《智能网联汽车整车信息安全技术要求》（送审稿）编制说明

一、项目背景

伴随着汽车智能化、网联化程度的加深，人们实现了对汽车的更多控制，为生活带来了各种便利，但随之而来的远程攻击、信息泄露甚至网联车辆被操控等安全隐患也日益凸显。而智能网联汽车的信息安全事件所造成的影响，也从单一车辆扩展到大范围的车辆群体及其相关的信息系统。联合国在 2020 年 6 月正式投票通过了汽车信息安全法规，目的是通过建立清晰的实施和审核要求来帮助车企解决信息安全风险，该法规将逐渐成为汽车信息安全领域具有国际协调和有约束力的准则，为汽车行业提供智能网联汽车信息安全层面的合规指导。

为有效指导汽车行业开展整车信息安全防护工作，从整车的角度开展系统性的分析、设计、实现与验证，有必要建立和完善汽车整车信息安全技术要求与试验方法。从汽车系统开发 V 模型的角度，在设计开发环节，需要首先从整车的角度分析汽车信息安全需求，再分解到零部件层级完成进一步细化需求和设计方案；在系统集成以及试验验证过程中，在完成零部件的信息安全试验及验证后，最终需要集成到整车的角度验证其信息安全需求是否最终满足。虽然，国内多家企业已经开始了基于整车的信息安全评估工作，但仍然处于研究状态，缺乏统一的标准。因此，汽车行业迫切需要加快制定基于整车的信息安全技术标准，以帮助智能网联汽车的生产企业和相关机构更好地实现并验证整车信息安全需求。

二、工作简况

（一）任务来源

为服务产业发展，构建企业廉洁合规智能网联汽车管理等相关标准体系，助力全市经济社会高质量发展。根据《深圳市市场监督管理局关于下达深圳市地方标准计划项目任务的通知》的相关要求，受深圳市工信局的委托，中汽研软件测评（天津）有限公司组织电子科技大学等标准起草单位开展了深圳市地方标准《智能网联汽车整车信息安全技术要求》的编制研究工作，为深圳市智能网联汽车道路测试和示范应用提供标准依据。

（二）主要工作过程

中汽研软件测评（天津）有限公司于 2021 年 7 月成立了标准预研工作组，开展了行业调研和地标可信性论证工作，并牵头组织项目组成员单位召开多次项目组会议，分析了联合国等国际标准法规组织的汽车标准法规现状，讨论确定了适应中国产业发展现状的汽车整车信息安全的技术要求并编写了标准草案。

（1） 本标准作为深圳市智能网联汽车准入管理标准，应侧重考量技术的广泛性和通用性，每条技术要求的提出都应力求必要、精简凝练；

（2） 标准编写要着重考虑国际协调，对于每一条要求都要提供充分的说明，尤其是针对已有相关法规增加的条款；

（3） 对于软件升级的信息安全要求，两个项目组独立开展编写，原则是遵循 R155 及 R156 的原文，暂不考虑合并要求和协同处理，等到完成后对比是否存在重叠的要求；

（4） 对于数据与代码安全的章节，需要回归到法规原文考虑技术要求，分级分类由另外的标准编制工作组负责；

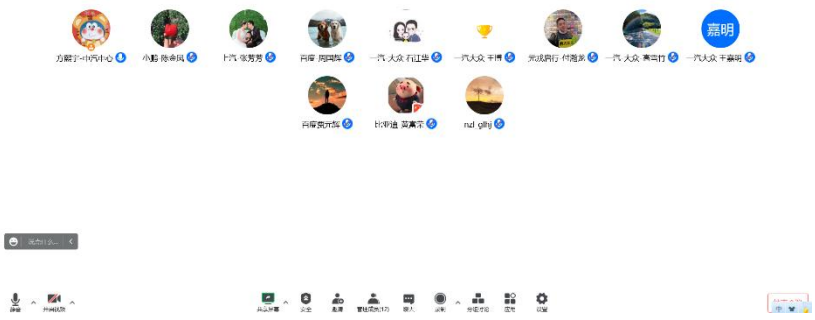


图 1 工作组线上会议

在此总体意见的基础上，项目组基于国家强制性标准《汽车信息安全技术要求》（草案），编制形成了适用于深圳市的《智能网联汽车整车信息安全技术要求》草案，并 2022 年 7 月提交地方标准立项申请。

