ICS 35.030
CCS L 80

团 体 标 准

T/CSAC 019—2025
T/WHCSA 008—2025

智能网联汽车网络安全检测技术要求

Technical requirements for network security test of intelligent connected vehicles

2025－05－22 发布　　2025-08－22 实施

中国网络空间安全协会
武汉市网络安全协会　联合发布

目　　次

前　言

本文件按照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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络空间安全协会和武汉市网络安全协会共同提出，并分别归口。

本文件起草单位：湖北天融信网络安全技术有限公司、国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心湖北分中心、武汉市公安局交通管理局、东风汽车集团有限公司研发总院、岚图汽车科技有限公司、东风悦享科技有限公司、东风商用车有限公司、襄阳达安汽车检测中心有限公司、中机寰宇认证检验股份有限公司、东风汽车集团股份有限公司猛士汽车科技公司、中移（上海）信息通信科技有限公司、武汉大学国家网络安全学院、华中科技大学网络空间安全学院、武汉理工大学、湖北大学网络空间安全学院、华中师范大学、湖北汽车工业学院，湖北省电子信息产品质量监督检验院、武汉安域信息安全技术有限公司、开源网安物联网技术（武汉）有限公司、广电计量检测（武汉）有限公司、宝牧科技（天津）有限公司武汉分公司。

本文件主要起草人：孙秉稷、范雪俭、左世涛、吕露、安高峰、胡雨翠、蔡倩楠、曹岚、李中戈、刘悦恒、乔奇、张玉萍、严媛、蒋凌云、张绳武、刘青、黄传明、付琳、陈翔、孙伟、陶先锋、刘翀、代薇、李宏伟、田明明、黄鑫、林凯、韩鹏、左少雄、翟亦康、牟飞、于乐、马禹昇、赵威、付超、曹越、庄园、胡胜山、向剑文、何鹏、潘俊杉、陈嘉耕、陈宇峰、徐煦、柳少凯、李永龙、张海春、唐迪、肖海涛、张瑶。

智能网联汽车网络安全检测技术要求

1 范围

本文件规定了智能网联汽车车端网络与车端联网零部件系统的网络安全检测项目、方法和要求。

本文件适用于汽车生产企业、汽车网络安全产品及服务提供商，以及汽车网络安全检测评估机构，对汽车网络安全开展的测试、评估和管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB 44495—2024 汽车整车信息安全技术要求

GB 38900—2020 机动车安全技术检验项目和方法

GB/T 40861—2021 汽车信息安全通用技术要求

3 术语和定义

GB/T 25069、GB 44495—2024、GB 38900—2020 和 GB/T 40861—2021 界定的以及下列术语和定义适用于本文件。

3.1

漏洞 vulnerability

在资产或缓解措施中,可被一个或多个威胁利用的弱点。

[来源：GB 44495—2024，3.6]

3.2

升级包 update package

用于进行软件升级的软件包。

3.3

软件 software

与计算机系统操作有关的计算机程序、规程、规则，以及可能有的文件、文档及数据。

4 缩略语

下列缩略语适用于本文件。

CAN：控制器局域网络（Controller Area Network）

CANFD：可变速率的控制器局域网络（CAN with Flexible Data rate）

ETC：电子不停车收费（Electronic Toll Collection）
GNSS：全球导航卫星系统（Global Navigation Satellite System）
Lin：局域互联网络（Local Interconnect Network）
MOST：面向媒体的系统传输总线（Media Oriented System Transport）
NFC：近距离无线通讯技术（Near Field Communication）
OBD：车载诊断(On-Board Diagnostics)
UDS：统一诊断服务（Unified Diagnostic Services）
USB：通用串行总线(Universal Serial Bus)
WLAN：无线局域网（Wireless Local Area Networks）

5 智能网联汽车网络安全检测要求

5.1 车端总线网络安全检测要求

5.1.1 车载 CAN/CANFD 总线安全检测要求

车载 CAN/CANFD 总线安全检测应包括：

a) 车载 CAN/CANFD 总线保密性、完整性、可用性、可控性、不可抵赖性等安全检测；
b) CAN/CANFD 总线模糊测试，包括报文结构模糊测试、通信行为模糊测试（报文发送间隔异常、帧类型混叠）、协议逻辑滥用测试等；
c) CAN/CANFD 总线拒绝服务攻击检测，包括高频率报文拒绝服务攻击、高负载率拒绝服务攻击、随机报文内容拒绝服务攻击、指定报文定向拒绝服务攻击、协议逻辑滥用型拒绝服务攻击等；
d) UDS 检测，包括 UDS 探测、CAN/CANFD 网络诊断协议检测、诊断协议安全性验证及漏洞扫描等检测。

