ICS35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术
车载网络设备信息安全技术要求

Information security technology — Cybersecurity technical requirements for invehicle network equipment

（征求意见稿）

2019.12.06

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：东软集团股份有限公司、中国信息安全测评中心、长城汽车股份有限公司、一汽轿车股份有限公司、公安部第一研究所、电子科技大学、公安部第三研究所、中国网络安全审查技术与认证中心、中国汽车工程研究院有限公司、北京百度网讯科技有限公司、华为技术有限公司、北京理工华创电动车技术有限公司、（中金金融认证中心有限公司）中国金融认证中心、山谷网安科技股份有限公司、北京航空航天大学、阿里云计算有限公司、北京天融信网络安全技术有限公司、公安部交通管理科学研究所、工业和信息化部电子第五研究所、中国科学院信息工程研究所、启明星辰信息技术集团股份有限公司、西华大学、北京银联金卡科技有限公司（银行卡检测中心）、网神信息技术（北京）股份有限公司、国家计算机网络应急技术处理协调中心、北京中电华大电子设计有限责任公司、紫光青藤微系统有限公司、联合汽车电子有限公司、恒安嘉新（北京）科技股份公司、国民技术股份有限公司、沈阳美行科技有限公司、北京娜迦信息科技发展有限公司、北京安天网络安全技术有限公司、中国信息通信研究院 、长春吉大正元信息技术股份有限公司、北京神州绿盟科技有限公司、河南森源鸿马电动汽车有限公司、博士（中国）投资有限公司、上海芯钛信息科技有限公司、中国软件评测中心、天地融科技股份有限公司、惠州市德赛西威智能交通技术研究院有限公司、国汽（北京）智能网联汽车研究院有限公司、宝马中国、普华永道商务咨询（上海）有限公司、北京智游网安科技有限公司（爱加密）、重庆邮电大学、北京奇虎科技有限公司、上海市信息安全测评认证中心、国家工业信息安全发展研究中心郑州信大捷安信息技术股份有限公司、重庆长安汽车股份有限公司、杭州安恒信息技术股份有限公司惠州华阳通用电子有限公司、北京四维图新科技股份有限公司、北京梆梆安全科技有限公司、北京华弘集成电路设计有限责任公司、锦图计算技术（深圳）有限公司。

本标准主要起草人：刘晓春、路娜、陈静相、邸丽清、唐迪、申永波、陈丽蓉、张小东、李彦奇、韩煜、唐晓莉、唐春蓬、周立勇、张宇、董爱道、许中奇、左洪强、刘冬、刘建行、冀浩杰、张大江、张屹、封正、贾世准、闫兆腾、赵元勋、李煜光、刘丹、王晖、程济源、訾小超、张裁会、苗澎锋尹子栋、杨贤伟、蒋鑫龙、王彦祥、王海罗、霍盛锟、郭盈、安高峰、王辉、安潇羽、王乃青、刘兴伟、牟宁波、巩金亮、王睿、梁松涛、李浩文、刘大鹏、徐光侠、何勇亮、程璐、宋俊男、李澜涛、魏超、董云鹏、王金龙、张若时。

引　言

车联网构建了新型的移动出行服务，是全球创新热点和未来汽车工业发展制高点，正在引起汽车产业的技术变革和商业模式创新。但随着汽车智能化、网络化程度的不断提高，借助网络可以实现对汽车的更多控制。汽车作为一个智能终端，暴露出容易被攻击和控制的安全隐患，在某种极端情况下，如联网车辆被大量控制，容易造成重大社会事件，安全风险巨大。车联网信息安全已引起全行业、全社会的广泛关注。车载网络设备是车联网信息安全的主要核心之一。

