中国汽车工程学会标准

T/CSAE 101.2-20xx

智能网联汽车车载端信息安全测试规程

Intelligent and Connected Vehicle On-Board Terminal Cyber Security Test Methods

（征求意见稿）

中国汽车工程学会

目　　次

前　言

本标准/本部分按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由中国智能网联汽车产业创新联盟提出，由中国汽车工程学会归口。

本标准起草单位：工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、北京航空航天大学、中国汽车工程学会、国汽（北京）智能网联汽车研究院有限公司、中国第一汽车集团有限公司、广州汽车集团股份有限公司、北京新能源汽车股份有限公司、上海汽车集团股份有限公司、重庆长安汽车股份有限公司、华为技术有限公司、电子科技大学、北京梆梆安全科技有限公司、惠州市德赛西威汽车电子股份有限公司、长城汽车股份有限公司、惠州华阳通用电子有限公司、深圳市纽创信安科技开发有限公司、广东为辰信息科技有限公司、四维创智（北京）科技发展有限公司。

本标准主要起草人：

—

智能网联汽车车载端信息安全测试规程

1 范围

本标准规定了对智能网联汽车车载端信息安全防护是否符合T/CSAE 101-2018的要求所对应的测评方法，包括整体安全、硬件安全、操作系统安全、应用软件安全、对内通信安全、对外通信安全和用户数据安全等的测评要求和评价标准。

本标准适用于整车企业、车载端供应商、第三方信息安全测评服务机构对车载信息安全保护状况进行安全测试评估。智能网联汽车车载端信息安全监管职能部门依法对车载端信息安全进行监督检查可以参考本标准。

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 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 34976-2017 信息安全技术-移动智能终端操作系统安全技术要求与测试评价

GB/T 34975-2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

T/CSAE 101-2018 智能网联汽车车载端信息安全技术要求

3 术语、定义和缩略语

3.1 智能网联汽车 intelligent and connected vehicles

智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与X（车、路、人、云等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶，并最终可实现替代人来操作的新一代汽车。

3.2 智能网联汽车车载端 intelligent and connected vehicles on-board terminal

智能网联汽车车载端是智能网联汽车的一个子系统，具备数据输入输出、计算处理、存储、通信等功能，可采集车内相关ECU数据并发送控制ECU的指令，集成定位、导航、娱乐等多种功能，是汽车网联化、接入移动互联网和车际网的功能单元。

3.3 用户 user

使用车载端资源的主体。

3.4 用户数据 user data

— 车载端采集、处理、生成，以及存储的用户个人信息和用户使用车辆的信息，包括但不限于车辆资产数据（车辆标识等）、用户标识信息、应用数据（在本地生成的数据、在用户许可后由外部进入用户数据区的数据等）。

3.5 授权 authorization

在用户身份经过认证后，根据预先设置的安全策略，授予用户相应权限的过程。

3.6 数字签名 digital signature

附件在数据单元上的数据，或是对数据单元所作的密码交换，这种数据或变换允许数据单元的接收者用以证明数据单元的来源和完整性，并保护数据单元的发送者和接收者以防止数据被第三方伪造，保护发送者以防止接收者伪造。

3.7 代码签名 code signature

利用数字签名机制，由具有签名权限的实体对全部或部分代码进行签名的机制。

3.8 缩略语

ICV Intelligentand Connected Vehicle 智能网联汽车
BGA Ball Grid Array 焊球阵列封装
LGA Land Grid Array 栅格阵列封装
SPA Simple Power Analysis 简单功耗分析
DPA Differential Power Analysis 差分功耗分析
CPA Correlation Power Analysis 相关功耗分析
ECU Electronic Control Unit 电子控制单元
CAN Controller Area Network 控制器局域网络
ECC Error Correcting Code 错误检查和纠正

4 概述及测试基本要求

4.1 概述

智能网联汽车信息安全体系以及车载端的安全架构如图1所示。车载端信息安全包括硬件安全、操作系统安全、应用安全、对外通信安全和对内通信安全，以及数据安全。

本标准描述了车载端信息安全技术要求的测试方法。测试结果有以下两种：

— 未见异常：通过评测方法没有发现存在安全风险或安全事件；

— 不符合要求：直接发现安全事件或不符合安全技术要求。

本章中所提及的技术要求参照T/CSAE 101-2018 《智能网联汽车车载信息安全技术要求》相应条目中的要求。

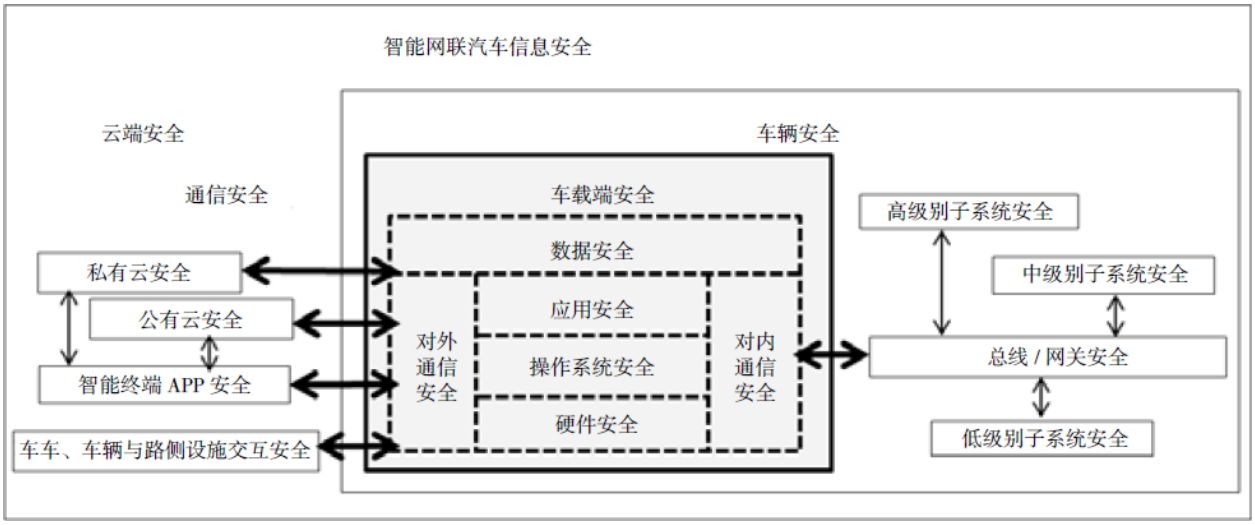

图1　智能网联汽车信息安全体系及车载端安全架构示意图

4.2　测试基本要求

车载端应满足车载端安全技术基本测试条件，包括提交车载端安全技术测试需求说明书、安全技术防护说明文档，提供可以正常工作的测试样品及相应的技术支持。

5　车载端安全技术测试方法

5.1　整体安全

5.1.1　安全技术的选择与实施

编号5.1.1.1	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.1.1.1 项，应通过风险评估过程，全面分析网联接口与威胁攻击路径，明确车辆整体安全需求与车载端安全需求，综合选择身份认证、访问控制、检测响应等多种技术措施对车载端自身进行安全防护，并将车载端安全防护作为车辆整体安全防护体三予有机组成部分，以实现车辆整体安全目标（例如：确保驾驶员和交通参与人员的人身安全）。	
测试条件：提交安全技术方案设计文档。	
测试步骤： 步骤（1）：检查厂商提交的文档，验证厂商是否通过风险评估，分析网联接口与威胁攻击路径，并且明确车辆整体安全需求与车载端安全需求； 步骤（2）：检查厂商提交的文档，验证厂商是否选择身份认证、访问控制、安全审计等安全功能策略对车载端进行安全防护，并将车载端安全防护作为车辆整体安全防护体系的有机组成部分，以实现车辆整体安全目标； 步骤（3）：所选择的技术处置措施与安全风险具备关联性。	
预期结果： （1）厂商提交的文档中描述风险评估过程，分析网联接口与威胁攻击路径，并且明确车辆整体安全需求与车载端安全需求； （2）安全技术方案选择身份认证、访问控制、安全审计等安全功能策略对车载端进行安全防护，并将车载端安全防护作为车辆整体安全防护体系的有机组成部分，以实现车辆整体安全目标。	

判定条件： 在步骤（1）后，如果提交文档分析过程不完备，或未明确车辆整体安全需求与车载端安全需求，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果未选身份认证、访问控制、安全审计等安全功能策略对车载端进行安全防护，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果所选择技术措施与识别的风险无明显相关性，则该项目评测结果为“不符合要求”，评测结束。

编号5.1.1.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.1.1.2 项，应综合考虑整体网络安全防护需求，车载端的安全技术措施能够有效地与云端安全技术措施和通信网络安全技术措施相配合。	
测试条件：提交整体安全技术方案文档	
测试步骤： 步骤（1）：检查厂商提交的文档，验证厂商是否考虑整体网络安全防护需求，车载端的安全技术措施是否可以与云端安全技术措施和通信网络安全技术措施配合。	
预期结果： （1）厂商考虑包括车端、车端与云端和通信网络信息交互的安全性等整体安全性，覆盖保密性、完整性和可用性等多方面的安全措施与云端和通信网络安全技术措施相配合。	
判定条件： 在步骤（1）后，如果厂商整体安全性考虑不完备，或车载端安全防护措施与云端安全技术措施、通信网络安全技术措施未配合，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。	

编号5.1.1.3	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.1.1.3 项，车载端安全技术措施的选择和实施，应与整车设计开发验证测试流程紧密结合。	
测试条件：提交安全技术方案实施过程相关文档，相关检测报告	
测试步骤： 步骤（1）：检查厂商提交的文档，验证文档中车载端安全技术措施是否实现。	
预期结果： （1）在文档中涉及车载端安全技术措施可以实现。	
判定条件： 在步骤（1）后，如果提交文档车载端安全技术措施未实现，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。	

