ICS 33.040.40
CCS M19

团　　体　　标　　准

T/SHV2X 3—2025

车联网服务平台风险评估实施指南

Implementation guidelines to risk assessment of service platform of Internet of vehicles

2025-01-15发布　　2025-01-15实施

上海市车联网协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由上海市车联网协会提出并归口。

本文件起草单位：上研智联智能出行科技（上海）有限公司、上海计算机软件技术开发中心、上海银基科技股份有限公司、润成安全技术有限公司、工业互联网创新中心（上海）有限公司、上海蔚来汽车有限公司、零束科技有限公司、上汽大众汽车有限公司、福特汽车（中国）有限公司、沃尔沃汽车技术(上海)有限公司、艾普拉斯（上海）质量检测有限公司、上海优咔网络科技有限公司。

本文件主要起草人：杨伟利、潘政伟、宋晓航、毛争艳、何旺君、李爽、严超、刘海、曹远晶、张孟、周悦、杨晓光、王菲、王艳艳，杜同祯、杨清羽、李泽惠、薛超、杨靖、王赛纳。

车联网服务平台风险评估实施指南

1 范围

本文件描述了车联网服务平台风险评估实施的过程和方法。

本文件适用于指导智能网联汽车生产企业、车联网服务平台运营企业等车联网服务平台相关企业以及评测机构对车联网服务平台风险评估的实施，也可供相关主管部门参考。

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。

T/CCSA 339—2021 车联网网络安全防护定级备案实施指南

T/CCSA 441—2023 车联网服务平台网络安全防护要求

3 术语和定义

下列术语和定义适用于本文件。

3.1.

车联网 Internet of vehicle

通过新一代网络通信技术实现与汽车、电子、道路交通运输等领域深度融合，实现车、路、人、平台等之间的全方位互联和信息交互，促进车辆行驶安全、交通效率服务以及支撑自动驾驶演进的复杂网络及相关系统。

[来源：T/CCSA 339—2021, 3.1]

3.2

车联网服务平台 service platform of Internet of vehicle

面向车联网业务应用，负责车辆及相关设备信息的接入、汇聚、计算、监控或管理等功能（可负责一种或多种功能），提供信息管理或服务等的信息系统/平台，例如车辆运营管理、信息娱乐、在线升级、远程诊断、远程控制、车联网卡管理等应用服务或管理功能。

[来源：T/CCSA 441—2023, 3.1]

3.3

企业敏感数据 organization sensitive data

智能网联汽车生产企业、车联网服务平台运营企业业务过程中涉及的，一旦被泄露或篡改、损毁，可能直接危害经济运行、社会稳定、公共健康和安全、个人权益，或对企业合法权益、经济利益造成严重危害的数据。

4 概述

4.1 评估对象

本文件给出了车联网结构层次的一般描述，并对应到车联网服务平台的类型上，如图1所示。

图1 车联网层次结构模型及对应的车联网服务平台类型

本文件的风险评估对象为图1中各类型车联网服务平台安全运行所涉及的必要要素，评估内容包括组成车联网服务平台的信息系统所涉及的物理环境、网络、系统、应用及管理等层面所面临的安全风险。

4.2 评估原则

对各类车联网服务平台实施风险评估遵循以下原则：

a) 关键业务原则：将被评估方的关键业务作为评估工作的核心，将涉及这些业务的相关网络与系统作为评估的重点；

b) 可控性原则：在风险评估项目实施过程中，严格按照标准的项目管理方法对服务过程、人员和工具等进行控制，保证风险评估实施过程的安全可控；

c) 最小影响原则：首要保障业务系统的稳定运行，而对于需要进行攻击性测试的工作内容，与被评估方沟通并进行应急备份，同时避开业务的高峰时间进行。

4.3 评估过程和方法

如图2所示，对车联网服务平台实施风险评估的过程可划分为风险评估准备、风险要素识别和风险分析三个阶段。

风险评估准备阶段需确认评估目标、范围、依据和评估方法，组建团队，制定实施方案，并完成信息调研和评估工具准备；风险要素识别阶段是对车联网服务平台中的资产、威胁、脆弱性、安全措施等风险要素进行识别与赋值的过程；风险分析阶段是对获得的车联网服务平台相关信息进行关联分析，并计算车联网服务平台所面临风险的大小；最终通过风险评估报告给出风险评估结果，说明车联网服务平台中存在的安全风险。

