ICS43.040.10

中国汽车工业协会团体标准 XXX

T/XXX-XXX-2020

自 动 驾 驶 系 统 功 能 测 试
第 9 部分：信息安全评价测试
Test methods for functions of automated driving system
Part 9:
Assessment Specification for Cybersecurity

（征求意见稿）

2020-xx-xx 发布　　2020-xx-xx 实施

中国汽车工业协会 发布

前　言

随着智能网联汽车快速发展，很多重大问题逐步凸显，其中安全问题成为制约联网快速发展的重要因素。目前智能网联汽车安全现状不容忽视，汽车攻击手段升级，正日益威胁人民的生命和财产安全。安全事件已突显。随着黑客攻击手段升级，多家汽车厂商曾遭遇攻击；汽车产业链过长，增加了汽车安全问题的复杂性；安全企业和整车厂合作深度不深；未建立其长效和稳固的合作。

为指导汽车整车信息安全评估的开展工作，本规范给出了汽车测评体系、评分机制和汽车零部件的评测方法清单的指导参考。

本标准参考有关国家标准、行业标准，结合我国生产企业实际情况及用户要求制定。

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中国汽车工业协会提出。

本标准由中国汽车工业协会归口。

本标准起草单位：中国汽车工业协会，中国第一汽车集团有限公司，北京汽车新能源有限公司，长城汽车股份有限公司，福特汽车（中国）有限公司，上海机动车检测认证技术研究中心有限公司，重庆车辆检测研究院有限公司，北京航空航天大学，清华大学，北京理工大学， 北京百度网讯科技有限公司（百度Apollo汽车信息安全实验室），上海犖联网络科技有限公司

本标准主要起草人：

目录

自动驾驶系统功能测试

第 9 部分：信息安全评价测试

1 范围

本规范规定了智能网联汽车信息安全的评估体系和评估方法。
本规范适用但不限于智能网联汽车车载 T-BOX、车载综合信息处理系统 In-Vehicle Infotainment、汽车网关和汽车 ECU 等车内控制器的信息安全评估。

2 规范性引用文件

GB/T 20271 信息安全技术 信息系统通用 安全技术要求
GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
GB/T 31509-2015 《信息安全技术 信息安全风险评估实施指南》
GB/T 30279-2013 信息安全技术 安全漏洞等级划分指南
GB/T 35273-2017 《信息安全技术 个人信息安全规范》
NIST SP 800-53 《美国国家标准技术研究所安全标准-信息系统与安全目标及风险级别对应指南》
NIST SP 800-60 《美国国家标准技术研究所安全标准-将信息和信息系统映射到安全类别的指南》
ISO (International Organization for Standardization). Road vehicles—Functional safety (ISO 26262:2011).
CCRA Members. Common Criteria for Information Technology Security Evaluation -Version 3.1, Revision 4.
Common Vulnerability Scoring System v3.0: User Guide (CVSS)
HEAling Vulnerabilities to ENhance Software Security and Safety V2.0(HEAVENS)
EVITA Project. E-safety Vehicle Intrusion Protected Applications (EVITA).
SAEJ3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
OWASP. OWASP Risk Rating Methodology &Threat Risk Modeling.
ETSI. Intelligent Transport Systems (ITS). Security; Threat, Vulnerability and Risk Analysis (TVRA).
ETSI. Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).
The Key Principles of Cyber Security for Connected and AutomatedVehicles. UK
Framework for Automotive Cy-bersecurity Best Practices. US

3 术语和定义

3.1 资产 asset

对组织具有价值的信息或资源，是安全策略保护的对象。

3.2 资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

3.3 可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

3.4 机密性 Confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

3.5 （信息安全）风险评估(information security)risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

3.6 信息系统 information system

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

典型的信息系统由三部分组成：硬件系统（计算机硬件系统和网络硬件系统）丰系统软件（计算机系统软件和网络系统软件）；应用软件（包括由其处理、存储的信息）。

3.7 完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

3.8 安全措施 security measure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响以及打击信息犯罪而实施的各种实践、规程和机制。

3.9 威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

3.10 脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

3.11 安全事件 security incident

系统、服务或网络的一种可识别状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或未预知的不安全状况。

3.12 组织 organization

由作用不同的个体为实施共同的业务目标而建立的结构。一个单位是一个组织．某个业务部门也可以是一个组织。

4 缩略语

表 1 缩略语

缩写	英文解释	中文解释
T-BOX	Telematics-Box	汽车通讯模块
GW	Gateway	汽车网关
CAN	Controller Area Network	控制局域网络
ECU	Electronic Control Unit	电子控制单元
IVI	In-Vehicle Infotainment	汽车信息娱乐系统
TSP	Telematics Service Provider	信息服务提供商
OTA	Over-The-Air	空中下载
STRIDE	Spoofing、Tampering、Repudiation、Information disclosure、Denial of Service、Elevation of Privilege	一种威胁建模模型
ES	Exploit Score	可用性得分
SS	Severity Scoring	严重性得分
AV	Attack Vector	攻击途径
TV	Time Vector	时间窗口
EV	Expert knowledge Vector	专业知识
KV	Knowledge Vector	目标知识
AE	Attack Equipment	攻击设备
AA	Attack Authorization	攻击授权
CI	Confidentiality Impact	机密性
II	Integrity Impact	完整性
AI	Availability Impact	可用性
SV	Safety Vector	人身安全
FV	Financial Vector	财产损失
PV	Privacy Vector	隐私安全
OV	Operation Vector	功能向量
EVITA	E-safety vehicle intrusion protected applications	欧盟第七框 架计划（Seventh Framework Programme）资助的项目（2008-2011）
HEAVENS	HEAling Vulnerabilities to ENhance Software Security and Safety	一种汽车安全风险评估模型
CVSS	Common Vulnerability Scoring System v3.0: User Guide	安全漏洞评分系统
V2X	vehicle to everything	车对外界的信息交换
TVRA	Threat, Vulnerability and Risk Assessment	威胁、脆弱性和风险评估
MPU	Microprocessor Unit	微处理器
JTAG	Joint Test Action Group	一种调试接口

5 安全体系架构

智能网联汽车信息安全架构如图 1 所示，整体安全由云端安全、通信安全、车辆安全等多个部分构成。其中车载端作为智能网联汽车内外通信的重要节点，是车辆安全的重要组成部分，保证汽车内部总线和子系统不因车辆具有联网功能而增加安全风险。

