ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/XXX XXXX—XXXX

汽车远程升级（OTA）信息安全测试规范

Test requirements of software update (OTA) cybersecurity

征集意见稿

（本草案完成时间：2023.02.24）

在提交反馈意见时，请将您知道的该标准所涉必要专利信息连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国汽车工程学会　　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。

本文件由中国智能网联汽车产业创新联盟提出。

本文件起草单位：国汽（北京）智能网联汽车研究院有限公司、惠州市德赛西威汽车电子股份有限公司、北汽福田汽车股份有限公司、陕西重型汽车有限公司、博世汽车部件（苏州）有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京百度网讯科技有限公司、北京航迹科技有限公司、北京汽车研究总院有限公司、重庆长安汽车股份有限公司、浙江长三角车联网安全技术有限公司、北京赛目科技股份有限公司、招商局检测车辆技术研究院有限公司、苏州挚途科技有限公司、中汽研软件测评（天津）有限公司、江苏智能网联汽车创新中心有限公司、中国标准化研究院长三角分院、襄阳达安汽车检测中心有限公司、中国汽车工程研究院股份有限公司、北京经纬恒润科技股份有限公司、北京万集科技股份有限公司、中国信息通信研究院、国汽智端(成都)科技有限公司、上海智能网联汽车技术中心有限公司、紫光国芯微电子股份有限公司、国家金融科技测评中心、国家工业信息安全发展研究中心、一汽奔腾轿车有限公司、江铃汽车股份有限公司、南德认证检测（中国）有限公司上海分公司、国家金融科技测评中心、宁波谦川科技有限公司等。

本文件主要起草人：

汽车远程升级（OTA）信息安全测试规范

1 范围

本文件适用于M类、N类汽车远程升级（OTA）的信息安全设计开发、验证和生产工作。

本文件规定了汽车远程升级（OTA）前的服务平台验证、升级中的访问控制和密码技术应用，及升级后的处置过程中的测试方法。

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 XXXXX 汽车软件升级通用技术要求

GB XXXXX 汽车整车信息安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GM/T 0005 随机性检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

软件升级 software update

将某版本的软件更新到新版本或更改配置参数的过程（包括更改软件功能的配置参数）。

注1 ：“软件升级”也称“软件更新”。

注2 ：“软件升级”包含“在线升级”和“离线升级”。

[来源：GB《汽车软件升级通用技术要求》，定义3.2]

3.2

升级包 updates package

用于进行软件升级的软件包。

[来源：GB《汽车软件升级通用技术要求》，定义3.6]

3.3

服务平台 service platform

包括为汽车OTA升级提供各项服务的信息化平台，为汽车OTA升级提供通道接入、任务管理和升级数据等服务。

3.4

补丁 patch

指为解决使用过程中暴露的系统漏洞而发布的解决问题的小程序。

3.5

测试服务平台 test service platform

在测试过程中，为避免因测试活动而阻塞、扰乱、破坏OTA服务平台的正常工作，而临时性搭建的、与生产用服务平台的安全功能与安全保障相一致的测试用服务器。

4 缩略语

以下缩略语适用于本文件。

OTA：空中下载（Over-the-Air）

CDN：内容分发网络（Content Delivery Network）
AES：高级加密标准（Advanced Encryption standard）
DES：数据加密标准（Data Encryption standard）
ECB：电码本（Electronic Codebook）

5 测试条件

5.1 测试环境

5.1.1 测试环境应包含实现汽车 OTA 软件升级功能所需的各种组件，包括 OTA 软件升级平台、通信链路、车载总线网络架构、车端待升级部件等。
5.1.2 测试环境应实现正常的汽车 OTA 软件升级全过程，同时应能模拟各种异常情况。
5.1.3 测试环境应保障在测试过程中与车辆、服务平台的稳定通信。
5.1.4 测试环境应保证车辆能安全运行，至少包含支持车辆多运行工况的台架环境。
5.1.5 测试环境应避免影响服务平台各服务器稳定运行。

5.2 测试服务平台

5.2.1 测试服务平台应能触发车辆的升级并完成整个升级过程。在测试开始之前，测试服务平台应配备软件升级功能介绍材料并在开始升级前进行至少一次完整升级过程的演示。
5.2.2 测试服务平台中业务系统服务器、升级服务器、CDN 服务器应可登录。
5.2.3 测试服务平台应能记录 OTA 平台操作的完整日志，测试服务平台在测试开始之前应进行至少一次平台操作的日志读取。
5.2.4 若测试车载设备支持上传日志功能，测试服务平台应能获取到测试车载设备的日志，测试服务平台在测试开始之前进行至少一次测试车载设备的日志读取。

5.3 测试通信链路

5.3.1 测试通信链路应能保证整个升级过程中通信稳定，在测试开始之前应进行至少一次升级验证。
5.3.2 若测试车载设备支持上传本地日志功能，则测试通信链路应能保证测试车载设备上传本地日志时通信畅通，在测试开始之前进行至少一次测试车载设备的日志上传验证。

