ICS 43.020

CCS T 40

中华人民共和国国家标准

GB XXXXX—XXXX

汽车整车信息安全技术要求

Technical requirements for vehicle cybersecurity

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由中华人民共和国工业和信息化部提出并归口。

汽车整车信息安全技术要求

1 范围

本文件规定了汽车信息安全管理体系要求、车辆信息安全一般要求、车辆信息安全技术要求、审核评估及测试验证方法。

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。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。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 XXX《智能网联汽车 数据通用要求》。

3 术语和定义

GB/T XXX《智能网联汽车 术语和定义》GB XXX《汽车软件升级通用技术要求》界定的以及下列术语和定义适用于本文件。

3.1

汽车信息安全管理体系 cybersecurity management system

一种基于风险的系统方法，包括组织流程、责任和治理，以处理与车辆网络威胁相关的风险并保护车辆免受网络攻击。

3.2

风险 risk

车辆信息安全不确定性的影响，可用攻击可行性和影响表示。

3.3

风险评估 risk assessment

发现、识别和描述风险，理解风险的性质以及确定风险级别，并将风险分析的结果与风险标准进行比较，以确定风险是否可接受的过程。

3.4

威胁 threat

可能导致系统、组织或个人受到伤害的意外事件的潜在原因。

3.5

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。

3.6

车载软件升级系统 on-board software update system

安装在车端并具备直接接收、分发来自车外的升级包等实现软件升级功能的软件和硬件。

3.7

在线升级 over-the-air update

通过无线方式而不是使用电缆或其他本地连接进行数据传输的软件升级。

3.8

离线升级 offline update

除在线升级以外的软件升级。

3.9

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，可能导致车主、驾驶人、乘车人、车外人员等受到歧视或者人身、财产安全受到严重危害的个人信息，包括车辆行踪轨迹、音频、视频、图像和生物识别特征等信息。

[来源：汽车数据安全管理若干规定（试行），第三条]

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）
ECU：电子控制单元（Electronic Control Unit）
HSM：硬件安全模块（Hardware Security Module）
MD5：MD5信息摘要算法(MD5 Message-Digest Algorithm)
NFC：近距离无线通讯技术(Near Field Communication)
TLS：安全传输层协议（Transport Layer Security）
USB：通用串行总线(Universal Serial Bus)
VLAN：虚拟局域网（Virtual Local Area Network）
VIN： 车辆识别代号（Vehicle Identification Number）
WLAN：无线局域网(Wireless Local Area Networks)

5 汽车信息安全管理体系要求

5.1 车辆生产企业应具备车辆全生命周期的汽车信息安全管理体系。

注：车辆全生命周期包括车辆的开发阶段、生产阶段及后生产阶段。

5.2 汽车信息安全管理体系应涵盖以下过程。

——应建立企业内部管理汽车信息安全的过程。

——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处置的过程，并确保车辆风险评估保持最新状态。

——应建立用于车辆信息安全测试的过程。

——应建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及漏洞上报过程，要求如下：

a) 应包含漏洞管理机制，明确漏洞收集、分析、报告、处置、发布、上报等活动环节；
b) 应建立针对网络攻击提供相关数据并进行分析的过程；

示例：企业具备从车辆数据和车辆日志中分析和检测网络攻击、网络威胁和漏洞的能力。

c) 应建立确保对网络攻击、网络威胁和漏洞进行持续监控的过程，且车辆纳入监控范围的时间应不晚于车辆注册登记的时间。
d) 应建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在时限内得到处置的过程；
e) 应建立评估所实施的信息安全措施在发现新的网络攻击、网络威胁和漏洞的情况下是否仍然有效的过程。

——应建立管理企业与合同供应商、服务提供商、车辆生产企业子组织之间汽车信息安全依赖关系的过程。

6 车辆信息安全一般要求

6.1 车辆产品开发流程应遵循汽车信息安全管理体系要求。

6.2 车辆生产企业应识别和管理车辆与供应商相关的风险。

6.3 车辆生产企业应识别车辆的关键要素，对车辆进行风险评估，并管理已识别的风险。

注1：风险评估的范围涵盖车辆的各个要素及其相互作用，并进一步考虑与外部系统的相互作用。

注2：关键要素包括但不限于有助于车辆安全、环境保护或防盗的要素，以及提供连接性的系统部件或车辆架构中对信息安全至关重要的部分等。

6.4 车辆生产企业应采取基于第 7 章、第 8 章、第 9 章、第 10 章的信息安全技术要求处置措施保护车辆不受风险评估中已识别的风险影响。

——若处置措施与所识别的风险不相关，车辆生产企业应说明其不相关性。

——若处置措施不足以应对所识别的风险，车辆生产企业应实施其它的处置措施， 并说明其使用措施的合理性。

6.5 如有专用环境，车辆生产企业应采取措施，以保护车辆用于存储和执行后装软件、服务、应用程序或数据的专用环境。

6.6 车辆生产企业应通过测试来验证所实施的信息安全措施的有效性。

6.7 车辆生产企业应针对车辆实施相应措施，以识别针对该车辆的网络攻击，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。