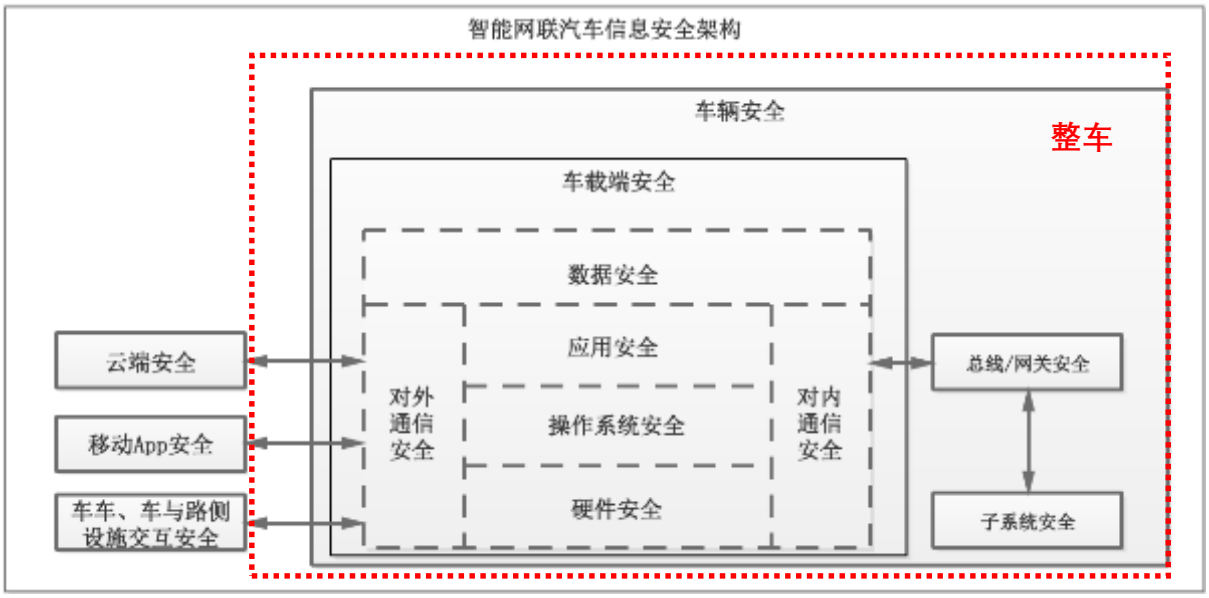

图 1 智能网联汽车信息安全体系架构

6 安全威胁分析及技术要求

6.1 汽车信息安全威胁分析

6.1.1 云服务平台

云服务平台可能存在安全漏洞，使得攻击者利用 Web 漏洞、数据库漏洞、接口 API 安全注入漏洞等攻击云平台，窃取敏感信息，以及面临拒绝服务攻击等问题。除了传统云服务平台漏洞外，云端与两端的传输安全、云端 OTA 升级整车零部件的安全问题也多次出现。

6.1.2 车载终端

车载终端包括 IVI、T-box、汽车网关、其它 ECU 电子器件、传感器、外部接口等，IVI、T-Box 等组件一般包含操作系统、APP 应用和大量的第三方库，并且具有丰富的通信连接。一方面，操作系统、第三方库、协议栈可能含有大量的已知漏洞，攻击者可以通过已知漏洞攻入汽车内部网络，进而进行下一步渗透测试；另一方面，ECU 电子器件、车内 CAN 网络可能存在漏洞，攻击者可以通过 IVI 或 T-Box 进一步攻击网关或其它 ECU 电子器件（例如动力域 ECU），进而形成完全控车威胁。

6.1.3 手机终端

移动 APP 成为智能网联汽车的标配，由于获取成本极低，通过技术手段可以破解通信密钥、分析通信协议，并结合车联网远程控制功能干扰用户使用，同时也可协助对 IVI/T-BOX 进行渗透测试，通过攻击车联网关键部件影响车辆行驶安全。

6.1.4 通信网络

车与云、车与车和车内的通信存在被攻击风险，主要风险如下：一是认证安全，用户通信网络未验证发送者的身份信息，存在伪造身份、动态劫持等风险。二是传输安全，车辆信息没有加密或加密强度弱，或所有车型都使用相同的对称密钥，进而导致密钥信息暴露。三是协议安全，公众通信网络

还面临协议伪装等风险。特别是在自动驾驶情况下，汽车根据 V2X 通信内容判断行驶路线，攻击者就有可能利用伪造消息来诱导车辆发生误判，进而影响车辆自动控制，导致交通事故的发生。

6.2 汽车信息安全威胁列表

参考《信息安全技术 信息系统安全等级保护基本要求》，使用 STRIDE 和 TVRA 分析方法建立威胁列表如下：

表 2 汽车信息安全威胁列表

评估对象	威胁组件	威胁描述（举例）	影响范围
云服务平台	OTA 升级	OTA 升级过程面临升级包泄露、篡改风险，从而攻击者可以获取敏感信息，或向升级包中置入后门。	TSP、T-Box
	管理平台登录	弱身份认证缺陷使得攻击者能通过伪造凭证的方式访问车联网管理平台，并进行网络攻击。	TSP
	服务端功能	后端服务中的管理错误，或者存储用于诊断车库数据时发生错误分享，导致信息泄露、共享。	TSP
	云端存储	敏感数据可能因第三方云服务提供商存储的攻击或事故，造成泄露或丢失	TSP
	服务端代码	代码可能存在 SQL 注入、跨站脚本、用户鉴权、账户口令等安全漏洞，使得攻击者利用漏洞窃取隐私、篡改等攻击。	TSP
车载终端	IVI	IVI 附属功能多、集成度高，因而攻击面大、风险多，所有接口都有可能成为黑客攻击的节点，攻击者可以通过攻击 IVI 作为跳板，进而控制车辆行驶，对整车系统造成篡改、拒绝服务、隐私泄露等安全威胁。	ECU、Gateway、T-BOX/IVI
	T-Box	攻击者通过逆向分析 T-BOX 固件，获取加密算法和密钥，从而解密通信协议，用于窃听隐私或伪造控车指令；或者通过 T-BOX 预留调试泄露内部信息用于攻击分析。	ECU、Gateway、T-BOX/IVI
	汽车网关	网关系统代码可能存在漏洞，攻击者利用车载以太网或 CAN 总线漏洞攻击网关，可以造成网关的篡改、拒绝服务、指令伪造等风险。	ECU、Gateway、T-BOX/IVI
	其它 ECU	车内各类 ECU 存在固件代码篡改、拒绝服务等威胁。	ECU、Gateway、T-BOX/IVI
	传感器	攻击者可以通过攻击胎压监测传感器漏洞进入汽车内部网络，对车内网络进行拒绝服务或进一步渗透攻击，进而影响车辆行驶安全。	ECU、Gateway、T-BOX/IVI

