

IVISTA

网联智能与隐私安全专项测评

编号: IVISTA-CIPS-SM-CSPS-CS-RP-A1-2023

网络与隐私安全 网络安全评价规程

Cybersecurity and Privacy Security

Cybersecurity Rating Protocol

(2023 版修订版)

中国汽车工程研究院股份有限公司 发布

目 次

1 范围.....	1
2 规范性引用文件.....	1
3 评分规则.....	1
4 评价方法.....	1
附录 A 数字钥匙安全评分规则.....	3
附录 B 导航定位安全评分规则.....	4
附录 C 远程控车安全评分规则.....	5
附录 D 车端接口安全评分规则.....	6
附录 E 网络通信安全评分规则.....	7

网络安全评价规程

1 范围

本文件规定了网络与隐私安全测评中网络安全的评价方法。

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。

IVISTA-CIPS-SM-CSPS. CS-TP-A1-2023 网络安全试验规程

3 评分规则

数字钥匙安全试验，满分 12 分，具体评分规则见附录A 数字钥匙安全评分规则；
导航定位安全试验，满分 4 分，具体评分规则见附录B 导航定位安全评分规则；
远程控车安全试验，满分 20 分，具体评分规则见附录C 远程控车安全评分规则；
车端接口安全试验，满分 15 分，具体评分规则见附录D 车端接口安全评分规则；
网络通信安全试验，满分 16 分，具体评分规则见附录E 网络通信安全评分规则；

4 评价方法

网络安全的评价分为优秀（G）、良好（A）、一般（M）和较差（P）共四个评价等级。以综合得分率进行评价等级的划分，如表 1 所示。

综合得分率=综合得分/得分区间值×100% （0≤得分率≤100%）

综合得分=数字钥匙安全试验得分+导航定位安全试验得分+远程控车安全试验得分+车端接口安全试验得分+网络通信安全试验得分-（-48）

得分区间值=67-（-48）=115

表 1 网络安全评价

网络安全评价	网络安全综合得分率
优秀 (G)	综合得分率 $\geq 80\%$
良好 (A)	$70\% \leq \text{综合得分率} < 80\%$
一般 (M)	$60\% \leq \text{综合得分率} < 70\%$
较差 (P)	综合得分率 $< 60\%$

附录 A

数字钥匙安全评分规则

数字钥匙安全评价总分 12 分，其中射频钥匙重放攻击试验 4 分、蓝牙钥匙重放攻击试验 4 分、NFC 钥匙中继攻击试验 4 分，如表 A.1 所示。

表 A.1 数字钥匙安全试验评分表

项目	试验场景	结果指标	得分情况	最高得分
数字钥匙安全	射频钥匙重放攻击试验	结果 1：车辆接收响应范围内，车辆未被解锁；结果 2：车辆接收响应范围外，车辆未被解锁。	4	4
		结果 1：车辆接收响应范围内，车辆未被解锁；结果 2：车辆接收响应范围外，车辆被解锁。	3	
		结果 1：车辆接收响应范围内，车辆被解锁。	-3	
		车辆无射频钥匙功能或其他不适用情况。	0	
	蓝牙钥匙重放攻击试验	车辆未被解锁。	4	4
		车辆被解锁。	-3	
		车辆无蓝牙钥匙功能或其他不适用情况。	0	
	NFC 钥匙中继攻击试验	结果 1：车辆具备实体卡片 NFC 钥匙，车辆未被解锁。	2	4
		结果 1：车辆具备实体卡片 NFC 钥匙，车辆被解锁。	-1	
		车辆无实体卡片 NFC 钥匙功能或其他不适用情况。	0	
		结果 2：车辆具备智能设备 NFC 钥匙，车辆未被解锁。	2	
		结果 2：车辆具备智能设备 NFC 钥匙，车辆被解锁。	-1	
		车辆无智能设备 NFC 钥匙功能或其他不适用情况。	0	

附录 B

导航定位安全评分规则

导航定位安全评价总分 4 分，包括 GNSS 信号伪造试验 4 分，如表 B.1 所示。

表 B.1 导航定位安全试验评分表

项目	试验场景	结果指标	得分情况	最高得分
导航定位安全	GNSS 信号伪造试验	结果 1：打开车辆无线通信，试验车辆定位准确，未被欺骗或干扰。结果 2：关闭车辆无线通信，试验车辆定位准确，未被欺骗或干扰。	4	4
		结果 1：打开车辆无线通信，试验车辆定位准确，未被欺骗或干扰。结果 2：关闭车辆无线通信，试验车辆定位不准确；或无法关闭车辆无线通信。	3	
		结果 1：打开车辆无线通信，试验车辆定位结果不准确。	-3	
		车辆无导航定位功能或其他不适用的情况。	0	

附录 C

远程控车安全评分规则

远程控车安全评价总分 20 分，包括控车App加固安全性试验 5 分、控车App通信安全性试验 5 分、App控车指令重放攻击试验 5 分、App控车指令篡改攻击试验 5 分。评分规则如表 C.1 所示。