6.8 车辆生产企业应采用符合国际通用、国家或行业标准要求的密码模块。若使用的密码模块不符合国际通用、国家或行业标准要求，则应说明其使用的合理性。应使用公开的、已发布的、有效的密码算法，并选择适当的参数和选项；应根据不同密码算法和业务场景，选择适当长度和有效的密钥。

6.9 车辆应采用默认安全设置。

示例：如 WLAN 的默认连接口令应满足复杂度的要求。

6.10 汽车数据处理活动中的数据车内处理、默认不收集、精度范围适用、脱敏处理、个人同意及显著告知等要求，应符合 GB/T XXX《智能网联汽车 数据通用要求》中 4.2.2 的规定。

7 车辆外部连接安全要求

7.1 一般安全要求

7.1.1 车端具备远程控制功能的系统、授权的第三方应用等外部连接系统不应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：处置包括消除漏洞、制定减缓措施等方式。

7.1.2 车辆应关闭不必要的网络端口。

7.2 远程控制安全要求

7.2.1 应对远程控制指令信息进行真实性和完整性验证，并应具备验证失败的处理能力。

7.2.2 应对远程控制指令设置访问控制，禁用非授权的远程控制指令。

7.2.3 应具备记录远程控制指令的安全日志功能，安全日志记录的内容至少包括远程控制指令的时间、发送主体、远程控制对象、操作结果等，留存相关的安全日志不少于六个月。

