ICS 43.020

CCS T40

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)

（工作组讨论稿）

（本草案完成时间：2022 年 7 月 29 日）

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.....II
1 范围.....3
2 规范性引用文件.....3
3 术语和定义.....3
4 缩略语.....5
5 信息安全管理体系要求.....6
6 车辆信息安全一般要求.....6
7 车辆外部连接安全要求.....7
8 车辆通信通道安全要求.....7
9 车辆软件升级安全要求.....9
10 车辆数据代码安全要求.....9
11 审核评估及测试方法.....10
12 车辆型式的变更和扩展.....10
13 实施日期.....11
附　录　A　（规范性）　车辆信息安全要求测试及核查方法.....12

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、车辆安全技术要求及评估、试验方法。

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类车辆及其车辆制造商等相关方，其他类型车辆可参考执行。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

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

消息仿冒 message imitation

攻击者利用单个节点来伪造多个身份存在于 P2P 网络中监视或干扰网络正常活动的行为。

3.3

恶意代码 malicious code

被专门设计用于损坏或中断系统、破坏保密性、完整性和 / 或可用性的代码。

3.4

开发阶段 development phase

车型获得批准之前的时期。

3.5

生产阶段 production phase

车型的生产持续期间。

3.6

后生产阶段 post-production phase

从车型不再生产，直至该车型的所有车辆使用寿命结束的时间。在这一阶段，该车型的车辆仍可使用，但不再继续生产。当不再有可使用的该车型车辆时，此阶段结束。

3.7

缓解措施 mitigation

降低风险的措施。

3.8

风险 risk

特定威胁将利用车辆的漏洞，从而对组织或个人造成伤害的可能性。

3.9

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或可承受。

3.10

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。

3.11

漏洞 vulnerability

资产或缓解措施的弱点，可被利用作为攻击路径的一部分。

3.12

关键要素 critical elements

与安全有关，其泄露或修改会危及安全的信息。

3.13

密码模块 cryptographic modules

计算平台中，提供密码运算功能，具有受保护存储空间的物理装置。

3.14

安全审计 security audit

对信息系统记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程三方面提出改进建议。

3.15

审计进程 security audit

获取审核证据并对其进行客观评价以确定满足审核准则程度的，系统的、独立的和文档化的过程。

3.16

消息认证码 message authentication code

消息认证码算法输出的位串。

3.17

身份密钥 identity key

控制密码验证身份的符号序列。

3.18

硬件安全模块 hardware security module

一种执行密码运算、安全生成和存储密钥的硬件设备。

3.19

垃圾数据 garbage data

事先未提出请求或同意接收的数据。

3.20

恶意代码 malicious code

被专门设计用于损坏或中断系统、破坏保密性、完整性和/或可用性的代码。

3.21

在线升级 over-the-air update

车内 ECU 通过网络连接至后台服务器进行软件下载、升级的过程。

[汽车软件升级 通用技术要求，定义3.3]

3.22

离线升级 offline update

除在线升级以外的车内 ECU 软件升级过程。

[汽车软件升级 通用技术要求，定义3.4]

3.23

重要数据 important data

重要数据是指在智能网联汽车及云端运行过程中，各主体间进行信息交互时的数据，通过这些数据能一定程度标识或识别到特定的车联网信息服务的主体、对象或其重要特征，且一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据。

注：重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。

4 缩略语

请选择适当的引导语

5 信息安全管理体系要求

5.1 车辆制造商应建立车辆全生命周期的信息安全管理体系。

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 信息安全管理体系中应建立必要流程，以确保充分考虑安全风险。

5.2.1 应建立企业内部管理信息安全的流程。

5.2.2 应建立识别、评估、分类、处置车辆信息安全风险，核实已识别风险得到适当处置的流程，并确保车辆风险评估保持最新状态。

5.2.3 应建立测试车辆信息安全的流程。

5.2.4 应建立针对车辆的网络攻击、网络威胁和漏洞的监测和响应流程。

a) 应包含漏洞管理机制，明确漏洞收集、分析、报告、修补、发布等活动环节；

b) 应针对网络攻击建立提供相关数据并进行分析的流程；

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

c) 应包含确保已识别的网络威胁和漏洞得到响应，且在合理的时限内得到缓解的流程；

d) 应包含评估所实施的信息安全措施在发现新的网络威胁和漏洞的情况下是否仍然有效的流程

e) 应包含确保对网络攻击、网络威胁和车辆漏洞进行持续监控的流程；

注：车辆登记后即纳入监控范围。

5.2.5 应建立管理企业与合同供应商、服务提供商、制造商子组织之间安全依赖关系的流程。

6 车辆信息安全一般要求

6.1 车辆产品开发流程应遵循信息安全管理体系要求。

6.2 应识别和管理车辆与供应商相关的风险。

6.3 应确认车辆的关键要素，对车辆进行详细的风险评估，合理管理已识别的风险。

注：风险评估可考虑车辆的各个要素及其相互作用，并进一步考虑与任何外部系统的相互作用。

6.4 应采取基于第七章、第八章、第九章、第十章相应的处置措施保护车辆不受风险评估中已识别的风险影响。若第七章、第八章、第九章、第十章相应的处置措施与所识别的风险不相关或不充分，则车辆制造商应确保实施其它适当的处置措施，并说明其使用措施的合理性。

6.5 如有专用网络环境，则应采取相应适当的措施，以保护车辆用于存储和执行售后软件、服务、应用程序或数据的专用网络环境。

6.6 应通过适当和充分的测试来验证所实施的安全措施的有效性。

6.7 应针对车辆实施相应措施，以检测和抵御针对该车辆的网络攻击，支持车辆制造商在检测与车辆相关的威胁、漏洞和网络攻击方面的监测能力，为分析网络攻击提供数据取证能力。

