ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 87.1-2022

车辆控制器信息安全技术要求
第 1 部分：通用技术要求

Technical requirements for information security of vehicle controller

Part 1: General technical requirements

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

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

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

近年来，我国智能网联汽车产业高速发展，汽车逐渐从封闭系统向智能化系统、开放性系统演进，如增加了LTE、蓝牙、wifi各种对外通信接口，娱乐应用、远程升级、远程控制、V2X等联网功能，信息安全越来越得到关注与重视，保护相关的安全资产及功能免受威胁。由于车辆对外接口的增多、攻击手段的提升，使得整车控制器都具有被入侵的风险，因此，有必要编制车辆控制器的信息安全技术要求，对整车控制器以形成通用的、标准化的信息安全技术要求，设置车辆控制器的信息安全基准线。

车辆控制器信息安全技术要求　第1部分：通用技术要求

1　范围

本文件规定了车辆控制器的硬件、固件、操作系统、车内通信、升级功能、敏感数据存储、密码算法的通用安全技术要求，提出了技术验证要求，并明确了控制器的信息安全分级要求。

本文件适用于指导车辆控制器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

GB/T 40857-2021　汽车网关信息安全技术要求及试验方法

GB/T 40861-2021　汽车信息安全通用技术要求

3　术语和定义

3.1

重放攻击　replay attacks

重放攻击是指攻击者通过记录通信会话，并在以后某个时刻重放整个会话或者会话的一部分，以达到欺骗系统的目的。

3.2

侧信道攻击　side channel attack

侧信道攻击是针对车载加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露而对加密设备进行攻击的方式。

3.3

漏洞扫描工具　vulnerability scanner

漏洞扫描工具是指基于权威漏洞平台漏洞数据库，通过扫描等手段对系统或应用的安全脆弱性进行检测，发现可利用漏洞的一种安全检测工具。

3.4

安全芯片　secure element

可独立含有密码算法、内部拥有独立的处理器和存储单元，可实现密钥管理机制的集成电路芯片。

3.5

硬件安全模块 hardware security module

硬件安全模块(HSM)应是ECU中使用的微处理器/微控制器中的专用可重新编程安全子系统。HSM应提供先进的安全功能、安全存储、安全高效地实施密码操作。

3.6

软件安全模块 secure software modules

通过软件密码算法形式，可以实现运算、加密等操作的软件模块。

3.7

密码数据 cryptographi material

密码数据指的是与密码学运算相关的密钥、数字证书、随机数等密码学相关数据材料。

3.8

入侵检测系统 intrusion detection system

入侵检测系统是一种对车辆文件异常访问读写，异常流量使用，资源异常占用，系统配置修改等异常信息进行即时监视，在发现这些可疑数据行为时，进行异常记录并发出警报的系统。

4 缩略语

下列缩略语适用于本文件：

ADB——安卓调试桥 (android debug bridge)；
APN——网络接入点 (access point name)；
BGA——球栅阵列封装 （ball grid array）；
ECU-SL——控制器信息安全等级（ECU security level）；
IP——网际互连协议 (internet protocol)；
JTAG——联合测试工作组 （joint test action group）；
REE——富执行环境 (rich execution environment)；
RTOS——实时操作系统 (real time operating system)；
TEE——可信执行环境 (trust execution environment)；
TSP——汽车远程服务提供商(Telematics Service Provider)；
UART——通用异步收发传输器 (universal asynchronous receiver transmitter)；
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