	OBD 接口	OBD 接口接入的外接设备可能存在攻击代码，接入后容易将安全威胁引入到汽车总线网络中，对汽车总线控制带来威胁。	ECU、Gateway、T-BOX/IVI
	充电接口	充电接口驱动存在漏洞，恶意攻击者通过在充电桩上置入病毒恶意代码，在汽车充电时“感染”汽车。	ECU、Gateway、T-BOX/IVI
	板载硬件	板载硬件中暴露可用的调试连接接口，攻击者可以使用连接泄露硬件内部信息或泄露，进而帮助攻击者进一步的车辆渗透。	ECU、Gateway、T-BOX/IVI
	固件	硬件 flash 中的固件未做防护，使得攻击者可提取、修改，造成代码、密钥等泄漏。	ECU、Gateway、T-BOX/IVI
	存储系统	攻击者可以使用侧信道攻击技术获取芯片中的隐私信息。	ECU、Gateway、T-BOX/IVI
手机终端	App	通过调试或者反编译应用来获取通信密钥、分析通信协议，并结合车联网远程控制功能伪造控制指令干扰用户使用，例如进行远程锁定、开启天窗等操作。	APP、TSP
	用户登录	可以伪造假的 TSP 骗取用户登录信息类似钓鱼网站的危害。	APP、TSP
	数据存储	私人或敏感数据（如付款信息，驾驶习惯等）可能会在汽车出售给其他用户时泄露，可能因交通事故或盗窃，敏感数据的泄漏造成人身伤害	APP
通信网络	TSP 通信网络	可以对 TSP 网络通信进行 dos 攻击，阻止其提供正常的服务	TSP、APP、T-Box
	蜂窝通信	攻击者通过伪基站、DNS 劫持等手段劫持 T-BOX 会话，监听通信数据，一方面可以用于通信协议破解，另一方面可窃取汽车敏感数据，如汽车标识 VIN、用户账户信息等。	T-BOX/IVI
	LTE-V2X 通信	车车通信中存在恶意节点入侵，可通过阻断、伪造、篡改车-车通信或者通过重放攻击影响车- 车通信信息的真实性，破坏车-车通信消息的真实性，影响路况信息的传递。	ECU、Gateway、T-BOX/IVI
	Wifi 通信	通过实现 WiFi 认证口令破解，攻击者可以接入到汽车内部网络，获取汽车内部数据信息或者进行渗透攻击。	T-BOX/IVI
	蓝牙通信	例如，蓝牙钥匙代码被篡改（例如固件篡改，置入后门）、权限提升（例如可能进行除开车门的其它高级功能）风险或蓝牙信号泄露数字钥匙信息。	T-BOX/IVI
	车载以太网	Wifi 与车载以太网不做隔离，导致攻击者可以通过 wifi 破解接入 T-Box、网关等车载以太网节点，进而对整车进行渗透测试。	ECU、Gateway、T-BOX/IVI

	CAN 总线	在车内总线上、车内服务系统上持续发送模拟数据信号，导致驾驶系统发生意外或者通过远程诊断漏洞向 T-Box 或 IVI 等置入后门。	ECU、Gateway、T-BOX/IVI

6.3 汽车信息安全技术要求

6.3.1 硬件安全技术要求

汽车零部件应避免存在用以标注芯片、端口和管脚功能的可读丝印；禁用设计验证阶段所使用的调试接口，若必须保留，则必须采用一定的安全访问控制措施；通过硬件措施来防范对固件的提取与逆向。

6.3.2 操作系统安全技术要求

汽车操作系统应及时进行补丁升级；提供安全调用控制与呈现能力；对必须保留的本地或远程管理功能，则要采取必要的安全访问控制措施；通过技术手段对整个系统进行必要的机密性、完整性和可用性防护。

6.3.3 应用安全技术要求

应用安全要保证安装在汽车上的应用软件具备相应的来源标识和保密性、完整性和可用性的防护措施，可以对抗逆向分析、反编译、篡改、非授权访问等各种针对应用的安全威胁，并确保应用产生、使用的数据得到安全的处理、车载端应用与相关服务器之间通信的安全性，保证应用为用户提供服务时，以及应用在启动、升级、登录、退出等各模式下的安全性。

6.3.4 通信安全技术要求

汽车敏感或重要信息通信过程，要对通信双方实施双向身份认证，对通信进行必要的加密处理；要能够防范重放攻击和中间人攻击。

6.3.5 数据安全技术要求

数据安全技术要求采取加密等安全机制保证采集、存储、传输过程中用户数据、车企数据以及供应商数据的安全性，确保数据的保密性、完整性和可用性得到有效的防护，同时具有清除机制，保护数据生命周期各环节的安全性。

6.3.6 第三库安全技术要求

第三库安全技术要求使用安全的第三库，禁止使用安全漏洞频发、认证鉴权等明显不符合安全要求以及缺乏高效更新机制的第三库。

6.3.7 OTA 升级安全技术要求

OTA 升级安全技术要求 OTA 升级过程中车端与服务端采用安全的双向认证、建立安全通道以及对 OTA 升级包进行验证，确保 OTA 升级包的完整性、机密性和可用性。

6.3.8 总线安全技术要求

总线安全技术要求车内总线通信发送节点不被恶意应用调用从而向车内网络发送恶意数据，同时车内总线通信接收节点应对接收到车内数据信息进行合法性校验，必要时可以对关键的信息采用一定保护机制（例如：防重放机制、加密机制）。

7 汽车整车信息安全测试内容

本节描述智能网联汽车整车信息安全测试内容框架如下：

按照用户远程操作智能网联车行为，将测试内容按照路径划分为六大组件，分别为移动用户终端、云端、无线通道、入口级零部件、网关和 ECU。每个组件从汽车业务功能出发，参考上述安全威胁和技术要求描述其具体测试内容及评测清单（附录 A）

图 2 汽车整车信评估体系

8 汽车整车信息安全测试和评价方法

本规范基于 EVITA 威胁严重性分类模型、HEAVENS 模型和 CVSS 通用漏洞评级系统给定整车信息安全测试和评价方法：

1、 评测项风险值

通过对零部件存在的风险项进行测试和评分，计算得出风险项的漏洞转化系数（λ）、可用性得分（Exploit Score，ES）和严重性得分（Severity Score，SS）

2、 整车评价

整车评价首先通过评测项风险值分别在人身安全、财产损失、隐私安全和功能失效这四个指标上进行求和得分，基于四个指标的四象限扩展模型得出整车安全评价（如图 4），四指标所围面积反应了整车的信息安全水平。