5.1.2 车载以太网总线安全检测要求

车载以太网总线安全检测应包括：

a) 车载以太网总线保密性、完整性、可用性、可控性、不可抵赖性等安全检测；
b) 车载以太网数据可用性（包括丢包率、时延）、完整性（包括校验和、错误计数）检测；
c) 车载终端专用网络认证机制检测，包括 MAC 地址过滤、802.1X 认证协议、数字证书认证、单一签名认证、预共享密钥等；
d) 车载以太网安全管理策略功能检测，包括通信名单过滤、命令来源校验、网络分域及访问控制等。

注：Lin总线、MOST总线等其他车载总线协议可参考此检测要求。

5.2 车端无线网络安全检测要求

5.2.1 车载蓝牙网络安全检测要求

车载蓝牙网络安全检测应包括：

a) 强化身份认证、数据加密、信任管理与证书验证等内容检测；
b) 车载蓝牙网络信息安全审计功能检测，包括事件的日期、用户、事件类型、事件成功与否及其他审计相关信息；
c) 车载蓝牙网络程序启动可信验证机制性检测。

5.2.2 车载 WLAN 网络安全检测要求

车载 WLAN 网络安全检测应包括：

a) 车载 WLAN 网络信息安全审计功能检测，检测是否记录用户行为和重要安全事件，包括事件的日期、用户、事件类型、事件成功与否及其他审计相关信息；
b) 车载 WLAN 网络程序启动安全检测，检测车载 WLAN 网络启动程序是否具有可信验证机制。

5.2.3 车载 NFC 网络安全检测要求

车载 NFC 网络安全检测应包括：

a) 外部 NFC 设备真实性检测，对通过 NFC 连接的外部 NFC 设备进行身份真实性校验；
b) 车载 NFC 网络信息安全审计功能检测，检测是否记录用户行为和重要安全事件，包括事件的日期、用户、事件类型、事件成功与否及其他审计相关信息；
c) 车载 NFC 网络程序启动安全检测，检测车载 NFC 网络启动程序是否具有可信验证机制。

5.2.4 车载 GNSS 安全检测要求

车载 GNSS 安全检测应包括：

a) 数据完整性检测，检测 GNSS 通信中是否具备数据完整性校验能力；
b) 数据保密性检测，检测 GNSS 通信中是否采用滚动码技术；
c) 模拟欺骗攻击检测，检测车载 GNSS 通信是否具备抗欺骗及抗干扰能力；
d) 车载 GNSS 程序启动安全检测，检测车载 GNSS 启动程序是否具有可信验证机制。

5.2.5 车载蜂窝网络安全检测要求

车载蜂窝网络安全检测应包括：

a) 手动开启或关闭蜂窝网络连接功能检测，检测是否具备手动开启与关闭蜂窝网络连接的功能；
b) 车云通信完整性校验机制检测，检测是否具备通信数据防止恶意篡改能力；
c) 车云通信加密机制检测，检测通信数据是否加密；
d) 车云通信身份认证机制检测，检测是否能够有效识别伪造通信实体；
e) 防止报文重放机制检测，检测通信通道是否具备抗报文重放攻击能力；
f) 网络入侵检测机制检测，检测是否能针对攻击源、攻击事件进行识别并进行告警；
g) 安全审计机制检测，检测是否能够针对用户行为和重要安全事件进行记录，包括事件的日期、用户、事件类型、事件成功与否及其他审计相关信息。

5.3 车端主机网络安全检测要求

5.3.1 车端固件安全检测要求

车端固件安全检测应包括：

a) 启动自检机制检测，如使用安全散列算法等方式进行固件的完整性检查；
b) 固件真实性进行校验，检测固件在执行引导程序前是否对签名的有效性进行验证；
c) 基于硬件的可信根检测，检测可信根在出厂后是否无法被修改；
d) 启动密钥安全存储检测，检测启动密钥是否禁止非授权访问和篡改。

5.3.2 车端接口安全检测要求

车端接口安全检测应包括：

a) USB 设备主动免疫功能检测，采用定制恶意代码攻击技术通过 USB 设备进行入侵，检测是否支持主动免疫功能；

b) OBD 设备非法接入行为识别功能检测，采用非授权 OBD 外部设备接入，检测是否能够识别非法接入行为，并进行阻止；
c) 非授权传感器接入行为识别功能检测，模拟非授权传感器设备接入，检测是否能够识别非授权传感器接入行为，并进行阻止；
d) 车端接口信息安全审计功能检测，检测是否能够记录用户行为和重要安全事件，包括事件的日期、用户、事件类型、事件成功与否及其他审计相关信息。

5.3.3 车端主机漏洞扫描要求

应采用漏洞扫描技术，检测固件、操作系统和应用软件是否存在国家权威漏洞平台公开发布 6 个月及以上的高中危安全漏洞，并生成检测报告。其中国家权威漏洞平台应至少包括：国家信息安全漏洞共享平台（CNVD）和国家信息安全漏洞库（CNNVD）。