5.1.1 防拆卸要求

控制器在防拆卸设计上应对控制器硬件的封装（外壳、封条等）进行完整性保护。

5.1.2 电路板要求

控制器在电路板设计上应满足以下安全要求：

a） 控制器的主控芯片和MCU芯片的输入、输出测试点不应在电路板上暴露；

b） 控制器的电路板上不应存在用以标注芯片端口和管脚功能的可读丝印；

c） 控制器电路板上芯片之间的关键通信线路宜采用内层布线方式进行线路隐蔽。

5.1.3 芯片要求

控制器在芯片设计上应满足以下安全要求：

a） 宜去除控制器电路板上具备数据处理及运算能力的芯片的丝印；

b） 控制器的主控芯片不宜暴露输入和输出引脚，控制器芯片宜采用BGA封装的芯片，增加引出芯片调试端口的难度；

c） 对控制器的数据存储芯片进行点胶处理，应使用具有芯片防拆功能的胶，增加攻击者拆解芯片和探测芯片间的传输数据的难度。

5.1.4 调试接口要求

控制器在调试接口设计上应满足以下安全要求：

a） 控制器不应存在对芯片内存进行未授权访问或者更改芯片功能的隐蔽接口；

b） 控制器在量产时壳体不应带有具有调试功能的接口，如UART接口、JTAG接口、USB接口；

c） 控制器在量产时应封闭具有调试功能的接口，如 UART接口、JTAG接口、USB接口、SSH接口、ADB接口等,在软件层面上关闭接口调试功能;如果控制器在量产时需要调试器端口保持运行，则需要采用身份认证等方式对调试口访问权限进行控制，并移除root权限。

d） 控制器使用的4G/5G、蓝牙、Wi-Fi模块等外围设备的调试接口应全部关闭，避免重要数据通过第三方设备泄露。

e） 控制器可以保留用于打印日志的输出接口，并采用身份认证机制，输出日志不应带有敏感信息，如密钥信息、关键配置信息、服务器信息、个人敏感信息等。

5.2 固件要求

5.2.1 防读取保护

控制器在芯片设计上宜具备固件防读取保护措施，在使用芯片时应选择开启固件防读保护功能。

5.2.2 混淆保护

控制器宜对固件进行混淆或特殊编译处理，提升敏感逻辑分析难度，避免固件代码被逆向分析。

5.3 操作系统

5.3.1 系统安全

控制器的linux、Android、QNX等操作系统应满足以下信息安全要求：

a） 控制器的操作系统应选择已经修复权威漏洞平台发布6个月及以上的高危安全漏洞的系统版本；

b） 控制器的操作系统应关闭没有使用到的服务；

c） 控制器的操作系统不应存在后门；

d） 控制器的操作系统的登陆权限应使用强复杂度的口令进行登陆；

e） 控制器必须关闭所有业务未用到的端口，禁止开放未使用的公共约定端口，实现端口服务最小化。

5.3.2 安全启动

控制器的linux、Android、QNX等操作系统、MCU的RTOS系统以及其他的嵌入式操作系统在启动设计上应满足以下安全要求：

a） 控制器的操作系统在加载之前应校验bootloader和系统的合法性，即该系统是可信任的；
b） 控制器的操作系统在加载之前应校验系统的完整性，即该系统是未被篡改过的；
c） 控制器的操作系统的启动应基于安全存储的密钥以及安全的运算环境。

5.3.3 系统权限控制

控制器的linux、Android、QNX等操作系统在系统权限控制上应根据业务功能明确最小化服务权限，对系统核心资源的访问进行权限限制，如根目录、内核文件、日志文件的访问权限等。

5.3.4 强制系统访问控制

控制器的linux、Android等操作系统应使用seLinux、seAndroid等强制访问控制系统。

5.3.5 系统日志输出

应限制控制器的日志输出内容，禁止输出包含密钥信息、关键配置信息、服务器信息等敏感信息。

5.4 车内外通信

5.4.1 车内通信

控制器的车内通信应满足以下安全要求：

a） 通过CAN或CANFD进行通信传输的关键报文，关键报文应进行完整性和可用性保护，包括核心控制类报文，如远控启动报文等；
b） 通过车载以太网进行通信传输的关键数据，关键数据应进行完整性和可用性保护，敏感数据传输应进行机密性保护；
c） 控制器的车内通信应与车外通信应能进行物理隔离或路由隔离；
d） 控制器应对CAN通信设置通信报文ID的白名单过滤。

