中 国 汽 车 工 程 学 会 标 准

T/CSAE xx-xxxx

智能网联汽车车载端信息安全技术要求

Intelligent and Connected Vehicle On-Board Terminal

Cyber Security Technical Requirements

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国汽车工程学会

目　　次

1　范围 4
2　规范性引用文件 4
3　术语、定义和缩略语 4
3.1 术语与定义 4
3.2 缩略语 5
4　车载端安全架构及目标 6
4.1 车载端安全架构 6
4.2 硬件安全目标 6
4.3 操作系统安全目标 6
4.4 应用安全目标 6
4.5 对内通信安全目标 7
4.6 对外通信安全目标 7
4.7 用户数据安全目标 7
5　车载端安全技术要求 8
5.1 整体安全性 8
5.2 硬件安全 8
5.3 操作系统安全 8
5.4 应用软件安全 9
5.5 对内通信安全 10
5.6 对外通信安全 10
5.7 用户数据安全技术要求 11
6　车载端安全技术要求分级 12

前　言

本部分按照GB/T 1.1-2009给出的规则起草。

请注意本部分的某些内容可能涉及专利。本部分的发布机构不承担识别这些专利的责任。

本标准由中国汽车工程学会归口。

1 范围

本标准规定了智能网联汽车车载端信息安全技术要求。智能网联汽车所涉及网络包括车内网、车际网和车载移动互联网。本标准仅适用于具备联网功能的车载终端，联网范畴包括车载移动互联网和车际网。

本标准适用但不限于车载 T-BOX、车载信息娱乐系统 In-Vehicle Infotainment（IVI）等车载端信息系统。

2 规范性引用文件

下列标准所包含的条文，通过在标准中引用而构成本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T5271 数据处理词汇

GB 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 19596 电动汽车术语

3 术语、定义和缩略语

3.1 术语与定义

3.3.1

智能网联汽车 ICV

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。

3.3.2

智能网联汽车车载端 ICV 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。

3.3.3

用户 User

使用车载端资源的对象，包括人或第三方应用程序。

3.3.4

用户数据 User Data

车载端上存储的用户个人信息和车辆信息，包括由车辆状态数据（诊断数据、运行数据等）、车辆资产数据（软件、协议、架构等）、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）等。

3.3.5

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。

3.3.6

数字签名 Digital Signature

由且只由信息发送者生成的附在数据后面的数字串，或对数据通过密码变换方式进行操作。数据的接收者可以通过验证数字签名来鉴别数据的来源和完整性，数字签名还可以保护数据不被篡改、伪造，保证数据的不可否认性。

3.3.7

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代码全部或部分功能进行签名的机制。

3.2 缩略语

ICV Intelligent and Connected Vehicle

BGA Ball Grid Array

LGA Land Grid Array

SPA Simple Power Analysis

DPA Differential Power Analysis

CPA Correlation Power Analysis

TEE Trusted Execution Environment

SE Secure Element

ECU Electronic Control Unit

CAN Controller Area Network

HTTPS Hyper Text Transfer Protocol over Secure Socket Layer

4　车载端安全架构及目标

4.1 车载端安全架构

智能网联汽车的新型业务需求之一是具备网联功能的车载端对外通过蜂窝网络、短距离通信、以及车车/车路通信协议与互联网、车际网建立连接，进行数据交换；对内与汽车总线及电子电气系统进行信息采集和指令下发。基于这样的通信和数据交换需求，结合相应的安全威胁分析，智能网联汽车车载端的安全架构应包括构成车载端本身的硬件、操作系统、应用三个层面的安全，对外通信和对内通信的安全，以及贯穿这几个环节的数据安全。其架构如图1所示。

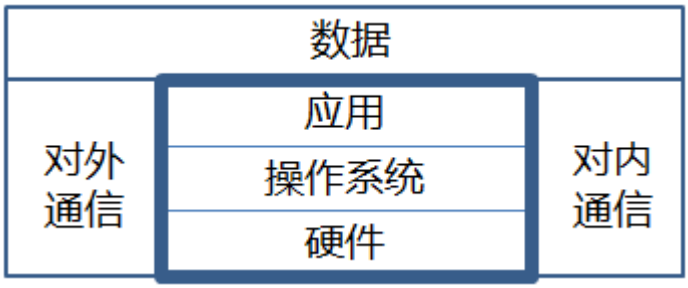

图1　车载端安全架构

4.2 硬件安全目标

车载端硬件安全目标是保证车载端系统使用的电路和芯片在实现数据运算和数据存储等功能时的安全性，能够对抗针对加解密操作的密码分析攻击，侧信道攻击，故障注入攻击等破坏数据保密性和完整性的安全威胁，保证车载端所存储的关键数据不被泄露或篡改，芯片功能可以正常使用。