6 智能网联汽车网络安全检测方法

6.1 车端总线网络安全检测方法

Lin 总线、MOST 总线等其他车载总线协议可参考此检测要求。

6.1.1 车载 CAN/CANFD 总线安全检测方法

车载 CAN/CANFD 总线安全检测按照下列流程及要求进行：
a) 接入伪造的 CAN/CANFD 外围设备，系统是否可检测出伪造 CAN/CANFD 外围设备，并报警提示；
b) 检查车端系统的 CAN/CANFD 协议，确认协议版本是否达到市场主流最新版本；
c) 检查车载 CAN/CANFD 总线上的数据传输速率和消息传输格式，确认是否符合 CAN/CANFD 协议规定的标准速率和格式要求；
d) 模拟 CAN/CANFD 消息进行注入攻击，检查系统是否能够检测到异常消息并做出适当处理；
e) 篡改 CAN/CANFD 消息进行欺骗攻击，检查系统是否能够及时识别到篡改行为并做出相应反应；
f) 对车载 CAN/CANFD 总线进行嗅探攻击模拟，检查系统是否具备必要的安全防护措施；
g) 对 CAN/CANFD 总线进行拒绝服务攻击模拟，检查系统是否具备稳定性和抗攻击能力；
h) 对 CAN/CANFD 总线上漏洞进行远程代码执行攻击模拟，检查系统是否能够及时发现并应对此类攻击行为；
i) 通过 OBD-II 等外部接口向 CAN/CANFD 总线上发送消息,验证系统是否支持实时监测 CAN/CANFD 总线活动并生成相应日志的功能。

6.1.2 车载以太网总线安全检测方法

车载以太网总线安全检测按照下列流程及要求进行：
a) 抓取车载以太网总线 SOME/IP、DoIP 的业务报文，对抓取的报文进行协议分析，检测 SOME/IP、DoIP 报文是否符合协议规范；
b) 模拟生成不符合协议矩阵的 SOME/IP、DoIP 报文，将不符合协议的报文注入车载以太网总线中，检测以太网总线对不符合协议的报文是否有报警检测；
c) 抓取车载以太网总线 SOME/IP、DoIP 的业务报文，对抓取的报文进行修改和重放，检测车辆对修改和重放的报文是否有告警提示机制；
d) 模拟生成大量的 ICMP、UDP、TCP 等异常流量报文，将生成的大量报文持续注入至车载以太网总线中，检测以太网总线在拒绝服务攻击的过程中，是否能保证业务正常运行；

e) 通过接入车载以太网总线，模拟生成不在车载以太网总线白名单中的报文，将未在白名单中的车载以太网报文注入车载以太网中线中，检测车辆是否会将未在白名单内的报文做丢弃处理；
f) 通过接入车辆，获取所有零部件的 IP 地址，通过零部件 IP 地址，使用不同零部件互相访问来检测车载以太网总线是否支持网络分域；
g) 通过抓取车载以太网总线业务报文，解析车载以太网报文结构，检测车载以太网总线在通讯过程中是否使用了加密处理。

6.2 车端无线网络安全检测方法

6.2.1 车载蓝牙网络安全检测方法

车载蓝牙网络安全检测按照下列流程及要求进行：
a) 利用专业的诊断工具（包括硬件端：OBD-II 扫描仪、CAN 总线分析器；软件端：蓝牙检测诊断软件、车辆制造商诊断软件）检查车载系统中蓝牙协议版本，确认是否为市场上最新的版本；
b) 通过近场访问点与车进行通信，查看审计日志，是否记录相关信息，包括日期、用户、具体事件类型（包括连接建立、数据传输等）、事件成功与否及其他审计相关信息（如数据传输大小、通信协议等）；
c) 修改近场通信程序（如插入恶意代码、绕过验证逻辑、修改配置设置或提升权限），尝试使用修改后的车载系统与其他设备通信，包括连接、发送虚假请求或试图访问数据，检查近场访问点程序运行情况，观察启动、处理请求和响应是否正常。

6.2.2 车载 WLAN 网络安全检测方法

车载 WLAN 网络安全检测按照下列流程及要求进行：
a) 检查系统 WLAN 功能，检测系统是否支持自行关闭 WLAN 网络自动连接功能；
b) 通过近场访问点与车进行通信，查看审计日志，是否记录相关信息，包括日期、用户、事件类型、事件成功与否及其他审计相关信息等；
c) 篡改车端近场访问点程序，模拟近场通信行为，检查车端近场程序是否正常启动并运行。

