IVISTA

网 联 智 能 与 隐 私 安 全 专 项 测 评

编号：IVISTA-CIPS-SM-CSPS.CS-RP-A0-2023

网络与隐私安全
网络安全评价规程

Cybersecurity and Privacy Security

Cybersecurity Rating Protocol

（2023 版）

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-CIPS-SM-CSPS.CS-TP-A0-2023 网络与隐私安全_网络安全试验规程（2023版）

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 14 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；

极限攻防安全试验，满分 7 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 7 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。以综合得分进行评价等级的划分，如表 1 所示。

综合得分=数字钥匙安全得分+导航定位安全得分+远程控车安全得分+车端接口安全得分+网络通信安全得分+极限攻防安全加分

优秀（G）：综合得分≥38；

良好（A）：26≤综合得分＜38；

一般（M）：10≤综合得分＜26；

较差（P）：综合得分＜10。

表 1 网络安全评价

评价方法	综合得分≥38	26≤综合得分＜38	10≤综合得分＜26	综合得分＜10
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

A.1 概述

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 2 分、蓝牙钥匙中继攻击试验 2 分、NFC 钥匙中继攻击试验 4 分，如表 A.1 所示。

表 A.1 数字钥匙安全评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
数字钥匙安全	射频钥匙重放攻击试验	通过：结果 1：车辆未被解锁； 不通过：结果 1：车辆被解锁。	3	-3	0
		加分项 通过：结果 2：车辆未被解锁； 不通过：结果 2：车辆被解锁。	+1	0	0
	蓝牙钥匙重放攻击试验	通过：车辆未被解锁； 不通过：车辆被解锁。	2	-1	0
	蓝牙钥匙中继攻击试验	通过：车辆未被解锁； 不通过：车辆被解锁。	2	-1	0
	NFC 钥匙中继攻击试验	通过：结果 1：车辆未被解锁； 不通过：结果 1：车辆被解锁。	2	-1	0
		通过：结果 2：车辆未被解锁； 不通过：结果 2：车辆被解锁。	2	-1	0

注:加分项：指在满足基础网络安全条件下，进行深层次网络安全性能测试的测试项目。加分项通过加分，加分项不通过不进行扣分。

A.2 射频钥匙重放攻击试验评分

a）针对射频钥匙重放攻击试验，若结果满足表 A.1 评价指标的要求，该对应试验工况得分，其中试验车辆处于静止锁车的状态场景，重放攻击下车辆未解锁（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），满足车辆未解锁（结果 1 ）则得 3 分，否则扣 3 分；

满足车辆未解锁（结果 2 ）得加分 1 分,总计得分 4 分；

b）若试验车辆未搭载射频钥匙功能，则射频钥匙重放攻击试验不得分。

A.3 蓝牙钥匙重放攻击试验评分

a）针对蓝牙钥匙重放攻击试验，若结果满足表 A.1 评价指标的要求，该对应试验工况得分，其中试验车辆处于静止锁车的状态场景，重放攻击下车辆未解锁（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），则得 2 分，否则扣 1 分；

b）若试验车辆未搭载蓝牙钥匙功能，则蓝牙钥匙重放攻击试验不得分。

A.3 蓝牙钥匙中继攻击试验评分

a）针对蓝牙钥匙中继攻击试验，若结果满足表 A.1 评价指标的要求，该对应试验工况得分，其中试验车辆处于静止锁车的状态场景，中继攻击下车辆未解锁（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），则得 2 分，否则扣 1 分；

b）若试验车辆未搭载蓝牙钥匙功能，则蓝牙钥匙中继攻击试验不得分。

A.4 NFC 钥匙中继攻击试验评分

a）针对 NFC 钥匙中继攻击试验，若结果满足表 A.1 评价指标的要求，该对应试验工况得分，其中试验车辆处于静止锁车的状态场景，进行 NFC 中继攻击车辆未解锁（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），满足车辆未解锁（结果 1 ），得 2 分，否则扣 1 分；满足车辆未解锁（结果 2 ），得 2 分，否则扣 1 分；