本标准有利于提高车载网络设备信息安全防护能力，保障我国车联网信息安全产业的健康快速发展。

信息安全技术　车载网络设备信息安全技术要求

1　范围

本标准规定了车载网络设备的信息安全技术要求。

本标准适用于指导和规范整车制造商、设备供应商进行车载网络设备信息安全功能的设计、研发、生产、实施以及测试评估，也可作为职能部门进行监督、检查和指导的依据。

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/T 17859 计算机信息系统安全保护等级划分准则

GB/T 18336 信息技术 安全技术 信息技术安全评估准则

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

3　术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010中界定的以及下列术语和定义适用于本文件。

3.1.1

汽车内部网络 invehicle network

汽车内部各种汽车电子系统或部件通过各种内部总线（比如CAN总线、LIN总线、FlexRay总线、车载以太网总线等）连接形成的内部通信网络。

3.1.2

汽车网关 invehicle gateway

汽车内部网络中的网络数据转发设备，通过它可以实现总线上信息的共享、数据转发和汽车内部的网络管理等功能。

3.1.3

车载网络设备 invehicle network equipment

部署于汽车内部网络并负责网络连接和网络通信的汽车内设备，包括负责建立汽车内部网络的汽车网关，负责汽车对外通信连接的车载T-Box和车载信息娱乐系统（IVI）等。

3.1.4

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

3.1.5

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。

3.1.6

数字签名 Digital Signature

附加在数据单元上的数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

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。

T-box	Telematics box	车载T-box
IVI	In-Vehicle Infotainment	车载信息娱乐系统
ECU	Electronic Control Unit	电子控制单元
OBD	On-Board Diagnostic	车载诊断系统
CAN	Controller Area Network	控制器局域网络
LIN	Local Interconnect Network	局域互联网络
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CNNVE	China National Vulnerability Database of Information Security	中国通用漏洞披露

4 安全架构和安全目标

4.1 威胁

4.1.1 通信窃听

攻击者通过监听汽车内部网络和对外通信网络，窃取网络传输内容或通过分析通信流量，非授权获取网络通信内容、通信目的等信息。

4.1.2 信息重放

攻击者通过监听车载网络设备的通信网络，发送一个目的主机已接收过的包，来达到欺骗系统的目的，发起诸如中间人攻击、会话劫持等攻击手段。该攻击特别是在认证的过程中，重复使用认证用户身份所接收的包，从而破坏认证的安全性。

4.1.3 旁路攻击

攻击者通过旁路绕过车载网络设备直接访问车载网络设备连接的汽车内部网络环境。

4.1.4 拒绝服务

攻击者通过向车载网络设备发送大量垃圾信息或干扰信息的方式，导致车载网络设备无法向正常用户提供服务。

4.1.5 暴力破解

非授权用户可能使用反复猜测鉴别数据和密码的方法，对车载网络设备及其连接的汽车内部网络进行攻击。

4.1.6 非授权访问

非授权用户尝试绕过安全机制和策略，操作使用车载网络设备以及接入汽车内部网络。

4.1.7 数据窃取

攻击者通过攻击车载网络设备及其连接的网络，获取存储和传输的数据。

4.1.8 隐私信息窃取

攻击者通过分析车载网络设备传输的通信流量、目的地址、信息内容等，获得用户的个人信息。

4.1.9 攻击行为抵赖

攻击者可能利用审计日志功能的缺失对车载网络设备和汽车内部网络发起攻击，从而逃避系统对攻击行为的检测和记录。

4.1.10 审计存储空间消耗

攻击者通过发送信息或攻击行为消耗审计日志存储空间，导致车载网络设备无法记录审计日志。

4.1.11 系统及软件漏洞

攻击者通过利用车载网络设备操作系统或其应用软件的漏洞进行恶意修改和攻击，如在软件中植入木马、后门，二次打包应用程序等。

4.2 安全架构

如图1所示，汽车网关、车载T-Box和车载信息娱乐系统（IVI）是汽车内部网络和对外通信的重要组成设备。汽车网关是汽车内部网络的核心设备，通过转发实现ECU之间的数据通信；车载T-Box和车载信息娱乐系统（IVI）负责汽车对外通信连接，是实现汽车与外界通信的功能单元。OBD是一种有线连接的外接方式，不在本标准范围。

