ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 87.2-2022

车辆控制器信息安全技术要求
第 2 部分：车载信息交互系统

Technical requirements for information security of vehicle controller

Part 2: on board information interaction system

2022-10-23 发布　　2022-10-24 实施

吉林省汽车电子协会　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。

本文件是T/GHDQ 87-2022 《车辆控制器信息安全技术要求》的第2部分，T/GHDQ 87-2022由以下3个部分组成：

——第1部分：通用技术要求；

——第2部分：车载信息交互系统；

——第3部分：中央网关系统。

本文件由中国第一汽车集团有限公司智能网联开发院提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：吴淼、李木犀、高长胜、刘毅、边泽宇、陈明、高铭霞、邵馨蕊、胡闯、于欢、陈后立、杨雪珠。

本文件参与起草单位：武汉路特斯科技有限公司、吉林大学汽车仿真与控制国家重点实验室、中国汽车技术研究中心有限公司、长春师范大学汽车工程学院、一汽奔腾轿车有限公司、重庆长安汽车股份有限公司、北京车和家科技有限公司、一汽解放汽车有限公司、富赛汽车电子有限公司、东风汽车集团有限公司技术中心。

本文件参与起草人：刘建鑫、李杰、李宝田、任峰、李文强、汪向阳、张贤、董威、谷倩、赵岩、周海鹰。

本文件审查人：周时莹（中国第一汽车集团有限公司智能网联开发院）、卢放（岚图汽车科技有限公司）、何文（重庆长安汽车股份有限公司）、夏国强（中国汽车工程研究院股份有限公司）、孔晓霜(中国第一汽车集团有限公司创新技术研究院)。

本文件为首次发布。

引　言

车载信息交互系统安装在车辆上的对外通信系统，属于信息交互或娱乐服务装置，通常指远程通信通信系统、车载信息娱乐系统以及其混合体等。

车载信息交互系统一般具有对外通信功能，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；文化娱乐等相关服务功能。

车载信息交互系统作为车内外信息交互的通信枢纽，面临的信息安全威胁风险较高，因此在车辆控制器信息安全通用要求基础上，针对其特殊功能场景补充其相应信息安全技术要求，同时增加车载信息交互系统的控制器分级要求，指导进行车载信息交互系统的威胁和风险评估后结合整车成本和实现难度选择适合的保护等级。

车辆控制器信息安全技术要求　第2部分:车载信息交互系统

1　范围

本文件规定了车载信息交互系统的硬件、固件、操作系统、应用软件、车内外通信、升级功能、敏感数据存储、密码算法、入侵检测系统的安全技术要求，提出了技术验证要求，并明确了车载信息交互系统的信息安全分级要求。

本文件适用于指导车载信息交互系统信息安全技术的设计开发、验证和生产等工作。

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本文件；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 40856—2021　车载信息交互系统信息安全技术要求及试验方法

3　术语和定义

3.1

可信执行环境　trust execution environment

可信执行环境是与设备上的REE并存的运行环境，并且给REE提供安全服务。TEE所能访问的软硬件资源是与REE分离的，比REE的安全级别更高。TEE提供了授权安全软件(TA)的安全执行环境，同时也保护安全软件的资源和数据的保密性，完整性和访问权限。

3.2

工厂模式　factory method

车载信息娱乐系统通常会隐藏一些功能界面，即工厂模式，用于开发人员进行调试、设置配置等操作。

3.3

产线模式　production method

车辆出厂后车载信息娱乐系统的初始界面为二维码界面，用户购车后，需通过扫描二维码激活车载信息娱乐系统进入正常界面。

4　缩略语

下列缩略语适用于本文件：

APN——网络接入点（access point name）；

ECU-SL——控制器信息安全等级（ECU security level）；

IP——网际互连协议 (internet protocol);
REE——富执行环境 (rich execution environment);
TEE——可信执行环境 (trust execution environment);
TSP——汽车远程服务提供商(Telematics Service Provider);
WPA2-PSK——预共享密钥WiFi保护协议 (wifi protected access - preshared key)。

5 安全技术要求

5.1 硬件要求

车载信息交互系统的硬件安全应执行GB/T 40856—2021中5.1规定的防拆卸要求、电路板要求、芯片要求、调试口要求。

5.2 固件要求

车载信息交互系统的固件安全应执行GB/T 40856—2021中5.2规定的防读取保护、混淆保护要求。

5.3 操作系统

5.3.1 系统安全

车载信息交互系统的系统安全应执行GB/T 40856—2021中5.3.1规定的系统安全要求。

5.3.2 安全启动

车载信息交互系统在启动设计上应执行GB/T 40856—2021中5.3.2规定的安全启动要求。

5.3.3 可信执行环境

车载信息交互系统的操作系统应实现可信执行环境,可信执行环境TrustZone/TEE应满足可信执行环境的设计要求,遵循GlobalPlatform TEE、移动终端可信环境技术要求等行业规范。