b）若试验车辆未搭载 NFC 钥匙功能，则 NFC 钥匙中继攻击试验不得分。

附录 B

导航定位安全评分规则

B.1 概述

导航定位安全评价总分 4 分，包括 GNSS 信号伪造场景 2 分、GNSS 信号干扰场景 2 分，如表 B.1 所示。

表 B.1 导航定位安全评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
导航定位安全	GNSS 信号伪造试验	通过：结果 1：试验车辆定位服务未被欺骗，未定位到指定位置； 不通过：结果 1：试验车辆定位服务被欺骗，定位到指定位置。	1	-1	0
		加分项 通过：结果 2：试验车辆定位服务未被欺骗，未定位到指定位置； 不通过：结果 2：试验车辆定位服务被欺骗，定位到指定位置。	+1	0	0
	GNSS 信号干扰试验	通过：结果 1：试验车辆定位服务未被干扰，可以正确定位； 不通过：结果 1：试验车辆定位服务被干扰，无法正确定位。	1	-1	0
		加分项 通过：结果 2：试验车辆定位服务未被干扰，可以正确定位； 不通过：结果 2：试验车辆定位服务被干扰，无法正确定位。	+1	0	0

注:加分项：指在满足基础网络安全条件下，进行深层次网络安全性能测试的测试项目。加分项通过加分，加分项不通过不进行扣分。

B.2 GNSS 信号伪造试验评分

a）针对 GNSS 信号伪造试验，若结果满足表 B.1 评价指标的要求，该对应试验工况得分，其中试验车辆具有导航功能，车辆具备抵抗虚假的 GNSS 信号避免车辆定位错误或者受到误导的能力，车辆定位服务未被欺骗（结果 1 ）则得 1 分，否则扣 1 分；车辆定位服务未被欺骗（结果 2 ）得加分 1 分,总计得分 2 分；

b）若试验车辆不具备导航功能，则 GNSS 信号伪造试验不得分。

B.3 GNSS 信号干扰试验评分

a）针对GNSS信号干扰试验，若结果满足表 B.1 评价指标的要求，该对应试验工况得分，其中试验车辆辆具有导航功能,车辆在使用GNSS系统进行定位时,不会受到外部干扰导致信号质量下降或定位精度受影响，车辆定位服务未被干扰（结果 1 ）则得 1 分，否则扣 1 分，车辆定位服务未被干扰（结果 2 ）得加分 1 分,总计得分 2 分；

b）若试验车辆不具备导航功能，则 GNSS 信号干扰试验不得分。

附录 C

远程控车安全评分规则

C.1 概述

远程控车安全评价总分 20 分，包括控车App安全扫描试验 8 分、控车App通信安全性试验 2 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。

C.2 控车 App 安全扫描试验评分

控车 App 安全扫描试验总分 8 分，其中 App 基线扫描试验 4 分、App 漏洞扫描试验 4 分，评分规则如表 C.1 所示。

表 C.1 控车 App 安全性试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
控车 App 安全扫描	App 基线扫描试验	通过：App 基线扫描安全； 不通过：App 基线扫描不安全。	4	-3	0
	App 漏洞扫描试验	通过：App 漏洞扫描安全（低危漏洞≤5，且无中高危漏洞）； 不通过：App 漏洞扫描不安全（低危漏洞＞5，或存在中高危漏洞）。	4	-3	0

在控车 App 安全扫描试验中，若 App 基线扫描安全则为通过得 4 分，反之为不通过扣 3 分；若 App 漏洞扫描低危漏洞≤5，且无中高危漏洞则为通过，得 4 分，其余情况为不通过扣 3 分。

C.3 控车 App 通信安全性试验评分

控车 App 通信安全性试验总分 2 分，评分规则如表 C.2 所示。

表 C.2 App 控车指令重放攻击试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
控车 App 通信安全性	控车 App 通信安全性试验	通过：使用了安全的传输协议； 不通过：未使用安全的传输协议。	2	-1	0

在控车 App 通信安全性试验中，若控车 App 数据通信使用 HTTPS 协议且经过 SSL/TLS 加密处理，TLS 版本大于等于 1.2；或使用 IPsec 协议为为通过，得 2 分，其他情况为不通过扣 1 分。

C.4 App 控车指令重放攻击试验评分

App 控车指令重放攻击试验总分为 5 分，评分规则如表 C.3 所示。

表 C.3 App 控车指令重放攻击试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
App 控车指令重放攻击	App 控车指令重放攻击试验	通过：车辆未执行控制操作； 不通过：车辆执行控制指令。	5	-4	0