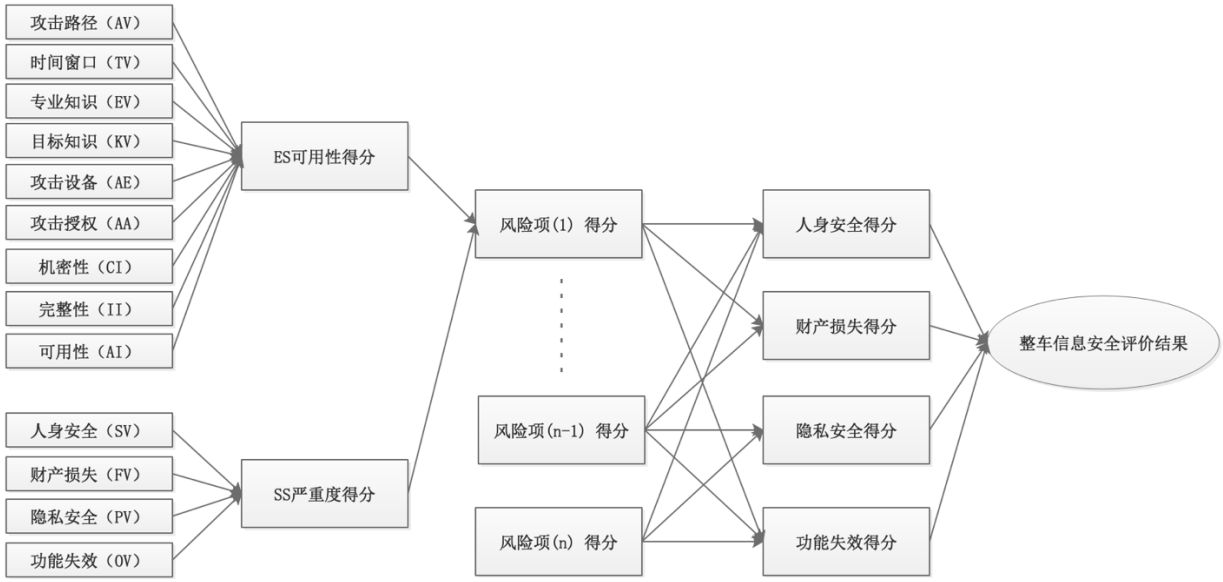

图 3 整车信息安全评价流程

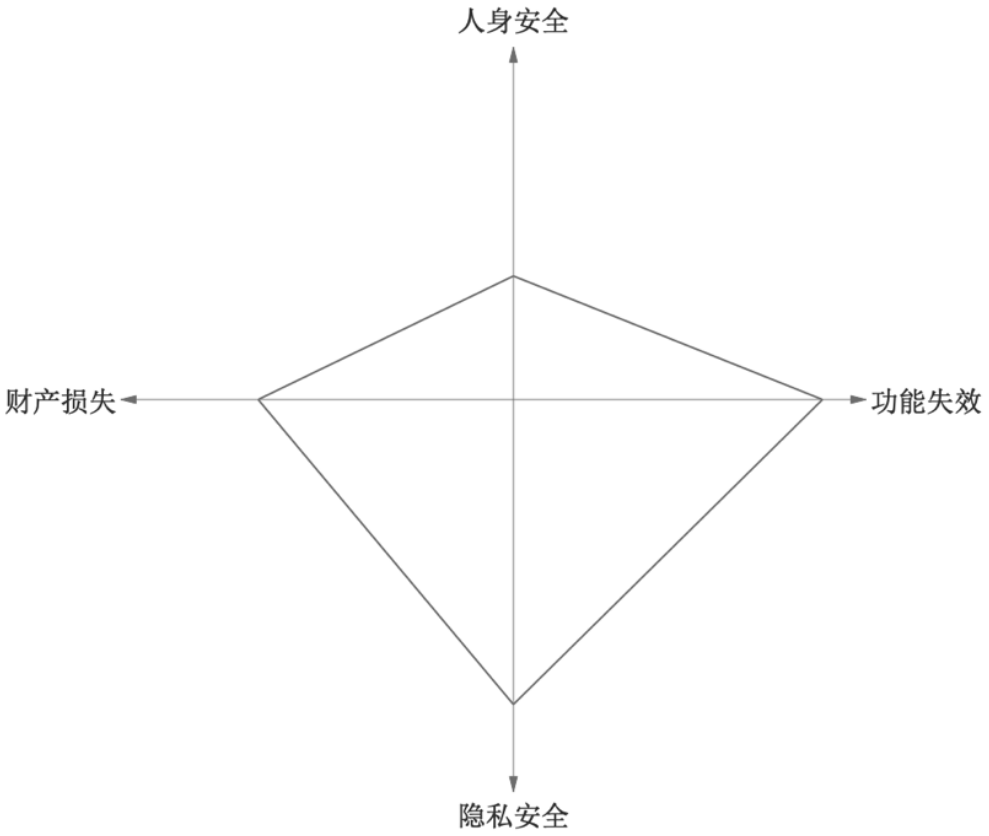

图 4 整车四指标评价模型

8.1.1 评测项风险值计算

8.1.1.1 漏洞转化系数（λ）

漏洞转化系数用以表征具体一项测试结果可以形成实际攻击漏洞的可能性，并进行数字量化。本规范从“专业知识、辅助工具、目标知识、目标环境、时间代码”5 个影响因子来衡量具体某个测试发现的风险项的漏洞转化系数。各影响因子如下表所示：

表 3 漏洞转化系数影响因子

因素	参数	值	参数说明
专业知识（VM_EV）	业余者	0.9	指只具备国内平均 IT 技能知识。比如：会使用计算机、WIFI、蓝牙、USB 设备进行设备互连与操作。
	熟手	0.7	具备一定的信息安全知识和能力，还对业务知识有一定了解，比如：对汽车领域相关知识。
	专家	0.4	在 IT 技能和汽车相关知识方面都有较为深入的了解与研究。
	多领域安全专家（组）	0.2	该风险需要多领域的专业知识
辅助工具（VM_AT）	公开可获得工具	0.9	使用公开软硬件工具（如开源软件、蓝牙发射器、编程器）即可实施漏洞挖掘。
	特殊工具	0.7	需要定制或专有的硬件设备和软件才可实施漏洞挖掘（如伪基站）。
目标知识（VM_KV）	公开	0.9	目标知识公开可获得
	受限	0.6	目标知识受限（如电路图）

	私有	0.2	目标知识保密，需要逆向
目标环境（VM_TE）	简单	0.9	容易接触，可通过网络接触或直接软件操作接触目标
	复杂	0.4	较难接触，需要硬件环境和软件环境的配合
时间代价（VM_TC）	一天以内	0.9	时间代价指耗费时间的数量级，影响因素包括环境搭建、目标研究、漏洞挖掘、漏洞验证等阶段
	一周以内	0.6	
	一个月以内	0.3	
	一个月以上	0.1	

$$\lambda = \begin{cases} 1, & \text{当风险项是明确} \\ \text{VM\_EV} * (\text{VM\_AT} + \text{VM\_KV} + \text{VM\_TE}) * 0.33 * \text{VM\_TC}, & \text{否则} \end{cases}$$

8.1.1.2 可用性（ES）

本规范从“攻击途径、时间窗口、专业知识、目标知识、攻击设备、攻击授权、机密性、完整性、可用性”9 个影响因子衡量单个风险项可被成功利用的具体情况，并将影响因子的属性分为 4 个类别，其中攻击途径为一组、 “时间窗口、专业知识、目标知识、攻击设备”为一组、攻击设备为一组、“机密性、完整性、可用性”为一组。各影响因子如下表所示，

表 4 风险项可用性影响因子

因素	参数	值
1 攻击途径（AV）	远距离无线网络	1.0
	短距离有线或无线网络	0.7
	物理接触	0.3
2 时间窗口（TV）	随时可访问攻击（钥匙、T-Box 激活）	1.0
	可频繁访问（车端通信）	0.9
	受业务触发限制（如 OTA）	0.8
3 专业知识（EV）	业余者	1.0
	熟手	0.9
	专家	0.8
	多领域安全专家（组）	0.6
4 目标知识（KV）	目标知识公开可用（如 JTAG）	1.0
	目标知识获取受限（如电路图）	0.8
5 攻击设备（AE）	公开的、开源的硬件设备和软件	1.0
	公开的专用硬件设备和软件	0.9
	定制或专有的硬件设备和软件	0.7
	多种定制或专有的硬件设备和软件	0.6
6 攻击授权（AA）	需要	0.7
	不需要	1.0
7 机密性（CI）	无影响	0
	影响程度低	0.7
	影响程度高	1.0
8 完整性（II）	无影响	0
	影响程度低	0.7
	影响程度高	1.0
9 可用性（AI）	无影响	0
	影响程度低	0.7
	影响程度高	1.0

