ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 89.2-2022

车载网络安全测试规范
第 2 部分：车载以太网安全测试规范

On board network security test specification

Part 2: on board Ethernet safety test specification

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2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：禹晶晶、高长胜、孙琦、汤利顺、安然、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、长春大学电子信息工程学院、中国汽车技术研究中心有限公司、一汽解放汽车有限公司、一汽奔腾轿车有限公司、中国汽车工程研究院股份有限公司、中汽创智科技有限公司、东风汽车集团有限公司技术中心、重庆长安汽车股份有限公司。

本文件参与起草人：李杰、于赫、朱永健、李军龙、王晓光、陈宇鹏、徐敏杰、周海鹰、汪向阳、张剑雄。

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

车载以太网是一种连接车内电子单元的新型局域网技术，在单对非屏蔽双绞线上可实现 100 Mbit/s 甚至 1 Gbit/s 的数据传输速率，同时满足汽车行业高可靠性、低电磁辐射、低功耗、带宽分配、低延迟以及同步实时性等方面的要求。由于以太网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。所以在以太网报文基础上增加新鲜值管理以及报文内容校验的防篡改、防重放的技术也应运而生。通过在通信的控制器双方增加新鲜值管理有效的防止报文被重放，通过通信控制器双方增加报文内容校验机制有效的防止报文被第三方非法篡改，达到了总线通信安全的目的。这些技术是否能保证以太网通信的安全可靠，需要进行系统化的测试进行验证。

本文件作为车载以太网的信息安全测试标准，明确了车载以太网安全的测试目的、测试环境、测试步骤以及评价指标，以达到对车载以太网安全的测试验证目标。

车载网络安全测试规范
第 2 部分：车载以太网安全测试规范

1 范围

本文件规定了车载以太网信息安全渗透测试的测试环境、测试内容和测试方法。

本文件适用于车载以太网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 13400-2 传输层协议和网络层服务(Transport protocol and network layer services,2012.)

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

下列术语和定义适用于本文件。

3.1

SOME/IP

Scalable Service-Oriented Middleware over IP，基于IP的可扩展面向服务的中间件，以太网应用层通信协议。

3.2

Telnet

远程登陆协议。

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
ADB	安卓调试桥（Android Debug Bridge）
DUT	Device under test，即待测设备或被测设备，非接入点
ECU	Electronic Control Unit,电子控制单元
ETH	Ethernet，以太网
SSh	Secure Shell，安全外壳协议，端口服务
UDS	Unified Diagnostic Services，统一诊断服务

5　测试环境

5.1　基本测试配置

车载网络信息安全测试主要由待测控制器、以太网测试设备、上位机组成。

5.1.1　以太网单件测试环境

单件测试环境见图1。

图1　单件测试环境

5.1.2　以太网整车测试环境

整车测试环境见图2。

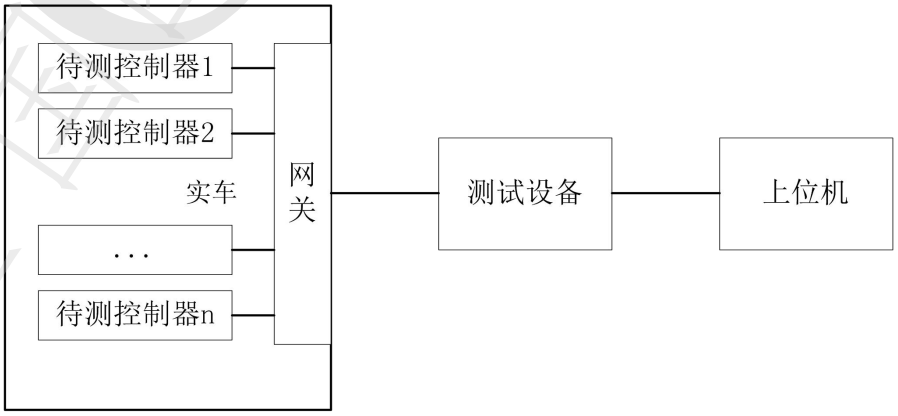

图2　整车测试环境

5.2 推荐测试用设备清单

推荐的测试用设备见表2。

表 2 测试组件功能解析

设备名称	数量	功能
测试设备	1	以太网测试软件集成环境
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 车载网络以太网通信信息安全测试

