推荐性国家标准

《汽车网关信息安全技术要求》

（征求意见稿）

编制说明

标准起草项目组

2020年4月

目　　次

《汽车网关信息安全技术要求》

（征求意见稿）

编制说明

一、 工作简况

（一） 任务来源

本项目是根据国家标准委[2019]11号文 《关于下达2019年第一批推荐性国家标准计划的通知》（计划项目编号20191070-T-339，标准项目名称《汽车网关信息安全技术要求》）进行制定。

（二）工作过程

任务下达后，汽标委智能网联汽车分标委组织成立标准起草项目组并面向工作组成员单位公开征集成员，经综合考虑，确定广州汽车集团股份有限公司为牵头单位，在此基础上明确了任务和分工，积极开展标准的前期预研等工作。

2017年11月，向国家标准委提交立项申请。

2018年05月～06月，项目组确定了标准制定的指导思想和原则，制定了标准的总体框架和工作计划。

2018年06月～2018年12月，收集、整理并系统地分析了与汽车网关信息安全相关的法规、标准、文献资料等，开展了相关技术研究。

2019年01月～06月，经过标准起草项目组合理分工和反复讨论，起草了标准草案。

2019年03月，国家标准委正式下达了该标准项目计划编号。

2019年06月～09月，开展标准测试验证工作，根据测试数据，讨论和完善标准文本。

2019年09月～11月，组织专家对标准草案进行了研讨和多次修改，形成工作组内征求意见稿，并面向工作组内各成员单位广泛征求意见。

2019年11月～2020年03月，根据组内征求意见对标准草案进行修改完善，编写标准编制说明。

2020年04月，完成标准公开征求意见稿。

1. 项目组第一次会议

2018年5月23日，项目组在广州组织召开了“汽车网关信息安全技术要求标准编制项目

组第一次工作会议”，正式启动标准制定工作。

会议对各参与单位及主要参与专家的基本情况进行了交流，对标准背景、标准基本内容框架进行了讨论，并围绕标准涉及的内容范围、国内外相关标准和法规现状以及时间安排等多个方面进行了深入讨论。经本次会议讨论，明确了标准的内容与定义，对标准范围进行了界定，明确了标准基于当前和将来车内网络结构的风险定义和风险管理需求，聚焦跨网关的通讯信息安全和基本应用安全，提出了基于风险和攻击的安全功能定义，为主机厂和供应商开发安全网关和安全审查提供依据。

2. 项目组第二次会议

2018年8月2日，项目组在长春召开了“汽车网关信息安全技术要求标准编制项目组第二次工作会议”，会议明确了标准编制范围不包括网关信息安全功能具体实现方法，不涉及网关开发流程的安全，不涉及硬件系统安全，不涉及网关操作系统的安全；会议重点讨论了标准草案的框架和目录，制定了初版目录并由工作组各成员分工编写标准文本。

3. 项目组第三次会议

2018 年 10 月 25 日，项目组在天津组织召开了“汽车网关信息安全技术要求标准编制项目组第三次工作会议”，会议审阅了标准目录初稿、讨论了部分章节的内容草案，例如在车内网络结构示意中要具有前瞻性并考虑域控制器的使用，明确标准将不提及对于网络协议和漏洞的分析，最终形成如下意见：

1) 目录框架内容达成一致意见；
2) 简化第五章中对于通信协议的描述；
3) 在标准中加入试验验证章节；
4) 标准编写的行文格式要遵循 GB/T 1.1-2009 的要求。

4. 项目组第四次会议

2018 年 12 月 20 日，项目组在北京组织召开了“汽车网关信息安全技术要求标准编制项目组第四次工作会议”。会议对总线通信协议的安全脆弱点、网关 CAN 协议通信安全、网关以太网协议通信安全几方面进行了深入的讨论。会议同时欢迎各成员单位更多专家踊跃参与到标准编制工作中，充分考虑各方意见，提高标准的广泛性。