参数说明：

1、 攻击途径：攻击者与被攻击设备之间空间距离上的度量。

1） 远距离有线或无线网络：指攻击者可以通过像蜂窝网络、4G 无线网络从远程即可发起攻击。

2） 短距离有线或无线网络：指攻击者只能通过像蓝牙、WIFI 等有线或无线网络从近程即可发起攻击。

3） 物理接触：指攻击者必须物理接触被攻击对象才能发起攻击。

2、 时间窗口：

1） 随时可访问攻击：指无论汽车处于启动或未启动状态均可发起攻击。

2） 可频繁访问（车端通信）：车辆处于某些状态时即可以频繁发起。

3） 受业务触发限制：指必须在某项业务处于活动状态时才可以发起攻击。

3、 专业知识：攻击者所需具备的专业知识能力的度量。

1） 业余者：指只具备国内平均 IT 技能知识。比如：会使用计算机、WIFI、蓝牙、USB 设备进行设备互连与操作。

2） 熟手：具备一定的信息安全知识和能力，还对业务知识有一定了解，比如：对汽车领域相关知识。

3） 专家：在 IT 技能和汽车相关知识方面都有较为深入的了解与研究。

4） 多领域安全专家（组）：仅一个领域的专家知识无法对漏洞做到有效利用，需要多个领域的专家一起配合才能实现漏洞有效利用。

4、 目标知识：漏洞攻击目标相关知识获取的难易程度。

5、 攻击设备：实施攻击所需设备获取的难易程度。

6、 攻击授权：成功实施攻击是否经过授权环节（比如需要经过认证或得到车主的某种配合）

7、 机密性：攻击对数据机密性的影响。详细说明如下：

1） 影响程度高：完全丧失机密性，导致受影响组件中的所有资源泄露给攻击者。或者，仅获得对某些受限信息的访问，但所公开的信息具有直接、严重的影响。例如，攻击者窃取管理员的密码或Web服务器的私有加密密钥。

2） 影响程度低：有一些机密性丢失。可以获得对某些受限信息的访问权限，但攻击者无法控制获取的信息，或者损失的数量或种类受到限制。信息披露不会对受影响的组件造成直接、严重的损失。

3） 无影响：受影响的组件内不会丢失机密性。

8、 完整性：攻击对数据完整性的影响。详细说明如下：

1） 影响程度高：完全丧失完整性或完全丧失保护。例如，攻击者能够修改受影响组件保护的任何文件。或者，只能修改某些文件，但恶意修改会对受影响的组件产生直接、严重的后果。

2） 影响程度低：可以修改数据，但是攻击者无法控制修改的后果，或者修改的数量受到限

制。数据修改不会对受影响的组件产生直接、严重的后果。

3） 无影响：受影响的组件内没有完整性损失。

9、 可用性：攻击对数据可用性的影响。详细说明如下：

1） 影响程度高：完全丧失可用性，导致攻击者能够完全拒绝访问受影响组件中的资源; 这种损失要么是持续的（当攻击者继续发动攻击时），要么是持久的（即使在攻击完成后情况仍然存在）。或者，攻击者可以拒绝某些可用性，但是可用性的丢失会对受影响的组件造成直接、严重的后果（例如，攻击者无法破坏现有连接，但可以阻止新连接;攻击者可以反复利用漏洞在每次成功攻击的情况下，只会泄漏少量内存，但在重复利用后会导致服务完全无法使用）。

2） 影响程度低：资源可用性降低了性能或中断。即使可能反复利用此漏洞，攻击者也无法完全拒绝向合法用户提供服务。受影响组件中的资源要么始终部分可用，要么仅在某些时间完全可用，但总体而言，受影响组件没有直接、严重的后果。

3） 无影响：受影响的组件中的可用性不会受到影响。

可用性评分计算公式：

$$\mathrm{ES} = 10 * \mathrm{AV} * (\alpha\mathrm{TV} + \beta EV + \gamma KV + \delta\mathrm{AE}) * \mathrm{AA} * (\mathrm{CI} + \mathrm{II} + \mathrm{AI}) * 0.333$$

注：

1、 当前 α = β = γ = δ =0.25，后续可以通过调整这 4 个因子的值来反映 TV/EV/KV/AE 各自的重要程度。

2、 信息安全三要素为必备因子，所以权值取 0.333。

3、 为了和 CVSS 的漏洞等级保持一致，这里增加常量系数 10

8.1.1.3 严重性 SS

严重性反馈了风险项可能给车主等利益相关方带来的危害程度。本规范严重性评估参考 HEAVENS 模型，从“人身安全、财产损失、隐私安全、功能失效”四个维度来进行评估。

表 5 风险项严重性影响因子

因素	参数	值	参数说明
人身安全（SV）	无	0	ISO 26262-3 -AIS 0及AIS 1-6可能性小于10% -不能被归为安全相关的损害
	轻度伤害	10	ISO 26262-3 -AIS 1-6 可能性大于 10%（不属于严重受伤和生命威胁等级）
	严重受伤	100	ISO 26262-3 -AIS 3-6 可能性大于 10%（不属于生命威胁等级）
	生命威胁	1000	ISO 26262-3 -AIS 5-6 可能性大于 10%
财产损失（FV）	无	0	不会造成财产损失。
	低	10	损坏普通，损失仍然可以被利益相关者所容忍。
	中	100	损坏较高，由此造成的损害会给利益相关者带来巨大的经济损失。
	高	1000	损坏非常高，财务损失严重影响利益相关者，甚至威胁到企业生存。

隐私安全（PV）	无	0	在侵犯隐私方面没有明显的影响。
	低	1	侵犯特定利益相关方（例如车主，司机）的隐私权，这可能不会导致滥用（例如假冒受害者以执行盗窃身份的行为）。
	中	10	侵犯特定利益相关方（例如车主，司机）的隐私权，导致滥用（例如假冒受害者以执行盗窃身份的行为）和媒体报道,或者侵犯多个利益相关者的隐私权，但不会导致滥用。
	高	100	侵犯多个利益相关者（例如车厂、多个车主）的隐私权，导致滥用（例如，冒充受害者以执行盗窃身份的行为）。 严重的隐私侵权可能导致广泛的媒体报道以及车厂和车队所有者在市场份额、业务运营、信任、声誉和财务损失方面的严重后果。
功能失效（OV）	无	0	车辆功能不受任何影响。
	低	1	资产被攻击后，车辆辅助功能性能下降如巡航控制或舒适/娱乐（cd-播放器、空调）功能操作不灵敏，或者车辆辅助功能轻微中断，但驾驶员可以人为消除，车辆行驶无影响，车辆辅助功能部分失效如巡航控制或舒适/娱乐（cd-播放器、空调）功能失效。
	中	10	资产被攻击后，适度中断，车辆主要功能性能下降，如驾驶员通过加大转向盘控制力以解决转向沉重导致的转向不足或者用力控制转向盘，纠正车辆行驶轨迹。
	高	100	资产被攻击后，功能出现重大中断，无法被人为控制消除，车辆主要功能组件部分仍可控，如转向被控制，制动仍可被操作或车辆主要功能如转向和制动均失效。

