ICS 43.020

CCS T 40

# 团　　体　　标　　准

T/GHDQ 88.2-2022

# 车辆无线通信信息安全测试规范
# 第 2 部分:车载 WLAN 安全测试规范

In vehicle wireless communication information cybersecurity test specification

Part2: In vehicle WLAN cybersecurity 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 88-2022《车辆无线通信信息安全测试规范》的第1部分，T/GHDQ 88-2022由以下2个部分组成：

——第1部分：蓝牙安全测试规范；

——第2部分：车载WLAN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：孙琦、高长胜、汤利顺、安然、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、东风汽车集团有限公司技术中心、一汽奔腾轿车有限公司、中汽研软件测评（天津）有限公司、长春大学电子信息工程学院、一汽解放汽车有限公司、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、重庆长安汽车股份有限公司。

本文件参与起草人：李杰、孙伟、王晓光、贺可勋、于赫、李军龙、陈宇鹏、阳志强、汪向阳、谭成宇。

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

WLAN技术已在智能网联汽车上普遍应用。主要作用是为用户提供网络热点以及供车机连接外部热点。

作为一种短距离无线通信技术，WLAN一旦被黑客攻破利用，则可能造成数据被窃取、车辆被控制等安全风险。

本文件作为WLAN的信息安全测试标准，明确了WLAN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WLAN安全的测试验证目标。

# 车辆无线通信信息安全测试规范
# 第 2 部分:车载 WLAN 通信安全测试规范

## 1 范围

本文件规定了车载WLAN通信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WLAN功能开发和测试。

## 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。

GB/T 31491-2015 无线网络访问控制技术规范
GB/T 32420-2015 无线局域网测试规范

## 3 术语和定义

下列术语和定义适用于本文件。

**Telnet**
远程登陆协议。
**SSID**
服务集标识。

## 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 |
|---|---|
| AP | 接入点 |
| ADB | 安卓调试桥 |
| ETH | 以太网 |
| MAC | 媒体存取控制 |
| SSH | 安全壳 |

## 5 测试环境

### 5.1 基本测试配置

车载 WLAN 信息安全测试主要由待测控制器、车载 WLAN 测试设备、上位机组成。测试环境见图 1。

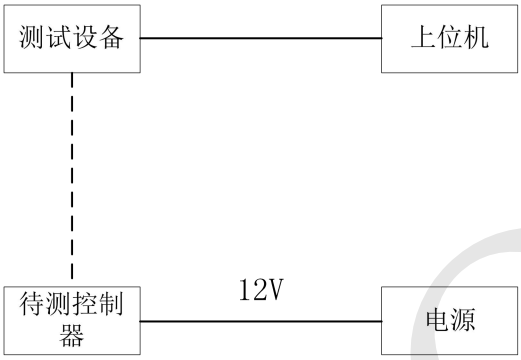


图1 测试环境

### 5.2 推荐测试设备列表

推荐的测试设备见表2。

表2 推荐测试设备列表

| 设备名称 | 数量 | 功能 |
|---|---|---|
| 测试设备 | 1 | WLAN抓包与解析、数据分析设备 |
| 上位机 | 1 | 预安装测试软件，进行各设备调用 |
| 待测控制器 | 1 | 用于进行测试的控制器 |
| 电源 | 1 | 12V |

