ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 40855—2021

电动汽车远程服务与管理系统信息安全技术要求及试验方法

Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles

2021-10-11 发布　　2022-05-01 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。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：东软集团股份有限公司、中国汽车技术研究中心有限公司、北京理工新源信息科技有限公司、戴姆勒大中华区投资有限公司、北京奇虎科技有限公司、北京汽车研究总院有限公司、国家计算机网络应急技术处理协调中心、大众汽车(中国)投资有限公司、福特汽车(中国)有限公司、中国第一汽车股份有限公司、华为技术有限公司、东风汽车集团股份有限公司技术中心、中国信息通信研究院、上汽通用五菱汽车股份有限公司。

本文件主要起草人：陈静相、解瀚光、刘晓春、方熙宇、陈奕昆、杜志彬、李刚、严敏睿、李峰、王晖、张丽佳、向小丽、李木犀、潘凯、陈化荣、桂丽、冯蘅。

电动汽车远程服务与管理系统信息安全技术要求及试验方法

1 范围

本文件规定了电动汽车远程服务与管理系统的信息安全要求及试验方法。

本文件适用于纯电动汽车、插电式混合动力电动汽车和燃料电池电动汽车的车载终端、车辆企业平台和公共平台之间的数据通信。

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 19596 电动汽车术语

GB/T 32960.1—2016 电动汽车远程服务与管理系统技术规范 第1部分：总则

GB/T 32960.3—2016 电动汽车远程服务与管理系统技术规范 第3部分：通信协议及数据格式

3 术语和定义

GB/T 19596、GB/T 32960.1—2016、GB/T 32960.3—2016 界定的以及下列术语和定义适用于本文件。

3.1

电动汽车远程服务与管理系统 remote service and management system for electric vehicles

对电动汽车信息进行采集、处理和管理，并为联网用户提供信息服务的系统。由公共平台、企业平台和车载终端组成。

[来源：GB/T 32960.1—2016，3.1]

3.2

公共平台 public service and management platform

国家、地方政府或其指定机构建立的、对管辖范围内电动汽车进行数据采集和统一管理的平台。

[来源：GB/T 32960.1—2016，3.2]

3.3

企业平台 enterprise service and management platform

整车企业自建或委托第三方技术单位，对服务范围内的电动汽车和用户进行管理，并提供安全运营服务与管理的平台。

[来源：GB/T 32960.1—2016，3.3]

3.4

车载终端 on-board terminal

安装在汽车上，采集及保存整车及系统部件的关键状态参数并发送到平台的装置或系统。

[来源：GB/T 32960.1—2016，3.4]

3.5

客户端平台　client platform

平台间进行数据交互时，作为车辆数据发送方的远程服务与管理平台。

[来源：GB/T 32960.3—2016，3.1]

3.6

服务端平台　server platform

平台间进行数据交互时，作为车辆数据接收方的远程服务与管理平台。

[来源：GB/T 32960.3—2016，3.2]