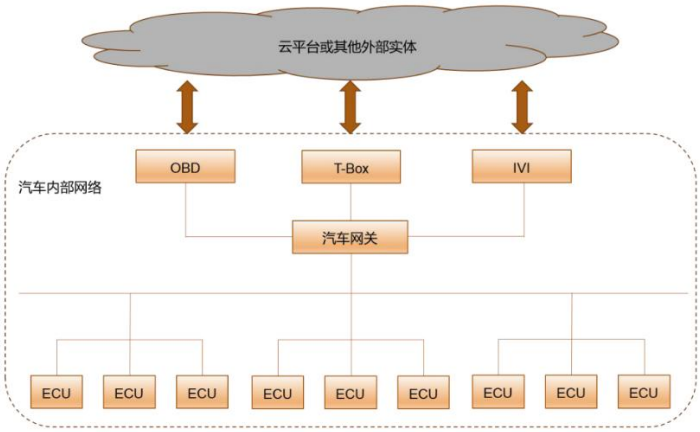

图1 汽车网络示意图

汽车网关、车载T-Box和车载信息娱乐系统（IVI）都应具有相应的安全要求，确保其正常运行。这些安全要求包括：硬件安全，操作系统安全，应用软件安全，数据安全和网络传输安全。安全要求的实现机制都是相同的。比如，机密性保护、完整性保护、审计、访问控制、认证和鉴权等，在每一个安全要求中都有体现。这些安全机制在本标准中归为安全支撑技术，如图2所示。

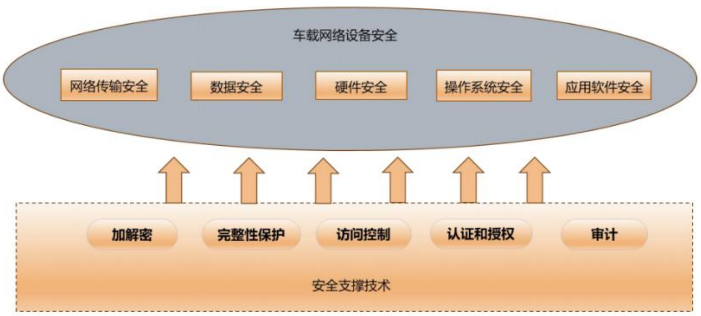

图2 车载网络设备安全支撑技术

4.3 安全目标

4.3.1 总则

车载网络设备应保证自身硬件设计和操作系统、应用软件的信息安全，保证系统按照预期提供正常的服务。

车载网络设备应保证网络传输的信息安全，保证网络传输过程的可认证、保密性和完整性。

车载网络设备应保证数据的安全性，确保数据在采集、处理、存储、传输、销毁等过程的全生命周期中不被非法获取和篡改。

车载网络设备应具有安全的远程升级机制，确保升级包的完整性、来源合法性，以及升级过程的安全运行。

车载网络设备应支持安全管理功能，提供对系统运行状态、网络通信、数据操作等过程的监视或管理。

4.3.2 机密性

确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

4.3.3 完整性

信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。

4.3.4 可用性

确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

4.3.5 可审计性

按照一定的安全策略，利用记录系统活动和用户活动等信息，检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。

4.3.6 可控性

对于系统可能存在的风险进行识别、分析、评估、预警，识别并制订对应的风险管控策略，处理现实的或者潜在的风险，控制并降低风险所带来的不利影响。

4.3.7 隐私保护

保障用户的隐私数据在传递、存储和使用过程中不被非法使用，并保证隐私信息数据在公布和使用过程对用户隐私信息进行脱敏处理。

5 安全技术要求

5.1 硬件安全要求

车载网络设备在硬件设计上应满足以下安全要求：

a) 在电路主板上，不应存在用以标注芯片、端口和管脚功能的可读丝印；
b) 在板载芯片中，不应存在可非法对芯片内存进行访问或者更改芯片功能的隐蔽接口。
c) 应对板载芯片调试接口进行禁用或实施安全访问控制；
d) 板载芯片的诊断接口应具有鉴权功能。；

e) 应具有存储和隔离敏感数据的安全区域或安全模块；
f) 应防止非授权获取或篡改在安全区域或安全模块中一次性写入的敏感信息；
g) 安全区域或安全模块应具有检测与处置非授权访问的机制。