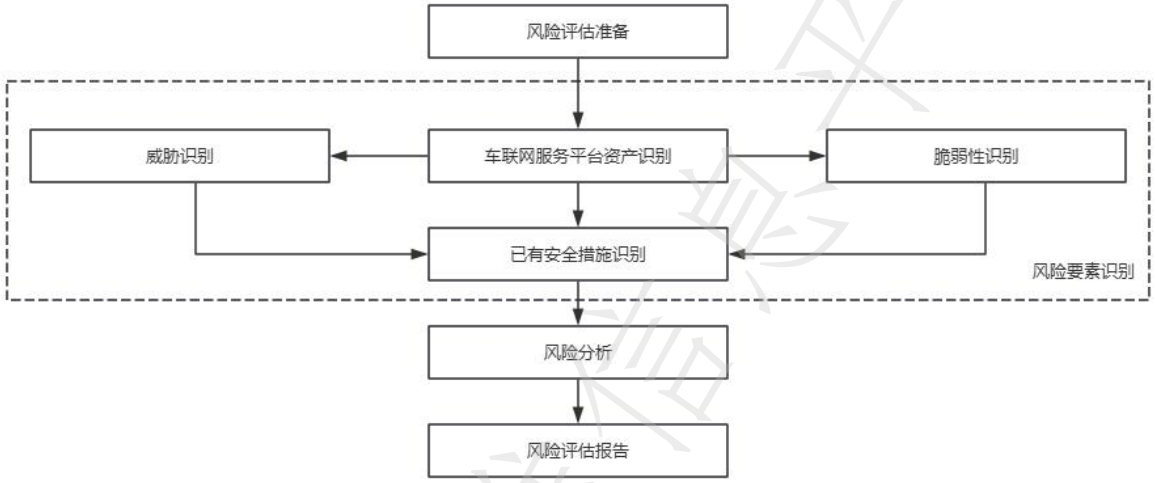

图2 车联网服务平台风险评估过程

对车联网服务平台的风险评估可综合采用人员访谈、文档审查、实地查看、配置核查、工具测试等手段对车联网服务平台及其相关设施的风险情况进行评估。评估可采取自评估和检查评估两种方式，自评估由车联网服务平台相关企业自身发起，组成机构内部评估小组或委托第三方评估机构进行评估，检查评估一般由车联网服务平台运营者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起评估工作。

5 风险评估实施

5.1 风险评估准备

5.1.1 确定评估目标和范围

根据车联网服务平台承载的业务需求、业务流程、系统规模和结构，识别当前运行环境中车联网服务平台的安全需求，针对车联网服务平台在技术和管理上的脆弱性和面临的威胁，确定车联网服务平台风险评估的目标。

确定评估目标后，进一步明确风险评估的评估范围，确定车联网服务平台相关的信息系统及其相关的信息资产、关键业务流程、管理机构等。在确定评估范围时，结合已确定的评估目标和车联网服务平台运营管理的实际情况，合理定义评估对象和评估边界，可以参考以下依据来确定评估范围：

a) 车联网服务平台的业务逻辑边界；

b) 组成车联网服务平台的网络及设备载体边界；

c) 车联网服务平台所在的物理环境边界；

d) 车联网服务平台的组织管理权限边界。

5.1.2 明确评估依据和手段

根据车联网服务平台的评估目标和范围，确定风险评估的评估依据和评估手段。

评估依据包括：

a) 适用的法律、法规；

b) 现行国际标准、国家标准、行业标准、团体标准；

c) 行业主管部门对车联网服务平台的管理要求；

d) T/CCSA 441—2023中与车联网网络安全防护级别相应的基本要求；

e) 被评估组织的安全要求。

评估手段包括：

a) 人员访谈；

b) 文档审查；

c) 实地查看；

d) 配置核查；

e) 工具测试。

5.1.3 组建团队和制定实施方案

对于自评估，风险评估团队由车联网服务平台运营管理各部门技术及业务负责人、风险评估专家等组成，明确风险评估工作中相关的管理和技术人员的任务，并由车联网服务平台安全责任人确认。