5. 项目组第五次会议

2019 年 5 月 8 日，项目组通过电话会议形式召开了“汽车网关信息安全技术要求标准编制项目组第五次工作会议”。会议对最新的标准草案进行了逐章逐条的详细讨论，包括“删除部分术语定义、对网络结构示意图增加描述”等十余条修改建议。会议同时讨论了后续标准编制工作的时间计划，本次会议以后，按照会议讨论结果，进一步修改和完善了标准草案。

6. 项目组第六次会议

2019 年 6 月 4 日，项目组在无锡组织召开了“汽车网关信息安全技术要求标准编制项目组第六次工作会议”。会议对修改后的标准草案进行了讨论，形成如下意见：

1） 为了和其他汽车产品信息安全标准统一，将标准的资料性内容转移到附录中，并按照硬件、软件、通信、数据等几个方面对草案进行调整；

2） 根据秘书处统一安排，在标准中加入测试验证的要求，请工作组成员单位尽快编制初稿，并开始组织测试验证工作。

7. 项目组第七次会议

2019 年 7 月 17 日，项目组在西安组织召开了“汽车网关信息安全技术要求标准编制项目组第七次工作会议”。会议重点对标准草案的试验测试部分进行了讨论，同时提出了试验计划，希望各成员单位踊跃提供测试样件供试验验证。

8. 项目组第八次会议

2019 年 11 月 6 日，项目组在杭州组织召开了“汽车网关信息安全技术要求标准编制项目组第八次工作会议”。会议首先讨论了工作组后续工作计划，并对标准的工作组内部征求意见稿进行了定稿讨论。会议同意在完成必要的修改后，在工作组内部征求意见。

9. 项目组第九次会议

2020 年 3 月 24 日，项目组通过电话会议形式组织召开了“汽车网关信息安全技术要求标准编制项目组第九次工作会议”。会议针对工作组内征求意见阶段收到的所有意见进行了逐条详细讨论，并对标准草案的公开征求意见稿及编制说明进行了定稿讨论。会议同意在完成个别条文的修改后，进行公开征求意见。

10. 工作组内部征求稿反馈意见回复

工作组内部征求意见稿发出后，共收到 106 条的反馈意见，根据反馈意见的内容，项目

组进行了讨论并给出结论，其中，66 条意见采纳，13 条意见部分采纳，27 条不采纳，在此基础上对标准进行了修改，形成公开征求意见稿。

（三） 主要参加单位和工作组成员及其所做的工作等

本标准由十余家单位共同起草。在本标准的制定过程中，多次组织行业专家进行了研讨，得到了相关单位的支持、协助与配合，取得了大量建设性意见、建议。

二、 国家标准编制原则和确定国家标准主要内容

（一）标准编制原则

1）本标准编写符合 GB/T 1.1《标准化工作导则》的要求；

2）在项目组内对标准内容广泛征求意见，并在工作组会议上充分讨论；

3）起草过程充分考虑国内外现有相关标准的统一和协调；

4）标准充分考虑了汽车主机厂、汽车零部件厂商和信息安全解决方案提供商的意见，在不偏离国际和国内当前行业技术水平的基础上前瞻性地考虑技术发展方向；

5）适当考虑标准条款对汽车网关零部件的软硬件成本的影响。

（二）标准主要内容

本标准规定了汽车网关产品硬件、通信、软件、数据的信息安全技术要求与测试方法。

根据调研成果，本标准普遍适用于商用车和乘用车的网关控制器。

1. 术语和定义

标准的术语和定义参考了GB/T 25069-2010《信息安全技术 - 术语》、GB/T 37935-2019《信息安全技术 可信计算规范 可信计算基》和同时在制定中的《汽车信息安全通用技术要求》中的部分术语和定义，并对标准最主要的“汽车网关”术语进行了标准化定义。