5.4.2 车外通信

控制器的车外通信应满足以下安全要求：

a） 控制器需要采用基于身份认证的方式建立连接，即保证对端通信身份的真实性；
b） 通信数据应进行完整性、可用性和机密性保护。

5.5 升级功能

5.5.1 本地升级

控制器的本地升级应满足以下安全要求：

a） 控制器需要校验升级文件的合法性，即该升级文件是来自厂商的，是可以被信任的；
b） 控制器需要校验升级文件的完整性，即该升级文件是未被篡改过的；
c） 当升级失败时，控制器应能恢复到可用版本或通过其他方式恢复控制器功能。

5.5.2 远程升级

控制器的远程升级应满足以下安全要求：

a） 控制器作为远程升级主控节点时，需要能对远程升级服务端的身份进行验证，并对远程升级交互指令进行解密；
b） 控制器作为远程升级主控节点时，需要能对升级文件进行解密；
c） 控制器能对升级文件的完整性和合法性进行检验；
d） 当升级失败时，控制器应能恢复到可用版本或通过其他方式恢复控制器功能。

5.6 敏感数据存储

5.6.1 敏感数据

控制器的敏感数据应满足以下安全要求：
a） 根据控制器的功能和应用场景识别敏感数据，如关键配置文件、设备唯一识别信息、密钥信息、证书信息等；
b） 控制器的敏感数据应进行安全存储保护。

5.6.2 安全芯片

如果控制器具备并使用安全芯片，应满足以下安全要求：
a） 敏感数据存储在控制器的安全芯片中；
b） 基于采用的安全芯片，写入控制器硬件安全芯片中的敏感信息无法非授权获取或者篡改；
c） 控制器的硬件安全芯片应具备对抗侧信道攻击的保密性,关键数据不被侧信道攻击暴露信息；
d） 控制器的硬件安全芯片应具备对抗故障注入攻击的健壮性、保障关键流程不被故障注入攻击改变运行逻辑；
e） 控制器的硬件安全芯片应支持密码算法要求中所需要的运算能力；
f） 控制器的硬件安全芯片应具有检测与处置非授权访问的机制。

5.6.3 硬件安全模块

如果控制器具备并使用硬件安全模块，应满足以下安全要求：
a） 敏感数据存储于硬件安全模块中；
b） 基于硬件安全模块，写入控制器的敏感信息无法非授权获取或者篡改；
c） 控制器的硬件安全模块应支持密码算法要求中所需要的运算能力。

5.6.4 软件安全模块

如果控制器不具备安全芯片和硬件安全模块，控制器必须使用软件安全模块实现安全存储，应满足以下安全要求：
a） 控制器应使用软件安全模块对敏感数据进行存储和隔离，如基于TrustZone和TEE安全执行环境提供的可信根的安全存储模块；
b） 控制器的软件安全模块应进行代码混淆保护。

5.7 密码算法

控制器为实现以上信息安全要求所使用到的密码算法应满足以下安全要求：
a） 身份认证宜采用数字证书机制，数字证书应能关联控制器的唯一标识；
b） 对称加密算法推荐采用SM4对称加密算法，密钥长度128位，如不具备使用国产商用密码算法条件，要求采用AES算法，密钥长度不低于128位；
c） 非对称加密算法推荐采用SM2非对称加密算法，密钥长度256位，如不具备使用国产商用密码算法条件，要求采用RSA算法，密钥长度不低于2048位；

d） 哈希算法推荐采用SM3哈希算法,如不具备使用国产商用密码算法条件，要求采用SHA256或以上；
e） 控制器的一个密钥或证书只能用于一项业务的加解密或签名验签服务。

5.8 入侵检测系统

入侵检测系统应满足以下安全要求：
a） 控制器的入侵检测系统应能进行系统监控，流量监控，资源监控，异常行为监控等功能；
b） 控制器应对入侵检测系统检测到的异常数据及文件进行记录；
c） 控制器需要根据设计策略，将异常数据、文件上传至入侵检测云端服务器。

