ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 40856—2021

车载信息交互系统信息安全技术要求及试验方法

Technical requirements and test methods for cybersecurity of on-board information interactive system

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：中国汽车技术研究中心有限公司、北京新能源汽车股份有限公司、华为技术有限公司、中国信息通信研究院、中国第一汽车股份有限公司、英飞凌科技(中国)有限公司、北京奇虎科技有限公司、国汽(北京)智能网联汽车研究院有限公司、上汽大众汽车有限公司、北京百度网讯科技有限公司、上海汽车集团股份有限公司技术中心、国家计算机网络应急技术处理协调中心、重庆长安汽车股份有限公司、东南(福建)汽车工业有限公司、浙江吉利汽车研究院有限公司、北京理工新源信息科技有限公司、上汽通用五菱汽车股份有限公司。

本文件主要起草人：张亚楠、孙航、张兆龙、潘凯、国炜、李木犀、陈汉顺、刘建鑫、王建、刘洋洋、阮旻枫、李显杰、费枭、王晖、汪向阳、金小红、杨成浩、陈奕昆、崔硕。

车载信息交互系统信息安全
技术要求及试验方法

1 范围

本文件规定了车载信息交互系统硬件、通信协议与接口、操作系统、应用软件、数据的信息安全技术要求与试验方法。

本文件适用于指导整车厂、零部件供应商、软件供应商等企业，开展车载信息交互系统信息安全技术的设计开发、验证与生产等工作。

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 25069 信息安全技术 术语

GB/T 40861 汽车信息安全通用技术要求

GM/T 0005—2012 随机性检测规范

3 术语和定义

GB/T 25069、GB/T 40861 界定的以及下列术语和定义适用于本文件。

3.1

车载信息交互系统 on-board information interactive system

安装在车辆上的通信系统，具备下列至少一项功能：

a) 对外可通过蜂窝网络、短距离通信等通信技术建立连接并进行数据交换等功能，对内可通过汽车总线与电子电气系统进行信息采集、数据传递与指令下发等功能；

b) 实现通话、录音、导航和娱乐等相关服务功能。

注 1：车载信息交互系统通常为远程车载信息交互系统(T-Box)、车载综合信息处理系统(IVI)以及其混合体。

注 2：典型的车载信息交互系统示意图见附录 A 中图 A.1。

3.2

对外通信 external communication

车载信息交互系统与车辆外部的无线通信。

注：包括基于移动蜂窝网络的远程通信、蓝牙、WLAN 等短距离通信等。

3.3

内部通信 internal communication

车载信息交互系统与车辆内电子电气系统的通信。

注：包括基于 CAN、CAN-FD、LIN、车载以太网等车辆内部的通信。

3.4

用户 user

使用车载信息交互系统资源的对象。

注：包括人、车辆或者第三方应用程序。

3.5

用户数据　user data

由用户产生或为用户服务的数据。

注：该数据不影响安全功能的运行。

3.6

代码签名　code signing

利用数字签名机制，由具备签名权限的实体对全部或部分代码进行签名的机制。

3.7

应用软件　application software

在车载信息交互系统上，为实现支付、娱乐等功能的一类软件。

注：包括在车载信息交互系统中已预装的应用软件和后期可安装的应用软件。

3.8

平台服务端　platform server

为车辆提供服务的平台。

注：包括企业自主运营平台及第三方平台等。

3.9

外部终端　external terminal

车辆外部的终端设备。

注：包括路侧单元、手机等。

3.10

车载公有远程通信协议　on-board public telecommunication protocol

适用于车载信息交互系统，并且经国际或国家标准化组织采纳或批准的标准通信协议。

注：包括 HTTP、FTP 等。

3.11

车载私有远程通信协议　on-board private telecommunication protocol

除 HTTP、FTP 等通信协议，整车厂或零部件厂与 TSP 自定义适用于车载信息交互系统的通信协议。

4　缩略语

下列缩略语适用于本文件。

CAN：控制器局域网络(Controller Area Network)

CAN-FD：控制器局域网络-灵活数据(Control Area Network-flexible data)

ECU：电子控制单元(Electronic Control Unit)

E-Call：紧急呼叫(Emergency Call)

FTP：文件传输协议(File Transfer Protocol)

HTTP：超文本传输协议(Hypertext Transfer Protocol)

ID：标识符 (Identifier)

JTAG：联合测试工作组(Joint Test Action Group)

LE：低功耗(Low Energy)

LIN：局域互连网络(Local Interconnect Network)

PCB：印制电路板(Printed Circuit Board)

PSK:预共享密钥(Pre-Shared Key)
SPI:串行外设接口(Serial Peripheral Interface)
SSP:安全简易配对(Secure Simple Pairing)
SU:切换用户(Switch User)
TLS:安全传输层协议 (Transport Layer Security)
TSP:终端服务平台(Telematics Service Provider)
UART:通用异步收发器(Universal Asynchronous Receiver/Transmitter)
URL:统一资源定位符(Uniform Resource Locator)
USB:通用串行总线(Universal Serial Bus)
WLAN:无线局域网(Wireless Local Area Networks)
WPA:无线局域网安全接入(WLAN Protected Access)

5 技术要求

5.1 硬件安全要求

5.1.1 车载信息交互系统所使用的芯片应满足以下要求:

a) 按照 6.1 a)进行测试,调试接口应禁用或设置安全访问控制;

b) 按照 6.1 b)进行测试,不存在后门或隐蔽接口。

5.1.2 按照 6.1 c)进行测试,车载信息交互系统所使用的处理器、存储模块、通信 IC 等用于处理、存储和传输个人敏感信息的关键芯片及安全芯片,应减少暴露管脚。