7.2.4 应对车端具备远程控制功能的系统进行完整性验证。

7.3 第三方应用安全要求

7.3.1 应对授权的第三方应用的真实性和完整性进行验证。

注：第三方应用是指车辆生产企业及其供应商之外的其他实体提供的面向用户提供服务的应用程序，包括第三方娱乐应用等。

7.3.2 应对非授权的第三方应用的安装进行提示，并对已安装的非授权的第三方应用进行访问控制，限制此类应用直接访问系统资源、个人信息等。

7.4 外部接口安全要求

7.4.1 应对外部接口进行访问控制保护，禁止非授权访问。

注：外部接口包括USB接口、诊断接口和其他可直接接触的物理接口。

7.4.2 应对 USB 接口、SD 卡接口接入设备中的文件进行访问控制，只允许读写指定格式的文件或安装执行指定签名的应用软件。

7.4.3 应具备识别或抵御 USB 接口接入设备中的病毒程序和携带病毒的媒体文件/应用软件的能力。

7.4.4 通过诊断接口发送车辆关键配置及标定参数的写操作指令时，应采用身份鉴别或访问控制等安全策略。

8 车辆通信安全要求

8.1 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。

8.2 车辆与车辆、路侧单元、移动终端等进行 V2X 直连通信时，应进行证书有效性和合法性的验证。

8.3 车辆应采用完整性保护机制保护外部无线通信通道。

示例：车辆外部通信通道包括移动蜂窝通信、WLAN、蓝牙等，不包括射频、NFC 等无线通信通道。

8.4 车辆应具备对来自车辆外部通信通道的数据操作指令的访问控制机制。

注：来自车辆外部通信通道的数据操作指令包括代码注入、数据操纵、数据覆盖、数据擦除和数据写入等指令。

8.5 车辆应验证所接收的外部关键指令数据的有效性或唯一性。

注：关键指令数据是指可能影响行车和财产安全的指令数据，包括但不限于车控指令数据。

示例：针对远程控制服务器发送的车控指令，车端可通过网关校验该类指令的有效性或唯一性。

8.6 车辆应对向车外发送的敏感个人信息实施保密性保护措施。

8.7 车辆应具备与外部直接无线通信的零部件的身份识别机制。

注：与外部存在直接无线通信的零部件包括但不限于车载信息交互系统等，不包括短距离无线传感器。

8.8 车辆与外部直接无线通信的零部件应具备安全机制防止非授权的特权访问。

注：非授权用户可能通过调试接口获得系统的根用户或特权用户权限。

8.9 应对车辆内部网络进行区域划分并对区域边界进行防护。跨域请求应进行访问控制，并遵循默认拒绝原则和最小化授权原则。

注：区域边界防护措施包括物理隔离、逻辑隔离（如采用白名单、防火墙、VLAN）等。

8.10 车辆应具备识别车辆通信通道遭受拒绝服务攻击的能力，并对攻击进行相应的处理。

注1：对攻击的处理包括对攻击数据包的拦截或丢弃、受影响系统的自动恢复、日志记录等。

注2：车辆通信通道包括移动蜂窝通信、V2X、CAN总线、车载以太网等。

8.11 车辆应具备识别恶意的 V2X 数据、恶意的诊断数据的能力，并采取保护措施。

注：V2X数据包括路侧单元发送到车辆的数据、车辆与车辆之间的数据。

8.12 应具备记录关键的通信信息安全事件日志的功能，安全事件日志存储时长为不低于 6 个月。

注：关键的通信信息安全事件由车辆生产企业根据风险评估的结果确定。

9 车辆软件升级安全要求

9.1 一般安全要求

9.1.1 车载软件升级系统应通过安全保护机制，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，或在被篡改后，通过安全保护机制使其无法正常启动。

9.1.2 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。

9.2 在线升级安全要求

9.2.1 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，并在下载中断恢复时重新验证。

示例：常见的认证方式包括使用证书进行身份认证等。

9.2.2 车辆应对下载的在线升级包进行真实性和完整性校验。

9.2.3 不通过车载软件升级系统、直接联网并完成在线升级的 ECU 应具备安全保护机制，保护可信根、引导加载程序、系统固件不被篡改，或在被篡改后，通过安全保护机制使其无法正常启动。

9.2.4 应对在线升级过程中发生的失败事件进行日志记录，日志存储时长为不低于 6 个月。

注：失败事件包括升级包校验失败等，记录内容包括事件时间、失败原因等。

9.3 离线升级安全要求

9.3.1 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。

9.3.2 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，且校验离线升级包的真实性和完整性。

10 车辆数据安全技术要求

10.1 车辆应采取安全访问技术或安全存储技术保护存储的对称密钥和非对称密钥中的私钥，防止其被非授权访问和获取。

10.2 车辆应采取安全访问技术、加密技术或其他安全技术保护存储在车内的敏感个人信息，防止其被非授权访问和获取。

10.3 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）等用于车辆身份识别的数据，防止其被非授权删除和修改。

注：防止数据被非授权删除和修改的安全防御机制包括安全访问技术、只读技术等。

10.4 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。

注：关键数据包括制动参数、安全气囊展开阈值、动力电池参数等关键配置参数，以及其他车辆运行过程中产生的可能影响行车安全的数据。

10.5 车辆应采取安全防御机制保护存储在车内的安全日志，防止其被修改和非授权删除。

10.6 车辆应具备个人信息删除功能，便于车辆用户在车辆转售、租借和报废等删除个人信息。法律、行政法规、强制性国家标准中规定的其他情形除外。

10.7 车辆不得直接向境外传输数据。

注：用户使用浏览器访问境外网站、使用通信软件向境外传递消息、自主安装可能导致数据出境的第三方应用等用户自主行为不受本条款限制。

11 审核评估及测试方法

11.1 依据本文件开展车辆型式检验前，应确认车辆生产企业满足第 5 章汽车信息安全管理体系要求。

11.2 车辆型式检验包括车辆信息安全一般要求评估和车辆信息安全技术要求检验。

12 车辆型式的扩展

12.1 总则

依据本文件通过型式检验的车型，其结果可扩展到符合12.2直接扩展判定条件a)-i)判定条件的其他车型。车型获得扩展后，此扩展车型不可再扩展到其他车型。

12.2 直接扩展判定条件

a) 车辆生产企业相同；
b) 通过汽车信息安全管理体系审核；
c) 车型整车电子电气架构相同且安全处置措施相同；
d) 中央网关的硬件型号相同；
e) 车载软件升级系统硬件型号相同；
f) 具备蜂窝移动通信系统功能的零部件硬件型号相同；
g) 车辆无线通信方式所使用的协议类型、协议版本、接口类型、数量相同或减少；

注：无线通信方式包含WLAN、蓝牙、NFC、蜂窝通讯、V2X等。

h) 车辆外部接口的类型、数量相同或减少；
i) 与车型直接连接并产生数据交互的车辆生产企业云平台 IP 地址或域名相同。

12.3 审核后扩展的判定条件

若车型发生涉及12.2直接扩展判定条件c)-i)的变更，经开展风险评估后，确认整车信息安全风险未增加的，应提交车型风险评估总结声明，经审批许可后获得扩展。

示例：常见的不影响整车信息安全的改动包括替换与信息安全无关的系统或部件、ECU 性能升级但不增加新的功能、变更 ECU 零部件供应商但不改变信息安全配置、用于修复漏洞或性能优化的软件升级、不影响信息安全的功能变更或新增功能（如在原有远程控车功能的基础上增加新的控车功能，且不涉及通信方式的改变）等。