5.4 测试车载设备

5.4.1 测试车载设备应能接收升级任务并完成整个升级过程。在测试开始之前，应参照设备配备软件升级功能介绍材料并在开始升级前进行至少一次完整升级过程的演示。
5.4.2 若测试车载设备支持上传日志功能，测试升级部件在测试开始之前进行至少一次日志上传。
5.4.3 若测试车载设备不支持上传日志功能，则应当提供获取本地升级日志的途径，在测试开始之前应对测试车载设备进行至少一次日志产生及读取验证。

6 服务平台安全测试

6.1 托管环境的安全测试

6.1.1 测试目的

检测OTA软件升级服务平台托管环境是否安全。

6.1.2 前置条件

OTA软件升级服务平台应在测试环境中进行并避免影响正常业务。

6.1.3 测试方法

测试按照以下内容进行：

a) 检查 OTA 软件升级服务平台所处的物理环境是否在物理访问控制、防盗窃、防破坏、防雷击、防火、防水、防潮、防静电、防爆、电磁防护等方面满足所需的安全物理环境要求，相关要求可参考 GB/T 22239-2019；
b) 检查 OTA 软件升级服务平台所处的网络环境是否在网络架构、通信传输、可信验证、网络设备防护、安全区域划分、边界隔离、访问控制、安全审计、入侵防范、恶意代码防护等方面满足所需的安全技术要求，相关要求可参考 GB/T 22239-2019；
c) 检查 OTA 软件升级服务平台所处的主机系统（含操作系统）是否在身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、漏洞防范等方面满足所需的安全技术要求，相关要求可参考 GB/T 22239-2019；

6.1.4 通过标准

通过标准如下：
a) OTA 软件升级服务平台所处的物理环境应符合该环境所需三级安全等级，可参考 GB/T 22239-2019 的安全防护要求；
b) OTA 软件升级服务平台所处的网络环境应符合该环境所需三级安全等级，可参考 GB/T 22239-2019 的安全防护要求；
c) OTA 软件升级服务平台所处的主机系统应符合该环境所需三级安全等级，可参考 GB/T 22239-2019 的安全防护要求。

6.2 服务平台公开安全漏洞测试

6.2.1 测试目的

检测OTA软件升级服务平台是否存在已公开安全漏洞。

6.2.2 前置条件

OTA软件升级服务平台中包含相关开源软件。

6.2.3 测试方法

测试按照以下内容进行：
a) 检查 OTA 软件升级服务平台所使用的组件版本、系统版本；
b) 在 CVE、CNNVD、CNVD 等行业权威漏洞库平台上查询所使用的组件版本是否存在公开漏洞，若存在则进行公开漏洞利用测试；
c) 直接使用漏洞扫描、二进制固件分析等工具对 OTA 软件升级服务平台进行漏洞分析，检查是否存在中高危漏洞。

6.2.4 通过标准

通过标准如下：
a) OTA 软件升级服务平台所使用相关的服务组件已打补丁或者为最新版本；
b) 使用漏洞扫描、二进制固件分析等工具对 OTA 软件升级服务平台进行分析后，未发现中高危漏洞。

6.3 服务平台访问控制机制测试

6.3.1 测试目的

检测OTA软件升级服务平台是否有访问控制机制以及访问机制是否存在缺陷。

6.3.2 前置条件

OTA软件升级服务平台白名单列表和系统用户权限配置文件。

6.3.3 测试方法

测试按照以下内容进行：

a) 使用白名单之外的 IP 地址访问 OTA 升级服务平台，检测服务平台是否正常响应；
b) 匿名访问 OTA 升级服务平台相关功能与服务，检测服务平台是否能正常响应；
c) 查看系统用户权限配置文件，检查系统是否采取最小权限原则、责任分离原则、数据抽象原则策略。

6.3.4 通过标准

通过标准如下：
a) OTA 软件升级服务平台采用白名单机制；
b) 匿名访问 OTA 软件升级服务平台相关功能失败；
c) OTA 升级服务平台采用了基于角色的访问控制，采用最小权限原则、责任分离原则、数据抽象原则。

6.4 服务平台用户凭据安全测试

6.4.1 测试目的

检测OTA软件升级服务平台用户凭据是否具备安全性。

6.4.2 前置条件

前置条件包括以下内容：
a) OTA 软件升级服务平台文档；
b) OTA 软件升级服务平台通信数据与测试账号。

6.4.3 测试方法

测试按照以下内容进行：
a) 查看功能文档或登录后台，检测对用户凭据是否有复杂度与定期更改的要求；
b) 查看设计文档，检测用户凭据是否为加密存储，且加密算法、密钥长度及密钥管理方式是否满足国际通用或国家标准要求。

6.4.4 通过标准

通过标准如下：
a) 用户凭据长度应至少 8 位，至少包含数字、大写字母、小写字母以及特殊字符中的三种或三种以上组合，且用户凭据应有定期更改提醒；
b) 用户凭据应采用国际通用或国家标准规定的加密算法进行加密且存储加密后的凭据。