5.1.3 按照 6.1 d)进行测试,车载信息交互系统所使用的关键芯片之间应减少暴露的通信线路数量,例如:使用多层电路板的车载信息交互系统可采用内层布线方式隐藏通信线路。

5.1.4 按照 6.1 e)进行测试,电路板及芯片不宜暴露用以标注端口和管脚功能的可读丝印。

5.2 通信协议与接口安全要求

5.2.1 对外通信安全

5.2.1.1 通信连接安全

按照 6.2.1.1 a)进行测试,车载信息交互系统应实现对平台服务端或外部终端的身份认证。当身份认证成功后,按照 6.2.1.1 b)进行测试,车载信息交互系统与平台服务端或外部终端才能进行业务数据的通信交互。

5.2.1.2 通信传输安全

按照 6.2.1.2 进行测试,车载信息交互系统与平台服务端或外部终端间传输的数据内容应进行加密,宜使用国密算法。

5.2.1.3 通信终止响应安全

车载信息交互系统进行通信时,应满足以下要求:

a) 按照 6.2.1.3 a)进行测试,数据内容校验失败时,应终止该响应操作;

b) 按照 6.2.1.3 b)进行测试,发生身份鉴权失败时,应终止该响应操作。

5.2.1.4 远程通信协议安全

5.2.1.4.1 车载公有远程通信协议安全

车载公有远程通信协议，按照 6.2.1.4.1 进行测试，应采用 TLS 1.2 版本及以上或至少同等安全级别的安全通信协议。

5.2.1.4.2 车载私有远程通信协议安全

车载私有远程通信协议应满足以下要求：

a) 按照 6.2.1.4.2 a)进行测试，支持以安全方式进行用于数据加密密钥的更新；

b) 按照 6.2.1.4.2 b)进行测试，其使用的密钥应进行安全传输。

5.2.1.5 短距离通信协议安全

5.2.1.5.1 短距离通信口令应用安全

短距离通信口令应用安全应满足以下要求：

a) 按照 6.2.1.5.1 a)进行测试，缺省口令应使用至少包括阿拉伯数字、大小写拉丁字母，长度不少于 8 位的强复杂度的口令；

注：蓝牙不限定于以上条款要求内。

b) 按照 6.2.1.5.1 b)进行测试，不同车载信息交互系统应使用不同的缺省口令；

c) 按照 6.2.1.5.1 c)进行测试，更改口令时，限定用户设置 a)要求的口令或向用户提示风险；

注：蓝牙不限定于以上条款要求内。

d) 按照 6.2.1.5.1 d)进行测试，对于人机接口或跨信任网络的不同车载信息交互系统之间接口的登录认证，应支持口令防暴力破解机制，且按照 6.2.1.5.1 e)进行测试，口令文件应设置安全访问控制。

5.2.1.5.2 车载蓝牙通信协议安全

对具有车载蓝牙通信功能的车载信息交互系统应满足以下要求：

a) 按照 6.2.1.5.2 a)进行测试，车载信息交互系统不应存在后门；

b) 按照 6.2.1.5.2 b)进行测试，外部设备请求与车载蓝牙配对的方式在经典(Classic)场合应为 SSP 模式，在 LE 场合应为低功耗安全连接(LE Secure Connection)模式；

c) 按照 6.2.1.5.2 c)进行测试，车载信息交互系统应验证配对请求；

d) 对于高安全要求的车载蓝牙通信功能，例如：利用蓝牙进行非接触控制车辆等，按照 6.2.1.5.2 d)进行测试，应对外部设备的访问权限进行控制以防止非法接入；

e) 对于高安全要求的车载蓝牙通信功能，例如：利用蓝牙进行非接触控制车辆等，按照 6.2.1.5.2 e)进行测试，应对相关数据进行加密处理。

5.2.1.5.3 车载 WLAN 通信协议安全

对具有 WLAN 热点功能的车载信息交互系统，按照 6.2.1.5.3 进行测试，应使用 WPA2-PSK 或更高安全级别的加密认证方式。

5.2.2 内部通信安全

当车载信息交互系统通过 CAN、车载以太网等类型总线与车内其他控制器节点进行数据交互时，按照 6.2.2 进行测试，应使用安全机制确保车辆控制指令等所传输重要数据的完整性和可用性。

5.2.3 通信接口安全

5.2.3.1 总体要求

车载信息交互系统的通信接口应满足以下要求：

a) 按照 6.2.3.1 a)进行测试，不应存在任何后门或隐蔽接口；

b) 按照 6.2.3.1 b)进行测试，访问权限等需授权内容不应超出正常业务范围。

5.2.3.2 车外通信接口安全

5.2.3.2.1 按照 6.2.3.2 a)进行测试，车载信息交互系统应支持路由隔离，隔离执行控制车辆指令、收集个人敏感信息等功能的核心业务平台的通信，隔离对内通信中非核心业务平台的内部通信以及对外通信中非核心业务平台的外网通信等。

注：非核心业务平台指除核心业务平台之外的业务平台。

5.2.3.2.2 按照 6.2.3.2 b)进行测试，车载信息交互系统与能执行控制车辆指令、收集个人敏感信息等功能的核心业务平台间通信宜采用专用网络或者虚拟专用网络通信，与公网隔离。

