《智能网联汽车整车信息安全技术要求》解读

《智能网联汽车整车信息安全技术要求》地方标准已于2023年8月22日发布，于2023年9月1日实施，现就编制背景和意义、适用范围和主要内容等进行解读如下：

一、 标准编制背景和意义

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防范信息安全风险，该法规具有国际协调约束力，已逐渐成为汽车信息安全领域的准则，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。按照汽车系统开发V模型，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、 标准主要内容

《智能网联汽车整车信息安全技术要求》包括十二个章节，以下对文件中的主要条款进行简要说明。

第一章：范围

本文件规定了智能网联汽车信息安全管理体系要求、车辆信息安全一般要求、车辆外部连接安全要求、车辆通信通道安全要求、车辆软件升级安全要求、车辆数据代码安全要求、审核评估及测试方法。

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类车辆，其他类型车辆可参考执行。

第二章：规范性引用文件

本文件没有规范性引用文件。

第三章：术语和定义

本章节给出了本文件编制过程中涉及到的术语和其定义，包括汽车信息安全管理体系、风险、风险评估、威胁、漏洞、车载软件升级系统、在线升级、离线升级和敏感个人

信息。

第四章：缩略语

本章节给出了本文件编制过程中涉及到的缩略语，包括CAN、HSM、MD5、NFC、TLS、USB、VLAN、VIN和WLAN。

第五章：汽车信息安全管理体系要求

本章节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，针对汽车信息安全管理体系提出了三类要求：（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；（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是否得到适当处置的流程，并确保车辆风险评估保持最新状态；（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。

第六章：车辆信息安全一般要求

本章节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)，针对车辆信息安全提出了四类一般要求：（1）车辆产品开发流程应遵循汽车信息安全管理体系要求；（2）识别和管理与供应商相关的车辆风险；（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；（4）应采用合规的密码算法。

第七章：车辆外部连接安全要求

本章节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），针对车辆的远程控制功能系统、第三方应用、外部接口和网络端口提出了安全要求，包括真实性完整性校验、访问控制、漏洞扫描等。

第八章：车辆通信通道安全要求

本章节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），针对车辆蜂窝通信、蓝牙、WLAN、射频等通信通道提出了安全要求，包括通信双方身份认证、通道完整保护、敏感个人信息传输加密、抵御非法攻击、安全日志记录等。

第九章：车辆软件升级安全要求

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），针对在线升级和离线升级两种软件升级模式分别提出了安

全要求，包括升级包真实性完整性校验、刷写端身份校验等。

第十章：车辆数据代码安全要求

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），针对车内存储的对称密钥、私钥、敏感个人信息、车辆识别代号、关键数据、安全日志提出了安全存储的要求，并限制车辆与境外直接进行通信。

第十一章：审核评估及测试方法

本章节明确了在依据本文件开展车辆信息安全一般要求评估和信息安全技术要求测试验证前，应通过汽车信息安全管理体系要求审核，且车辆信息安全技术要求测试验证依据本文件附录A执行。

附录

附录A（规范性）车辆信息安全技术要求测试验证方法规定了车辆外部连接安全要求、车辆通信安全要求、车辆软件升级安全要求和车辆数据代码安全要求的测试验证方法。

三、 附则

本文件由深圳市工业和信息化局提出并归口。本文件由深圳市工业和信息化局起草。