12.4 测试验证后扩展的判定条件

若车型发生涉及12.2直接扩展判定条件c)-i)的变更，经开展风险评估后，确认整车信息安全风险增加，但未严重影响整车信息安全的，应提交车型风险评估总结声明，并针对受影响的项目补充测试验证，测试验证通过后可获得扩展。

示例：常见的未严重影响整车信息安全的改动包括通信系统升级但不引入新的通信方式（如使用第五代移动通信系统替换第二代移动通信系统），影响信息安全的 ECU 功能变更或增加新的功能等。

12.5 无法扩展的判定条件

a) 车辆生产企业发生变更；
b) 汽车信息安全管理体系失效；
c) 若车型发生涉及 12.2 直接扩展判定条件 c)-i)的变更，经开展车型风险评估后，确认严重影响整车信息安全的。

示例：常见的严重影响整车信息安全的变更包括改变车辆网络拓扑（如增加新的网关）、增添新的外部接口类型、增加新的网络通信方式（如增加 CAN/车载以太网）。

13 实施日期

对于新申请型式批准的车型，自本文件实施之日起开始执行。
对于已获得型式批准的车型，自本文件实施之日起第 25 个月开始执行。

附 录 A
（规范性）
车辆信息安全要求测试验证方法

A.1 概述

本附录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安全要求的测试验证方法。开展测试验证前，应评估确认满足第6章车辆信息安全一般要求。

A.2 测试条件

A.2.1 应在车辆运行安全的环境下进行测试，如汽车转鼓试验台。

A.2.2 应在车辆通信环境不被干扰的环境下进行测试，如信号屏蔽室。

A.2.3 车辆生产企业应按照测试要求提供测试整车车辆，必要时需提供测试台架。

A.2.4 车辆生产企业应按照测试方法对车辆进行预处理。

A.3 车辆外部连接安全测试方法

A.3.1 具备远程操控功能的系统安全测试方法

A.3.1.1 真实性和完整性校验的测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.1.1的要求：

a）登录车辆远程控制程序账户，触发远程车辆控制指令；

b）尝试伪造、篡改并发送远程车辆控制指令，检查车辆是否执行该指令，是否按照企业设定的验证失败处理机制进行处理，若无法伪造、篡改该指令或不执行该指令，则测试通过，否则不通过。

A.3.1.2 远程控制指令控制测试方法

测试人员应依据企业提供的车辆远程控制指令应用场景和使用权限，并按照如下测试方法，检验测试车辆是否满足正文7.1.2的要求：

尝试发送超出权限的远程控制指令，检查车辆是否执行该指令，若无法发送该指令或车辆不执行该指令，则测试通过，否则不通过。

A.3.1.3 安全日志记录功能测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.1.3的要求：

a) 触发车辆远程控制功能，检验安全日志记录的内容是否包含远程控制指令的时间、发送主体、远程控制对象、操作结果等信息，若包括远程控制指令的时间、发送主体、远程控制对象、操作结果等信息，则测试通过，否则测试不通过；

b) 核查安全日志记录的时间跨度是否不少于六个月或是否具备留存安全事件日志不少于六个月的能力，若时间跨度不少于六个月或具备留存安全事件日志不少于六个月的能力，则核查通过，否则核查不通过。

A.3.1.4 远程控制功能系统完整性校验核查方法

测试人员应按照如下核查方法，核查测试车辆是否满足正文7.1.4的要求：

核查具备远程控制功能的系统的完整性验证的安全检测报告，若对该系统进行完整性验证，则测试通过，否则测试不通过。

A.3.2 第三方应用安全测试方法

A.3.2.1 授权第三方应用真实性完整性验证测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.2.1的要求：

a) 获取授权的第三方应用，使用工具篡改其代码；
b) 尝试安装并执行篡改后的授权第三方应用，测试是否可以正常安装或运行，若不可正常安装或运行，则测试通过，否则测试不通过。

注：若限制篡改后的授权第三方应用访问超出访问控制权限的资源，视为应用非正常运行，满足要求。

A.3.2.2 非授权第三方应用访问控制测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.2.2的要求：

a) 尝试安装非授权第三方应用，测试车辆是否进行提示，应有明确提示；
b) 尝试使用非授权第三方应用访问超出访问控制权限的资源，若无法访问控制权限外的资源，则测试通过，否则测试不通过。

