ICS 03.100
CCS A 00

DBXXXX

深　　圳　　市　　地　　方　　标　　准

DBXXXX

智能网联汽车整车信息安全技术要求

Technical requirements for intelligent connected vehicle cybersecurity

2022-XX-XX 发布　　202X-XX-XX 实施

深圳市市场监督管理局　　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。

本文件是深圳市实施《深圳经济特区智能网联汽车管理条例》的重要支撑文件，文件中约束了参与深圳市智能网联汽车道路测试和示范应用、准入和登记、使用管理等活动的整车生产企业、技术支撑机构和车辆的信息安全管理体系要求、一般要求、技术要求和审核评估及测试验证方法。

本文件以强制性国家标准《汽车整车信息安全技术研究》草案（征求意见稿）（计划号：20214422-Q-339）为基础制定，主要用于支持深圳市智能网联汽车准入管理工作的实施，原标准由中华人民共和国工业和信息化部提出，全国汽车标准化技术委员会（SAC/ TC114）归口，其起草单位、主要起草人、采标情况等与最终发布的推荐性国家标准一致。

本文件由深圳市市场监督管理局提出并归口。

智能网联汽车整车信息安全技术要求

1 范围

本文件规定了具备智能网联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

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

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

[来源：GB/T xxxxx 智能网联汽车 术语和定义]

3.2

开发阶段 development phase
车型获得批准之前的时期。

3.3

生产阶段 production phase
车型生产持续的时期。

3.4

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期。在这一阶段，该车型的车辆仍可使用，但不再继续生产，当该车型不再有可使用的车辆时，此阶段结束。

3.5

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。

3.6

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。

3.7

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。

3.8

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。

3.9

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

安装在车端并具备升级包接收、校验和分发等功能的软件和硬件。

3.10

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。

3.11

离线升级 offline update

除在线升级以外的软件升级。

3.12

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（Control Area Network）

ECU：电子控制单元（Electronic Control Unit）

HSM：硬件安全模块（Hardware Secure 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 车辆生产企业应建立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中应涵盖必要流程，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及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 应建立用于车辆信息安全测试的流程。

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，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攻击、网络威胁和漏洞的能力。

c) 应建立确保已识别的网络攻击、网络威胁和漏洞得到响应，且在合理的时限内得到处置的流程；

d) 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流程；

e) 应建立确保对网络攻击、网络威胁和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、车辆生产企业子组织之间信息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汽车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 应识别车辆的关键要素，对车辆进行详细的风险评估，合理管理已识别的风险。

注：风险评估应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。

示例：关键要素包括有助于车辆安全、环境保护或防盗的要素，提供连接性的部件或车辆架构中对信息安全至关重要的部分等。

6.4 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。

注1：若处置措施与所识别的风险不相关， 则车辆制造商应说明其不相关性。

注2：若处置措施与所识别的风险不充分， 则车辆制造商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，则应采取相应适当的措施，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 应通过适当和充分的测试来验证所实施的信息安全措施的有效性。

6.7　应针对车辆实施相应措施，以识别和防御针对该车辆的网络攻击、网络威胁和漏洞，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　应采用符合国际通用、国家或行业标准要求的密码模块。若使用的密码模块未采用国际通用、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场景，选择适当长度和有效的密钥。

注：有效的密码算法指安全有效且未被破解的算法，如MD5已被破解，此类算法相对不安全。

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。

7　车辆外部连接安全要求

7.1　远程控制系统安全要求

7.1.1　应对远程控制系统的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。

7.1.2　应对远程控制系统的指令设置访问控制，禁用非授权的远程控制指令。

7.1.3　应具备远程控制系统的安全日志记录功能，安全日志记录的内容至少包括远程控制指令的日期、时间、发送主体、远程控制对象、操作结果等。

7.1.4　应对车端具备远程控制功能的系统的程序和配置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法人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。

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

7.3　外部接口安全要求

7.3.1　应对外部接口进行访问控制保护，禁止非授权访问。

示例：外部接口包括 USB 接口、诊断接口和其他接口等。

7.3.2　应对 USB 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。

7.3.3　应具备抵御 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。

7.3.4　通过诊断接口发送车辆关键参数的写操作请求时，应采用身份鉴别、访问控制等安全策略。

7.4　车辆远程控制系统、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。

7.5　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　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 等短距离无线通信通道。