5.2 硬件安全

5.2.1 设计安全

编号5.2.1.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.2.1.1 项，车载端系统所使用的芯片不能存在可以非法对芯片内存进行访问或者更改芯片功能的隐蔽接口。芯片在设计验证阶段使用的调试接口应在上市产品中禁用。	
测试条件：提交芯片相关文档，提交硬件安全性测试电路板。	
测试步骤： 步骤（1）：检测车载终端所用芯片是否存在非法对芯片内存进行访问或更改芯片功能的隐蔽接口； 步骤（2）：使用调试工具检测，在非授权的情况下访问芯片内容或更改芯片功能，检测是否可以通过接口读取或改写车载终端内存。	
预期结果： （1）车载端所用芯片不存在可以非法对车载终端内存进行访问或更改车载终端功能的隐蔽接口； （2）在非授权的情况下，无法通过调试接口读取芯片内容或改写芯片功能。	
判定条件： 在步骤 （1）后，如果发现可以访问芯片内存或更改芯片功能的隐蔽接口，或发现研发阶段使用的调试接口，则该项目评测结果为“不符合要求”，评测结束； 在步骤 （2）后，如果在非授权的情况下可以通过调试接口读取芯片内容或改写芯片功能，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。	

编号5.2.1.2	级别：4级
技术要求：参照 T/CSAE 101-2018 第 5.2.1.2 项，车载端系统的电路板不能存在用以标注芯片、端口和管脚功能的可读丝印。	
测试条件：提交硬件安全性测试的电路板	
测试步骤： 步骤（1）：检查厂商硬件安全性测试电路板，是否存在用以标注芯片、端口和管脚功能的可读的丝印。	
预期结果： （1）车载端系统的电路板不存在用以标注芯片、端口和管脚功能的可读丝印。	
判定条件： 在步骤 （1）后，如果电路板有用以标注芯片、端口和管脚功能的可读丝印，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。	

编号5.2.1.3	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.2.1.3 项，车载端系统芯片之间敏感数据的通信线路应尽量隐蔽（例如：使用多层电路板的车载端系统采用内层布线方式隐藏通信线路），对抗针对车载端内部数据传输的窃听和伪造攻击。	
测试条件：提交电路板布线图，提交硬件安全性测试电路板	
测试步骤： 步骤（1）：使用工具（例如示波器等）检查电路板，敏感数据通信线路是否隐蔽，使用多层电路板	

的车载端系统是否采用内层布线方式隐藏通信线路。
预期结果： （1）电路板上敏感数据通信线路隐蔽，使用多层电路板的车载端系统采用内层布线方式隐藏通信线路。
判定条件： 在步骤 （1）后，如果敏感数据通信线路显露，或多层电路板未将敏感数据通信线路在内层布线，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。

编号5.2.1.4	级别：4级
技术要求：参照 T/CSAE 101-2018 第 5.2.1.4 项，车载端所使用的关键芯片应尽量减少暴露管脚（例如：采用 BGA/LGA 封装的芯片）。	
测试条件：提交芯片相关文档和具体型号，提交硬件安全性测试电路板	
测试步骤： 步骤（1）：检查厂商提交的文档中是否描述关键芯片隐藏管脚，是否要求采用如BGA或LGA等封装的芯片； 步骤（2）：检查电路板，关键芯片是否隐藏管脚，是否采用了 BGA 或 LGA 等封装的芯片。	
预期结果： （1）厂商提交的文档中描述关键芯片隐藏管脚，并要求采用如BGA或LGA等封装的芯片； （2）电路板上关键芯片隐藏管脚，采用了BGA或LGA等封装的芯片。	
判定条件： 在步骤 （1）后，厂商提交的文档中未描述关键芯片隐藏管脚，或未要求芯片封装技术，则该项目评测结果为“不符合要求”，评测结束； 在步骤 （2）后，如果关键芯片没有隐藏管脚，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。	

5.2.2 访问控制

编号5.2.2.1	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.2.2.1 项，车载端具备硬件实现的安全区域或安全模块，实现车载端设备重要数据安全存储与隔离。	
测试条件：提交安全存储区域相关说明文档。	
测试步骤： 步骤（1）：检查车载端是否通过硬件实现安全区域或安全模块； 步骤（2）：查看相应的安全区域或安全模块运行日志，是否在重要数据存储与隔离的过程中使用安全区域或安全模块。	
预期结果： （1）车载端硬件具备通过硬件实现的安全区域或安全模块； （2）可以在重要数据存储与隔离的过程中使用安全区域或安全模块，并记录在安全区域或安全模块运行日志中。	

判定条件：

在步骤（1）后，如果未通过硬件设置安全区域或安全模块，则该项目评测结果为“不符合要求”，评测结束；

在步骤（2）后，如果未在重要数据存储与隔离的过程中使用安全区域或安全模块，或未记录在安全区域或安全模块运行日志中，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。

编号5.2.2.2	级别：3—4级

技术要求：参照 T/CSAE 101-2018 第 5.2.2.2 项，在安全区域或安全模块中一次性写入的敏感信息，应保证无法非授权获取或者篡改。

测试条件：提交安全存储区域相关说明文档，提交硬件安全性测试电路板

测试步骤：

步骤（1）：检查厂商提交的文档，查看安全区域或安全模块中一次性写入的敏感信息列表；

步骤（2）：非授权情况下尝试获取或修改安全区域或安全模块中的敏感信息，检测是否可以获取和修改敏感信息。

预期结果：

（1）厂商提交的文档对安全区域或安全模块中一次性写入的敏感信息进行了说明；

（2）非授权情况下获取或修改安全区域或安全模块中的敏感信息失败。

判定条件：

在步骤（1）后，如果提交文档未对安全区域或安全模块中一次性写入的敏感信息进行说明，则该项目评测结果为“不符合要求”，评测结束；

在步骤（2）后，如果在非授权情况下可以获取或修改安全区域或安全模块中的敏感信息，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。

编号5.2.2.3	级别：4级

技术要求：参照 T/CSAE 101-2018 第 5.2.2.3 项，安全区域或安全模块应具备检测与处置非授权访问的能力，对抗暴力破解。

测试条件：提交安全存储区域相关说明文档，送检车载端系统处于正常工作状态

测试步骤：

步骤（1）：检查厂商提交的文档，查看安全区域或安全模块检测和处置非授权访问的说明；

步骤（2）：尝试非授权访问安全区域或安全模块，检测车载端是否可以检测并阻止非授权访问安全区域或安全模块。

预期结果：

（1）厂商提交的文档中说明安全区域或安全模块检测和处置非授权访问机制；

（2）车载端可以检测到安全区域或安全模块非授权访问，并阻止访问。

判定条件：

在步骤（1）后，如果提交文档未对安全区域或安全模块检测和处置非授权访问机制进行说明，则该项目评测结果为“不符合要求”，评测结束；

在步骤（2）后，如果车载端未检测到安全区域或安全模块非授权访问，或未阻止非授权访问，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。

—

5.2.3 抗攻击防护

编号5.2.3.1	级别：4级
技术要求：参照 T/CSAE 101-2018 第 5.2.3.1 项，使用必要的安全机制（例如：封装），防御针对芯片的电压、时钟、电磁、激光等方式的故障注入攻击。	
测试条件：提交密码方案介绍性文档，提交硬件安全性测试电路板。	
测试步骤： 步骤（1）：使用测试工具制造电压、时钟、电磁、激光等故障，采集系统在故障条件下运行的特征数据； 步骤（2）：分析采集到的数据，查看是否存在信息泄漏，包括但不限于密钥。	
预期结果： （1）系统在电压、时钟、电磁、激光等方式的故障条件下运行的特征数据不存在信息泄露，包括但不限于密钥。	
判定条件： 在步骤（2）后，如果存在信息泄露，可以破解密钥，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。	

编号5.2.3.2	级别：4级
技术要求：参照 T/CSAE 101-2018 第 5.2.3.2 项，使用必要的防护措施，对抗针对加密芯片的简单功耗分析（SPA）攻击、一阶差分功耗分析（DPA）攻击、相关功耗分析（CPA）攻击，以及利用运行时间、温度等其它信息进行的侧信道攻击。	
测试条件：提交密码方案介绍性文档，提交硬件安全性测试电路板，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：使用芯片测试工具，对加密运算过程中的功率轨迹波形和相应密文进行一定量的收集； 步骤（2）：针对收集到的信息，利用SPA、DPA、CPA等方法对密钥进行分析破解； 步骤（3）：实施运行时间、温度等其它信息进行的侧信道攻击。	
预期结果： （1）车载端使用必要的防护措施，对抗SPA、DPA、CPA，以及利用运行时间、温度等其它信息进行的侧信道攻击。	
判定条件： 在步骤（1）后，如果可以利用SPA、DPA、CPA等方法对密钥进行分析破解，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果可以利用运行时间、温度等信息进行的侧信道攻击导致系统不能正常运行，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。	

编号5.2.3.3	级别：4级
技术要求：参照 T/CSAE 101-2018 第 5.2.3.3 项，使用必要的防护机制，对抗针对车载端设备内存的侵入和篡改攻击。	

测试条件：提交密码方案介绍性文档，提交硬件安全性测试电路板
测试步骤： 步骤（1）：检查厂商提交的文档，查看针对侵入和篡改车载端设备内存的防护机制； 步骤（2）：尝试非授权访问车载端设备内存，并修改内存中的文件，检测车载端是否提示并阻止非授权访问和修改车载端设备内存文件。
预期结果： （1）厂商提交的文档中说明针对侵入和篡改车载端设备内存的防护机制； （2）车载端可以检测到内存非授权访问和修改，并报警提示、阻止访问和修改。
判定条件： 在步骤（1）后，如果提交文档未对安全区域或安全模块检测和处置非授权访问机制进行说明，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未检测到安全区域或安全模块非授权访问，或未进行报警提示，或未阻止非授权访问，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。