6.8 若使用的密码模块未采用国际通用或国家标准要求，则应说明其使用的合理性。应根据不同加密算法和场景，选择合适长度和有效期的加密密钥；使用开放的、已发布的、有效的密码算法，并选择适当的参数和选项，定期检查以采取相应措施。

注1：适当的参数和选项指处理速度、带宽要求、存储空间等。

注2：有效的密码算法指在安全有效期内且未被破解的算法，如MD5已被破解，此类算法相对不安全；

注3：定期检查包括定期更新算法、定期审核密码算法有效期等措施。

6.9 车辆应采用默认安全设置

示例：如 WIFI、蓝牙的默认连接密码应满足复杂度的要求。

7 车辆外部连接安全要求

7.1 远控系统安全要求

7.1.1 应对远程控制功能的指令信息进行真实性和完整性校验。

7.1.2 包含远程钥匙等远程控制功能的系统，应具备远程控制功能的指令信息真实性和完整性校验失败的处理功能。

7.1.3 应对远程控制指令设置访问控制，禁用控制外的远程控制指令操控系统。

7.1.4 应具备安全审计功能，审计记录的内容包括远程控制指令的日期、时间、发送主体、操作是否成功等。

7.1.5 应对审计记录应进行保护，避免非预期的删除、修改或覆盖等。

7.1.6 应对审计进程进行保护，防止未授权的中断。

7.1.7 应对车端具备远程操控功能的系统的程序和数据进行完整性验证。

7.2 第三方应用安全要求

7.2.1 应对第三方应用的真实性和完整性进行检验。

示例：第三方应用包括第三方娱乐应用等。

7.2.2 应对第三方应用的访问资源进行访问控制，禁止安装和运行非法使用控制外的资源应用。

7.3 外部接口安全要求

7.3.1 应对 USB 端口接入设备中的文件进行访问控制，只允许媒体文件读写或指定签名的应用软件安装或执行。

7.3.2 应对 Jtag 接口、其他调试接口进行访问控制保护，禁止非授权用户访问。

示例：外部接口包括 USB 接口、OBD 接口和其他接口等。

7.3.3 应具备抵御 USB 端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。

7.3.4 通过 OBD 接口发送写操作请求时，应采用身份鉴别、访问控制等安全策略。

注：写操作请求包括基于UDS协议的Control、Clear、Reset请求。

7.3.5 车辆外部连接系统（包括远控功能系统、短距离无线和传感器、第三方应用、外部接口等）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：处置包括消除漏洞、制定减缓措施等方式。