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期或唯一性。

8.6　车辆应对发送的敏感个人信息实施保密性保护措施。

8.7　车辆与外部直接通信的零部件应具备身份识别机制。

注：与外部存在直接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　车辆与外部直接通信的零部件应具备安全机制防止非授权的系统特权访问。

注：非授权用户可能通过调试接口获得系统的根用户权限。

8.9　车辆内部网络应划分安全区域，并实现安全区域之间的隔离，对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：隔离措施包括物理隔离、逻辑隔离（如采用白名单、防火墙等措施），如车载以太网可采用VLAN技术实现不同功能域之间的逻辑隔离。

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，并对攻击数据包进行相应的处理。

注：对攻击数据包的处理包括拦截、丢弃等。

示例：车辆通信通道包括移动蜂窝通信、V2X 等车外通信通道，也包括 CAN 总线和车载以太网等车内通信通道。

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

注1：V2X数据包括道路设施发送到车辆的数据、车辆与车辆之间的数据。

注2：专有数据指正常发送自车辆生产企业或车辆组件、系统及功能供应商的数据。

8.12　车辆应对关键的通信信息安全事件进行日志记录。

注：关键的通信信息安全事件由车企根据风险评估的结果确定。

9 车辆软件升级安全要求

9.1 通用安全要求

9.1.1 车载软件升级系统应具备安全启动的功能，应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，或被篡改后无法正常启动。

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。

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 车载软件升级系统应对下载的在线升级包进行真实性和完整性校验。

9.2.3 车载软件升级系统应记录在线升级过程中发生的失败事件日志。

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、事件类型等。

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，或者校验离线升级包的真实性和完整性。

10 车辆数据代码安全要求

10.1 车辆应安全地存储对称密钥和私钥，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、加密技术等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）和用于身份识别的数据，防止其被非授权删除和修改。

示例：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：关键数据包括车辆关键配置参数和车辆运行过程中产生的可能影响行车安全的数据。

示例：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。

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，防止其被非授权删除和修改。

10.6　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。

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信息安全一般要求评估和信息安全技术要求测试验证前，应通过汽车信息安全管理体系要求审核。

11.2　车辆信息安全技术要求测试验证应按照本文件附录 A 进行，在测试验证前应开展车辆信息安全一般要求评估，确认车辆采取了基于第 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。

注1：若基于第7章、第8章、第9章、第10章的信息安全技术要求处置措施与企业所识别的风险不相关，无需对不相关的条款开展测试，仅需开展评估确认。

注2：若基于第7章、第8章、第9章、第10章的信息安全技术要求处置措施无法覆盖企业所识别的风险，应在按照附录A开展测试验证的基础上，对企业实际所使用的处置措施开展评估确认。

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代码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 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整车转鼓环境下进行。

A.2.2 测试环境应保证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 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 车辆生产企业应提供技术人员、刷写工具等必要的支持协助完成测试。

A.3 测试输入信息

测试开始前，应根据车辆信息安全一般要求评估的结果，确认与测试车辆相关的测试项，并获取如下测试输入信息：

注：测试输入信息的获取可在车辆生产企业认可的安全场景下进行，如在企业现场审阅相关文档。

a) 测试车辆远程控制功能，包括远程控制指令应用场景和使用权限、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；
b) 测试车辆授权第三方应用真实性和完整性校验方式；
c) 测试车辆非授权第三方应用的访问控制机制；
d) 测试车辆的外部接口；
e) 与测试车辆通信的车辆生产企业云平台；
f) 测试车辆通信方法，包括采用的通信协议类型；
g) 测试车辆的 V2X 功能；
h) 测试车辆向外传输敏感个人信息的通信通道；
i) 测试车辆与外部直接通信的零部件；
j) 测试车辆内部通信方案及通信矩阵样例，包括专用数据通信矩阵样例；
k) 测试车辆车载软件升级系统可信根、引导加载程序、系统固件的访问方式和地址；
l) 测试车辆实现离线软件升级的方式及工具；
m) 测试车辆对称密钥和私钥的存储方式及说明文档；
n) 测试车辆内部存储敏感个人信息存储地址；
o) 测试车辆内存储的车辆识别代号和用于身份识别的数据清单及存储地址；
p) 测试车辆内存储的关键数据清单及存储的地址；
q) 测试车辆个人信息清除功能及防恢复机制。

