ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 89.1-2022

车载网络安全测试规范
第 1 部分：车载 CAN 总线安全测试规范

On board network security test specification

Part 1: safety test specification for on-board can bus

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 89-2022《车载网络安全测试规范》的第1部分。T/GHDQ 89-2022由以下2个部分组成：

——第1部分：车载CAN总线安全测试规范；

——第2部分：车载以太网安全测试规范；

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：安然、高长胜、孙琦、汤利顺、禹晶晶、张翘楚、张东波。

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、中国汽车工程研究院股份有限公司、长春大学电子信息工程学院、一汽奔腾轿车有限公司、一汽解放汽车有限公司、中国汽车技术研究中心有限公司、北京车和家科技有限公司、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。

本文件参与起草人：李杰、陈宇鹏、于赫、王晓光、李军龙、朱永健、董威、汪向阳、张剑雄、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

汽车 CAN 总线因其速率高，抗干扰性强，成本适中，已被广泛应用在各种类型的汽车上。由于 CAN 本身是没有考虑过信息安全的问题，明文传输、报文广播传输、极少网络分段、无内容校验等特性，让别有用心者能很轻松进入车内网络进行窃听，甚至可以伪造报文对车辆进行控制。所以测试 CAN 通信的防篡改、防重放、安全访问技术是十分有必要的。这些技术是否能保证 CAN 通信的安全可靠，需要进行系统化的测试进行验证。

本文件作为 CAN 总线的信息安全测试标准，明确了 CAN 总线安全的测试目的、测试环境、测试步骤以及评价指标，以达到对 CAN 总线安全的测试验证目标。

车载网络安全测试规范
第 1 部分：车载 CAN 总线安全测试规范

1 范围

本文件规定了车载CAN总线安全测试的测试环境、测试内容和测试方法。

本文件适用于车载CAN总线安全功能开发与测试。

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。

ISO 11898-1 道路车辆 控制局域网络 第1部分：数据链路层和物理信令(Road vehicles — Controller area network(CAN) —Part 1:Data link layer and physical signalling)

ISO 11898-2 道路车辆 控制局域网络 第2部分：高速媒体存取单元(Road vehicles — Controller area network(CAN) —Part 2:High-speed medium access unit)

ISO 14229-1 道路车辆 统一诊断服务 第1部分：规范和要求(Road vehicles — Unified diagnostic services (UDS) — Part 1：Specification and requirements)

ISO 15765-2 道路车辆 局域网络诊断服务 第2部分：网络层服务(Road vehicles — Diagnostics on Controller Area Network (CAN) — Part 2：Network layer services)

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

表1中的缩略语适用于本文件。

表1 缩略语

缩写	定义
ECU	电子控制单元
UDS	统一的诊断服务
DUT	被测设备
CAN	控制器局域网

5 测试环境

5.1 基本测试配置

车载CAN总线信息安全测试主要由待测控制器、CAN总线测试设备、上位机组成。

5.1.1 CAN 单件测试环境

单件测试环境见图1。

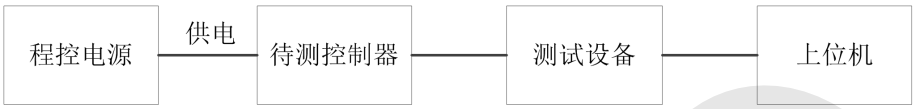

图1 单件测试环境

5.1.2 CAN 整车测试环境

整车测试环境见图2。

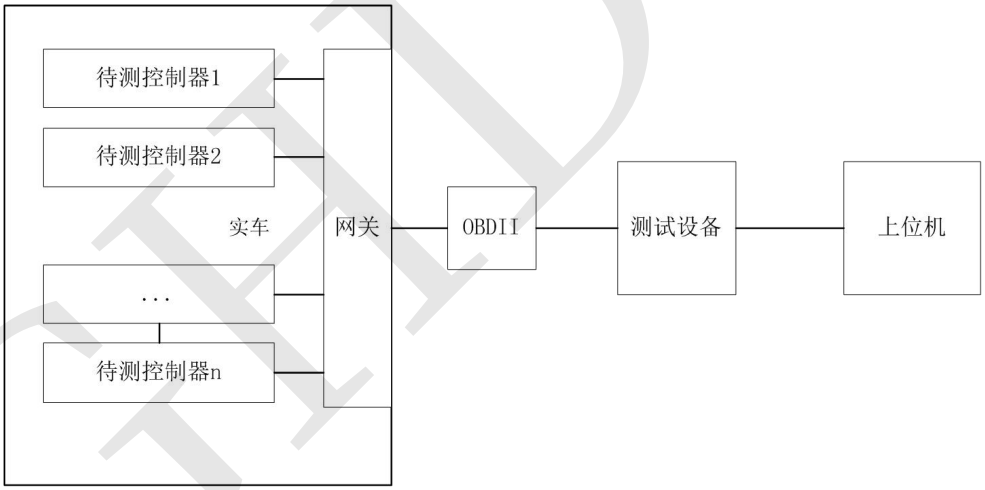

图 2 整车测试环境

5.2 推荐的测试设备列表

推荐的测试设备见表2。

表2 推荐测试设备表

设备名称	型号/版本	数量	功能
测试设备	-	1	CAN测试软件集成环境
程控电源	-	1	0～30V可调，输出电流≥60A
上位机	-	1	预安装测试软件，进行各设备调用
线束	-	1	用于ECU与测试设备间的连接

