ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 87.3-2022

车辆控制器信息安全技术要求
第 3 部分：中央网关系统

Technical requirements for information security of vehicle controller

Part 3: central gateway 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3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：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、武汉路特斯科技有限公司、中国汽车技术研究中心有限公司、一汽奔腾轿车有限公司、一汽解放汽车有限公司、富赛汽车电子有限公司、重庆长安汽车股份有限公司、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。

本文件参与起草人：李杰、任峰、刘建鑫、朱永健、李文强、谷倩、赵岩、汪向阳、谭成宇、周海鹰、董威。

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

汽车中央网关作为整车网络的数据交互枢纽，是整车电子电气构架中的核心部件，使数据在车辆内部的多个网络中安全可靠得进行传输是其核心功能。网关作为汽车网络系统的核心控制装置，负责协调不同网络之间的通信协议转换、网络隔离、数据交换、故障诊断等工作。汽车中央网关依据网络拓扑结构一般分为CAN网关、以太网网关及混合型网关。汽车中央网关作为车内网络枢纽，有必要在车辆控制器通用信息安全技术要求之上，补充其个性化信息安全技术要求。

车辆控制器信息安全技术要求　第3部分：中央网关系统

1　范围

本文件规定了中央网关硬件、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，并明确了中央网关的信息安全分级要求。

本文件适用于指导中央网关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 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

GB/T 40861-2021 界定的以及下列术语和定义适用于本文件。

3.1

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。

3.2

汽车网关　vehicle gateway

用于安全可靠地在车辆内的多个网络间进行数据转发和传输的电子控制单元，也称中央网关。

3.3

DoS攻击　denial of service attack

即拒绝服务攻击，用数据包淹没本地系统，使得所有可用的操作系统资源都被消耗殆尽，导致服务器无法处理合法用户的请求。

4　缩略语

下列缩略语适用于本文件：

ACM——访问控制（Access Control Mode）；

APN——网络接入点（Access Point Name）；

CAN——控制器局域网络（Controller Area Network）；
ECU-SL——控制器信息安全等级（ECU security level）；
ID——身份标识号（Identity Document）；
MCU——微控制单元（Microcontroller Unit）；
OBD——车载自诊断（On-Board Diagnostics）；
OTA——空中下载技术（Over the Air）；
TSP——汽车远程服务提供商（Telematics Service Provider）；
UDS——标准诊断协议（Unified Diagnostic Services）。

5 安全技术要求

5.1 硬件要求

中央网关的硬件安全应执行GB/T 40857-2021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

中央网关的固件安全应执行GB/T 40857-2021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

中央网关的linux、Android或者QNX系统应执行GB/T 40857-2021中5.3.1规定的系统安全要求。

5.3.2 安全启动

中央网关的linux、Android或者QNX系统和MCU实时操作系统在启动设计上应执行GB/T 40857-2021中5.3.2规定的安全启动要求。

5.3.3 系统权限控制

中央网关的linux、Android或者QNX系统在系统权限控制上应执行GB/T 40857-2021中5.3.3规定的系统权限控制要求。

5.3.4 强制系统访问控制

中央网关的linux、Android或者QNX系统应执行GB/T 40857-2021中5.3.4规定的强制系统访问控制要求。

5.3.5 系统日志输出

执行GB/T 40857-2021中5.3.5规定的系统日志输出安全要求。

5.3.6 系统日志审计

中央网关的系统日志审计应满足以下安全要求：
a） 中央网关应具有日志记录功能，日志包括用户操作、系统日志等；
b） 中央网关应对系统内存占用、文件资源占用等异常情况进行记录；
c） 中央网关应具备通讯流量的异常监控记录；

d) 在将中央网关的日志传输至车联网平台TSP时应满足安全传输协议要求。

注：宜对中央网关的日志进行安全存储。

5.3.7 CAN 防火墙

中央网关的CAN防火墙应设置白名单，按照白名单所定义的校验规则进行报文路由。白名单校验规则包括：

a） 报文ID检测：应进行报文ID检测，将收到的报文ID与白名单中的定义进行一致性校验，否则不允许转发；

b） 报文长度检测：应进行报文长度检测，将收到的报文长度与白名单中的定义进行一致性校验，否则不允许转发；

c） 报文频率检测：宜进行报文频率检测，将收到的报文频率与白名单中的定义进行一致性校验，否则不允许转发。

5.3.8 以太网防火墙

中央网关的以太网防火墙应满足以下安全要求：

a） 中央网关应支持网络分域；

b） 中央网关应设置基于IP地址过滤、MAC地址过滤、VLAN划分等机制的访问控制策略，对不符合访问控制策略的数据包进行拦截、丢弃、记录等；

c） 中央网关应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。

5.3.9 拒绝服务攻击检测

中央网关的拒绝服务攻击检测应执行GB/T 40857-2021中6.2.1.2及6.2.2.3规定的拒绝服务攻击检测要求。

5.3.10 OBD 接口防护

中央网关作为OBD诊断入口时，应满足OBD接口防护的相关安全要求：

a） 针对UDS设置完整的ACM，定义每个UDS请求的权限等级；

b） 按照ACM检查诊断设备的UDS请求，对于低权限可直接进行诊断的UDS请求路由至目标ECU；

c） 按照ACM检查诊断设备的UDS请求，对于发出高权限UDS请求的诊断设备进行身份认证，确认诊断设备的合法性后再将请求路由至目标ECU。

5.4 应用软件

中央网关的非实时操作系统应用软件应满足以下安全要求：

a） 中央网关的应用软件不应进行非授权收集用户隐私、泄露用户隐私、非法数据外传等恶意行为；

b） 中央网关的应用软件如果存在后装应用，系统应对第三方后装应用软件在系统中的运行或安装进行限制；

c） 中央网关的应用软件的核心代码宜使用混淆、加壳、加密等安全机制以提高应用程序被逆向的成本；

d） 中央网关应用软件不应使用带有已知能构成威胁的高危漏洞或者后门等问题的开源库。

5.5 车内外通信

5.5.1 车云通信

中央网关与车联网服务平台（如TSP、OTA平台等）的通信安全应基于安全传输通信协议，实现通信双方的身份认证和通信数据加密。

5.5.2 车内通信

中央网关的车内通信应执行GB/T 40857-2021中5.4规定的车内通信安全要求。

5.6 升级功能

中央网关的升级安全执行GB/T 40857-2021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

中央网关的敏感数据存储应执行GB/T 40857-2021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