A.4 车辆外部连接安全测试方法

A.4.1 具备远程操控功能的系统安全测试方法

A.4.1.1 真实性和完整性校验的测试方法

应依据附录A.3 a)测试车辆远程控制功能，并按照如下测试方法，检验测试车辆是否满足正文7.1.1的要求：

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，是否按照企业设定的验证失败处理机制进行处理，并记录测试结果，应不响应该指令。

A.4.1.2 远程控制指令控制测试方法

应依据附录A.3 a)测试车辆远程控制功能，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：

构建非授权的远程控制指令，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。

A.4.1.3 安全日志记录功能测试方法

应依据附录A.3 a)测试车辆远程控制功能，并按照如下测试方法，检验测试车辆是否满足正文7.1.3的要求：

构建并触发远程控制系统信息安全事件，使用授权的用户或工具，导出远程控制系统安全日志文件，验证文件记录的内容是否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，并记录验证结果，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.4.1.4 远程控制功能系统程序和数据完整性校验测试方法

应依据附录A.3 a)测试车辆远程控制功能，并按照如下测试方法，检验测试车辆是否满足正文7.1.4的要求：

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，测试车辆是否告警或不执行该控制指令，并记录测试结果，应告警或不执行该控制指令。

A.4.2 第三方应用安全测试方法

A.4.2.1 授权第三方应用真实性完整性验证测试方法

测试人员应依据附录A.3 b) 测试车辆授权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7.2.1的要求：

r) 使用二进制工具，依据授权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；

s) 尝试安装执行篡改后的授权第三方应用程序，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 非授权第三方应用访问控制测试方法

测试人员应依据附录A.3 c) 测试车辆非授权第三方应用的访问控制机制，并按照如下测试方法，检验测试车辆是否满足正文7.2.2的要求：

t) 尝试安装并执行非授权第三方应用，测试车辆是否进行提示，并记录测试结果，应有明确提示；

u) 尝试使用非授权第三方应用程序访问超出访问控制权限的资源，并记录测试结果，应不可访问控制权限外的资源。

A.4.3 外部接口安全测试方法

A.4.3.1 外部接口访问控制测试方法

测试人员应依据附录A.3 d)测试车辆外部接口，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，并记录测试结果，应无法成功建立连接。

A.4.3.2 USB 接口访问控制测试方法

测试人员应依据附录A.3 d)测试车辆的外部接口，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：

v) 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；

w) 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.4.3.3 USB 防病毒测试方法

测试人员应依据附录A.3 d)测试车辆的外部接口，并按照如下测试方法，检验测试车辆是否满足正文7.3.3的要求：

x） 在具备USB接口的移动存储介质中注入病毒文件；

y） 将移动存储介质连接到车辆 USB 接口，尝试执行病毒文件，测试车辆系统是否可以测试出移动存储介质中的病毒文件或拒绝执行病毒文件，并记录测试结果，应能识别出病毒文件或拒绝执行病毒文件。

A.4.3.4 诊断接口身份鉴别测试方法

测试人员应依据附录A.3 d)测试车辆的外部接口，并按照如下测试方法，检验测试车辆是否满足正文7.3.4的要求：

z） 使用非授权用户或工具在诊断接口发送车辆关键参数写操作请求，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；

aa） 使用授权用户在诊断接口发送超出权限的车辆关键参数写操作请求，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。

A.4.4 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：

bb） 使用漏洞扫描工具对车辆外部连接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；

cc） 如存在权威漏洞平台 6 个月前公布的高危及以上的安全漏洞，对照企业提交的漏洞处置方案清单，确认企业提交的漏洞处置方案清单中是否覆盖该漏洞，并记录测试结果，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。

A.4.5 车辆关闭不必要接口测试方法

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7.5的要求：

dd） 测试人员通过 WLAN、车载以太网等形式将测试车辆与扫描测试设备组网，查看配置文件获得被测车辆的IP地址；

ee） 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 车辆通信安全测试方法

A.5.1 云平台通信身份真实性验证测试方法

测试人员应依据附录A.3 e） 与测试车辆通信的车辆生产企业云平台、附录A.3 f） 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：

ff） 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，验证通信网络技术报告，确定通信网络类型，并记录验证结果。

gg） 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；

hh） 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，对私有通信协议方案进行验证，并记录测试结果，私有通信协议方案应能对通信对象的身份真实性进行验证。