表 C.1 远程控车安全试验评分表

项目	试验场景	结果指标	得分情况	最高得分
远程控车安全	控车 App 加固安全性试验	控车 App 具备加固壳。	3	5
		控车 App 不具备加固壳。	-2	
		控车 App 具备代码混淆机制。	1	
		控车 App 不具备代码混淆机制。	-1	
		控车 App 具备安全检测机制，且安全机制绕过失败。	1	
		控车 App 不具备安全检测机制；或控车 App 具备安全检测机制，但安全机制绕过成功。	-1	
		车辆无 App 控车功能或其他不适用的情况。	0	
	控车 App 通信安全性试验	使用了安全的传输协议。	5	5
		未使用安全的传输协议。	-4	
		车辆无 App 控车功能或其他不适用的情况。	0	
	App 控车指令重放攻击试验	车辆未执行控制操作。	5	5
		车辆执行控制指令。	-4	
		车辆无 App 控车功能或其他不适用的情况。	0	
	App 控车指令篡改攻击试验	车辆未执行控制操作。	5	5
		车辆执行控制指令。	-4	
		车辆无 App 控车功能或其他不适用的情况。	0	

附录 D

车端接口安全评分规则

车端接口安全评价总分 15 分，包括USB接口试验 9 分、OBD接口试验 3 分、远程连接端口试验 3 分，如表 D.1 所示。

表 D.1 车端接口安全试验评分表

项目	试验场景	结果指标	得分情况	最高得分
车端接口安全	USB 接口访问控制试验	车机仅能识别清单允许格式的文件。	3	3
		车机能识别清单允许格式以外其他格式文件。	-2	
		车机无 USB 接口或其他不适用的情况。	0	
	USB 接口防病毒试验	车机未运行恶意程序。	3	3
		车机运行恶意程序。	-2	
		车机无 USB 接口或其他不适用的情况。	0	
	ADB 调试安全 全检查试验	不可接入 ADB 调试。	3	3
		可接入 ADB 调试，但不可启用 root 权限。	-2	
		可接入 ADB 调试，且可启用 root 权限。	-3	
		车辆无 ADB 调试功能或其他不适用的情况。	0	
	OBD 接口访问控制试验	车辆 OBD 接口访问控制机制有效。	3	3
		车辆 OBD 接口访问控制机制无效。	-2	
	远程连接端口试验	车辆不存在未授权的远程连接端口开放。	3	3
		车辆存在未授权的远程连接端口开放。	-2	

附录 E

网络通信安全评分规则

网络通信安全评价总分 16 分，其中 Wi-Fi/热点攻击试验 8 分、蓝牙攻击试验 6 分、蜂窝网络攻击试验 2 分，如表 E.1 所示。

表 E.1 网络通信安全试验评分表

项目	试验场景	结果指标	得分情况	最高得分
网络通信安全	Wi-Fi/热点破解攻击试验	结果 1：车辆 Wi-Fi/热点默认密码是 8 位以上数字、大小写字母、特殊符号两种以上的组合。	1	2
		结果 1：车辆 Wi-Fi/热点默认密码不是 8 位以上数字、大小写字母、特殊符号两种以上的组合。	-1	
		结果 2：车辆修改 Wi-Fi/热点密码有强度提示。	1	
		结果 2：车辆修改 Wi-Fi/热点密码无强度提示。	-1	
		车辆无 Wi-Fi/热点功能或其他不适用的情况。	0	
	Wi-Fi/热点断连攻击试验	车辆 Wi-Fi/热点未与测试设备断开连接。	2	2
		车辆 Wi-Fi/热点与测试设备断开连接。	-1	
		车辆无 Wi-Fi/热点功能或其他不适用的情况。	0	
	Wi-Fi/热点恶意钓鱼攻击试验	车辆未连接至恶意钓鱼 Wi-Fi/热点；或车辆自动连接至恶意钓鱼 Wi-Fi/热点，并向用户发出风险提示。	2	2
		车辆自动连接至恶意钓鱼 Wi-Fi/热点，且未向用户发出风险提示。	-1	
		车辆无 Wi-Fi/热点功能或其他不适用的情况。	0	
	Wi-Fi/热点协议模糊攻击试验	车辆 Wi-Fi/热点正常工作。	2	2
		车辆 Wi-Fi/热点不能正常工作。	-1	
		车辆无 Wi-Fi/热点功能或其他不适用的情况。	0	
	蓝牙通信信息窃取攻击试验	通信数据具备安全配对流程。	2	2
		通信数据无安全配对流程。	-1	
		车辆无低功耗蓝牙或其他不适用的情况。	0	

	蓝牙协议模糊攻击试验	低功耗蓝牙正常工作。	2	4
		低功耗蓝牙无法正常工作。	-1	
		车辆无低功耗蓝牙或其他不适用的情况。	0	
		经典蓝牙正常工作。	2	
		经典蓝牙无法正常工作。	-1	
		车辆无经典蓝牙或其他不适用的情况。	0	
	GSM 网络劫持攻击试验	车辆未接入伪基站。	2	2
		车辆接入伪基站，不可正常对外通信。	-1	
		车辆接入伪基站，可正常对外通信。	-2	
		车辆无蜂窝通信功能或其他不适用的情况。	0	