ICS 35.030
CCS L 80

团　　体　　标　　准

T/CSAC XXX—2024
T/WHCSA XXX—2024

车联网网络安全检测技术要求

Technical requirements of detection for vehicle cybersecurity

（征求意见稿）

2024－XX－XX 发布　　2025－XX－XX 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。

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（CNCERT）、国家计算机网络应急技术处理协调中心（CNCERT）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、武汉达安科技有限公司、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、武汉理工大学计算机与人工智能学院、湖北大学网络空间安全学院、华中师范大学计算机学院、湖北汽车工业学院汽车工程师学院、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、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、韩鹏、左少雄、翟亦康、牟飞、付超、曹越、庄园、胡胜山、向剑文、何鹏、陈嘉耕、陈宇峰、徐煦、柳少凯、李永龙、张海春、唐迪、张瑶、肖海涛。

车联网网络安全检测技术要求

1 范围

本文件规定了汽车车端网络与车端联网零部件系统的网络安全检验项目、方法和要求。

本文件适用于 M、N 类及至少装置 1 个电子控制单元的 O 类车辆，其他车辆可参考执行。

2 术语和定义

GB/T 25069、GB 38900、GB/T 40429、GB/T 40857-2021、GB/T 40861-2021、GA 802 和 YD/T 3750-2020 界定的术语和定义适用于本文件。

3 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：可变缩率的控制器局域网络（CAN with Flexible Data rate）

ECU：电子控制单元（Electronic Control Unit）

ETC：电子不停车收费（Electronic Toll Collection）

GNSS：全球导航卫星系统（Global Navigation Satellite System ）

HSM：硬件安全模块（Hardware Secure Module）

NFC：近距离无线通讯技术（Near Field Communication）

RFID：射频识别（Radio Frequency Identification）

WLAN：无线局域网（Wireless Local Area Networks）

4 检验项目

车联网网络安全检测技术项目见表 1 所示，适用于智能网联汽车车端网络与车端联网零部件系统。

表 1 车联网网络安全检测技术项目

检测级别	检验项目	
通用安全检测	车端总线网络安全检测	车载CAN/CANFD总线安全
		车载以太网总线安全
	车端无线网络安全	车载蓝牙网络安全
		车载WLAN网络安全

检测级别	检验项目	
		车载NFC网络安全
		车载GNSS安全
		车载蜂窝网络安全
	车端主机网络安全	车端固件安全
		车端接口安全
		车载主机漏洞扫描

5 车联网网络安全检测技术要求

5.1 车端总线网络安全检测

5.1.1 车载 CAN/CANFD 总线安全检测

车载 CAN/CANFD 总线安全检测要求包括：

a) 应采用车载 CAN/CANFD 总线数据真实性、保密性、完整性、可用性、访问可控性、抗抵赖、可核查性、可预防性等安全检测技术；

b) 应支持如下报文检测内容：

1) 具备CAN/CAN FD报文模糊测试；
2) 具备按照配置报文类型（CAN、CANFD）和格式（标准帧、扩展帧）配置测试内容；
3) 具备配置报文发送时间间隔；
4) 具备按照随机及枚举配置模糊策略；
5) 具备配置报文ID、DLC模糊点；
6) 具备按位配置报文payload模糊内容。

c) 应支持总线泛洪攻击测试，具体包括：

1) 具备CAN/CAN FD泛洪攻击测试；
2) 具备按照报文类型配置泛洪攻击测试内容；
3) 具备发送时间间隔、频率、负载率等配置策略。
4) 具备按照随机及指定报文内容进行泛洪攻击测试。

d) 应支持 UDS 检测，具体内容包括：

1) 具备UDS探测功能；
2) 具备CAN/CAN FD网络诊断协议测试；
3) 具备诊断协议的安全性验证；
4) 具备UDS诊断协议漏洞扫描。

5.1.2 车载以太网总线安全检测

车载以太网总线安全检测要求包括：

a) 应采用车载以太网总线数据真实性、保密性、完整性、可用性、访问可控性、抗抵赖、可核查性、可预防性等安全检测技术；

b) 协议要求包括：

1) 应覆盖数据链路层、网络层、传输层和应用层协议；

2) 具备提供不同协议层的流量仿真、流量解析、流量监控、流量统计和流量回放等基础功能；
3) 覆盖Ethernet II、TCP、UDP、IP、ICMP、ARP、SOME/IP、DoIP、DDS、MQTT等协议模块。

c) 应具备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；
d) 应具备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；
e) 应具备车载以太网安全管理策略检测：
1) 通信名单过滤检测；
2) 命令来源校验检测；
3) 网络分域检测；
4) 车载以太网访问控制策略检测。