2022 年 10 月在深圳市智能网联汽车整车信息安全标准工作组进行征集意见，收集反馈意见并召开意见协调会，形成意见处理结论。

2022 年 12 月 5 日～2022 年 12 月 9 日，通过电子邮件的方式征求了深圳市交通运输局、深圳市公安局交通警察局、深圳市发展和改革委员会、深圳市市场监督管理局、中国银行保险监督管理委员会深圳监管局、深圳市政务服务数据管理局、深圳市住房和建设局、深圳市人民政府国有资产监督管理委员会、深圳市前海深港现代服务业合作区管理局、各区政府（福田区、罗湖区、南山区、宝安区、龙岗区、坪山区、龙华区、光明区、大鹏新区、深汕特别合作区）的意见，并根据意见修改标准草案。

三、主要技术要求的依据及以及与国内领先、国际先进标准的对标情况

本文件编写符合 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。起草过程充分考虑国内外现有相关标准的统一和协调，标准的要求充分考虑了国内当前的行业技术水平，对草案内容进行多次征求意见和充分讨论。

本标准未采用国际标准，基于国内行业发展现状和管理需求自主制定。

2020 年 6 月，联合国世界车辆法规协调论坛（WP29）通过并发布 R 155《关于网络安

全和网络安全管理系统的汽车型式批准统一规定》，在网络安全管理系统的符合性证明、网络安全管理系统要求、车型要求、车型修改及扩展、生产一致性等方面做出规定，并在其附录中给出了主要的汽车网络安全风险及缓解措施。该法规已于 2021 年 1 月 1 日实施。从 2022 年 7 月起，欧盟范围内所有新车型如果不满足 R 155 将无法获取 WVTA（Whole Vehicle Type Approval）证书，无法上市销售，2024 年 7 月起制造的车辆必须满足该要求方可出厂销售。同时日本也将 R 155 纳入其汽车法规体系。

本标准主要内容包括汽车信息安全管理体系、车辆管理要求、整车信息安全技术要求及试验方法。本标准的制定借鉴联合国世界车辆法规协调论坛(UN/WP29)已发布《关于网络安全和网络安全管理系统的汽车型式批准统一规定》法规的思路，在满足政府管理需求和符合行业发展现状的基础上自主制定。

四、主要条款的说明以及主要技术指标

（一）适用范围

本文件规定了具备自动驾驶功能的智能网联汽车信息安全管理体系、车辆管理要求、整车信息安全技术要求及试验方法。

本文件适用于 M 类、N 类及至少装有 1 个电子控制单元的 O 类汽车整车及其车辆制造商等相关方，其他类型车辆可参考执行。

（二）主要技术内容

本标准主要技术内容包括6个部分，以下选择标准技术要求的部分重点内容进行说明：

第 5 章 信息安全管理体系要求

基于国内行业技术发展现状，参考 R155 法规第 7.2 章节的内容，针对如下方面提出要求：

（1）车辆制造商应建立车辆全生命周期的信息安全管理体系。

说明：本标准条款所要求的信息安全管理体系以车辆产品为核心，应覆盖车辆的全生命周期。若流程、规定等仅与企业经营管理、组织自身运营相关，并不涉及车辆产品信息安全相关话题，则不在本标准所要求的体系范围内。

（2）应建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到适当处置的流程，并确保车辆风险评估保持最新状态。

说明：本条款要求汽车生产企业针对车辆的信息安全风险进行识别、评估、分类、处置等相关管控活动，并建立相应的流程。此处的流程应能够应对车辆全生命周期的风险管控，企业可自行定义实施路线。

（3）应包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布等活动环节。

说明：本条款明确要求企业建立漏洞管理机制，并且需涵盖收集、分析、报告、处置、发布等关键环节。

第 6 章 车辆信息安全一般要求

基于国内行业技术发展现状，参考 R155 法规中第 7.3 章节的内容，及附录 5 中的部分相关内容（表 A1 4.3.4、4.3.7 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B3、B5 中有关的缓解措施），针对如下方面提出要求：