对于检查评估，风险评估团队由被评估方的技术及业务负责人、检查方指定评估机构相关人员组成，被评估方有支持和配合的责任和义务，以确保检查评估的有序进行。

风险评估团队组建完成后制定风险评估实施方案，用于指导评估工作的开展过程和实施内容，使评估各阶段工作有序进行。风险评估实施方案需得到被评估方的确认。风险评估实施方案内容包括：

a) 风险评估目标、范围、依据等；

b) 风险评估团队成员、职责等；

c) 风险评估工作计划，包括实施阶段、实施内容、实施方法、时间进度安排、交付物等；

d) 技术测试方案，包括技术测试方法、工具选择、工作环境要求、应急预案等。

5.1.4 信息调研和准备工具

信息调研是了解和熟悉被评估车联网服务平台的过程，风险评估团队对车联网服务平台相关业务过程、信息系统和应用、管理过程进行充分的调研，以保障风险评估过程的顺利实施。信息调研内容包括：

a) 车联网服务平台网络安全防护定级备案等级（参照T/CCSA 339—2021）；

b) 车联网服务平台支撑的业务内容和流程；

c) 车联网服务平台的网络结构和网络环境；

d) 车联网服务平台的组成软件和硬件及相应的基础设施；

e) 车联网服务平台中的数据；

f) 车联网服务平台的用户、管理和维护人员；

g) 车联网服务平台的安全管理组织建设和人员职责情况；

h) 车联网服务平台的安全管理制度和合规要求；

i) 车联网服务平台的安全防护措施；

j) 其它与车联网服务平台安全风险相关的内容。

根据车联网服务平台技术特点、评估目标和范围准备适当的技术评估工具，技术评估工具的选择和使用遵循以下原则：

a) 车联网服务平台脆弱性技术评估工具具备已知脆弱性核查与检测能力；

b) 技术评估工具的检测规则库能够及时更新；

c) 技术评估工具使用的检测策略和检测方式不对车联网服务平台正常运营造成影响；

d) 可采用多种技术评估工具对同一测试对象进行检测，如果出现检测结果不一致的情况，进一步采用必要的人工检测和关联分析，并给出与实际情况最为相符的结果判定；

e) 技术评估工具的选择和使用符合国家有关规定。

根据车联网服务平台技术特点、评估目标和范围准备适当的评估过程指导和记录文件，在文件使用前：

a) 确认文件发布前是得到批准的；

b) 确认文件的更改和现行修订状态是可识别的；

c) 确认文件的分发得到适当的控制，并确认在使用时可获得有关版本的适用文件；

d) 防止作废文件的非预期使用，若因任何目的需保留作废文件时，对这些文件进行适当的标识；

e) 规定文件的标识、存储、保护、检索、保存期限以及处置所需的控制。

5.1.5 规避评估风险

风险评估工作自身的风险，一是来自于评估结果是否准确有效，二是评估中的某些测试操作可能给被评估组织或信息系统引入新的风险。

风险评估工作实行质量控制，保证评估结果准确有效。风险评估工作的各阶段要根据相应的管理规范开展评估工作，保证数据采集的准确性和有效性，并充分了解被评估方的业务和安全特性要求。

在进行脆弱性识别前做好应急准备。评估方需对测试工具进行核查，包括测试工具是否安装了必要的系统补丁，是否存有与本次评估工作无关的残余信息、病毒木马，漏洞库或检测规则库的升级情况，以及工具运行情况；核查人员需填写测试工具核查记录；评估人员需事先将测试方法与被评估方充分沟通；测试过程中，评估人员需在被评估方相关人员配合下进行测试操作。

5.2 风险要素识别

5.2.1 资产识别

5.2.1.1 概述

车联网服务平台资产包括设备、机房及相关设施、企业敏感数据、网络及服务、系统及应用、管理制度及文档、人员等。通过资产识别形成资产清单以记录车联网服务平台的资产及其对应的属性，并通过资产赋值（见5.2.1.3）明确各项资产的价值大小。

5.2.1.2 资产分类

从风险评估实施的角度出发，对资产进行分类有助于提高资产识别的全面性和准确性。表1给出了资产分类方法的参考。

表1 资产分类方法参考

分类	说明
设备	网络设备：路由器、交换机等 服务器设备：服务器、虚拟机等 存储设备：磁盘阵列等 安全设备：认证网关等
机房及相关设施	通信线路：光纤通信适配器等 电力设施：不间断电源等 保障设施：消防设施等
企业敏感数据	保存在设备上的各种敏感数据资料，包括源代码、数据库数据等
网络及服务	各种网络设备、设施及其提供的网络连接服务等
系统及应用	车联网服务平台相关的信息系统及应用
管理制度及文档	规定组织内部管理体系和制度流程的成文信息及其载体
人员	掌握重要技术的人员，如数据库管理人员、网络维护人员、网络或业务的研发人员等
其他	企业形象、客户关系等