6 车载 CAN 总线通信信息安全测试

6.1 CAN 总线信息安全测试（单件测试）

6.1.1 CAN 总线支路黑白名单测试

6.1.1.1 测试目的

测试 DUT 的 CAN 总线上存在的报文是否符合总线设计要求。

6.1.1.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与DUT连接正常。

6.1.1.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) DUT 上电；
b) 监听 DUT 报文 1 分钟时间，采集 CAN ID；
c) 将采集到的 CAN ID 分类归总。

6.1.1.4 评价指标

将实际测试到的 CAN ID 与总线协议的设计要求进行对比,如有未在设计要求中的有效 ID，则有风险。

6.1.2 CAN 总线路由表测试

6.1.2.1 测试目的

测试 CAN 总线网段间的路由规则是否符合整车 CAN 总线设计要求。

6.1.2.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与 DUT 连接正常。

6.1.2.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) DUT 上电；
b) 总线上遍历报文 ID，并设定所有的数据字节为 0xEE；
c) 对 CAN 报文进行检索，筛选出全部字节为 0xEE 的 ID；
d) 确定每两条总线之间的数据路由规则；
e) 将实际测试的路由规则与总线设计的路由规则进行对比，找出不符合路由规则的测试项。

6.1.2.4 评价指标

实际测试的路由规则与总线设计的路由规则进行对比不匹配为有风险。

6.2 CAN 总线信息安全测试（整车测试）

6.2.1 CAN 总线报文重放测试

6.2.1.1 测试目的

测试具备防重放功能的 CAN 总线网段的防重放功能是否满足要求。

6.2.1.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.1.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 整车上电；
b) 执行实车的控制动作，如升降车窗；
c) 记录 CAN 报文；
d) 将记录的数据 CAN 报文进行重放；
e) 监测实车状态。

6.2.1.4 评价指标

数据重放导致实车动作为有风险。

6.2.2 CAN 总线控制报文防篡改测试

6.2.2.1 测试目的

测试具备防篡改功能的 CAN 总线网段的防止控制报文被篡改功能是否满足要求。

6.2.2.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.2.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 整车上电；
b) 记录控制报文的报文数据位变化及其状态控制；
c) CAN 原始报文做数据控制位篡改并保留控制部分。

6.2.2.4 评价指标

数据发送导致实车动作为有风险。

6.2.3 CAN 总线 UDS 诊断认证种子长度测试

6.2.3.1 测试目的

测试总线 UDS 的诊断认证种子长度是否足够强壮。

6.2.3.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.3.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 切换 UDS 服务会话；
b) 进行 UDS 诊断服务的数据认证种子请求；
c) 查看种子长度是否大于等于 4 个字节。

6.2.3.4 评价指标

种子长度小于 4 字节为有风险。

6.2.4 CAN 总线 UDS 诊断认证访问次数测试

6.2.4.1 测试目的

测试总线 UDS 的诊断认证访问次数是否有限制。

6.2.4.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.4.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 切换 UDS 服务会话；
b) 进行 UDS 诊断服务的数据认证种子请求；
c) 确认是否存在 m 次请求限制的设计，进行 n 次请求（n＞m），查看是否在 m+1 次到 n 次测试中都可以返回数据。

6.2.4.4 评价指标

m+1次到n次请求都返回数据为有风险。

6.2.5 CAN 总线 UDS 诊断认证访问禁止测试

6.2.5.1 测试目的

测试总线 UDS 的诊断认证访问是否有错误请求禁止限制。

6.2.5.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.5.3 测试步骤

按照以下测试步骤进行信息安全测试：

a) 切换 UDS 服务会话；
b) 进行 UDS 诊断服务的数据认证种子请求；
c) 进行 n 次错误请求，查看是否都可以返回请求错误,n 取值依照具体规范要求设定。

6.2.5.4 评价指标

n次错误请求后无通信限制为有风险。

6.2.6 CAN 总线认证种子随机度测试

6.2.6.1 测试目的

测试总线的认证访问种子回复是否满足随机性要求。

6.2.6.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常；
b) 上位机软件正常运行；
c) 测试设备与整车连接正常。

6.2.6.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 切换 UDS 服务会话；
b) 进行 UDS 诊断服务的数据认证种子请求；
c) 记录随机数。

6.2.6.4 评价指标

请求50次随机数，有重复为有风险。