5.2 车端无线网络安全检测

5.2.1 车载蓝牙网络安全检测

车载蓝牙网络安全检测要求包括：
a) 应采用外部 ETC 设备真实性检测技术，检测外部 ETC 设备的真实性；
b) 车载蓝牙网络安全检测应确保外部 ETC 设备真实性，具备强化身份认证、数据加密、信任管理与证书验证等技术，具备定期安全评估与更新机制，具备安全风险分析（包括未授权访问、数据篡改、身份伪装）；
c) 应采用蓝牙协议版本识别技术，检测整车蓝牙协议为最新版本保证其安全性；
d) 车载蓝牙协议版本检测应具备专业诊断工具与适配的移动应用通过车辆的 OBD-II 端口获取详细信息，制造商应提供完整车辆手册或网站获取蓝牙版本信息，通过在线更新方式更新蓝牙固件；
e) 应采用车载蓝牙访问技术，检测车载蓝牙网络信息安全审计功能，记录通过近场访问点进行通信的用户行为和重要安全事件，包括事件的日期、用户、时间类型、事件成功与否及其其他审计相关信息；
f) 车载蓝牙网络信息安全审计功能应包括记录车联网系统发生的安全相关事件（如登录和登出事件、权限更改、文件访问、网络活动等），具备实时监视网络异常流量、系统日志、文件访问权限等安全事件和行为，具备行为分析识别异常行为和具有攻击迹象的行为，具备安全事件响应机制，具备报告与分析功能进行安全状况评估提出改进建议；
g) 应采用车载蓝牙网络程序启动技术，检测车载蓝牙网络启动程序是否具有可信验证机制；
h) 采用车载蓝牙网络程序启动技术检测可信验证机制，应通过安全审计、静态和动态分析以及渗透测试综合评估车载蓝牙系统的安全性，具备验证加密通信的实施情况和认证过程的强度，确保只有授权的设备和用户可以访问和控制车载网络，具备定期检查软件和固件更新。

5.2.2 车载 WLAN 网络安全检测

车载 WLAN 网络安全检测要求包括：
a) 应采用外部 ETC 设备真实性检测技术，检测外部 ETC 设备的真实性；
b) 应检测关闭 WLAN 网络自动连接功能；

c) 应检测车载 WLAN 网络信息安全审计功能，记录通过近场访问点进行通信的用户行为和重要安全事件，包括事件的日期、用户、时间类型、事件成功与否及其其他审计相关信息；
d) 应采用车载 WLAN 网络程序启动技术，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

车载 NFC 网络安全检测要求包括：
a) 应采用外部 ETC 设备真实性检测技术，检测外部 ETC 设备的真实性；
b) 应采用外部 RFID 设备真实性检测技术，检测外部 RFID 设备的真实性；
c) 应检测车载 NFC 网络信息安全审计功能，记录通过近场访问点进行通信的用户行为和重要安全事件，包括事件的日期、用户、时间类型、事件成功与否及其其他审计相关信息；
d) 应检测车载 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

车载 GNSS 安全检测要求包括：
a) 应采用数据完整性检测技术，检测远程访问通信中是否有校验技术和密码技术；
b) 应采用数据保密性检测技术，检测远程访问通信中是否密码技术；
c) 应采用模拟攻击技术，检测车载 GNSS 网络是否具备入侵检测设备；
d) 应能够通过远程访问点访问车载 GNSS 网络，检测车载 GNSS 网络是否具备信息安全审计功能；
e) 应采用车载 GNSS 非法启动技术，检测车载 GNSS 是否有可信验证机制。

