ICS 点击此处添加 ICS 号

点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

电动汽车远程服务与管理系统信息安全技术要求

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

（征求意见稿）

本稿完成日期：202004

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

本标准按照GB/T 1.1 -2009给出的规则起草。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国汽车标准化技术委员会（SAC/TC114）归口。

本标准的起草单位：

本标准的主要起草人：

电动汽车远程服务与管理系统信息安全技术要求

1 范围

本标准规定了电动汽车远程服务与管理系统的信息安全要求。

本标准适用于纯电动汽车、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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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/T19596 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 32960.2-2016 电动汽车远程服务与管理系统技术规范 第2部分：车载终端

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/T32960.3-2016界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 32960.1-2016和GB/T32960.3-2016中的某些术语和定义。

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。

[GB/T 32960.1-2016,定义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。

[GB/T 32960.1-2016,定义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。

[GB/T 32960.1-2016,定义3.3]

3.4

车载终端 on-board unit

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。

[GB/T 32960.1-2016,定义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。

[GB/T 32960.3-2016,定义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。

[GB/T 32960.3-2016,定义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。

3.8

安全重要参数 safety important parameter

与安全相关的信息，包含秘密和私有密码秘钥、口令之类的鉴别数据、证书或其他密码相关参数的信息。

3.9

主体subject

车载终端内，实施操作的实体，即一个基本执行单元，也可称为进程。

3.10

客体object

车载终端内，被主体实施操作的实体，如资源、文件系统、目录、文件、消息队列、套接字、共享内存、信号量、端口、设备等。

4 信息安全要求

4.1 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。

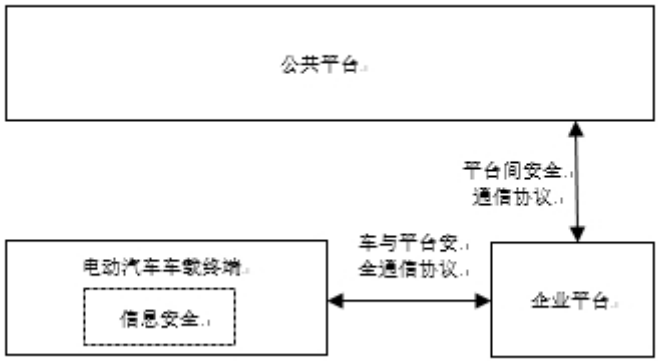

图 1　电动汽车远程服务与管理系统信息安全总体结构

4.2 车载终端安全要求

4.2.1 一般要求

车载终端应保证硬件、固件、软件系统、数据存储、网络接口传输、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。

若车载终端和其它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标准的要求。

4.2.2 功能要求

4.2.2.1 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。

4.2.2.2 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。

4.2.2.3 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。

4.2.2.4 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；

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。

4.2.2.5 车载终端网络接口传输安全

车载终端网络接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接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） 应对进入车内的数据进行入侵检测，对恶意网络数据与攻击的识别率不低于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。

4.2.2.6 车载终端远程升级功能

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，确保升级包的完整性以及来源真实性。

4.2.2.7 车载终端日志功能

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) 应保证所存储日志信息的保密性和完整性；

d) 车载终端日志应只允许被授权的应用以授权方式读取；

e) 应具有日志的上传机制，并使用安全通信协议将日志信息发送到企业平台。

4.2.2.8 车载终端系统安全

车载终端不应存在由权威漏洞平台公开发布6个月及以上且未经处置的高危安全漏洞。

4.3 平台间通信安全要求

4.3.1 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。

4.3.2 通信协议栈要求

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。

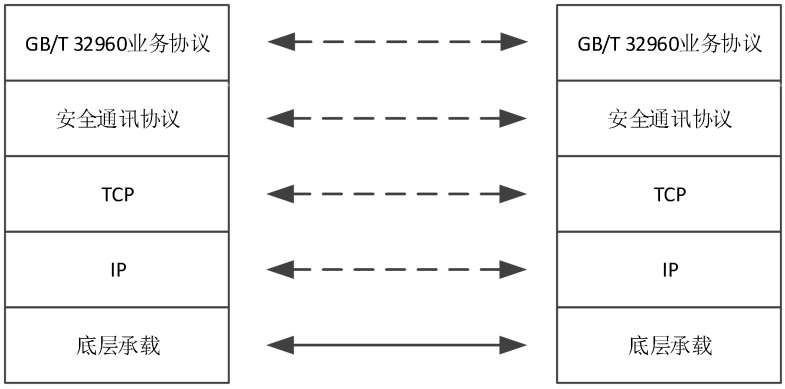

图 2　电动汽车远程服务与管理系统安全通信协议栈

4.3.3 安全通信协议要求

安全通信协议要求如下：

a) 应使用TLS1.2或以上版本；

b) 应不允许降级（降到TLS1.1、TLS1.0或SSLv3）；

c) 应禁用会话重协商；

d) 应禁用TLS压缩；

e) 若使用基于非对称密钥的身份认证的TLS协议，应具有对应的证书更新及撤销机制，宜使用SM2、RSA(长度不低于2048位)或同级别以及更高级的加密算法，证书的有效期宜不超过365天；