在 App 控车指令重放攻击试验中，若控车 App 无法进数据流量代理，或可进行数据流量代理且测试结果为车辆未执行控制操作，则为通过得 5 分，反之为不通过扣 4 分。

C.5 App 控车指令篡改攻击试验评分

App 控车指令篡改试验总分为 5 分，评分规则如表 C.4 所示。

表 C.4 App 控车指令篡改攻击试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
App 控车指令篡改攻击	App 控车指令篡改攻击试验	通过：车辆未执行控制操作； 不通过：车辆执行控制指令。	5	-4	0

在 App 控车指令篡改攻击试验中，若控车 App 无法进数据流量代理，或可进行数据流量代理且测试结果为车辆未响应篡改后的攻击数据包，则为通过得 5 分，反之为不通过扣 4 分。

附录 D

车端接口安全评分规则

D.1 概述

车端接口安全评价总分 14 分，包括USB接口试验 7 分、OBD接口试验 2 分、充电接口试验 3 分、远程连接服务接口试验 2 分。

D.2 USB 接口试验评分

D.2.1 概述

USB接口试验总分 7 分，其中USB接口访问控制试验 2 分、USB接口防病毒试验 2 分、ADB调试安全检查试验 3 分，如表 D.1 所示。

表 D.1 USB 接口试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
USB 接口	USB 接口访问控制试验	通过：车机仅能识别清单允许格式的文件； 不通过：车机能识别清单允许格式以外其他格式文件。	2	-1	0
	USB 接口防病毒试验	通过：车机不可运行恶意程序； 不通过：车机可运行恶意程序。	2	-1	0
	ADB 调试安全检查试验	通过：不可接入 ADB 调试； 不通过：可接入 ADB 调试。	3	-2	0
		附加项 通过：ADB 调试无 root 权限； 不通过：ADB 调试有 root 权限。	0	-1	0

注:附加项：指在不满足网络安全条件下，完善网络安全性能测试的测试项目。附加项通过不扣分，附加项不通过进行扣分。

D.2.2 USB 接口访问控制试验评分

a）针对 USB 接口访问控制试验，若结果满足表 D.1 评价指标的要求，该对应试验工况得分，若车机仅能识别清单允许格式的文件,则得 2 分;若车机能识别清单允许格式以外其他格式文件,则扣 1 分；

b）若试验车辆未搭载 USB 接口功能，则 USB 接口访问控制试验不得分。

D.2.3 USB 接口防病毒试验评分

a）针对 USB 接口防病毒试验，若结果满足表 D.1 评价指标的要求，该对应试验工况得分，若车机不可运行恶意程序，则得 2 分，反之扣 1 分；

b）若试验车辆未搭载 USB 接口功能，则 USB 接口防病毒试验不得分。

D.2.4 ADB 调试安全检查试验评分

a）针对 ADB 调试安全检查试验，若结果满足表 D.1 评价指标的要求，该对应试验工况得分。若无法接入 ADB 调试权限则得 3 分；若 ADB 具备调试功能但无 root 权限则扣 2 分；若 ADB 具备调试功能且有 root 权限则扣 3 分；

b）若试验车辆未搭载 USB 接口功能，则 ADB 调试安全检查试验不得分。

D.3 OBD 接口访问控制试验评分

D.3.1 概述

OBD接口访问控制试验 2 分，如表 D.2 所示。

表 D.2 OBD 接口试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
OBD 接口	OBD 接口访问控制试验	通过：车辆 OBD 接口访问控制机制有效； 不通过：车辆 OBD 接口访问控制机制无效。	2	-1	0

D.3.2 OBD 接口访问控制试验评分

针对 OBD 接口试验，若结果满足表 D.2 评价指标的要求，该对应试验工况得分，若试验车辆 OBD 接口访问控制机制有效，则得 2 分，反之扣 1 分。

D.4 充电接口试验评分

D.4.1 概述

充电接口试验总分 3 分，其中直流充电接口模糊攻击试验 1 分、直流充电口的CAN隔离试验 2 分，如表 D.3 所示。

表 D.3 充电接口试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
充电接口	直流充电接口模糊攻击试验	通过：车辆充电状态未受影响； 不通过：车辆充电状态受影响。	1	-1	0
	直流充电口的 CAN 隔离	通过：车辆不响应非充电相关的 CAN 消息； 不通过：车辆响应非充电相关的 CAN 消息。	2	-1	0