4.3 操作系统安全目标

操作系统安全目标是通过符合车载端应用场景的身份权限管理和访问控制机制，正确地响应授权操作和处理异常行为，对抗针对操作系统的溢出攻击、暴力破解、中间人攻击、重放、篡改、伪造等多种安全威胁，保证操作系统文件和数据的可用性、保密性、完整性和可审计性，保证对各类资源的正常访问，系统能够按照预期正常运行或在各种操作情况之下处于安全状态。

4.4 应用安全目标

应用安全目标是要保证安装在车载端上的应用软件具备相应的来源标识和保密性、完整性的防护措施，可以对抗逆向分析、反编译、篡改、非授权访问等各种针对应用的安全威胁，并确保应用产生、使用的数据得到安全的处理、车载端应用与相关服务器之间通信的安全性，保证应用为用户提供服务时，以及应用在启动、升级、登录、退出等各模式下的安全性。金融类应用应遵循支付类应用相关技术要求中的安全性要求。

4.5 对内通信安全目标

对内通信是指车载端与车内总线以及电子电气系统之间的通信。其安全目标是根据应用场景对通信和数据交换的需求，保证外部威胁与内部网络之间的安全隔离，保证车载端不向内部关键电子电气系统发送伪造、重放等攻击方式的指令和数据，不非法占用内部总线资源，保证车内子系统和数据的保密性、完整性，保证汽车功能正常。

4.6 对外通信安全目标

对外通信连接包括车载端与蜂窝网络的通信，与移动终端间的短距离通信，以及与其它车辆和路侧设施的通信。对外通信安全的目标是根据应用场景对通信和数据交换的需求，保证车载端建立通信连接时采取必要的认证、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，及通信质量。

4.7 用户数据安全目标

用户数据安全目标是要保证车载端所采集、存储、处理、传输的用户数据的安全性，确保用户数据的机密性、完整性和可用性得到有效的防护，同时具有清除机制，保护数据生命周期各环节的安全性。

5 车载端安全技术要求

5.1 整体安全性

5.1.1 安全技术的选择与实施

5.1.1.1 安全设计综合考虑整体网络安全防护需求,即车载端的安全技术措施能够有效地与云端安全措施和通信网络安全措施相配合。
5.1.1.2 车载端安全方案的设计和实施，应与整车设计开发验证测试流程紧密结合。

5.2 硬件安全

5.2.1 硬件设计安全

5.2.1.1 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。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。
5.2.1.2 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。
5.2.1.3 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。
5.2.1.4 车载端具备硬件实现的安全区域或安全模块,能够有效地实现敏感数据安全存储和运算的物理隔离，应使用必要的安全机制保证此区域的数据不能够被非授权访问。

5.2.2 抗攻击防护

5.2.2.1 使用必要的安全机制，防御针对芯片的电压、时钟的单次故障注入攻击。
5.2.2.2 使用必要的安全机制，防御针对芯片的电磁、激光的单次故障注入攻击。
5.2.2.3 使用必要的防护措施，对抗针对加密芯片的侧信道简单功耗分析（SPA）攻击。
5.2.2.4 使用必要的防护措施，对抗针对加密芯片的侧信道一阶差分功耗分析（DPA）攻击。
5.2.2.5 使用必要的防护措施，对抗针对加密芯片的侧信道相关功耗分析（CPA）攻击。

5.3 操作系统安全

5.3.1 操作系统安全启动

5.3.1.1 系统启动时应使用可信机制，在验证操作系统签名后，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。

5.3.2 操作系统加载启动可信应用程序

5.3.2.1 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（例如：使用白名单的方式或者签名技术），保证应用的完整性，避免运行恶意程序。