5.2.3.3 车内通信接口安全

车载信息交互系统应满足以下要求：

a) 按照 6.2.3.3 a)进行测试，对合法指令设置白名单；

b) 按照 6.2.3.3 b)进行测试，对总线控制指令来源进行校验。

5.3 操作系统安全要求

5.3.1 操作系统安全配置

车载信息交互系统在其操作系统安全配置方面，应满足以下要求：

a) 按照 6.3.1 a)进行测试，禁止最高权限用户直接登录，且限制普通用户提权操作；

b) 按照 6.3.1 b)进行测试，删除或禁用无用账号，并使用至少包括阿拉伯数字、大小写拉丁字母，长度不少于 8 位的强复杂度口令；

c) 按照 6.3.1 c)进行测试，具备访问控制机制控制用户、进程等主体对文件、数据库等客体进行访问；

d) 按照 6.3.1 d)进行测试，禁止不必要的服务，例如：FTP 服务等，按照 6.3.1 e)进行测试，禁止非授权的远程接入服务。

5.3.2 安全调用控制能力

5.3.2.1 通信类功能受控机制

5.3.2.1.1 拨打电话

具有拨打电话功能的车载信息交互系统应满足以下要求：

a) 按照 6.3.2.1.1 a)进行测试，在用户明示同意后，调用拨打电话操作才能执行；

b) 按照 6.3.2.1.1 b)进行测试，向用户明示业务内容，且在用户明示同意后，调用拨打电话开通呼叫转移业务操作才能执行。

注：紧急情况下，E-Call 等应急功能不限定于以上条款要求内。

5.3.2.1.2 三方通话

具有三方通话功能的车载信息交互系统，按照 6.3.2.1.2 进行测试，应在用户明示同意后，调用三方

通话操作才能执行。

5.3.2.1.3 发送短信

具有发送短信功能的车载信息交互系统，按照 6.3.2.1.3 进行测试，应在用户明示同意后，调用发送短信操作才能执行。

注：紧急情况下，E-Call 等应急功能不限定于以上条款要求范围内。

5.3.2.1.4 发送彩信

具有发送彩信功能的车载信息交互系统，按照 6.3.2.1.4 进行测试，应在用户明示同意后，调用发送彩信操作才能执行。

5.3.2.1.5 发送邮件

具有发送邮件功能的车载信息交互系统，按照 6.3.2.1.5 进行测试，应在用户明示同意后，调用发送邮件操作才能执行。

5.3.2.1.6 移动通信网络连接

具有交互界面的车载信息交互系统，在移动通信网络连接时，应满足以下要求：

a) 按照 6.3.2.1.6 a)进行测试，应具备允许开启或关闭移动通信网络连接功能；

b) 按照 6.3.2.1.6 b)进行测试，向用户进行提示，且在用户明示同意后，调用移动通信网络连接功能的操作才能执行；

c) 按照 6.3.2.1.6 c)进行测试，向用户提供通过配置应用软件调用移动通信网络连接的功能；

d) 当移动通信网络处于已连接状态时，按照 6.3.2.1.6 d)进行测试，应在交互界面上给用户相应的状态提示；

e) 当正在传送数据时，按照 6.3.2.1.6 e)进行测试，应在交互界面上给用户相应的状态提示；

f) 上述 d)和 e)中，按照 6.3.2.1.6 f)进行测试，状态提示的方式应不同。

注：紧急情况下，E-Call 等应急功能不限定于以上条款要求内。

5.3.2.1.7 WLAN 网络连接

具有交互界面的车载信息交互系统，在 WLAN 网络连接时，应满足以下要求：

a) 按照 6.3.2.1.7 a)进行测试，应具备允许开启或关闭 WLAN 网络连接功能；

b) 按照 6.3.2.1.7 b)进行测试，向用户进行提示，且在用户明示同意后，调用 WLAN 网络连接功能的操作才能执行；

c) 当 WLAN 网络处于已连接状态时，按照 6.3.2.1.7 c)进行测试，应在交互界面上给用户相应的状态提示；

d) 当正在传送数据时，按照 6.3.2.1.7 d)进行测试，应在交互界面上给用户相应的状态提示；

e) 上述 c)和 d)中，按照 6.3.2.1.7 e)进行测试，状态提示的方式应不同。

5.3.2.2 本地敏感功能受控机制

5.3.2.2.1 定位功能

具有交互界面的车载信息交互系统，在调用定位功能时，应满足如下要求：

a) 按照 6.3.2.2.1 a)进行测试，在用户明示同意后，才能执行定位功能；

b) 按照 6.3.2.2.1 b)进行测试，向用户提供后台定位控制功能以配置应用软件是否可调用定位功能；

c) 上述 a)和 b)中,按照 6.3.2.2.1 c)进行测试,应让用户分别操作。

d) 当调用定位功能时,按照 6.3.2.2.1 d)进行测试,宜在交互界面上给用户相应的状态提示。

5.3.2.2.2 通话录音功能

具有交互界面的车载信息交互系统,在调用通话录音功能时,按照 6.3.2.2.2 进行测试,应在用户明示同意后,才能执行通话录音功能。

5.3.2.2.3 人机交互功能

具有交互界面的车载信息交互系统,在调用人机交互功能时,按照 6.3.2.2.3 进行测试,应在用户明示同意后,才能执行人机交互功能。

注:此处人机交互功能是指涉及指纹、语音、图像、视频等个人生物特征信息的交互功能。

5.3.2.2.4 对用户数据的操作

处理用户数据时,按照 6.3.2.2.4 进行测试,操作系统应得到相应授权,例如:当应用软件需要调用对电话本数据、通话记录、上网记录、短信数据、彩信数据的读或写操作时,操作系统应在应用软件授权的情况下方可执行。

5.3.3 操作系统安全启动

车载信息交互系统应满足以下要求:

a) 按照 6.3.3 a)进行测试,操作系统的启动应始于一个无法被修改的信任根;

b) 按照 6.3.3 b)进行测试,应在可信存储区域验证操作系统签名后,才能加载车载端操作系统,防止加载被篡改的操作系统;

c) 在执行其他的安全启动代码前,按照 6.3.3 c)进行测试,应验证代码完整性。

5.3.4 操作系统更新

车载信息交互系统应满足以下要求:

a) 按照 6.3.4 a)进行测试,应具备系统镜像的防回退校验功能;

b) 当更新镜像安装失败时,按照 6.3.4 b)进行测试,应恢复到更新前的版本或者进入安全状态;

