智能网联汽车信息安全风险评估规范

2024

目 录

智能网联汽车信息安全风险评估规范

1 目的

为规范开展智能网联汽车信息安全测评工作，特制定本规范作为智能网联信息安全测评工作的依据。

2 范围

本标准规定了智能网联汽车信息安全风险评估术语和定义、测评原则、测评环境要求、测评内容、判定标准、产生文档、以及测评方法和工具。本标准涉及的风险评估范围包括智能网联汽车所包含的全部信息及与信息处理相关的各类资产。

3 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，凡是不注日期的引用文件，其最新版本适用于本标准。

1) （T/CSAE 101－2018）《智能网联汽车车载端信息安全技术要求》（参照车载端测试的维度）
2) GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则
3) CSTCQBYAJB058 移动应用软件安全测试规范V2.0
4) 《GB/T 18336.1-2015 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型》
5) 《GB/T 18336.2-2015信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件》
6) 《GB/T 18336.3-2015 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求》
7) 《GB-T 20984-2007 信息安全技术信息安全风险评估规范 第5部分：风险评估实施》

4 术语和定义

4.1 工作单元

工作单元是安全测评的最小工作单位，由测评项、测评方式、测评对象、测评实施和结果判定等组成，分别描述测评目的和内容、测评使用的方式方法、测试过程中涉及的测评对象、具体测试实施取证过程要求和测评证据的结果判定规则与方法。

4.2 测评强度

测评的广度和深度，体现测评工作的实际投入程度。

4.3 检查

不同于行政执法意义上的监督检查，是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。

4.4 测试

测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，查看、分析输出结果，获取证据以证明信息系统安全保护措施是否有效的一种方法。