5.2 操作系统安全要求

5.2.1 操作系统加固

车载网络设备的操作系统应满足以下安全要求：
a) 应禁用或删除无用账号；
b) 应加强口令复杂度；
c) 应禁止root用户直接登录；
d) 应具有访问控制机制，依据安全策略控制用户、进程等主体对文件、数据库等客体的访问；
e) 应关闭不必要的服务；
f) 不应存在后门，也不存在于中国汽车行业漏洞共享平台（CAVD）、国家信息安全漏洞共享平台（CNVD）、中国国家信息安全漏洞库（CNNVD）、CVE、CNCVE等公开发布了6个月及以上的高危安全漏洞。

5.2.2 操作系统安全启动

车载网络设备的操作系统应满足以下安全要求：
a) 操作系统的启动应始于一个可信代码或者信任根。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操作系统；
b) 应能够验证应用的来源和完整性，保证操作系统只加载启动可信的应用程序。

5.2.3 操作系统隔离

如车载网络设备存在多个操作系统时，应采用隔离机制，保证不同操作系统之间的安全防护。

5.2.4 操作系统更新

车载网络设备的操作系统应满足以下安全要求：
a) 软件更新时，应保证更新软件包的来源可靠性，并对接收到的更新文件进行完整性校验；
b) 应具有备份和恢复能力，能够在软件更新失败时进行必要的操作，比如回滚到更新之前的版本，避免更新失败导致系统失效；
c) 软件更新应在约定的工况（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，并在用户确认后执行。

5.2.5 操作系统日志审计

车载网络设备的操作系统应满足以下安全要求：

a) 应具有对内存、CPU、文件等资源进行监视的功能；
b) 应具有日志功能，包括用户操作、系统日志等的记录；
c) 应支持日志上传，并采取安全的方式传输；
d) 应采取访问控制机制，对日志读取写入的权限进行管理；
e) 应对日志存储进行安全防护。

5.3 应用软件安全要求

5.3.1 应用软件基础安全

车载信息娱乐系统（IVI）的应用软件应满足如下安全要求：

a) 不应存在后门，也不存在于中国汽车行业漏洞共享平台（CAVD）、国家信息安全漏洞共享平台（CNVD）、中国国家信息安全漏洞库（CNNVD）、CVE、CNCVE等公开发布了6个月及以上的高危安全漏洞；
b) 不应有非授权收集或泄露用户信息、非法数据外传等恶意行为；
c) 禁止以明文形式存储用户敏感信息 （例如：用户口令、证件号码、交易信息、私钥等）；
d) 宜具有对抗逆向分析的安全机制；
e) 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；
f) 安全机制应考虑全生命周期过程，包括开发、上传、检测、加固、签名、发布、更新和下线等各个环节。

5.3.2 应用软件通信安全

车载信息娱乐系统（IVI）的应用软件应满足如下安全要求：

a) 应用程序与服务器之间的交互，应使用安全通信协议；
b) 应用程序需实现通信端之间的双向认证机制。

5.3.3 应用软件运行安全

车载信息娱乐系统（IVI）的应用软件应满足如下安全要求：

a) 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；
b) 应用软件运行期间，应具有运行验证及编译混淆能力，明确应用程序对系统资源的访问和操作权限；
c) 应防止和检测应用软件之间未授权的访问；
d) 应用软件退出时，应擦除内存中的敏感信息。

5.3.4 应用软件日志审计

车载信息娱乐系统（IVI）的应用软件应满足如下安全要求：

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

5.4 网络传输安全要求

5.4.1 汽车网关通信安全要求

5.4.1.1 边界安全要求

汽车网关应提供边界隔离和访问控制功能，对跨安全域的通信进行路由控制和边界控制（如白名单、数据流向、数据内容等），建立安全的访问路径，禁止非授权访问。

5.4.1.2 网络传输安全要求

汽车网关应满足如下的网络传输安全要求：

a) 应采用加密、认证等安全措施保护关键通信数据的保密性、完整性、可用性和抗重放攻击；
b) 应具有网络安全监测机制，提供针对报文异常和非法入侵的实时监测，并提供分析统计和告警等；
c) 应能够抵抗拒绝服务攻击；
d) 应具有安全存储功能，将用于安全通信的密钥等相关信息进行加密存储；
e) 应对需要网络通信的业务的按照重要性划分优先等级，优先保障高优先级业务的网络通信需求；
a) 应对网络通信的相关访问操作和安全事件生成日志记录。