A.3.3 外部接口安全测试方法

A.3.3.1 外部接口访问控制测试方法

测试人员应依据企业提供的车辆外部接口的总结文档或车辆外部接口清单，并按照如下测试方法，检验测试车辆是否满足正文7.3.1的要求：

使用非授权的用户或工具访问车辆的外部接口，测试是否可以成功建立连接并访问相应的信息，若无法成功建立连接，则测试通过，否则测试不通过。

A.3.3.2 USB 接口、SD 卡接口访问控制测试方法

测试人员应依据企业提供的USB接口、SD卡接口的总结文档或USB接口、SD卡接口支持的文件类型清单，并按照如下测试方法，检验测试车辆是否满足正文7.3.2的要求：

a) 分别在具备 USB 接口、SD 卡接口的移动存储介质中注入指定格式文件、 指定签名的应用软件和其它非指定格式文件和非指定签名的应用软件；
b) 将移动存储介质分别连接到车辆 USB 接口、SD 卡接口，测试车辆是否可以读写非指定格式文件，是否可以安装执行非指定签名的应用软件，若无法读写非指定格式文件和安装执行非指定签名的应用软件，则测试通过，否则测试不通过。

A.3.3.3 USB 防病毒测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.3.3的要求：

a) 在具备 USB 接口的移动存储介质中注入病毒程序和携带病毒的媒体文件/应用软件等病毒文件；
b) 将移动存储介质连接到车辆 USB 接口，测试车辆系统是否可以识别出移动存储介质中的病毒文件或抵御病毒文件，若能识别出病毒文件或抵御病毒文件，则测试通过，否则测试不通过。

A.3.3.4 诊断接口身份鉴别测试方法

测试人员应按照以下两种测试方法中适用的测试方法，检验测试车辆是否满足正文7.3.4的要求：

a) 使用非授权用户或工具在诊断接口发送车辆关键配置及标定参数的写操作指令，测试车辆是否执行该操作指令，若无法执行该操作指令，则测试通过，否则测试不通过；

b) 使用工具在诊断接口发送车辆关键配置及标定参数的写操作指令，测试车辆是否存在访问控制机制，若存在访问控制机制，则测试通过，否则测试不通过。

A.3.4 车辆外部连接系统漏洞扫描测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文7.4的要求：

a) 使用漏洞扫描工具对车辆外部连接系统进行漏洞检测，检测是否存在权威漏洞平台 6 个月前公布的高危及以上的安全漏洞，若不存在，则测试通过；

b) 若存在高危及以上的安全漏洞，则检查厂商是否提供了该漏洞的处置方案，若存在处置方案，则测试通过，否则测试不通过。

A.3.5 车辆关闭不必要端口测试方法

测试人员应依据企业提供的车辆业务端口列表，按照如下测试方法，检验测试车辆是否满足正文7.5的要求：

a) 测试人员通过 WLAN、车载以太网、蜂窝网络等形式将测试车辆与扫描测试设备组网；

b) 使用扫描测试设备查看测试车辆所开放的端口，并将车辆开放的端口列表与车辆业务端口列表进行对比，测试车辆是否开放非必要的网络端口，若仅开放必要的网络端口，则测试通过，否则测试不通过。

A.4 车辆通信安全测试方法

A.4.1 云平台通信身份真实性验证测试方法

测试人员应依据企业提供的车辆生产企业云平台清单及采用的通信协议类型，并按照如下测试方法，检验测试车辆是否满足正文8.1的要求：

a) 若车辆与车辆生产企业云平台通信采用专用网络或虚拟专用网络环境进行通信，核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过；

b) 若车辆与车辆生产企业云平台通信采用公共网络环境进行通信，且使用公有通信协议，采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查车辆是否对生产企业云平台进行身份真实性验证，若对其通信对象的身份真实性进行验证，则测试通过，否则测试不通过；

注：若采用网络数据抓包工具无法进行数据抓包，则核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过；

c) 若车辆与车辆生产企业云平台通信采用公共网络环境进行通信，且使用私有通信协议，核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过。

A.4.2 V2X通信身份认证测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文8.2的要求：

a) 将车辆置于A.2.2所述环境中，由测试设备向测试车辆下发合法证书并与测试车辆进行正常通信，测试车辆应能够接收测试设备的直连通信消息；
b) 测试设备分别生成失效证书和身份伪造证书，向车辆发送通信消息，测试车辆是否能够识别失效证书和身份伪造证书，应验证证书的有效性和合法性，并采取措施。

