ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 88.1-2022

车辆无线通信安全测试规范
第 1 部分:车载蓝牙安全测试规范

In vehicle wireless communication information cybersecurity test specification

Part1: In vehicle Bluetooth 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、长春大学电子信息工程学院、中国汽车工程研究院股份有限公司、中汽研软件测评（天津）有限公司、一汽解放汽车有限公司、一汽奔腾轿车有限公司、重庆长安汽车股份有限公司、北京车和家科技有限公司。

本文件参与起草人：李杰、孙伟、于赫、陈宇鹏、贺可勋、李军龙、王晓光、汪向阳、张鹏、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

经典蓝牙和低功耗蓝牙已在智能网联汽车上普遍应用。其中，经典蓝牙主要应用于车机娱乐系统，用于语音等数据传输。低功耗蓝牙主要应用于数字钥匙，用于手机控车。

作为一种短距离无线通信技术，蓝牙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。

本文件作为蓝牙的信息安全测试标准，明确了蓝牙安全的测试目的、测试环境、测试步骤以及评价指标，以达到对蓝牙安全的测试验证目标。

车辆无线通信安全测试规范
第1部分:车载蓝牙安全测试规范

1 范围

本文件规定了车载蓝牙安全测试规范。

本文件适用于车载蓝牙安全测试。

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。

蓝牙核心协议规范 V4.2 (SIG Bluetooth Core Specification v4.2)

蓝牙安全指南 800-121 V1——标准和技术推荐(NIST Special Publication 800-121 Revision 1: Guide to BluetoothSecurity - Recommendation of the National Institute of Standards and Technology)

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
DUT	被测样件
ETH	以太网

5 测试环境

5.1 基本测试配置

车载经典蓝牙信息安全测试主要由待测控制器、测试设备、上位机工具组成。测试环境见图1。

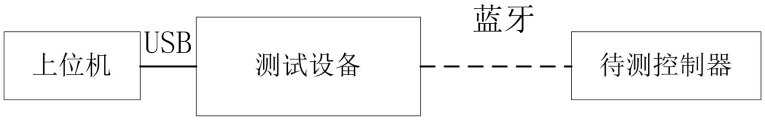

图1　车载经典蓝牙测试环境

车载低功耗蓝牙信息安全测试主要由测试设备、上位机工具、待测控制器、手机APP组成。测试环境见图1。

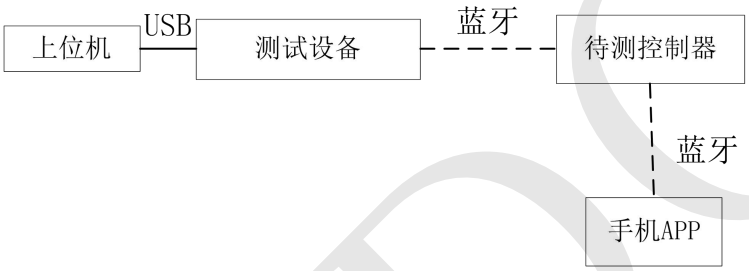

图2　车载低功耗蓝牙测试环境

5.2　推荐测试设备列表

推荐的测试设备列表见表2。

表2　推荐测试设备列表

设备名称	数量	功能
测试设备	1	蓝牙抓包与解析、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（蓝牙协议4.0及以上）

6　车载蓝牙信息安全测试

6.1　车载经典蓝牙通信安全测试

6.1.1　车载经典蓝牙安全配对模式测试

6.1.1.1　测试目的

检测车载经典蓝牙是否使用安全配对模式。

6.1.1.2　初始条件

车载经典蓝牙与测试设备未配对过。

6.1.1.3　测试步骤

测试步骤如下：

a) DUT 上电并将车载经典蓝牙置于可发现状态；
b) 找到 DUT 对应的 MAC 地址,测试设备与其进行配对；
c) 查看能否直接与 DUT 配对。

6.1.1.4 评价

如果能直接与 DUT 配对，则 DUT 默认使用的配对方式为 Just Works，认为存在风险。

6.1.2 车载经典蓝牙协议栈已知漏洞测试

6.1.2.1 测试目的

检测车载经典蓝牙协议栈是否存在已知漏洞。

6.1.2.2 初始条件

无。

6.1.2.3 测试步骤

测试步骤如下：
a) DUT 上电；
b) 使用漏洞扫描工具对被测样件进行漏洞扫描；
c) 查看扫描结果。

6.1.2.4 评价

蓝牙协议栈不应存在近6个月以上的已知漏洞。

6.2 车载低功耗蓝牙安全测试

6.2.1 车载低功耗蓝牙安全配对模式测试

6.2.1.1 测试目的

检测车载经典蓝牙是否使用安全配对模式。

6.2.1.2 初始条件

车载低功耗蓝牙与测试设备未配对过。

6.2.1.3 测试步骤

测试步骤如下：
a) DUT 上电并将车载低功耗蓝牙置于可发现状态；
b) 找到 DUT 对应的 MAC 地址,测试设备与其进行配对；
c) 查看使用的配对模式。

6.2.1.4 评价

如果能直接与 DUT 配对，则 DUT 默认使用的配对方式为 Just Works，认为存在风险。

6.2.2 低功耗蓝牙控车业务数据加密性测试

6.2.2.1 测试目的

测试车载蓝牙模块的低功耗蓝牙业务数据是否加密。

6.2.2.2 初始条件

无。

6.2.2.3 测试步骤

测试步骤如下：

a) 手机 APP 与 DUT 配对；
b) 使用 APP 向 DUT 发送控制指令；
c) 获取并分析数据。

6.2.2.4 评价

如果控制指令明文传输，未加密则认为存在问题。

6.2.3 车载低功耗蓝牙控车业务数据重放测试

6.2.3.1 测试目的

测试车载低功耗蓝牙模块的BLE业务功能能否抵抗重放攻击。

6.2.3.2 初始条件

无。

6.2.3.3 测试步骤

测试步骤如下：

a) DUT 上电将车载低功耗蓝牙置于可发现状态；
b) 手机 APP 与 DUT 配对；
c) 使用 APP 向 DUT 发送控制指令；
d) 获取所写入的数据；
e) 再次使用该功能；
f) 将发送的数据修改为上次获取的数据；
g) 观察结果。

6.2.3.4 评价

成功使用了该控制功能则认为存在风险。

6.2.4 车载低功耗蓝牙控车业务数据篡改测试

6.2.4.1 测试目的

测试车载低功耗蓝牙模块的低功耗蓝牙业务功能是否可防篡改。

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；

6.2.4.3 测试步骤

测试步骤如下：

a) DUT 上电将车载低功耗蓝牙置于可发现状态；
b) 手机 APP 与 DUT 配对；
c) 使用 APP 发送控制指令；
d) 使用测试设备截取并篡改后发送至 DUT；
e) 观察结果。

6.2.4.4 评价

成功使用了该控制功能则认为存在风险。