6 技术验证要求

6.1 硬件验证

6.1.1 防拆卸验证

通过采用开盒方式观察控制器总成的封装是否使用了完整性保护，如拆卸后是否留下痕迹。

6.1.2 电路板验证

应按照下述方法验证是否满足电路板要求：
a） 通过采用开盒观察方法，检查电路板上是否存在主控芯片和MCU芯片的输入、输出测试点；
b） 通过采用开盒观察方法，检查电路板上是否存在用以标注芯片端口和管脚功能的可读丝印；
c） 通过采用开盒观察方法，检查电路板上核心芯片之间的通信线路是否已经被隐蔽。

6.1.3 芯片验证

应按照下述方法验证是否满足芯片要求：
a） 通过采用开盒观察方法，检查具备数据处理及运算能力的芯片丝印是否可读；
b） 通过采用开盒观察方法，检查主控芯片的输入和输出引脚是否被暴露；
c） 通过采用开盒观察方法，检查数据存储芯片是否使用了芯片防拆胶。

6.1.4 调试口验证

应按照下述方法验证是否满足调试口要求：
a） 通过采用开盒观察方法，使用光学放大镜，检查电路板是否存在隐蔽接口；
b） 观察控制器的壳体是否带有具有调试功能的接口；
c） 通过采用开盒观察方法，观察电路板中是否存在暴露的调试接口，如果存在则使用测试工具检查是否具有调试权限；
d） 连接调试接口，使用测试工具检查调试口是否具有调试权限；
e） 通过采用开盒观察方法，检查调试口，或审查相应文档，判断是否已经关闭全部外围设备的调试接口功能；
f） 通过连接日志输出接口，检查日志输出接口输出的日志是否携带敏感信息。

6.2 固件验证

6.2.1 防读取保护验证

检查MCU、主控芯片和通信模组的芯片手册和设置，核对是否具备固件防读取保护功能，并查看是否正常开启了固件防读取保护功能，验证是否满足防读取保护要求。

6.2.2 混淆保护验证

使用逆向工具进行代码分析，检查固件代码，验证是否满足混淆保护要求。

6.3 系统验证

6.3.1 系统安全验证

应按照下述方法验证是否满足系统安全要求：

a） 查看系统版本，并使用漏洞扫描工具对操作系统进行漏洞检测，检查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；
b） 查看正在运行的应用服务，检查是否关闭了没有使用到的应用服务；
c） 尝试登陆系统，检查口令的复杂度；
d） 通过端口扫描，检查是否存在业务未用到的端口。

6.3.2 安全启动验证

应按照下述方法验证是否满足安全启动要求：

a） 提取系统签名部分，使用软件调试工具对签名部分进行篡改，检查是否能正常运行；
b） 提取系统代码部分，使用软件调试工具对系统代码部分进行篡改，检查是否能正常运行；
c） 审查安全存储设计，使用软件调试工具尝试写入密钥或证书，检查是否可以写入安全存储区域。

6.3.3 系统权限控制验证

审查系统权限设计，使用授权身份对目标资源进行操作（读、写等），检查操作是否可以成功；使用非授权身份对目标资源进行操作（读、写等），检查操作是否失败。

6.3.4 强制系统访问控制验证

审查系统设计，检查是否使用强制访问控制系统。

6.3.5 系统日志输出验证

通过连接日志输出接口，检查输出的日志是否携带敏感信息。

6.4 车内外通信验证

6.4.1 车内通信验证

应按照下述方法验证是否满足车内通信要求：

a） 接入CAN或CAN FD网络中，截取报文数据，篡改数据后发送，检查是否判断了数据的完整性；
b） 接入车载以太网网络中，截取报文数据，检查是否是明文数据，篡改数据后发送，检查是否判断了数据的完整性；
c） 通过尝试访问不同区域网络，检查车内通信应与车外通信是否进行隔离；
d） 接入CAN网络，尝试在网络中发送非合法报文ID的CAN报文，检查控制器是否处理该报文。