5.2.5 车载蜂窝网络安全检测

车载蜂窝网络安全检测要求包括：
a) 车辆应具备允许用户手动开启或关闭蜂窝网络连接的功能，应当检测是否具备手动开启与关闭蜂窝网络连接的功能；
b) 车辆与云端服务平台通信应采用完整性校验机制，保护通信数据防止恶意篡改，应当检测通信数据是否具有完整性保护机制；
c) 车辆与云端通信应采用加密机制保护通信数据机密性，应当检测通信数据是否加密；
d) 车辆与云端通信应采用身份认证机制避免恶意攻击者伪造通信实体，应当检测通信是否采用身份认证机制；
e) 应当具备防止报文重放的机制，避免报文重放攻击，应当检测通信数据是否具备防重放机制；
f) 车辆宜具备入侵检测功能，能够检测到攻击源、攻击事件，同时发出警报，应当检测是否具备蜂窝网络入侵检测能力；
g) 车辆应具备安全审计功能，记录通过远程访问点访问蜂窝网络进行通信的用户行为和重要安全事件，包括事件的日期、用户、时间类型、事件成功与否及其其他审计相关信息，应当检测车辆是否具备蜂窝网络安全审计功能；
h) 车辆宜采用车载蜂窝网络安全启动技术，应检测车载蜂窝网络是否有可信验证机制。

5.3 车端主机网络安全检测

5.3.1 车端固件安全检测

车端固件安全检测要求包括：

a) 应具备启动自检机制，保证固件的完整性，例如使用安全散列算法等方式进行固件的完整性检查；
b) 在对固件进行启动操作时，应对固件真实性进行校验，不应执行未经合法有效签名的引导程序及固件，且在执行引导程序前应对签名的有效性进行验证；
c) 安全启动宜始于基于硬件的可信根，可信根在出厂后应无法被修改；
d) 应对安全启动的密钥进行安全存储，禁止非授权访问和篡改。

5.3.2 车端接口安全检测

车端接口安全检测要求包括：

a) 应采用可定制恶意代码攻击技术通过 USB 设备进行入侵，检测 USB 设备是否具备主动免疫功能；
b) 应采用模拟非授权 OBD 外部设备接入技术，检测 OBD 设备是否具有识别非法接入行为，并进行阻止；
c) 应采用模拟非授权传感器设备接入技术，检测传感器接口是否具有识别非授权传感器接入行为，并进行阻止；
d) 应采用模拟车端接口接入技术，检测车端接口信息安全审计功能，是否记录通过接触式访问点进行通信的用户行为和重要安全事件，包括事件的日期、用户、时间类型、事件成功与否及其其他审计相关信息；
e) 应采用模拟车端接触式访问启动程序技术，直接对其进行启动，检测车端接口启动程序是否具有可信验证机制。

5.3.3 车载主机漏洞扫描

应采用漏洞扫描技术，检测固件、操作系统和应用软件不应存在未经处置的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，并生产检测报告。

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 车联网网络安全检测技术验证方法

6.1 车端总线网络安全检测技术验证

6.1.1 车载 CAN/CANFD 总线安全检测技术验证

车载 CAN/CANFD 总线安全检测技术验证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，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 消息的注入攻击，检查系统是否能够检测到异常消息并做出适当处理；

e) 模拟通过篡改 CAN/CANFD 消息实现的欺骗攻击，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) 模拟车载 CAN/CANFD 总线上的嗅探攻击，检查系统是否具备足够的安全防护措施；
g) 模拟 CAN/CANFD 总线上的拒绝服务（DoS）攻击，检查系统是否具备足够的稳定性和抗攻击能力；
h) 模拟利用 CAN/CANFD 总线上漏洞实现的远程代码执行攻击，检查系统是否能够及时发现并应对此类攻击行为；
i) 模拟用户通过 OBD-II 等外部接口向 CAN/CANFD 总线上发送消息，验证系统是否具备实时监测 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技术验证

车载以太网总线安全检测技术验证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，判断 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，判断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，检测以太网总线在泛洪攻击的过程中，是否能保证正常业务正常运行；
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，判断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技术验证