注:安全状态指不通过车载信息交互系统对整车引入安全威胁的状态。

c) 按照 6.3.4 c)、d)进行测试,应具有验证更新镜像完整性和来源可靠的安全机制。

5.3.5 操作系统隔离

按照 6.3.5 进行测试,除必要的接口和数据,例如:拨打电话等功能和电话本和短信等数据,可共享外,预置功能平行的多操作系统之间不应进行通信。

5.3.6 操作系统安全管理

车载信息交互系统应满足以下要求:

a) 针对车机类操作系统,按照 6.3.6 a)进行测试,应对应用软件运行的实时环境进行监控,对异常状况,例如:异常网络连接、内存占用突增等状况进行告警;

b) 针对车机类操作系统,按照 6.3.6 b)进行测试,应支持 FTP、HTTP 等服务,以及 SU 登录等操作的审计功能;

c) 按照 6.3.6 c)进行测试,应具备重要事件,例如:关键配置变更、非系统的安全启动校验失败等事件的日志记录功能,并若具有网联功能,按照 6.3.6 d)进行测试,应能按照策略上传至服

务器；

d) 按照 6.3.6 e)进行测试，应对日志文件进行安全存储；

e) 按照 6.3.6 f)进行测试，应采取访问控制机制，对日志读取写入的权限进行管理；

f) 按照 6.3.6 g)进行测试，应对开发者调试接口进行管控，禁止非授权访问；

g) 按照 6.3.6 h)进行测试，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。

h) 按照 6.3.6 i)进行测试，宜具备识别、阻断应用软件以高敏感权限，例如：最高权限用户权限、涉及非业务内控车行为的权限等运行的能力。

5.4 应用软件安全要求

5.4.1 应用软件基础安全

车载信息交互系统上的应用软件基础安全应满足以下要求：

a) 按照 6.4.1 a)进行测试，从安全合规的来源下载和安装软件；

b) 按照 6.4.1 b)进行测试，不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。

c) 按照 6.4.1 c)进行测试，不存在非授权收集或泄露个人敏感信息、非授权数据外传等恶意行为；

d) 按照 6.4.1 d)进行测试，不以明文形式存储个人敏感信息；

e) 按照 6.4.1 e)进行测试，具备会话安全保护机制，例如：使用随机生成会话 ID 等机制；

f) 按照 6.4.1 f)进行测试，使用至少包括阿拉伯数字、大小写拉丁字母，长度不少于 8 位的强复杂度口令或向用户提示风险；

g) 按照 6.4.1 g)进行测试，符合密码学要求，不直接在代码中写入私钥；按照 6.4.1 h)进行测试，使用已验证、安全的加密算法和参数；按照 6.4.1 i)进行测试，同一个密钥不复用于不同用途；

h) 按照 6.4.1 j)进行测试，使用到的随机数符合 GM/T 0005—2012 等随机数相关标准，保证由已验证、安全的随机数生成器产生。

5.4.2 应用软件代码安全

车载信息交互系统上的应用软件代码安全应满足以下要求：

a) 按照 6.4.2 a)进行测试，应用软件的开发者在使用第三方组件时应识别其涉及公开漏洞库中已知的漏洞并安装补丁；

b) 对于非托管代码，按照 6.4.2 b)进行测试，应确保内存空间的安全分配、使用和释放；

c) 按照 6.4.2 c)进行测试，应用软件安装包应采用代码签名认证机制；

d) 按照 6.4.2 d)进行测试，发布后应禁用调试功能，并删除调试信息；

e) 在非调试场景或非调试模式下，按照 6.4.2 e)进行测试，应用软件日志不应包含调试输出；

f) 按照 6.4.2 f)进行测试，宜使用构建工具链提供的代码安全机制，例如：堆栈保护、自动引用计数等；

g) 按照 6.4.2 g)进行测试，宜使用安全机制，例如：混淆、加壳等，防止被逆向分析。

5.4.3 应用软件访问控制

车载信息交互系统上的应用软件访问控制应满足以下要求：

a) 按照 6.4.3 a)进行测试，应支持权限管理，按照 6.4.3 b)进行测试，不同的应用软件基于实现特定功能分配不同的接口权限；

b) 按照 6.4.3 c)进行测试,对外部输入的来源,例如:用户界面、URL 等来源进行校验;
c) 身份校验时,按照 6.4.3 d)进行测试,应至少进行本地验证。

5.4.4 应用软件运行安全

车载信息交互系统上的应用软件运行安全应满足以下要求:
a) 按照 6.4.4 a)进行测试,与控制车辆、支付相关等关键应用软件在启动时应执行自检机制;
b) 当输入个人敏感信息时,按照 6.4.4 b)进行测试,应采取安全措施确保个人敏感信息不被其他应用窃取,并通过使用安全软键盘等防止录屏;
c) 应用软件正常退出时,按照 6.4.4 c)进行测试,应擦除缓存文件中的个人敏感信息;
d) 按照 6.4.4 d)进行测试,应用软件进程间通信不宜明文传输个人敏感信息;
e) 按照 6.4.4 e)进行测试,不宜利用进程间通信提供涉及个人敏感信息功能的接口。

5.4.5 应用软件通信安全

车载信息交互系统上的应用软件通信安全应满足以下要求:
a) 对外传输个人敏感信息时,按照 6.4.5 a)进行测试,应采用数据加密传输方式;
b) 按照 6.4.5 b)进行测试,实现通信端之间的双向认证后,才能发送个人敏感信息;
c) 按照 6.4.5 c)进行测试,使用已验证、安全的参数设置,按照 6.4.5 d)进行测试,只允许验证通过 OEM 授信 CA 签发的证书。