7.3.6 车辆应关闭不必要的网络端口。

8 车辆通信通道安全要求

8.1 数据防欺骗安全要求

8.1.1 车辆应验证所接收数据的真实性和完整性，以防止被仿冒的数据欺骗。

示例：车辆接收的数据类型可能是 V2X 数据、GNSS 数据等。

8.1.1.1 车辆与车辆、路侧单元、服务平台等的通信，应实施身份认证。

8.1.1.2　应采用完整性保护和校验机制，防止车辆接收的数据被篡改或伪造。

注1：在传输数据中带有验证信息（例如采用消息认证码）的方式可实施完整性保护。

注2：常用的数据的完整性保护技术包括校验技术和密码技术。

8.1.2　应对存储的密钥实施安全控制，以防止 V2X 数据仿冒攻击。

8.2　防止未授权操作安全要求

8.2.1　应采用完整性保护和校验机制，以防止通过通信通道注入篡改的代码。

示例：例如通过通信通道注入被篡改的软件二进制代码到通信流中。

8.2.2　应对车辆内部网络进行安全区域划分，对区域边界进行防护，对于不需要通信的物理设备之间至少应实现逻辑隔离。

示例：隔离措施包括采用物理隔离、黑白名单、防火墙等措施。

注1：对于以太网可采用VLAN技术实现不同功能域之间的逻辑隔离。

注2：车内网络可根据功能需要进行隔离，并对跨域请求进行访问控制，访问控制列表应遵循默认拒绝原则及最小化授权原则。

8.2.3　应采用访问控制及相关技术，防止来自外部通道的数据对车辆数据的非法操纵、覆盖、清除，或非法数据代码写入。

8.2.4　应具备对与外部存在通信的零部件的身份识别机制。

8.3　通信数据安全要求

8.3.1　车辆应验证所接收数据的真实性，以防止接收不可靠或不可信来源的数据，或遭受中间人攻击/会话劫持。

8.3.2　车辆应验证所接收数据的有效期或唯一性，以防止遭受重放攻击。

示例：如车辆的远程控制服务器传输的车控指令，车端通过校验该类指令的有效期或唯一性，可防止车控指令被用于重放攻击。

8.4　应建立机密性保护措施，保护车辆接收和发送的机密数据，防止因车辆的通信信息被拦截、干扰辐射或通信监听而导致的敏感信息泄露。

示例：机密数据包括整车故障报警数据、车辆控制类数据、个人敏感信息等。

8.5　防止拒绝服务攻击安全要求

8.5.1　应采取措施测试拒绝服务攻击，并应从该类攻击中恢复，防止通过通信（包括车外通信和车内通信）通道注入大量垃圾数据到车辆通信系统中导致其不能正常提供服务。

8.5.2　应采取措施测试黑洞攻击并从该类攻击中恢复。

注：黑洞攻击可能用于阻止传递给其他车辆的信息，从而中断车辆之间的通信。

8.6　应采取措施测试和防止非特权用户获得对系统的特权访问。

注：非特权用户可能通过调试接口获得系统的根用户权限。

8.7　应通过识别恶意代码攻击等技术措施，识别病毒通过通信媒介的入侵行为。

8.8　防止恶意数据接收安全要求。

8.8.1　应具备测试恶意内部数据或行为的措施。

注：内部数据包括车内总线通信数据。

8.8.2　车辆应对接收的数据进行真实性和完整性校验，以识别恶意的 V2X 数据、恶意的诊断数据、恶意的专有数据等，并采取防护措施，防止车辆受到恶意数据的攻击。

注1：V2X数据如道路设施发送到车辆的数据、车辆与车辆之间的数据（例如CAM, DENM）。

注2：专有数据指正常发送自OEM或组件/系统/功能供应商的数据。

9 车辆软件升级安全要求

9.1 在线升级安全要求

9.1.1 车辆和在线升级服务器应进行身份认证，至少通过证书等方式，验证彼此身份的真实性。

示例：常见的认证方式包括使用证书进行身份认证等。

9.1.2 车辆应对升级包进行真实性和完整性校验。

9.1.3 车辆软件升级程序应将 OTA 软件升级流程中发生的失败事件进行日志记录。

注1：失败事件包括升级包校验失败等。

注2：日志记录内容包括事件时间、事件类型等。

9.2 离线升级安全要求

9.2.1 若车辆使用车载软件升级系统进行离线升级，车辆应对刷写接入端进行身份认证，验证其身份的真实性。

注：常见的认证方式包括使用证书进行身份认证。

9.2.2 若车辆使用车载软件升级系统进行离线升级，车辆应对升级包真实性和完整性进行校验。

9.2.3 若车辆不使用车载软件升级系统进行离线升级，应采取防护措施保证刷写接入端的安全性。

9.3 车载软件升级系统应具备安全启动的功能，可信根、Bootloader 程序及系统固件不应被篡改，或被篡改后无法正常启动。

9.4 车载软件升级系统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。

10 车辆数据代码安全要求

10.1 防提取安全要求

10.1.1 车辆应采取防止非法提取版权或专有软件的加固防御机制。

注1：版权或专有软件清单由企业评估后提出。

注2：防御机制可采用安全访问控制或其他有效的设计保护机制。

10.1.2 车辆应加密存储个人敏感信息，并防止被非授权访问和获取。

10.1.3 车辆应安全存储加密密钥，防止其被非授权访问和获取。

示例：常见的安全存储方式包括存储在 TEE、SE、HSM 等安全模块，也包括安全的软件存储形式。

10.2 车辆应保证存储在车内的车辆唯一标识数据、用于身份识别的数据不被篡改。

示例：常见的防篡改技术措施包括对访问者进行身份鉴别和权限控制等，也可使用只读等技术措施保证数据不被篡改。

10.3 车辆应防止存储在车内的重要数据被非授权访问和获取，防止其被未授权删除和修改。

10.4 车辆应安全存储系统日志文件，防止其被未授权删除和修改。

示例：系统日志文件包括监管日志、数据操作日志、安全日志等。

10.5 车辆应采取限制措施，防止安装或运行带有恶意行为的软件。

示例：常见的限制措施包括白名单机制、黑名单机制等，包括只允许通过企业许可的应用商店下载应用、通过特定

的移动存储设备安装软件、仅能通过 OTA 的方式安装和更新软件等。

10.6 车辆应安全存储车辆关键配置参数，防止其被未授权删除和修改。

示例：常见的车辆关键配置参数包括制动数据、安全气囊展开阈值、电池参数、自动驾驶参数等影响车辆行车、人员保护功能的配置参数。

注1：常见的防止未授权删除和修改技术措施包括对访问者进行身份鉴别和权限控制，也可使用只读等技术措施保证车辆配置相关参数不被未授权删除和修改。

注2：车辆应具备个人信息清除功能及防恢复机制，便于在转售、租借或报废时清除个人信息。

10.7 车辆不得直接向境外传输数据。

11 审核评估及测试方法

依据本标准开展车辆信息安全一般要求评估前，应通过信息安全管理体系要求审核。

依据本标准开展车辆信息安全测试及核查前，应通过车辆信息安全一般要求评估。

车辆信息安全测试及核查应按照附录A的方法进行，确认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和车辆数据代码安全要求满足本文件第7-10章的要求。

12 车辆型式的变更和扩展

12.1 总则

依据本标准通过型式检验的车型,其结果可扩展到符合12.2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 判定条件

12.2.1 整车生产企业相同；

12.2.2 使用的汽车信息安全管理体系相同；

12.2.3 当送检车型具有多种选装方案时，可只针对全覆盖的车型开展测试，即只要具备上述所有部件或系统的车型通过检验，可不再进行组合检验。

12.2.4 车型整车 E-E 架构相同或仅有不改变整车 E-E 架构信息安全的改动；

注：常见的不改变整车E-E架构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安全配置、不新增业务功能的软件升级（修复漏洞、性能优化）等。