f) 若使用基于对称密钥的身份认证的TLS协议，应具有对应的密钥更新机制，宜使用SM4、AES(长度不低于128位)或同级别以及更高级的加密算法。

4.3.4 数据单元加密要求

GB/T 32960.3-2016所要求的远程服务与管理数据加密要求如下：

a) 数据单元加密方式应采用SM4、AES（长度不低于128位）或其它同级别以及更高级的加密算法来进行数据加密；

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。

4.4 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所要求的远程服务与管理数据时，应按照4.3.4进行加密处理。车载终端到平台的安全通信协议宜满足本标准4.3.3的技术要求。

4.5 平台安全要求

4.5.1 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。

4.5.2 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。

5 测试方法

电动汽车远程服务与管理系统信息安全要求相关测试方法见附录A。

附 录 A
（规范性附录）
电动汽车远程服务与管理系统信息安全试验方法

A.1 概述

本附录规范了电动汽车远程服务与管理系统信息安全测试方法，测试内容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测试样件信息安全功能验证。

A.2 车载终端信息安全测试样件要求

A.2.1 时区校准

车载终端测试样件应确定时区为：UTC+08:00 北京，并校准。

A.2.2 配套技术文档

车载终端测试样件应配套如下辅助技术文档：

a) 车载终端接口定义文档；
b) 车载终端安全启动可信根存储区域访问方法和地址范围文档；
c) 车载终端安全规则更新扩展方案文档；
d) 车载终端安全事件日志记录规则文档；
e) 车载终端日志存储区域和地址范围文档；
f) 车载终端系统高危漏洞处置方案文档。