6.2.3 车载 NFC 网络安全检测方法

车载 NFC 网络安全检测按照下列流程及要求进行：
a) 接入伪造的 NFC 外围设备，验证系统是否能够检测到伪造的 NFC 设备并触发报警提示机制；
b) 检查车载系统中 NFC 协议版本，确认 NFC 协议是否为最新版本；
c) 模拟未经授权的 NFC 设备接入，检测系统是否能够识别和阻止未经授权的 NFC 设备接入；
d) 篡改 NFC 通信数据或插入恶意代码，检测系统是否可识别并响应异常通信行为，同时报警提示。

6.2.4 车载 GNSS 安全检测方法

车载 GNSS 安全检测按照下列流程及要求进行：
a) 检查是否在数据在通信过程中使用校验技术或密码技术来保证完整性，记录具体的措施，检测验证密码技术的组件是否能保证通信过程中的数据完整性；
b) 检查是否在通信过程中采用保密措施，记录具体的保密措施，检测验证在通信过程中是否对数据进行加密；

c) 模拟安全攻击，查看系统是否支持入侵检测功能，并检测是否能够识别攻击源、攻击事件，并进行报警提示；
d) 通过远程访问点与车进行通信，查看审计日志，是否记录相关信息，包括日期、用户、事件类型、事件成功与否及其他审计相关信息等；
e) 篡改车端远程访问点程序，模拟远程通信行为，检查车端远程访问点程序是否正常启动并运行。

6.2.5 车载蜂窝网络安全检测方法

车载蜂窝网络安全检测按照下列流程及要求进行：
a) 基于使用文档检测车辆是否具有手动开启/关闭蜂窝网络连接的功能；
b) 在厂商支持下利用通信报文调试工具抓取报文，对报文进行修改后发送报文，检测接收方是否能够识别篡改后的报文并按照设计要求正确处理报文；
c) 在厂商支持下利用抓包工具抓取蜂窝网络通信数据，检测是否可以解析出具有明确意义的通信报文；检测基于厂商声明的密码算法、密钥检测算法是否与声明一致，安全强度是否达到声明的要求；
d) 在厂商支持下利用抓包工具抓取车辆通信报文，获取车辆通信协商机制，检测通信是否具有利用证书、公钥等进行身份认证的安全机制；
e) 在厂商支持下抓取车辆通信报文，利用工具重放请求报文，通过响应报文检测车辆或者云端是否支持报文防重放机制；
f) 模拟针对车辆信息娱乐系统等车载系统的远程攻击，检测车辆是否能够识别攻击类型、记录攻击事件并提供告警警示；
g) 通过远程访问点与车进行通信，查看审计日志，是否记录相关信息，包括日期、用户、事件类型、事件成功与否及其他审计相关信息等；
h) 篡改车端远程访问点程序，模拟远程通信行为，检查车端远程访问点程序是否正常启动并运行。

6.3 车端主机网络安全检测方法

6.3.1 车端固件安全检测方法

车端固件安全检测按照下列流程及要求进行：
a) 采用网络安全检测工具对固件进行检测，查看检测报告是否有固件为不完整固件记录；
b) 采用网络安全检测工具对固件进行检测，查看检测报告是否有固件为非真实固件记录；
c) 修改固件可信根，查看检测报告中是否有可信根非基于硬件的出厂可信根检测结果；
d) 修改密钥存储方式为非安全存储，查看检测报告中是否有密钥非安全存储记录。

6.3.2 车端接口安全检测方法

车端接口安全检测按照下列流程及要求进行：
a) 采用携带病毒或恶意程序的USB外部设备接入车端USB接口，查看是否提示病毒或恶意程序入侵，并能有效阻止其运行；
b) 采用非授权的OBD设备接入OBD接口，查看系统是否能检出非授权OBD设备，并阻止非授权OBD设备与车进行通信；
c) 采用非授权的传感器设备接入车端，查看系统是否能检测出非授权传感器设备，并阻止非授权传感器设备与车进行通信；

d) 模拟用户操作 USB 外部设备、OBD 设备和传感器设备接入访问点，并进行通信，查看审计日志，是否记录相关信息，包括日期、用户、事件类型、事件成功与否及其他审计相关信息等；

e) 篡改车端接触式访问点程序，并插入 USB 设备、非授权 OBD 设备和非授权传感器设备，启动系统，查看系统是否能阻止程序运行。

6.3.3 车端主机漏洞扫描方法

采用网络安全检测工具对车端主机进行漏洞扫描，检测车端主机中是否存在国家权威漏洞平台公开发布 6 个月及以上的高中危安全漏洞。

参考文献

[1] GA/T 681—2018 信息安全技术 网关安全技术要求
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 37092—2018 信息安全技术 密码模块安全要求
[4] GM/T 0008—2012 安全芯片密码检测准则
[5] YD/T 3746—2020 车联网信息服务 用户个人信息保护要求
[6] DB4403/T 355—2023 智能网联汽车整车信息安全技术要求