（1）车辆产品开发流程应遵循汽车信息安全管理体系要求。

说明：车辆产品应按照汽车信息安全管理体系中定义的相关流程、制度开展开发工作。

（2）识别和管理车辆与供应商相关的风险。

说明：此处“供应商”关注与车辆产品风险相关的供应商，包括合同供应商、服务提供商等。

（3）应针对车辆实施相应措施，以识别和防御针对该车辆的网络攻击、网络威胁和漏洞，并为车辆生产企业在识别与车辆相关的网络攻击、网络威胁和漏洞方面提供监测能力，以及为分析网络攻击、网络威胁和漏洞提供数据取证能力。

说明：车辆产品端应实施相应的措施，与企业在汽车信息安全管理体系中建立的网络攻击、网络威胁和漏洞的监测和响应流程进行协同，从而保障企业可以针对车辆产品进行网络攻击、网络威胁和漏洞方面的监测，并且支持数据取证。

第 7 章 车辆外部连接安全要求

基于国内行业技术发展现状，参考 R155 法规附录 5 中的相关内容（表 A1 4.3.1、4.3.5 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B4 中有关的缓解措施），针对如下方面提出要求：

（1）对具备远程控制功能系统的安全要求，包括对远程控制指令信息的真实性和完整性验证、验证失败的处理功能、对远程控制指令设置访问控制、安全日志记录、对车端远程操控功能系统的程序和配置数据的完整性验证要求等。

（2）对第三方应用安装运行的要求，第三方应用是指汽车制造商及其供应商之外的其他法人实体提供的面向用户提供服务的应用程序，包括通过应用商店或浏览器或USB等用户安装的应用软件，汽车制造商应对其授权和认可的第三方应用的真实性和完整性进行验证，防止该应用被篡改；汽车制造商应对其未授权的第三方应用的安装运行采取防护措施，如在安装时进行提示、限制其访问权限，避免非授权的第三方应用对车辆系统等的资源配置、关键参数、重要数据等进行访问。

（3）对外部接口的安全要求，包括对USB接口、诊断接口和其他接口的设备进行访问控制，禁止非授权访问。应对USB端口接入设备中的文件进行访问控制，只允许指定格式的文件读写或指定签名的应用软件安装或执行，应具备USB端口接入设备中病毒程序或携带病毒的媒体文件/应用软件的鉴别并禁止安装的能力，对通过诊断接口发送的对车辆关键参数写操作请求时，进行身份鉴别、访问控制等安全策略。

（4）对车辆外部连接系统漏洞管理的要求，包括但不限于远程控制系统、授权的第三方应用等，应不存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞，处

置措施包括消除漏洞、制定减缓措施等。

（5）对网络端口的安全要求，应关闭不必要网络端口，如TCP连接或UDP消息的逻辑信道端点等。

第 8 章 车辆通信安全要求

基于国内行业技术发展现状，参考 R155 法规附录 5 中的相关内容（表 A1 4.3.2 有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表 B1、B5 中有关的缓解措施），针对如下方面提出要求：

（1）车辆与车辆生产企业云平台通信时，应对其通信对象的身份真实性进行验证。

说明：本文件并未强制要求双向认证、也未强制要求必须使用证书保护机制。

（2）车辆与车辆、路侧单元、移动终端等进行直连通信时，应进行证书有效性和合法性的验证。

说明：本条款主要是针对V2X场景提出的要求。

（3）车辆应采用完整性保护机制保护外部通信通道。

说明：本条款主要针对能够在通信协议层面实现完整性保护机制的外部通信通道。某些外部通信通道例如 RFID、NFC 等，不适用此条款；无线传感器与车载设备之间的通信、语音交互也不适用于本条款；对于企业采用的完整性保护技术类型和强度，本文件不做具体要求。

（4）应对车辆发送的敏感个人信息实施保密性保护。

说明：本文件旨在对车辆的信息安全风险提出安全要求，具体“敏感个人信息”的定义以汽车数据安全相关管理要求和标准规定为准。

（5）车辆与外部直接通信的零部件应具备安全机制防止非授权的系统特权访问。

说明：本条款仅包含与外部直接通信的零部件，利用 T-BOX，车载信息交互系统间接与外部通信的零部件不适用于本条款的要求；射频、NFC 等短距离无线通信的传感器也不适用于本条款要求；身份识别机制包括基于密码的认证机制、DTC 记录、日志记录、异常提醒等，对外部通信零部件进行身份识别的技术可通过云端来实现。