A.4.3 通信通道完整性保护核查方法

测试人员应按照如下核查方法，核查测试车辆是否满足正文8.3的要求：

核查车辆移动蜂窝通信、WLAN、蓝牙等外部通信通道完整性的安全检测报告，若采用完整性保护机制进行保护，则测试通过，否则测试不通过。

A.4.4 防非授权操作测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文8.4的要求：

使用非授权身份尝试通过车辆外部通信通道对车辆的数据依次进行超出访问控制机制的操作、清除和写入，测试是否可以成功操作、清除和写入，若无法超出访问控制权限的操作、清除和写入数据，则测试通过，否则测试不通过。

A.4.5 关键指令数据有效性或唯一性验证测试方法

测试人员应依据企业提供的关键指令数据列表，并按照如下方法，检验测试车辆是否满足正文8.5的要求：

使用测试设备录制关键指令数据，重新发送录制的指令数据，测试车辆是否做出响应，若不响应，则测试通过，否则测试不通过。

A.4.6 敏感个人信息保密性保护核查方法

测试人员应按照如下核查方法，核查测试车辆是否满足正文8.6的要求：

核查车辆向外发送敏感个人信息的安全检测报告，若对发送的敏感个人信息实施保密性保护措施，则核查通过，否则核查不通过。

A.4.7 对外通信零部件身份识别测试方法

测试人员应依据企业提供的对外直接无线通信的零部件清单，并按照如下测试方法，检验测试车辆是否满足正文8.7的要求。

a) 使用和测试车辆与外部直接无线通信零部件功能相同的零部件替换安装在整车相同的位置；
b) 启动车辆，测试零部件是否功能异常或车辆是否有异常部件连接告警，若不正常工作或有异常告警提示，则测试通过，否则测试不通过。

A.4.8 车辆与外部直接通信零部件防非授权特权访问测试方法

测试人员应依据企业提供的对外直接无线通信零部件系统权限设计方案,并按照如下测试方法，检验测试车辆是否满足正文8.8的要求：

a）若系统只存在特权访问的用户，尝试登录进入系统，若无法登录，则测试通过，否则不通过；

b）若系统存在或可配置多种权限用户，依据非特权用户登录系统方式进入系统，使用系统提权方法尝试对系统进行特权访问，若不可特权访问，则测试通过，否则不通过。

A.4.9 车内安全区域隔离测试方法

测试人员应依据企业提供的通信矩阵、访问控制列表样例，并按照如下测试方法，检验测试车辆是否满足正文8.9的要求：

a）对于使用物理隔离措施的车辆，验证车辆生产企业提供的物理隔离方案，若实现物理隔离，则测试通过，否则测试不通过；

b）对于使用逻辑隔离措施的车辆，根据车辆生产企业提供的逻辑隔离策略，发送不符合策略的数据帧，在指定的目的端口测试是否可以接收到相应的数据帧，若无法接收到相应的数据帧，则测试通过，否则测试不通过。

A.4.10 拒绝服务攻击识别测试方法

测试人员应按照如下测试方法，检验测试车辆移动蜂窝通信、V2X、CAN总线、车载以太网等通信通道拒绝服务攻击识别防护能力是否满足正文8.10的要求。

a） 将车辆置于A.2.1所述环境中，使车辆分别处于静止和运动状态，使用拒绝服务攻击测试设备攻击车辆的通信通道；

b） 查看车辆是否能够识别攻击并进行处理，若能对攻击进行识别并处理，则测试通过，否则测试不通过。

A.4.11 恶意数据识别测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文8.11的要求。

a） 将车辆置于A.2.2所述环境中，使用模糊测试设备向车辆发送当前车况非预期的恶意数据；

b） 测试车辆能否识别并采取保护措施，若能识别并采取保护措施，则测试通过，否则测试不通过。

A.4.12 通信信息安全日志测试方法

测试人员应依据企业提供的车辆关键通信信息安全事件日志记录机制及其存储路径，并按照如下测试方法，检验测试车辆是否满足正文8.12的要求：

a） 构建并触发车辆关键通信信息安全事件，检验车辆是否按照关键通信信息安全事件日志记录机制记录该事件，若按照机制记录该安全事件，则测试通过，否则测试不通过；

b） 核查安全事件日志记录的时间跨度是否不少于六个月或是否具备留存安全事件日志不少于六个月的能力，若时间跨度不少于六个月或具备留存安全事件日志不少于六个月的能力则核查通过，否则核查不通过。