A.5.2 V2X通信身份认证测试方法

测试人员应依据附录A.3 f） 测试车辆通信方法、附录A.3 g） 测试车辆的V2X功能，并按照如下测试方法，检验测试车辆是否满足正文8.2的要求：

a） 使用合法证书，利用V2X仿真测试设备模拟车辆、路侧单元和移动终端，并尝试与测试车辆建立通信连接；

b） 清除V2X仿真测试设备的通信记录，并将证书替换为无效证书或非法证书，测试替换证书后测试车辆是否依然能和V2X仿真测试设备通信，并记录测试结果，应断开通信连接。

A.5.3 通信通道完整性保护测试方法

测试人员应依据附录A.3 f） 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8.3的要求：

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.5.4 防非授权操作测试方法

测试人员应依据附录A.3 f） 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8.4的要求：

a） 使用非授权身份对尝试对车辆通信部件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。

b） 使用非授权身份对尝试对车辆通信部件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。

c） 使用非授权身份对尝试对车辆通信部件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。

d） 使用非授权身份对尝试对车辆通信部件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.5.5 关键指令数据有效性和唯一性验证测试方法

测试人员应按照如下方法，检验测试车辆是否满足正文8.5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.5.6 敏感个人信息保密性保护测试方法

测试人员应依据附录A.3 h)测试车辆向外传输敏感个人信息的通信通道，并按照如下测试方法，检验测试车辆是否满足正文8.6的要求：

a） 依据车辆数据传输的方案，验证是否正确使用声明的加密算法对车辆传输的数据进行加密，并记录验证结果，应进行加密；

b） 验证使用的加密算法强度是否满足需求，并记录验证结果，算法强度应满足要求。

A.5.7 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 i)测试车辆与外部直接通信的零部件,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，测试零部件是否正常工作或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.5.8 车辆与外部直接通信零部件防非特权访问测试方法

测试人员应依据附录A.3 i)测试车辆与外部直接通信的零部件,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） 构建一个非授权用户，尝试对该用户进行身份提权；

b） 使用尝试提权后的用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，应不可访问。

A.5.9 车内安全区域隔离测试方法

测试人员依据附录A.3 j） 测试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8.9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，并记录测试结果，应实现物理隔离。

b） 对于使用逻辑隔离措施的车辆，根据车辆厂商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，并记录测试结果，不应接收到相应的数据帧。

c） 对于采用VLAN技术实现域隔离的车辆，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.5.10 拒绝服务攻击识别测试方法

A.5.10.1 CAN 总线拒绝服务攻击识别测试方法

测试人员应依据附录A.3 j）测试车辆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CAN总线通信拒绝服务攻击识别防护能力是否满足正文8.10的要求。

a） 将拒绝服务攻击测试设备接入车辆的CAN总线，识别该通道总线波特率，测试设备对该通道发起大于80%总线负载率的拒绝服务攻击，如果有多个通道，则依次分别进行测试试验；

b） 在拒绝服务攻击时，测试车辆未受攻击的CAN通道通信性能和预设的功能是否受到影响，并记录测试结果，应能不受影响；

c） 在拒绝服务攻击结束后，测试车辆是否按照预设方案处理攻击数据包，并记录测试结果，应按照预设的方案处理攻击数据包。

A.5.10.2 以太网拒绝服务攻击识别测试方法

测试人员应依据附录A.3 j）测试车辆车内通信方案及通信矩阵样例，并按照如下测试方法，检验测试车辆以太网通信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，测试车辆未受攻击的部件性能和预设的功能是否受到影响，并记录测试结果，应能不受影响。

c） 在拒绝服务攻击结束后，测试车辆是否按照预设方案处理攻击数据包，并记录测试结果，应按照预设的方案处理攻击数据包。

A.5.10.3 V2X 通信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V2X通信拒绝服务攻击识别防护能力是否满足正文8.10的要求：

a） 使用V2X仿真测试设备模拟构建不少于150辆可与测试车辆正常通信的虚拟车辆，并保持通信；

b） 任选一辆虚拟车辆，将其与拒绝服务攻击设备连接，向测试车辆发起拒绝服务攻击；

c） 在拒绝服务攻击结束后，测试车辆的V2X功能是否恢复并可正常运行，并记录测试结果，应从攻击中恢复并正常运行。

A.5.11 恶意数据识别测试方法

测试人员应依据车辆接受消息类型，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8.11的要求。

a） 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。

b） 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。

c） 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.5.12 通信信息安全日志测试方法

测试人员应依据车辆通信信息安全日志记录机制，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：

构建并触发车辆通信信息安全事件，测试车辆是否会按照通信信息安全日志记录机制记录该事件，并记录测试结果，应按照机制要求记录该安全事件。

A.6 车辆软件升级安全测试方法

A.6.1 通用安全要求测试方法

A.6.1.1 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 k）测试车辆车载软件升级系统可信根、引导加载程序、系统固件的访问方式和地址，按照如下测试方法，检验测试车辆是否满足正文9.1.1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，重复测试不少于三次，测试是否可将数据写入该存储区域，并记录测试结果，应无法将数据写入该存储区域；