3.7

可信验证　trusted verification

基于可信根对设备的目标程序进行完整性验证。

4　缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

IP：网际互连协议（Internet Protocol）

JTAG：联合测试工作组（Joint Test Action Group）

LTE：长期演进（Long Term Evolution）

PCB：印制电路板（Printed Circuit Board）

SPI：串行外设接口（Serial Peripheral Interface）

SSL：安全套接层协议（Secure Sockets Layer）

TCP：传输控制协议（Transmission Control Protocol）

TLS：安全传输层协议（Transport Layer Security）

UART：通用异步收发器（Universal Asynchronous Receiver/Transmitter）

USB：通用串行总线（Universal Serial Bus）

UTC：世界协调时间（Universal Time Coordinated）

5　信息安全要求

5.1　总体结构图

电动汽车远程服务与管理系统信息安全总体结构见图1。

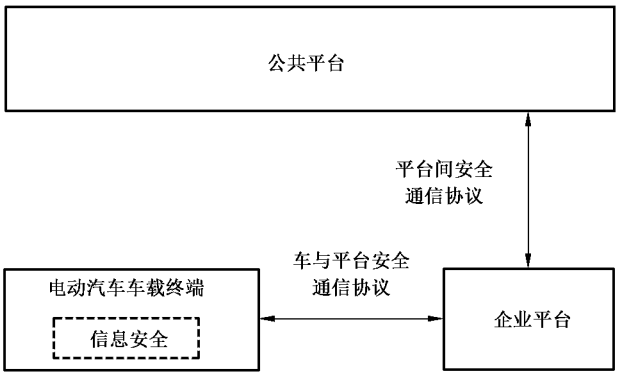

图1　电动汽车远程服务与管理系统信息安全总体结构图

5.2 车载终端安全要求

5.2.1 一般要求

车载终端应保证硬件、固件、软件系统、数据存储、网络端口传输、远程升级、日志和系统的信息安全，满足保密性、完整性、可用性的基本要求。

若车载终端和其他信息交互系统存在共用硬件的情况，则整个设备软硬件也应满足本文件的要求。

5.2.2 功能要求

5.2.2.1 车载终端硬件

车载终端的硬件安全要求如下：

a) 不应存在后门或隐蔽接口；

b) 调试接口应禁用或设置安全访问控制。

5.2.2.2 车载终端固件

车载终端应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。

5.2.2.3 车载终端软件系统

车载终端软件系统要求如下：

a) 应具备判定和授予应用程序对系统资源的访问和操作权限的能力；

b) 宜进行可信验证。

5.2.2.4 车载终端数据存储

车载终端数据存储要求如下：

a) 应保证按照 GB/T 32960.3—2016 要求所存储的远程服务与管理数据的保密性和完整性，宜支持 SM2、SM3、SM4、AES、RSA 等密码算法；

b) 车载终端的安全重要参数在存储以及使用过程中，应只允许被授权的应用以授权方式读取和修改。

5.2.2.5 车载终端网络端口传输安全

车载终端网络端口传输安全要求如下：

a) 应通过对数据包的源地址、目的地址、源端口、目的端口和协议进行检查决定允许或拒绝数据包进出；

b) 应具备根据会话状态信息为进出数据流判定允许或拒绝访问的能力；

c) 应基于应用协议和应用内容对进出网络端口的数据流实现访问控制；

d) 应关闭非业务相关的网络服务端口，并对业务相关的网络服务端口进行访问控制；

e) 应对进入车载终端的带有攻击行为特征的网络数据进行识别，且识别率不低于 95%；

f) 宜采用专用网络或者虚拟专用网络通信，与公网隔离；

g) 宜具备更新扩展安全规则的能力。

5.2.2.6 车载终端远程升级

若车载终端具备远程升级功能，车载终端应具备升级包校验机制，校验升级包的完整性以及来源真

实性。

5.2.2.7 车载终端日志

车载终端日志功能要求如下：

a) 应记录车载终端在远程服务过程中发生的信息安全相关事件，如检测受到网络攻击行为等；
b) 应使每个信息安全事件日志信息记录的内容包括但不限于：日期和时间（精确到秒）、车辆唯一识别码、事件类型；
c) 应保证所存储信息安全事件日志信息的完整性；
d) 宜保证所存储信息安全事件日志信息的保密性；
e) 车载终端信息安全事件日志应只允许被授权的应用以授权方式读取；
f) 应具有信息安全事件日志的上传机制，并使用安全通信协议将信息安全事件日志信息发送到企业平台。

5.2.2.8 车载终端系统安全

车载终端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。

5.3 平台间通信安全要求

5.3.1 一般要求

电动汽车远程服务与管理系统应满足传输数据的保密性、完整性和可用性要求。电动汽车远程服务与管理系统在客户端平台进行平台登入之前，应和服务端平台进行双向身份鉴别。

5.3.2 通信协议栈

电动汽车远程服务与管理系统通信协议栈应包含安全通信协议，在客户端平台和服务端平台之间建立安全通信连接，保障 GB/T 32960.3—2016 定义的业务应用层通信的安全性。安全通信协议应基于 TCP/IP 之上、业务应用层之下，如图 2 所示。