6.5 服务平台认证失败处理安全测试

6.5.1 测试目的

OTA软件升级服务平台认证失败处理安全性测试。

6.5.2 前置条件

前置条件包括以下内容：
a) OTA 软件升级服务平台文档；
b) OTA 软件升级服务平台通信数据与测试账号。

6.5.3 测试方法

测试按照以下内容进行：
a) 查看功能文档中，检测系统是否提供认证失败处理机制；
b) 检测系统在认证用户身份时是否具备认证失败处理机制，如是否采取结束会话、限制非法登陆次数和自动退出等措施；
c) 检测系统在认证失败后，提供的认证失败信息是否模糊。

6.5.4 通过标准

通过标准如下：

a） 系统具备合理的认证失败处理功能，如采取结束会话、限制非法登陆次数和自动退出等措施；

b） 系统在提示客户认证失败时，提示信息不具备指向性。

6.6 服务平台数据处理活动安全测试

6.6.1 测试目的

OTA软件升级服务平台数据处理活动是否安全。

6.6.2 前置条件

OTA软件升级服务平台通信数据与测试账号。

6.6.3 测试方法

测试按照以下内容进行：

a） 对 OTA 软件升级服务平台中的数据进行分析，检查服务平台中是否存在对个人敏感信息进行非授权收集或泄露、非授权数据外传等恶意行为；

a） 使用分析、查找方法，检查服务平台中是否以明文形式存储个人敏感信息；

b） 检测系统中是否存在的测试程序、后门程序、密钥、执行脚本、敏感字段等；

c） 对代码进行查找和分析，检查在代码中是否存在硬编码密钥；

d） 检查该服务平台中是否使用国际通用或国家标准规定的加密算法和参数；

e） 检查是否存在将同一个密钥复用于多种不同用途。

6.6.4 通过标准

通过标准如下：

a） 服务平台不存在对个人敏感信息进行非授权收集或泄露、非授权数据外传等恶意行为；

b） 平台的配置文件、后门程序、密钥文件、执行脚本、日志不存在明文形式的个人敏感信息；

c） 代码中不存在硬编码密钥；

d） 服务平台使用国际通用或国家标准规定的加密算法；

e） 不存在将同一密钥复用于多种不同用途的情况。

6.7 服务平台会话安全机制测试

6.7.1 测试目的

检测OTA软件升级服务平台是否存在会话安全漏洞。

6.7.2 前置条件

前置条件包括以下内容：

a) OTA 软件升级服务平台文档；

b) OTA 软件升级服务平台通信数据与测试账号。

6.7.3 测试方法

测试按照以下内容进行：

a） 检查设计文档是否有会话安全的设计；

b） 分析会话内容，检验 OTA 软件升级服务平台是否具备会话安全保护机制，查看服务器会话是否随机分配 session ID；

c） 核查安全通信协议是否禁用会话重协商和 TLS 压缩功能。

6.7.4 通过标准

通过标准如下：

a） 设计文档中存在会话安全的设计；

b） OTA 软件升级服务平台的不同会话的 session ID 不同或无规律变化；

c） 安全通信协议禁用会话重协商和 TLS 压缩功能。

6.8 服务平台随机数生成机制安全测试

6.8.1 测试目的

检测OTA软件升级服务平台是否存在随机数不安全漏洞。

6.8.2 前置条件

OTA 软件升级服务平台文档。

6.8.3 测试方法

使用设计文档分析的方法并验证，检查使用到的随机数是否由已验证的、安全的随机数生成器产生。

6.8.4 通过标准

使用密码学安全伪随机数生成器(CSPRNG)或经过权威机构认定TRNG生成随机数，使得随机数的生成更为严格，其熵更大，使其可用于安全敏感的功能。

6.9 服务平台日志机制安全测试

6.9.1 测试目的

检测OTA软件升级服务平台日志机制安全。

6.9.2 前置条件

OTA软件升级服务平台通信数据与测试账号。

6.9.3 测试方法

测试按照以下内容进行：

a） 进入服务平台，打开日志信息记录文件，查看内容是否包括但不限于日期和时间、主体身份、事件类型、事件结果等组成部分；
b） OTA 软件升级服务平台日志信息的存储保密性算法是否采用国际通用或国家标准规定加密算法；
c） 以非授权的用户进行 OTA 软件升级服务平台日志存储区域读取写入操作，检查是否存在访问控制机制；
d） 使用逆向分析工具配合系统命令读取日志功能区域内容，检测是否为密文存储；
e） 日志记录保存周期从生产到报废整个生命周期，并对日志记录进行备份保存。

6.9.4 通过标准

通过标准如下：

a） OTA 软件升级服务平台日志完整，包括日期和时间、主体身份、事件类型、事件结果等组成部分；
b） OTA 软件升级服务平台日志功能使用的安全算法满足要求，存储保密性算法采用国际通用或国家标准规定的加密算法；
c） OTA 软件升级服务平台对日志读写存在权限管理；
d） OTA 软件升级服务平台应用日志为密文存储；
e） 日志记录存储空间已满时，应能够实现删除最旧的记录以存储新记录。