严重性评分计算公式：

$$\mathrm{SS} = \mathrm{SV} + \mathrm{FV} + \mathrm{PV} + \mathrm{OV}$$

8.1.1.4 风险值计算公式

单个风险项评分计算公式：

$$\mathrm{VS} = \lambda * \mathrm{ES} * \mathrm{SS}$$

8.1.2 整车评价方法

首先对人身安全、财产损失、隐私安全和功能失效四个信息安全影响指标进行计算求和，然后使用四象限图模型给出整车信息安全的综合评价。

8.1.2.1 人身安全指标计算

汽车整车在人身安全维度的状态情况取决如下：
1、 风险项的漏洞转化系数
2、 风险项可用性程度
3、 风险项在人身安全方面的严重性程度

基于以上给出汽车整车在人身安全维度的评分计算公式如下：

$$\mathrm{SVScore} = \sum_{k=1}^{n} (\lambda_K * ES_K * SV_K)$$

8.1.2.2 财产损失指标计算

汽车整车在财产损失维度的状态情况取决如下：
1、 风险项的漏洞转化系数
2、 风险项可用性程度
3、 风险项在财产损失方面的严重性程度

基于以上给出设计汽车整车在财产损失维度的评分计算公式如下：

$$\text{FVScore} = \sum_{k=1}^{n} (\lambda_K * ES_K * FV_K)$$

8.1.2.3 隐私安全指标计算

汽车整车在隐私安全维度的状态情况取决于如下四个方面：

1、 风险项的漏洞转化系数
2、 风险项可用性程度
3、 风险项在隐私安全方面的严重性程度

基于以上设计汽车整车在隐私安全维度的评分计算公式如下：

$$\text{PVScore} = \sum_{k=1}^{n} (\lambda_K * ES_K * PV_K)$$

8.1.2.4 功能失效指标计算

汽车整车在功能失效维度的状态情况取决于如下：

1、 风险项的漏洞转化系数
2、 风险项的可用性程度
3、 风险项在功能失效方面的严重性程度

基于以上计汽车整车在功能失效维度的评分计算公式如下：

$$\text{OVScore} = \sum_{k=1}^{n} (\lambda_K * ES_K * OV_K)$$

8.1.3 整车信息安全评价

通过上述人身安全、财产损失、隐私安全和功能失效四个信息安全影响指标的计算，最终在整车四指标评价模型图中进行数值标定。

通过标定后的数值，计算评价模型图中的面积，给出整车综合得分。

附录 A　汽车信息安全评测清单

A.1 汽车 IVI 安全评测清单

表 A.1　IVI 测试项清单

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
IVI	硬件安全	IVI-1.限管理	判断当前 MPU 芯片是否有可用的调试口（串口、JTAG、支持 ADB 的 USB 接口、BDM）	
		IVI-2.限管理	判断当前蓝牙模块是否有可用的调试口（串口）	
		IVI-3.限管理	判断当前 WIFI 模块是否有可用的调试口（串口）	
		IVI-4.限管理	判断当前蜂窝通讯模块是否有可用的调试口（串口、JTAG、USB）	
		IVI-5.限管理	判断当前 MCU 模块是否有可用的调试口（串口、JTAG、BDM）	
		IVI-6.口及网络扫描	判断当前 IVI 电路板是否存在用以标注芯片、端口和管脚功能的可读丝	
		IVI-7.件提取	检查是否有防固件提取措施	
	操作系统安全	IVI-8.弱性组件	检测操作系统是否存在已知漏洞	
		IVI-9.户安全	检查 root 登录是否存在弱密码漏洞	
		IVI-10.户安全	检查 root 登录是否存在暴力破解漏洞	
		IVI-11.户安全	在有远程 TELNET 登录功能的情况下，检查 TELNET 服务是否存在暴力破解漏洞	
		IVI-12.户安全	在有远程 SSH 登录功能的情况下，检查 SSH 服务是否存在暴力破解漏洞	
		IVI-13.户安全	在有远程 ADB 调试功能的情况下，检查 ADB 服务是否存在无需登录认证即可直接访问的功能	
		IVI-14.限管理	在有远程 ADB 调试功能的情况下，检查 ADB 服务是否赋予了 root 权限	
		IVI-15.限管理	检查对外围接口接入的存储介质上的文件类型是否做了限制（文件上传）	
		IVI-16.限管理	检查是否禁止运行外围接口接入的存储介质上的文件（代码执行、命令执行）	
		IVI-17.限管理	检查 android 系统是否是 debug 版本发布（信息泄漏）	
		IVI-18.能审计	测试能否使用 USB HID 设备进行操作（错误的输入验证）	
		IVI-19.能审计	测试 IVI 镜像篡改后能否正常引导	

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
		IVI-20.限管理	检查应用软件是否可被篡改	
		IVI-21.限管理	若为 QNX 系统，则检查是否留存有远程调试代理 pdebug（仿冒攻击、后门）	
		IVI-22.限管理	若为 QNX 系统，则检查是否留存了开发服务 qconn（仿冒攻击、后门）	
		IVI-23.限管理	应用软件调用执行拨打电话操作时，是否获得用户的确认才实际执行拨打操作（紧急救援电话除外）（未授权访问）	
		IVI-24.限管理	应用软件开通呼叫转移业务时，是否明示用户业务内容，且在用户确认的情况下执行操作（未授权访问）	
		IVI-25.限管理	用户是否可操作开启/关闭蓝牙无线连接（未授权访问）	
		IVI-26.限管理	用户是否可操作开启/关闭 WIFI 无线连接（未授权访问）	
		IVI-27.限管理	用户是否可操作开启/关闭 NFC 无线连接（未授权访问）	
		IVI-28.限管理	用户是否可操作开启/关闭蜂窝通讯网络数据连接（未授权访问）	
		IVI-29.限管理	应用软件调用启动本地录音功能时，是否在用户确认后启动录音操作（未授权访问）	
		IVI-30.限管理	检查车载模块用户界面是否提供云端对车辆定位功能的开关（如车辆隐身模式）（未授权访问）	
	第三方库	IVI-31.弱性组件	检测第三方库是否存在已知漏洞	
	应用安全	IVI-32.用测试	尝试 IVI 监听端口应用层报文重放，检测重放是否有效	
		IVI-33.弱性组件	检测系统浏览器是否存在已知漏洞	
		IVI-34.限管理	若为 linux，检查非操作系统原生应用程序的用户权限是否全为 root（越权访问）	
		IVI-35.户安全	检查车机提供的服务对于其上帐户登录访问是否存在暴力破解漏洞	

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
		IVI-36.户安全	若车机上软件有记录密码功能，则检查本地密码是否存在信息泄露风险	
		IVI-37.限管理	检查应用业务申请的敏感权限与业务对该权限使用的必要性，出评估结（未授权访问）	
		IVI-38.能审计	检查固件升级是否有升级包校验机制（篡改）	
		IVI-39.能审计	测试固件升级能否进行降版本攻击	
	通讯安全	IVI-40.用测试	蓝牙：尝试蓝牙重放攻击（比如伪造 MAC 地址攻击），检测能否任意连接到 IVI	
		IVI-41.用测试	蓝牙：尝试蓝牙中间人攻击，检测能否监测到 IVI 和手机间的通信数据	
		IVI-42.限管理	蓝牙：尝试蓝牙匿名文件传输，检测能否匿名上传文件成功	
		IVI-43.用测试	蜂窝通讯：如果支持蜂窝通讯，尝试短信和信令重放，检测能否重放成功	
		IVI-44.能审计	判断当前 WIFI 模块配置是否仅支持 WPA/WPA2	
		IVI-45.能审计	检查 WIFI 热点密码是否有强度要求（至少包含八个字符，至少包含一个数字、小写字符和大写字符）（弱密码）	
		IVI-46.口及网络扫描	基于以太网/车载以太网/蓝牙/WIFI/蜂窝通信模块版本信息和芯片型号信息，检查是否存在已知漏洞（其中以太网模块要精确到端口及对应程序已知漏洞）	
		IVI-47.能审计	测试 IVI 与云端 TSP 通讯是否可以仿冒伪造（比如：有无身份认证）	
		IVI-48.能审计	检查跟 TSP 的通讯是否加密（信息泄露）	
		IVI-49.能审计	测试 IVI 与云端 TSP 的通信是否可篡改	
	数据安全	IVI-50.户安全	若有不同驾驶员个性化适配功能（比如：亲人、代泊车者），则检查不同驾驶员间的隐私数据是否存在信息泄露风险	
		IVI-51.能审计	测试系统和应用日志是否泄露敏感信息，如调试信息	
		IVI-52.能审计	检查是否对通讯录数据进行了加密存储（信息泄露）	
		IVI-53.能审计	检查是否对通话记录数据进行了加密存储（信息泄露）	
		IVI-54.能审计	检查是否对录音数据进行了加密存储（信息泄露）	
		IVI-55.能审计	检查是否对位置信息进行了加密存储（信息泄露）	