A.5 车辆软件升级安全测试方法

A.5.1 通用安全要求测试方法

A.5.1.1 车载软件升级系统安全保护机制核查方法

测试人员应应按照如下核查方法，核查测试车辆是否满足正文9.1.1的要求：

核查车载软件升级系统的可信根、引导加载程序、系统固件的安全保护机制的安全检测报告，若经过充分和有效的测试验证，证明系统的可信根、引导加载程序、系统固件不能被篡改，或者被篡改后无法正常启动，则核查通过，否则核查不通过。

A.5.1.2 车载软件升级系统安全漏洞扫描测试方法

测试人员应照如下测试方法，检验测试车辆是否满足正文9.1.2的要求：

a) 使用漏洞扫描工具对车载软件升级系统进行漏洞检测，检测是否存在权威漏洞平台 6 个月前公布的高危及以上的安全漏洞，若不存在，则测试通过；

b) 若存在高危及以上的安全漏洞，则检查厂商是否提供了该漏洞的处置方案，若存在处置方案，则通过测试，否则测试不通过。

A.5.2 在线升级安全测试方法

A.5.2.1 软件升级服务器身份认证测试方法

测试人员应依据企业提供的在线升级服务器清单及采用的通信协议类型，并按照如下测试方法，检测测试车辆是否满足正文9.2.1的要求：

a) 若车辆与车辆生产企业云平台通信采用专用网络或虚拟专用网络环境进行通信，核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过；

b) 若车辆与车辆生产企业云平台通信采用公共网络环境进行通信，且使用公有通信协议，采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查车辆是否对生产企业云平台进行身份真实性验证，若对其通信对象的身份真实性进行验证，则测试通过，否则测试不通过；

注：若采用网络数据抓包工具无法进行数据抓包，则核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过；

c) 若车辆与车辆生产企业云平台通信采用公共网络环境进行通信，且使用私有通信协议，核查通信身份真实性的安全检测报告，若车辆对其通信对象的身份真实性进行验证，则核查通过，否则核查不通过。

A.5.2.2 升级包真实性和完整性校验核查方法

测试人员应按照如下核查方法，核查测试车辆是否满足正文9.2.2的要求：

核查车辆对在线升级包真实性、完整性校验的安全检测报告，若车辆具备在线升级功能，且经过充分和有效的测试验证，证明升级包被伪造、篡改之后，无法执行在线升级或升级失败，则核查通过，否则核查不通过。

A.5.2.3 在线升级 ECU 安全保护机制核查方法

测试人员应按照如下测试方法，核查测试车辆是否满足正文9.2.3的要求：

核查不通过车载软件升级系统、直接联网并完成在线升级的ECU的可信根、引导加载程序、系统固件的安全保护机制的安全检测报告，若经过充分和有效的测试验证，证明ECU的可信根、引导加载程序、系统固件不能被篡改，或者被篡改后无法正常启动，则核查通过，否则核查不通过。

A.5.2.4 失败事件日志记录测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文9.2.4的要求：

a) 构造升级失败事件，检验是否存在升级失败事件日志，若记录本次升级失败事件，则测试通过，否则测试不通过；

b) 核查失败事件日志记录的时间跨度是否不少于六个月或是否具备留存安全事件日志不少于六个月的能力，若时间跨度不少于六个月或具备留存安全事件日志不少于六个月的能力则核查通过，否则核查不通过。

A.5.3 离线升级安全要求测试方法

A.5.3.1 使用车载软件升级系统的离线升级安全测试方法

若车辆使用车载软件升级系统进行离线升级，测试人员应按照如下测试方法，检验测试车辆是否满足正文9.3.1的要求：

a) 构造被伪造、篡改的离线升级包；

b) 使用离线升级工具将该升级包下载或传输到车载端，执行软件升级，若不执行升级或升级失败，则测试通过，否则测试不通过。

A.5.3.2 不使用车载软件升级系统的离线升级安全测试方法

若不使用车载软件升级系统进行离线升级，测试人员应按照以下方法依次开展测试，检验测试车辆是否满足正文9.3.2的要求：

a) 测试人员将非认证的刷写接入端接入车辆刷写接口尝试进行升级，查看车辆是否能识别非认证的刷写接入端，若能阻止非认证刷写接入端与车辆进行通信，则测试通过，否则测试不通过；

b) 构造被伪造、篡改破坏的离线升级包，使用认证的刷写接入端接入车辆刷写接口，执行软件升级，若不执行升级或升级失败，则测试通过，否则测试不通过。

A.6 车辆数据代码安全测试方法

A.6.1 密钥防非法获取和访问测试方法

测试人员应依据车辆密码使用方案，确认测试零部件，并按照如下测试方法，检验测试车辆是否满足正文10.1的要求：

a) 通过对车辆零部件级的访问接口与零部件在车辆级状态的访问接口进行破解、提取等攻击操作，若无法实现对零部件中密钥的非授权访问和获取，则测试通过，否则按如下测试步骤进行测试；

b) 若采取 HSM 等硬件安全模块存储密钥，应依据硬件安全模块安装位置说明文档，验证车辆是否安装了硬件安全模块来保护密钥，并记录验证结果,若在文档标识位置安装硬件安全模块，则测试通过，否则测试不通过；

c) 若采取安全的软件存储形式存储密钥，核查车辆密钥安全存储检测报告，若该存储形式经过充分和有效的的测试验证，证明采用该方案存储的秘钥无法被非授权访问和获取，则核查通过，否则核查不通过。

