汽车信息安全风险评估标准需求研究报告

汽标委智能网联汽车分标委

汽车信息安全标准工作组

2021 年 7 月

目　录

前　言

伴随汽车网联化、智能化趋势，汽车信息安全已成为保障车辆行驶安全的重要问题。开展信息安全风险评估分析作为“防患于未然”的重要方式，引导企业采用风险评估的方式，对防护对象的“可用性”、“保密性”、“完整性”及车辆的“攻击可行性”等进行分析，最终确定其风险等级，发现并解决潜在安全问题。因此，如何有效开展汽车信息安全风险评估成为各家汽车企业保障信息安全的首要工作。

本文件将为汽车整车企业、零部件供应商、第三方评估机构等开展汽车信息安全风险评估工作提供指导依据。

组织指导：汽标委智能网联汽车分标委。

牵头单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心），中国汽车技术研究中心有限公司。

参与单位：国汽（北京）智能网联汽车研究院有限公司，东风汽车集团有限公司技术中心，东风商用车有限公司，上汽集团股份有限公司，中国第一汽车股份有限公司，大众汽车（中国）投资有限公司，北京航空航天大学，博世汽车部件（苏州）有限公司，中国信息通信研究院，沃尔沃汽车技术(上海)有限公司，广东为辰信息科技有限公司。

参与人员：郭盈，张亚楠，宋娟，孙航，朱科屹，王海均，李宝田，赵浩，刘书勇，陈彦，杨洋，李红波，李木犀，赵闻，冀浩杰，郑亮，张宁，张成鑫，贾晓红。

1 研究背景及意义

1.1研究背景

1.1.1 汽车信息安全问题凸显

智能网联汽车的发展带来了信息安全问题，不同于传统的主动安全和被动安全，汽车信息安全问题一旦爆发，轻则造成驾乘人员隐私泄露、财产安全，重则危及到社会稳定、国家安全。因此，不解决汽车信息安全问题，智能网联汽车未来将无法上路。

国家高度重视智能网联汽车信息安全问题。我国将汽车信息安全上升为国家网络安全的重要组成部分，高度重视信息安全带来的风险，加快推进智能网联汽车信息安全技术的研发及应用、建立标准法规、制定相应的测试规范，有效实现多部门的协同机制，实现全方位的安全防护。2020 年 2 月，国家发改委、中央网信办、科技部、工信部、公安部、交通部等 11 个部委为顺应新一轮科技革命和产品变革趋势，抓住产业智能化发展战略机遇，加快推进智能汽车创新发展，联合印发了《智能汽车创新发展战略》。战略提出，到 2025 年，中国标准智能汽车的技术创新、产业生态、基础设施、法规标准、产品监管和网络安全体系基本形成。

汽车企业日益认识到汽车信息安全的重要性，并加快推动智能网联汽车网络安全技术能力建设。汽车企业加强对网络加密技术、可信计算等网络传输安全技术、针对智能网联汽车终端设备的认证机制的研究，确保终端设备的可信性，避免未经认证的终端设备连入智能网联汽车，对汽车造成安全威胁。

1.1.2 整车风险评估的重要性

随着智能汽车智能网联汽车的迅猛发展，信息安全问题也日益凸显。汽车智能化、网联化在带来节约能源、减少排放、提高驾驶体验等效益的同时，也面临信息泄露、非法入侵、非法远程控制等信息安全风险，对给汽车产业健康发展带来巨大的挑战。智能网联汽车融合了汽车技术和网络通信技术，打破了原本汽车系统内部相对独立的网络状态。这种融合，使得汽车成为网络空间的节点，进而产生了新的安全风险。近年来，越来越多的汽车厂商和零部件供应商开始重视关注汽车信息安全问题，积极布局汽车信息安全领域开展信息安全技术研究，持续提升汽车信息安全水平，降低汽车信息安全问题而带来的经济损失和社会以降低风险，提升品质。如何提升汽车企业信息安全水平和能力，其中风险评估是非常重要的一个环节是解决信息安全问题的关键环节。通过风险评估，确定利益相关方或利益相关方代表可能受到潜在环境或事件影响的程度，有助于认识风险及其对目标的潜在影响，揭示系统和组织的薄弱环节，明确需要优先处理的风险事件，为决策者选择应对策略提供信息；也可为汽车信息安全准入、监管提供参考。