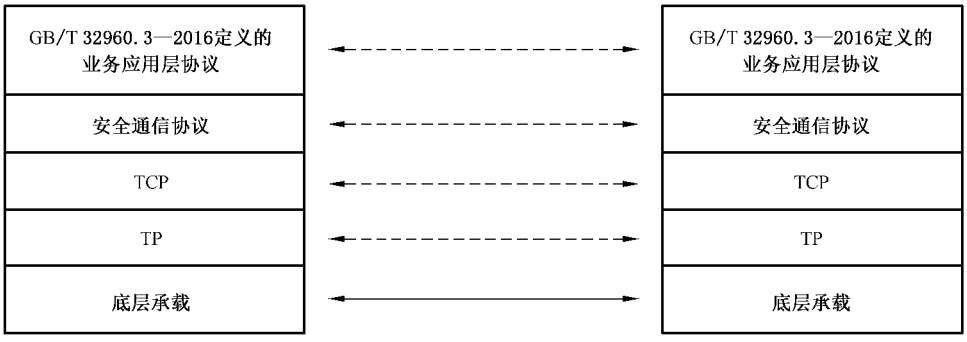

图 2 电动汽车远程服务与管理系统安全通信协议栈

5.3.3 安全通信协议

安全通信协议要求如下：

a) 应使用 TLS 1.2 或以上版本；
b) 应不允许降级，例如降到 TLS 1.1、TLS 1.0 或 SSL 3.0、SSL 2.0；

c) 应禁用 TLS 会话重协商；
d) 应禁用 TLS 压缩；
e) 若使用基于非对称密钥的身份认证机制，宜使用 SM2、密钥长度不低于 2 048 位的 RSA 或同级别以及更高级的密码算法，应具有对应的证书更新及撤销机制，证书的有效期宜不超过 365 d，证书更新过程应确保密钥安全性；
f) 若使用基于对称密钥的身份认证机制，宜使用 SM4、密钥长度不低于 128 位的 AES 或同级别以及更高级的密码算法，应具有对应的密钥更新机制，更新过程中应确保密钥安全性。

5.3.4 数据单元加密

GB/T 32960.3—2016 所要求的远程服务与管理数据，至少包括 GB/T 32960.3—2016 中 7.2 实时信息上报数据，加密要求如下：

a) 数据单元加密方式应采用 SM4、密钥长度不低于 128 位的 AES 或其他同级别以及更高级的密码算法；
b) 加密数据单元的密钥应与安全通信协议所使用的密钥不同。

5.4 车载终端与平台通信安全要求

车载终端到平台的通信应满足双向身份鉴别和传输数据的保密性、完整性和可用性要求。车载终端向平台实时上报 GB/T 32960.3—2016 所要求的实时信息上报数据时，应按照 5.3.4 进行加密处理。车载终端到平台的安全通信协议宜满足 5.3.3 的技术要求。

