ICS 33.050

M 30

电信终端产业协会标准

T/TAF XXX-XXXX

车载 TBOX 信息安全技术要求和测试方法

Information Security Technical Requirement and Test Method on Telematics BOX

XXXX- XX-XX 发布　　2020- XX-XX 实施

电信终端产业协会　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院，北京豆荚科技有限公司，高通无线通信技术(中国)有限公司，北京三星通信技术研究有限公司，北京奇虎科技有限公司。

本标准主要起草人：傅山，国炜，刘富洋，王江胜，杜志敏，窦丽娟，吴春雨，宋戈，詹鹏翼。

引　　言

TBOX作为车辆与云端平台实现互通的关键设备，不仅能把采集到的车辆数据（如新能源汽车的驱动电机数据、整车数据、电池数据、状态数据等等）发送给云平台，也能把云平台发送过来的控制指令转发给车辆。

TBOX作为汽车联网的关键部分，安全自然就成了最受关注的部分，同时TBOX对于车联网的普及，势必占据关键性的位置，因此TBOX能否真正发挥其价值，制定其信息安全标准尤显重要。

车载 TBOX 信息安全技术要求

1 范围

本标准规定了车载TBOX的信息安全技术要求，包括硬件安全、操作系统安全、软件安全、数据安全和通信安全。

本标准适用于TBOX的研制、生产、测试、评估与认证。

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，仅所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/T 25069-2010 信息安全技术 术语

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 18336-2015 信息技术 安全技术 信息技术安全性评估准则

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069-2010、GB/T 35273-2017和GB/T 18336-2015界定的术语和定义适用于本文件。

3.1.1 车载终端 TBOX Telematics BOXF

具备数据输入输出、数据存储、计算处理以及通信等功能，可采集车内相关ECU数据，可发送ECU控制指令，还可集成定位、热点等多种功能的车联网控制单元。

3.1.2 移动互联 mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

3.1.3 CAN 总线 CAN bus

CAN总线是ISO国际标准化的串行通信协议。

3.2 缩略语

CAN	控制器局域网络	Controller Area Network
CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CNVD	国家信息安全漏洞共享平台	China National Vulnerability Database
ECU	电子控制单元	Electronic Control Unit

IP	网络互联的协议	Internet protocol
IVI	车载信息娱乐系统	In-Vehicle Infotainment
MCU	微控制单元	Microcontroller Unit
TBOX	车联网盒子	Telematics BOX
TOE	评估对象	Target of Evaluation
TSP	车联网服务平台	Telematics Service Provider

4 总体说明

车载TBOX，指安装在汽车上用于采集车身信息并进行控制跟踪的控制单元。TBOX具备硬件、操作系统和软件等，可能的软件有定位、导航、娱乐等。车载TBOX与主机通过CAN总线通信，实现对车辆状态信息、控制指令、远程诊断和按键状态信息等的传递；以数据链路的方式通过后台TSP系统与PC端网页或移动端App实现双向通信。当用户通过PC端或移动端发送控制指令后，后台会发出指令到车载TBOX，车辆在获取到控制命令后，通过CAN总线发送控制报文并实现对车辆的控制。