7 通信链路安全测试

7.1 升级前访问认证安全测试

7.1.1 测试目的

检测OTA软件升级服务平台是否包含通信认证以及认证是否有缺陷。

7.1.2 前置条件

前置条件包括以下内容：

a) 测试车辆或者测试部件。
b) OTA软件升级服务平台通信数据与测试账号。
c) OTA软件升级系统文档。

7.1.3 测试方法

测试按照以下内容进行：

a) 检查 OTA 软件升级服务平台是否采用 TLS1.2 及以上版本的通信协议、是否采用双向认证机制，以及数据是否进行加密传输（例如使用 SM4、AES 加密算法）；
b) 检测认证通信报文是否具有数字签名或其他的消息真实性防护措施。

7.1.4 通过标准

通过标准如下：

a) OTA 软件升级服务平台采用双向认证机制以及数据进行加密传输，若认证失败后拒绝进行升级，并记录安全日志；
b) 认证通信报文具有数字签名或其他的消息真实性防护措施。

7.2 通信数据传输安全测试

7.2.1 测试目的

检测OTA软件升级服务平台通信报文是否为加密传输。

7.2.2 前置条件

前置条件包括以下内容：

a) 测试车辆或者测试部件。
b) OTA 软件升级服务平台通信数据与测试账号。
c) OTA 软件升级系统文档。

7.2.3 测试方法

测试按照以下内容进行：

a) 查看 OTA 软件升级系统文档或分析 OTA 软件升级服务平台通信报文，检测其通信链路是否采用加密通道传输数据以及加密算法是否符合国际通用或国家标准要求；
b) 分析 OTA 软件升级服务平台通信报文，检测其通信敏感数据是否为明文传输。

7.2.4 通过标准

通过标准如下：

a) OTA 软件升级服务平台通信链路使用加密通道传输数据、加密算法符合国际通用或国家标准要求；
b) OTA 软件升级服务平台通信敏感数据加密后传输。

7.3 密钥生成策略测试

7.3.1 测试目的

检测服务平台和车载设备之间的通信所使用的的密码算法是否符合国际通用或国家标准要求。

7.3.2 前置条件

前置条件包括以下内容：

a） 有足够的权限进入 OTA 软件升级服务平台客户端和服务端；
b） 测试系统能够获得链路加密的会话密钥。

7.3.3 测试方法

测试按照以下内容进行：
a） 检测生成的对称密钥值是否为真随机数序列；
b） 检测生成的对称密钥生命周期是否满足会话密钥动态性要求。

7.3.4 通过标准

通过标准如下：
a） 生成的对称密钥不是伪随机数序列，具备随机性；
b） 生成的对称密钥生命周期满足会话密钥动态性要求。

7.4 密钥强度与算法安全测试

7.4.1 测试目的

检测OTA软件升级服务平台密钥强度与算法是否符合国际通用或国家标准要求。

7.4.2 前置条件

前置条件包括以下内容：
a） 测试车辆或者测试部件；
b） OTA 软件升级服务平台通信数据与测试账号；
c） OTA 软件升级系统文档。

7.4.3 测试方法

测试按照以下内容进行：

a) 分析OTA软件升级服务平台通信报文、查看OTA软件升级系统文档，检测其通信链路加密算法密钥强度是否满足国际通用或国家标准要求；
b) 核查OTA软件升级服务平台中所采用的密钥算法是否为强加密算法（不包含弱加密算法，如MD5、SHA-1、AES ECB模式、DES默认模式等）。

7.4.4 通过标准

通过标准如下：

a) 通信链路加密算法密钥强度应满足国际通用或国家标准要求；
b) OTA软件升级服务平台所使用的的密钥算法应采用SM2、SM3、SM4、长度不低于2048位的RSA、长度不低于128位的AES、哈希（HASH）摘要等强加密算法（不包含弱加密算法，如MD5、SHA-1、AES ECB模式、DES默认模式等）。

7.5 密钥存储安全测试

7.5.1 测试目的

检测OTA软件升级服务平台密钥存储是否有缺陷。

7.5.2 前置条件

有足够的权限进入OTA软件升级服务平台客户端和服务端。

7.5.3 测试方法

测试按照以下内容进行：

a） 检测 OTA 软件升级服务平台中所存储的密钥是否为硬编码或明文存储；
b） 检测 OTA 软件升级服务平台中所存储的密码是否存储在可信区域。

7.5.4 通过标准

通过标准如下：

a) OTA 软件升级服务平台中所存储的密钥不是硬编码或明文存储，无法通过非授权方式读取或操作；
b) OTA 软件升级服务平台中所存储的密码存储在可信区域，宜采用硬件安全存储。