12.2.5 中央网关的硬件型号和软件版本相同；

12.2.6 用于实现软件升级的电子控制系统硬件和软件版本相同；

12.2.7 具备移动通信系统（包含 GPRS、3G、4G、5G）功能的零部件硬件型号和软件版本相同；

12.2.8 所有暴露的外部接口的类型、数量、硬件和安全配置相同；

注：外部接口包括USB、OBD等硬件接口和NFC、蓝牙等无线接口。

12.2.9 具备 WIFI 通信功能的零部件硬件和软件版本相同；

12.2.10 具备蓝牙通信功能的零部件硬件和软件版本相同；

12.2.11 具备导航定位功能的零部件硬件和软件版本相同；

12.2.12 数据采集零部件硬件型号和软件版本相同；

注：车辆数据采集部件包括传感器、摄像头、雷达等。

12.2.13　与车型产生数据交互的云平台软件版本和地址相同。

12.3　其他要求

12.3.1　发生影响整车生产企业、使用的汽车信息安全管理体系的改动时，应重新进行整车试验；

12.3.2　发生影响车型整车 E-E 架构信息安全的改动时，应重新进行整车型式检验；

注：常见的影响整车E-E架构信息安全的改动包括添加新的网关改变网络拓扑、增添新的外部接口、改变网络通信方式（如用5G通信单位替代2G通信单元、增加车载以太网）、ECU功能变更或增加新的功能等。

12.3.3　发生不影响车型整车 E-E 架构信息安全，但涉及 12.2.5-12.2.13 相关系统或部件改动时，应针对受影响的项目开展补充验证测试。

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及核查方法

A.1 概述

本附录规定了车辆外部连接安全要求、车辆通信通道安全要求、车辆软件升级安全要求和车辆数据代码安全要求的测试及核查方法。开展测试及核查前，应确认车辆信息安全一般要求评估满足本标准第6章要求。

A.2 测试条件

A.2.1 测试环境应保证测试车辆能安全运行，影响车辆状态的测试应在多运行工况的台架环境下进行。

A.2.2 测试环境应能保障车辆通信稳定且测试不会对公网环境产生影响，影响公网环境的测试应在具备通信功能的整车暗室或类似环境中进行。

A.2.3 测试应在整车上进行，应按照确认的测试项目要求处理车辆。若车型在量产阶段移除了调试接口，应进行申明，并在测试时保留必要的调试接口以满足测试需求。

A.3 测试项清单确认

测试开始前，应对照车辆信息安全一般要求评估时提交的文档，确认如下信息：

a) 适用于测试车辆的测试项清单；
b) 测试车辆远程控制功能清单，包括远程控制指令应用场景和使用权限清单、远程控制指令审计方式及审计日志记录地址、车辆记录异常指令的地址；
c) 测试车辆第三方应用真实性和完整性校验方式；
d) 测试车辆外部接口清单；
e) 测试车辆通信部件清单；
f) 与测试车辆通信的云服务平台清单；
g) 测试车辆 V2X 功能清单；
h) 测试车辆通信方法，包括采用的通信协议类型；
i) 测试车内通信方案及通信矩阵样例，包括专用数据通信矩阵样例；
j) 测试车辆传输机密数据清单；
k) 测试车辆实现离线软件升级的方式及工具；
l) 测试车辆实现在线软件升级的电子控制系统安全启动信任根的访问方式和地址；
m) 测试车辆的版权或专有软件清单和加固方式；
n) 测试车辆存储的个人敏感信息清单及存储的位置；
o) 测试车辆秘钥的存储方式及说明文档
p) 测试车辆的重要数据清单及存储的地址；
q) 测试车辆关键配置参数清单及存储的地址。

A.4 车辆外部连接安全测试及核查方法

A.4.1 具备远程操控功能的系统安全测试方法

应依据附录A.3 b)测试车辆远程控制功能清单，选择A.4.1.1-A.4.1.7中适用的方法，检验测试车辆是否满足正文7.1的要求。

A.4.1.1 真实性和完整性校验的测试方法

尝试伪造、篡改并发送远程车辆控制指令，检查车辆是否响应该指令，并记录测试结果，应不响应该指令。

A.4.1.2 远程钥匙信息真实性、完整性校验失败的处理功能测试方法

尝试篡改、伪造签名等方法进行模拟攻击，检查车辆在接收到异常远程钥匙指令后是否按企业设定的流程记录、处理该指令，并记录测试结果，应按照设定的流程记录、处理该指令。

A.4.1.3 远程控制指令控制测试方法

a) 选择任意控制外的车控指令，发送至测试车辆，检查车辆是否响应该指令，并记录测试结果，应不响应该指令；
b) 选择任意控制内的车控指令，依照通信规则将其修改成任意控制外的指令，并发送至测试车辆，测试车辆是否响应修改后的指令信息，并记录测试结果，应不响应修改后的指令信息。

A.4.1.4 安全审计功能测试方法

使用具备访问权限的用户或工具，导出远程控制指令安全审计日志文件，核查日志文件中是否有包含远程控制指令的日期、时间、发送主体、操作是否成功等信息，并记录核查结果，应包括远程控制指令的日期、时间、发送主体、操作是否成功的信息。

A.4.1.5 审计记录防护测试方法

c) 使用非授权用户或工具进入系统，尝试对审计记录进行删除操作，测试是否可以删除并记录测试结果，应不可删除；
d) 使用非授权用户或工具进入系统，尝试读取审计记录，测试是否可以读取审计记录信息，并记录测试结果，应不可读取；
e) 使用非授权用户或工具进入系统，尝试修改审计记录，测试是否可以进行修改，并记录测试结果，应不可修改；
f) 使用非授权用户或工具进入系统，尝试使用伪造的同名文件对审计记录进行覆盖操作，测试是否可以覆盖，并记录测试结果，应不可覆盖。

A.4.1.6 审计进程防护测试方法

a) 手动输入指令进入审计进程，尝试进行禁用进程操作，测试是否可以禁用该进程，并记录测试结果，应不可禁用；
b) 尝试使用非授权的系统用户中断车辆远程控制指令的审计进程，测试是否可以中断该进程，并记录测试结果，应不可中断。