调研结果表明，国外的一些顶尖 OEM 已经将风险评估应用到汽车生命周期的全过程。而目前国内对汽车信息安全风险评估的研究尚处于初级阶段，风险评估意识不足，对风险评估的适用范围、主要活动内容、关键步骤、使用方法等理解不够深刻。整车汽车制造商和零部件制造商，多是依靠技术人员的经验对生产的汽车整车或零部件进

行风险评估，主观性强，难以系统、全面、准确的识别资产、威胁以及资产的脆弱性，从而导致评估效率低，评估结果的一致性较差，参考价值较低。

本项目研究汽车信息安全风险评估方法、风险评估应用实践等，研究成果有助于指导汽车企业开展风险评估活动，实现威胁建模覆盖威胁场景，对汽车信息安全进行风险评估，及时发现汽车存在的安全问题及隐患，并提出对应的安全需求及修复方案，降低风险处置的成本，为整车企业、检测机构提供完善的风险评估方法与实践数据支撑。提升信息安全设计能力，缩小与国际先进水平的差距，推动我国汽车行业在汽车信息安全领域的发展。

1.2 研究意义

本项目的开展是落实《国家智能网联汽车发展战略》和《网络安全法》的重要举措，通过对汽车风险评估理论的研究，及时发现智能网联汽车存在的安全问题，有效保障驾乘人员的人身安全、财产安全，维护社会稳定，保障国家安全，推动智能网联汽车的健康可持续发展。

具体意义如下：

（1）维护社会稳定、保障国家安全的重要举措。智能网联汽车一旦爆发大规模汽车信息安全问题，不仅会影响到个人财产安全、人身安全，甚至会影响到国家安全和社会稳定。通过本项目的开展，可有效提升智能网联汽车安全水平，及时发现存在的安全问题和安全风险，降低大规模安全事件发生的概率，对提升社会问题和国家安全具有重大意义。

（2）实现国家汽车强国的重要保障。智能网联汽车是汽车产业技术变革和转型升级的重要突破口和战略制高点。智能网联汽车采用先进的探测、控制和通信技术，使得车辆电子化、自动化和智能化程度不断提高，促使行业提升技术水平和核心竞争力，推动我国汽车产业转型升级。信息安全是智能网联汽车的重要保障，通过本项目的研究，可快速定位汽车信息安全风险问题，提升智能网联汽车信息安全水平，助力智能网联汽车产业的健康可持续发展，稳固我国在智能网联汽车领域的国际领先地位。

（3）推动智能网联汽车产业的快速发展。通过对汽车信息安全风险方面的研究，一方面，依托基于国家标准编制的智能网联汽车安全风险评估体系，可以加快推动智能网联汽车安全相关国家标准的快速落地实施，为开展智能网联汽车安全技术提升提供依据；另一方面，通过可落地的指导规范助力行业企业智能网联汽车安全技术水平的提升。同时将本项目的研究成果在行业内进行应用推广，与业内企业共建共享，共同提高智能网联汽车产业行业的快速发展。

2 信息安全风险评估方法

对于智能网联汽车整个信息安全生命周期过程而言，网络安全威胁分析与风险评估是非常重要的环节。针对威胁分析与风险评估的研究，目前在传统信息系统领域有《GB /T 20984-2007 信息安全风险评估规范》将风险评估的实施步骤与过程提出标准化要求。

关于如何将传统信息系统的威胁分析与风险评估应用到智能网

联汽车上面，国际上已经开展了一些研究工作，主要的有欧盟 EVITA 以及 HEAVENS 项目。此外，近年的 ISO/SAE 21434《道路车辆 信息安全工程》标准文件的内容框架也围绕威胁分析和风险评估管理这一核心环节展开。以下为各研究项目在威胁分析与风险评估方面的概述与介绍。

2.1 传统 IT 风险评估

2.1.1 概述

《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》，此项标准适用于针对传统信息系统进行风险评估与分析，在汽车信息安全领域仍具备一定的参考价值。通过理解该标准在风险评估执行方法的核心思想与流程，对智能网联汽车的信息安全风险评估过程更加全面和完善，利用此方法可针对车联网服务平台开展信息安全风险评估互动，准确有效识别车联网服务平台的信息安全风险。

2.1.2 评估方法

基于国标 GB/T 20984-2007 的风险评估方法，风险分析中要涉及资产、威胁、脆弱性三个基本要素。每个要素有各自的属性，资产的属性是资产价值;威胁的属性可以是威胁主体、影响对象、出现频率、动机等;脆弱性的属性是资产弱点的严重程度。