（6）车辆应具有识别恶意的V2X数据、恶意的诊断数据、恶意的专有数据等的能力，并采取防护措施。

说明：恶意的诊断数据包括非法诊断请求、非法诊断应答、暴力请求认证、非法开启 DTC 主动上传、恶意连续复位等；本条款使用“数据”而不是消息或指令等表述方式，是为了全文统一考虑，其本身是广义的概念，可指代原文的“恶意消息”具；体恶意数据的定义由厂家决定并提供清单作为测试的输入。

（7）车辆应对关键的通信信息安全事件进行日志记录。

说明：本条款对车辆通信信息安全事件日志记录提出了要求，安全日志防护应满足第 10 章数据代码章节的要求。

第 9 章 软件升级安全要求

基于国内行业技术发展现状，参考R155法规附录5以及R156法规中的相关内容（表A1 4.3.3有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表B2中有关的缓解措施），针对如下方面提出要求：

（1）车载软件升级系统应具备安全启动的功能，应保护车载软件升级系统的可信根、引导加载程序、系统固件不被篡改，或被篡改后无法正常启动。

说明：车载软件升级系统在行业和某些企业也被称为车端 OTA Master，包括系统软件和硬件；该条款的正常启动是指车载软件升级系统默认加载程序的启动；本文件中将除默认加载程序的启动之外，均视为非正常启动。

（2）车载软件升级系统应不存在由权威漏洞平台6个月前公布且未经处置的高危及以上的安全漏洞。注：处置方式包括消除漏洞、制定减缓措施等方式。

说明：本条款的说明参见第 7 章的相关说明。

（3）在线软件升级时，车辆和在线升级服务器应进行身份认证，验证其身份的真实性，车载软件升级系统应对下载的在线升级包进行真实性和完整性校验，车载软件升级系统应记录在线升级过程中发生的失败事件日志。

说明：该条款是对在线软件升级场景（OTA 场景）提出的要求；在线升级包在解包和分发之前，需要由车载软件升级系统校验其真实性和完整性，以保证在线升级包的真实来源和未受修改，其他环节是否进行校验不在本文件中进行要求。

（4）离线软件升级时，若车辆使用车载软件升级系统进行离线升级，车辆应对离线升级包真实性和完整性进行校验，若车辆不使用车载软件升级系统进行离线升级，应采取保护措施保证刷写接入端的安全性，或者校验离线升级包的真实性和完整性。

说明：若车辆不使用车载软件升级系统进行离线升级，主要有以下两类升级方式：a）使用诊断仪等基于 OBD 端口的设备进行刷写升级；b）使用 USB 端口进行直刷（不经过车载软件升级系统）。如果采用 a）方式，要求车端刷写准入端采用如 27 服务等防护措施对诊断仪等设备进行认证之后，才能进行刷写操作；如果采用 b）方式，要求 ECU 在被刷写之前对离线升级包的真实性和完整性进行校验。

第 10 章 数据代码安全要求

基于国内行业技术发展现状，参考R155法规附录5中的部分相关内容（表A1 4.3.6有关脆弱性/威胁的描述、漏洞及攻击方法示例，以及表B5、B7、C3中有关的缓解措施），针对以下方面提出要求：

（1）车辆应安全的地存储对称密钥和私钥，防止其被非授权访问和获取。

说明：常见的安全的存储方式包括存储在 HSM、SE、TEE 等安全模块，也包括安全的软件存储形式。

（2）车辆应采取安全防御机制保护存储在车内的车辆识别代号（VIN）和用于身份识

别的数据，防止其被非授权删除和修改。

说明：此条要求中用于身份识别的数据由企业自行确定，包括直接用于身份识别的数据和组合起来间接识别身份的数据。

（3）车辆应采取安全防御机制保护存储在车内的关键数据，防止其被非授权删除和修改。

说明：关键数据由企业根据车型的业务场景和风险评估来确认。

（4）车辆应具备个人信息清除功能及防恢复机制，便于在转售、租借或报废时清除个人信息。

说明：国家要求存储在车内不允许修改的数据除外，例如 DSSAD、EDR 内存储的数据，防恢复机制在本标准中不提出强度要求，未来以数据安全标准要求的强度为准。

（5）车辆不得直接向境外传输数据。

说明：此条款主要是避免车型设计时预留了数据出境的功能或接口，导致大批量的车辆避开管理部门的监管向境外直传数据。车辆通过国内云平台中转间接向境外传递数据，用户个人行为的跨境数据传输均不受本条款的要求。