2. 条款 5 汽车网关拓扑结构

本条款对汽车 CAN 网关、汽车以太网网关、汽车混合网关对应的总线拓扑结构进行了说明。

3. 条款 6.1 硬件信息安全要求

在网关硬件层面，主要对网关芯片和调试接口两个方面进行了要求。

4. 条款 6.2 通信信息安全要求

由于网关的主要功能为在车内多个网络间进行数据转发和传输，因此本部分是标准的核

心内容。

6.2.1 和 6.2.2 分别是 CAN 网关和以太网网关的通信信息安全要求，6.2.3 要求对于其他类型的混合网关，CAN 通信和以太网通信的信息安全要求应按照本标准的 6.2.1 和 6.2.2 章节执行，其他协议通信的信息安全要求也可参照执行。

对于 CAN 网关通信信息安全，分别从访问控制、抗拒绝服务攻击、数据帧健康检查、数据帧异常检测、UDS 会话检测 5 个方面提出了要求。

对于以太网网关通信信息安全，分别从安全区域划分、访问控制、抗拒绝服务攻击、协议状态检测 4 个方面提出了要求。

5. 条款 6.3 软件信息安全要求

在网关软件层面，主要对安全启动、安全日志记录和安全漏洞三个方面进行了要求。

对于汽车网关，安全启动功能能够发现网关固件系统的任何恶意变更，并在恶意变更发生时阻止网关系统启动，从而使攻击者无法对网关固件进行篡改。因此6.3.1要求网关应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。其中“可信根实体”的定义详见GB/T 37935-2019 《信息安全技术 可信计算规范 可信计算基》。