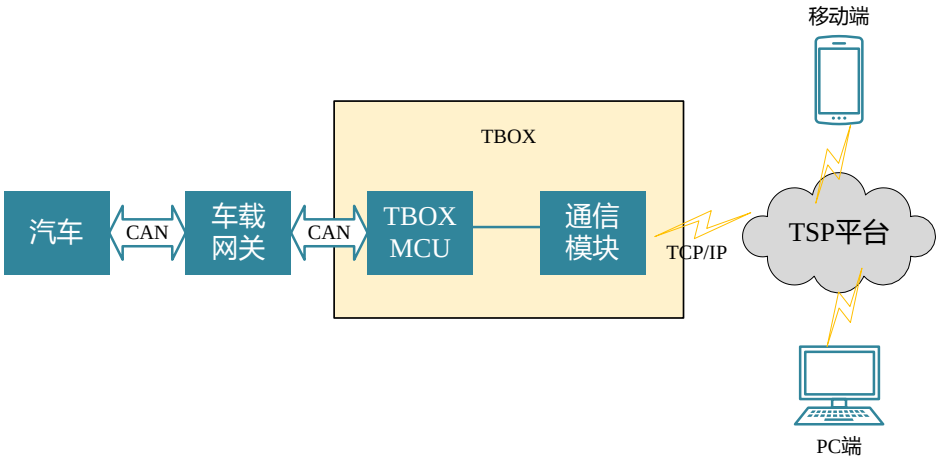

图1 TBOX结构与逻辑示意图

5 车载 TBOX 信息安全技术要求

5.1 硬件安全

硬件安全应满足如下要求：

a) 具备防拆保护措施，包括但不限于开盖检测、拆机告警等方式；

b) 设备如开放调试接口的应在上市前进行禁用或采用安全调试模式；

c) 具备足够的安全机制保证密钥的产生、分发、存储和销毁过程的安全性；

d) 关键加密算法实现应具备抵抗侧信道分析和故障注入分析等物理攻击的能力，防止根密钥被破解。

5.2 操作系统安全

操作系统安全应满足如下要求：

a) 应支持安全启动机制，对引导程序或固件等进行有效性验证，只有通过验证的才能执行；
b) 升级过程应对升级文件进行签名校验和完整性校验，并制定完整有效的机制，确保升级失败后，操作系统能有效恢复至升级前的正常工作状态；
c) 操作系统不应含有 CNVD 与 CNNVD6 个月前公布的高危漏洞；
d) 支持对重要事件的日志记录功能，记录的内容至少包含事件主体、事件发生的时间、事件类型、事件是否成功等要素，并能按照策略上传至服务器。重要事件包括但不限于：登录尝试、文件的创建、打开或删除，权限设置等；应具有保证日志文件安全性的措施，防止非授权访问；
e) 应定义并限制外围存储介质（如 U 盘、SD 卡等）上可读取和可执行的文件类型，避免来自外围储存介质的恶意攻击；
f) 具备 CAN 总线控制器安全控制功能，将内网 CAN 总线和对外接口（如 USB、SD 等）隔离。

5.3 软件安全

如TBOX支持安装软件或配套软件，则软件安全应满足如下要求：

a) 应采用签名认证机制，未经签名的应用软件仅当用户确认后才能执行下一步操作；
b) 不应非授权收集、传输用户个人信息；
c) 应具备代码混淆、加壳等安全措施，防止被逆向攻击；
d) 应采取访问控制机制，防止对系统资源和其他软件的非授权访问；
e) 应用软件不应含有 CNVD 与 CNNVD6 个月前公布的高危漏洞；
f) 应具有记录应用状态及使用情况的日志功能，并支持上传和集中管理。

5.4 数据安全

数据安全应满足如下要求：

a) 设备采集用户数据应对用户进行明确告知，在用户授权后可继续下一步操作，支持关闭数据采集的功能；
b) 重要数据应加密存储，保证重要数据在存储过程中的完整性和保密性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和个人信息等；
c) 安全运行环境应提供可靠的时间戳服务；
d) 安全运行环境应具备抵抗恶意代码访问受保护资源的能力，受保护资源包括但不限于随机数源、内存、缓冲区、中断资源；
e) 数据的传输应进行完整性保护，防止数据被篡改和伪造；
f) 具备彻底删除的能力，数据被删除后不可被恢复、重新使用或访问。

5.5 通信安全

通信安全应满足如下要求：

a) 应具备对通信数据的消息校验和认证机制，防止攻击者伪造、篡改信息；
b) 应采用控制策略避免大量集中地向 CAN 总线发送数据包，以避免造成总线拥塞和拒绝服务；
c) 应明确定义与 CAN 总线的通信功能，且仅包含业务相关功能，不应使用透传功能。