风险分析的主要内容为:

（a） 对资产进行识别，并对资产的价值进行赋值;

（b） 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值;

（c） 对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值;

（d） 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性;

（e）根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失;

（f） 根据安全事件发生的可能性以及安全事件出现后的损失， 计算安全事件一旦发生对组织的影响，即风险值。

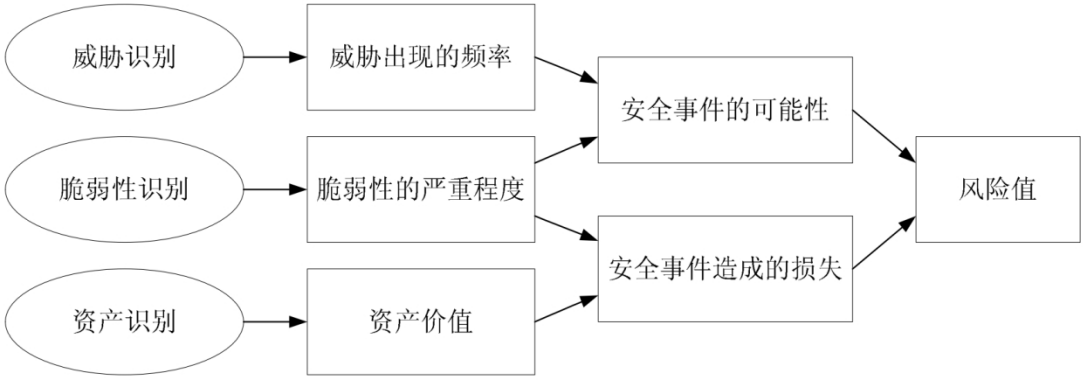

图 2.1 风险分析原理图

参考：GBT 20984-2007 信息安全技术 信息安全风险评估规范

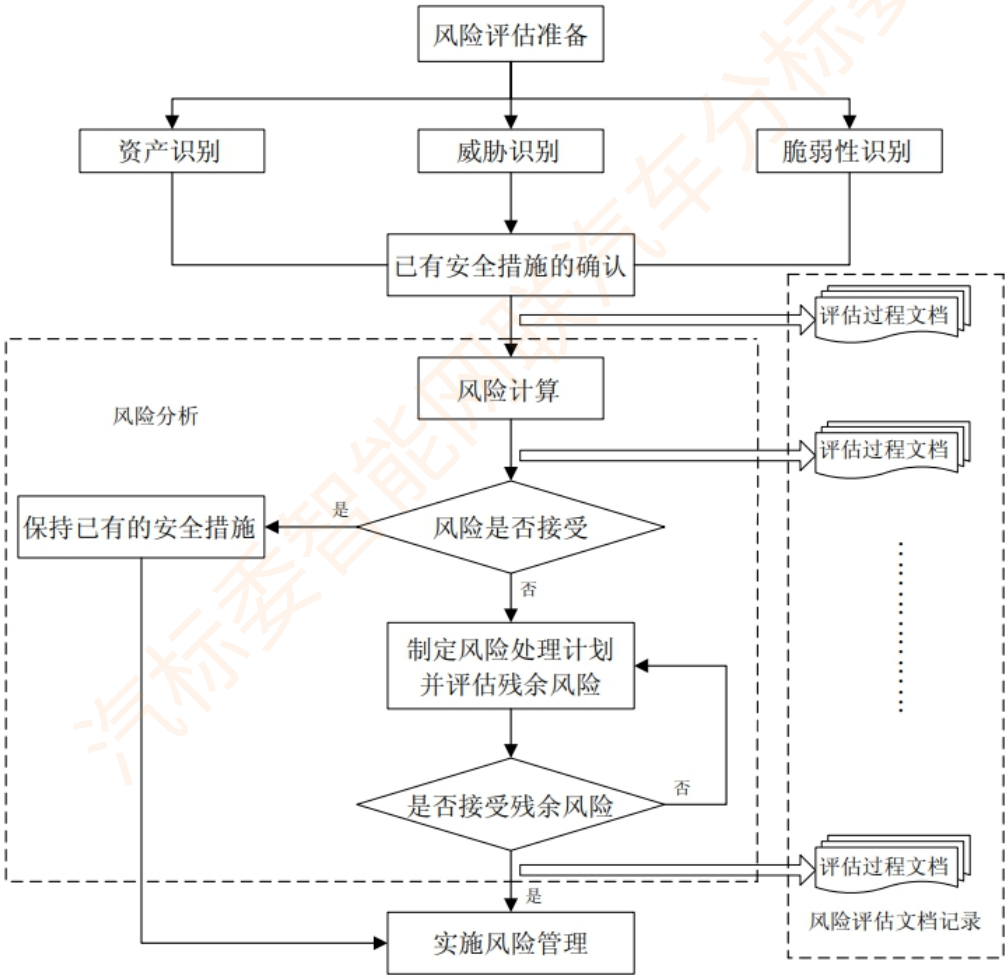

图 2.2 风险评估实施流程

参考：GBT 20984-2007 信息安全技术 信息安全风险评估规范

（1） 资产识别

保密性、完整性和可用性是评价资产的三个安全属性。风险评估中资产的价

值不是以资产的经济价值来衡量，而是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决定的。安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性、以及已采用的安全措施都将对资产安全属性的达成程度产生影响。为此应对组织中的资产进行识别。

在一个组织中，资产有多种表现形式;同样的两个资产也因属于不同的信息系统而重要性不同，而且对于提供多种业务的组织， 其支持业务持续运行的系统数量可能更多。这时首先需要将信息系统及相关的资产进行恰当的分类， 以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。根据资产的表现形式，可将资产分为数据、软件、硬件、服务、人员等类型。

（2） 资产赋值

表 2.1 资产保密性赋值表

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等

表 2.2 资产完整性赋值表

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补

4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略

表 2.3 资产可用性赋值表

赋值	**标识**	**定义**
5	很高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断
4	高	可用性价值较高，合法使用者对信息及信息系统的可用度达到每天 90%以上， 或系统允许中断时间小于 10min
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到70%以上，或系统允许中断时间小于 30min
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到25%以上，或系统允许中断时间小于 60min
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%

资产价值应依据资产在保密性、完整性和可用性上的赋值等级， 经过综合评定得出。综合评定方法可以根据自身的特点，选择对资产保密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果; 也可以根据资产保密性、完整性和可用性的不同等级对其赋值进行加权计算得到资产的最终赋