A.4.1.7 远程控制功能系统程序和数据完整性校验测试方法

篡改车端执行远程控制功能的系统的程序和数据，并下发远程控制指令，测试篡改后该功能是否依然正常执行，并记录测试结果，应无法正常执行该指令。

A.4.2 第三方应用环境安全测试方法

测试人员应依据附录A.3 c)测试车辆第三方应用真实性和完整性校验方式，并按照如下测试方法，检验测试车辆是否满足正文7.2的要求：

A.4.2.1 第三方应用真实性和完整性校验测试方法

a) 使用二进制工具，依据第三方应用真实性和完整性校验方式，篡改第三方应用程序的代码；
b) 尝试安装执行篡改后的第三方应用程序，测试是否可以正常运行，并记录测试结果，应不可正常运行。

A.4.2.2 第三方应用访问控制测试方法

a) 运行授权的第三方应用程序，核查初次启动时是否会明确提示该应用所需使用的权限，并记录核查结果，应有明确提示且与第三方应用程序在企业备案的结果一致；
b) 构建可使用控制外资源的第三方应用程序，尝试安装并运行该程序，测试是否可以安装或正常运行，并记录测试结果，应不可安装或无法正常运行。

A.4.3 外部接口安全测试方法

测试人员应依据附录A.3 d)测试车辆通信部件清单和附录A.3 e)测试车辆外部接口清单，并按照如下测试方法，检验测试车辆是否满足正文7.3的要求。

A.4.3.1 USB 端口访问控制测试方法

a) 在具备 USB 接口的移动存储介质中注入媒体文件、指定签名的应用软件和其它文件；
b) 将移动存储介质连接到车辆 USB 接口，测试车辆是否可以执行除媒体文件和指定签名的应用软件外的其他文件，并记录测试结果，应无法执行除媒体文件和指定签名的应用软件外的其他文件。

A.4.3.2 调试接口访问控制测试方法

使用非授权的用户或工具访问车辆的调试接口，测试是否可以成功建立连接并访问相应的信息，并记录测试结果，应无法成功建立连接。

A.4.3.3 USB 防病毒测试方法

a) 在具备 USB 接口的移动存储介质中注入恶意软件或病毒文件；
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测试出移动存储介质中的恶意软件或病毒文件，并记录测试结果，应能识别出恶意软件或病毒文件。

A.4.3.4 OBD 身份鉴别测试方法

a) 使用非授权用户或工具在 OBD 端口发送写操作请求，测试车辆是否执行该操作请求，并记录测试结果，应无法执行该操作请求；

b） 使用授权用户发送超出权限的操作请求，测试车辆是否执行该操作请求，并记录测试结果，应无法执行该操作请求。

A.4.3.5 车辆外部连接系统漏洞扫描测试方法

使用漏洞扫描工具对车辆通信部件进行漏洞扫描测试，测试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，并记录测试结果，应不存在权威漏洞平台6个月前公布的高危及以上的安全漏洞，或存在高危漏洞但是企业提交了该漏洞的处置方案。

A.4.3.6 车辆关闭不必要接口测试方法

a） 测试人员通过 Wi-Fi、网线等形式依次将测试车辆与测试台架组网，查看配置文件获得被测车辆的 IP 地址；
b） 使用扫描工具软件查看测试车辆所开放的端口，并将车辆开放的端口列表与提交的车辆业务列表进行对比，测试车辆是否有开放非必要的网络端口，并记录测试结果，应仅开放必要的网络端口。

A.5 车辆通信信道安全测试及核查方法

A.5.1 数据防欺骗测试方法

测试人员应依据附录A.3 f)与测试车辆通信的云服务平台清单、附录A.3 g)测试车辆V2X功能清单和附录A.3 h) 测试车辆通信方法，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.5.1.1 接收数据真实性和完整性校验测试方法

A.5.1.1.1 接收数据身份认证测试方法

A.5.1.1.1.1 与服务平台通信的身份认证测试及核查方法

a） 若车辆与服务平台通信采用专用网络或虚拟专用网络环境进行通信，核查通信网络技术报告，确定通信网络类型，并记录核查结果。
b） 若车辆与服务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，检查是否采用如 TLS V1.2 同等安全级别或以上要求的安全通信层协议，并记录测试结果，应使用 TLS V1.2 同等安全级别或以上要求的安全通信层协议；
c） 若车辆与服务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，对私有通信协议方案进行审核，核查通信协议中的加密密钥衍生、更新及存储策略是否支持以安全方式进行定期更新，并以安全的方式存储加密密钥，并记录核查结果，应支持以安全方式进行定期更新，并以安全的方式存储加密秘钥。

A.5.1.1.1.2 车辆与车辆通信的身份认证测试方法

a） 使用合法证书，建立测试车辆与V2X仿真测试设备的通信连接；
b） 替换V2X仿真测试设备的证书，测试替换后测试车辆是否依然和V2X仿真测试设备保持通信连接，并记录测试结果，应断开通信连接。

A.5.1.1.1.3 车辆与路边单元通信的身份认证测试方法

a） 使用合法证书，建立测试车辆与路边单元的通信连接；
b） 替换路边单元的证书，替换后测试车辆是否依然和路边单元保持通信连接，并记录测试结果，应断开通信连接。

A.5.1.1.2 接收数据完整性校验测试方法

a） 在车辆端设备与外部通信对象完成正常的身份认证之后，采用网络数据抓包工具，解析通信报文数据，判断传输数据是否应用了完整性保护措施。
b） 将对传输数据进行篡改或伪造后的报文发送到车辆端，测试车辆端是否对数据的完整性实施校验并做出适宜的响应，并记录测试结果，应进行校验并拒绝该消息。