5.3.4 系统权限控制

车载信息交互系统的操作系统在系统权限控制上应执行GB/T 40856—2021中5.3.3规定的系统权限控制要求。

5.3.5 强制系统访问控制

车载信息交互系统的操作系统应执行GB/T 40856—2021中5.3.4规定的强制系统访问控制要求。

5.3.6 系统日志输出

执行GB/T 40856—2021中5.3.5规定的系统日志输出安全要求。

5.3.7 系统日志审计

车载信息交互系统的系统日志审计应满足以下安全要求:
a) 车载信息交互系统应具有日志记录功能,日志包括用户操作、系统日志等;
b) 车载信息交互系统应对系统内存占用、文件资源占用等异常情况进行记录;
c) 在将车载信息交互系统的日志传输至车联网平台TSP时应满足安全传输协议要求。

5.3.8 边界防火墙

车载信息交互系统的边界防火墙应满足以下安全要求：

a） 车载信息交互系统应使用黑白名单配置功能，限制远程访问IP地址，只允许与TSP和授权的服务器建立通信，远程通信时禁止车载信息交互系统之间能互相访问，并禁止外网地址直接访问车载信息交互系统；

b） 车载信息交互系统应对流经的数据流进行访问控制、会话控制、攻击行为检测；

c） 车载信息交互系统的边界防火墙策略能通过软件升级等方式进行更新；

d） 边界防火墙应对不符合策略的数据进行拦截拒绝并记录日志。

5.3.9 浏览器安全

车载信息交互系统应使用高版本无公开漏洞的浏览器或禁止浏览器功能。

5.3.10 工厂模式安全

车载信息交互系统需要在量产版本中去掉工厂模式。若必须使用工厂模式，则需要满足以下要求：

a） 需设置进入工厂模式的密码，要求强复杂度且长度不少于8位，并对密码进行安全存储；

b） 严格保护工厂模式的启动逻辑，防止操作逻辑泄露；

c） 减少工厂模式中可以操作的功能、降低工厂模式的操作权限。

5.3.11 产线模式安全

车辆下线后，存在开发人员绕过二维码进入正常界面进行升级、测试、验证等操作的需求。为防止攻击者通过该入口进行非法操作，对绕过初始二维码进入正常界面的安全要求如下：

a） 需设置绕过初始二维码界面进入正常界面的密钥，并对密钥进行安全存储；

b） 对密钥进行严格管理，限制密钥发放人员；

c） 限制操作权限，不得提供除绕过二维码进入正常界面功能外的其它特殊权限；

d） 操作完成后，需恢复初始二维码界面，直到用户激活为止。

5.4 应用软件

5.4.1 应用软件基础要求

车载信息交互系统的应用软件基础要求应执行 GB/T 40856—2021中5.4.1规定的应用软件基础要求。

5.4.2 应用软件代码安全

车载信息交互系统的代码安全应执行 GB/T 40856—2021中5.4.2规定的应用软件代码安全要求。

5.4.3 应用软件访问控制

车载信息交互系统的代码安全应执行 GB/T 40856—2021中5.4.3规定的应用软件访问控制要求。

5.4.4 应用软件运行安全

车载信息交互系统的应用软件运行安全应执行 GB/T 40856—2021中5.4.4规定的应用软件运行安全要求。同时应满足以下运行安全要求：

a） 需要区别用户身份的应用软件运行前，需进行用户身份认证，登录页面要采取防暴力破解机制。对于使用账号登陆的应用软件，应使用强复杂度的口令，至少包括数字、大小写字母，长度不少于8位；