A.2.3 配套测试材料

车载终端测试样件应配套如下辅助测试材料：

a) 车载终端系统镜像；
b) 车载终端Bootloader程序；
c) 车载终端远程升级安装包。

A.3 车载终端信息安全测试环境

A.3.1 硬件测试环境

车载终端信息安全硬件测试的拓扑结构，如图A.1所示：

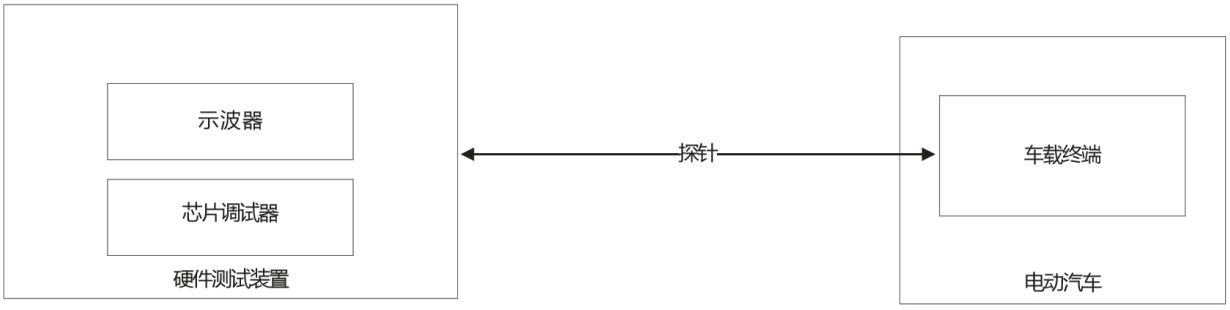

图 A.1 车载终端信息安全硬件测试示意图

A.3.2 通信测试环境

车载终端信息安全通信测试和验证的拓扑结构，如图 A.2 所示：

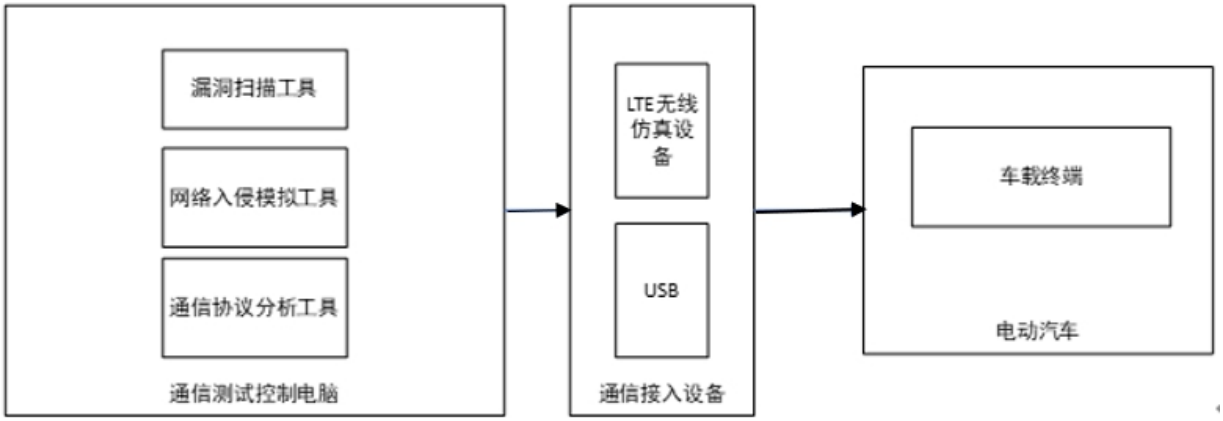

图 A.2 车载终端信息安全通信测试示意图

A.3.3 软件测试环境

车载终端信息安全软件测试和验证的拓扑结构，如图 A.3 所示：

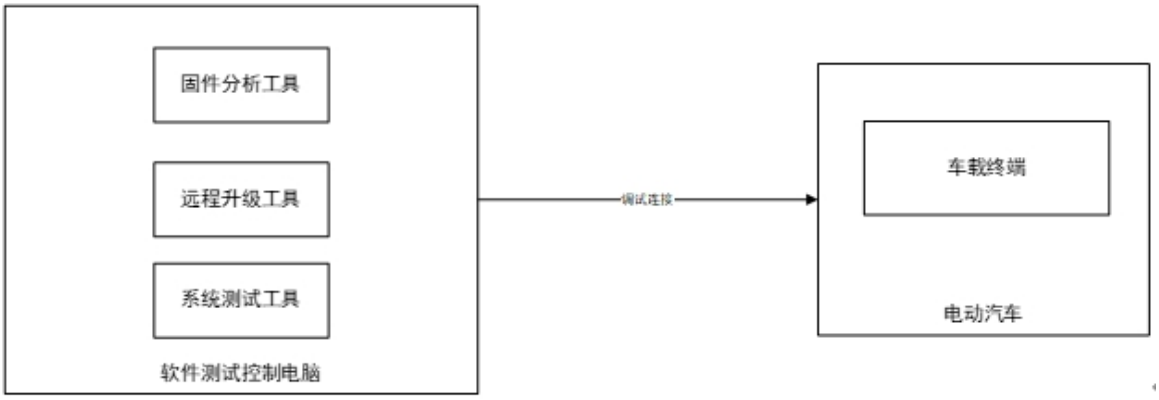

图 A.3 车载终端信息安全软件测试示意图

A.4 车载终端信息安全测试

A.4.1 车载终端硬件信息安全测试

应通过如下方法检测车载终端的硬件信息安全并满足4.2.2.1要求：

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，检查是否存在可以非法对芯片进行访问或者更改芯片功能的隐蔽接口；

b) 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。

A.4.2 车载终端固件信息安全测试

A.4.2.1 概述

基于硬件实现安全启动时应按照A.4.2.2、A.4.2.3和A.4.2.4进行车载终端固件信息安全测试；基于软件实现安全启动时应按照A.4.2.4和A.4.2.5进行车载终端固件信息安全测试，并满足4.2.2.2要求。

A.4.2.2 车载终端硬件安全启动可信根防篡改测试

根据安全启动可信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，重复多次验证是否可将数据写入该存储区域。

A.4.2.3 车载终端硬件安全启动Bootloader程序校验测试

使用软件调试工具对该Bootloader程序的签名数据进行破坏，将破坏签名后的Bootloader程序写入到车载终端内的指定区域，监测车载终端芯片是否校验Bootloader程序签名，并在校验不成功时停止加载下一阶段系统镜像。

A.4.2.4 车载终端软件安全启动Bootloader防篡改测试

根据安全启动可信根存储区域的访问方法和地址，尝试使用软件调试工具对该Bootloader区域程序地址的存储数据签名数据进行篡改或替换破坏，监测车载终端是否禁止将篡改或替换后的Bootloader程序写入到车载终端内的指定区域。