7.6 通信协议安全测试

7.6.1 测试目的

检测OTA软件升级服务平台通信协议是否有缺陷。

7.6.2 前置条件

已获得OTA升级服务平台通信数据包。

7.6.3 测试方法

测试按照以下内容进行：

a) 核查安全通信协议是否为TLS1.2版本及以上或至少同等安全级别，是否允许降级（降到TLS1.1、TLS1.0 或 SSLv3）；
a) 核查安全通信协议是否禁用会话重协商和 TLS 压缩功能。

7.6.4 通过标准

通过标准如下：

a) 通信协议为 TLS1.2 版本及以上或至少同等安全级别，且不允许降级到 TLS1.2 以下版本。
b) 安全通信协议禁用会话重协商和 TLS 压缩功能。

8 车载设备安全测试

8.1 升级设备计算环境（安全基线）安全测试

8.1.1 测试目的

启用设备引导固件、带外管理模块固件存储区保护机制，验证其完整性保护机制是否有效；

8.1.2 前置条件

无。

8.1.3 测试方法

测试按照以下内容进行：

a) 在带外管理模块固件访问设备引导固件时，验证其授权控制功能是否有效；
b) 配置可信策略，启动设备并验证是否通过可信根对设备引导固件和主引导分区/初始化程序加载器完整性进行了检测；
c) 模拟设备引导固件和主引导分区/初始化程序加载器完整性受到破坏，验证设备启动后的安全措施（如停止启动、自动恢复、报警等）是否有效；

8.1.4 通过标准

通过标准如下：

a) 在带外管理模块固件访问设备引导固件时，其授权控制功能有效；
b) 配置可信策略，启动设备并可以通过可信根对设备引导固件和主引导分区/初始化程序加载器完整性进行检测；

c） 模拟设备引导固件和主引导分区/初始化程序加载器完整性受到破坏，设备启动后的安全措施（如停止启动、自动恢复、报警等）有效。

8.2 升级设备密码模块安全测试

8.2.1 测试目的

验证升级设备密码模块采用的密码技术是否生效。

8.2.2 前置条件

无。

8.2.3 测试方法

测试按照以下内容进行：

a） 验证升级设备调用硬件的模块加密、解密功能，如是否能按照需求的加密算法、解密算法对升级包进行加密、解密；

b） 验证升级设备调用硬件的模块签名验证功能，如是否能按照需求的算法对升级包进行验签。

8.2.4 通过标准

通过标准如下：

a） 密码模块应按照需求的加密算法、解密算法进行加密、解密；

b） 密码模块应按照需求的算法进行签名验证。

8.3 升级设备数据处理活动安全测试

8.3.1 测试目的

检测升级设备中的数据处理活动是否具备安全性。

8.3.2 前置条件

无。

8.3.3 测试方法

测试按照以下内容进行：

a） 对升级设备应用软件中数据进行分析，检查升级设备应用软件是否存在对个人敏感信息非授权收集或泄露、非授权数据外传等恶意行为；

b） 使用分析、查找方法，检查升级设备应用软件是否以明文形式存储个人敏感信息；

c） 检查升级设备中是否存在的测试程序、后门程序、密钥、执行脚本、敏感字段等；

d） 对代码进行查找和分析，检查在代码中是否存在硬编码密钥；

e） 检查该升级设备应用软件是否使用已验证的、安全的加密算法和参数；

f） 检查是否存在将同一个密钥复用于多种不同用途。

8.3.4 通过标准

通过标准如下：

a） 升级设备应用软件不存在对个人敏感信息非授权收集或泄露、非授权数据外传等恶意行为；

b） 升级设备应用软件应以密文形式存储个人敏感信息；

c） 升级设备中不存在的测试程序、后门程序、密钥、执行脚本、敏感字段等；

d） 升级设备应用软件代码中不存在硬编码密钥；

e） 升级设备应用软件使用的是安全的加密算法；

f） 升级设备应用软件不存在将同一密钥复用于多种不同用途的情况。

8.4 非授权软件安全校验机制测试

8.4.1 测试目的

检测车载设备安装非授权软件是否存在安全校验机制。

8.4.2 前置条件

车载设备具备通过U盘等外接存储设备安装其中软件的能力。

8.4.3 测试方法

测试按照以下内容进行：

a） 将非授权软件或病毒软件加载入车载设备（比如 U 盘），接入系统尝试识别和安装；

b） 在具有访问权限的前提下使用数据线安装非授权软件。

8.4.4 通过标准

车载设备拒绝安装非授权软件并有弹窗报警提示。

8.5 系统访问控制（权限管理）机制安全测试

8.5.1 测试目的

检测系统访问控制（包括访问级别和权力）和权限管理（所能够执行的操作和访问的数据）机制，并验证相应机制的有效性。

8.5.2 前置条件

无。

8.5.3 测试方法

测试按照以下内容进行：

a） 模拟不同用户角色权限下的不同操作，验证系统是否进行鉴权；

b） 横向越权测试：配置多个拥有相同权限的用户，验证拥有相同权限的用户之间的资源是否可以相互访问。从用户身份处理和资源 ID 处理的维度进行验证；

c） 纵向越权测试：分别配置低级别权限的用户和高级别权限的用户，验证低级别权限用户是否可以访问高级别权限用户的资源。从用户身份处理和资源 ID 处理的维度进行验证。