5.3 操作系统安全

5.3.1 操作系统安全启动

编号5.3.1.1	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.1.1 项，在安全存储区域存储操作系统签名。操作系统启动时应使用可信机制，在验证操作系统签名并判定通过后，再从可信存储区域加载车载端操作系统，避免加载被篡改的操作系统。	
测试条件：提交安全技术方案设计相关文档，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看设计过程中操作系统签名是否存储在安全区域并验证； 步骤（2）：使用系统调试工具检测车载端系统启动时是否采用安全机制，在验证操作系统签名并判定通过后，再从可信存储区域加载车载端操作系统； 步骤（3）：检测是否可以通过更改设置或者修改代码旁路安全启动； 步骤（4）：采取多种方式破坏信任链，检测安全启动是否仍然执行。	
预期结果： （1）厂商提交的文档中要求操作系统签名储存在安全区域内； （2）车载端系统启动时采用安全机制，在验证操作系统签名并判定通过后，再从可信存储区域加载车载端操作系统； （3）车载端系统在被旁路安全启动后提示并报警系统异常，不能进入正常工作状态。 破坏信任链后，安全启动不执行，提示并报警系统异常。	
判定条件： 在步骤（1）后，如果厂商提交的文档中未说明操作系统签名储存在安全区域内，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果被测车载端不具有利用硬件可信机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果被测车载端旁路安全启动后仍能进入正常工作状态，则该项目评测结果为“不符合要求”，评测结束； 在步骤（4）后，如果破坏信任链后，系统安全启动仍然执行，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。

5.3.2 多操作系统隔离

编号5.3.2.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.2.1 项，如车载端存在多个操作系统，须采用隔离机制，保证不同操作系统之间的安全防护。	
测试条件：提交安全技术方案设计相关文档，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端是否存在多个操作系统，操作系统间是否采用隔离机制； 步骤（2）：通过上层应用调用或数据处理等方式验证各操作系统资源是否隔离。	
预期结果： （1）文档中说明车载端是否存在多操作系统，并说明多操作系统之间采用的隔离机制； 各操作系统间资源进行隔离。	
判定条件： 在步骤（1）后，如果预置的多个操作系统之间未采用访问隔离机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果各操作系统间资源未进行隔离，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。	

5.3.3 操作系统加载应用程序

编号5.3.3.1	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.3.1 项，应提供安全机制，保证操作系统只能加载启动可信的车载端应用程序，能够验证应用的来源和完整性，避免运行恶意程序。	
测试条件：提交安全技术方案设计相关文档，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，验证车载端操作系统是否具有安全加载启动可信的车载端应用程序机制； 步骤（2）：安装可信的（授权的）车载端应用程序到被测车载端，检测车载端是否可以加载该应用； 步骤（3）：如果可信的（授权的）车载端应用程序修改后，安装到被测车载端，验证车载端是否可以验证应用的完整性； 步骤（4）：安装非授权的车载端应用程序到被测车载端，查看车载端是否可以提示并阻止非授权的车载端应用程序安装。	

预期结果： （1）车载端操作系统具有安全加载启动可信的车载端应用程序机制； （2）可以安装可信的（授权的）车载端应用程序； （3）车载端提示并阻止修改后可信的（授权的）车载端应用程序的安装，可以验证应用的完整性； （4）车载端可以提示并阻止非授权的车载端应用程序安装。
判定条件： 在步骤（1）后，如果被测车载端不具有加载启动可信应用程序的机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端不可以正常安装可信的（授权的）车载端应用程序，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果修改后可信的（授权的）车载端应用程序可以安装成功并未提示或阻止安装，则该项目评测结果为“不符合要求”，评测结束； 在步骤（4）后，如果非授权的车载端应用程序可以安装成功并未提示或阻止安装，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。

5.3.4 系统安全防护

编号5.3.4.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.4.1 项，应采用完整性校验手段（例如：基于哈希算法的数字摘要技术或数字签名技术），对关键代码或文件进行完整性保护。	
测试条件：完整性校验机制说明，提供修改关键代码或文件的权限，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，检查完整性校验机制（如：是否采用基于哈希算法的数字摘要技术或数字签名技术）； 步骤（2）：修改关键代码或文件，验证系统是否对其进行完整性校验。	
预期结果： （1）车载端系统具有完整性校验机制； （2）修改关键代码或文件，系统可以校验完整性，系统相应功能不可以正常工作。	
判定条件： 在步骤（1）后，如果厂商提交的文档未说明关键代码或文件的完整性防护机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果修改关键代码或文件后，系统未进行完整性校验，相应功能仍可以正常工作，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。	

编号5.3.4.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.4.2 项，车载端系统不存在后门，也不存在于“中国汽车行业漏洞共享平台（CAVD）“以及”国家信息安全漏洞共享平台（CNVD）”发布了6个月及以上的高危安全漏洞。系统应具有能够及时进行漏洞修复的方式。	
测试条件：漏洞修复方式说明，送检车载端系统处于正常工作状态	
测试步骤：	

步骤（1）：使用漏洞扫描工具，对车载终端进行测试，检查是否存在已知漏洞； 步骤（2）：如存在已发布漏洞检查是否有可以进行漏洞修复的方式。
预期结果： （1）系统不存在已发布的漏洞； （2）如存在漏洞可以及时启用漏洞修复方式进行漏洞修复。
判定条件： 在步骤（1）后，如果系统存在已发布的漏洞，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果系统不存在漏洞修复的方式，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。

5.3.5 资源访问控制

编号5.3.5.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.5.1 项，应采取适用于汽车各应用场景的告知和控制方式，实现当应用对系统敏感资源调用（例如：使用位置信息）时用户可知。并提供设置开关，供用户同意或者拒绝该项调用。	
测试条件：提供敏感资源列表，包括但不限于关键电子电气系统、用户隐私数据等。	
测试步骤： 步骤（1）：检测敏感资源列表中的功能，如通信功能、媒体功能等在被调用时，是否以适用于汽车各应用场景的告知用户，查看用户是否可以选择使用或者拒绝使用该功能； 步骤（2）：检测涉及用户敏感数据的文件资源在被访问时，是否以适用于汽车各应用场景的方式告知用户，查看用户是否可以选择访问或者拒绝访问相应资源； 步骤（3）：检测是否有设置开关，用户可以通过开关更改对敏感资源访问的设置。	
预期结果： （1）敏感资源列表中的功能，如通信功能、媒体功能等在被调用时，以适用于汽车各应用场景的告知和控制方式告知用户，并且用户可以选择使用或者拒绝使用该功能； （2）用户敏感数据的文件资源在被访问时，可以以适用于汽车各应用场景的方式告知用户，并且用户可以选择访问或者拒绝访问相应资源； （3）有设置开关，用户可以通过开关更改对敏感资源访问的设置。	
判定条件： 在步骤（1）后，如果功能被调用时用户未被告知，或者被告知但无法控制是否使用，或者告知方式不适合场景，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果文件资源被访问时用户未被告知，或者被告知但无法控制是否访问，或者告知方式不适合场景，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果没有设置开关，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。	

编号5.3.5.2	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.5.2 项，通过可信执行环境，为基于敏感数据的关键应用提供安全执行空间，控制对关键资源（例如：密钥、CAN 控制器）的访问，保护资源和数据的保密性和完整性，对抗非授权访问和篡改等多种攻击。	
测试条件：提供的软件层面可信执行环境的解决方案。	

测试步骤： 步骤（1）：检测是否通过可信执行环境解决方案对关键资源（例如：密钥、CAN 控制器）的访问设置访问控制； 步骤（2）：非授权访问和修改关键资源（例如：密钥、CAN 控制器）。
预期结果： （1）通过可信执行环境，为基于敏感数据的关键应用提供安全执行空间，对关键资源（例如：密钥、CAN 控制器）提供访问控制； （2）非授权用户不能对关键资源（例如：密钥、CAN 控制器）进行访问和修改。
判定条件： 在步骤（1）后，如果未为基于敏感数据的关键应用提供安全执行空间，或未对关键资源（例如：密钥、CAN 控制器）提供访问控制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果关键资源（例如：密钥、CAN 控制器）可以被非授权访问和篡改，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。

5.3.6 安全日志记录及审计控制

编号5.3.6.1	级别：2—4 级
技术要求：参照 T/CSAE 101-2018 第 5.3.6.1 项，支持对操作系统关键事件的日志功能，记录事件的时间、对象、描述和结果等。	
测试条件：日志上传及管理说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：模拟用户对车载端进行连续鉴别、存储耗尽、参数设置、网络访问等操作； 步骤（2）：使用系统调试工具，检查操作系统日志，是否有系统运行日志、报警日志、操作日志、应用软件运行日志等日志，记录事件发生的时间、对象、描述和结果等。	
预期结果： （1）操作系统可以记录系统运行日志、报警日志、操作日志、应用软件运行日志等关键事件的时间、对象、描述和结果等。	
判定条件： 在步骤（2）后，如果没有日志，或者有明显的要素缺失，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。	

编号5.3.6.2	级别：2—4 级
技术要求：参照 T/CSAE 101-2018 第 5.3.6.2 项，支持日志上传功能，上传时对云端进行认证；根据云端管理需求，采取安全的方式传输日志，确保数据的完整性和可认证性。	
测试条件：日志上传及管理说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看日志上传机制； 步骤（2）：触发日志上传机制，抓取日志上传时车载端与云端的通信数据；	

步骤（3）：查看车载端上传日志时是否对云端进行认证、是否采用云端要求的安全方式上传日志。
预期结果： （1）车载端具有日志上传功能，上传时对云端进行认证； （2）车载端采取云端管理需求中要求的安全方式上传日志，确保数据的完整性和可认证性。
判定条件： 在步骤（1）后，如果文档中未说明日志上传及管理机制，或者有明显的要素缺失，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果日志未上传，或者有明显的要素缺失；或者日志上传时对云端未进行认证；或者未按照云端管理需求中要求的安全方式上传，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。