5.4.2 车载 T-Box 和车载信息娱乐系统（IVI）通信安全技术要求

5.4.2.1 网络接入安全要求

车载T-Box和车载信息娱乐系统（IVI）应满足如下的网络接入安全要求：

a) 不应存在未经声明的外围介质（例如：CD/DVD、SD卡、USB）接口；
b) 应对外部实体发起的通信连接请求进行身份认证；
c) 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，并限制通过接口对车载网络设备进行的操作类型；
d) 应关闭用于监听外部服务的网络服务端口。

5.4.2.2 网络传输安全要求

车载T-Box和车载信息娱乐系统（IVI）应满足如下的网络传输安全要求：

a) 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，与公网隔离；
b) 与远程服务平台进行通信时，应能够互相认证对方的身份，当双方身份相互验证合法后，建立通信链路连接；
c) 应具有针对网络传输的访问控制功能；
d) 应采用安全通信协议或数据加密的机制；
e) 应对外界接入访问进行监视和入侵防御；
f) 具有安全存储功能，将用于安全通信的密钥等相关信息进行加密存储，并保证其完整性；
g) 应具有日志审计功能。

5.5 数据安全防护要求

5.5.1 数据采集

车载网络设备的数据采集应满足如下安全要求：

a) 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，并说明数据采集所依据的国家法律法规或者业务需求；
b) 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，并且应在用户同意的情况下方可继续；
c) 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。

5.5.2 数据存储

车载网络设备的数据存储应满足如下安全要求：

a) 用户敏感数据（例如：用户身份、位置信息）应存储在物理或软件隔离的专用存储区域，同时为保存数据的文件设置适当的访问权限；
b) 应采用加密形式保存涉及用户生物特征的数据；
c) 未向用户明示或未经用户同意禁止擅自修改用户数据；
d) 安全存储的文件应具有标识信息。

5.5.3 数据传输

车载网络设备的数据传输应满足如下安全要求：

a) 应使用安全的传输协议传输数据；
b) 应对重要的数据进行加密传输。。

5.5.4 数据销毁

车载网络设备的数据销毁应满足如下安全要求：

a) 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；
b) 通过车载网络设备采集的用户数据，在传送到云端服务器后，应具有防止用户隐私泄露的脱敏措施；
c) 车载网络设备更换件后，应同步相关用户数据至新件，并删除换下的旧件中存放的数据并；
d) 应对不再使用的敏感数据销毁并且不能被恢复。

5.6 系统远程升级安全防护要求

5.6.1 身份认证

系统升级时，车载网络设备和远程服务器之间应采用双向认证。

5.6.2 传输加密

升级包的传输应采用加密措施。

5.6.3 完整性校验

接收升级包完毕后，应对升级包的数字签名信息进行验证，校验升级包的完整性。

5.6.4 失败恢复

应具有升级管理功能，包括：版本管理、版本备份、升级失败回滚等，保证正在更新的系统能够从失败或者中断的更新中恢复。

5.7 管理安全要求

车载网络设备的安全管理应满足如下安全要求：

a) 应对运行状态进行监视；
b) 应对网络通信过程进行日志记录；
c) 应对数据操作（生成，传输，处理，存储，删除）的全流程进行日志记录；
d) 运行状态监视和日志记录应支持上传和集中管理；
e) 运行状态信息和日志信息的存储应满足敏感数据的存储要求。

参考文献

[1] GB/T 25056-2010 信息安全技术 证书认证系统 密码及其相关安全技术规范
[2] GB/T 32960.1-2016 电动汽车远程服务与管理系统技术规范
[3] CSAE 101-2018《智能网联汽车车载端信息安全技术要求》
[4] IPA Approaches for Connected Vehicle Security
[5] IPA Approaches for Vehicle Information Security
[6] EVITA Hardware Security Modules
[7] SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
[8] FIPS 140-2 Security requirements for cryptographic modules
[9] RFC 4086 Randomness Requirements for Security