D.4.2 直流充电接口模糊攻击试验评分

a）针对直流充电接口模糊攻击试验，若结果满足表 D.3 评价指标的要求，该对应试验工况得分，其中测试车辆在充电过程中，模糊攻击无法对车辆充电造成影响，则得 1 分，反之扣 1 分；

b）若试验车辆不具有直流充电功能，则不得分。

D.4.3 直流充电口 CAN 隔离试验评分

a）针对直流充电口的 CAN 隔离试验，若结果满足表 D.3 评价指标的要求，该对应试验工况得分，其中测试车辆在充电过程中，发送与充电无关的 CAN 消息，若试验车辆不响应，则得 2 分，反之扣 1 分；

b）若试验车辆不具有直流充电功能，则不得分。

D.5 远程连接服务试验评分

D.5.1 概述

远程连接服务试验总分 2 分，如表 D.4 所示

表 D.4 远程连接服务试验评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
远程连接服务	远程连接服务试验	通过：车辆不存在未授权的远程连接服务； 不通过：车辆存在未授权的远程连接服务。	2	-1	0

D.5.2 远程连接服务试验评分

a）针对车辆远程连接服务试验，若结果满足表 D.4 评价指标的要求，该对应试验工况得分，其中车辆不存在未授权的远程连接服务，则得 2 分；反之扣 1 分；

b）若试验车辆不具有 Wi-Fi 及热点功能，则不得分。

附录 E

网络通信安全评分规则

E.1 概述

网络通信安全评价总分 16 分，其中 Wi-Fi 攻击试验 5 分、蓝牙攻击试验 4 分、GSM 网络劫持攻击试验 4 分，升级刷写设备认证试验 3 分，如表 E.1 所示。

表 E.1 网络通信安全评分表

项目	试验场景	评价指标	通过	不通过	无此项功能
网络通信安全	Wi-Fi 热点破解攻击试验	通过：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； 不通过：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	-1	0
		加分项： 通过：结果 2：车辆修改密码有强度提示； 不通过：结果 2：车辆修改密码无强度提示。	+0.5	0	0
		加分项： 通过：结果 3：车辆修改密码有强制要求； 不通过：结果 3：车辆修改密码无强制要求。	+0.5	0	0
	Wi-Fi 断连攻击试验	通过：车辆未断开连接； 不通过：车辆断开连接。	1	-1	0
	恶意钓鱼 Wi-Fi 攻击试验	通过：车辆未自动连接到恶意钓鱼 Wi-Fi； 不通过：车辆自动连接到恶意钓鱼 Wi-Fi。	1	-1	0
	Wi-Fi 协议模糊攻击试验	通过：车辆 Wi-Fi 正常工作； 不通过：车辆 Wi-Fi 不能正常工作。	1	-1	0
	蓝牙通信信息窃取试验	通过：通信过程具备安全配对流程； 不通过：通信过程无安全配对流程。	2	-1	0
	蓝牙协议模糊攻击试验	通过：低功耗蓝牙正常工作； 不通过：低功耗蓝牙无法正常工作。	1	-1	0

		通过：经典蓝牙正常工作； 不通过：经典蓝牙无法正常工作。	1	-1	0
	GSM 网络劫持攻击试验	通过：结果 1：车辆未接入伪基站； 不通过：结果 1：车辆接入伪基站。	4	-3	0
		附加项 通过：结果 2：车辆可以正常对外通信； 不通过：结果 2：车辆无法正常对外通信。	0	-1	0
	升级刷写设备认证试验	通过：车辆未返回肯定响应； 不通过：车辆返回肯定响应。	3	-2	0

注 1：加分项：指在满足基础网络安全条件下，进行深层次网络安全性能测试的测试项目。加分项通过加分，加分项不通过不进行扣分。

注 2：附加项：在不满足网络安全条件下，完善网络安全性能测试的测试项目。附加项通过不扣分，附加项不通过进行扣分。

E.2 Wi-Fi 热点破解攻击试验评分

a）针对 Wi-Fi 热点破解攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆 Wi-Fi 功能正常，可开启 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（结果 1 ）则得 1 分，否则扣 1 分；车辆修改密码有强度提示（结果 2 ）加 0.5 分，车辆修改密码有强制要求（结果 3 ）加 0.5 分，得分总计 2 分；

