ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 100-2022

智能网联汽车控制器硬件信息安全测试规范

Test Specification for controller hardware of intelligent and connected vehicles

2022-11-02 发布　　2022-11-03 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。

本文件由中国第一汽车股份有限公司智能网联开发院、一汽解放汽车有限公司商用车开发院联合提出。

本文件由吉林省汽车电子协会归口。

本文件主要起草单位：一汽解放汽车有限公司商用车开发院、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：梁亚丽、郑岩、付盈、李木子、詹悦、高德志、谷倩、杨南、孙琦、安然。

本文件参与起草单位：广东为辰信息安全有限公司、北京奇虎科技有限公司、中国汽车技术研究中心有限公司、吉林大学汽车仿真与控制国家重点实验室、联通智网科技股份有限公司、岚图汽车科技有限公司、中国第一汽车集团有限公司检测试验院、重庆长安汽车股份有限公司、一汽奔腾轿车有限公司、东风汽车集团有限公司技术中心。

本文件参与起草人：王志鹏、卜启航、李宝田、李杰、刘书勇、龚军、郑建明、汪向阳、雷凯、孙伟、周海鹰。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、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，随着汽车与电子、软件、通信、人工智能、大数据等多个产业的跨界融合和协同创新，中国智能网联汽车已经逐渐形成了覆盖“车、路、云”的立体网状生态系统。这样车辆电气功能越来越复杂、和外界的通信越来越多，故车辆和外界通信方式越来越多样、车辆采用操作系统的控制器越来越多，故对车辆信息安全的开发及实现质量及水平要求越来越高。

而控制器的硬件往往是黑客进行车辆攻击的起点，只有对其实现了有效的防控才能有效支撑车辆信息安全。故对其设计要求及测试方法进行了规范化规定。

智能网联汽车控制器硬件信息安全测试规范

1. 范围

本文件规定了智能网联汽车控制器硬件信息安全设计及测试内容、要求及准则。
本文件适用于智能网联汽车信息安全控制器硬件信息安全的设计及测试工作。

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 25056-2018 和 T/GHDQ 85-2021 界定的以及下列术语和定义适用于本文件。

3.1

智能网联汽车 intelligent connected vehicles；ICV
具备环境感知、智能决策和自动控制，或与外界信息交互，乃至协同控制功能的汽车。

3.2

信息安全测试 Cybersecurity Test
是为了证明信息安全网络防御按照预期计划正常运行而提供的一种机制，主要包含设计规范符合性测试、模糊测试及渗透测试。