编号5.3.6.3	级别：2—4级
技术要求：参照T/CSAE 101-2018 第5.3.6.3项，应采取访问控制机制，对日志读取写人的权限进行管理;应对日志存储进行安全防护。	
测试条件：日志管理说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端是否提供日志访问控制机制、是否采取日志存储的安全防护措施； 步骤（2）：使用授权用户读、写日志，验证该请求是否被允许； 步骤（3）：使用非授权用户读、写日志，查看该请求是否被拒绝。	
预期结果： （1）车载端具有日志上传功能，上传时对云端进行认证； （2）车载端采取云端管理需求中要求的安全方式上传日志，确保数据的完整性和可认证性。车载端采取日志访问控制机制、采取日志存储的安全防护措施； （3）车载端允许授权用户读、写日志；	
判定条件： 在步骤（1）后，如果文档中未说明日志访问控制机制、采取日志存储的安全防护措施，或者有明显的要素缺失，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）车载端拒绝授权用户读、写日志，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果日志允许非授权用户读、写日志，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。	

5.3.7 软件更新与固件更新

编号5.3.7.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.3.7.1 项，只接收在约定的工况（例如：非行驶状态）和车辆系统状态（例如：电瓶电量满足要求）下发起的车载端操作系统和应用等软件的更新请求，并在用户确认后执行更新操作。	
测试条件：提供软件与固件更新说明，提供软件升级包，送检安装车载端系统的车辆并处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端操作系统或应用更新机制；	

步骤（2）：模拟车辆处于非约定的工况（例如：行驶状态）或者非车辆系统状态（例如：电瓶电量不满足升级要求）时，发起车载端操作系统或应用等软件的更新请求；
步骤（3）：发起的车载端操作系统和应用等软件的更新请求，验证系统或应用是否启动升级；
步骤（4）：模拟车辆在约定的工况（例如：非行驶状态）和车辆系统状态（例如：电瓶电量满足要求）下发起的车载端操作系统和应用等软件的更新请求；
步骤（5）：验证系统是否提示升级，是否需人工选择确认后执行更新升级，选择拒绝后停止升级。

预期结果：

（1）厂商提交的文档中说明车载端操作系统或应用更新时车辆所需要具备的条件等内容；
（2）车辆处于非约定的工况（例如：行驶状态）或者非车辆系统状态（例如：电瓶电量不满足升级要求）时，车载端操作系统或应用等软件不能正常启动升级；
（3）车辆在约定的工况（例如：非行驶状态）和车辆系统状态（例如：电瓶电量满足要求）下发起的车载端操作系统和应用等软件的更新请求，在用户确认执行后更新升级，选择拒绝后停止升级。

判定条件：

在步骤（1）后，如果文档中未说明车载端操作系统或应用更新时车辆所需要具备的条件等更新机制的内容，则该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，如果系统和应用自动升级，则该项目评测结果为“不符合要求”，评测结束；
在步骤（5）后，如果未经用户确认即开始更新或者未按人工选择执行，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。

编号5.3.7.2	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.3.7.2 项，软件更新时，应能够对提供更新软件包的来源进行鉴别，并对接收到的更新文件进行完整性校验。软件升级应不影响用户设置和用户数据。系统应具有备份和恢复能力，能够在软件更新发生异常时进行必要的操作，避免更新失败导致系统失效。系统应对连续升级行为进行记录，设定一段时间内升级尝试次数上限，避免通过车载端升级尝试对车辆资源进行过度消耗。

测试条件：提供软件与固件更新说明，提供软件升级包，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端软件更新机制，是否说明更新过程异常处理情况、一段时间内升级尝试次数上限等内容；
步骤（2）：修改厂家提供的升级包并重新打包签名，发起更新，检测是否能执行升级；
步骤（3）：使用厂家提供的软件升级包，发起更新，检查车载端是否在更新前提供备份可选项；
步骤（4）：在更新过程中，采取措施（例如：断电）中断或取消更新，检查车载端状态；
步骤（5）：使用厂家提供的软件升级包，发起更新，更新结束后查看用户设置和用户数据是否丢失或被更改；
步骤（6）：使用厂家提供的软件升级包，在一段时间内多次发起更新，查看车载端是否对连续升级行为进行记录，并且是否设置一段时间内升级尝试次数上限。

预期结果：

（1）厂商提交的文档中说明车载端软件更新机制，包括更新过程异常处理情况、一段时间内升级尝试次数上限等内容；
（2）系统阻止升级并提示报警；
（3）车载端在更新前提供备份可选项；
（4）在更新过程中，采取措施（例如：断电）中断或取消更新后，车载端可以恢复正常工作，并且回滚到升级前版本；
（5）软件升级后原有用户设置和用户数据未被更改；

在一段时间内多次发起更新时，车载端记录连续升级行为，并且设置一段时间内升级尝试次数上限，达到该上限值时进行报警提示或停止升级，恢复之前版本。
判定条件： 在步骤（1）后，如果文档中未说明车载端软件更新机制，或未说明升级过程中异常处理机制，或未设置一段时间内升级尝试次数上限等内容，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果系统仍然能够更新，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果系统未能提供备份选项，则该项目评测结果为“不符合要求”，评测结束； 在步骤（4）后，如果系统未能回退到更新前的正常工作状态，则该项目评测结果为“不符合要求”，评测结束； 在步骤（5）后，如果用户设置和用户数据丢失或被更改，则该项目评测结果为“不符合要求”，评测结束； 在步骤（6）后，如果车载端未记录连续升级行为，或未设置一段时间内升级尝试次数上限，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。

编号5.3.7.3	级别：3—4 级
技术要求：参照 T/CSAE 101-2018 第 5.3.7.3 项，车载端在向其他车内系统或设备（例如：ECU）传输更新文件和更新命令的时候，应能够及时声明自己的身份和权限，供车内系统或设备进行认证;只有认证通过后，操作才可以继续执行。	
测试条件：提供软件与固件更新说明，提供车载端向其他车内系统或设备需要传输更新文件和更新命令的内容和权限（例如：ECU 固件升级包），送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端在向其他车内系统或设备（例如：ECU）传输更新文件和更新命令的认证机制，以及权限说明； 步骤（2）：修改由车载端转发的 ECU 固件升级包的内容，对 ECU 发起升级请求，检测是否能够执行 ECU 更新操作。	
预期结果： （1）厂商提交的文档中说明车载端在向其他车内系统或设备（例如：ECU）传输更新文件和更新命令的认证机制和权限； （2）车载端在向其他车内系统或设备（例如：ECU）传输更新文件和更新命令的时候，提供身份和权限校验，修改由车载端转发的ECU固件升级包内容，对ECU发起升级请求，ECU拒绝按照该升级包升级。	
判定条件： 在步骤（1）后，如果厂商提交的文档中未说明车载端在向其他车内系统或设备（例如：ECU）传输更新文件和更新命令的认证机制和权限，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果ECU使用该升级包升级并刷新仍然能够成功，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。	

5.3.8 介质接口安全

编号5.3.8.1	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.3.8.1 项，车载端不应存在未经声明的外围介质（例如：	

CD/DVD、SD卡、USB）接口。

测试条件：车载端介质接口说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端声明的外围接口，检查车载端实际与声明的一致性；
步骤（2）：使用声明中的相关介质访问接口，是否能且仅能实现声明的功能。

预期结果：

（1）车载端实际外围介质接口与声明的一致；
（2）使用声明中的相关介质访问接口可以实现声明的功能，不可以实现声明以外的功能。

判定条件：

在步骤（1）后，如果发现未经声明的外围接口，则该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果发现不能实现声明的功能，或者具有未经声明的功能，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。

编号5.3.8.2　　级别：1—4级

技术要求：参照T/CSAE 101-2018 第5.3.8.2项，车载端应定义通过外围接口接入的存储介质上的文件类型和权限，并限制通过介质接口对车载端进行的操作类型。

测试条件：车载端介质接口说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端是否定义通过外围接口接入的存储介质上的文件类型和权限，并说明通过介质接口对车载端进行的操作类型的限制；
步骤（2）：检测车载端是否在要求的权限范围内对外围接口接入的存储介质上允许操作的文件类型进行操作。

预期结果：

（1）厂商提交的文档定义了通过外围接口接入的存储介质上的文件类型和权限，并限制通过介质接口对车载端进行的操作类型；
（2）车载端在要求的权限范围内对外围接口接入的存储介质上允许操作的文件类型进行操作。

判定条件：

在步骤（1）后，如果未经说明外围接口接入的存储介质上的文件类型和权限，或未限制通过介质接口对车载端进行的操作类型，则该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果车载端可以对通过外围接口接入的存储介质上的非法文件进行操作，或未按照权限要求进行操作，则该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，车载端存在接口漏洞，可以通过非授权的端口对车载端进行操作，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”。

编号5.3.8.3　　级别：2—4级

技术要求：参照T/CSAE 101-2018 第5.3.8.3项，应使用必要的方法，对可能修改系统配置或者运行状态的文件进行检测，并根据检测结果告警及处置。

测试条件：修改系统配置或者运行状态的文件检测机制说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端对可能修改系统配置或者运行状态的文件检测机制，是否采取措施，并且是否根据检查结果告警及处置；

步骤（2）：使用系统调试工具，在车载端运行修改系统配置或运行状态的文件，查看车载端是否对其进行检测，是否告警，是否对其进行处置，如阻止文件运行等。
预期结果： （1）厂商提交的文档中说明车载端采取检测措施，对可能修改系统配置或者运行状态的文件进行检测，并且根据检查结果告警及处置； （2）在车载端运行修改系统配置或运行状态的文件时，车载端告警并阻止文件运行。
判定条件： 在步骤（1）后，如果厂商提交的文档中未说明车载端对可能修改系统配置或者运行状态的文件的检测机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端可以运行修改系统配置或运行状态的文件，或未报警阻止，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”

5.4 应用软件安全

5.4.1 应用软件安全基本要求

编号5.4.1.1	级别：2—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.1.1 项，通用应用软件不应存在后门，也不存在于“中国汽车行业漏洞共享平台（CAVD）”以及“国家信息安全漏洞共享平台（CNVD）”发布了 6 个月及以上的高危安全漏洞。	
测试条件：提交应用软件产品质量测试报告，送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：使用漏洞扫描工具，对应用软件进行分析，是否存在后门，是否存在已发布了6个月以上的高危安全漏洞； 步骤（2）：对工具检测结果进行人工验证。	
预期结果： （1）应用软件不应存在后门，也不存在已发布了6个月以上的高危安全漏洞，或对已知漏洞采用补丁机制。	
判定条件： 在步骤（2）后，如果应用软件存在后门，或存在已发布了6个月以上的高危安全漏洞，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	