6. 条款 6.4 数据信息安全要求

在网关数据层面，主要对网关中的安全重要参数的存储和处理进行了要求。其中“安全重要参数”的定义详见 GB/T《汽车信息安全通用技术要求》。

7. 条款 7 信息安全测试方法

根据本标准“6.技术要求”中各项信息安全技术要求，逐一对应提出了本部分测试方法。

三、 主要试验（或验证）情况分析

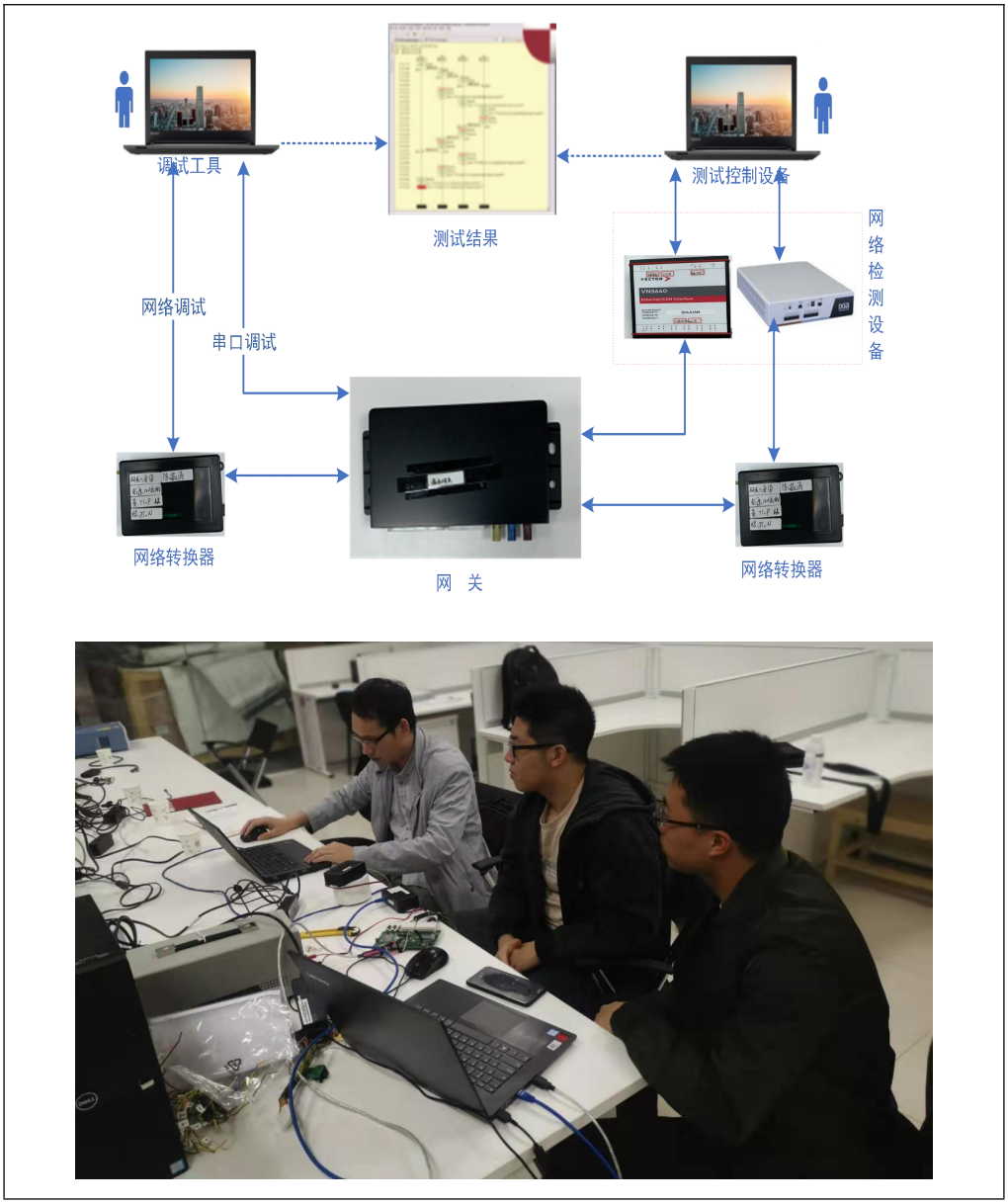
（一） 测试概况

测试时间：2019年9月至10月

测试地点：天津 中汽中心 17号楼 2楼测试间

测试单位：中汽研汽车检验中心（天津）有限公司

测试目标物：	CAN 网关、以太网网关
测试环境：	根据标准文稿搭建测试
测试方法：	根据标准文稿规定的测试方法编制具体测试 case。



（二） CAN网关测试

1. 测试工具

CAN网关测试中，使用了以下测试工具设备：

工具名	作用
CAN 报文工具	用于收发报文，向 CAN 网关发送攻击报文、正常报文并接收 CAN 网关转发的报文。
芯片检测展示台	用于检查是否存在可非法对芯片进行访问或者更改芯片功能的隐蔽接口，如 JTAG、串口等调试接口。
芯片调试工具	用于篡改、调试 CAN 网关系统固件程序，读写内存。
测试控制电脑	发包工具，测试软件。

2. 测试方法

测试类别	使用的测试方法	测试目的
硬件信息安全测试	硬件安全核查方法	1、检查网关所使用的芯片是否存在可以对芯片进行非授权访问或更改芯片功能的隐蔽接口； 2、检查网关硬件的 PCB 板上，是否有暴露的调试接口。
CAN 网关通信信息安全测试	访问控制策略测试方法 泛洪攻击测试方法 报文健康检查测试方法 报文异常检查测试方法 UDS 异常检查测试方法	1、检测符合访问控制策略的报文是否正常转发； 2、检测不符合控制策略的报文是否丢弃和记录； 3、检测泛洪攻击报文是否被丢弃和记录； 4、检测符合 UDS 诊断协议的诊断报文是否正常转发； 5、检测不符合 UDS 诊断协议的诊断报文是否丢弃和记录。
软件信息安全测试	安全启动系统固件测试方法	检测系统固件程序被篡改后，CAN 网关在系统固件签名验证失败时是否停止加载运行系统固件程序，并通过日志记录。
数据信息安全测试	数据安全测试方法	检测访问数据受保护区域能否扫描出关键字或特征码，如密钥等。