附录 A（规范性） 车辆信息安全要求测试验证方法

对测试条件、测试输入信息、车辆外部连接安全测试方法、车辆通信通道安全测试方法、车辆软件升级安全测试方法、车辆数据代码安全测试方法等内容进行了规定，并分别与正文第7章~第10章的要求条款进行对应，给出具体的通过条件。

（三）主要试验（或）验证情况分析

根据工作安排，中汽研软件测评（天津）有限公司与比亚迪汽车工业有限公司、上海汽车集团股份有限公司、广州小鹏汽车科技有限公司等单位进行了相关的标准验证的试运行工作。验证内容包括标准草案确定的体系要求和主要试验项目。由于验证内容比较多，以下仅选择有代表性的验证内容对主要验证情况进行说明。

1. 汽车信息安全管理体系审核评估结果

在审核期间，汽车生产企业依据工作组发出的《体系审核表》进行材料准备，采取文件展示、现场演示等方式，通过现场/远程方式进行审核，评估企业是否满足本标准草案中的要求。经审核发现，所有参与验证活动的整车生产企业均建立汽车信息安全管理体系框架，初步形成面向汽车产品的信息安全管理制度，能够覆盖本标准第5章的条款要求，但不同企业的落地执行方式不同、所执行颗粒度有所差异。为便于行业理解以及加强企业落地可操作性，特作如下说明：

（1）车辆制造商应建立车辆全生命周期的信息安全管理体系。

说明：ISO 21434《道路车辆 信息安全工程》可作为证明和评估信息安全管理体系所需阶段的依据。第9章“概念阶段”、第10章“产品开发”和第11章“信息安全验证”可用于评估信

息安全管理体系的开发阶段。第12章“生产”可用于评估信息安全管理体系的生产阶段。第7章“持续的信息安全活动”、第13章“操作和维护”以及第14章“报废”可用于评估信息安全管理体系的后生产阶段；

（2）应建立企业内部管理信息安全的流程。

说明：本条款中提及的企业内部管理信息安全的流程，指在组织层级与车辆信息安全强相关的流程，对于组织本身的信息安全流程，如：针对企业IT系统的信息安全管理流程等不在本标准考虑范围内。此外，本条款可参考ISO 21434《道路车辆 信息安全工程》中第五章“组织信息安全管理”中的要求，从治理文化、信息共享、安全审核、工具管理、持续改进等方面进行开展。

（3）应建立识别、评估、分类、处置车辆信息安全风险及核实已识别风险得到适当处置的流程，并确保车辆风险评估保持最新状态。

说明：本条款中提及的风险指车辆全生命周期中的信息安全风险，覆盖研发阶段、生产阶段、后生产阶段。企业根据实际需求与业务场景，定义车辆全生命周期中的信息安全风险管控流程。此外，ISO 21434《道路车辆 信息安全工程》中第十五章提及的威胁分析与风险评估方法论可供参考，企业可自行选择是否采用。

（4）应建立针对车辆的网络攻击、网络威胁和漏洞的监测和响应流程，要求如下：

a)应包含确保已识别的网络威胁和漏洞得到响应，且在合理的时限内得到处置的流程；

说明：本条款中提及的“合理时限”当前可由企业结合实际情况自行定义，“处置”包括采取缓解措施、修复、持续监测等方式。

此外，此次审核发现：针对于合资企业和外资企业，其部分体系文档（尤其是车辆产品开发相关制度）保存在国外，且供应商来自于各个国家，在审核时存在无法提供资料或提供的资料难以审查（非中英版本）的情况，需在标准中进行明确约束。

2. 车辆信息安全一般要求评估结果

经审核评估发现，汽车生产企业针对部分新车型已开展信息安全活动，但由于车型项目尚处于概念阶段，无法依据所建立的汽车信息安全管理体系开展全部活动。且部分企业执行的信息安全活动与建立的流程规定并不一致。考虑到目前汽车生产企业的信息安全管理体系亦正处于建设过程中，需预留充足时间供其新款车型研发验证。同时，在审核时发现，对于风险评估活动而言，企业开展形式不一；对于供应商管理而言，汽车企业能够提出明确的信息安全技术要求，但针对于职责划分、工作内容等，企业开展形式不一等等。总体来说，被审核的汽车生产企业对于本标准的第六章条款要求理解无明显偏差。