5.2.1.3 资产赋值

5.2.1.3.1 概述

车联网服务平台资产的赋值体现出资产的安全状况对于车联网服务平台持续正常运营的重要性。资产赋值综合考虑资产的社会影响力、业务价值和可用性三方面属性。

5.2.1.3.2 社会影响力

根据车联网服务平台资产在社会影响力上的不同，将其分为5个不同的等级，表示资产在被破坏后对社会公共利益、社会稳定性、社会公众集体等的影响。表2提供了一种车联网服务平台资产社会影响力赋值的参考。

表 2 车联网服务平台资产社会影响力赋值

赋值	标识	定义
5	很高	资产的社会影响力价值非常高，资产被破坏会对社会造成特别严重的损害或潜在影响
4	高	资产的社会影响力价值较高，资产被破坏会对社会造成严重损害或潜在影响
3	中等	资产的社会影响力价值中等，资产被破坏会对社会造成一定损害或潜在影响
2	低	资产的社会影响力价值较低，资产被破坏会对社会造成轻微损害或潜在影响
1	很低	资产的社会影响力价值非常低，资产被破坏会对社会造成的危害或潜在影响可以忽略

5.2.1.3.3 业务价值

根据车联网服务平台资产所提供业务的价值的不同，将其分为5个不同的等级，分别对应资产在业务价值缺失时对整个车联网服务平台支撑业务运营和满足用户需求方面的影响。表3提供了一种车联网服务平台资产业务价值赋值的参考。

表 3 车联网服务平台资产业务价值赋值

赋值	标识	定义
5	很高	资产所提供业务的价值非常关键，资产被破坏，导致业务无法正常运行，会对车联网服务平台造成特别严重的或无法接受的影响
4	高	资产所提供业务的价值较高，资产被破坏，导致业务无法正常运行，会对车联网服务平台造成严重影响
3	中等	资产所提供业务的价值中等，资产被破坏，导致业务无法正常运行，会对车联网服务平台造成一定影响
2	低	资产所提供业务的价值较低，资产被破坏，导致业务无法正常运行，会对车联网服务平台造成轻微影响
1	很低	资产所提供业务的价值非常低，资产被破坏，导致业务无法正常运行，会对车联网服务平台造成的影响可以忽略

5.2.1.3.4 可用性

根据车联网服务平台资产在可用性上的不同要求，将其分为5个不同的等级，分别对应资产在可用性上满足车联网服务平台正常运营的不同程度。表4提供了一种车联网服务平台资产可用性赋值的参考。

表 4 车联网服务平台资产可用性赋值

赋值	标识	定义
5	很高	可用性要求非常高，可用性在正常工作时间达到年度99.999%以上
4	高	可用性要求较高，可用性在正常工作时间达到年度99.99%以上
3	中等	可用性要求中等，可用性在正常工作时间达到年度99.9%以上
2	低	可用性要求较低，可用性在正常工作时间达到年度99%以上
1	很低	可用性要求非常低，可用性在正常工作时间低于年度99%

5.2.1.3.5 资产赋值方法

根据资产在社会影响力、业务价值和可用性这三个安全属性上的赋值等级，通过加权计算得到车联网服务平台资产价值。附录A中给出了车联网服务平台资产价值的具体计算方法。

车联网服务平台资产按最终计算结果划分为5级，表5中提供了一种资产价值等级描述。重要资产的范围可根据资产赋值结果确定，并作为风险评估的关键对象。

表 5 车联网服务平台资产价值等级及含义描述

等级	标识	定义
5	很高	非常重要，其安全属性被破坏后可能对车联网服务平台造成非常严重的损失
4	高	重要，其安全属性被破坏后可能对车联网服务平台造成比较严重的损失
3	中等	比较重要，其安全属性被破坏后可能对车联网服务平台造成中等程度的损失
2	低	不太重要，其安全属性被破坏后可能对车联网服务平台造成较低的损失
1	很低	不重要，其安全属性被破坏后可能对车联网服务平台造成非常低的损失，甚至忽略不计

5.2.2 威胁识别

5.2.2.1 概述

威胁是客观存在的可能导致危害车联网服务平台的安全事故的潜在起因，是一种对车联网服务平台资产构成潜在破坏的可能性因素。威胁可以通过威胁主体、动机、途径等多种属性来描述，造成威胁的因素包括技术因素、环境因素和人为因素等。威胁作用形式可以是对车联网服务平台及相关设施直接或间接的攻击，在社会影响力、业务价值和可用性等方面造成损害。