b）若试验车辆未搭载 Wi-Fi 热点功能，则 Wi-Fi 热点破解攻击试验不得分。

E.3 Wi-Fi 断连攻击试验评分

a）针对 Wi-Fi 断连攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆 Wi-Fi 功能正常，可开启 Wi-Fi 热点，断连攻击下车辆热点与测试设备未断开连接则得 1 分，否则扣 1 分；

b）若试验车辆未搭载 Wi-Fi 热点功能，则 Wi-Fi 断连攻击试验不得分。

E.4 恶意钓鱼 Wi-Fi 攻击试验评分

a）针对恶意钓鱼 Wi-Fi 攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆 Wi-Fi 功能正常，可开启 Wi-Fi 热点，车辆未自动连接到恶意钓鱼 Wi-Fi 则得 1 分，否则扣 1 分；

b）若试验车辆未搭载 Wi-Fi 热点功能，则恶意钓鱼 Wi-Fi 攻击试验不得分。

E.5 Wi-Fi 协议模糊攻击试验评分

a）针对 Wi-Fi 协议模糊攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆 Wi-Fi 功能正常，可开启 Wi-Fi 热点，车辆 Wi-Fi 正常工作则得 1 分，否则扣 1 分；

b）若试验车辆未搭载 Wi-Fi 热点功能，则 Wi-Fi 协议模糊攻击试验不得分。

E.6 蓝牙通信信息窃取攻击试验评分

a）针对蓝牙通信信息窃取攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆具备蓝牙功能，蓝牙通信数据具备安全配对流程则得 2 分，否则扣 1 分；

b）若试验车辆未搭载蓝牙功能，则蓝牙通信信息窃取攻击试验不得分。

E.7 蓝牙协议模糊攻击试验评分

a）针对蓝牙协议模糊攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆具备蓝牙功能，低功耗蓝牙正常工作则得 1 分，否则扣 1 分；经典蓝牙正常工作则得 1 分，否则扣 1 分；

b）若试验车辆未搭载蓝牙功能，则蓝牙协议模糊攻击试验不得分。

E.8 GSM 网络劫持攻击试验评分

a）针对 GSM 网络劫持攻击试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆具备对外通信功能（定位服务功能、蜂窝网络功能），车辆未接入伪基站（结果 1 ）则得 4 分，否则扣 3 分；车辆接入伪基站，车辆可以正常对外通信则满足要求，否则扣 1 分；

b）若试验车辆未搭载对外通信功能，则 GSM 网络劫持攻击试验不得分。

E.9 升级刷写设备认证试验评分

a）针对升级刷写设备认证试验，若结果满足表 E.1 评价指标的要求，该对应试验工况得分，其中试验车辆处于静止锁车的状态场景，对恶意升级指令返回否定响应或不响应，则得 3 分，否则扣 2 分；

b）若试验车辆不具备近端升级功能，则刷写设备认证试验不得分。

附录 F

极限攻防安全评分规则

F.1 评分方法

极限攻防安全试验总分 7 分，评分规则如下：

a）针对每一项生产制造商提供的输入项目，远程调试接口和零部件满足一项即可加 0.5 分，单项最多加 0.5 分，总计最多可加 2 分，生产制造商未提供输入则不得分；

b）测试过程结束，低危漏洞数量≤ 40、中危漏洞≤ 5、无高危漏洞、无严重漏洞，加 5 分；低危漏洞数量＞ 40，或中危漏洞＞ 5，或存在高危漏洞，或存在严重漏洞则不得分。

注：发现漏洞库中的已知漏洞按照对应漏洞库的评级计算，自由渗透阶段发现的漏洞按照 CVSS 计算漏洞评级。

具体评价标准如表 F.1 所示。

表 F.1 极限攻防安全评分表

项目	试验场景	评价指标	得分
极限攻防安全试验	车企输入	车载信息娱乐系统/IVI 远程调试接口或零部件及主要外部接口说明	+0.5
		车载通信系统/TBOX 远程调试接口或零部件及主要外部接口说明	+0.5
		车载网关 远程调试接口或零部件及主要外部接口说明	+0.5
		自动驾驶域控制器 远程调试接口或零部件及主要外部接口说明	+0.5
	渗透测试	低危漏洞数量≤ 40、中危漏洞数量≤ 5、无高危漏洞、无严重漏洞	+5