此外，由于合资企业属性，车辆产品由国内外团队共同完成，但国外团队并不会向国内团队提供完整的风险评估和相关处置文档，因此，存在车型产品开发完成后，但实际风险评估不充分的可能性，车型产品的安全性存在较大风险。

3. 车型技术要求试验结果

测试开始前，需结合车辆信息安全一般要求的评估结果确认适用于该车型的测试项，并获取必要的测试输入信息。

测试输入信息并不一定需要提供完整的文本材料，车辆生产企业针对不同的测试输入信息可以采用不同的方式提供测试输入，不同的测试输入信息提供方式如下：

（1）测试人员和车辆生产企业技术人员通过会议沟通确认：测试车辆远程控制功能，包括远程控制指令应用场景和使用权限；测试车辆授权第三方应用真实性和完整性验证方式；测试车辆非授权第三方应用的访问控制机制；测试车辆外部接口；与测试车辆通信的车辆生产企业云平台；测试车辆通信方法，包括采用的通信协议类型；测试车辆V2X功能；测试车辆向外传输敏感个人信息的通信通道；测试车辆与外部直接通信零部件；测试车辆个人信息清除功能及防恢复机制。

（2）车辆生产企业技术人员先提供目录清单，然后测试人员在车辆生产企业现场确认测试必须的详细信息：远程控制指令审计方式及审计日志记录地址、车辆记录异常指令的地址；测试车内通信方案及通信矩阵样例，包括专用数据通信矩阵样例；测试车辆对称密钥和私钥的存储方式及说明文档；测试车辆内部存储敏感个人信息存储地址；测试车辆内存储的车辆识别代号和用于身份识别的数据清单及存储地址；测试车辆内存储的关键数据清单及存储的地址。

（3）车辆生产企业安排技术人员携带相应的工具在检测机构现场协助完成测试，测试结束后工具收回：测试车辆车载软件升级系统可信根、引导加载程序、系统固件的访问方式和地址；测试车辆实现离线软件升级的方式及工具。

按照2021年10月项目组第6次会议形成的文件开展了验证测试，不同车辆测试项目并不完全相同（全覆盖为80项测试项），下表中给出了标准验证的总体情况。

序号	标准条款	通过情况	不可行/未通过试验主要原因
1	外部连接安全要求 对应15项测试项	通过数量：11 不通过数量：2 未试验数量：2	完成13项测试项的验证，剩余2项测试项被GB 34660-2017覆盖未开展验证试验； 13项测试项中有11项测试方法得到认可，2项测试方法需进行调整。
2	通信安全要求 对应40项测试项	通过数量：25 不通过数量：8 未试验数量：7	完成33项测试项的验证，剩余7项与V2X相关，由于本次送检车型均不具备V2X功能，未开展验证试验； 33项中有25项测试方法得到了认可，8项测试方法需要进行调整。
3	软件升级安全要求 对应13项测试项	通过数量：7 不通过数量：6 未试验数量：0	完成了全部测试项的验证； 13项测试项中有7项方法得到了认可，6项测试方法需进行调整。
4	数据代码安全要求 对应12项测试项	通过数量：11 不通过数量：1 未试验数量：0	完成了全部测试项的验证； 12项测试项中有11项方法得到了认可，1项测试方法需进行调整。

测试验证情况总体总结及重点问题说明：

（1）车型流程审核是开展车型技术要求试验验证的基础，车型技术要求试验验证是对车型流程审核结果的补充确认。

（2）测试验证时发现测试项可能无法完全覆盖技术要求，若企业风险评估后的缓解措施多于技术要求，多出来的企业自定义安全措施需进行评估确认，不再进行测试。

（3）部分测试方法可能会影响企业平台运行。示例：标准原文-8.1.1.1 车辆与车辆、路边单元、服务平台等的通信，应实施身份认证。测试项-A.5.1.1.1.1 与服务平台通信的身份认证试验方法：

a) 若车辆与服务平台通信采用公有通信协议，采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查是否采用如TLS V1.2同等安全级别或以上要求的安全通信层协议；