编号5.4.1.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.1.2 项，应用软件不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。	
测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：启动应用软件，使用抓包工具，对应用软件的通信数据进行采集；	

步骤（2）：关闭应用软件，保持送检产品的网络连接，使用抓包工具，对应用软件对外通信流量进行静默状态下的数据采集； 步骤（3）：对工具检测结果进行人工分析。
预期结果： （1）应用软件不含有非授权收集或泄露用户信息、非法数据外传等恶意行为。
判定条件： 在步骤（3）后，如果经过人工分析存在未经用户授权的数据收集和传输，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。

编号5.4.1.3	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.1.3 项，应用不以明文形式存储用户敏感信息（例如：用户口令、证件号、交易口令、私钥）。	
测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：验证应用是否以明文形式存储用户敏感信息（例如：用户口令、证件号、交易口令、私钥）。	
预期结果： （1）应用不以明文形式存储用户敏感信息（例如：用户口令、证件号、交易口令、私钥）。	
判定条件： 在步骤（1）后，如果发现应用明文形式存储用户敏感信息（例如：用户口令、证件号、交易口令、私钥），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。	

编号5.4.1.4	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.1.4 项，应用软件应使用安全机制（例如：混淆、加壳），对抗针对应用的逆向分析。	
测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：使用反编译工具反编译被测应用软件，查看其是否使用安全机制，例如混淆、加壳等； 步骤（2）：尝试逆向被测应用软件，查看其是否可以对被测应用软件逆向分析。	
预期结果： （1）应用软件应使用混淆、加壳等安全机制； （2）被测应用软件可以防止逆向分析。	
判定条件： 在步骤（1）后，如果被测应用软件未使用混淆或加壳等安全措施，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果被测应用软件可以被逆向分析，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。	

5.4.2 应用软件签名认证机制

编号5.4.2.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.2.1 项，应用软件应采用代码签名认证机制，且代码签名机制符合相关标准要求。	
测试条件：车载端应用软件说明，送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看是否说明应用软件采用签名认证机制； 步骤（2）：验证应用软件签名认证机制，分析签名内容，并对签名进行合规性检查。	
预期结果： （1）检查厂商提交的文档说明应用软件采用签名认证机制； （2）应用软件应采用签名认证机制，且代码签名机制符合相关标准要求。	
判定条件： 在步骤（1）后，如果厂商提交的文档未说明应用软件采用签名认证机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果应用软件未采用签名认证机制，或者存在与相关标准不符合之处，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。	

5.4.3 应用软件运行要求

编号5.4.3.1	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.3.1 项，关键应用程序在启动时应执行自检，检查程序运行时所必须的条件，确保程序自身和所处运行环境的安全性。	
测试条件：提供车载端内置关键应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看应用程序启动所需检查的配置文件和环境参数； 步骤（2）：对其中的文件或参数进行修改，使其不满足应用启动条件，检测应用是否仍然能正常启动。	
预期结果： （1）应用程序启动所需配置文件和环境参数不满足应用启动条件时，应用不能正常启动。	
判定条件： 在步骤（2）后，如果应用仍然能正常启动，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。	

编号5.4.3.2	级别：2—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.3.2 项，应用软件运行期间，应具备运行验证及编译混淆能力，防止运行数据被非法分析或代码被非法执行。	
测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤：	

步骤（1）：检测软件运行期间是否采用编译混淆等措施防止运行数据被非法分析或代码被非法执行；
步骤（2）：修改源代码并执行，查看应用是否运行。

预期结果：
（1）应用软件具备运行验证和编译混淆能力；
（2）阻止修改后的源代码执行。

判定条件：
在步骤（1）后，可以获得源代码并且源代码未被编译混淆，可以分析代码逻辑功能、函数及变量关系，则该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果修改源代码后程序可以运行，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。

编号5.4.3.3	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.4.3.3 项，使用安全机制，防止和检测应用软件之间不必要的访问，避免数据泄漏、非法提权等安全问题。

测试条件：车载端应用软件说明，送检产品明确内置应用列表送检安装应用软件的车载端系统处于正常工作状态。

测试步骤：
步骤（1）：检查厂商提交的文档，查看软件是否采用安全机制来防止和检测应用软件之间不必要的访问，避免数据泄露、非法提权等内容；
步骤（2）：检查应用是否设置防止备份的防护，检测是否可以提取访问数据权限；
步骤（3）：尝试访问其他应用的数据和文件，检测是否可以访问成功。

预期结果：
（1）厂商提交的文档说明软件采用安全机制来防止和检测应用软件之间不必要的访问，避免数据泄露、非法提权等内容；
（2）应用设置防止备份的防护，设置提取访问数据权限；
（3）阻止访问其他应用的数据和文件。

判定条件：
在步骤（1）后，文档中未说明防止和检测应用软件之间不必要的访问的安全机制，则该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果应用未设置防止备份的防护，或可以提取访问数据权限，则该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，如果可以访问其他应用的数据或文件，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。

编号5.4.3.4	级别：2—4级

技术要求：参照 T/CSAE 101-2018 第 5.4.3.4 项，具备识别、阻断恶意软件的能力，隔绝已经被感染的文件，拒绝软件的恶意访问。

测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。

测试步骤：
步骤（1）：构造恶意软件，尝试在车载端安装，检测是否可以识别并阻断恶意软件的安装。

预期结果： （1）车载端可以识别并阻断恶意软件的安装。
判定条件： 在步骤（1）后，如果可以安装恶意软件，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。

5.4.4 安全审计要求

编号5.4.4.1	级别 2—4 级
技术要求：参照 T/CSAE 101-2018 第 5.4.4.1 项，应用程序应具备记录应用状态及使用情况的日志功能，并支持集中管理。	
测试条件：送检产品明确内置应用列表，送检安装应用软件的车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查应用日志，查看是否记录应用状态及使用情况等信息； 步骤（2）：检测是否支持日志集中管理。	
预期结果： （1）应用程序具备记录应用状态及使用情况的日志功能； （2）支持日志集中管理。	
判定条件： 在步骤（1）后，如果没有日志，或者有明显的要素缺失，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果没有日志集中管理功能，则该项目评测结果为“不符合要求”； 否则，该项目评测结果为“未见异常”，评测结束。	

5.4.5 应用流程安全性要求

编号5.4.5.1	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.4.5.1 项，应用程序与服务器之间的交互，应使用可靠的安全通信协议（例如：TLS1.2）。	
测试条件：应用程序与服务器交互说明，送检安装应用软件的车载端系统处于正常工作状态，应用程序与服务器通信正常。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看是否说明应用程序与服务器之间的交互时通信协议； 步骤（2）：在测试环境中启动应用程序，触发应用程序访问服务器； 步骤（3）：使用抓包工具抓取通信数据，检查应用是否使用了可靠的安全通信协议。	
预期结果： （1）厂商提交的文档中说明应用程序与服务器之间的交互时通信协议； （2）应用程序与服务器之间的交互，使用可靠的安全通信协议。	
判定条件： 在步骤（1）后，如果未说明应用程序与服务器之间的交互时通信协议，则该项目评测结果为“不符合要求”，评测结束；	

在步骤（3）后，如果未使用安全通信协议，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。

编号5.4.5.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.4.5.2 项，应用程序访问服务器需有双向认证机制。	
测试条件：应用程序与服务器交互说明，送检安装应用软件的车载端系统处于正常工作状态，应用程序与服务器通信正常。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看是否说明应用程序与服务器交互时双向认证机制； 步骤（2）：在测试环境中启动应用程序，触发应用程序访问服务器； 步骤（3）：使用抓包工具抓取通信数据，检查应用程序访问服务器时双方是否进行双向认证。	
预期结果： （1）厂商提交的文档中说明应用程序与服务器交互时双向认证机制； （2）应用程序访问服务器时双方进行双向认证。	
判定条件： 在步骤（1）后，如果未说明应用程序与服务器之间的交互时双向认证机制，则该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果未进行双向认证，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。	

5.5 对内通信安全

5.5.1 对车内子系统访问的安全控制

编号5.5.1.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.5.1.1 项，使用必要的技术手段，对包括车载端在内的车内各电子电气系统进行子系统或者域的划分。子系统或者域应有不同的信息安全等级。	
测试条件：提供车载端安全级别相关文档。	
测试步骤： 步骤（1）：检查安全策略及子系统或者域划分相关文档，检查子系统或者域划分的依据，子系统或者域是否有不同的信息安全等级。	
预期结果： （1）文档中说明包括车载端在内的车内各电子电气系统进行子系统或者域的划分依据，信息安全等级说明。	
判定条件： 在步骤（1）后，如果文档中未能说明安全域划分的依据，等级划分不明晰，技术实现机制不健全，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。	

编号5.5.1.2	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.5.1.2 项，建立跨子系统或者域间通信的安全访问策略，车载端与高安全级别的子系统（例如：动力系统）之间应采取访问控制措施。并通过与功能逻辑设计的配合，避免由于车载端的信息安全问题造成该类子系统功能的错误或异常。
测试条件：提供安全防护方案相关文档。
测试步骤： 步骤（1）：检查安全防护方案相关文档，查看跨子系统或者域间的通信是否设置安全访问策略，车载端与高安全级别的子系统（例如：动力系统）之间通信是否采取访问控制措施； 步骤（2）：根据访问策略内容，检测车载端是否可以访问高安全级别的子系统（例如：动力系统）； 步骤（3）：根据访问策略内容，检测车载端是否可以访问高安全级别的子系统（例如：动力系统）中拒绝访问的资源，查看是否可以访问。
预期结果： （1）跨子系统或者域间的通信设置安全访问策略，车载端与高安全级别的子系统（例如：动力系统）之间通信采取访问控制措施； （2）车载端可以访问高安全级别的子系统（例如：动力系统）在访问策略中允许访问的资源； （3）高安全级别的子系统（例如：动力系统）拒绝车载端非授权访问在访问策略中拒绝访问的资源。
判定条件： 在步骤（1）后，如果跨子系统或者域间的通信未设置安全访问策略，车载端与高安全级别的子系统（例如：动力系统）之间通信未采取访问控制措施，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端被拒绝访问高安全级别的子系统（例如：动力系统）在访问策略中允许访问的资源，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果高安全级别的子系统（例如：动力系统）允许车载端非授权访问在访问策略中拒绝访问的资源，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。