6 车载 TBOX 信息安全测试方法

6.1 硬件安全

测试编号	6.1.1
测试项目	主芯片具备防拆保护措施，包括但不限于开盖检测、拆机告警等方式
项目要求	见 5.1 a)
测试条件	TBOX 设备外观完好
测试步骤	步骤1：使用拆解工具对TBOX进行拆解； 步骤2：观察检查其是否出现报警、自毁等现象。
预期结果	在步骤 2 后，如果未出现报警、自毁等现象，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.1.2
测试项目	设备如开放调试接口的应在上市前进行禁用或采用安全调试模式
项目要求	见 5.1 b)
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：使用串口/JTAG调试工具发送测试命令，测试所有调试接口和测试接口是否关闭； 步骤2：如存在开放接口，测试其是否采用安全调试模式。
预期结果	在步骤 2 后，如果调试接口和测试接口未关闭，且未采用安全调试模式，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.1.3
测试项目	具备足够的安全机制保证密钥的产生、分发、存储和销毁过程的安全性
项目要求	见 5.1 c)
测试条件	提供密钥管理的相关文档
测试步骤	步骤1：审查厂商提供的文档，判断密钥生成的安全性，检查根密钥的随机数熵值； 步骤2：检查密钥分发、存储和销毁的方式，评估密钥安全风险。
预期结果	在步骤 1 后，如果未随机数熵值不满足随机性要求，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果密钥分发、存储和销毁过程存在泄露风险，则项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.1.4
测试项目	关键加密算法应具备抵抗侧信道分析和故障注入分析等物理攻击的能力,防止根密钥被破解
项目要求	见 5.1 d)

测试条件	提供加密方案实现的文档，提交供硬件物理攻击测试的电路板
测试步骤	步骤1：参考厂商提供的文档，使用工具对加密运算的过程进行侧信息收集或故障注入攻击； 步骤2：利用分析工具对测试电路板进行相应的密码安全性分析； 步骤3：得到密钥安全性分析的结果。
预期结果	在步骤 3 后，如果获得密钥，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

6.2 操作系统安全

测试编号	6.2.1
测试项目	应支持安全启动机制，对引导程序或固件等进行有效性验证，只有通过验证的才能执行
项目要求	见 5.2 a)
测试条件	车载 TBOX 处于正常工作状态，提供引导程序或固件文件
测试步骤	步骤1：检测系统是否开启安全启动模式； 步骤2：使用无签名的固件进行烧写，测试是否能够正常启动； 步骤3：使用有签名的固件进行烧写，测试是否能够正常启动。
预期结果	在步骤 2 后，如果系统正常启动，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 3 后，如果系统未正常启动，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.2.2
测试项目	升级过程应对升级文件进行签名校验和完整性校验，并制定完整有效的机制，确保升级失败后，操作系统能有效恢复至升级前的正常工作状态
项目要求	见 5.2 b)
测试条件	提供升级文件，车载 TBOX 处于正常工作状态
测试步骤	步骤1：修改厂家提供的升级包并签名，执行系统更新，检测升级过程能否正常运行； 步骤2：使用厂家提供的升级包进行系统更新，在升级过程中进行断点等操作强制中止升级，检查设备是否能恢复到正常工作状态。
预期结果	在步骤 1 后，如果升级过程正常运行，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果设备未恢复到正常工作状态，该项目评测结果在“不符合要求”，评测结束；如果设备恢复到正常工作状态，该项目评测结果为“未见异常”，评测结束。