A.4.2.5 车载终端安全启动系统镜像校验测试

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，监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。

A.4.3 车载终端软件系统信息安全测试

A.4.3.1 概述

应按照A.4.3.2、A.4.3.3和A.4.3.4检测车载终端的软件系统信息安全，并满足4.2.2.3要求。

A.4.3.2 车载终端软件系统访问控制测试

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调用受保护的软件应用程序资源，监测受保护的软件应用程序资源是否被调用。

A.4.3.3 车载终端软件系统可信根存储区域测试

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。

A.4.3.4 车载终端软件系统可信验证测试

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，监测加载破坏后的系统镜像的车载终端是否能正常工作。

A.4.4 车载终端数据存储信息安全测试

A.4.4.1 概述

应按照A.4.4.2、A.4.4.3和A.4.4.4检测车载终端的数据存储信息安全，并满足4.2.2.4要求。

A.4.4.2 车载终端关键数据存储保密性测试

使用逆向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。

A.4.4.3 车载终端关键数据存储完整性测试

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，检测是否可以进行读取或修改。

A.4.4.4 车载终端关键安全参数信息安全测试

使用非授权的应用程序读取系统数据区域的关键安全参数内容，测试是否可以读取或使用。

A.4.5 车载终端网络接口传输信息安全测试

A.4.5.1 概述

应按照A.4.5.2、A.4.5.3、A.4.5.4、A.4.5.5、A.4.5.6、A.4.5.7、A.4.5.8、A.4.5.9、A.4.5.10和A.4.5.11检测车载终端网络接口传输信息安全，并满足4.2.2.5要求。

A.4.5.2 车载终端网络接口传输通信协议信息安全核查

A.4.5.2.1 协议版本核查

核查安全通信协议是否为TLS1.2或以上版本，是否允许降级（降到TLS1.1、TLS1.0或SSLv3）。

A.4.5.2.2 协议功能核查

核查安全通信协议是否禁用会话重协商和TLS压缩功能。

A.4.5.2.3 安全算法核查

核查TLS协议的安全算法的选择是否满足如下要求：

a) 若使用基于非对称密钥的身份认证的TLS协议，是否使用SM2加密算法、RSA(长度不低于2048位)或同级别以及更高级的加密算法，证书的有效期是否超过365天；

b) 若使用基于对称密钥的身份认证的TLS协议，是否使用SM4加密算法、AES(长度不低于128位)或同级别以及更高级的加密算法。

A.4.5.3 车载终端网络接口访问控制机制测试

使用网络扫描工具对车载终端进行网络端口扫描,并使用外部网络工具检测是否可以针对开放的网络端口建立非授权访问控制连接。

A.4.5.4 车载终端冗余网络接口测试

使用网络扫描工具对车载终端进行网络端口扫描,检测车载终端是否开放非业务所需的冗余网络端口。

A.4.5.5 车载终端网络接口传输协议测试

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TLS1.2或以上版本协议。

A.4.5.6 车载终端网络接口传输双向身份认证测试

进入车载终端控制台，在通信链路捕获车载终端与平台通信流量包，分析捕获的数据报文，监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。。

A.4.5.7 车载终端网络传输数据加密性测试

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。

A.4.5.8 车载终端网络传输数据完整性测试

对传输的数据进行破坏，监测数据破坏后，车载终端与平台之间传输是否失败。

A.4.5.9 车载终端安全扫描功能测试

将车载终端接入测试网络，使用攻击案例对车载终端注入恶意数据、实施攻击，监测车载终端对恶意网络数据与攻击的识别率。

A.4.5.10 车载终端专用网络认证机制测试

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以建立通信。

A.4.5.11 车载终端安全规则更新扩展能力核查

核查车载终端是否具备安全规则更新扩展的能力。

A.4.6 车载终端远程升级功能信息安全测试

A.4.6.1 概述

应按照A.4.6.2和A.4.6.3检测车载终端远程升级功能信息安全，并满足4.2.2.6要求。

A.4.6.2 升级包完整性校验测试

使用软件调试工具破坏升级包的任意一段代码，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，监测车载终端加载升级包时是否进行完整性校验。