A.6.2 敏感个人信息防泄露测试方法

测试人员应依据敏感个人信息功能清单和存储地址清单，确认测试零部件，并按照如下测试方法，检验已存储敏感个人信息的测试车辆是否满足正文10.2的要求：

a) 依据系统登录方式进入系统，对测试零部件进行敏感个人信息检索，若未检索出不在敏感个人信息功能清单和存储地址清单中存储的敏感个人信息，则测试通过，否则通过不测试；

b) 若采用安全访问技术保护存储的敏感个人信息，依据敏感个人信息存储区域和地址范围说明，通过零部件调试接口，使用未添加访问控制权限的用户访问存储的敏感个人信息，若能够非授权访问敏感个人信息，则测试不通过，若不可非授权访问敏感个人信息，则测试通过；

c) 若采取加密技术保护存储的敏感个人信息，依据敏感个人信息存储区域和地址范围说明，通过零部件调试接口，尝试使用软件分析工具提取存储的敏感个人信息，若为密文存储，则测试通过，否则测试不通过。

A.6.3 车辆身份识别数据防非授权删除和修改测试方法

测试人员应依据车辆内存储的车辆识别代号等用于车辆身份识别的数据清单及存储地址，确定测试零部件，并按照如下测试方法，检验测试车辆是否满足正文10.3的要求：

依据车辆内存储的车辆识别代号等用于车辆身份识别的数据清单及存储地址，尝试使用软件分析工具非授权删除和修改存储在车辆内的车辆识别代号等用于车辆身份识别的数据，测试是否可以被非授权删除和修改，若不可被非授权删除和修改，则测试通过，否则测试不通过。

A.6.4 关键数据防非授权删除和修改测试方法

测试人员应依据车辆内存储的关键数据清单及存储的地址，确定测试零部件，并按照如下测试方法，检验测试车辆是否满足正文10.4的要求：

依据关键数据存储区域和地址范围说明，通过零部件调试接口，尝试使用软件分析工具篡改存储在车内的关键数据，测试是否可以被非授权删除和修改，若不可被非授权删除和修改，则测试通过，否则测试不通过。

A.6.5 日志文件防修改和非授权删除测试方法

测试人员应依据车辆内存储的安全日志清单及存储的地址，确定测试零部件，并按照如下测试方法，检验测试车辆是否满足正文10.5的要求：

a) 依据车型开发档案文件中车辆内存储的安全日志清单及存储的地址，通过零部件调试接口，尝试使用使用企业提供的调试工具修改安全日志文件，测试是否可以使用企业的调试工具修改安全日志文件，若不可被修改，则测试通过，否则测试不通过；

b) 依据车型开发档案文件中车辆内存储的安全日志清单及存储的地址，通过零部件调试接口，尝试使用软件分析工具非授权删除安全日志文件，测试是否可以非授权删除安全日志文件，若不可被非授权删除，则测试通过，否则测试不通过。

A.6.6 个人信息清除功能测试方法

测试人员应依据车型开发档案文件中车辆内存储的个人信息清单及存储的地址，并按照如下测试方法，检验测试车辆是否满足正文10.6的要求：

a) 尝试使用测试车辆个人信息清除功能， 清除车辆内存储的个人信息。

b) 依据车型开发档案文件中车辆内存储的个人信息清单及存储的地址，通过零部件调试接口，查看个人信息是否被删除，若被删除，则通过测试，否则不通过。

A.6.7 防数据直接出境测试方法

测试人员应按照如下测试方法，检验测试车辆是否满足正文10.7的要求：

a) 开启车辆全部移动蜂窝通信网络、WLAN 通信网络，依次模拟测试车辆处于未上电、仅上电、各项预装的数据传输功能正常启用的状态；

b) 使用网络数据抓包工具对对外通信网络通道同时抓包，且抓包时长不少于 3600 秒，，解析通信报文数据，分析目的 IP 地址中是否包含境外 IP 地址，如不包含境外 IP 地址，则测试通过，否则测试不通过。