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
		IVI-56.能审计	检查是否对相册数据进行了加密存储（信息泄露）	
		IVI-57.能审计	检查是否对短信数据进行了加密存储（信息泄露）	
		IVI-58.能审计	检查是否对日程数据进行了加密存储（信息泄露）	
		IVI-59.能审计	检查是否对浏览记录进行了加密存储（信息泄露）	
		IVI-60.能审计	检查是否对蓝牙配置信息进行了加密存储（信息泄露）	
		IVI-61.能审计	检查是否对 WIFI 的配置信息进行了加密存储（信息泄露）	
		IVI-62.能审计	检查能否从 PFX 证书中提取私钥（信息泄露）	
		IVI-63.能审计	检查私钥是否加密存储（信息泄露）	
		IVI-64.件分析	查看固件中是否有敏感信息泄露（如 root 口令、密钥、车辆身份证书等）	
	OTA升级	IVI-65.能审计	检验是否能从 OTA 升级过程中获取到固件升级包（信息泄露）	
	总线安全	IVI-66.用测试	IVI 上面 MCU 模块发出的 CAN 指令是否存在重放攻击漏洞	
	安全设计	IVI-67.限管理	检查是否开启 SELinux 功能	
		IVI-68.限管理	查看敏感文件（如/etc/shadow，/etc/passwd,/etc/group，rhosts）的访问控制权限	
		IVI-69.能审计	检查是否启用硬件安全保护措施（如 TEE）	
		IVI-70.能审计	检查是否有防火墙功能	

A.2 汽车 T-BOX 安全评测清单

表 A.2　T-BOX 测试项清单

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
T-BOX	硬件安全	TBOX-1. 权限管理	判断当前 MPU 芯片是否有可用的调试口（串口、JTAG、支持 ADB 的 USB 接口、BDM）	
		TBOX-2. 权限管理	判断当前 WIFI 模块是否有可用的调试口（串口、JTAG、BDM）	
		TBOX-3. 权限管理	判断当前蜂窝通讯模块是否有可用的调试口（串口、JTAG、BDM）	
		TBOX-4. 权限管理	判断当前 MCU 模块是否有可用的调试口（串口、JTAG、BDM）	
		TBOX-5. 接口及网络扫描	判断当前 T-BOX 电路板是否存在用以标注芯片、端口和管脚功能的可读丝印（信息泄露）	
		TBOX-6. 固件分析	检查是否有防固件提取措施（信息泄露）	
	操作系统安全	TBOX-7. 脆弱性组件	检测系统是否存在已知漏洞	
		TBOX-8. 账户安全	检查 root 登录是否存在弱密码漏洞	
		TBOX-9. 账户安全	检查 root 登录是否存在暴力破解漏洞	
		TBOX-10. 账户安全	在有远程 TELNET 登录功能的情况下，检查 TELNET 服务是否存在暴力破解漏洞	
		TBOX-11. 账户安全	在有远程 SSH 登录功能的情况下，检查 SSH 服务是否存在暴力破解漏洞	
		TBOX-12. 权限管理	检查 android 系统是否是 debug 版本发布（信息泄漏）	
		TBOX-13. 功能审计	在有远程 ADB 调试功能的情况下，检查 ADB 服务是否存在无需登录认证即可直接访问的功能	
		TBOX-14. 权限管理	在有远程 ADB 调试功能的情况下，检查 ADB 服务是否赋予了 root 权限	
		TBOX-15. 功能审计	检查 T-Box 镜像篡改后能否正常引导	
		TBOX-16. 权限管理	调试权限的限制：若为 QNX 系统，则检查是否留存有远程调试代理 pdebug（仿冒攻击 / 后门）	
		TBOX-17. 权限管理	调试权限的限制：若为 QNX 系统，则检查是否留存了开发服务 qconn（仿冒攻击 / 后门）	
	第三方库	TBOX-18. 脆弱性组件	检测第三方库是否存在已知漏洞	
	应用安全	TBOX-19. 权限管理	若为 linux，检查非操作系统原生应用程序的用户权限是否全为 root（越权访问）	
		TBOX-20. 重用测试	尝试重放 T-Box 监听端口应用层报文，检测重放是否有效	
		TBOX-21. 功能审计	检查固件升级是否有升级包校验机制（篡改）	
		TBOX-22. 功能审计	测试固件升级能否进行降版本攻击	
	通讯安全	TBOX-23. 重用测试	如果支持蜂窝通信，尝试短信和信令重放，检测能否重放成功（比如唤醒 T-Box 或者开空调等功能）	

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
		TBOX-24. 接口及网络扫描	判断当前 WIFI 模块是否仅支持 WPA/WPA2（其他加密算法容易被破解）	
		TBOX-25. 功能审计	检查 WIFI 热点密码是否有强度要求（至少包含八个字符，至少包含一个数字、小写字符和大写字符）（弱密码）	
		TBOX-26. 接口及网络扫描	基于以太网/车载以太网/WIFI/蜂窝通信模块版本信息和芯片型号信息，检测是否存在已知漏洞（其中以太网模块精确到端口及对应程序已知漏洞）	
		TBOX-27. 功能审计	测试 T-Box 与云端 TSP 通讯是否可以仿冒伪造（比如：有无身份认证）	
		TBOX-28. 功能审计	检查 T-Box 跟 TSP 的通讯是是否加密（信息泄露）	
		TBOX-29. 功能审计	检查 T-Box 跟 TSP 的通讯是否可以被篡改	
	数据安全	TBOX-30. 功能审计	检查系统和应用日志是否泄露敏感信息，如调试信息	
		TBOX-31. 功能审计	检查是否对 WIFI 的配置信息进行了加密存储（信息泄露）	
		TBOX-32. 功能审计	检查能否从 PFX 证书中提取私钥（信息泄露）	
		TBOX-33. 功能审计	检查私钥是否加密存储（信息泄露）	
		TBOX-34. 固件分析	查看固件中是否有敏感信息泄露（如 root 口令，密钥，车辆身份证书等）	
	OTA 升级	TBOX-35. 功能审计	检验是否能从 OTA 升级过程中获取到固件升级包（信息泄露）	
	总线安全	TBOX-36. 重用测试	T-Box 上的 MCU 模块下发的 CAN 指令是否存在重放攻击漏洞（通过尝试获取相同操作下 T-Box 上 MCU 模块下发的 CAN 指令是否一致来判断）	
	安全设计	TBOX-37. 权限管理	检查是否开启 SElinux 策略	
		TBOX-38. 权限管理	列出敏感文件（如/etc/shadow，/etc/passwd,/etc/group，rhosts）的访问控制权限	
		TBOX-39. 功能审计	检查是否启用硬件安全保护措施（如 TEE）	
		TBOX-40. 功能审计	检查是否有防火墙功能	