6.2.1 车载蓝牙网络安全检测技术验证

车载蓝牙网络安全检测技术验证按照下列流程及要求进行：
a) 接入伪造的 ETC 外围设备，通过强化认证机制验证正在通信的 ETC 设备身份。数据传输加密，保护通信不被监听和篡改，通过信任管理，实时检查 ETC 设备的证书状态，一旦检测到伪造设备，自动触发报警提示机制；
b) 接入伪造的 RFID 外围设备，通过强化认证机制验证正在通信的 RFID 设备身份。数据传输加密，保护传输不被监听和篡改，通过信任管理，为 RFID 标签和读写器实施证书管理机制，实时检查 RFID 标签的证书状态，一旦检测到伪造设备，自动触发报警提示机制；
c) 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：蓝牙测试诊断软件、车辆制造商诊断软件、移动诊断应用）检查车载系统中实现的蓝牙协议版本，确认是否为市场上最新的版本；

d) 模拟用户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、具体时间类型（包括连接建立、数据传输等）、事件成功与否及其其他审计相关信息（如数据传输大小、通信协议等）；
e) 模拟攻击中，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），模拟者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。评估者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，记录问题并提出改进建议。

6.2.2 车载 WLAN 网络安全检测技术验证

车载 WLAN 网络安全检测技术验证按照下列流程及要求进行：
a) 接入伪造的 ETC 外围设备，系统是否可检测出伪造 ETC 设备，并报警提示；
b) 接入伪造的 RFID 外围设备，系统是否可检测出伪造 RFID 设备，并报警提示；
c) 检查车端系统的蓝牙协议，协议版本是否达到市场主流最新版本；
d) 检查系统 WLAN 功能，用户是否具备自行关闭 WLAN 网络自动连接功能；
e) 模拟用户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、时间类型、事件成功与否及其其他审计相关信息等；
f) 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 网络安全检测技术验证

车载 NFC 网络安全检测技术验证按照下列流程及要求进行：
a) 接入伪造的 ETC 外围设备，系统是否可检测出伪造 ETC 设备，并报警提示；
b) 接入伪造的 RFID 外围设备，系统是否可检测出伪造 RFID 设备，并报警提示；
c) 检查车端系统的蓝牙协议，协议版本是否达到市场主流最新版本；
d) 检查系统 WLAN 功能，用户是否具备自行关闭 WLAN 网络自动连接功能；
e) 模拟用户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、时间类型、事件成功与否及其其他审计相关信息等；
f) 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。

6.2.4 车载 GNSS 安全检测技术验证

车载 GNSS 安全检测技术验证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，测试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，测试验证在通信过程中是否对数据进行加密；
c) 采用安全渗透测试模拟安全攻击，查看系统是否具备入侵检测功能，并能是被攻击源、攻击事件，并同时进行报警提示；
d) 模拟用户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、时间类型、事件成功与否及其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技术验证

车载蜂窝网络安全检测技术验证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) 在场上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，检测接收方是否接收并处理报文；
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；基于厂商声明的密码算法、密钥检测算法是否与声明一致，是否具备足够安全强度；
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具备报文防重放机制；
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) 模拟用户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、时间类型、事件成功与否及其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技术验证

6.3.1 车端固件安全检测技术验证

车端固件安全检测技术验证按照下列流程及要求进行：

a) 车端采用非完整固件，网络安全测试工具对固件进行检测，查看测试报告是否有固件为不完整固件记录；
b) 车端采用非真实固件，网络安全测试工具对固件进行检测，查看测试报告是否有固件为非真实固件记录；
c) 修改固件可信根，查看测试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，查看测试报告中是否有密钥非安全存储记录。

6.3.2 车端接口安全检测技术验证

车端接口安全检测技术验证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) 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) 非授权的传感器设备接入车端，查看系统是否检测非授权传感器设备，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、时间类型、事件成功与否及其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，系统应阻止程序运行。

6.3.3 车载主机漏洞扫描技术验证

车载主机中植入国家权威漏洞平台（注：5.3.3 释义）公开发布 6 个月及以上的高中危安全漏洞，网络安全测试工具应在检测报告中对漏洞进行汇总。

参考文献

[1] DB4403/T 355-202 智能网联汽车整车信息安全技术要求
[2] 20214422-Q-339 汽车整车信息安全技术要求
[3] GA/T 681-2018 信息安全技术网关安全技术要求
[4] GB/T 35273-2020 信息安全技术 个人信息安全规范
[5] GB/T 37092-2018 信息安全技术 密码模块安全要求
[6] GM/T 0008-2012 安全芯片密码检测准则
[7] YD/T 3746-2020 车联网信息服务用户个人信息保护要求