测试编号	6.2.3

测试项目	操作系统不应含有 CNVD 与 CNNVD6 个月前公布的高危漏洞
项目要求	见 5.2 c）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：分析已公布的与操作系统相关的高危漏洞； 步骤2：利用相关工具、脚本对设备进行测试。
预期结果	在步骤 2 后，如果发现存在相应漏洞，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.2.4
测试项目	支持对重要事件的日志记录功能，记录的内容至少包含事件主体、事件发生的时间、事件类型、事件是否成功等要素，并能按照策略上传至服务器。重要事件包括但不限于：登录尝试、文件的创建、打开或删除，权限设置等；应具有保证日志文件安全性的措施，防止非授权访问
项目要求	见 5.2 d）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：检查操作系统的和日志的上传策略； 步骤2：检查日志是否记录事件主体、发生时间、事件类型和是否成功等要素，并能按照策略上传至服务器。
预期结果	在步骤 2 后，如果没有日志或日志要素缺失，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.2.5
测试项目	应定义并限制外围存储介质（如 U 盘、SD 卡等）上可读取和可执行的文件类型，避免来自外围储存介质的恶意攻击
项目要求	见 5.2 e）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：检查外围存储介质的可读取和可执行的文件类型。
预期结果	在步骤 1 后，如果没有对外围存储介质的可读取和可执行的文件类型进行定义，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.2.6
测试项目	具备 CAN 总线控制器安全控制功能，将内网 CAN 总线和对外接口（如 USB、SD 等）隔离
项目要求	见 5.2 f）
测试条件	车载 TBOX 处于正常工作状态

测试步骤	步骤1：检查CAN总线控制器是否具备安全控制功能； 步骤2：检查内网CAN总线与对外接口是否隔离。
预期结果	在步骤 1 后，如果不具备安全控制功能，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果不能够隔离，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

6.3 软件安全

测试编号	6.3.1
测试项目	应采用签名认证机制，未经签名的应用软件仅当用户确认后才能执行下一步操作
项目要求	见 5.3 a）
测试条件	提供应用软件列表，应用软件在车载 TBOX 上正常运行
测试步骤	步骤1：使用签名分析工具对列表中的应用软件进行签名检查； 步骤2：尝试安装未签名的应用，检测安装过程是否提示并告知风险； 步骤3：运行未签名的应用，检测是否经过用户确认后才执行下一步操作。
预期结果	在步骤 1 后，如果存在签名不可信的应用软件，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果未提示或未告知风险，则该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 3 后，如果存在未经用户确认即运行下一步的情况，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.3.2
测试项目	不应非授权收集、传输用户敏感信息
项目要求	见 5.3 b）
测试条件	提供应用软件列表，应用软件在车载 TBOX 上正常运行
测试步骤	步骤1：调用应用软件的敏感功能； 步骤2：检查其是否符合“可知可控”原则。
预期结果	在步骤 2 后，如果存在不符合“可知可控”原则的现象，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.3.3
测试项目	应具备代码混淆、加壳等安全措施，防止被逆向攻击
项目要求	见 5.3 c）

测试条件	提供应用软件列表，应用软件在车载 TBOX 上正常运行
测试步骤	步骤1：使用工具对应用软件进行逆向分析； 步骤2：检测其是否具备代码混淆、加壳等措施。
预期结果	在步骤 2 后，如果未进行代码混淆、加壳等措施，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.3.4
测试项目	应采取访问控制机制，防止对系统资源和其他软件的非授权访问
项目要求	见 5.3 d）
测试条件	提供应用软件列表，应用软件在车载 TBOX 上正常运行
测试步骤	步骤1：检查应用软件的访问控制机制； 步骤2：尝试绕过访问机制，访问系统资源和其他软件。
预期结果	在步骤 2 后，如果访问控制机制被绕过，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.3.5
测试项目	应用软件不应含有 CNVD 与 CNNVD6 个月前公布的高危漏洞
项目要求	见 5.3 e）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：分析已公布的与应用软件相关的高危漏洞； 步骤2：利用相关工具、脚本对设备进行测试。
预期结果	在步骤 2 后，如果发现存在相应漏洞，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.3.6
测试项目	应具有记录应用状态及使用情况的日志功能，并支持上传和集中管理
项目要求	见 5.3 f）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：检查应用软件的日志； 步骤2：检查日志中是否记录应用状态和使用情况。
预期结果	在步骤 2 后，如果没有日志或日志要素缺失，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