A.5.1.2 防 V2X 数据仿冒测试方法

模拟一定数量的通信车辆和路边单元，部分模拟车辆和路边单元使用真实通信证书，部分模拟车辆和路边单元使用仿冒身份证书，同时向测试车辆发起通信请求，测试被测试车辆是否能识别仿冒身份证书的车辆，并记录测试结果，应能识别仿冒身份的车辆和路边单元。

A.5.2 防未授权操作测试方法

A.5.2.1 数据通道完整性测试方法

测试人员应按照如下测试及核查方法，检验测试车辆是否满足正文8.2.1的要求。

A.5.2.1.1 通信数据包完整性和校验机制测试方法

通过抓包等手段获取通信数据，分析通信数据包是否采取了完整性保护和校验机制，并记录测试结果，应具备完整性保护和校验机制。

A.5.2.1.2 通信信道防注入机制核查方法

依据车辆的通信信道清单，依次核查车辆关于各通信信道的防护方案，是否具备防注入测试机制，并记录核查结果，所有通信信道均应具备防注入机制。

A.5.2.2 车内网络隔离测试方法

测试人员依据附录A.3 i)车内通信方案及通信矩阵样例，并按照如下测试方法，检验测试车辆是否满足正文8.2.2的要求。

A.5.2.2.1 网络隔离测试方法

对于应用车内通信网络隔离功能的ECU，根据车辆厂商提供的隔离策略，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，并记录测试结果，不应接收到相应的数据帧。

A.5.2.2.2 以太网域隔离测试方法

对于车内通信网络实现域隔离功能的ECU，根据车辆厂商提供的域隔离策略，测试是否能够跨域转发数据帧，并记录测试结果，不应跨域转发数据帧。

A.5.2.3 防非法操纵、覆盖、清除写入数据代码测试方法

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8.2.3的要求。

A.5.2.3.1 防非法读取数据代码测试方法

使用非授权身份对具备对外通信的ECU未授权的数据/代码进行读取，测试是否可以成功操作，并记录测试结果，应不可读取。

A.5.2.3.2 防非法覆盖数据代码测试方法

使用非授权身份对具备对外通信的ECU未授权的数据/代码进行覆盖，测试是否可以成功操作，并记录测试结果，应不可覆盖。

A.5.2.3.3 防非法清除数据代码测试方法

使用非授权身份对具备对外通信的ECU未授权的数据/代码进行清除，测试是否可以成功操作，并记录测试结果，应不可清除。

A.5.2.3.4 防非法写入数据代码测试方法

使用非授权身份对具备对外通信的ECU未授权的数据/代码进行写入，测试是否可以成功操作，并记录测试结果，应不可写入。

A.5.2.4 对外通信零部件身份识别测试方法

测试人员应依据附录A.3 e)测试车辆通信部件清单,并按照如下测试方法，检验测试车辆是否满足正文8.2.4的要求。

a） 使用与测试车辆对外通信部件信号相同的零部件替换安装在整车相同的位置；
b） 启动车辆，测试车辆是否有异常部件连接告警，并记录测试结果，应有异常告警提示。

A.5.3 通信消息真实性和有效性检验测试方法

A.5.3.1 防接收不可靠数据测试方法

测试人员应按照如下方法，检验测试车辆是否满足正文8.3.1的要求：

c） 使用真实源向车辆发送消息数据，测试车辆是否接收消息数据；
d） 伪造身份，冒充真实源向车辆发送消息数据，测试车辆是否接收消息数据，并记录测试结果，应不接收消息数据。

A.5.3.2 防中间人攻击和防会话劫持测试方法

测试人员应选择以下两种方法中的一种，检验测试车辆是否满足正文8.3.2的要求：

a） 监听通信数据，检查通信双方是否进行证书校验，测试车辆是否可识别接收数据的真实性，并记录测试结果，应进行证书校验；
b） 采用数据流重定向等技术实施中间人攻击/会话劫持，测试车辆是否可识别接收数据的真实性，并记录测试结果，应抵御中间人攻击。

A.5.3.3 车辆接收数据的完整性和有效期验证测试方法

测试人员应按照如下方法，检验测试车辆是否满足正文8.3.3的要求：

a） 录制正常会话指令，修改其中的一段数据，发送修改后的会话指令，测试车辆是否做出响应，并记录测试结果，应不响应；
b） 录制正常会话指令，间隔一段时间后，重新发送录制的会话指令，测试车辆是否做出响应，并记录测试结果，应不响应。

A.5.4 数据防泄露核查方法

测试人员应依据附录A.3 j) 测试车辆传输机密数据清单，并按照如下核查方法，检验核查车辆是否满足正文8.4的要求：

a） 依据车辆传输机密数据的方案，核查是否正确使用声明的加密算法对车辆传输的机密数据进行加密，并记录核查结果，应进行加密；
b） 核查使用的加密算法强度是否满足需求，并记录核查结果，算法强度应满足要求。

A.5.5 防拒绝服务攻击测试方法

A.5.5.1 防拒绝服务攻击测试

测试人员应依据附录A.3 i)车内通信方案及通信矩阵样例，并按照如下测试方法，检验测试车辆是否满足正文8.5.1的要求。

A.5.5.1.1 CAN 总线拒绝服务攻击测试方法

a） 将拒绝服务攻击测试设备接入车辆的各路CAN总线，识别总线波特率，尝试向总线发起拒绝服务攻击数据；
b） 在拒绝服务攻击时，尝试运行车辆的各项功能，测试是否可以正常运行；
c） 在拒绝服务攻击结束后，检查车辆是否监测并记录了该次拒绝服务攻击，并记录测试结果，应记录该次拒绝服务攻击。