5.4.6 应用软件日志安全

车载信息交互系统上的应用软件日志安全应满足以下要求:
a) 按照 6.4.6 a)进行测试,采取访问控制机制管理日志读取和写入的权限;
b) 按照 6.4.6 b)进行测试,对用于记录用户支付历史记录、导航检索历史记录等事件的重要日志文件进行安全存储;
c) 按照 6.4.6 c)进行测试,对个人敏感信息进行脱敏或其他防护后,才能写入应用日志。

5.5 数据安全要求

5.5.1 数据采集

车载信息交互系统数据采集应满足以下要求:
a) 采集用户数据时,按照 6.5.1 a)进行测试,应告知用户采集目的和范围,取得授权同意,并提供关闭数据采集的功能;
b) 采集个人敏感信息时,按照 6.5.1 b)进行测试,应取得用户的明示同意,并确保个人信息主体的明示同意是其在完全知情的基础上自愿给出的、具体的、清晰明确的意愿表示;
c) 采集远程控制、远程诊断等功能场景下所发送的指令数据时,按照 6.5.1 c)进行测试,应取得用户授权同意;
d) 按照 6.5.1 d)进行测试,宜在提供相应服务的同时进行用户数据采集。

5.5.2 数据存储

车载信息交互系统数据存储应满足以下要求:
a) 按照 6.5.2 a)进行测试,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)摘要等加密算法存储个人敏感信息,宜采用硬件安全存储方式;
b) 按照 6.5.2 b)进行测试,应实现安全重要参数的安全存储和运算,可采用硬件防护方式;

c) 存储用户数据时，按照 6.5.2 c)进行测试，应防止非授权访问；
d) 按照 6.5.2 d)进行测试，应采用技术措施处理后再进行存储个人生物识别信息，例如：仅存储个人生物识别信息的摘要等方式；
e) 按照 6.5.2 e)进行测试，未经用户授权不应修改、删除用户数据；
f) 按照 6.5.2 f)进行测试，应对用户数据采集、传输、存储、销毁等操作进行日志存储。

5.5.3 数据传输

按照 6.5.3 进行测试，车载信息交互系统应采取管理措施和技术手段，保护所传输用户数据的保密性、完整性和可用性。

5.5.4 数据销毁

车载信息交互系统数据销毁应满足以下要求：
a) 按照 6.5.4 a)进行测试，应具备用户数据销毁的功能，且销毁后数据不能恢复；
b) 对共享类应用，例如：共享汽车等应用场景，在当前用户退出后，按照 6.5.4 b)进行测试，应清空个人敏感信息。

6 试验方法

6.1 硬件安全试验

按照下列流程进行：
a) 检查是否存在暴露在 PCB 板上的 JTAG 接口、USB 接口、UART 接口、SPI 接口等调试接口，如存在则使用测试工具尝试获取调试权限；
b) 拆解被测样件设备外壳，取出 PCB 板，检查 PCB 板硬件是否存在后门或隐蔽接口；
c) 通过采用开盒观察方法，检查关键芯片管脚暴露情况，或审查相应文档，是否有减少暴露管脚的考量；
d) 查看 PCB 布线及设计，检查芯片之间通信线路是否做隐蔽处理，检查敏感数据的通信线路数量或审查相应文档，检查通信线路是否有做隐蔽处理与减少通信线路数量的考量；
e) 通过采用开盒观察方法，检查车载信息交互系统的电路板及电路板上的芯片是否存在用以标注端口和管脚功能的可读丝印。

6.2 通信协议与接口安全试验

6.2.1 对外通信协议安全试验

6.2.1.1 通信连接安全试验

按照下列流程进行：
a) 采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查车载信息交互系统与平台服务端或外部终端的通信有无身份认证；
b) 采用网络数据抓包工具进行数据抓包，解析通信报文数据，模拟中间人攻击方式，检查车载信息交互系统与平台服务端或外部终端是否无法建立通信连接。

6.2.1.2 通信传输安全试验

采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查车载信息交互系统与平台服务端或外部终端间传输的数据内容是否经过加密。

6.2.1.3 通信终止响应安全试验

按照下列流程进行：

a) 采用网络数据抓包工具进行数据抓包，解析通信报文数据，将其篡改，发送篡改数据，触发数据内容校验失败，检查车载信息交互系统是否终止该响应操作；

b) 采用网络数据抓包工具进行数据抓包，解析通信报文数据，模拟伪造签名的报文数据，触发身份鉴权失败，检查车载信息交互系统是否终止该响应操作。

6.2.1.4 远程通信协议安全试验

6.2.1.4.1 车载公有远程通信协议安全试验

采用网络数据抓包工具进行数据抓包，解析通信报文数据，检查是否采用如 TLS 1.2 同等安全级别或以上要求的安全通信协议。

6.2.1.4.2 车载私有远程通信协议安全试验

按照下列流程进行：

a) 对车载私有远程通信协议方案进行审核，采用网络数据抓包的方法进行数据抓包，解析通信报文数据中加密密钥衍生和更新策略，检查是否支持以安全方式进行定期更新；

b) 对车载私有远程通信协议方案进行审核，采用网络数据抓包的方法进行数据抓包，解析通信报文数据中加密密钥传输策略，检查安全传输协议是否以安全的方式传输数据加密密钥。