3. 测试结果

测试方法	测试结果
硬件安全核查方法	正式量产产品不存在 JTAG、UART 调试接口，或存在 JTAG、UART 调试接口，不能通过调试接口读写、调试固件程序，通过。
访问控制策略测试方法	1.发送正常报文，网关将报文进行转发； 2.发送异常报文，网关将不对报文进行处理； 3.无日志，未通过。
泛洪攻击测试方法	1.发送泛洪攻击报文，网关对攻击报文不进行处理； 2.发送泛洪攻击报文同时发送正常报文，正常报文正确转发； 3.无日志，未通过。
报文健康检查测试方法	1.报文长度异常的报文，网关对该报文不进行处理； 2.网关对报文长度异常的报文无日志记录，未通过。
报文异常检查测试方法	1.信号长度异常的报文，网关对该报文不进行处理； 2.信号值不符合通信矩阵的报文，网关对该报文不进行处理； 3.无日志，未通过。
UDS 异常检查测试方法	1.向网关样件发送不符合诊断规范定义的诊断时序报文，网关对该报文不进行处理； 2.向网关样件发送不符合诊断规范定义的诊断报文，网关对该报文不进行处理； 3.无日志，未通过。

安全启动系统固件测试方法	1.对系统固件任意位置篡改后，网关样件在系统固件签名验证失败时重复加载运行系统固件程序； 2.打印固件验证失败信息，通过（功能点应保证对应条款功能的进入、打开方式）。
数据安全测试方法	受保护区域内存不能读取，通过。

（三） 以太网网关测试

1.测试工具

以太网网关测试中，使用了以下测试工具设备：

工具名	作用
网络检测工具	用于发送泛洪、典型网络攻击。
网络转换器	用于 PC 机与以太网网关连接（T1 转 TX）。
X-shell	用于 SSH 登录以太网网关、读取日志操作。
Wireshark	用于抓取网络数据包。
芯片专用调试工具	用于篡改以太网网关系统固件程序，读写内存。
芯片检测展示台	用于检查是否存在可非法对芯片进行访问或者更改芯片功能的隐蔽接口，如 JTAG、串口等调试接口。

2.测试方法

测试类别	使用的测试方法	测试目的
硬件信息安全测试	硬件安全核查方法	1、检查网关所使用的芯片是否存在可以对芯片进行非授权访问或更改芯片功能的隐蔽接口； 2、检查网关硬件的 PCB 板上，是否有暴露的调试接口； 3、暴力破解是否成功。
以太网网关通信信息安全测试	访问控制策略测试方法 典型攻击测试方法 VLAN 域隔离测试方法	1、检测符合访问控制策略的报文是否正常转发； 2、检测不符合控制策略的报文是否丢弃和记录； 3、检测典型攻击报文是否被丢弃和记录； 4、检测网络分域之间是否不能发送广播报文。
软件信息安全测试	安全可信根测试方法 安全启动Bootloader测试方法 安全启动内核镜像测试方法 关键配置变更测试方法	1、检测网关安全启动可信根是否防篡改并记录篡改事件； 2、检测 Bootloader 被破坏后是否停止加载下一阶段固件并记录； 3、检测网关安全启动系统镜像校验失败，网关是否停止启动并记录； 4.检测关键配置变更网关是否有记录。