A.5.5.1.2 以太网拒绝服务攻击测试方法

a） 将拒绝服务攻击测试设备与车辆的车载以太网进行组网，并尝试向车载以太网发起拒绝服务攻击；
b） 在拒绝服务攻击时，尝试运行车辆的各项功能，检查是否可以正常运行；
c） 在拒绝服务攻击结束后，核查车辆是否监测并记录了该次拒绝服务攻击，并记录测试结果，应记录该次拒绝服务攻击。

A.5.5.2 防黑洞攻击测试方法

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8.5.2的要求：

a） 在实验室使用V2X仿真测试设备模拟构建一批可与测试车辆正常通信的车辆，并保持通信；
b） 任选一辆模拟车辆，将其与拒绝服务攻击设备连接，尝试向测试车辆发起拒绝服务攻击；
c） 在拒绝服务攻击时，检查车辆是否依然和其他模拟车辆保持正常通信；
d） 在拒绝服务攻击结束后，核查车辆是否监测并记录了该次黑洞攻击，并记录测试结果，应记录该次黑洞攻击。

A.5.6　防止非特权用户获得访问特权测试方法

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8.6的要求：

a） 构建一个非特权用户账号，尝试对该用户进行身份提权；
b） 使用尝试提权后的账户对系统进行特权访问，测试车辆是否有异常响应或动作，并记录测试结果，应不可提权访问。

A.5.7　防接收恶意数据测试方法

A.5.7.1　防接收车内恶意数据测试方法

测试人员应依据附录A.3 i)车内通信方案及通信矩阵样例，并按照如下测试方法，检验测试车辆是否满足正文8.7.1的要求：

a） 构建并发送非预期消息数据，测试车内总线通道上出现非预期消息时，相应控制器是否能够鉴别并拒绝响应，并记录测试结果，应拒绝响应；
b） 构建并发送超出正常参数范围的消息数据，测试车内总线通道上出现了超出参数范围的消息数据时，接收控制器是否能够鉴别并拒绝响应，并记录测试结果，应拒绝响应。

A.5.7.2　防接收车外恶意数据测试方法

测试人员应依据车辆对外交互消息类型，从如下方法中选择适用的方法，检验测试车辆是否满足正文8.7.2的要求。

A.5.7.2.1　防接收恶意 V2X 消息测试方法

依据V2X通信规则，构建并向车辆发送恶意的V2X消息数据时，测试车辆能否鉴别并拒绝响应，并记录测试结果，应拒绝响应。

A.5.7.2.2　防接收恶意诊断消息测试方法

依据诊断通信规则，构建并向车辆发送恶意的诊断消息数据时，测试车辆能否鉴别并拒绝响应，并记录测试结果，应拒绝响应。

A.5.7.2.3　防接收恶意专有消息测试方法

依据专有消息通信规则，构建并向车辆发送恶意的专有消息数据时，测试车辆能否鉴别并拒绝响应，并记录测试结果，应拒绝响应。

A.6　车辆软件升级安全测试及核查方法

A.6.1　在线升级安全测试方法

A.6.1.1　软件升级服务器身份认证测试及核查方法

测试人员应按照附录A.5.1.1.1.1　与服务平台通信的身份认证测试及核查方法，检测测试车辆是否满足正文9.1.1的要求。

A.6.1.2　升级包真实性和完整性校验测试方法

测试人员应确认OTA升级功能正常执行，并按照如下测试方法，检验测试车辆是否满足正文9.1.2的要求。

A.6.1.2.1 真实性校验测试方法

a） 构造一个真实性被破坏的升级包（篡改签名或证书等）；
b） 将该升级包下载到车载端，执行软件升级，测试并记录升级结果，应不执行升级。

A.6.1.2.2 完整性校验测试方法

a） 构造一个完整性被破坏的升级包（篡改部分信息等）；
b） 将该升级包下载到车载端，执行软件升级，测试并记录升级结果，应不执行升级。

A.6.1.3 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9.1.3的要求：

a） 分别构造完整性或真实性被破坏的升级包，触发升级，检查升级结果和检查日志中的事件记录，并记录测试结果，应记录本次失败事件。
b） 更换OTA服务器的身份认证信息，触发软件升级，检查升级结果和检查日志中的事件记录，并记录测试结果，应记录本次失败事件。

A.6.2 离线升级安全要求测试方法

测试人员应依据附录A.3 k)实现离线软件升级的方式及工具，选择适用的方法，检验测试车辆是否满足正文9.2的要求。

A.6.2.1 身份认证测试方法

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9.2.1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
b） 查看车辆是否能检出接入了非认证的刷写接入端，并记录测试结果，应能阻止非认证刷写接入端与车辆进行通信。

A.6.2.2 离线升级包真实性和完整性校验测试方法

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9.2.2的要求。

A.6.2.2.1 真实性校验测试方法

a） 构造一个真实性被破坏的升级包（篡改签名或证书等）；
b） 通过刷写接入端下载到车载端节点，执行软件升级，并记录测试结果，应不执行真实性被破坏的升级包。

A.6.2.2.2 完整性校验测试方法

a） 构造一个完整性被破坏的升级包（篡改部分信息等）；

b） 通过刷写接入端下载到车载端节点，执行软件升级，并记录测试结果，应不执行完整性被破坏的升级包。

A.6.2.3 离线升级工具安全测试方法

若车辆未使用车载软件升级系统进行离线升级，尝试绕过企业提供的保护机制，使用非授权的刷写接入端进行离线升级，测试是否可以进行离线升级，并记录测试结果，应不可进行离线升级。