编号5.5.1.3	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.5.1.3 项，车载端应在与车内各电子电气系统的通信数据上加载身份标识，供其他车内电子电气系统验证。同时车载终端应具有验证所接收到的通信数据的发送方身份的能力。	
测试条件：正常工作的整车。	
测试步骤： 步骤（1）：使用车内网络通信数据检测工具，读取车载端与车内各电子电气系统通信数据，识别身份标识； 步骤（2）：伪造身份标识，或者重放已获取的身份标识并构造数据包，检测接收系统是否能验证数据包身份。	
预期结果： （1）车载端发给车内各电子电气系统通信数据加载身份标识； （2）车载端可以验证接收到的通信数据的发送方身份，可以识别伪造的身份或者重放的通信数据并。	
判定条件： 在步骤（1）后，如果车载端发给车内各电子电气系统通信数据未加载身份标识，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未对通信数据的发送方身份进行验证，或未识别伪造的身份或者重放的通信数据，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。

5.5.2 对车内部通信可靠性和可用性的安全防护

编号5.5.2.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.5.2.1 项，车载端具备冗余备份和重发机制，保证对电子电气系统发送重要数据时（例如：ECU 固件升级包），传输数据的可靠性。	
测试条件：车载端与车内通信机制说明，正常工作的整车。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看是否说明车载端对电子电气系统发送重要数据时（例如：ECU固件升级软件包）具备冗余备份和重发机制； 步骤（2）：选取目标电子电气系统，发送重要数据（例如ECU固件升级软件包），中断数据传输，验证车载端是否对重要数据进行冗余备份，是否可以重传； 步骤（3）：验证数据传输出现问题时，系统是否有相应的提示信息，是否有效处理被破坏的数据包并保持系统按照预期状态运行。	
预期结果： （1）厂商提交的文档说明车载端对电子电气系统发送重要数据时（例如：ECU固件升级软件包）具备冗余备份和重发机制； （2）车载端对电子电气系统发送重要数据时（例如：ECU固件升级软件包），中断数据传输后，车载端对重要数据进行冗余备份，可以重传； （3）数据传输出现问题时，车载端有相应的提示信息，可以有效处理被破坏的数据包并保持系统按照预期状态运行。	
判定条件： 在步骤（1）后，如果文档没有说明冗余和重传机制，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果系统没有冗余和重传机制，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果接收系统不能发现并正确处理数据传输异常，或者处理异常后，系统为非预期状态，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。	

编号5.5.2.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.5.2.2 项，车载端向车内电子电气系统发送数据和转发数据时，应采用相应技术避免大量集中发送数据包导致的总线拥塞和拒绝服务。	
测试条件：车载端与车内通信机制说明，正常工作的整车。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端是否应采用相应技术避免发送大量数据攻击包导致的总线拥塞和拒绝服务； 步骤（2）：命令车载端向车内电子电气系统高频率、发送大量数据包，实施拒绝服务攻击，使用车内网络通信数据检测工具监测总线状态和电子电气系统工作状态。	

预期结果： （1）车载端应采用相应技术避免发送大量数据攻击包导致的总线拥塞和拒绝服务； （2）当车载端向车内电子电气系统发送或转发的数据包的频率和数量超出正常要求时，车载端做出报警提示并阻止高频率、大量发送数据包，避免总线拥塞和拒绝服务。
判定条件： 在步骤（1）后，文档中未说明车载端采用相应技术避免发送大量数据攻击包导致的总线拥塞和拒绝服务，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果出现总线拥塞，或者电子电气系统异常，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。

编号5.5.2.3	级别：2—4级
技术要求：参照 T/CSAE 101-2018 第 5.5.2.3 项，车载端应建立监测模块，实时监测向车内电子电气系统发送数据的数量与质量，对于异常情况应及时发现并告警。	
测试条件：车载端与车内通信机制说明，正常工作的整车。	
测试步骤： 步骤（1）：向车内电子电气系统实施拒绝服务攻击，使用车内网络通信数据检测工具监测总线状态和电子电气系统工作状态； 步骤（2）：在攻击期间发送正常数据通信包，检测相应电子电气系统是否能正常接收并处理。	
预期结果： （1）车载端实时监测向车内电子电气系统发送数据的数量与质量，当向车内电子电气系统发送的数据频率和内容不符合要求时，车载端告警并拒绝接收超过正常要求的数据； （2）在攻击期间发送正常数据通信包，相应电子电气系统可以正常接收并处理。	
判定条件： 在步骤（1）后，如果出现总线拥塞，或者电子电气系统异常，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果接收系统不能正常接收处理正常数据包，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。	

5.6 对外通信安全

5.6.1 蜂窝网络通信安全

编号5.6.1.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.1.1 项，车载端应使用安全机制，识别伪基站，确保接入真实可靠的蜂窝网络。	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：检查厂商提供的文档，查看车载端接入蜂窝网络时是否使用安全机制； 步骤（2）：接入网络，检测车载端是否对接入网有认证机制；	

步骤（3）：设立伪基站，检测是否可以识别伪基站等非真实网络，是否影响车载端接入正常的蜂窝网络。

预期结果：

（1）车载端接入蜂窝网络时使用安全机制；
（2）车载端对接入网进行认证；
（3）车载端可以识别伪基站，在附件有伪基站的情况下仍可以接入正常的蜂窝网络。

判定条件：

在步骤（1）后，如果未使用安全机制，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果车载端未进行认证，该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，如果车载端连接到伪基站，或未能接入正常的蜂窝网络，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。

编号5.6.1.2　　级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.6.1.2 项，车载端与核心业务平台的通信应采用专用网络或者虚拟专用网络通信，与公网隔离。

测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端与核心业务平台的通信需求，采用专用网络或者虚拟专用网络通信，与公网隔离；
步骤（2）：在车载端连接核心业务平台，验证通信网络类型是否为专用网络或者虚拟专用网络通信，是否与公网隔离。

预期结果：

（1）厂商提交的文档中要求车载端与核心业务平台的通信采用专用网络或者虚拟专用网络通信，与公网隔离；
（2）车载端连接核心业务平台时采用专用网络或者虚拟专用网络通信，与公网隔离。

判定条件：

在步骤（1）后，如果未说明车载端与核心业务平台的通信网络要求，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果未使用专用网络或者虚拟专用网络通信，未与公网隔离，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。

编号5.6.1.3　　级别：2—4级

技术要求：参照 T/CSAE 101-2018 第 5.6.1.3 项，车载端应能够识别来自蜂窝网络的非法连接请求，过滤恶意数据包。

测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端对蜂窝网络连接请求的确认机制；
步骤（2）：经蜂窝网络发起非授权连接请求，检测是否能够连接成功；
步骤（3）：经蜂窝网络向车载端发送恶意数据包，检测是否能够过滤。

预期结果：

（1）厂商提交的文档中说明车载端对蜂窝网络连接请求的确认机制；
（2）车载端可以识别来自蜂窝网络的非法连接请求，并阻止非法连接；
（3）车载端可以过滤恶意数据包。

判定条件：

在步骤（1）后，如果未说明车载端对蜂窝网络连接请求的确认机制，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果连接成功，该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，如果不能过滤恶意数据包，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。

编号5.6.1.4	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.6.1.4 项，车载端应采取技术措施，禁用业务所不需要的蜂窝网络通信功能（例如：彩信）。

测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端禁用蜂窝网络通信功能列表；
步骤（2）：根据被禁用功能列表，检测被禁用功能是否已关闭开发接口。

预期结果：

（1）厂商提交的文档中说明车载端禁用蜂窝网络通信功能列表；
（2）车载端禁用业务所不需要的蜂窝网络通信功能（例如：彩信），被禁用功能关闭开发接口。

判定条件：

在步骤（1）后，如果文档未说明车载端禁用蜂窝网络通信功能，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果被禁用功能没有关闭开发接口，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。

编号5.6.1.5	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.6.1.5 项，通过蜂窝网络传送的针对车载端的关键操作（例如：用户号码写入），应采用强验证手段，确保只有授权的主体可以实施相应的操作。

测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交的文档，查看车载端是否对通过蜂窝网络传送的关键操作（例如：用户号码写入）采用强验证手段；
步骤（2）：伪造身份认证凭据，发起关键操作，验证认证机制的有效性。

预期结果：

（1）厂商提交的文档中说明车载端对通过蜂窝网络传送的关键操作（例如：用户号码写入）采用强验证手段；
（2）车载端对通过蜂窝网络传送的关键操作（例如：用户号码写入）进行验证，只有授权的主体可以实施相应的操作。

判定条件： 在步骤（1）后，如果文档未说明对通过蜂窝网络传送的关键操作（例如：用户号码写入）采用强验证手段，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果伪造身份仍然能够执行关键操作，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。

编号5.6.1.6	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.1.6 项，应根据不同应用的重要性划分优先级，保障关键业务（例如：监管平台信息采集）具有网络通信的优先使用权。	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看不同应用提供根据业务的重要程度和对时效性的要求进行的优先级划分方案； 步骤（2）：在低优先级应用使用网络的情况下，尝试发送高优先级数据，检测是否按照优先级使用网络。	
预期结果： （1）厂商提交的文档中说明不同应用提供根据业务的重要程度和对时效性的要求进行的优先级划分方案； （2）高优先级数据优先使用网络。	
判定条件： 在步骤（1）后，如果未说明根据不同应用的重要性划分优先级，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果没有按照优先顺序使用网络，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。	