8.5.4 通过标准

通过标准如下：

a） 系统针对不同权限的用户的不同操作会分别进行访问控制判断和权限判断，并给出相应的反馈。对于无相应权限的操作，系统拒绝授权；

b） 对于相同权限的不同用户之前的资源访问，系统拒绝授权；

c） 低级别权限用户访问高级别权限用户的资源，系统拒绝授权。

9 OTA 过程安全测试

9.1 用户提示及交互过程测试

9.1.1 测试目的

验证是否存在升级告知、用户授权选项和升级结果通知。

9.1.2 前置条件

OTA服务端配置了OTA升级任务。车端已经检测到OTA升级包，并开始下载。

9.1.3 测试方法

测试按照以下内容进行：

d） 下载升级包成功后，检查是否通知用户升级；

a） 执行升级前，查看用户是否可以主动选择升级、取消（或者下次再说）等；

b） 查看升级提示中，是否包含内容：升级目的、更新内容、升级时长和升级注意事项；
c） 升级完成后，检查是否有告知车辆用户升级的结果；
d） 升级成功，检查是否有告知用户更新内容；
e） 升级失败，检查是否有处理建议。

9.1.4 通过标准

通过标准如下：
a） 执行升级前，有告知用户升级；
b） 执行升级前，用户可以授权升级（确定升级）、取消升级或延缓升级；
c） 升级提示中，有升级目的、更新内容、升级时长和升级注意事项；
d） 执行升级后，有告知用户升级结果（成功或失败）；
e） 若升级成功，有告知车辆用户实施的更新，以及更新车载电子用户手册（如果有）；
f） 若升级失败，有告知车辆用户处理建议。

9.2 升级启动前安全检查机制测试

9.2.1 测试目的

验证升级前是否有充足的安全检查、安全控制。

9.2.2 前置条件

车辆制造商定义的升级前安全检查机制，包括但不限于电量检查。

9.2.3 测试方法

测试按照以下内容进行：
a） 升级包下载完成后，通知用户升级；
b） 使用技术手段，调整车辆不满足安全检查机制，然后用户确认升级；
c） 使用技术手段，调整车辆满足安全检查机制，然后用户确认升级。

9.2.4 通过标准

通过标准如下：
a） 升级前存在车况的安全检查；
b） 条件不满足时停止升级；
c） 初始条件不满足，后期条件满足且用户确认后可以进入升级。

9.3 升级启动后自检机制安全测试

9.3.1 测试目的

验证升级启动后，是否具备安全控制。

9.3.2 前置条件

前置条件包括以下内容：
a） 送检车辆处于可行驶的正常状态；
b） 车辆制造商提供车辆启动的方法；
c） 车辆制造商提供在执行升级中影响驾驶安全的升级包；
d） 车辆制造商提供在执行升级中不影响驾驶安全的升级包；
e） 车辆制造商提供影响车辆安全或升级成功执行的车辆功能清单。

9.3.3 测试方法

测试按照以下内容进行：

a) 使用车辆制造商提供的影响驾驶安全的升级包进行测试；执行升级活动，进入安装过程；安装过程中，通过车辆启动、切换档位至行驶档、松开制动、踩油门踏板等方式尝试将车辆置于行驶状态，并实时记录操作状态。
b) 使用车辆制造商提供的不影响驾驶安全的升级包进行测试；执行升级活动，进入安装过程；安装过程中，正常行驶车辆和倒车，并实时记录操作状态。
c) 根据影响车辆安全或升级成功执行的车辆功能清单，逐条使用功能，尝试改变车辆功能状态，并实时记录执行状态。
d) 执行 OTA 升级过程中，从车内开启和关闭车门。

9.3.4 通过标准

通过标准如下：

a) 使用车辆制造商提供的影响驾驶安全的升级包进行测试的结果为：车辆在执行升级过程中不能行驶；车辆在执行升级过程中，影响车辆安全或升级成功执行的车辆功能不可使用。
b) 使用车辆制造商提供的不影响驾驶安全的升级包进行测试的结果为：车辆在倒车和正常行驶过程中，均可正常执行 OTA 升级过程；车辆在执行升级过程中，影响车辆安全或升级成功执行的车辆功能不可使用。
c) 车辆在执行升级过程中，从车内可以开启和关闭车门。