6.4.2 车外通信验证

应按照下述方法验证是否满足车外通信要求：

a） 采用网络数据抓包工具进行数据抓包，检查数据是否进行身份认证；

b） 采用网络数据抓包工具解析传输数据，检查传输数据是否进行加密。

6.5 升级功能验证

6.5.1 本地升级验证

应按照下述方法验证是否满足本地升级应用要求：

a） 篡改升级文件的签名，使用软件刷写工具，检查升级文件是否会被执行；

b） 篡改升级文件的数据包文件，使用软件刷写工具，检查升级文件是否会被执行；

c） 使用软件刷写工具，执行一次失败的刷写过程，检查是否能恢复到更新前的版本。

6.5.2 远程升级验证

应按照下述方法验证是否满足远程升级应用要求：

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

b） 检查收到的升级文件，检查升级文件是否是明文；

c） 篡改升级文件的签名，再次通过远程下发，检查升级文件是否会被执行；篡改升级文件的数据包文件，再次通过远程下发，检查升级文件是否会被执行；

d） 执行一次失败的远程升级过程，检查是否能恢复到更新前的版本。

6.6 敏感数据存储验证

6.6.1 敏感数据验证

应按照下述方法验证是否满足敏感数据要求：

a） 查看业务数据，检查敏感数据的分类是否合理；

b） 尝试读取敏感数据，检查敏感数据是否进行加密保护。

6.6.2 安全芯片验证

应按照下述方法验证是否满足安全芯片要求：

a） 检查敏感数据是否进行加密保护；

b） 使用软件调试工具，尝试获取或者篡改敏感数据，检查是否能更改敏感数据；

c） 使用侧信道攻击等攻击手段，尝试获取敏感数据，检查是否能抵抗这种攻击手段；

d） 使用故障注入攻击等手段，尝试改变代码执行逻辑，检查是否能抵抗这种攻击手段；

e） 审查安全芯片手册，检查控制器的安全芯片是否支持密码算法要求中所需要的运算能力；

f） 使用非授权身份，检查控制器的安全芯片是否能检测并处置非授权访问。

6.6.3 硬件安全模块验证

应按照下述方法验证是否满足硬件安全模块要求：

a） 检查敏感数据是否进行加密保护；

b） 使用软件调试工具，尝试获取或者篡改敏感数据，检查是否能读取、修改敏感数据；

c） 审查硬件安全模块手册，检查控制器的硬件安全模块是否支持密码算法要求中所需要的运算能力。

6.6.4 软件安全模块验证

应按照下述方法验证是否满足软件安全模块要求：

a） 检查敏感数据是否进行加密保护；

b） 使用逆向工具进行代码分析，检查软件安全模块代码是否能保护敏感数据信息。

6.7 密码算法验证

通过审查设计文件，检查是否满足密码算法要求。

6.8 入侵检测系统验证

应按照下述方法验证是否满足入侵检测系统要求：

a） 模拟异常情况，检查控制器的入侵检测系统是否能捕获异常情况；

b） 模拟异常情况，检查控制器的入侵检测系统是否对异常情况进行记录；

c） 模拟异常情况，检查入侵检测云端服务器是否记录了异常情况。

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，控制器的防护强度分为三个级别。应在进行控制器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

7.2.1 ECU-SL1 级

ECU-SL1级属于基础保护级，是防护强度最低的一级，符合ECU-SL1级别的控制器具备基本的控制器信息安全防护要求以及通信安全要求，能达到避免较容易的被非授权获取敏感信息或数据的恶意行为，能基本保证控制器不会由于信息安全问题影响控制器基本功能。

7.2.2 ECU-SL2 级

ECU-SL2级是在ECU-SL1级基础上提高对系统权限控制的安全要求，增加安全监控和审计要求，能根据监控或审计结果进行动态安全防护，达到自主动态防御的能力。

7.2.3 ECU-SL3 级

ECU-SL3级在ECU-SL2级别基础上提高信息安全的硬件要求、固件要求，加强安全技术的有效性和可靠性，达到全面的控制器防御能力。

7.3 分级要求

具体的等级划分详见表1。

表1　控制器信息安全分级

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-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	●	●	●
车内外通信-车内通信	●	●	●
车内外通信-车外通信	●	●	●
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		●	●