5.3.3 系统安全防护

5.3.3.1 应采用完整性校验手段（例如：基于 SHA2 等哈希算法的数字摘要技术、数字签名技术），对关键代码或文件进行完整性保护。

5.3.3.2 车载端系统不存在后门、以及在中国汽车行业漏洞应急响应平台发布一段时间（例如：6 个月）的高危安全漏洞。系统提供能够及时进行漏洞修复的方式。

5.3.4 资源访问控制

5.3.4.1 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。
5.3.4.2 能够通过软件层面可信执行环境（例如：TEE 技术），为可信关键应用提供安全执行环境，隔离对关键资源和数据（例如：通信密钥、CAN 控制器）的访问，保护资源和数据的保密性、完整性和访问控制。
5.3.4.3 能够通过硬件解决方案（例如：SE 安全模块技术）为关键数据提供存储空间，并且为基于这些数据的运算提供安全的空间，保护关键重要数据的保密性和完整性。

5.3.5 安全日志记录及审计控制

5.3.5.1 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。
5.3.5.2 支持日志上传功能，根据云端管理需求，采取安全的方式传输日志。
5.3.5.3 应采取访问控制机制，对日志读取写入的权限进行管理；应提供日志存储的安全保护功能。

5.3.6 系统软件更新与固件更新

5.3.6.1 只接收在约定的车辆运动状态（例如：非行驶状态并且）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。
5.3.6.2 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回滚操作，避免更新失败导致系统失效。
5.3.6.3 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。并且能够处理车内系统或设备对更新文件的认证和校验请求，并返回相应结果。当认证或校验不通过时，车载端系统能够向相应的云端服务器返回错误信息，并对升级进行阻断。

5.3.7 介质接口安全

5.3.7.1 车载端不应存在未经声明的外围介质接口（例如：CD/DVD、SD、USB）。
5.3.7.2 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。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，并规定对通过介质接口对车载端进行的操作类型的限制。

5.4 应用软件安全

5.4.1 应用软件安全基本要求

5.4.1.1 通用应用软件不应存在后门，和在中国汽车行业漏洞应急响应平台发布一段时间（例如：6

个月）的高危安全漏洞。
5.4.1.2 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。
5.4.1.3 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）。
5.4.1.4 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。

5.4.2 应用软件签名认证机制

5.4.2.1 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。
5.4.2.2 未经代码签名的应用软件当且仅当用户确认后才能执行下一步操作。

5.4.3 应用启动自检要求

5.4.3.1 关键应用程序在启动时应执行自检程序，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。

5.4.4 安全审计要求

5.4.4.1 应用程序应具备记录用户行为、应用状态的日志功能，并支持集中管理。

5.4.5 应用通信安全

5.4.5.1 应用程序与服务器之间的通信，应使用安全通信协议（例如：HTTPS）。

5.5 对内通信安全

5.5.1 对车内子系统访问的安全控制

5.5.1.1 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安全域的划分。安全域应有相应的等级，并建立跨域通信的安全访问策略。
5.5.1.2 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。

5.5.2 对车内部通信可靠性和可用性的安全防护

5.5.2.1 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。
5.5.2.2 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。

5.6 对外通信安全

5.6.1 蜂窝网络通信安全

5.6.1.1 车载端应使用安全机制，确保接入真实可靠的网络。
5.6.1.2 车载端与核心业务平台的通信信道，应与公开网络逻辑隔离。
5.6.1.3 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。
5.6.1.4 车载端应采取技术措施，禁用不必要的蜂窝网络通信功能。
5.6.1.5 通过蜂窝网络传送的针对车载端的关键操作（例如：用户信息写入），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。
5.6.1.6 应根据不同应用的重要性划分优先级，保障关键业务具有网络通信的优先使用权。

5.6.2 车车通信、车路协同通信安全

5.6.2.1 车载端具备符合标准的身份标识，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）的车载端进行身份验证。
5.6.2.2 车载端应支持用于身份认证、通信加密和完整性保护的证书或密钥生成机制。

5.6.3 短距离无线连接安全（包括但不限于 Wi-Fi、蓝牙、ZigBee）

5.6.3.1 车载端具备用户手动打开、关闭短距离无线连接的能力。
5.6.3.2 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。
5.6.3.3 对于外来通信连接请求，车载端能够在保证车辆安全的前提下，向用户提供符合应用场景的处理方式，保证连接的可控性。
5.6.3.4 对于车载端的应用调用短距离无线连接的请求，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。
5.6.3.5 车载端只在某种特定状态下接受外来通信连接请求（例如：蓝牙连接配对请求），并对连接设备进行认证授权操作。非该状态时，仅允许已通过认证授权的设备连接。

5.7 用户数据安全技术要求

5.7.1 数据安全采集

5.7.1.1 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。
5.7.1.2 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。
5.7.1.3 车载端采集车辆状态和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。

5.7.2 数据安全存储

5.7.2.1 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。
5.7.2.2 存储涉及用户生物特征的数据时，应采用加密形式保存。
5.7.2.3 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。

5.7.3 数据安全传输

5.7.3.1 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。
5.7.3.2 应使用符合国家相关要求的加密算法对重要数据进行加密传输。

5.7.4 数据安全删除

5.7.4.1 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。
5.7.4.2 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。

6 车载端安全技术要求分级

根据车载端技术要求的防护强度，将车载端技术要求自低到高划分为5个等级，第五级是最高安全等级。车载端可选不同等级的安全要求及措施，以达到相应安全级别。每一等级明确了车载端在该等级所应满足的技术要求的最小集合，当车载端满足该集合中的所有安全技术要求时才能标识为达到该安全级别。具体的等级划分详见表1。

表1 车载端安全技术要求分级

安全技术要求		安全技术要求等级				
		一级	二级	三级	四级	五级
1.	5.1.1.1	√	√	√	√	√
2.	5.1.1.2	√	√	√	√	√
3.	5.2.1.1	√	√	√	√	√
4.	5.2.1.2		√	√	√	√
5.	5.2.1.3			√	√	√
6.	5.2.1.4			√	√	√
7.	5.2.2.1			√	√	√
8.	5.2.2.2				√	√
9.	5.2.2.3			√	√	√
10.	5.2.2.4				√	√
11.	5.2.2.5					√
12.	5.3.1.1			√	√	√
13.	5.3.2.1		√	√	√	√
14.	5.3.3.1	√	√	√	√	√
15.	5.3.3.2	√	√	√	√	√
16.	5.3.4.1	√	√	√	√	√
17.	5.3.4.2			√	√	√
18.	5.3.4.3			√	√	√
19.	5.3.5.1	√	√	√	√	√
20.	5.3.5.2	√	√	√	√	√
21.	5.3.5.3		√	√	√	√
22.	5.3.6.1	√	√	√	√	√
23.	5.3.6.2	√	√	√	√	√
24.	5.3.6.3		√	√	√	√
25.	5.3.7.1	√	√	√	√	√
26.	5.3.7.2		√	√	√	√
27.	5.4.1.1	√	√	√	√	√
28.	5.4.1.2	√	√	√	√	√
29.	5.4.1.3	√	√	√	√	√
30.	5.4.1.4	√	√	√	√	√
31.	5.4.2.1	√	√	√	√	√

32.	5.4.2.2	√	√	√	√	√
33.	5.4.3.1			√	√	√
34.	5.4.4.1	√	√	√	√	√
35.	5.4.5.1	√	√	√	√	√
36.	5.5.1.1		√	√	√	√
37.	5.5.1.2		√	√	√	√
38.	5.5.2.1	√	√	√	√	√
39.	5.5.2.2			√	√	√
40.	5.6.1.1	√	√	√	√	√
41.	5.6.1.2	√	√	√	√	√
42.	5.6.1.3		√	√	√	√
43.	5.6.1.4	√	√	√	√	√
44.	5.6.1.5	√	√	√	√	√
45.	5.6.1.6		√	√	√	√
46.	5.6.2.1	√	√	√	√	√
47.	5.6.2.2	√	√	√	√	√
48.	5.6.3.1	√	√	√	√	√
49.	5.6.3.2	√	√	√	√	√
50.	5.6.3.3		√	√	√	√
51.	5.6.3.4		√	√	√	√
52.	5.6.3.5			√	√	√
53.	5.7.1.1	√	√	√	√	√
54.	5.7.1.2	√	√	√	√	√
55.	5.7.1.3		√	√	√	√
56.	5.7.2.1	√	√	√	√	√
57.	5.7.2.2		√	√	√	√
58.	5.7.2.3	√	√	√	√	√
59.	5.7.3.1	√	√	√	√	√
60.	5.7.3.2			√	√	√
61.	5.7.4.1	√	√	√	√	√
62.	5.7.4.2	√	√	√	√	√