中央网关使用的密码算法应执行GB/T 40857-2021中5.7规定的密码算法要求。

5.9 入侵检测系统

中央网关应具备入侵检测系统，并满足以下安全要求：

a） 中央网关的入侵检测系统应能检测整车网络报文的长度异常，周期异常，信号路由异常，信号阈值异常，负载异常，诊断报文异常等情况；

b） 中央网关应对入侵检测系统检测到的异常数据及文件进行记录；

c） 中央网关应根据设计策略，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

中央网关的硬件安全验证应执行GB/T 40857-2021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

中央网关的固件安全验证应执行GB/T 40857-2021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

中央网关的系统安全验证应执行GB/T 40857-2021中6.3.1规定的系统安全验证要求。

6.3.2 安全启动验证

中央网关的启动验证应执行GB/T 40857-2021中6.3.2规定的安全启动验证要求。

6.3.3 系统权限控制验证

审查系统权限设计，应执行GB/T 40857-2021中6.3.3规定的系统权限控制验证要求。

6.3.4 强制系统访问控制验证

审查系统设计，应执行GB/T 40857-2021中6.3.4规定的强制系统访问控制验证要求。

6.3.5 系统日志输出验证

中央网关的系统日志输出验证应执行GB/T 40857-2021中6.3.5规定的系统日志输出验证要求。

6.3.6 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。

6.3.7 CAN 防火墙验证

应按照下述方法验证是否满足CAN防火墙要求：

a） 模拟发送报文格式为白名单定义的报文，检查中央网关是否正常路由；
b） 模拟发送报文ID为非白名单定义的报文，检查中央网关是否拒绝路由；
c） 模拟发送报文长度为非白名单定义的报文，检查中央网关是否拒绝路由；
d） 模拟发送报文频率为非白名单定义的报文，检查中央网关是否拒绝路由。

6.3.8 拒绝服务攻击检测验证

应按照下述方法验证是否满足拒绝服务攻击检测要求：

a） CAN网络拒绝服务攻击检测验证应执行GB/T 40857-2021中7.2.1 c)d)规定的进行检测验证；
b） 以太网网络拒绝服务攻击检测验证应执行GB/T 40857-2021中7.2.2 d)规定的进行检测验证。

6.3.9 以太网防火墙验证

应按照下述方法验证是否满足以太网防火墙要求：

a） 审查是否进行网络分域；
b） 通过端口扫描，检查是否存在业务未用到的端口；
c） 尝试连接非白名单地址，检查是否能正常访问；
d） 审查是否对非法数据的处理进行记录。

6.3.10 OBD 接口防护验证

应按照下述方法验证是否满足OBD接口防护要求

a） 审查配置的ACM，是否对UDS进行权限分级；
b） 使用合法诊断设备连接网关，检查身份认证是否成功，认证成功后是否能路由高权限等级UDS请求；
c） 使用未经认证的非法诊断设备连接中央网关，检查是否能路由低权限等级UDS请求，是否拒绝路由高权限等级UDS请求。

6.4 应用软件验证

应按照下述方法验证是否满足应用软件要求：

a） 对应用软件中数据进行分析，检查应用软件对个人敏感信息是否非授权收集、泄露或外传；

b） 尝试在系统环境下是否可以安装或运行非法软件；

c） 使用逆向工具进行代码分析，检查应用软件代码，检查是否满足混淆、加壳、加密等保护要求；

d） 使用漏洞扫描工具对应用软件进行漏洞检测，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。

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） 尝试使用中央网关与车联网服务后台（如TSP、OTA平台等）的通信通道访问公网，检查中央网关与车联网服务平台后台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

中央网关的车内通信验证应执行GB/T 40857-2021中6.4规定的车内通信验证要求。

6.6 升级功能验证

中央网关的升级安全验证应执行GB/T 40857-2021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

中央网关的敏感数据存储验证应执行GB/T 40857-2021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

中央网关使用的密码算法应执行GB/T 40857-2021中6.7规定的密码算法验证要求。

6.9 入侵检测系统验证

应按照下述方法验证是否满足入侵检测系统要求要求：

a） 模拟CAN报文异常情况（长度异常、周期异常，信号路由异常，信号阈值异常，负载异常，诊断报文异常），检查中央网关的入侵检测系统是否能捕获异常报文；

b） 检查中央网关入侵检测系统是否记录异常日志；

c） 检查中央网关入侵检测系统是否将异常数据，日志上传。

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，中央网关的防护强度分为三个级别。应在进行中央网关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 40857-2021中7.2的ECU-SL1、ECU-SL2和ECU-SL3分级描述。

7.3 分级要求

中央网关系统的具体等级划分详见表1。

表1 中央网关信息安全分级

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	●	●	●
操作系统-系统日志审计			●
操作系统-CAN防火墙	●	●	●
操作系统-以太网防火墙	●	●	●
操作系统-拒绝服务攻击检测	●	●	●
操作系统-OBD接口防护		●	●
应用软件	●	●	●
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		●	●