b） 应用软件不应含有非授权收集或泄露个人敏感信息、非法数据外传等恶意行为。应用软件不

应以明文形式存储个人敏感信息，如身份证件号码、交易信息、通信记录等，应使用系统提供的安全存储机制；

c） 对于支付密钥等敏感信息的输入，应采取安全措施确保个人敏感信息不被其他应用窃取；

d） 应用软件不应利用进程间通信提供传输敏感信息的接口，基于业务需求必须提供的，应在获得用户授权后，采取加密等防护措施后在传输。

5.4.5 应用软件通信安全

车载信息交互系统的应用软件运行安全应执行 GB/T 40856—2021中5.4.5规定的应用软件通信安全要求。

5.4.6 应用软件日志安全

车载信息交互系统的应用软件日志安全应执行 GB/T 40856—2021中5.4.6规定的应用软件日志安全要求。

5.4.7 应用软件升级安全

应用软件应满足以下升级安全要求：

a） 远程下载升级包的通道采用TLS1.2协议及以上或国产商用密码SSL VPN安全通道进行；

b） 升级包采用委托方颁发的证书进行签名保护完整性及合法性，系统下载完毕后需要进行签名验证；

c） 升级成功后删除升级文件。

5.5 车内外通信

5.5.1 车云通信

车载信息交互系统在车云通信中应满足以下安全要求：

a） 车载信息交互系统与车联网服务平台TSP通信应采用基于运营商专用网络构建的安全通信加密链路或者虚拟专用网络，与公网隔离，如使用APN通道；

b） 车载信息交互系统与车联网服务平台TSP的通信安全应基于安全传输通信协议，实现通信双方双向的身份认证和通信数据加密。

5.5.2 车内通信

车载信息交互系统的车内通信应执行GB/T 40856—2021中5.4规定的车内通信安全要求。

5.5.3 车车或车路通信

车载信息交互系统在直连通信的车车或车路通信过程中应满足以下安全要求：

a） 车载信息交互系统能对消息来源进行认证，保证接收到的消息是合法的；

b） 车载信息交互系统能对消息的完整性进行验证，并且能抗重放攻击，确保消息在传输时不被伪造、篡改、重放；

c） 车载信息交互系统应能消息的敏感数据进行机密性保护，确保消息的敏感数据在传输时不被窃听；

d) 车载信息交互系统需要对终端真实身份标识及位置等敏感信息进行安全保护。

5.5.4 Wi-Fi 应用

车载信息交互系统的Wi-Fi应用应满足以下安全要求：

a） 车载信息交互系统的Wi-Fi应用应执行 GB/T 40856—2021中5.2.1.5规定的车载WLAN 通信协议安全要求；
b） 车载信息交互系统的Wi-Fi的用户名和密码应满足每个设备均设置不相同的用户名和密码，密码至少包括数字、字母，长度不少于8位，且需要进行安全存储。在用户初次使用Wi-Fi时，车载信息交互系统应提示用户进行Wi-Fi用户名和密码的修改，密码的设置应满足限制要求，或者为用户提示安全风险；
c） 宜在车载信息交互界面提示用户进行MAC地址绑定操作，防止非授权设备接入。

5.5.5 蓝牙应用

车载信息交互系统的蓝牙应用安全应执行 GB/T 40856—2021中5.2.1.5中规定的车载蓝牙通信协议安全要求。

5.5.6 USB 应用

车载信息交互系统应限制USB模式，在量产状态时关闭USB调试、快速启动、下载模式等功能，或者增加使用高等级密码保护的权限控制。

5.6 升级功能

车载信息交互系统的升级安全执行GB/T 40856—2021中5.5规定的本地升级、远程升级安全要求。

5.7 敏感数据存储

车载信息交互系统的敏感数据存储应执行GB/T 40856—2021中5.6规定的敏感数据、硬件安全芯片、硬件安全模块、软件安全模块安全要求。

5.8 密码算法

车载信息交互系统使用的密码算法应执行GB/T 40856—2021中5.7规定的密码算法要求。

5.9 入侵检测系统

车载信息交互系统的入侵检测系统应执行GB/T 40856—2021中5.8规定的入侵检测系统要求。

5.10 虚拟化要求

车载信息交互系统的虚拟化应满足以下安全要求：
a） 虚拟化的系统只能访问分配给它的共享内存区域，进行读或写的操作，分配给其他虚拟化系统的内存区域不能访问；
b） 虚拟化的系统只能访问其正常操作所需的密码密钥。如通过设计存储器访问映射关系，指定哪些虚拟化的系统应该访问哪个存储器块；
c） 只允许在虚拟化的系统之间交换白名单中包含的消息；
d） 管理程序应强制执行以上策略，以确保虚拟化的系统只能访问有限(严格需要)数量的资源；
e） 车载信息交互系统的全部虚拟化系统都应遵循对操作系统、应用软件的安全要求。