6.2.1.5 短距离通信协议安全试验

6.2.1.5.1 短距离通信口令应用安全试验

按照下列流程进行：

a) 使用暴力破解的方法，检查缺省口令的复杂度；

b) 通过对同一产品的多个样品验证缺省口令的方式，检查缺省口令是否具有唯一性；

c) 设置较低复杂度口令，检查修改过程中是否给出明确的风险提示或不允许设置；

d) 对于人机接口或跨信任网络的不同车载信息交互系统之间接口的登录认证，使用暴力破解的方法，检查是否成功触发防暴力破解机制；

e) 通过尝试篡改口令文件，检查是否设置了访问控制。

6.2.1.5.2 车载蓝牙通信协议安全试验

按照下列流程进行：

a) 模拟遍历连接车载信息交互系统上的蓝牙设备，检查是否不存在后门提供其他车辆服务；

b) 采用蓝牙抓包工具进行数据抓包，解析蓝牙通信数据，检查针对 Classic 场合，是否采用 SSP 模式或针对 LE 场合，是否采用 LE Secure Connection 模式；

c) 向车载蓝牙设备发出配对请求，检查车载蓝牙设备是否对配对请求进行验证；

d) 利用未具有访问权限的外部设备，尝试进行控制车辆，检查是否不能成功接入；

e) 在利用蓝牙进行非接触控制车辆业务时，采用蓝牙抓包工具进行数据抓包，解析蓝牙通信数据，检查是否对相关数据进行安全加密处理。

6.2.1.5.3 车载 WLAN 通信协议安全试验

通过获取 WLAN 热点安全类型，检查 WLAN 热点是否采用 WPA2-PSK 或更高安全级别的加密认证方式。

6.2.2 车内通信协议的安全试验

采用车内网络报文抓包、解析及发送数据的方法，检查车载信息交互系统通过 CAN 或车载以太网等总线与车内其他控制器节点进行数据交互、传输重要数据时，是否使用安全机制保证传输数据的完整性及可用性。

6.2.3 通信接口的安全试验

6.2.3.1 总体要求试验

按照下列流程进行：

a) 对软硬件接口进行探测、对端口进行扫描，检查是否不存在未公开接口，是否不存在可绕过系统安全机制对系统或数据进行访问的功能；
b) 对通信接口进行遍历，检查其访问权限是否满足最小权限原则。

6.2.3.2 车外通信接口安全试验

按照下列流程进行：

a) 访问车载信息交互系统中不同区域的数据，检查车载信息交互系统是否支持路由隔离，是否可以隔离核心业务平台的通信、内部通信、外网通信等；
b) 使用公网访问车载信息交互系统和核心业务平台，检查车载信息交互系统与核心业务平台的通信是否采用专用网络或者虚拟专用网络通信，与公网隔离。

6.2.3.3 车内通信接口安全试验

按照下列流程进行：

a) 调用非白名单指令，检查车载信息交互系统是否针对发送和接收到的指令进行白名单过滤；
b) 模拟恶意应用，发送控制指令，检查车载信息交互系统是否实现总线控制指令来源的校验。

6.3 操作系统安全试验

6.3.1 操作系统安全配置试验

按照下列流程进行：

a) 使用最高权限用户账号登录，并使用普通账号登录后尝试进行提权，检查系统是否禁止最高权限用户直接登录，限制普通用户提权操作；
b) 查看系统中的账号列表，检查是否存在无用账号，或者尝试登录其中的无用账号，验证是否无法登陆，通过设置弱口令，检查系统是否提示口令安全弱，账号口令至少包括阿拉伯数字、大小写拉丁字母，并且长度不小于 8 位；
c) 使用授权身份或授权进程对文件、数据库等进行访问，检查访问是否被允许，使用非授权身份或非授权进程对文件、数据库等进行访问，检查访问是否无法成功；
d) 查看正在运行的应用服务，检查是否关闭了不必要的应用服务；
e) 使用授权身份进行远程接入，检查是否可以成功远程接入，使用非授权身份进行远程接入，检查是否不能远程接入服务。

6.3.2 安全调用控制能力试验

6.3.2.1 通信类功能受控机制安全试验

6.3.2.1.1 拨打电话安全试验

按照下列流程进行：

a) 在应用软件内调用拨打电话操作，检查应用软件调用执行拨打电话操作时，是否在用户明示同意的情况下，才能执行拨打操作；
b) 在应用软件内调用拨打电话开通呼叫转移业务操作，检查应用软件调用执行拨打电话开通呼叫转移业务时，是否向用户明示业务内容，且在用户明示同意的情况下才能执行操作。

6.3.2.1.2 三方通话安全试验

在应用软件内调用三方通话操作，检查应用软件调用执行三方通话操作时，是否在用户明示同意的情况下才能执行三方通话操作。

6.3.2.1.3 发送短信安全试验

在应用软件内调用发送短信操作，检查应用软件调用执行发送短信操作时，是否在用户明示同意的情况下才能执行发送短信操作。

6.3.2.1.4 发送彩信安全试验

在应用软件内调用发送彩信操作，检查应用软件调用执行发送彩信操作时，是否在用户明示同意的情况下才能执行发送彩信操作。

6.3.2.1.5 发送邮件安全试验

在应用软件内调用发送邮件操作，检查应用软件调用执行发送邮件操作时，是否在用户明示同意的情况下才能执行发送邮件操作。

6.3.2.1.6 移动通信网络连接安全试验

按照下列流程进行：

a) 检查车载信息交互系统是否提供了开启或关闭移动通信网络数据连接的功能，开启时检查是否可使用移动通信网络数据连接，关闭时检查是否无法使用移动通信网络数据连接；
b) 检查应用软件调用开启通信网络数据连接功能时，是否对用户进行了相应的提示，且是否在用户明示同意后才开启通信网络数据连接功能，当用户未确认时是否没有开启；
c) 检查车载信息交互系统是否向用户提供通过配置应用软件调用移动通信网络连接的功能；
d) 检查当移动通信网络的数据连接处于已连接状态时，车载信息交互系统是否在用户界面上有相应的状态提示；
e) 当移动通信网络正在传送数据时，检查车载信息交互系统是否在用户界面上有相应的状态提示；
f) 检查 d)和 e)的两种状态提示是否不同。