## 6 车载 WLAN 通信安全测试用例

### 6.1 车载 WLAN 密码保护测试

#### 6.1.1 测试目的

测试车载WLAN是否设置了连接密码以保护热点安全性。

#### 6.1.2 初始条件

本测试需初始条件如下：

a) 车载无线 AP 上电并开启无线服务；
b) 车载无线测试终端未与车辆WLAN热点连接过。

#### 6.1.3 测试步骤

按照以下测试步骤进行测试：

a) 打开车载无线AP ，确保其正常服务；
b) 使用车载无线测试终端连接车辆WLAN热点。

#### 6.1.4 评价指标

若无须输入密码即可连接则存在风险。

### 6.2 车载 WLAN 密码口令强度测试

#### 6.2.1 测试目的

检测车载WLAN 连接密码强度是否符合要求。

#### 6.2.2 初始条件

车载无线 AP 上电并开启无线服务。

#### 6.2.3 测试步骤

按照以下测试步骤进行测试：

a) 查看车载WLAN默认密码，判断密码复杂度；
b) 尝试更改密码。

#### 6.2.4 评价指标

若默认密码强度和可修改的密码强度是非8位数字字母大小写组合则测试不通过。

### 6.3 AP 端口服务扫描测试

#### 6.3.1 测试目的

检测车载 WLAN AP 设备是否开启了高危端口及服务。

#### 6.3.2 初始条件

车载无线 AP 上电并开启无线服务。

#### 6.3.3 测试步骤

按照以下测试步骤进行测试：

a) 在车载WLAN测试终端扫描车载无线设备IP；
b) 观察开放了哪些服务。

#### 6.3.4 评价指标

检测是否开启非默认服务端口，若开放了非默认服务端口且进程可疑，则存在安全风险。非默认服务端口依设计需求设定。

### 6.4 WLAN 加密协议测试

#### 6.4.1 测试目的

检测车载无线 AP 是否采用不安全的加密协议WEP。

#### 6.4.2 初始条件

车载无线 AP 上电并开启无线服务。

#### 6.4.3 测试步骤

按照以下测试步骤进行测试：

a) 使用测试设备连接车载WLAN；

b) 对无线网络进行嗅探；

c) 查看使用的加密算法。

### 6.4.4 评价指标

若未使用WPA2/WPA-PSK等以上安全级别的加密认证方式，则认为存在风险。

## 6.5 车载 WLAN SSID 默认字符串测试

### 6.5.1 测试目的

检测车载WLAN默认SSID是否泄漏了AP设备名称、型号等信息。

### 6.5.2 初始条件

车载无线 AP 上电并开启无线服务。

### 6.5.3 测试步骤

按照以下测试步骤进行测试：

a) 观察默认车载WLAN热点名称；

b) 查看名称是否包含AP设备名称、型号等信息。

### 6.5.4 评价指标

若默认的SSID包含了设备名称、型号等信息，则存在安全风险。

## 6.6 车载 WLAN 与车内 ETH 网络隔离测试

### 6.6.1 测试目的

检测车载 AP 网络是否与车载以太网内网隔离。

### 6.6.2 初始条件

车载无线 AP 上电并开启无线服务。

### 6.6.3 测试步骤

按照以下测试步骤进行测试：

a) 使用车载WLAN测试终端连接车载AP网络后扫描车载以太网内网IP；

b) 查看扫描到的IP。

### 6.6.4 评价指标

若能够扫描到车内设备端口情况，则说明车载 WLAN 网络和以太网内网没有隔离，存在安全风险。

## 6.7 车载 WLAN 固件密码存储安全测试

### 6.7.1 测试目的

检测无线连接密码是否安全存储。

#### 6.7.2 初始条件

车载无线 AP 上电并开启无线服务。

#### 6.7.3 测试步骤

按照以下测试步骤进行测试：

a) 搜索车载WLAN配置文件；

b) 查看车载WLAN配置文件。

#### 6.7.4 评价指标

若发现明文存储的车载WLAN 密码则存在安全风险。

### 6.8 车载 WLAN 已知漏洞分析测试

#### 6.8.1 测试目的

检测车载热点是否存在已知漏洞。

#### 6.8.2 初始条件

车载无线 AP 上电并开启无线服务。

#### 6.8.3 测试步骤

按照以下测试步骤进行测试：

a) 使用测试设备对目标AP执行已知漏洞检测；

b) 分析测试结果。

#### 6.8.4 评价指标

若发现存在6个月以上的已知漏洞则存在安全风险。