3.3

汽车电子控制单元硬件 Vehicle ECU hardware
构成汽车控制单元的硬件元件或设备，是和汽车控制单元软件相对应的概念。

3.4

丝印 Silk Screen Printing
存在于 PCB 板或芯片上能够表征芯片型号、芯片及硬件设备功能及管脚功能的标识。

3.5

硬件安全模块 Hardware Security Module
即 HSM，是一种能够安全可靠进行数据存储及计算的硬件模块，可用于存储数字签名、算法、密

钥等重要信息并执行加密和解密功能。

3.6

调试接口 Debug Interface

用于连接外部设备，进行程序调试处理的非托管接口。常用的有USB，UART，JTAG，RDI，SPI等。

4. 缩略语

下列缩略语适用于本文件：

GW:网关控制单元(Gateway)；

JTAG:一种联合测试工作组定义的接口（Joint Test Action Group)；

MCU: 微控制单元(Microcontroller Unit)；

MPU: 微处理器(Microprocessor Unit)；

PCB：印刷电路板（Printed Circuit Board）；

SIM：用户识别卡（Subscriber Identity Module）；

TBOX: 远程通信模块（Telematics box）；

UART: 通用异步收发传输器（Universal Asynchronous Receiver/Transmitter)；

USB:通用串行总线(Universal Serial Bus)；

VIST: 车载信息服务终端（Vehicle information service terminal)；

WPA：保护无线电脑网络安全系统（Wi-Fi Protected Access)；

XCP: 显式控制协议（Explicit Control Protocol)。

5. 信息安全测试规范

5.1. 测试前提

在进行智能网联汽车硬件测试前，应准备如下信息：

a） 被测零件及其针脚定义或测试线束；

b） 调试口类型及其连接方法。

5.2. 测试环境

控制器硬件信息安全测试环境通常由硬件调试设备通过测试线束连接到相应的被测件上，同时硬件调试设备和人机交互设备相连，具体如图1所示。

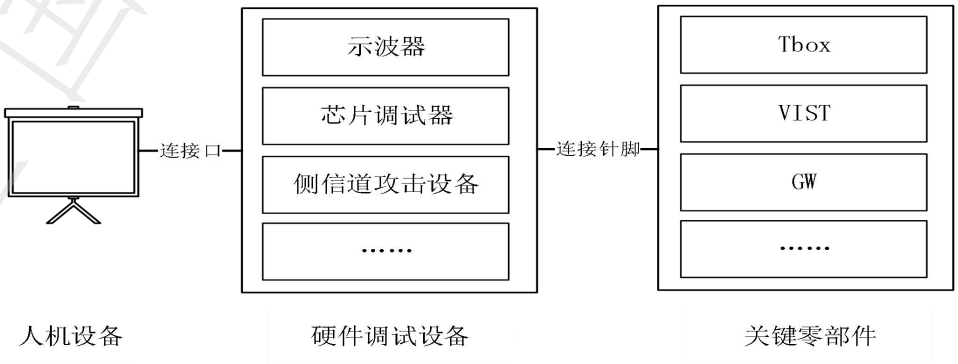

图1 控制器硬件信息安全测试环境示意图

示波器主要用于通过波形信号破译控制器的电子信号报文；芯片调试器主要用于在芯片拆除后连接人机交互设备及芯片，对芯片内容进行删改读写等操作；侧信道攻击设备主要用于对监控控制器硬件的能量消耗、电磁辐射、运行时间等信息进行检测从而对其信息信号进行破译。

5.3. 测试要求

智能网联汽车控制器硬件测试信息安全要求如下：

a） 在PCB板中不应存在后门或隐蔽接口；
b） 芯片应禁用软件调试功能；
c） 对于有联网功能而需进行证书验证并存储重要、个人敏感数据的控制器应配备HSM单元或SE模块等硬件安全模块；
d） MCU、MPU、内存单元上应不存在表征其通用型号的丝印；
e） PCB板上应去除输入输出管脚、调试接口等相关丝印；
f） 调试接口应禁用或设置安全身份认证及访问控制权限；
g） 应设置SIM卡信息识别功能；
h） 应隐蔽芯片的封装引脚或禁用锁定该访问端口；
i） 应配备支持wifi6或WPA3认证方式的wifi模块
j） Wifi模块应关闭其网络模式及安全加密协议的向下兼容功能；
k） 系统芯片间敏感数据的通信线路应尽量隐蔽，对抗内部数据传输窃听和伪造攻击；
l） 采用必要的防护措施，对抗针对HSM及SE的功耗分析，或利用运行时间、温度等信息进行的侧信道攻击；
m） 应具备防御故障注入攻击的安全设计。

