、云端平台网络安全、个人信息保护、数据安全、通信安全、应用安全等领域的相关法律法规和标准规范，结合深圳市智能网联汽车网络安全现状及需求，确定地方标准定位、范围、规范对象等。聚焦智能网联汽车涉及的核心技术、网络安全技术等，完成项目相关模型和前沿技术的研究，实现对技术的上层抽象和提取。

2022 年 3 月，形成标准草案。结合前期预研和技术研究成果，组织参编单位和编写人员形成标准草案。

2022 年 4 月，完成标准草案的第一轮征求意见，收到产业界三个代表单位的意见反馈，经分析研讨，完成标准草案的修订。

2022 年 6 月，进行第二轮征求意见，收到产业界五个代表单位的意见反馈，经分析研讨，完成标准草案的二次修订。

2022 年 6 月 23 日召开专家咨询会，对标准草案进行质询讨论，最终得到与会专家一致通过，形成送审材料。

三、编制原则及技术依据

1、编制原则

通用性：按照本标准实现的公共数据安全技术要求，实现了公共数据在数据安全通用安全、数据处理活动中可能涉及的风险进行覆盖。

实用性：根据我国有关法律法规、政策文件、标准规范等编制本标准，使其在指导公共数据保护方面具有很强的实用性。

符合性：符合国家有关法律法规和已有标准规范的相关要求。

2、编制依据

a）标准格式按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

b）本标准制定依据以下规范性引用文件：

GB/T 25069—2022　信息安全技术　术语

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 40861—2021　汽车信息安全通用技术要求

c）本标准制定参考以下文献：

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 38628—2020　信息安全技术　汽车电子系统网络安全指南

GB/T 40855—2021　电动汽车远程信息服务与管理系统信息安全技术要求

GB/T 40857—2021　汽车网关信息安全技术要求及测试方法

DB4403/T 271—2022　公共数据安全要求

YDB 102—2012　通信网支持智能交通系统总体框架

YDB 124—2013　车联网总体技术要求

3、**对标情况**

本标准主要围绕深圳市智能网联汽车网联的网络安全要求，内容包括智能网联汽车车载设备安全要求、通信安全要求、应用服务安全要求、数据安全要求、网络安全保障要求，主要参照了工信部于2022年2月25日发布的智能网联汽车网络安全和数据安全标准体系建设指南中提到的为贯彻《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》，根据《新能源汽车产业发展规划（2021-2035年）》《车联网（智能网联汽车）产业发展行动计划》《汽车数据安全管理若干规定》《关于加强车联网网络安全和数据安全工作的通知》要求，工业和信息化部在现有国家智能网联汽车产业标准体系的要求基础上，结合深圳市市场发展的特点，以需求为导向，聚焦深圳市主要业务的发展方向，聚焦重点、急用先行。

其中与国家及行业标准存在的主要差异点包括：

1）总体安全框架设计不同，智能网联汽车网络安全和数据安全标准体系建设指南中把标准体系建设分为总体于基础共性、终端于设施网络安全、网联通信安全、数据安全、应用服务安全和安全保障于支撑6大部分。本标准在充分考虑各个部分的目标于建设方向的基础上，定义了适合深圳市智能网联汽车发展规划的网络安全总体框架，在共性技术、车载设备安全、通信安全、应用服务安全、数据安全和网络安全保障这些方面进行了详细技术要求说明。

2）标准内容方面:

总体与基础共性标准部分是智能网联汽车网络安全和数据安全的总体性、通用性和指导性标准，本标准在密码安全和算法安全进行了详细的技术规定，并调整到网络安全保证章节；终端与设施网络安全标准部分，本标准的主要要求方向在车载设备和路侧设备的通信安全要求，路侧设备自身的安全要求不在本标准的要求范围内；网联通信安全部分除满足通信安全要求和身份认证，本标准在车内网络通信也进行了相应的技术要求；数据安全部分，本标准依据公共数据级别划分基本要求，

数据安全相关国家标准均未按照此方式明确标准内容；例如 GB/T 37988—2019 主要围绕数据生命周期及安全管理要求，本标准除数据生命周期及基本安全管理要求外，还增加技术安全要求。

3）本标准在参考或引用相关标准基础上，结合深圳市智能网联汽车的网络安全实际需求，提出了基本的安全要求。

四、主要条款说明

为了确保智能网联汽车的网络安全，完善智能网联汽车自主研发体系，制定智能网联汽车和其他设备网络安全相关标准，落实相关能力及防护措施，以提升智能网联汽车产业网络安全防护能力，特制定本标准。智能网联汽车网联安全技术要求除应符合本标准外，还应符合国家、行业及深圳市现行法律、行政法规、标准等规定。本标准拟提出智能网联汽车网联安全技术要求内容如下：

前言

1 范围

本标准提出了智能网联汽车网络安全总体框架，规定了智能网联汽车车载设备安全要求、智能网联汽车通信安全要求、智能网联汽车应用服务安全要求、智能网联汽车数据安全要求、智能网联汽车网络安全保障要求。

本标准适用于指导智能网联汽车相关生产方、运营方、服务提供方等对智能网联汽车网络安全的建设和实施。

2 规范性引用文件

本章节输出了标准编制过程中引用的相关文件。

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本标准。

4 缩略语

本章节输出了标准编制过程中引用的相关缩略语。

5 智能网联汽车网络安全总体框架

智能网联汽车网络架构主要根据智能网联汽车的基本构成进行划分，分为智能网联汽车车载设备安全要求、智能网联汽车通信安全要求、智能网联汽车数据安全要求、智能网联汽车应用服务安全要求和智能网联汽车网络安全保障要求。智能网联汽车网络标准框架主要涵盖以下部分，主要描述标准框架的组成关系，分别对每

个层级的安全措施提出要求。

6 智能网联汽车车载设备安全要求

规范了智能网联汽车设备安全要求，包括安全启动、操作系统、硬件安全模块、接口安全、入侵检测方面的安全要求。

7 智能网联汽车通信安全要求

规范了智能网联汽车车内通信安全要求、车外通信安全要求，实现针对安全隔离、安全防护的车内通信安全，以及针对有线通信、近距离无线通信、蜂窝网络通信、V2X 通信的车外通信安全。

8 智能网联汽车应用服务安全要求

规范了车载应用安全、联网平台安全。

9 智能网联汽车数据安全要求

规范了智能网联汽车数据处理活动中的安全要求，数据处理活动围绕数据采集、存储、传输、使用、共享、销毁环节。

10 智能网联汽车网络安全保障要求

规范了智能网联汽车网络安全保障要求，包括密码安全、算法安全、风险评估、安全监测、应急响应要求。

五、知识产权情况说明

本标准不涉及专利及知识产权问题。

六、重大意见分歧的处理依据和结果

无。

七、实施标准的措施建议

无。

八、其它应予说明的事项

无。