5.5 平台安全要求

5.5.1 企业平台

企业平台应对车载终端的信息安全进行监视管理，应能在车载终端产生信息安全问题后，为信息安全应急响应提供车载终端相关数据以及追溯手段。

5.5.2 公共平台

公共平台可对车载终端的信息安全状况进行监测。

6 试验方法

6.1 概述

电动汽车远程服务与管理系统信息安全试验方法包括电动汽车远程服务与管理系统信息安全技术文档核查和试验样件信息安全功能验证。

6.2 车载终端信息安全试验样件要求

车载终端试验样件应确定时区为：UTC+08:00 北京，并校准。

6.3 车载终端信息安全试验环境

6.3.1 硬件试验环境

车载终端信息安全硬件测试的拓扑结构，如图 3 所示。

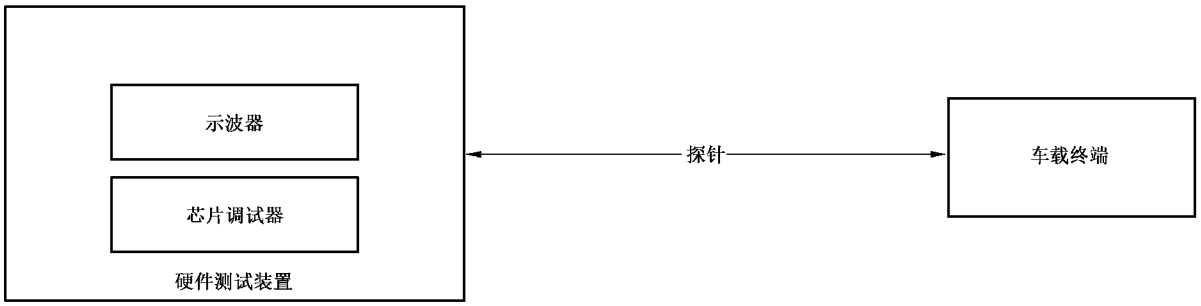

图 3　车载终端信息安全硬件试验示意图

6.3.2　通信试验环境

车载终端信息安全通信试验和验证的拓扑结构，如图 4 所示。

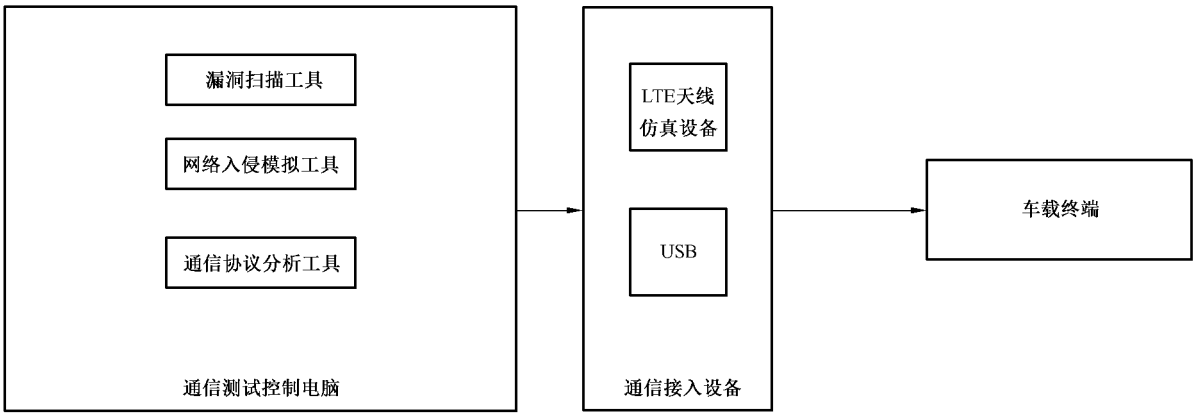

图 4　车载终端信息安全通信试验示意图

6.3.3　软件试验环境

车载终端信息安全软件试验和验证的拓扑结构，如图 5 所示。

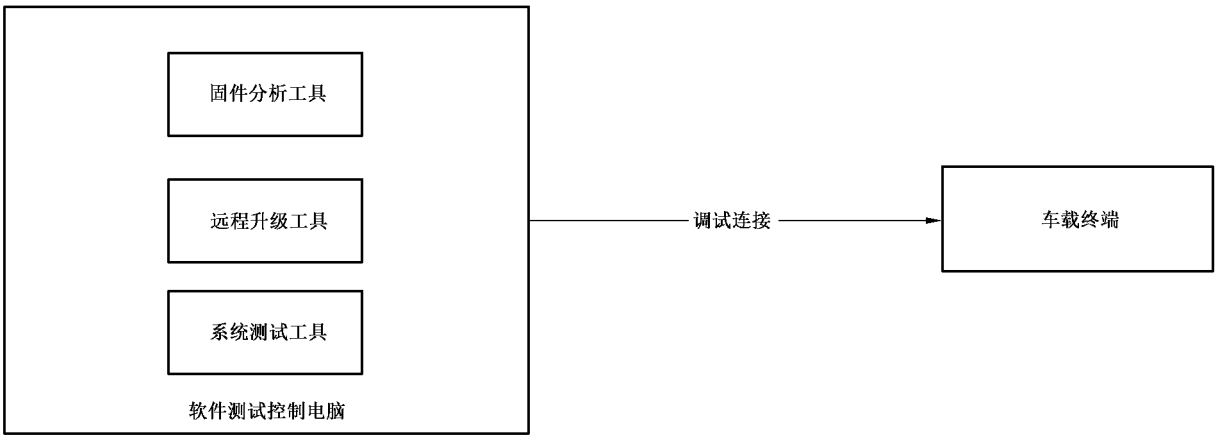

图 5　车载终端信息安全软件试验示意图

6.4 车载终端信息安全试验

6.4.1 车载终端硬件信息安全试验

通过如下方法检测车载终端的硬件信息安全：

a) 拆解被测样件设备外壳，取出 PCB 板，将 PCB 板放大至少 5 倍，观察 PCB 板，检查是否存在可非法对芯片进行访问或者更改芯片功能的隐蔽接口；

b) 根据车载终端接口定义说明，检查是否有存在暴露在 PCB 板上的 JTAG 接口、USB 接口、UART 接口、SPI 接口等调试接口，并使用测试工具尝试获取调试权限。