6.4 数据安全

测试编号	6.4.1
测试项目	设备采集用户数据应对用户进行明确告知，在用户授权后可继续下一步操作，支持关闭数据采集的功能
项目要求	见 5.4 a）
测试条件	提供设备采集用户数据的说明文档
测试步骤	步骤1：审阅厂家提供的文档，判断其是否明确告知采集用户数据的内容、业务用途等内容； 步骤2：检测设备运行中实际采集用户数据情况是否与说明文档一致。
预期结果	在步骤 1 后，如果文档缺少对内容和业务用途等的描述，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果出现不一致的情况，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.4.2
测试项目	重要数据应加密存储，保证重要数据在存储过程中的完整性和保密性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和个人信息等
项目要求	见 5.4 b）
测试条件	对重要数据加密方式的相应说明文档
测试步骤	步骤1：尝试以非授权的身份访问重要数据； 步骤2：审查厂家提供的加密方式的说明文档，检查其加密方案是否涵盖必要的重要数据； 步骤3：尝试读取重要数据，验证其为加密存储。
预期结果	在步骤 1 后，如果可以访问重要数据，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果加密方案不完善或加密方案未涵盖必要的重要数据，则该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 3 后，如果读取重要数据为明文存储或部分明文存储，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.4.3
测试项目	安全运行环境应提供可靠的时间戳服务
项目要求	见 5.4 c)
测试条件	提供有关时间戳的说明文档
测试步骤	步骤1：审查厂家提供的时间戳的说明文档，检查其时间戳方案是否合理。

预期结果	在步骤 1 后，如果方案不完善，则该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.4.4
测试项目	安全运行环境应具备抵抗恶意代码访问受保护资源的能力,受保护资源包括但不限于随机数源、内存、缓冲区、中断资源
项目要求	见 5.4 d）
测试条件	提供安全运行环境对资源的保护方案
测试步骤	步骤1：审查厂家提供的保护方案，检查其方案能否覆盖随机数源、内存、缓冲区和终端资源等； 步骤2：检查安全运行环境是否具备抵抗恶意代码访问受保护资源的能力。
预期结果	在步骤 1 后，如果方案不完善，则该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果检查过程中发现安全运行环境不具备抵抗恶意代码的能力，则该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.4.5
测试项目	数据的传输应进行完整性保护，防止数据被篡改和伪造
项目要求	见 5.4 e）
测试条件	提供数据传输完整性保护方案
测试步骤	步骤1：审查厂商提供的数据传输完整性保护方案； 步骤2：使用篡改、伪造等方式实施攻击，检测是否攻击成功。
预期结果	在步骤 1 后，如果没有数据传输完整性保护方案，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果攻击成功，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.4.6
测试项目	具备彻底删除的能力，数据被删除后不可被恢复、重新使用或访问
项目要求	见 5.4 f）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：对选定数据执行删除操作； 步骤2：尝试恢复、使用或访问被步骤1中删除的数据。

预期结果	在步骤 2 后，如果出现恢复、使用或访问成功的现象，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

6.5 通信安全

测试编号	6.5.1
测试项目	应具备对通信数据的消息校验和认证机制，防止攻击者伪造、篡改信息
项目要求	见 5.5 a）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：修改通信数据的内容，并重新计算消息校验值； 步骤2：使用非授权的身份对步骤1后的数据进行访问； 步骤3：使用授权的身份对步骤1后的数据进行访问。
预期结果	在步骤 2 后，如果访问成功，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 3 后，如果访问成功，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.5.2
测试项目	应采用控制策略避免大量集中地向CAN总线发送数据包，以避免造成总线拥塞和拒绝服务
项目要求	见 5.5 b）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：审查厂家提供的控制策略文档，应能避免造成总线拥塞和拒绝服务。
预期结果	在步骤 1 后，如果不具备控制策略文档或控制策略不完善，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

测试编号	6.5.3
测试项目	应明确定义与 CAN 总线的通信功能，且仅包含业务相关功能，不应使用透传功能
项目要求	见 5.5 c）
测试条件	车载 TBOX 处于正常工作状态
测试步骤	步骤1：检查TBOX与CAN总线的通信功能是否仅包含业务相关功能； 步骤2：尝试使用透传功能。
预期结果	在步骤 1 后，如果包含与业务无关功能，该项目评测结果为“不符合要求”，评测结束；否则，评测继续； 在步骤 2 后，如果能否使用透传功能，该项目评测结果为“不符合要求”，评测结束；否则，该项目评测结果为“未见异常”，评测结束。