9.4 升级失败回滚机制安全测试

9.4.1 测试目的

验证是否具备安全可靠的升级失败回滚机制。

9.4.2 前置条件

车辆具备升级失败回滚功能。

9.4.3 测试方法

测试按照以下内容进行：

a) 单 ECU 升级，OTA 服务端配置一个会升级失败的升级包，让车辆升级过程中出现升级失败；升级失败后，查看车辆是否恢复到升级前的状态；
b) 多 ECU 升级（假定 A、B、C 三个 ECU）：OTA 服务端配包时，其中一个 ECU（假定为 C）的升级包配置成会升级失败的包，ECU 之间处于功能依赖的关系；C 升级失败后，查看车辆是否恢复到升级前的状态（A、B、C 三个 ECU 的版本，均回滚到升级前的状态）；
c) 单 ECU 升级时，使用测试技术手段破坏升级过程（如断电、重启、熄火等），导致车辆升级失败；升级失败后，查看车辆是否能恢复到升级前的状态；
d) 多 ECU 处于互相依赖状态，进行 OTA 升级时，使用其他手段破坏升级过程（如断电、重启、熄火等），导致车辆升级失败后，查看车辆是否能恢复到升级前的状态。

9.4.4 通过标准

车辆在升级失败后，应确保将系统恢复到以前的可用版本，或确保车辆处于安全状态。

9.5 升级成功功能自检和审计机制测试

9.5.1 测试目的

验证车辆升级成功后的版本一致性。

9.5.2 前置条件

前置条件包括以下内容：

a) 车辆制造商提供车辆当前各零部件的软件版本号（原版本号）。
b) 车辆制造商提供OTA升级包中各零部件的软件版本号（目标版本号）。
c) 车辆通过OTA升级的方式，可以升级成功。

9.5.3 测试方法

测试按照以下内容进行：

a) 车辆进行OTA升级前，查看并记录车辆中各零部件软件版本号。
b) 车辆升级完成，弹出升级成功提示后，查看车辆中各零部件的软件版本号，是否与OTA升级包中各零部件的软件版本号一致。
c) 在OTA服务端上，查看对应车辆的零部件软件版本号是否已经为目标版本号。

9.5.4 通过标准

通过标准如下：

a) 车辆升级成功后，车辆上的零部件软件版本号，必须更新为目标版本号。
b) 车辆升级成后，OTA服务端上，查看对应车辆的零部件软件版本号，必须更新为目标版本号。

9.6 数据及隐私保护机制测试

9.6.1 测试目的

验证OTA升级过程中，用户数据和隐私是否受到保护。

9.6.2 前置条件

9.6.3 测试方法

测试按照以下内容进行：

a) 车辆整个OTA过程中，查看OTA服务端，是否有用户隐私数据上报。
b) 车辆整个OTA过程中，查看展示的界面上，是否有泄露用户隐私数据。
c) 车端涉及到用户数据（USER data分区）升级后是否被破坏，是否被清除。

9.6.4 通过标准

通过标准如下：

a) 车辆OTA过程中，不会泄露和获取用户的隐私数据。
b) OTA升级不会清除和破坏车端用户数据（USER data分区）。

9.7 升级过程日志记录与存储安全测试

9.7.1 测试目的

验证升级失败后日志是否上传到服务器，进行安全存储。

9.7.2 前置条件

9.7.3 测试方法

测试按照以下内容进行：

a) 车辆执行升级过程，升级失败后，查看OTA服务端中指定位置，是否存在整个过程的升级日志。
b) 升级日志应包括但不限于：升级任务接收时间、升级开始时间、升级结束时间、升级结果、失败原因（升级失败情况下）等信息。

9.7.4 通过标准

车辆OTA升级失败后，其升级过程的日志，应上传到OTA服务端。

9.8 断电保护安全测试

9.8.1 测试目的

验证OTA升级过程中的断电保护安全机制。

9.8.2 前置条件

9.8.3 测试方法

测试按照以下内容进行：

a） 下载过程中断电，车辆电源恢复后，查看是否继续下载；

b） 升级过程中断电，车辆电源恢复后，查看是否继续升级。

9.8.4 通过标准

通过标准如下：

a) 下载过程中断电恢复，车辆可以继续下载；

b) 升级过程中断电恢复，车辆可以恢复升级。如果未恢复，升级失败，车辆需要回滚到升级前的状态。

9.9 升级中断恢复机制测试

9.9.1 测试目的

验证OTA升级中断恢复机制，确保升级过程的可靠性。

9.9.2 前置条件

9.9.3 测试方法

测试按照以下内容进行：

a) 车辆进行OTA升级时，在安装刷写阶段，断电重启后，查看升级情况；

b) 车辆进行OTA升级时，在安装刷写阶段，中止升级进程，然后恢复升级进程，查看升级情况；

c) 车辆进行OTA升级时，在安装刷写阶段，断开车辆网络，查看升级情况。恢复车辆网络，并重启车辆后，查看OTA服务平台上改车辆的升级执行信息；

d) 车辆进行OTA升级时，在安装刷写阶段，车辆熄火后，查看升级情况；

e) 车辆进行OTA升级时，在安装刷写阶段，车辆倒车，查看升级情况。

9.9.4 通过标准

通过标准如下：

a） 车辆进行 OTA 升级时，在安装刷写阶段，断电重启后，车辆可以继续 OTA 升级成功或者升级失败但回滚成功；

b） 车辆进行 OTA 升级时，在安装刷写阶段，中止升级进程，然后恢复升级进程，车辆可以继续 OTA 升级成功或者升级失败但回滚成功；

c） 车辆进行 OTA 升级时，在安装刷写阶段，断开车辆网络，车辆可以继续升级并升级成功。恢复车辆网络，并重启车辆后，可以在 OTA 服务端上看到该车辆升级成功；