b）获取正常运行的引导加载程序，使用软件调试工具修改该引导加载程序的签名信息，将修改后的引导加载程序写入到指定区域，检查是否正常加载引导加载程序，并记录测试结果，应不正常加载引导加载程序；

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.6.1.2 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；

b）如存在权威漏洞平台6个月前公布的高危及以上的安全漏洞，对照企业提交的漏洞处置方案清单，确认企业提交的漏洞处置方案清单中是否覆盖该漏洞，并记录测试结果，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。

A.6.2 在线升级安全测试方法

A.6.2.1 软件升级服务器身份认证测试方法

测试人员应按照附录A.5.1 云平台通信身份真实性验证测试方法，检测测试车辆是否满足正文9.2.1的要求。

A.6.2.2 升级包真实性和完整性校验测试方法

测试人员应确认在线升级功能正常执行，并按照如下测试方法，检验测试车辆是否满足正文9.2.2的要求：

a）构造被篡改破坏的在线升级包；

b）将该升级包下载或传输到车载端，执行软件升级，测试并记录升级结果，应不执行升级。

A.6.2.3 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9.2.3的要求：

a）构造完整性或真实性被破坏的在线升级包，

b）触发车辆软件升级，检查升级事件日志，并记录测试结果，应记录本次升级失败事件。

A.6.3 离线升级安全要求测试方法

A.6.3.1 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，测试人员应依据附录A.3 l)实现离线软件升级的方式及工具，并按照如下测试方法，检验测试车辆是否满足正文9.3.1的要求：

a） 构造被篡改破坏的离线升级包；

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，测试并记录升级结果，应不执行升级。

A.6.3.2 不使用车载软件升级系统的离线升级安全测试方法

若车辆不使用车载软件升级系统进行离线升级，测试人员应依据附录A.3 l)实现离线软件升级的方式及工具，并选择以下两种方法中适用的一种开展测试并记录测试结果，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，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；

b） 构造被篡改破坏的离线升级包，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，测试并记录升级结果，应不执行升级。

A.7 车辆数据代码安全测试方法

A.7.1 密钥防非法获取和访问测试方法

测试人员应按照附录A.3 m）测试车辆对称密钥和私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测试并记录测试结果，测试车辆应满足正文10.1的要求：

a） 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,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密钥，应依据密钥存储区域和地址范围说明文档，验证是否采取了防非授权提取技术或加密存储技术，并记录验证结果，应采取防非授权提取技术或加密存储技术。

A.7.2 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）测试车辆内部存储敏感个人信息存储地址，选择以下两种方法中适用的一种开展测试并记录测试结果，测试结果应满足正文10.2的要求：

a） 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，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。

b） 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，尝试使用软件分析工具提取存储的敏感个人信息，测试是否为密文存储，并记录测试结果，应为密文存储。

A.7.3 身份识别数据防篡改测试方法

测试人员应依据附录A.3 o）测试车辆内存储的车辆识别代号和用于身份识别的数据清单及存储地址，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和用于身份识别的数据清单及存储地址说明，尝试使用软件分析工具篡改存储在车辆识别代号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.7.4 重要数据防篡改测试方法

测试人员应依据附录A.3 p）测试车辆内存储的关键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10.4的要求：

依据关键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关键数据，测试是否可以被篡改，并记录测试结果，应不可被篡改。

A.7.5 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10.5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；

b） 尝试修改和删除安全日志文件，测试是否可以未授权删除和修改安全日志文件，并记录测试结果，应不可未授权删除和修改安全日志文件。

A.7.6 个人信息清除功能测试方法

测试人员应依据附录A.3 q）测试车辆个人信息清除功能及防恢复机制，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，并记录测试结果，应可以被删除。

b） 尝试恢复被删除的个人信息，并记录测试结果，应不可被恢复。

A.7.7 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，依次模拟测试车辆各项预装的数据传输功能

使用网络数据抓包工具进行不少于3600秒的数据抓包，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，并记录测试结果，应不包含境外IP地址。