6.4.2 车载终端固件信息安全试验

6.4.2.1 车载终端硬件安全启动可信根防篡改试验

根据车载终端安全启动可信根存储区域访问方法和地址范围说明，使用软件或硬件调试工具写入数据，重复多次验证是否可将数据写入该存储区域。

6.4.2.2 车载终端硬件安全启动引导加载程序（Bootloader）校验试验

根据车载终端安全启动可信根存储区域访问方法和地址范围说明，使用软件调试工具对该 Bootloader 的签名数据进行破坏，如成功破坏签名数据，则使用安全刷写工具对破坏签名后的 Bootloader 进行刷写，如成功写入到车载终端内的指定区域，检测车载终端芯片是否校验 Bootloader 签名，并在校验不成功时停止加载下一阶段系统镜像。

6.4.2.3 车载终端软件安全启动 Bootloader 防篡改试验

根据车载终端安全启动可信根存储区域访问方法和地址范围说明，尝试使用软件调试工具对 Bootloader 区域的存储数据进行篡改或替换破坏，检测车载终端是否禁止将篡改或替换后的 Bootloader 写入到车载终端内的指定区域。

6.4.2.4 车载终端安全启动系统镜像校验试验

使用软件调试工具对系统镜像的签名数据进行破坏，将破坏签名后的系统镜像写入到车载终端内的指定区域，检测车载终端是否校验系统镜像签名，并在校验不成功时停止工作。

6.4.3 车载终端软件系统信息安全试验

6.4.3.1 车载终端软件系统访问控制试验

按照访问控制规则创建一个未添加访问控制权的软件应用程序，使用该未添加访问控制权的软件应用程序尝试访问受保护的软件应用程序资源，检测受保护的软件应用程序资源是否可被访问。