b) 若车辆与服务平台通信采用私有通信协议，对私有通信协议方案进行审核，采用网络数据抓包的方法进行数据抓包，解析通信报文数据中加密密钥衍生、更新及存储策略，检查是否支持以安全方式进行定期更新，并以安全的方式存储加密密钥。

c) 依据车辆端通信部件清单，使用车辆端设备和服务平台的合法证书，检测双方是否能够完成身份认证以进行后续通信；

d) 分别替换伪造的车辆端设备和服务平台的证书，测试是否能够通过身份认证并进行后续通信。

说明：送检车辆连接的平台均为实际生产平台，进行证书替换，采用私有APN通讯的认证方式可能影响已售车辆运行。

（4）部分企业产品采取的防护技术可能会影响测试项执行，将通过审核的方式补充证明。示例：测试项- A.5.4.1 车辆传输的机密数据保密性试验/防止敏感信息泄露试验。测试人员应依据车辆传输机密数据清单，按照如下方法，检验测试车辆是否满足正文8.4.1的要求：

a) 抓取通讯数据包，检查是否正确使用声明的加密算法对车辆传输的机密数据进行加密；

b) 检查使用的加密算法强度是否满足需求。

说明：标准技术要求“8.1.1.1 车辆与车辆、路侧单元、服务平台等的通信，应实施身份认证”，企业为满足此条款要求，采用了TLS1.2以上安全通讯协议时，测试人员无法通过技术测试验证的方式核查此时传输的数据消息体本身是否依照声明的算法进行数据加密；