A.4.6.3 升级包真实性验证测试

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，监测车载终端加载升级包时是否进行授权校验。

A.4.7 车载终端日志功能信息安全测试

A.4.7.1 概述

应按照A.4.7.2、A.4.7.3、A.4.7.4、A.4.7.5和A.4.7.6检测车载终端日志功能信息安全，并满足4.2.2.7要求。

A.4.7.2 车载终端日志功能信息安全核查

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。

A.4.7.3 车载终端日志功能安全算法核查

核查车载终端日志功能使用的安全算法是否满足如下要求：

a) 车载终端日志信息的存储保密性算法是否采用SM4、AES（密钥长度为128及以上）或同等强度以及更高强度的加密算法。

b) 车载终端日志信息的存储完整性算法是否采用SM2、RSA（密钥长度为2048或以上）或同等强度以及更高强度的加密算法。

A.4.7.4 车载终端日志功能访问权限信息安全测试

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。

A.4.7.5 车载终端日志功能保密性信息安全测试

使用逆向分析工具读取日志功能区域内容，检测是否为密文存储。

A.4.7.6 车载终端日志功能完整性信息安全测试

使用非授权的应用程序读取日志功能区域内容，检测是否可以读取或修改。

A.4.8 车载终端系统信息安全测试

应通过如下方法检测车载终端系统信息安全，并满足4.2.2.8要求：

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发布6个月及以上的高危安全漏洞；

b) 若存在高危漏洞，则检查厂商是否提供了该高危漏洞的处置方案。

A.5 平台间通信安全测试

A.5.1 概述

应按照A.5.2、A.5.3、A.5.4、A.5.5、A.5.6和A.5.7检测平台间通信信息安全，并满足4.3.1要求；按照A.5.8、A.5.9、A.5.10和A.5.11检测平台间安全通讯协议信息安全，并满足4.3.3要求。

A.5.2 认证机制核查

核查平台间通信接入是否具有认证机制。

A.5.3 通信保密性传输测试

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

A.5.4 通信完整性传输测试

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。

A.5.5 非授权访问测试

通过网络扫描工具对企业平台进行网络端口扫描；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以建立非授权访问连接。

A.5.6 冗余网络接口测试

通过网络扫描工具对企业平台进行网络端口扫描，检测企业平台是否有开放非业务所需的冗余网络端口。

A.5.7 中间人连接测试

使用有线网络将企业平台接入中间服务器（中间体），再通过中间服务器接入公共平台，检测企业平台是否可通过中间服务器（中间体）间接接入到公共平台。

A.5.8 协议版本核查

核查安全通信协议是否为TLS1.2或以上版本，是否允许降级（降到TLS1.1、TLS1.0或SSLv3）。

A.5.9 协议功能核查

核查安全通信协议是否禁用会话重协商和TLS压缩功能。

A.5.10 安全算法核查

核查TLS协议的安全算法的选择是否满足如下要求：

a) 若使用基于非对称密钥的身份认证的TLS协议，是否使用SM2加密算法、RSA(长度不低于2048位)或同级别以及更高级的加密算法 ，证书的有效期是否超过365天；
b) 若使用基于对称密钥的身份认证的TLS协议，是否使用SM4加密算法、AES(长度不低于128位)或同级别以及更高级的加密算法。

A.5.11 安全通信协议一致性测试

监听网络传输数据，分析网络传输数据格式是否与本标准4.3.3的要求一致。

A.6 车载终端与平台通信安全测试

A.6.1 概述

应按照A.6.2、A.6.3、A.6.4、A.6.5和A.6.6检测车载终端与平台通信安全，并满足4.4要求。

A.6.2 车载终端与平台通信安全核查

A.6.2.1 协议版本核查

核查安全通信协议是否为TLS1.2或以上版本，是否允许降级（降到TLS1.1、TLS1.0或SSLv3）。

A.6.2.2 协议功能核查

核查安全通信协议是否禁用会话重协商和TLS压缩功能。

A.6.2.3 安全算法核查

核查TLS协议的安全算法的选择是否满足如下要求：

a) 若使用基于非对称密钥的身份认证的TLS协议，是否使用SM2加密算法、RSA(长度不低于2048位)或同级别以及更高级的加密算法 ，证书的有效期是否超过365天；
b) 若使用基于对称密钥的身份认证的TLS协议，是否使用SM4加密算法、AES(长度不低于128位)或同级别以及更高级的加密算法。

A.6.3 车载终端与平台通信传输协议测试

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TLS1.2或以上版本协议。

A.6.4 车载终端与平台通信双向身份认证测试

在通信链路捕获平台间通信流量包，分析捕获的数据报文，监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。

A.6.5 车载终端与平台通信数据加密性测试

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。

A.6.6 车载终端与平台通信数据完整性测试

对传输的数据进行破坏，监测数据破坏后，车载终端与平台之间传输是否失败。