数据信息安全测试	数据安全测试方法	1、检测授权用户能否访问安全区域； 2、检测非授权用户能否访问安全区域。

3.测试结果

测试方法	测试结果
硬件安全核查方法	1.产品不存在 JTAG、UART 调试接口，或存在 JTAG、UART 调试接口，不能通过调试接口读写、调试固件程序。通过。 2. 暴力破解成功，未通过（暴力破解的字典、阈值，不少于 10000 条）。
访问控制策略测试方法	1.源设备 ping 目的设备，目的设备接收到 ping 包； 2.源设备向目的设备发送攻击报文（Ping of Death），网关拦截攻击报文并记录攻击事件，不符合策略规定的报文被拦截并记录； 3.检测设备向网关进行 TCP SYN 攻击，同时发送正常 ping 包，网关记录 TCP SYN 攻击并一直能 ping 通。通过。
防火墙黑/白名单测试方法	1.白名单内 IP 和端口通信测试 ping 白名单 IP 成功、白名单端口通信成功。 2.非白名单内 IP 和端口通信测试 ping 非白名单 IP 失败、非白名单端口通信失败。通过。
VLAN 域隔离测试方法	VLAN 1 的设备 ping VLAN 2 的设备不能成功。无日志，未通过。
安全可信根测试方法	1.网关样件使用 NXP 的 CPU，具备可信根安全区域； 2.存放公钥、hash 值的内存不能写，公钥可以读，hash 值读出来为全 F。通过。
安全启动 Bootloader 测试方法	1.BootLoader 任意位置篡改后不能正常启动，一直不断重启； 2.启动失败信息保存在寄存器，无法查看。通过。
安全启动内核镜像测试方法	1.对系统固件任意位置篡改后，网关样件在系统固件签名验证失败时重复加载运行系统固件程序； 2.打印固件验证失败信息。通过。
关键配置变更	改变网关样件任意的配置文件(包括访问控制列表、路由表)，日志记录该配置文件被修改。通过。
数据安全测试方法	1.通过非 root 账户登录，不能读取安全事件日志内容； 2.通过 root 账户登录，可以读取安全事件日志内容； 3.存放公钥、hash 值的内存不能写，公钥可以读，hash 值读出来为全 F。通过。

（四）测试总结分析

1） 验证测试中，合计测试项29个，其中通过23个，未通过的6个测试项均因为没有记录对应的日志。经过调研，受限于网关计算能力和存储资源的限制，当前市面上的网关产品中日志记录的功能尚未普及。针对上述情况，经过项目组讨论，将标准中关于日志记录的要求修改为非必须项。

2） 通过测试验证，确认本标准的技术要求均能够落地实施，不存在技术壁垒。

3） 通过测试验证，确认本标准的测试方法均可实际操作。

四、 标准中涉及专利的情况

本标准不涉及专利问题。

五、 预期达到的社会效益等情况

本标准的制定和实施，将为行业管理部门提供技术支撑，引导网关零部件和汽车整车生产企业产品满足行业信息安全要求，大大提升我国车辆的信息安全技术水平。

随着车辆智能化网联化的快速推进，越来越多的车辆已经与外部互联网产生通信，从而引入了巨大的信息安全风险。一旦车辆受到恶意攻击，将对交通参与者的生命安全造成无法预知的威胁。网关作为车内网络的核心节点，推进网关信息安全标准的广泛应用，可以大幅降低信息安全风险，具有巨大的经济效益和社会效益。

六、 采用国际标准和国外先进标准的情况

本标准没有采用国际标准。

本标准制定过程中未查到同类国际、国外标准。

本标准修订过程中未测试国外的样品、样机。

本标准水平为国内先进水平。

七、 与现行相关法律、法规、规章及相关标准的协调性

本标准与我国现行有关法律、法规和强制性国家标准不矛盾。

八、 重大分歧意见的处理经过和依据

无。

九、 标准性质的建议说明

鉴于本标准在《国家车联网产业标准体系建设指南（智能网联汽车）》中的项目定位与规划。根据标准化法和有关规定，建议本标准的性质为推荐性国家标准。

十、 贯彻标准的要求和措施建议

1.首先应在实施前保证本标准文本的充足供应，使每个制造厂、设计单位以及检测机构

等都能及时获得本标准文本，这是保证新标准贯彻实施的基础。

2. 本次指定的《汽车网关信息安全技术要求》不仅与生产企业有关，而且与设计单位、检测机构等相关。对于标准使用过程中容易出现的疑问，起草单位有义务进行必要的解释。

3. 可以针对标准使用的不同对象，如制造厂、质量监管等相关部门，有侧重点地进行标准的培训和宣贯，以保证标准的贯彻实施。

十一、 废止现行相关标准的建议

无。

十二、 其他应予说明的事项

无。