A.6.3 车载软件升级系统安全启动测试方法

测试人员应依据附录A.3 l)实现在线软件升级的电子控制系统安全启动信任根的访问方式和地址，按照如下测试方法，检验测试车辆是否满足正文9.3的要求：

a） 获取安全启动信任根存储区域的访问方法和地址，使用软件调试工具写入数据，重复多次检查是否可将数据写入该存储区域；
b） 获取正常运行的Bootloader程序，使用软件调试工具修改该Bootloader程序的签名信息，将修改后的Bootloader程序写入到指定区域，检查是否正常加载Bootloader，并记录测试结果，应不正常加载Bootloader；
c） 获取升级程序的系统固件，使用软件调试工具对其进行篡改，将修改后的系统固件写入到指定区域，检查升级程序是否正常工作，并记录测试结果，升级程序应不工作。

A.6.4 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9.4的要求：

使用漏洞扫描工具对车载软件升级系统进行漏洞扫描测试，测试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，并记录测试结果，应不存在权威漏洞平台6个月前公布的高危及以上的安全漏洞，或存在高危漏洞但是企业提交了该漏洞的处置方案。

A.7 车辆数据代码安全测试及核查方法

A.7.1 数据代码防提取测试及核查方法

A.7.1.1 版权或专有软件防提取测试方法

测试人员应依据附录A.3 n）测试车辆的版权或专有软件清单和加固方式，选择以下两种测试方法中的一种开展测试并记录测试结果，测试结果应满足正文10.1.1的要求：

a） 若采取访问控制保护版权或专有软件，按照访问控制规则创建一个未添加访问控制权限的用户，尝试从车载信息交互系统、自动驾驶域控制器等部件中提取版权软件或专有软件，测试是否可以非法提取版权或专有软件，并记录测试结果，应不可非法提取版权或专有软件。
b） 若采取其他保护机制保护版权或专有软件，尝试绕过企业提供的保护机制，从车载信息交互系统、自动驾驶域控制器等部件中提取版权软件或专有软件，测试是否可以非法提取版权或专有软件，并记录测试结果，应不可非法提取版权或专有软件。

A.7.1.2 敏感个人信息防泄露测试方法

测试人员应依据附录A.3 n)测试车辆存储的个人敏感信息清单及存储的位置，按照如下测试方法开展测试并记录测试结果，测试结果应满足正文10.1.2的要求：

A.7.1.2.1 敏感个人信息非授权访问测试方法

a） 依据敏感个人信息存储区域和地址范围说明，按照访问控制规则创建一个未添加访问控制权限的用户；
b） 尝试访问存储的敏感个人信息，测试是否可以非授权访问敏感个人信息，并记录测试结果,应不可非授权访问敏感个人信息。

A.7.1.2.2 敏感个人信息加密存储测试方法

依据敏感个人信息存储区域和地址范围说明，尝试使用软件分析工具提取存储的个人敏感信息，测试是否为密文存储，并记录测试结果，应为密文存储。

A.7.1.3 秘钥防泄露核查方法

测试人员应按照附录A.3 o)车辆秘钥的存储方式及说明文档，选择以下两种方法中适用的一种开展核查并记录核查结果，测试车辆应满足正文10.1.3的要求：

a） 若采取HSM等硬件安全模块存储秘钥，应依据硬件安全模块安装位置说明文档，核查车辆是否安装了硬件安全模块来保护秘钥，并记录核查结果,应在文档标识位置安装硬件安全模块。
b） 若采取安全的软件存储形式存储秘钥，应依据秘钥存储区域和地址范围说明文档，核查是否采取了防非授权提取技术或加密存储技术，并记录核查结果，应采取防非授权提取技术或加密存储技术。

A.7.2 数据代码防篡改测试方法

测试人员应依据附录A.3 p)测试车辆的重要数据清单及存储的地址，并按照如下测试方法，检验测试车辆是否满足正文10.2的要求。

A.7.2.1 唯一标识数据防篡改测试方法

尝试使用软件分析工具篡改存储在车内的车辆唯一标识数据和用于身份识别的数据,测试是否可以被篡改，并记录测试结果，应不可被篡改。

A.7.2.2 重要数据防篡改测试方法

依据重要数据存储区域和地址范围说明，尝试使用软件分析工具篡改存储在车内的重要数据，测试是否可以被篡改，并记录测试结果，应不可被篡改。

A.7.3 日志文件防篡改测试方法

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10.3的要求：

a） 按照访问控制规则创建一个未添加访问控制权限的用户，并登陆；
b） 尝试修改和删除系统日志文件，测试是否可以未授权删除和修改系统日志文件，并记录测试结果，应不可未授权删除和修改系统日志文件。

A.7.4 恶意软件防护测试方法

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10.4的要求：

a） 按照软件安装控制规则构建一个非法应用程序；
b） 尝试在车辆上安全该程序，测试车辆是否可以防止安装或运行带有恶意软件行为的软件，并记录测试结果，应不可安装或运行带有恶意软件行为的软件。

A.7.5 关键配置参数防篡改测试方法

测试人员应依据附录A.3 q)测试车辆关键配置参数清单及存储的地址，并按照如下测试方法，检验测试车辆是否满足正文10.5的要求：

依据车辆关键配置参数存储区域和地址范围说明，尝试使用软件分析工具篡改车辆关键配置参数，测试是否可以被篡改，并记录测试结果，应不可被篡改。

A.7.6 关键配置参数防篡改测试方法

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10.6的要求：

采用网络数据抓包工具进行数据抓包，解析车辆对外传输的数据，检查车辆对外传输数据是否向境外传输，并记录测试结果，应不存在直接向境外传输的数据。