5.2.2.2 威胁分类

通过识别车联网服务平台威胁的来源，可对威胁进行粗略分类以快速判断存在威胁的领域。表6提供了一种根据威胁来源的车联网服务平台威胁分类方法。

表 6 车联网服务平台威胁来源分类

来源		威胁描述
技术因素		由于车联网服务平台设备自身的软硬件故障、系统本身设计缺陷或软件缺陷
环境因素	物理环境	断电、静电、灰尘、潮湿、温度、电磁干扰等，车联网服务平台意外事故或通信线路方面的故障
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、闪电
人为因素	恶意人员	内部人员对车联网服务平台的网络或系统进行恶意破坏，或采用自主或内外勾结的方式盗窃机密信息或进行篡改，以获取利益；外部人员利用车联网服务平台的脆弱性，对车联网服务平台进行破坏，以获取利益或炫耀能力
	无恶意人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训，专业技能不足，不具备岗位技能要求而导致车联网服务平台故障或被攻击

基于表现形式对车联网服务平台威胁进行分类的方式可以直观地体现威胁的外在特征，表7提供了一种基于表现形式威胁分类方法。

表 7 基于表现形式的车联网服务平台威胁分类

种类	描述
软硬件故障	由于设备硬件故障、通信链路中断、系统本身设计或软件缺陷导致对业务高效稳定运行的影响
物理环境威胁	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题和自然灾害
无作为或操作失误	由于应该执行而没有执行相应的操作或无意地执行了错误的操作，对车联网及相关系统造成影响
管理不到位	安全管理无法落实、不到位，造成安全管理不规范或者管理混乱，从而破坏车联网及相关系统正常有序运行
恶意代码和病毒	具有自我复制、自我传播能力，对车联网及相关系统构成破坏的程序代码
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用职权，做出破坏车联网及相关系统的行为
黑客攻击技术	利用黑客工具和技术，例如侦查、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对车联网及相关系统进行攻击和入侵
物理攻击	物理接触、物理破坏、盗窃
泄密	机密信息泄露给他人
篡改	非法修改信息
抵赖	不承认收到的信息和所做的操作或交易

5.2.2.3 威胁赋值

基于车联网服务平台威胁行为出现的频率对威胁进行赋值，并设定相应的评级方法进行等级划分，等级越高表示威胁利用脆弱性的可能性越大。不同等级分别代表威胁出现频率的高低，等级数值越大，威胁出现的频率越高。车联网服务平台威胁的频率可根据经验并参考组织、行业和区域有关的统计数据进行判断，综合考虑以下方面，形成车联网服务平台运行环境中各种威胁出现的频率：

a) 以往安全事件报告中出现过的威胁及其频率统计；

b) 实际环境中通过检测工具以及各种日志发现的威胁及其频率统计；

c) 近期公开发布的社会或特定行业威胁及其频率统计，以及发布的威胁预警。

表8给出了一种车联网服务平台威胁频率的赋值方法。可在附录B中的“威胁”部分对车联网服务平台及相关系统给出威胁分析和识别结果。

表 8 车联网服务平台威胁频率赋值

等级	标识	描述
5	很高	出现的频率很高，或在大多数情况下几乎不可避免或可以证实频繁发生过
4	高	出现的频率较高，或在大多数情况下很有可能会发生或可以证实多次发生过
3	中等	出现的频率中等，或在某种情况下可能会发生或被证实曾经发生过
2	低	出现的频率较小，或一般不太可能发生或没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

5.2.3 脆弱性识别

5.2.3.1 概述

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别，脆弱性是资产本身存在的，威胁总是要利用资产的脆弱性才可能造成危害。车联网服务平台中资产脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现。在识别已经运行的车联网服务平台资产脆弱性时，尽量避免影响车联网服务平台的正常运行。

脆弱性识别对物理环境层、设备和系统层、网络层、数据库、业务/应用层各层面的资产中存在的可能被威胁利用的脆弱性进行识别，并同时对脆弱性的严重程度进行评估。

5.2.3.2 脆弱性识别内容

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理环境层、设备和系统层、网络层、数据库、业务/应用层等各个层面的安全问题；管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

表9提供了一种脆弱性识别内容的参考。

表 9 脆弱性识别内容

类型	识别对象	识别内容
技术脆弱性	物理环境层	从机房场地、机房防火、机房供配电、机房防静电、

		机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别
	设备和系统层（含操作系统）	从物理保护、用户账号、口令策略、资源共享、访问控制、新系统配置（初始化）等方面进行识别
	网络层	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络安全配置等方面进行识别
	数据库	从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份及恢复机制、敏感数据加密存储和传输等方面进行识别
	业务/应用层	从访问控制策略、业务连续性、通信、鉴别机制、密码保护、人工智能模型与内容安全等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全等方面进行识别