6.1 车载以太网总线信息安全测试（单件测试）

6.1.1 车载以太网总线 adb 服务端口扫描

6.1.1.1 测试目的

测试车载以太网总线是否开启 adb 危险端口。

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 12V；
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) 设置上位机与 DUT 对应车载以太网端口在同一网段；
b) 扫描目标 ip；
c) 对疑似端口进行 adb 服务链接；
d) 确认目标是否开启 adb 服务。

6.1.1.4 评价

车载以太网上开放有 adb 端口为有风险。

6.1.2 车载以太网总线 telnet 服务端口扫描

6.1.2.1 测试目的

测试车载以太网总线是否开启 telnet 危险端口。

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 12V；
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) 设置上位机与 DUT 对应车载以太网端口在同一网段；
b) 扫描目标 ip；
c) 对疑似端口进行 telnet 服务链接；
d) 确认目标是否开启 telnet 服务。

6.1.2.4 评价

车载以太网上开放有 telnet 端口为有风险。

6.1.3 车载以太网总线 ssh 服务端口扫描

6.1.3.1 测试目的

测试车载以太网总线是否开启 ssh 危险端口。

6.1.3.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常 12V；
b) 上位机软件正常运行；
c) 测试设备与 DUT 连接正常。

6.1.3.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 设置上位机与 DUT 对应车载以太网端口在同一网段；
b) 扫描目标 ip；
c) 对疑似端口进行 ssh 服务链接；
d) 确认目标是否开启 ssh 服务。

6.1.3.4 评价

车载以太网上开放有 ssh 端口为有风险。

6.1.4 车载以太网总线服务端口扫描

6.1.4.1 测试目的

测试车载以太网总线是否开启未预期危险端口。

6.1.4.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常 12V；
b) 上位机软件正常运行；
c) 测试设备与 DUT 连接正常。

6.1.4.3 测试步骤

按照以下测试步骤进行信息安全测试：
a) 设置上位机与 DUT 对应车载以太网端口在同一网段；
b) 扫描目标 ip；
c) 记录监测到的服务端口；

d) 比对开放的服务端口是否符合预期设计。

6.1.4.4 评价

实际测试的开放端口与规定开放的端口不一致为有风险。其中，规定开放的端口是根据厂商的规定来执行。

6.2 车载以太网总线信息安全测试（整车测试）

6.2.1 车载以太网总线 SOME/IP 报文重放测试

6.2.1.1 测试目的

测试车载以太网总线是否有总线数据防重放措施。

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 12V；
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) 记录实车控制动作的数据 log；
d) 将数据 log 对目标执行件进行控制报文重放；
e) 查看实车的车辆状态。

6.2.1.4 评价

数据重放导致目标执行件执行车控动作为有风险。

6.2.2 车载以太网总线 UDS 诊断认证种子长度测试

6.2.2.1 测试目的

测试总线 UDS 的诊断认证种子长度是否足够强壮。

6.2.2.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常 12V；
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) 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。

6.2.2.4 评价

种子长度小于 4 字节为有风险。

6.2.3 车载以太网总线 UDS 诊断认证访问次数测试

6.2.3.1 测试目的

测试总线 UDS 的诊断认证访问次数是否有限制。

6.2.3.2 初始条件

本测试需初始条件如下：
a) 测试设备供电正常 12V；
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) 确认是否存在 m 次请求限制的设计，进行 n 次请求（n＞m），查看是在否在 m+1 次到 n 次测试中都可以返回数据。

6.2.3.4 评价

m+1次到n次请求都返回数据为有风险。

6.2.4 车载以太网总线 UDS 诊断认证访问禁止测试

6.2.4.1 测试目的

测试总线 UDS 的诊断认证访问是否有时间禁止限制。

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) 进行 n 次错误请求，查看是否都可以返回请求错误（其中，n 为设计规范规定的数据认证种子请求次数）。

6.2.4.4 评价

多次错误请求后有通信限制为无风险，否则为有风险。其中，请求次数依照具体规范要求设定。

6.2.5 车载以太网总线 UDS 认证种子随机度测试

6.2.5.1 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。

6.2.5.2 初始条件

本测试需初始条件如下：

a) 测试设备供电正常 12V；
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) 记录随机数。

6.2.5.4 评价

请求50次随机数，有重复为有风险。