附 录 A
（资料性附录）
安全威胁和目标

A.1 安全威胁

A.1.1 硬件安全威胁

芯片内系统程序、终端参数、安全数据、用户数据、系统配置、安全配置被篡改或非法获取，芯片被拆解攻击和被恶意代码直接访问加密芯片接口、内网接口等，密钥被物理攻击的方式获取。

A.1.2 操作系统安全威胁

操作系统文件和系统数据被窃取或篡改，系统中保存的用户敏感数据被窃取或篡改，操作系统的运行被非授权干扰或中断。

A.1.3 软件安全威胁

应用软件被恶意篡改导致的恶意代码和恶意行为，已安装的应用软件源代码或敏感数据被非授权访问，暴露组件被攻击调用，应用软件的启动、升级和退出过程被非授权干扰或中断。

A.1.4 数据安全威胁

收集的数据被拦截或篡改，数据在传输过程中被窃取或篡改，恶意数据在传输环节被注入，在数据被用户删除后未彻底清除或未设置防恢复保护，导致数据被窃取作为攻击样本。

A.1.5 通信安全威胁

总线数据和私有协议被非授权的攻击者读取，车载TBOX与TSP间通信被嗅探或攻击，使通信数据被窃取或篡改。

A.2 安全目标

A.2.1 硬件安全目标

车载TBOX的硬件安全目标是在硬件芯片保证数据运算和存储的安全性，能够抵抗拆解攻击和针对密钥的非侵入式和半侵入式物理攻击，确保芯片内系统程序、终端参数、安全数据、用户数据不被篡改或非法获取。硬件芯片应提供安全运行环境的支撑，防止恶意代码直接访问加密芯片接口、内网接口。

A.2.2 操作系统安全目标

车载TBOX的操作系统安全目标是能够进行安全启动、安全升级以及诊断远程异常问题，能够保证符合车载TBOX应用场景的身份认证管理机制，保证操作系统文件和系统数据的保密性和完整性，能够正常运行且处于安全状态。

A.2.3 软件安全目标

车载TBOX的软件安全目标是保证运行可信来源的软件，具备抵抗逆向分析、反编译、重放攻击、篡改、非授权访问等安全威胁，暴露组件能够抵抗攻击调用，保证应用启动、升级和退出时的安全。

A.2.4 数据安全目标

车载TBOX的数据安全目标是保证其对用户数据、总线数据的收集、加工、转移、删除过程的安全性，确保用户数据不被非法访问、获取和篡改。

A.2.5 通信安全目标

车载TBOX通信安全目标包括对内通信和对外通信，对内通信是指车载TBOX与车内总线间的通信，对外通信是指车载TBOX与TSP间进行蜂窝移动通信。

对内通信安全目标是保证车载TBOX与车内总线间的通信安全，防止非授权的攻击者对总线数据和私有协议进行读取，保证TBOX不向内部ECU发送伪造、重放等攻击方式的指令，不非法占用内部总线资源，保证内部数据的保密性和完整性。

对外通信安全目标是保证车载TBOX与TSP间蜂窝移动通信的安全，保证通信连接具有必要的认证、加密和完整性校验手段，可以对抗嗅探、中间人攻击、重放等多种针对通信的安全威胁，保证数据的保密性完整性和保证通信质量。

参 考 文 献

[1] GB/T 32960.2 电动汽车远程服务于管理系统技术规范 第2部分：车载终端
[2] YD/T 2407-2013 移动智能终端安全能力技术要求
[3] YD/T 2408-2013 移动智能终端安全能力测试方法
[4] YD/T 3082-2016 移动智能终端上的个人信息保护技术要求
[5] T/CSAE 101-2018 智能网联汽车车载端信息安全技术要求

电信终端产业协会团体标准

车载 TBOX 信息安全技术要求和测试方法

T/TAF XXX—XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn