ICS35.240.99
T 36

# 团　　体　　标　　准

T/TIAA 016—2019

# 智能网联汽车车载终端信息安全要求

Requirements of intelligent and connected vehicle

on-Board terminal cyber security



2019-07-12 发布　　2019-07-12 实施

中关村车载信息服务产业应用联盟　　发布

# 目　　次

# 前　言

本标准按照 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。

本标准由中关村车载信息服务产业应用联盟标准化委员会提出并归口。

本标准起草单位：北京航空航天大学、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）、中国汽车工程研究院股份有限公司、国汽（北京）智能网联汽车研究院有限公司、电子科技大学、中国汽车工程学会、中汽认证中心有限公司、上海汽车集团股份有限公司、中国第一汽车集团有限公司、重庆长安汽车股份有限公司、长城汽车股份有限公司、广州汽车集团股份有限公司、上海鲲石汽车技术有限公司、中关村车载信息服务产业应用联盟、广东为辰信息科技有限公司、启明信息技术股份有限公司、惠州德赛西威智能交通技术研究院有限公司、惠州华阳通用电子有限公司、四川省信息安全测评中心、四维创智（北京）科技发展有限公司、北京梆梆安全科技有限公司、智车优行科技（北京）有限公司。

本标准主要起草人：王云鹏、刘法旺、罗璎珞、宋娟、郭盈、于海洋、秦洪懋、王建、周唯、刘建行、罗蕾、陈丽蓉、薛晓卿、朱科屹、陈晓东、李允、李秋实、陈博、汪向阳、罗薇、刘真谛、张金池、丁淑兰、庞春霖、赵焕宇、罗建超、张淼、张裁会、苗澎锋、王丹琛、李雷、黄乙衷、卢佐华、季申。

# 智能网联汽车车载终端信息安全要求

## 1 范围

本标准给出了智能网联汽车车载终端信息安全架构，规定了车载终端安全要求和车载终端安全要求分级。

本标准适用于智能网联汽车车载终端，设计、研制、使用和验收。

## 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，凡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 20984-2007 信息安全技术信息安全风险评估规范

## 3 术语、定义和缩略语

### 3.1 术语与定义

下列术语和定义适用于本文件。

#### 3.1.1 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。

#### 3.1.2 智能网联汽车车载终端 intelligent and connected vehicles on-board terminal

智能网联汽车车载终端是智能网联汽车的一个子系统或功能单元。

#### 3.1.3 用户 user

使用车载终端资源的主体。

3.1.4 **用户数据** user data

车载终端上存储的用户个人信息和车辆信息。

3.1.5 **授权** authorization

赋予某一主体可实施某些动作的权利的过程。

3.1.6 **数字签名** Digital Signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.1.7 **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进行签名的机制。

## 3.2 缩略语

下列缩略语适用于本文件。

BGA 焊球阵列封装 Ball Grid Array

CAN 控制器局域网络 Controller Area Network

CD 光盘 Compact Disc

DVD 数字视频光盘 Digital Video Disc

ECU 电子控制单元 Electronic Control Unit

ICV 智能网联汽车 Intelligent and Connected Vehicle

IVI 车载信息娱乐系统 In-Vehicle Infotainment

LGA 栅格阵列封装 Land Grid Array

SD 安全数字 Secure Digital

SE 安全单元 Secure Element

TEE 可信执行环境 Trusted Execution Environment

USB 通用串行总线 Universal Serial Bus

# 4 车载终端安全架构

车载终端智能网联汽车车载终端安全架构如图 1 所示。

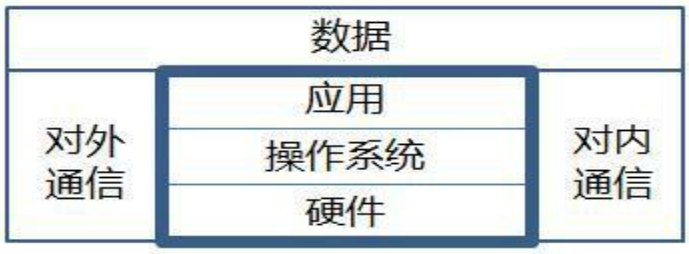


图1　智能网联汽车车载终端安全架构

## 5　车载终端安全要求

### 5.1　整体安全性

#### 5.1.1　安全技术的选择与实施

5.1.1.1　按 GB/T 20984 进行风险评估分析，全面分析网络接口与威胁攻击路径，明确车辆整体安全需求与车载终端安全需求，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终端自身进行安全防护，并将车载终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（例如：确保驾驶员和交通参与人员的人身安全）。

5.1.1.2　应综合考虑整体网络安全防护需求，车载终端的安全技术措施能够有效地与后台服务器安全技术措施和通信网络安全技术措施相配合。

### 5.2　硬件安全

#### 5.2.1　设计安全

5.2.1.1　车载终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　车载终端系统的电路板上不应标注芯片、端口和管脚功能的可读信息。

5.2.1.3　车载终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终端系统采用内层布线方式隐藏通信线路），对抗针对车载终端内部数据传输的窃听和伪造攻击。

5.2.1.4　车载终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）。

5.2.1.5　车载终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障此区域的数据不被非授权访问。

#### 5.2.2 访问控制

5.2.2.1 车载终端具备硬件实现的安全区域或安全模块，实现车载终端设备重要数据安全存储与隔离。

5.2.2.2 在安全区域或安全模块中一次性写入的敏感信息，应不能非授权获取或者篡改。

5.2.2.3 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。

#### 5.2.3 抗攻击防护

5.2.3.1 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。

5.2.3.2 使用必要的防护措施，对抗针对加密芯片的简单功耗分析、差分功耗分析、相关功耗分析，以及利用运行时间、温度等其它信息进行的侧信道攻击。

5.2.3.3 使用必要的防护机制，对抗针对车载终端设备内存的侵入和篡改攻击。

### 5.3 操作系统安全

#### 5.3.1 操作系统安全启动

应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终端操作系统，避免加载被篡改的操作系统。

#### 5.3.2 多操作系统隔离

如车载终端存在多个操作系统，应采用隔离机制，保障不同操作系统之间的安全防护。

#### 5.3.3 操作系统加载应用程序

应提供安全机制，保障操作系统只能加载启动可信的车载终端应用程序，能够验证应用的来源和完整性，避免运行恶意程序。

#### 5.3.4 系统安全防护

5.3.4.1 应采用完整性校验手段，对关键代码或文件进行完整性保护。

5.3.4.2　车载终端系统不应存在国家漏洞管理机构发布了 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功能。

### 5.3.5 资源访问控制

5.3.5.1　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。

5.3.5.2　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。

### 5.3.6 安全日志记录及审计控制

5.3.6.1　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。

5.3.6.2　支持日志上传功能，上传时应对后台服务器进行认证；根据后台服务器管理需求，采取安全的方式传输日志，确保数据的完整性和可认证性。

5.3.6.3　应采取访问控制机制，对日志读取写入的权限进行管理；应对日志存储进行安全防护。

### 5.3.7 系统软件更新与固件更新

5.3.7.1　应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）下发起的车载终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。

5.3.7.2　软件更新时，应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，避免通过车载终端升级尝试对车辆资源进行过度消耗。

5.3.7.3　车载终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，操作才可继续执行。

### 5.3.8 媒体接口安全

5.3.8.1　车载终端不应存在未经声明的外围媒体（例如：CD/DVD、SD 卡）接口。

5.3.8.2　车载终端应定义通过外围接口接入的存储媒体上的文件类型和权限，并限制通过媒体接口对车载终端进行的操作类型。

5.3.8.3　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。

## 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　应用软件不应存在国家漏洞管理机构发布了 6 个月及以上的高危安全漏洞。

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

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。

### 5.4.3　应用软件运行要求

5.4.3.1　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。

5.4.3.2　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。

5.4.3.3　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。

5.4.3.4　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。

### 5.4.4　安全审计要求

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。

### 5.4.5　应用流程安全性要求

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 TLS1.2）。

5.4.5.2　应用程序访问服务器需有双向认证机制。

## 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，对包括车载终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。

5.5.1.2　建立跨子系统或者域间通信的安全访问策略，车载终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，避免由于车载终端的信息安全问题造成该类子系统功能的错误或异常。

5.5.1.3　车载终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　车载终端具备冗余备份和重发机制，保障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　车载终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。

5.5.2.3　车载终端应建立监测模块，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。

## 5.6　对外通信安全

### 5.6.1　蜂窝网络通信安全

5.6.1.1　车载终端应使用安全机制，识别伪基站，确保接入真实可靠的蜂窝网络。

5.6.1.2　车载终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。

5.6.1.3　车载终端与核心业务平台的通信应使用安全通信协议（例如 TLS1.2）。

5.6.1.4　车载终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。

5.6.1.5　车载终端应采取技术措施，禁用业务所不需要的蜂窝网络通信功能。

5.6.1.6　通过蜂窝网络传送的针对车载终端的关键操作（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。

5.6.1.7　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。

### 5.6.2 车车通信、车路协同通信安全

5.6.2.1　车载终端具备保障唯一性的身份标识，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。

5.6.2.2　车载终端应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。

### 5.6.3 短距离无线连接安全

5.6.3.1　车载终端应具备用户手动打开、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　车载终端的应用调用短距离无线连接功能时，车载终端能够明示用户，并提供配置能力和符合场景的配置方式。

5.6.3.4　车载终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）以保障车辆安全，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。

5.6.3.5　车载终端发起对外连接时，应对外部设备进行认证，并应使用安全通信协议（例如TLS1.2）支持的安全模式进行通信。

## 5.7　用户数据安全要求

### 5.7.1 数据安全采集

5.7.1.1　车载终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，应说明数据采集的依据。

5.7.1.2　车载终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采集。

5.7.1.3　车载终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。

5.7.1.4　车载终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。

#### 5.7.2 数据安全存储

5.7.2.1　车载终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　车载终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。

5.7.2.4　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。

#### 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　应使用国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：共享汽车上的应用），在当前用户退出后，该用户的敏感数据应被清空。

5.7.4.2　通过车载终端采集的用户数据，在传送到后台服务器服务器后，应具备相应的脱敏措施，防止用户隐私信息泄露。

5.7.4.3　车载终端设备更换件后，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。

## 6　车载终端安全要求分级

### 6.1　各级之间的关系

根据车载终端技术要求的防护强度，将车载终端信息安全要求自低到高划分为四个等级，第四级是最高安全等级。车载终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终端在该等级所应满足的技术要求的最小集合，当车载终端满足该集合中的所有适用的安全要求时才能标识为达到该安全级别。

### 6.2　分级描述

#### 6.2.1 一级

一级为基本安全级，即车载终端具备初步的信息安全认证授权和访问控制措施，对系统和数据采取多种方式保护其信息安全属性，能够基本避免由于信息安全导致的个人隐私泄露或财产损失，且能够基本保障不会由于信息安全问题导致功能安全问题或者社会安全问题。

#### 6.2.2 二级

第二级在第一级的基础上，增加信息安全威胁监测和安全事件审计能力，以及根据监测审计结果进行处置的能力，在实现多层面多方面安全防护的同时提供监管能力。

#### 6.2.3 三级

第三级在第二级的基础上，通过以密码方案为基础的技术措施，构建完备的可信的信息安全防护体系，能够实现操作系统、应用、通信及数据多方面的安全目标。

#### 6.2.4 四级

第四级是在第三级的基础上，加强安全技术的有效性和可靠性，使各种安全措施能够充分地发挥作用，实现包括硬件安全目标在内的各安全目标和整体安全目标，在多种可能的信息安全攻击的情况下，系统仍然能够按照预期的方式工作。

### 6.3 分级要求

等级划分见表 1。

表 1 车载端安全技术要求分级

| 安全技术要求 | | 等级 | | | |
|---|---|---|---|---|---|
| | | 一级 | 二级 | 三级 | 四级 |
| 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. | 5.2.1.5 | | | | √ |
| 8. | 5.2.2.1 | | | √ | √ |
| 9. | 5.2.2.2 | | | √ | √ |
| 10. | 5.2.2.3 | | | | √ |

| 安全技术要求 | | 等级 | | | |
|---|---|---|---|---|---|
| | | 一级 | 二级 | 三级 | 四级 |
| 11. | 5.2.3.1 | | | | √ |
| 12. | 5.2.3.2 | | | | √ |
| 13. | 5.2.3.3 | | | | √ |
| 14. | 5.3.1 | | | √ | √ |
| 15. | 5.3.2 | √ | √ | √ | √ |
| 16. | 5.3.3 | | | √ | √ |
| 17. | 5.3.4.1 | √ | √ | √ | √ |
| 18. | 5.3.4.2 | √ | √ | √ | √ |
| 19. | 5.3.5.1 | √ | √ | √ | √ |
| 20. | 5.3.5.2 | | | √ | √ |
| 21. | 5.3.6.1 | | √ | √ | √ |
| 22. | 5.3.6.2 | | √ | √ | √ |
| 23. | 5.3.6.3 | | √ | √ | √ |
| 24. | 5.3.7.1 | √ | √ | √ | √ |
| 25. | 5.3.7.2 | √ | √ | √ | √ |
| 26. | 5.3.7.3 | | | √ | √ |
| 27. | 5.3.8.1 | √ | √ | √ | √ |
| 28. | 5.3.8.2 | √ | √ | √ | √ |
| 29. | 5.3.8.3 | | √ | √ | √ |
| 30. | 5.4.1.1 | √ | √ | √ | √ |
| 31. | 5.4.1.2 | √ | √ | √ | √ |
| 32. | 5.4.1.3 | √ | √ | √ | √ |
| 33. | 5.4.1.4 | √ | √ | √ | √ |
| 34. | 5.4.2 | √ | √ | √ | √ |
| 35. | 5.4.3.1 | | | √ | √ |
| 36. | 5.4.3.2 | | √ | √ | √ |
| 37. | 5.4.3.3 | √ | √ | √ | √ |
| 38. | 5.4.3.4 | | √ | √ | √ |
| 39. | 5.4.4 | | √ | √ | √ |
| 40. | 5.4.5.1 | √ | √ | √ | √ |
| 41. | 5.4.5.2 | √ | √ | √ | √ |
| 42. | 5.5.1.1 | √ | √ | √ | √ |

| 安全技术要求 | | 等级 | | | |
|---|---|---|---|---|---|
| | | 一级 | 二级 | 三级 | 四级 |
| 43. | 5.5.1.2 | √ | √ | √ | √ |
| 44. | 5.5.1.3 | √ | √ | √ | √ |
| 45. | 5.5.2.1 | √ | √ | √ | √ |
| 46. | 5.5.2.2 | √ | √ | √ | √ |
| 47. | 5.5.2.3 | | √ | √ | √ |
| 48. | 5.6.1.1 | √ | √ | √ | √ |
| 49. | 5.6.1.2 | √ | √ | √ | √ |
| 50. | 5.6.1.3 | √ | √ | √ | √ |
| 51. | 5.6.1.4 | | √ | √ | √ |
| 52. | 5.6.1.5 | √ | √ | √ | √ |
| 53. | 5.6.1.6 | √ | √ | √ | √ |
| 54. | 5.6.1.7 | √ | √ | √ | √ |
| 55. | 5.6.2.1 | | | √ | √ |
| 56. | 5.6.2.2 | | | √ | √ |
| 57. | 5.6.3.1 | √ | √ | √ | √ |
| 58. | 5.6.3.2 | √ | √ | √ | √ |
| 59. | 5.6.3.3 | √ | √ | √ | √ |
| 60. | 5.6.3.4 | √ | √ | √ | √ |
| 61. | 5.6.3.5 | √ | √ | √ | √ |
| 62. | 5.7.1.1 | √ | √ | √ | √ |
| 63. | 5.7.1.2 | √ | √ | √ | √ |
| 64. | 5.7.1.3 | √ | √ | √ | √ |
| 65. | 5.7.1.4 | √ | √ | √ | √ |
| 66. | 5.7.2.1 | √ | √ | √ | √ |
| 67. | 5.7.2.2 | √ | √ | √ | √ |
| 68. | 5.7.2.3 | √ | √ | √ | √ |
| 69. | 5.7.2.4 | | | √ | √ |
| 70. | 5.7.3.1 | √ | √ | √ | √ |
| 71. | 5.7.3.2 | | | √ | √ |
| 72. | 5.7.4.1 | √ | √ | √ | √ |
| 73. | 5.7.4.2 | √ | √ | √ | √ |
| 74. | 5.7.4.3 | √ | √ | √ | √ |