4.5 缩略语

IVI In-Vehicle Infotainment 车载信息娱乐系统

T-Box Telematics BOX 车载T-BOX

JTAG Joint Test Action Group 联合测试工作组

UART Universal Asynchronous Receiver/Transmitter 通用异步收发传输器

SDK Software Development Kit 软件开发工具包

5 智能网联汽车信息安全风险评估原则

5.1 客观性和公正性原则

测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

5.2 经济性和可重用性原则

基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

5.3 可重复性和可再现性原则

不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

5.4 结果完善性原则

测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求。

6 测评环境要求

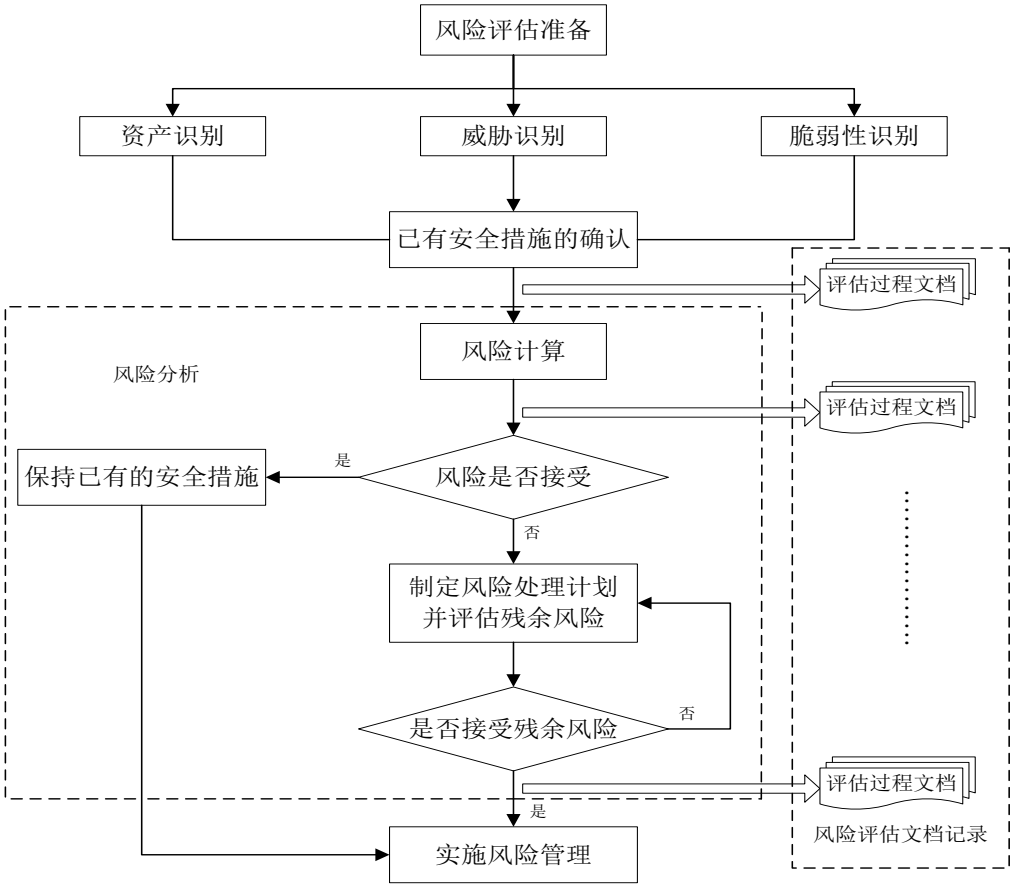
测评前需要对被测评的对象进行环境确认，须满足以下要求：

a) 原则上，测评须在对象的实际工作环境和工作状态中进行，如有特殊需求，个别工作单元的测评可以在模拟环境中进行，但要求与实际环境完全一致。

b) 实际测试环境与所提供的对象的相关资料的描述一致，且真实有效。相关资料包括：系统设计/验收文档、操作手册、相关证书和检验报告等。

7 智能网联汽车信息安全风险评估流程

智能网联汽车信息安全风险评估的实施流程如下图所示：



风险评估实施流程图

8 智能网联汽车信息安全风险评估准备

8.1 资产识别

8.1.1 资产分类

根据《GB-T 20984-2007 信息安全技术信息安全风险评估规范》，将保密性、完整性和可用性作为本标准评价资产的三个安全属性。在风险评估中，由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来评定资产的价值。

根据资产的表现形式，将资产分为数据、软件、硬件、服务、人员等类型,表 1 列出了基于表现形式的资产分类方法。

表1　一种基于表现形式的资产分类方法

分类	示例
数据	保存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等
软件	系统软件：操作系统、数据库管理系统、语句包、开发系统等 应用软件：应用软件、APP、底层控制软件、数据库软件、各类工具软件等 源程序：各种共享源代码、自行或合作开发的各种代码等
硬件	网络设备：网关、OBD、IVI、T-Box等 存储设备：光盘、软盘、车载硬盘等 传输线路：CAN总线、LIN总线、FlexRay、车载以太网等 保障设备：供电设备、冷却设备、消防设备等 安全设备：防火墙、入侵检测系统、身份鉴别等
服务	非授权访问控制、网络访问的保护措施、证书校验的机制,、加密所使用密钥应具有定期更新机制、关闭可导致隐私泄露的端口、使用安全的通信协议、使用最新版本的蓝牙协议、避免蓝牙协议漏洞攻击、使用的安全的WiFi协议、避免WiFi协议漏洞攻击、服务后台系统或APP通信时进行双向身份认证、对传输数据采取加密机制（加密算法、加密通道等）、安全存储日志的机制、分权限使用日志的功能、证书管理、密钥管理功能、证书定期更新机制。
人员	掌握重要信息和核心业务的人员，如使用人员和维护人员等。
其它	OTA 升级等

8.1.2　资产赋值

8.1.2.1　　保密性赋值

根据资产在保密性上的不同要求，将其分为五个不同的等级，分别对应资产在保密性上应达成的不同程度或者保密性缺失时对整个组织的影响。表 2 提供了一种保密性赋值的参考。

表 2　　资产保密性赋值表