5.4. 测试方法及判断依据

智能网联汽车控制器硬件信息安全测试方法如下：

a） 将被测零件外壳拆除，取出PCB板并用放大镜将其放大5倍以上，观察PCB板。如果存在可以非法对芯片进行访问或更改芯片功能的隐蔽接口，则测试不通过。反之满足5.3中a条款要求。注：接口包含但不限于JTAG、UART（TTL、RS232）、XCP通道、USB；
b） 检查芯片是否可以通过软件进行调试，如为否则满足5.3中b条款要求，反之不满足5.3中b条款要求；
c） 对于有联网功能而需进行证书验证并存储重要、个人敏感数据的控制器，需查看其安全设计文档确定其安全设计方案；如其采用外置HSM或SE模块方案需将其外壳拆除，取出PCB板并用放大镜查看，如果有HSM或SE模块则满足5.3中c条款要求；如其采用HSM或SE模块集成于MPU中的设计方案，则需控制器供应商提供相应的MPU型号及芯片手册，能够确认其存在HSM或SE模块后则满足5.3中c条款要求；如非以上两种情况则不满足5.3中c条款要求；
d） 将被测零件拆除，取出其PCB板并用放大镜查看，如其MCU、PCU、内存单元上的有表征其通用型号的丝印则不满足5.3中d条款要求,如果表征通用型号的丝印被擦除、覆盖或采用内部型号等方式处理，则满足5.3中d条款要求；
e） 将被测零件拆除，取出其PCB板并用放大镜查看，如在其上发现了Rx、Tx、调试接口等与信息传输强相关的丝印信息则不满足5.3中e条款要求，反之满足5.3中e条款要求；
f） 将被测零件拆除，取出其PCB板，如果芯片不存在调试功能引脚且PCB上也不存在调试接口，则满足5.3中e条款要求；如有，则查看进入调试接口是否设置身份认证及访问权限限制，如有安全可靠的身份认证及访问权限控制则满足5.3中f条款要求；如未被物理屏蔽且进入调试接口无安全可靠的身份认证及访问权限限制则不满足5.3.f条款要求；

g） 确定蜂窝数据模块中SIM卡类型，如为SIM类型卡则将其拆除并更换另外一张SIM卡，此时如模块能工作则不满足5.3中h条款要求,反之满足5.3中g条款要求；如为ESIM类型卡，则根据样件ESIM卡相关引脚定义将线束引至外部SIM卡槽，此时如模块能工作则不满足5.3中g条款要求,反之满足5.3中g条款要求；

h） 将被测零件外壳拆除，取出PCB板并用放大镜将其放大5倍以上，观察PCB板。采用飞线的方式恢复已屏蔽的接口，如有可恢复的屏蔽接口且能够利用恢复的接口对被测零件进行调试则不满足5.3中h条款要求；反之满足5.3中h条款要求；

i） 先将配备WIFI功能的控制器开启热点功能，通过开启目标控制器热点功能，将其加密方法选择至WPA3；在Kali系统中插入支持监听模式的无线网卡并执行命令airodump-ng wlan0，对当前空口Wifi信号进行扫描，验证目标热点SSID对应的加密方式，如为WPA3，则该Wifi硬件模块能够支持Wifi6或WPA3认证方式，故满足5.3中i条款要求，反之不满足5.3中i条款要求；

j） 检查wifi模块是否关闭了向下兼容wifi5等网络模式及WPA2、WPA等安全加密协议的功能，如关闭则满足5.3中j条款要求，反之不满足5.3中j条款要求；

k） 需提交被测件电路线路板布线图，检查电路板敏感数据通信线路是否隐蔽，使用多层电路板的车载终端系统是否采用内层布线方式进行隐蔽，如果敏感数据通信线路显露或多层电路板未将敏感数据通信线路在内层布线则不满足5.3中k条款要求；

l） 使用侧信道攻击设备对HSM及SE模块加密运算过程中的功率轨迹波形和密文进行收集,并进行分析，如果能破解则不满足5.3中l条款要求；对运行时间、温度等信息进行侧信道攻击，如果系统不能正常运行，则不满足5.3中l条款要求;反之满足5.3中l条款要求；

m） 向芯片中引入电压、时钟、电磁、激光等方式的故障，芯片在在故障条件下运行的特征数据不存在信息泄露或被干扰后导致芯片数据可用性被破坏的现象,则满足满足5.3中m条款要求；反之不满足5.3中m条款要求。