d） 车辆进行 OTA 升级时，在安装刷写阶段，车辆熄火恢复后，车辆可以继续 OTA 升级成功或者升级失败但回滚成功。

9.10 低版本升级阻断测试

9.10.1 测试目的

验证OTA升级过程中车辆阻止低于当前系统版本的升级包进行升级，避免入侵者利用旧版本的系统漏洞对设备发起攻击。

9.10.2 前置条件

前置条件包括以下内容：

a) 车辆已升级到最新版本。

b) 用于验证低版本升级阻断的升级包版本低于当前车辆上正在运行的版本。

9.10.3 测试方法

将低版本的升级包部署至OTA服务端；车辆端触发升级流程，观察升级是否成功。

9.10.4 通过标准

车辆不会检测到升级任务或者不会进入升级流程。

附录 A
（资料性）
OTA 升级包安全测试

A.1 升级包组件安全漏洞测试

A.1.1 测试目的

检测OTA升级包使用的组件是否存在已公开安全漏洞。

A.1.2 前置条件

无

A.1.3 测试方法

测试按照以下内容进行：

a） 核查软件升级包中所包含的公开组件版本。
b） 在 CVE、CNNVD、CNVD 等行业权威漏洞库平台查询所包含的组件版本是否存在公开漏洞，若存在则进行漏洞利用测试；
c） 直接使用漏洞扫描、代码分析或二进制固件分析等工具对升级包进行漏洞扫描，检查是否存在漏洞。

A.1.4 通过标准

通过标准如下：
a） 升级包中所使用相关的服务组件针对公开的漏洞利用失败；
b） 使用漏洞扫描、代码分析或二进制固件分析等工具对升级包进行漏洞扫描后，未发现漏洞。

A.2 升级包签名测试

A.2.1 测试目的

检测OTA升级包签名过程是否存在缺陷。

A.2.2 前置条件

前置条件包括以下内容：
a） OTA 升级包；
b） 测试车辆或者测试部件。

A.2.3 测试方法

测试按照以下内容进行：

a） 对 OTA 升级包进行非法签名，检测车辆是否可以升级成功；
b） 对 OTA 升级包不签名，直接进行升级，检测车辆是否可以升级成功；
c） 对 OTA 升级包进行篡改,将篡改后的升级包下载到车载终端指定区域,下发升级包升级指令，监测车载终端加载升级包时是否进行完整性校验。

A.2.4 通过标准

通过标准如下：
a） 对 OTA 升级包进行非法签名，车辆升级失败；
b） 对 OTA 升级包不签名，车辆升级失败；
c） 篡改 OTA 升级包后，终端进行完整性校验，升级包完整性校验失败。

A.3 升级包隐藏调试接口与函数测试

A.3.1 测试目的

检测OTA升级包是否隐藏调试接口。

A.3.2 前置条件

OTA 升级包。

A.3.3 测试方法

测试按照以下内容进行：

a） 定位 OTA 升级包关键应用，查看系统中是否存在调试段、符号表；
b） 使用调试分析方法，检查 OTA 升级包是否包含调试功能及调试信息；
c） 检查应用软件日志是否包含调试输出。

A.3.4 通过标准

通过标准如下：

a） OTA 升级包不存在调试段、符号表；
b） OTA 升级包不包含调试功能和调试信息，日志不存在调试输出。

A.4 升级包保护机制测试

A.4.1 测试目的

检测OTA升级包是否存在保护机制。

A.4.2 前置条件

OTA 软件升级包。

A.4.3 测试方法

测试按照以下内容进行：

a） 对 OTA 软件升级包进行解压，检测升级包内容是否进行加密；
b） 对 OTA 软件升级包内固件进行溢出测试，检测固件是否存在堆栈溢出保护机制。

A.4.4 通过标准

通过标准如下：

a） OTA 软件升级包已加密处理；
b） OTA 软件升级包存在栈溢出保护机制。

A.5 升级包签名密钥安全测试

A.5.1 测试目的

检测OTA升级包签名使用密钥是否公开泄漏、是否为系统默认密钥对。

A.5.2 前置条件

OTA软件升级包签名密钥。

A.5.3 测试方法

对密钥进行测试，确定是否泄漏、确定是否是为企业自主生成。

A.5.4 通过标准

升级包签名私钥自主生成，企业独有，不同车型采用独占密钥，不存在泄漏情况。

参 考 文 献

[1] GB/T xxxxx
[2] GB/T xxxxx
[3] GB/T xxxxx