5.2.3.3 脆弱性赋值

可以根据对资产损害程度、技术实现的难易程度、脆弱性流行程度，对已识别的脆弱性的严重程度进行赋值。对于引起同一方面问题的或可能造成相似后果的脆弱性，赋值时综合考虑这些脆弱性的共同作用，最终确定某一方面的脆弱性的严重程度。对一项具体的车联网服务平台资产，其技术脆弱性的严重程度还受到该资产所属车联网服务平台管理脆弱性的影响，因此资产的脆弱性赋值需要综合考虑技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可按等级化进行赋值，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。表10提供了脆弱性严重程度的一种赋值方法。

表 10 车联网服务平台脆弱性严重程度赋值

等级	标识	描述
5	很高	如果被威胁利用，将对车联网服务平台资产造成特别严重损害
4	高	如果被威胁利用，将对车联网服务平台资产造成严重损害
3	中等	如果被威胁利用，将对车联网服务平台资产造成一般损害
2	低	如果被威胁利用，将对车联网服务平台资产造成较小损害
1	很低	如果被威胁利用，将对车联网服务平台资产造成的损害可以忽略

在附录B中的“脆弱性”部分对车联网服务平台中各项资产给出脆弱性识别和赋值结果。

5.2.4 已有安全措施确认

对车联网服务平台中已采取的安全措施的有效性进行确认。安全措施可以分为预防性安全措施和保护性安全措施两种，预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生对资产造成的影响，如业务持续性计划。

车联网服务平台中已有安全措施的确认需要注意与脆弱性识别之间存在的联系。以确认安全措施的有效性为目标，确认安全措施的使用可降低车联网服务平台资产的脆弱性，但确认过程并不与脆弱性识别过程同步，不需具体到每个资产的脆弱性，而只需确认一类具体措施的集合。例如，确认防火墙的访问控制策略的有效性，不需描述具体的端口控制策略、用户控制策略，只需确认已采用的访问控制措施。

已有安全措施确认的结果是识别出车联网服务平台针对已知风险具备的各项安全措施，并综合评判其对车联网服务平台中各项资产及其对应的威胁和脆弱性的防护程度，可通过已有安全措施有效率的方式来衡量已有安全措施对威胁和脆弱性的防护，已有安全措施有效率表示某项具体的安全措施对资产的防护效果，以数值方式量化标识已有安全措施对具体资产所起到的保护作用（见表11）。

已有安全措施有效率的赋值如下：

表11 已有安全措施有效率赋值

已有安全措施有效率赋值	定义
0.1	针对该脆弱点基本未采取安全防护措施
0.5	针对该脆弱点采取了较为简单的安全防护措施
0.9	针对该脆弱点采取的措施能进行有效的安全防护

5.3 风险分析

5.3.1 概述

对车联网服务平台进行风险分析时，需要整体考虑车联网服务平台的资产及其脆弱性、威胁和已有安全措施等基本因素，可针对可能发生安全事件的车联网服务平台资产，采用综合考虑了已有安全措施有效性的资产价值、威胁值、脆弱性值的“相乘法”作为车联网服务平台风险值计算的方法，风险分析的原理如图3所示。