（5）通过本次标准验证试验，对部分测试方法进行优化调整：

a) 若基于第7-10章安全技术要求的风险处置措施与企业所识别的风险不相关，无需对不相关的条款开展测试，仅需开展评估确认。

b) 若基于第7-10章安全技术要求的风险处置措施无法覆盖企业所识别的风险，应在按照附录A开展测试验证的基础上，对企业实际所使用的处置措施开展评估确认。

c) 若基于第7-10章安全技术要求的风险处置措施适用于企业所识别的风险，按照附

录A.4-A.7的要求开展验证，其中适用于现场测试的条款依照文件中列出的条款开展测试进行确认，不适用于现场测试的条款通过审核研发阶段的第三方测试报告进行确认。

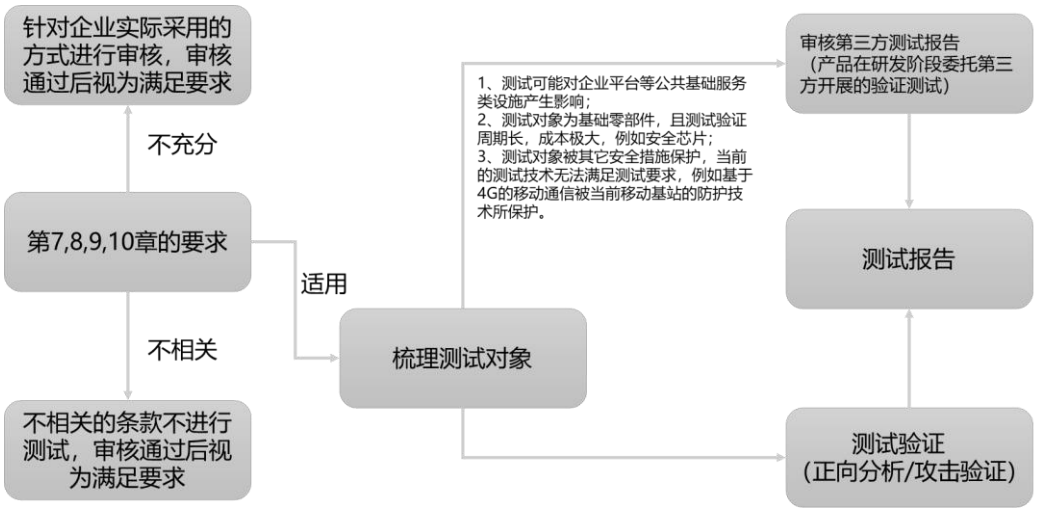


图 2 试验验证流程总结

五、涉及专利的有关说明

本标准不涉及专利。

六、重大分歧意见的处理过程、处理意见及其依据

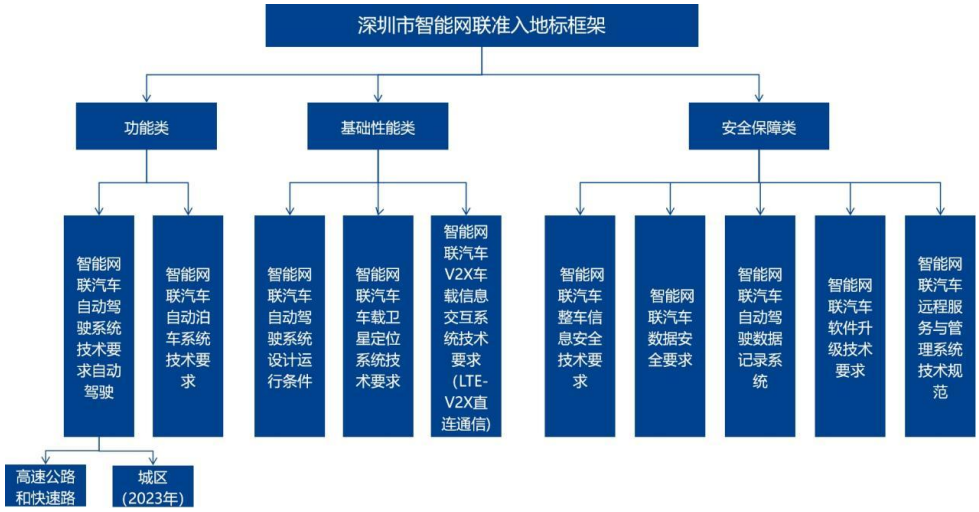
本标准修订过程中无重大分歧。

七、实施地方标准的措施建议

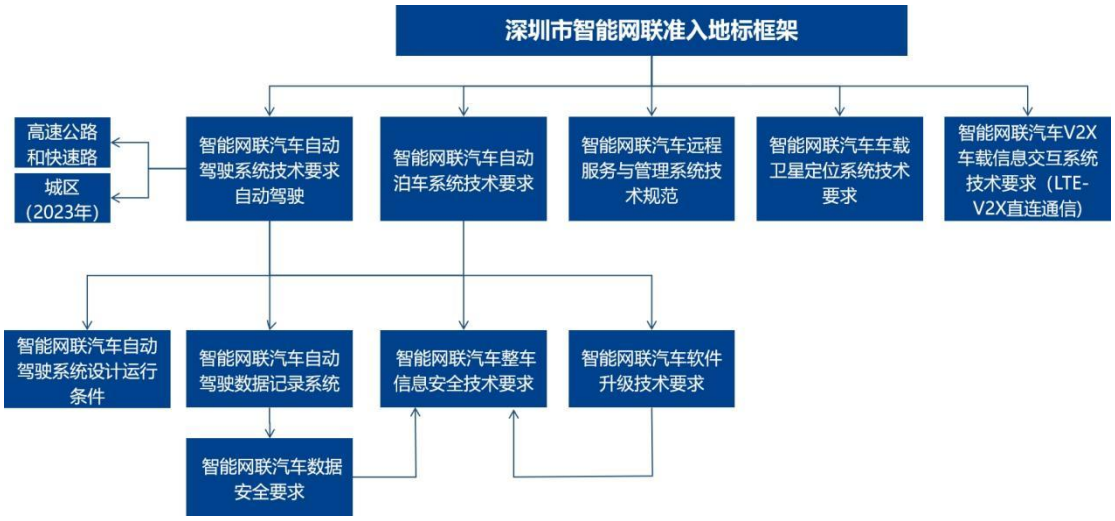
考虑到企业的研发改进周期，建议体系要求和车型要求分步实施。

八、其他需要说明的事项

深圳市智能网联汽车准入标准框架：



深圳市智能网联汽车准入标准间引用关系：


深圳市智能网联准入地标框架
高速公路和快速路
城区（2023年）
智能网联汽车自动驾驶系统技术要求 自动驾驶
智能网联汽车自动泊车系统技术要求
智能网联汽车远程服务与管理系统技术规范
智能网联汽车车载卫星定位系统技术要求
智能网联汽车V2X车载信息交互系统技术要求（LTE-V2X直连通信）
智能网联汽车自动驾驶系统设计运行条件
智能网联汽车自动驾驶数据记录系统
智能网联汽车整车信息安全技术要求
智能网联汽车软件升级技术要求
智能网联汽车数据安全要求