6.3.2.1.7 WLAN 网络连接安全试验

按照下列流程进行：

a) 检查车载信息交互系统是否有开启或关闭的 WLAN 网络连接功能，开启时检查是否可使用 WLAN 网络连接，关闭时检查是否不能使用 WLAN 网络连接；
b) 检查应用软件调用开启 WLAN 网络连接功能时，是否对用户进行相应的提示，且是否在用户明示同意后才开启 WLAN 网络连接，当用户未确认时是否没有开启；
c) 检查当 WLAN 网络连接处于已连接状态时，车载信息交互系统是否在用户界面上有相应的状态提示；
d) 检查当 WLAN 网络正在传送数据时，车载信息交互系统是否在用户界面上有相应的状态

提示；

e) 检查 c)和 d)的两种状态提示是否不同。

6.3.2.2 本地敏感功能受控机制试验

6.3.2.2.1 定位功能试验

按照下列流程进行：

a) 检查当应用软件在使用期间调用定位功能时，车载信息交互系统是否要求用户明示同意允许使用定位功能，用户未确认时是否会停止调用定位功能；

b) 检查车载信息交互系统是否提供了后台定位控制能力，且用户是否可为每个应用软件选择开启和关闭后台定位功能；

c) 检查 a)和 b)是否让用户分别操作；

d) 检查当应用软件调用定位功能时，车载信息交互系统是否在用户界面上有相应的状态提示。

6.3.2.2.2 通话录音功能试验

检查当应用软件调用通话录音功能时，是否要求用户明示同意，用户未确认时是否不开启通话录音。

6.3.2.2.3 人机交互功能试验

检查应用软件调用人机交互功能时，是否要求用户明示同意，用户未确认时是否不开启人机交互功能。

6.3.2.2.4 对用户数据的操作试验

使用授权的应用软件对用户数据进行处理，检查是否可以成功执行，使用非授权的应用软件对用户数据进行处理，检查是否无法成功。

6.3.3 操作系统安全启动试验

按照下列流程进行：

a) 获取操作系统安全启动信任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，重复多次检查是否可将数据写入该存储区域；

b) 提取操作系统签名，使用软件调试工具对签名进行篡改，将修改后签名写入到车载终端内的指定可信区域内，检查是否正常工作；

c) 获取操作系统的系统固件等其他安全启动代码，使用软件调试工具对其进行篡改，将修改后的启动代码写入到车载终端内的指定区域，检查是否正常工作。

6.3.4 操作系统更新安全试验

按照下列流程进行：

a) 将镜像替换为过期的镜像，检查是否无法成功加载；

b) 如通过在更新镜像时人为断电等方法，确认更新镜像安装失败时，系统安装之前的版本是否可用或是否进入安全状态；

c) 修改更新镜像，检查更新流程是否无法执行；

d) 使用非官方授信的更新镜像，检查更新流程是否无法执行。

6.3.5 操作系统隔离试验

审查设计文档，检查是否采用了操作系统隔离措施，即除拨打电话、电话本和短信等必要的接口和数据可以共享外，不同操作系统之间不能进行通信。

6.3.6 操作系统安全管理试验

按照下列流程进行：

a) 针对车机类操作系统，引入异常状况，例如：异常网络连接、内存占用突增等，检查是否会对异常情况进行告警；
b) 针对车机类操作系统，审查文档，检查操作系统是否对重要服务和重要操作具有审计功能；
c) 打开日志查询界面，检查操作系统是否对重要事件进行了日志记录；
d) 审查文档，检查操作系统是否设定了将日志上传至服务器的策略；
e) 通过尝试覆盖、删除日志存储区域，检查日志的存储是否存在安全防护；
f) 使用授权身份进行日志读取或写入，检查是否可以成功操作，使用非授权身份进行日志读取或访问，检查是否无法成功；
g) 使用授权身份通过调用调试接口访问内部数据，检查是否可以成功操作，使用非授权身份通过调用调试接口访问内部数据，检查是否无法成功；
h) 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；若存在高危漏洞，则检查该高危漏洞处置方案的技术文件；
i) 通过应用软件进行最高权限用户权限运行和业务不包含控车的应用软件进行控车行为操作，检查该操作是否会被阻断。

6.4 应用软件安全试验

6.4.1 应用软件基础安全试验

按照下列流程进行：

a) 尝试下载和安装未使用官方签名的应用软件，检查是否不可以正常下载和安装；
b) 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；若存在高危漏洞，则检查该高危漏洞处置方案的技术文件；
c) 对应用软件中数据进行分析，检查应用软件对个人敏感信息是否非授权收集或泄露、非授权数据是否外传等恶意行为；
d) 使用分析、查找方法，检查应用软件是否以明文形式存储个人敏感信息；
e) 分析会话内容，检验车载信息交互系统是否具备会话安全保护机制，如：使用随机生成的会话 ID 等；
f) 使用暴力破解方法，检查用户口令长度、字符类型等策略，是否满足要求或未使用强复杂度的口令时，检查是否向用户提示风险；
g) 对代码进行查找和分析，检查是否在代码中不存在私钥；
h) 对代码进行查找和分析，检查该应用软件是否使用已验证的、安全的加密算法和参数；
i) 对代码进行查找和分析，检查是否不存在将同一个密钥复用于多种不同用途；
j) 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并符合随机数标准。