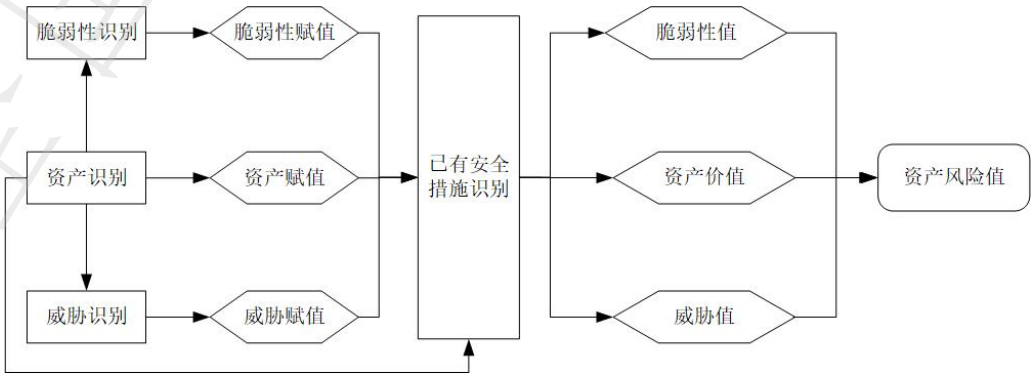

图3 车联网服务平台风险分析原理

5.3.2 风险值计算

如图3所示的风险分析过程，在完成了车联网服务平台的资产识别及相应的威胁识别、脆弱性识别和赋值后，再对资产已有安全措施的有效率进行确认。这些赋值使得车联网服务平台风险的计算方法可采用“相乘法”计算风险值。这一计算过程可以确定车联网服务平台中各项资产面临的威胁利用资产固有的脆弱性导致安全事件发生的可能性，综合资产价值及脆弱性的严重程度，整合已有安全措施的正面影响，判断安全事件一旦发生后造成车联网服务平台资产损失的风险，最终计算得出的车联网服务平台风险值。

对车联网服务平台风险计算原理可以采用以下公式表示：

$$Risk = AV \times T \times Vul \times (1 - E)$$

其中，$Risk$表示车联网服务平台风险值，AV为资产价值，T为威胁值，Vul为脆弱性，E为已有安全措施有效率。

5.3.3 风险结果判定

为了方便对车联网服务平台风险的管理与控制，可以进一步对车联网服务平台风险评估过程中得出的风险值进行等级化处理。按车联网服务平台风险值的计算范围将风险等级划分为五级，每个等级代表了相应风险的严重程度，等级越高，风险越高。表12、表13提供了风险等级判定标准。

表 12 风险等级判定

风险等级	**5**	**4**	**3**	**2**	**1**
风险值	$Risk > 90$	$60 < Risk \leq 90$	$30 < Risk \leq 60$	$10 < Risk \leq 30$	$Risk \leq 10$

表 13 风险等级描述

等级	**标识**	**描述**
5	很高	一旦发生将使车联网服务平台及相关系统遭受非常严重破坏，组织利益受到非常严重损失，如组织信誉严重破坏、严重影响组织业务的正常运行、经济损失重大、社会影响恶劣
4	高	如果发生将使车联网服务平台及相关系统遭受比较严重的破坏，组织利益受到很严重损失
3	中等	发生后将使车联网服务平台及相关系统受到一定的破坏，组织利益受到中等程度的损失
2	低	发生后将使车联网服务平台及相关系统受到的破坏程度和利益损失一般
1	很低	即使发生只会使车联网服务平台及相关系统受到较小的破坏

根据评估准备阶段确定的风险评估依据，可将车联网服务平台风险分为可接受风险和不可接受风险，通过对计算得出的风险值设置具体的阈值来区分，其中风险值低于可接受风险阈值的风险为可接

受风险，高于可接受风险阈值的风险为不可接受风险。如表14中的阈值给出车联网服务平台中不同资产类型在不同安全防护等级下区分可接受风险和不可接受风险的具体阈值参考值。

表 14 风险阈值

对象的安全等级		1级	2级	3级	4级	5级
风险阈值（风险值大于此阈值的风险视为不可接受）	设备类风险（包括设备、机房、数据、网络）	60	45	25	10	5
	人员类风险	90	60	40	20	10
	管理制度、文档类风险	80	50	30	10	5

5.4 风险评估报告

车联网服务平台风险分析完成后，对风险评估过程进行总结，并编制风险评估报告。风险评估报告内容包括：

a) 概述，说明车联网服务平台风险评估的背景和目的、内容及范围、风险评估方法和风险评估依据；
b) 资产分析，说明车联网服务平台所包含的资产，包括资产清单、重要资产列表、资产赋值方法和资产赋值的结果；
c) 威胁识别，说明车联网服务平台中资产所面临的威胁，包括威胁概述、威胁列表和威胁赋值的结果；
d) 脆弱性分析，说明车联网服务平台中资产所存在的脆弱性，包括脆弱性概述、脆弱性列表和脆弱性赋值的结果；
e) 已有安全措施，说明车联网服务平台中已采取的安全防护措施，包括概述和已有安全措施的统计列表；
f) 安全风险分析，说明对车联网服务平台中的资产进行风险分析的过程和结果，包括风险计算方法、风险阈值确定、风险分析列表、风险结果判定；
g) 安全整改建议，根据安全风险的严重程度、加固措施实施的难易程度、降低风险的紧迫性、需投入的成本等因素，综合给出整改建议；
h) 总结，说明评估完成后所确认的车联网服务平台风险总体状况；
i) 附录，提供对车联网服务平台进行风险评估过程中所收集的证据材料和执行的技术测试记录，以支持风险分析过程中得出的各项结果。