6 技术验证要求

6.1 硬件验证

车载信息交互系统的硬件安全验证应执行GB/T 40856—2021中6.1规定的防拆卸验证、电路板验证、芯片验证、调试口验证要求。

6.2 固件验证

车载信息交互系统的固件安全验证应执行GB/T 40856—2021中6.2规定的防读取保护验证、混淆保护验证要求。

6.3 操作系统验证

6.3.1 系统安全验证

车载信息交互系统的系统安全验证应执行GB/T 40856—2021中6.3.1规定的系统安全验证要求。

6.3.2 安全启动验证

车载信息交互系统的启动验证应执行GB/T 40856—2021中6.3.2规定的安全启动验证要求。

6.3.3 可信执行环境验证

审查系统设计，判断是否采用了可信执行环境，检查可信执行环境TrustZone/TEE是否满足可信执行环境的设计要求，满足GlobalPlatform TEE、移动终端可信环境技术要求等行业规范。

6.3.4 系统权限控制验证

审查系统权限设计，应执行GB/T 40856—2021中6.3.3规定的系统权限控制验证要求。

6.3.5 强制系统访问控制验证

审查系统设计，应执行GB/T 40856—2021中6.3.4规定的强制系统访问控制验证要求。

6.3.6 系统日志输出验证

车载信息交互系统的系统日志输出验证应执行GB/T 40856—2021中6.3.5规定的系统日志输出验证要求。

6.3.7 系统日志审计验证

应按照下述方法验证是否满足系统日志审计要求：

a） 提取系统日志，检查是否包括用户操作、系统日志等内容；
b） 提取系统日志，检查是否包括系统内存占用、文件资源占用等异常情况；
c） 采用网络数据抓包工具进行数据抓包，解析传输数据，检查传输数据是否进行加密，是否进行身份认证。

6.3.8 边界防火墙验证

应按照下述方法验证是否满足边界防火墙要求：

a） 尝试连接非白名单地址，检查是否能正常访问；
b） 模拟数据流量，检查边界防火墙是否对数据进行合法性判断；
c） 更新边界防火墙策略，再进行恶意流量模拟，检查边界防火墙是否按照更新的策略处理；
d） 模拟恶意数据流量，检查边界防火墙日志记录内容。