A.3 汽车 GW、ECU 安全评测清单

表 A.3　GW、ECU 测试项清单

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
GW、ECU	通信安全	GW-1.　重用测试	检查能否从 IVI 上重放控车指令	
		GW-2.　重用测试	检查能否从 T-Box 上重放控车指令	
		GW-3.　重用测试	检查能否从 OBD 上重放控车指令	
		GW-4.　网络隔离	将其它 CAN 子网的报文注入到 IVI 所在的 CAN 子网，检查网关是否存在异常转发的情况	
		GW-5.　网络隔离	将其它 CAN 子网的报文注入到 TBOX 所在的 CAN 子网，检查网关是否存在异常转发的情况	
		GW-6.　网络隔离	将其它 CAN 子网的报文注入到 OBD 所在的 CAN 子网，检查网关是否存在异常转发的情况	
		GW-7.　网络隔离	检查能否从 OBD 上收集到某一路 CAN 子网的所有 CAN 报文	
		GW-8.　网络隔离	若网关存在车载以太网，检查以太网是否划分了子域。（前提是能拆到网关）	
		GW-9.　帐户安全	检查 ECU 安全服务认证状态是否锁定	
		GW-10.　帐户安全	计算 seed 返回数据长度是否大于等于 4 个字节	
		GW-11.　帐户安全	检查 seed 值是否满足随机性分布	
		GW-12.　帐户安全	检查 seed&key 尝试是否有次数限制	
		GW-13.　帐户安全	检查 ECU 安全服务是否有锁定时间限制	
		GW-14.　帐户安全	检测一个 seed 可以发送的 key 的尝试次数是否有限制	
		GW-15.　帐户安全	检测是否能成功碰撞出 ECU 的 seed&key	
		GW-16.　帐户安全	检查 ECU 是否有连续请求 seed 的限制	
		GW-17.　权限管理	读取 DID 内容（敏感信息泄露）	
		GW-18.　权限管理	检查是否可以通过 UDS 篡改 DID 信息（篡改 ECU 配置）	
		GW-19.　权限管理	检测是否可以通过 UDS / XCP 篡改 ECU 内存信息（是否存在内存篡改漏洞）	
		GW-20.　权限管理	是否可通过 UDS / XCP 协议读取 ECU 敏感信息	
		GW-21.　功能审计	尝试是否可控制 ECU 的收发策略（篡改 ECU 配置，可能导致拒绝服务）	
		GW-22.　功能审计	尝试是否可更改 ECU 通信速率（篡改 ECU 配置）	

汽车部件	安全分类	评测类	评测项及方法描述	评测结果
		GW-23. 功能审计	检查 XCP 协议中 CAL/PAG、DAQ、STIM、PGM 是否使用 seed/key 认证机制	
		GW-24. 功能审计	检测能否不经过安全认证直接操纵 ECU 内部的运行参数（越权访问）	
		GW-25. 功能审计	检测能否不经过安全认证直接调用 Routine Control 服务（越权访问）	
		GW-26. 功能审计	检测是否有厂商自定义服务的接口	
		GW-27. 功能审计	检测能否模拟 RequestDownload 服务（越权访问）	

附录 B 汽车 IVI 信息安全评分参考

漏洞	漏洞转化系数	可用性打分										严重性打分					最后得分
		攻击途径	时间窗口	专业知识	目标知识	攻击设备	授权	机密性	完整性	可用性	评分	人身安全	财产损失	隐私安全	功能失效	评分	
电路板存在明显标注的 ARM 调试口	1	0.3	1	0.9	1	1	1	1	1	1	2.922075	0	10	10	1	21	61.36358
电路板存在明显标注的 MCU 调试口	1	0.3	1	0.9	1	1	1	1	1	1	2.922075	0	10	10	1	21	61.36358
热点密码设置不符合复杂度要求，可设置纯数字密码	1	0.7	0.8	0.9	1	1	1	0.7	0	0.7	3.018645	0	10	10	1	21	63.39155
热点默认密码配置弱（升级后默认密码固定为 00000000 的弱密码）	1	0.7	0.8	1	1	1	1	0.7	0	0.7	3.10023	0	10	100	1	111	344.1255
热点登录认证密码明文存储	1	0.3	1	1	1	1	0.7	1	0	0	0.6993	0	10	10	1	21	14.6853
热点配置信息明文存储	1	0.3	1	1	1	1	0.7	0.7	0	0	0.48951	0	10	10	1	21	10.27971
收音机在后台开启了针对所有网段的 XXXX 端口服务，增加了受攻击面。	0.0792	1	0.9	1	1	1	1	0.7	0	0	2.272725	0	10	100	1	111	19.97998
后台收音机机进程存在拒绝服务攻击漏洞，而此进程还跟其它业务进程有	1	1	0.9	0.9	1	1	1	0	0	0.7	2.21445	0	0	0	1	1	2.21445

漏洞	漏洞转化系数	可用性打分										严重性打分					最后得分
		攻击途径	时间窗口	专业知识	目标知识	攻击设备	授权	机密性	完整性	可用性	评分	人身安全	财产损失	隐私安全	功能失效	评分	
通讯，所以会造成车机相关业务受影响。																	
系统内置的 webview.apk 包存在 CVE-2016-6754 漏洞（需 RD 从代码级最终确认）	1	1	0.9	0.8	1	1	1	1	1	1	9.24075	10	100	100	1	211	1949.798
非操作系统原生应用程序的用户权限全为 root，容易被攻击者利用。	0.0594	0.3	0.9	1	1	1	0.7	1	1	1	2.045453	10	100	100	1	211	25.63647
蓝牙同步的通讯录数据是明文存储的，存在泄露风险。	1	0.3	0.9	1	1	1	0.7	0.7	0	0	0.477272	0	0	10	0	10	4.772723
蓝牙通话记录数据是明文存储的，存在泄露风险。	1	0.3	0.9	1	1	1	0.7	0.7	0	0	0.477272	0	0	10	0	10	4.772723
蓝牙配置信息明文存储，存在泄露风险。	1	0.3	0.9	1	1	1	0.7	0.7	0	0	0.477272	0	0	1	0	1	0.477272

漏洞	漏洞转化系数	可用性打分										严重性打分					最后得分
		攻击途径	时间窗口	专业知识	目标知识	攻击设备	授权	机密性	完整性	可用性	评分	人身安全	财产损失	隐私安全	功能失效	评分	
录音数据明文存储，存在泄露风险。	1	0.3	0.9	1	1	1	0.7	0.7	0	0	0.477272	0	0	10	0	10	4.772723
UDB 接口可使用 USB HID 设备进行操作车机，可以仿冒键盘或鼠标对车机进行一系列操作（如修改密码、打开热点）	1	0.3	1	1	1	1	1	1	1	1	2.997	0	0	1	1	2	5.994