IVISTA

网 联 智 能 与 隐 私 安 全 专 项 测 评

编号：IVISTA-XXXX-XX-XXXX.XX-XX-XX-XXXX

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

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-XXXX-XX-XXXX.XX-XX-XX-XXXX 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 25 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 17 分，具体评分规则见附录E 网络通信安全评分规则；

极限攻防安全试验，满分 5 分，具体评分规则见附录F 极限攻防安全评分规则。若测试车型参与极限攻防安全试验且通过，则在网络安全测评五个系统总分基础上加 5 分。

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+极限攻防安全试验加分-（-53）

得分区间值=73-（-53）=126

表 1 网络安全评价

评价方法	综合得分率≥90%	80%≤综合得分率＜90%	70%≤综合得分率＜80%	综合得分率＜70%
评价等级	优秀（G）	良好（A）	一般（M）	较差（P）

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；且，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；但，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	

注：车辆解锁状态包括车灯闪烁、车后视镜折叠展开、车门把手弹出、车辆车门解锁提示声等。

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（蜂窝网络、蓝牙通信、Wi-Fi 通信），试验车辆定位位置准确，未被欺骗或干扰。且，结果 2：关闭车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi 通信），试验车辆定位位置准确，未被欺骗或干扰。	4	4
		结果 1：打开车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi 通信），试验车辆定位位置准确，未被欺骗或干扰。结果 2：关闭车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi 通信），试验车辆定位位置不准确；或无法关闭车辆无线通信。	3	
		结果 1：打开车辆无线通信（蜂窝网络、蓝牙通信、Wi-Fi 通信），试验车辆定位位置不准确。	-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 25 分，包括控车App加固安全性试验 5 分、控车App漏洞扫描试验 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；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 漏洞扫描试验	低危漏洞数量（个）≤5	若不存在中、高危或严重漏洞，则根据低危漏洞数量判定得分情况；若存在中、高危或严重漏洞，则在得分基础上进行扣分，1 个中危漏洞扣 1 分、1 个高危漏洞或严重漏洞扣 2 分，最多扣至-4 分。	5	5
		5＜低危漏洞数量（个）≤7		4	
		7＜低危漏洞数量（个）≤9		3	
		9＜低危漏洞数量（个）≤11		2	
		11＜低危漏洞数量（个）≤13		1	
		低危漏洞数量（个）＞13		0	
		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、远程连接服务试验 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	车机不可运行恶意程序。	3	3
		车机可运行恶意程序。	-2	
		车机无 USB 接口或其他不适用的情况。	0	
	ADB 调试安全检查试验	不可接入 ADB 调试。	3	3
		可接入 ADB 调试，但无 root 权限。	-2	
		可接入 ADB 调试，且有 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	
	未授权的远程连接服务试验	车辆不存在未授权的远程连接服务。	3	3
		车辆存在未授权的远程连接服务。	-2	

附录 E

网络通信安全评分规则

网络通信安全评价总分 17 分，其中 Wi-Fi 攻击试验 9 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 热点破解试验	结果 1：车辆热点默认密码是 8 位以上数字、大小写字母、特殊符号两种以上的组合。	1	3
		结果 1：车辆热点默认密码不是 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：车辆修改密码有强度提示。	1	
		结果 2：车辆修改密码无强度提示。	-1	
		结果 3：车辆修改密码有强制要求。	1	
		结果 3：车辆修改密码无强制要求。	-1	
		车辆无 Wi-Fi 热点功能或其他不适用的情况。	0	
	Wi-Fi 断连攻击试验	车辆未断开连接。	2	2
		车辆断开连接。	-1	
		车辆无 Wi-Fi 热点功能或其他不适用的情况。	0	
	恶意钓鱼 Wi-Fi 攻击试验	车辆未自动连接到恶意钓鱼 Wi-Fi。	2	2
		车辆自动连接到恶意钓鱼 Wi-Fi。	-1	
		车辆无 Wi-Fi 功能或其他不适用的情况。	0	
	Wi-Fi 协议模糊攻击试验	车辆 Wi-Fi 正常工作。	2	2
		车辆 Wi-Fi 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	
	蓝牙通信信息窃取试验	通信过程具备安全配对流程。	2	2
		通信过程无安全配对流程。	-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	

附录 F

极限攻防安全评分规则

极限攻防安全试验总分 5 分。若控车App深度对抗试验、车内网络攻防试验全部测试项扣分合计小于20分，则极限攻防安全试验整体得5分；若扣分大于或等于20分，则极限攻防安全试验整体不得分。

F.1 极限攻防安全试验评分表

项目	试验场景	结果指标	得分情况
极限攻防安全	控车 App 深度对抗试验	能对控车 App 进行脱壳	-1
		不能对控车 App 进行脱壳	0
		能绕过 Frida/Xposed 检测	-1
		不能绕过 Frida/Xposed 检测	0
		能绕过 SSL Pinning 检测	-1
		不能绕过 SSL Pinning 检测	0
		不存在身份认证机制	-2
		存在身份认证机制，但是可以被绕过	-1
		存在身份认证机制，无法被绕过	0
		通信数据包无校验字段	-2
		通信数据包存在校验字段，且算法能被还原	-1
		通信数据包存在校验字段，且无法被还原	0
		不存在权限控制	-2
		存在权限控制，但是可以被绕过	-1
		存在权限控制，且无法被绕过	0
		成功解锁车辆	-20
		无法解锁车辆	0
	车内网络攻防试验	可以识别以太网接口，且能够完成通信嗅探	-1
		无法识别以太网接口，或识别出的以太网接口无法完成通信嗅探	0
		识别出的已知高危及严重漏洞数	-20/个
		识别出的已知中危漏洞数	-5/个

		识别出的已知低危漏洞数	-1/个
		能够获取调试接口权限的零部件数量	-1/个
		通过调试接口能够获取到 system/root 权限的零部件数量	-5/个
		能够受控发送以太网/CAN 通信，以控制车辆解锁或车身动作的零部件数量	-5/个
		可通过 Wi-Fi/蓝牙控制车辆解锁或车身动作	-20
		不可通过 Wi-Fi/蓝牙控制车辆解锁或车身动作	0