6.4 应用软件验证

6.4.1 应用软件基础安全验证

车载信息交互系统的应用软件基础安全验证应执行 GB/T 40856—2021中6.4.1规定的应用软件基础安全试验。

6.4.2 应用软件代码安全验证

车载信息交互系统的应用软件代码安全验证应执行 GB/T 40856—2021中6.4.2规定的应用软件代码安全试验。

6.4.3 应用软件访问控制验证

车载信息交互系统的应用软件访问控制验证应执行 GB/T 40856—2021中6.4.3规定的应用软件访问控制试验。

6.4.4 应用软件运行安全验证

车载信息交互系统的应用软件运行安全验证应执行 GB/T 40856—2021中6.4.4规定的应用软件运行安全试验。

6.4.5 应用软件通信安全验证

车载信息交互系统的应用软件通信安全验证应执行 GB/T 40856—2021中6.4.5规定的应用软件通信安全试验。

6.4.6 应用软件日志安全验证

车载信息交互系统的应用软件日志安全验证应执行 GB/T 40856—2021中6.4.6规定的应用软件日志安全试验。

6.4.7 应用软件升级安全验证

应按照下述方法验证是否满足应用软件升级安全要求：

a） 远程升级采用网络抓包分析下载通道采用TLS1.2协议及以上或国产商用密码SSL VPN安全通道进行；

b） 下载非委托方证书签名的升级包，验证是否能成功安装；

c） 应用软件升级完毕，检查车载信息娱乐系统中是否残留升级文件。

6.5 车内外通信验证

6.5.1 车云通信验证

应按照下述方法验证是否满足车云通信要求：

a） 尝试在车载信息交互系统与车联网服务平台TSP使用的通信通道访问公网，检查车载信息交互系统与车联网服务平台TSP使用的通信通道是否与公网隔离；

b） 采用网络数据抓包工具进行数据抓包，解析传输数据，检查传输数据是否进行加密，是否进行身份认证。

6.5.2 车内通信验证

车载信息交互系统的车内通信验证应执行GB/T 40856—2021中6.4规定的车内通信验证要求。

6.5.3 车车或车路通信验证

应按照下述方法验证是否满足车车或车路通信要求：

a） 采用网络数据抓包工具进行数据抓包，解析传输数据，检查传输敏感数据是否进行加密，是否进行身份认证；

b） 采用网络数据抓包工具进行数据抓包，解析传输数据，检查终端真实身份标识及位置等敏感信息是否能被获取或关联。

6.5.4 Wi-Fi 应用验证

应按照下述方法验证是否满足Wi-Fi应用要求：

a） 车载信息交互系统的Wi-Fi应用验证应执行 GB/T 40856—2021中6.2.1.3规定的车载WLAN 通信协议安全要求；

b） 尝试连接Wi-Fi，检查密码是否符合复杂度要求；尝试修改密码，检查是否有密码复杂度检查。

6.5.5 蓝牙应用验证

车载信息交互系统的蓝牙应用验证应执行GB/T 40856—2021中规定的6.2.1.5.2 蓝牙通信协议安全测试方法。

6.5.6 USB 应用验证

尝试使用车载信息交互系统的USB，检查是否可以通过USB接口进行USB调试、快速启动、下载模式等功能，或者是否增加了高等级密码保护的权限控制。

6.6 升级功能验证

车载信息交互系统的升级安全验证应执行GB/T 40856—2021中6.5规定的本地升级验证、远程升级验证要求。

6.7 敏感数据存储验证

车载信息交互系统的敏感数据存储验证应执行GB/T 40856—2021中6.6规定的敏感数据验证、硬件安全芯片验证、硬件安全模块验证、软件安全模块验证要求。

6.8 密码算法验证

验证车载信息交互系统使用的密码算法应执行GB/T 40856—2021中6.7规定的密码算法验证要求。

6.9 入侵检测系统验证

验证车载信息交互系统的态势感知与入侵检测系统应执行GB/T 40856—2021中6.8规定的入侵检测系统验证要求。

6.10 虚拟化验证

车载信息交互系统的虚拟化应满足以下安全要求：

a） 通过调试系统，检查虚拟化的系统只能访问分配给它的共享内存区域，进行读或写的操作，不能访问分配给其他虚拟化系统的内存区域；

b） 通过调试系统，检查只允许在虚拟化的系统之间交换白名单中包含的消息。

7 分级要求

7.1 分级关系

根据攻击风险和防御成本的平衡考虑，车载信息交互系统的防护强度分为三个级别。应在进行车载信息交互系统的威胁和风险评估后结合整车成本和实现难度选择适合的保护等级。

7.2 分级描述

参照GB/T 40856—2021中7.2的ECU-SL1、ECU-SL2和ECU-SL3分级描述。

7.3 分级要求

硬件要求、固件要求、系统安全、安全启动、系统权限控制、强制系统访问控制、系统日志输出、车内通信、本地升级、远程升级、敏感数据存储、密码算法等要求的信息安全等级划分参照GB/T 40856—2021中7.3的表1控制器信息安全分级，其他安全要求的具体等级划分详见表1。

表1 车载信息交互系统信息安全分级

安全技术要求	ECU-SL1	ECU-SL2	ECU-SL3
硬件安全-防拆卸要求	●	●	●
硬件安全-电路板要求			●
硬件安全-芯片要求			●
硬件安全-调试口要求	●	●	●
固件安全-防读取保护	●	●	●
固件安全-混淆保护			●
操作系统-系统安全	●	●	●
操作系统-安全启动	●	●	●
操作系统-可信执行环境		●	●
操作系统-系统权限控制		●	●
操作系统-强制系统访问控制			●
操作系统-系统日志输出	●	●	●
操作系统-系统日志审计			●
操作系统-边界防火墙	●	●	●
操作系统-浏览器安全	●	●	●
操作系统-工厂模式安全	●	●	●
操作系统-产线模式安全	●	●	●
应用软件-基础要求	●	●	●
应用软件-代码安全	●	●	●
应用软件-访问控制	●	●	●
应用软件-运行安全	●	●	●
应用软件-通信安全	●	●	●
应用软件-日志安全	●	●	●
应用软件-升级安全	●	●	●
车内外通信-车云通信	●	●	●
车内外通信-车内通信	●	●	●
车内外通信-车车或车路通信	●	●	●

表 1　车载信息交互系统信息安全分级（续）

安全技术要求	ECU-SL1	ECU-SL2	ECU-SL3
车内外通信-Wi-Fi应用	●	●	
车内外通信-蓝牙应用	●	●	●
车内外通信-USB应用	●	●	●
升级功能-本地升级	●	●	●
升级功能-远程升级	●	●	●
敏感数据存储-敏感数据	●	●	●
敏感数据存储-安全芯片		●	●
敏感数据存储-硬件安全模块		●	●
敏感数据存储-软件安全模块	●	●	
密码算法	●	●	●
入侵检测系统		●	●
虚拟化要求	●	●	●