5.6.2 车车通信、车路协同通信安全

编号5.6.2.1	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.2.1 项，车载端具备保证唯一性的身份标识，并可以对所连接的通信节点（例如：路侧设施，请求通信连接的车辆）进行身份验证，且该身份标识不应泄露用户隐私。	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端是否具有对外通信时唯一性的身份标识，是否说明与通信节点连接时身份验证机制； 步骤（2）：发起车载端与通信节点（例如：路侧设施，请求通信连接的车辆）连接，用工具获取通信数据，检测车载端是否具有唯一性的身份标识、检测车载端和通信节点是否进行身份验证； 步骤（3）：查看车载端的身份标识是否泄漏用户隐私。否按照优先级使用网络。	

预期结果： （1）厂商提交的文档中说明车载端对外通信时唯一性的身份标识，说明与通信节点连接时身份验证机制； （2）车载端具备保证唯一性的身份标识，并可以对所连接的通信节点（例如：路侧设施，请求通信连接的车辆）进行身份验证； （3）车载端的身份标识未泄露用户隐私。
判定条件： 在步骤（1）后，如果未说明车载端对外通信时唯一性的身份标识，或未说明与通信节点连接时身份验证机制，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未对通信节点进行身份验证，或通信节点未对车载端进行身份验证，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果车载端的身份标识包含用户隐私，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。

编号5.6.2.2	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.2.2 项，车载端具备保证唯一性的身份标识，并可以对所连接的通信节点（例如：路侧设施，请求通信连接的车辆）进行身份验证，且该身份标识不应泄露用户隐私。	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端是否支持数字证书或完备的密钥生成机制和管理机制，用于身份认证、通信加密和完整性保护； 步骤（2）：验证车载端的数字证书及密钥生成功能，密钥是否可以正常生成，证书是否可以正常下发，可以通过下发的证书与密钥与通信节点进行正常通信。	
预期结果： （1）厂商提交的文档中说明车载端支持数字证书或完备的密钥生成机制和管理机制，用于身份认证、通信加密和完整性保护； （2）验证车载端的数字证书及密钥生成功能，密钥可以正常生成，证书可以正常下发，可以通过下发的证书与密钥与通信节点进行正常通信。	
判定条件： 在步骤（1）后，如果未说明车载端支持数字证书或完备的密钥生成机制和管理机制，或未用于身份认证、通信加密和完整性保护，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果密钥不可以正常生成，或证书不能正常下发，或不能通过下发的证书与密钥与通信节点进行正常通信，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。	

5.6.3 短距离无线连接安全

编号5.6.3.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.3.1 项，车载端应具备用户手动打开、关闭短距离无线连接的能力。	

测试条件：送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。
测试步骤： 步骤（1）：检查车载端是否提供短距离无线连接开启/关闭的选项； 步骤（2）：如果车载端提供上述选项，则使用该选项开启短距离无线连接，验证是否可以连接成功； 步骤（3）：使用开关关闭短距离无线连接，验证是否断开连接。
预期结果： （1）车载端提供关闭短距离无线连接的开启/关闭选项； （2）用户可以手动打开短距离无线连接； （3）用户可以手动关闭短距离无线连接。
判定条件： 在步骤（1）后，在车载端上未找到开启/关闭短距离无线连接接口的开关，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，未成功开启车载端的短距离无线连接，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，未成功关闭车载端的短距离无线连接，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。

编号5.6.3.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.3.2 项，已建立的短距离无线连接，应在相应的输出设备上有明确的连接状态显示。	
测试条件：送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：车载端建立无线连接； 步骤（2）：查看车载端是否有明确显示连接状态。	
预期结果： （1）车载端建立无线连接后，车载端有明确的连接状态显示。	
判定条件： 在步骤（1）后，如果车载端没有明确显示连接，则该项目评测结果为“不符合要求”，测评结束； 否则，该项目评测结果为“未见异常”，测评结束。	

编号5.6.3.3	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.6.3.3 项，车载端的应用调用短距离无线连接功能时，车载端能够明示用户，并提供配置能力和符合场景的配置方式。	
测试条件：提供使用无线连接的应用列表，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：打开使用无线连接的应用； 步骤（2）：查看车载端是否提示用户该应用将使用无线连接，并且用户可以选择同意或者拒绝使用。	
预期结果： （1）车载端提示用户该应用将使用无线连接，并且用户可以选择同意或者拒绝使用。	

判定条件：
在步骤（2）后，如果没有提示，或者有提示但是未提供配置能力和 符合场景的配置方式；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。

编号5.6.3.4	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.6.3.4 项，车载端只在特定工况下接受外来通信连接请求（例如：蓝牙连接配对请求）以保证车辆安全，并对发起连接请求的设备进行认证授权。需要用户操作的步骤，应向用户提供符合应用场景的处理方式。	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：检查厂商提交的文档，查看车载端接受的通信连接请求的功能说明及接受请求的状态； 步骤（2）：测试终端发起对车载端需要用户操作的连接请求（例如：蓝牙连接配对请求），查看车载端是否提示，是否向用户提供符合应用场景的处理方式（例如：允许或拒绝配对）； 步骤（3）：允许连接时，检测车载端是否对发起连接请求的设备进行认证授权。	
预期结果： （1）厂商提交的文档中说明车载端接受的通信连接请求的功能说明及接受请求的状态； （2）车载端在允许的工况下接受外来通信连接请求（例如：蓝牙连接配对请求），并向用户提供符合应用场景的处理方式； （3）车载端对发起连接请求的设备进行认证授权。	
判定条件： 在步骤（1）后，如果未说明车载端接受的通信连接请求的功能，或未说明接受请求的状态，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端在说明不允许的工况下接受外来通信连接请求，或不提示连接请求，或在需要用户操作时未向用户提供符合应用场景的处理方式，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果车载端未对发起连接请求的设备进行认证授权，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。	

编号5.6.3.5	级别：1—4 级
技术要求：参照 T/CSAE 101-2018 第 5.6.3.5 项，车载端发起对外连接时，应对外部设备进行认证，并尽量启用通信协议所支持的安全模式进行通信。注：短距离无线连接包括但不限于 Wi-Fi、蓝牙、ZigBee	
测试条件：车载端对外通信安全说明，送检车载端系统处于正常工作状态，连接对象及网络处于正常状态。	
测试步骤： 步骤（1）：检查厂商提供的文档，查看车载端连接外部设备时是否使用安全机制； 步骤（2）：发起车载端与外部设备连接（例如：与用户移动通信终端的连接），用工具获取通信数据，验证车载端是否对外部设备进行认证，并启用通信协议所支持的安全模式进行通信。	

预期结果： （1）车载端连接外部设备时使用身份认证、安全通信协议和通信模式等安全机制； （2）车载端对外部设备进行认证，并启用通信协议所支持的安全模式进行通信。
判定条件： 在步骤（1）后，如果未使用身份认证、安全通信协议和通信模式等安全机制，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未对外部设备进行认证，或未启用通信协议所支持的安全模式进行通信，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。 注：短距离无线连接包括但不限于 Wi-Fi、蓝牙、ZigBee。

5.7 用户数据安全

5.7.1 数据安全采集

编号5.7.1.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.1.1 项，车载端所采集的与用户身份、位置信息等相关的敏感数据，应通过显式的方式告知用户并获得用户确认，应说明数据采集所依据的国家法律法规或者业务需求。	
测试条件：提供用户数据采集说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检测车载端在采集与用户身份、位置信息等相关的敏感数据时是否通过显式的方式通知用户，是否在用户确认后再采集用户数据； 步骤（2）：检查采集数据时是否说明相关采集内容、法律依据、业务需求、数据用途和数据扩散范围等内容。	
预期结果： （1）车载端在采集与用户身份、位置信息等相关的敏感数据时，通过显式的方式告知用户，在并获得用户确认后再采集用户数据； （2）车载端在采集数据时说明相关采集内容、法律依据、业务需求、数据用途和数据扩散范围等内容。	
判定条件： 在步骤（1）后，如果系统无告知，或者告知方式隐蔽，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果系统的告知说明里，缺少对采集内容、法律依据、业务需求、数据用途和数据扩散范围等任一方面的描述，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。	

编号5.7.1.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.1.2 项，车载端对用户数据的采集应在提供相应服务的同时进行。若出于业务需要而必须事先采集相关数据，应向用户明示事先采集的目的和范围，并且只有在用户同意的情况下方可继续。	
测试条件：提供用户数据采集说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查车载端对用户数据的采集是否在提供相应服务的同时进行；	

步骤（2）：对事先采集相关数据，检查车载端是否向用户明示事先采集的目的和范围，用户是否可以选择同意或者不同意；
步骤（3）：用户选择不同意，是否不再进行数据采集，并且已采集数据自动删除，不上传。

预期结果：

（1）车载端对用户数据的采集在提供相应服务的同时进行；
（2）若出于业务需要而必须事先采集相关数据，车载端向用户明示事先采集的目的和范围，并且用户可以选择同意或者不同意；
（3）用户选择不同意时，车载端不再进行数据采集，并且已采集数据自动删除，不上传。

判定条件：

在步骤（1）后，如果未在提供相应服务的同时采集用户数据，或未告知用户就进行事先采集数据行为，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果车载端未向用户明示事先采集的目的和范围，或车载端事先采集数据时不提供用户选择，该项目评测结果为“不符合要求”，评测结束；
在步骤（3）后，如果车载端未按用户选择执行数据采集，或用户在拒绝采集时已采集数据未删除或继续上传，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。

编号5.7.1.3　　级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.7.1.3 项，车载端采集用户使用行为等用户数据时，应提示用户并向用户提供关闭数据采集的功能。在执行此类操作前，应首先对用户身份进行认证。

测试条件：提供用户数据采集说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：在用户选择操作过程中，检查车载端是否首先登录用户身份，包括生物特征、密码或已认证设备等多种认证方式。
步骤（2）：检查车载端采集用户使用行为等用户数据时，车载端是否弹出提示框提示用户，是否向用户提供关闭采集功能；
步骤（3）：关闭后查看数据存储容量是否继续变化，判断是否继续采集数据。