6.4.2 应用软件代码安全试验

按照下列流程进行：

a) 使用代码扫描工具，对应用软件代码进行扫描，检查应用软件构建设置是否满足安全要求，应用软件使用的第三方组件是否识别已知漏洞并安装补丁；
b) 对于非托管代码，使用代码扫描工具，检查是否可确保内存空间的安全分配、使用和释放；
c) 分析设计文档，检查应用软件是否采用代码签名机制；
d) 使用调试分析方法，检查应用软件发布后是否可用调试功能或包含调试信息；
e) 在非调试场景或非调试模式下，使用调试工具进行分析，检查应用软件日志是否包含调试输出；
f) 使用代码扫描工具，检查是否使用构建工具链提供的代码安全机制，例如堆栈保护、自动引用计数；
g) 使用逆向工具进行分析，检查应用软件是否使用混淆、加壳等安全机制，对抗针对应用的逆向分析。

6.4.3 应用软件访问控制试验

按照下列流程进行：
a) 通过遍历调用所有接口的方式，检查是否授予超出其实际业务需求的权限；
b) 采用分析设计文档和测试的方法，检查不同的应用软件是否分配不同的接口权限集合；
c) 通过对应用软件的输入接口进行模糊测试的方式，检查应用软件是否对输入信息的来源，包括用户界面、URL 等进行校验；
d) 采用分析设计文档的方法，检查身份验证是否至少在本地进行。

6.4.4 应用软件运行安全试验

按照下列流程进行：
a) 篡改或替换关键应用软件的部分代码，检查关键应用程序能否正常启动运行；
b) 检验输入个人敏感信息时，检查是否使用安全软键盘或其他安全措施，确保敏感信息不被其他应用窃取，并防止录屏；
c) 应用软件正常终止时，读取内存数据，检查是否包含个人敏感信息；
d) 截取进程间通信内容，进行分析，检查进程间通信是否涉及明文的个人敏感信息；
e) 遍历接口，截取各接口通信内容，进行分析，检查应用软件是否利用进程间通信提供敏感功能的接口。

6.4.5 应用软件通信安全试验

按照下列流程进行：
a) 采用网络数据抓包工具进行数据抓包，解析应用软件对外传输的数据，检查个人敏感信息是否加密；
b) 采用网络数据抓包工具进行数据抓包，解析通信数据，检查通信端是否进行双向认证；
c) 采用网络数据抓包工具进行数据抓包，解析通信数据，检查是否使用已验证、安全的参数设置；
d) 采用网络数据抓包工具进行数据抓包，解析通信数据，获取证书，检查证书是否是通过 OEM 授信的 CA 签发的。

6.4.6 应用软件日志安全试验

按照下列流程进行：
a) 通过尝试日志读取写入操作，检查是否存在访问控制机制，检查是否对日志读写进行权限管理；

b) 通过尝试覆盖、删除日志存储区域，检查重要日志是否实现了安全存储；
c) 分析应用软件存储的日志，检查是否包含未脱敏的个人敏感信息。

6.5 数据安全试验

6.5.1 数据采集安全试验

按照下列流程进行：

a) 检查车端在采集用户数据时，是否通过明确告知采集目的和范围等方式得到用户的授权同意和提供关闭数据采集的功能；
b) 检查车端在采集个人敏感信息时，是否通过主动点击“同意”等方式得到用户的明示同意；
c) 检查车端在远程控制、远程诊断等功能场景下发送指令数据时，是否通过明确告知等方式得到用户的授权同意；
d) 启动一项服务，检查是否在服务启动之后才进行数据采集，终止服务时停止数据采集。

6.5.2 数据存储安全试验

按照下列流程进行：

a) 通过尝试读取存储包含个人敏感信息的文件，检查个人敏感信息是否使用 SM2、SM3、SM4、长度不低于 2048 位的 RSA、长度不低于 128 位的 AES、Hash 摘要等加密算法进行了加密存储；
b) 通过查看车载信息交互系统设计文档，检查是否有效实现重要安全参数的安全存储和运算；
c) 使用非授权身份访问存储用户数据的文件，检查是否无法访问文件信息；
d) 检查存储在车载信息交互系统中的个人生物识别信息，是否使用了仅存摘要等技术措施；
e) 通过尝试修改和删除存储的用户数据，检查是否无法成功，用户同意之后，尝试修改和删除存储的用户数据，检查是否成功；
f) 检查车载信息交互系统是否支持采集、传输、存储、销毁等数据操作日志的存储功能。

6.5.3 数据传输安全试验

使用篡改、伪造等方法进行模拟攻击，检查对于数据完整性、保密性和可用性的防护措施是否有效。

6.5.4 数据销毁安全试验

按照下列流程进行：

a) 通过更换零部件操作或者应用安装后删除等操作，检查车载信息交互系统是否具备数据销毁的功能；对销毁的数据尝试进行恢复，检查是否能恢复销毁数据；
b) 启动共享应用程序，执行用户退出后再次登录，检查是否可以获取到个人敏感信息。

附 录 A
（资料性）
车载信息交互系统示意图

车载信息交互系统对外可与基站、钥匙等外部终端或服务平台进行通信，对内可与网关、ECU 等车内电子系统进行通信，其示意图见图 A.1。

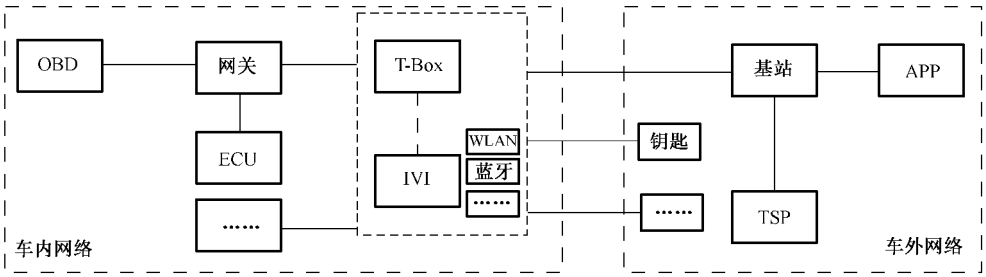

图 A.1 车载信息交互系统示意图