5.5 风险评估文件

车联网服务平台风险评估文件包括在风险评估过程中产生的评估过程文档和评估结果文档：

a) 风险评估方案：阐述风险评估的目标、范围、人员、评估方法和依据、评估内容和过程、评估结果形式和计划进度等；

b) 资产识别清单：根据风险评估文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门；

c) 重要资产清单：根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等；

d) 威胁列表：根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；

e) 脆弱性列表：根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体脆弱性的名称、描述、类型及严重程度等；

f) 已有安全措施确认表：根据已采取的安全措施确认的结果，形成已有安全措施确认表，包括已有安全措施名称、类型、功能描述及实施效果等；

g) 风险评估报告：对整个风险评估过程和结果进行总结，详细说明被评估对象，风险评估方法，资产、威胁、脆弱性的识别结果，风险分析、风险统计和结论等内容；

h) 风险评估记录：要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

附 录 A

（规范性）

资产赋值计算

为确保资产等级化赋值时的一致性和准确性，进一步明确资产价值评价尺度，并指导资产赋值，对资产赋值计算进行如下说明：

安全风险评估中的资产赋值综合考虑资产的社会影响力、业务价值、可用性三个安全属性，对于不同类型的资产，这三个属性通过不同的指标进行衡量，衡量方法如表A.1所列举。

表 A.1 资产安全属性衡量指标

资产类别	资产安全属性		
	社会影响力 I	业务价值 V	可用性 A
设备（硬件和软件）、机房、企业敏感数据、服务、网络	地域的重要性（从政治、经济、文化的角度衡量）；服务的规模（所覆盖的地域和人数）；提供的服务类型（通信、计费、网管等）	所提供的服务对企业的重要性	所提供的服务可正常工作的时间
人员	人员与国家安全、社会秩序、公众利益的相关性	人员与企业利益的相关性	评估人员工作时间，工作效率
管理制度和文档	管理制度、文档与社会、公众的相关性，（技术文档可参考所提供的服务类型）	管理制度、文档与企业利益的相关性	考察管理制度的执行力度，考察文档的实用性和有效性

资产价值可用如下公式计算：

$$AV = Round1(\log_2 \alpha \times 2^I + \beta \times 2^V + \gamma \times 2^A)$$

其中，AV代表计算得到的资产价值；I代表社会影响力赋值；V代表业务价值赋值；A代表可用性赋值；$Round1(\ \ )$表示四舍五入处理，保留1位小数；α、β和γ分别表示社会影响力、业务价值和可用性所占的权重，根据三项安全属性在具体网络业务中的情况确定α、β和γ的取值，α、β和γ值的确定应该充分考虑这三个安全属性的关联性及其在资产价值计算中的比重大小，$\alpha \geq 0$，$\beta \geq 0$，$\gamma \geq 0$，且$\alpha + \beta + \gamma = 1$。

附 录 B
（资料性）
风险评估列表

B.1 设备类风险

序号	资产				资产安全属性				威胁			脆弱性			风险		接受风险阈值	已有安全措施	整改措施建议	责任部门/责任人
	资产大类	资产子类	资产名称	资产描述	社会影响力	资产价值	可用性	资产赋值	威胁名称	威胁描述	威胁赋值	脆弱性名称	脆弱性描述	脆弱性赋值	风险描述	风险值（自动计算）				
1																				

B.2　人员类风险

序号	资产				资产安全属性				威胁			脆弱性			风险		接受风险阈值	已有安全措施	整改措施建议	责任部门/责任人
	资产大类	资产子类	资产名称	资产描述	社会影响力	资产价值	可用性	资产赋值	威胁名称	威胁描述	威胁赋值	脆弱性名称	脆弱性描述	脆弱性赋值	风险描述	风险值（自动计算）				
1																				

B.3　管理制度、文档类风险

序号	资产				资产安全属性				威胁			脆弱性			风险		接受风险阈值	已有安全措施	整改措施建议	责任部门/责任人
	资产大类	资产子类	资产名称	资产描述	社会影响力	资产价值	可用性	资产赋值	威胁名称	威胁描述	威胁赋值	脆弱性名称	脆弱性描述	脆弱性赋值	风险描述	风险值（自动计算）				
1																				

参 考 文 献

[1] GB/T 18336—2015 信息技术安全性评估准则

[2] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[3] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

[4] YD/T 1730—2024 电信网和互联网安全风险评估规范

[5] YD/T 3752—2020 车联网信息服务平台安全防护技术要求