预期结果：

（1）在用户选择操作过程中，车载端首先对用户身份进行确认，包括生物特征、密码或已认证设备等多种认证方式；
（2）车载端采集用户使用行为等用户数据时，提示用户并向用户提供关闭数据采集的功能，用户选择关闭后不继续采集数据。

判定条件：

在步骤（1）后，如果车载端不对用户身份进行认证，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果未提示用户，或没有选择功能，或者选择关闭后监测到车载端仍然在采集，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。

编号5.7.1.4　　级别：1—4级

技术要求：参照T/CSAE 101-2018 第5.7.1.4项，车载端应具备支持国家监管部门依法进行数据采集工作的能力。

测试条件：提供用户数据采集说明，送检车载端系统处于正常工作状态。

测试步骤：

步骤（1）：检查厂商提交文档，查看车载端是否具备支持国家监管部门依法进行数据采集工作的能力； 步骤（2）：按照说明，验证车载端是否可以采集国家监管部门要求采集的数据。
预期结果： （1）厂商提交文档中说明车载端具备支持国家监管部门依法进行数据采集工作的能力； （2）车载端可以采集国家监管部门要求采集的数据。
判定条件： 在步骤（1）后，如果未说明车载端具备支持国家监管部门依法进行数据采集工作的能力，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未能采集国家监管部门要求采集的数据，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。

5.7.2 数据安全存储

编号5.7.2.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.2.1 项，车载端在将用户敏感数据（例如：用户身份、位置信息）存储在车内系统时，应为保存数据的文件设置适当的权限，以防止未授权的访问和篡改。	
测试条件：提供数据存储说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：以非授权身份通过车载端访问存储在车内系统的用户敏感数据（例如：用户身份、位置信息）； 步骤（2）：以非授权身份尝试对存储在车内系统的用户敏感数据（例如：用户身份、位置信息）进行修改。	
预期结果： （1）载端可以阻止非授权访问存储在车内系统的用户敏感数据（例如：用户身份、位置信息）； （2）车载端可以阻止非授权身份修改在车内系统的用户敏感数据（例如：用户身份、位置信息）。	
判定条件： 在步骤（1）后，如果可以访问读取用户敏感数据，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果可以对用户敏感数据进行非授权修改，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“不符合要求”，评测结束。	

编号5.7.2.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.2.2 项，存储涉及用户生物特征的数据时，应采用加密形式保存。	
测试条件：提供数据存储说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查涉及用户生物特征的数据的加密存储方案和被加密信息的列表； 步骤（2）：尝试不经解密直接访问列表中涉及用户生物特征的数据，验证是否为密文存储。	

预期结果：
（1）涉及用户生物特征的数据有对应的加密存储方案，并具有被加密信息的列表；
（2）涉及用户生物特征的数据采用加密形式保存。

判定条件：
在步骤（1）后，如果没有加密存储方案，或者被加密信息列表有缺失，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果非解密即可对数据进行读取，且显示明文存储数据，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。

编号5.7.2.3	级别：1—4级

技术要求：参照 T/CSAE 101-2018 第 5.7.2.3 项，车载端不应有未向用户明示且未经用户同意，擅自修改用户数据的行为。

测试条件：提供数据存储说明，送检车载端系统处于正常工作状态。

测试步骤：
步骤（1）：检查厂商提交文档，查看用户数据收集的类型和内容，及相应的处理、存储、传输机制；
步骤（2）：尝试修改用户数据，检测车载端是否向用户明示，用户选择拒绝修改后是否仍继续修改用户数据。

预期结果：
（1）厂商提交文档中描述用户数据收集的类型和内容，及相应的处理、存储、传输机制；
（2）车载端未有未向用户明示且未经用户同意，擅自修改用户数据的行为。

判定条件：
在步骤（1）后，厂商提交文档中未描述用户数据收集的类型和内容，或相应的数据处理、存储、传输机制，该项目评测结果为“不符合要求”，评测结束；
在步骤（2）后，如果存在收集到的用户数据被修改，且修改行为没有告知用户并得到用户授权，该项目评测结果为“不符合要求”，评测结束；
否则，则该项目评测结果为“未见异常”，评测结束。

编号5.7.2.4	级别：3—4级

技术要求：参照 T/CSAE 101-2018 第 5.7.2.4 项，安全存储的文件应具备标识信息，无法在非授权设备中使用。

测试条件：提供数据存储说明，送检车载端系统处于正常工作状态。

测试步骤：
步骤（1）：检查厂商提交文档，查看对安全存储的文件标识信息的说明，是否有授权访问安全存储文件的设备列表；
步骤（2）：尝试通过非授权设备访问和调用车载端中安全存储的文件。

预期结果：
（1）厂商提交文档中说明安全存储的文件具有的标识信息，说明授权访问安全存储文件的设备；
（2）车载端中安全存储的文件无法在非授权设备中使用。

判定条件：

在步骤（1）后，如果安全存储的文件无标识信息，或未说明授权访问安全存储文件的设备，则该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果非授权设备可以访问和调用车载端中安全存储的文件，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。

5.7.3 数据安全传输

编号5.7.3.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.3.1 项，应使用防护措施，对所传输数据的完整性和可认证性进行保护。	
测试条件：提供数据传输说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交文档，查看对传输数据完整性保护方案和可认证性相关机制； 步骤（2）：使用通信数据检测工具监测传输数据，使用篡改、伪造等方法模拟攻击，检测防护措施有效性。	
预期结果： （1）厂商提交的文档说明对传输数据完整性保护方案和可认证性相关机制； （2）使用防护措施，可以对所传输数据的完整性和可认证性进行保护，可以识别篡改、伪造后的传输信息。	
判定条件： 在步骤（1）后，如果没有完整性保护方案和可认证性相关机制，或缺少相关内容描述，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果车载端未能识别篡改、伪造后的传输信息，该项目评测结果为“不符合要求”，评测结束； 否则，则该项目评测结果为“未见异常”，评测结束。	

编号5.7.3.2	级别：3—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.3.2 项，应使用国密算法对重要数据进行加密传输。	
测试条件：提供数据传输说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交文档，查看重要数据列表及其加密传输要求； 步骤（2）：通信数据检测工具，获取通信数据，检查重要数据在传输过程中是否加密，加密算法是否符合国家要求。	
预期结果： （1）厂商提交文档说明重要数据列表及其加密传输要求； （2）重要数据在传输过程中加密，加密算法符合国家要求。	
判定条件： 在步骤（1）后，如果重要数据列表有明显缺失，或未说明重要数据传输加密要求，该项目评测结果为“不符合要求”，评测结束；	

在步骤（2）后，如果重要数据在传输过程中未加密，或加密算法不符合国家要求，该项目评测结果为“不符合要求”，评测结束； 否则，则该项目评测结果为“未见异常”，评测结束。

5.7.4 数据安全删除

编号5.7.4.1	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.4.1 项，共享类应用（例如：共享汽车），在当前用户退出后，该用户的敏感数据应被清空。	
测试条件：提供数据删除说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：选择共享类应用，退出当前用户登录，查看应用及车载系统中该用户的敏感数据是否被清空； 步骤（2）：尝试恢复该用户的敏感数据，检测是否可以恢复用户敏感数据。	
预期结果： （1）共享类应用（例如：共享汽车），在当前用户退出后，该用户的敏感数据应被清空； （2）清空的用户敏感数据不可被恢复。	
判定条件： 在步骤（1）后，如果用户的敏感数据未清空，或有残留，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果可以恢复用户敏感数据，该项目评测结果为“不符合要求”，评测结束； 否则，则该项目评测结果为“未见异常”，评测结束。	

编号5.7.4.2	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.4.2 项，通过车载端采集的用户数据，在传送到云端服务器后，应具备相应的脱敏措施，防止用户隐私信息泄露。	
测试条件：提供数据删除说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：检查厂商提交文档，查看车载端采集的用户数据类型及上传云端时相应的脱敏方案； 步骤（2）：使用通信数据检测工具，检查车载端采集的用户数据传输到云端服务器的用户数据类型，是否包含用户隐私，检查脱敏方案有效性； 步骤（3）：对仍需保留在云端的用户隐私数据，检测访问控制策略的有效性。	
预期结果： （1）厂商提交文档说明车载端采集的用户数据类型及上传云端时相应的脱敏方案； （2）车载端采集的用户数据，在传送到云端服务器后，进行用户隐私信息脱敏处理； （3）对仍需保留在云端的用户隐私数据，设置访问控制策略且有效。	
判定条件： 在步骤（1）后，如果厂商提交文档未说明车载端采集的用户数据类型及上传云端时相应的脱敏方案，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果应被脱敏操作去除的用户数据仍然可见，该项目评测结果为“不符合要求”，评测结束；	

在步骤（3）后，如果云端用户隐私数据缺少必要的访问控制，该项目评测结果为“不符合要求”，评测结束； 否则，则该项目评测结果为“未见异常”，评测结束。

编号5.7.4.3	级别：1—4级
技术要求：参照 T/CSAE 101-2018 第 5.7.4.3 项，车载端设备更换件后，换下的旧件所存放的数据需安全删除，相关用户数据需同步新件，以防止用户数据泄漏或丢失。	
测试条件：提供数据删除说明，送检车载端系统处于正常工作状态。	
测试步骤： 步骤（1）：车载端设备更换件后，检查换下的旧件所存放的数据是否安全删除； 步骤（2）：尝试恢复该旧件存储的用户数据，检测是否可以恢复用户数据； 步骤（3）：检查更换新设备后，相关用户数据是否同步到新设备。	
预期结果： （1）车载端设备更换件后，换下的旧件所存放的数据安全删除且不可恢复； （2）更换新设备后，相关用户数据应同步到新设备。	
判定条件： 在步骤（1）后，如果用户的数据未清空，或有残留，该项目评测结果为“不符合要求”，评测结束； 在步骤（2）后，如果可以恢复旧设备中的用户数据，该项目评测结果为“不符合要求”，评测结束； 在步骤（3）后，如果用户数据未更新到新设备，该项目评测结果为“不符合要求”，评测结束； 否则，则该项目评测结果为“未见异常”，评测结束。	