6.4.3.2 车载终端软件系统可信根存储区域试验

根据车载终端安全启动可信根存储区域访问方法和地址范围说明，使用软件调试工具向软件系统可信根存储区域写入数据，重复多次验证是否可将数据写入该存储区域。

6.4.3.3 车载终端软件系统可信验证试验

使用软件调试工具破坏系统镜像的受保护的关键代码段，并将破坏后的系统镜像写入车载终端，检测加载破坏后的系统镜像的车载终端是否能正常工作。

6.4.4 车载终端数据存储信息安全试验

6.4.4.1 车载终端数据存储保密性试验

使用软件分析工具读取存储远程服务与管理数据区域内容，检测是否为密文存储。

6.4.4.2 车载终端数据存储完整性试验

使用非授权的应用程序读取存储远程服务与管理数据区域内容，检测是否可进行修改，若可修改，则检测修改后，终端是否依然可正常调用该数据。

6.4.4.3 车载终端安全重要参数信息安全试验

使用非授权的应用程序读取系统数据区域的安全重要参数，测试是否可读取或使用。

6.4.5 车载终端网络端口传输信息安全试验

6.4.5.1 车载终端网络端口访问控制策略信息安全核查

6.4.5.1.1 车载终端网络端口控制策略信息安全核查

核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数。

6.4.5.1.2 车载终端网络端口数据流控制策略信息安全核查

核查是否采用会话认证等机制为进出数据流提供明确的允许或拒绝访问的能力。

6.4.5.2 车载终端网络端口访问控制策略试验

在被测样件设置符合标准规定的访问控制策略，检测设备向列表指定的源端口发送不符合策略规定的报文，并在列表指定的目的端口检测接收报文和日志。

6.4.5.3 车载终端网络端口冗余及非授权访问试验

使用网络扫描工具对车载终端进行网络端口扫描：

a) 检测车载终端是否开放非业务所需的冗余网络端口；

b) 检测是否可针对开放的网络端口建立非授权访问控制连接。

6.4.5.4 车载终端安全扫描功能试验

将车载终端接入测试网络，使用攻击案例对车载终端实施攻击，检测车载终端对攻击的识别率。

6.4.5.5 车载终端专用网络认证机制试验

若车载终端到平台采用专用网络或者虚拟专用网络进行通信，尝试在非授权网络条件下，将车载终端连接远程网络服务平台，多次重复检测是否可建立通信。

6.4.5.6 车载终端安全规则更新扩展能力核查

根据车载终端安全规则更新扩展方案说明，核查车载终端是否具备安全规则更新扩展的能力。

6.4.6 车载终端远程升级功能信息安全试验

6.4.6.1 升级包完整性校验试验

使用软件调试工具破坏升级包的任意内容，将被破坏的升级包下载到车载终端指定区域，并下发升级包升级指令，检测车载终端加载升级包时是否进行完整性校验。

6.4.6.2 升级包来源真实性验证试验

将非授权签名的升级包下载到车载终端指定区域，并下发升级包升级指令，检测车载终端加载升级包时是否进行授权校验。

6.4.7 车载终端日志功能信息安全试验

6.4.7.1 车载终端日志功能信息安全核查

根据车载终端安全事件日志记录规则说明，核查车载终端日志信息记录的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。

6.4.7.2 车载终端日志功能保密性信息安全试验

根据车载终端日志存储区域和地址范围说明，使用日志分析工具读取日志功能区域内容，检测是否为密文存储。

6.4.7.3 车载终端日志功能完整性信息安全试验

根据车载终端日志存储区域和地址范围说明，使用非授权的应用程序读取日志功能区域内容，检测是否可修改，若可修改，则检测修改后，是否依然可正常读取该日志。

6.4.7.4 车载终端日志功能访问权限信息安全试验

根据车载终端日志存储区域和地址范围说明，以非授权的用户应用程序访问审计信息存储区域，检测访问是否成功。

6.4.7.5 车载终端日志上传信息安全试验

将车载终端接入测试网络，使用攻击案例对车载终端实施恶意攻击，核查攻击结束后，是否可在企业平台上检索到本次安全攻击事件日志。

6.4.8 车载终端系统信息安全试验

通过如下方法检测车载终端系统信息安全：

a) 使用漏洞扫描工具对车载终端进行漏洞检测，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；

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。

6.5 平台间通信安全试验

6.5.1 认证机制核查

核查平台间通信接入是否具有认证机制。

6.5.2 通信保密性传输试验

使用网络监听工具，监听网络传输数据，检测企业平台与公共平台之间传输的数据是否为密文。

6.5.3 通信完整性传输试验

对车载终端上报的数据进行破坏后，检测企业平台与公共平台之间传输是否失败。

6.5.4 网络端口冗余及非授权访问试验

通过网络扫描工具对企业平台进行网络端口扫描：

a) 检测企业平台是否有开放非业务所需的冗余网络端口；

b) 在非授权网络条件下，使用外部网络工具，检测针对开放的网络端口是否可建立非授权访问连接。

6.5.5 协议版本核查

核查安全通信协议是否为 TLS 1.2 或以上版本，是否允许降级，例如降到 TLS 1.1、TLS 1.0 或 SSL 3.0、SSL 2.0。

6.5.6 协议功能核查

核查安全通信协议是否禁用 TLS 会话重协商和 TLS 压缩功能。

6.5.7 安全算法核查

核查 TLS 协议的安全算法的选择是否满足 5.3.3e)和 f)的要求。

6.6 车载终端与平台通信安全试验

6.6.1 车载终端与平台通信安全核查

6.6.1.1 协议版本核查

核查安全通信协议是否为 TLS 1.2 或以上版本，是否允许降级，例如降到 TLS 1.1、TLS 1.0 或 SSL 3.0、SSL 2.0。

6.6.1.2 协议功能核查

核查安全通信协议是否禁用 TLS 会话重协商和 TLS 压缩功能。

6.6.1.3 安全算法核查

核查 TLS 协议的安全算法的选择是否满足 5.3.3e)和 f)的要求。

6.6.2 车载终端与平台通信传输协议试验

使用网络抓包工具监听车载终端对外网络传输数据，分析数据包是否采用 TLS 1.2 或以上版本协议。

6.6.3 车载终端与平台通信双向身份认证试验

在通信链路捕获车载终端与平台间通信流量包，分析捕获的数据报文，检测通信双方有无交换证书

流量特征或者有无安全认证心跳包流量特征等双向认证方式。

6.6.4 车载终端与平台通信数据加密性试验

使用网络抓包工具监听网络传输数据，检测车载终端与平台之间传输的数据是否为密文。

6.6.5 车载终端与平台通信数据完整性试验

对传输的数据进行破坏，检测数据破坏后，车载终端与平台之间传输是否失败。