值结果。加权方法可根据组织的业务特点确定。

表 2.4 资产等级及含义描述

等级	标识	描述
5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失
3	中等	比较重要，其安全属性破坏后可能对组织造成中等程度的损失
2	低	不太重要，其安全属性破坏后可能对组织造成较低的损失
1	很低	不重要，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计

（3） 威胁识别

威胁是指可能导致危害系统或组织的不希望事故的潜在起因。威胁是一个客观存在的，无论对于多么安全的信息系统，它都存在，威胁的存在，组织和信息系统才会存在风险。因此风险评估工作中需全面、准确地了解组织和信息系统所面临的各种威胁。

表 2.5 威胁来源列表

来源		描述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益 外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，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信息系统故障或被攻击

威胁源是产生威胁的主体。根据威胁源的不同可以将威胁分为非人为的和人

为的。

非人为的主要是自然灾害和由于技术的局限性，造成系统不稳定，不可靠等情况。人为的安全威胁主体可以来自组织内部也可以来自组织外部。

从威胁动机来看，人为的安全威胁又可以分为非恶意行为和恶意攻击行为。非恶意行为主要包括粗心或未接受良好培训的管理员或用户，由于特殊原因导致的无意识行为。恶意攻击行为带有明显的目的性，一般经过精心的策略和准备。

不同的威胁源带有不同的攻击能力，衡量攻击能力主要包括：施展攻击的知识、技能、经验和必要的资金、人力和技术资源等。

表 2.6 一种基于表现形式的威胁分类表

种类	描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	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
无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作	维护错误、操作失误等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等
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，或者滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限、泄露秘密信息等

网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等

威胁途径是指威胁源对组织或信息系统造成破坏的手段和途径。

非人为的威胁途径表现为：

- 自然灾难
- 出现恶劣的物理环境
- 出现软硬件故障
- 性能降低等

人为的威胁手段包括：

- 主动攻击
- 被动攻击
- 临近攻击
- 分发攻击
- 误操作等

威胁源对威胁客体造成破坏，有时候并不是直接的，而是通过中间若干媒介的传递，形成一条威胁路径。在风险评估工作中，调查威胁路径有利于分析各个环节威胁发生的可能性和造成的破坏。威胁路径调查要明确威胁发生的起点、威胁发生的中间点以及威胁发生的终点，并明确威胁在不同环节的特点。

威胁可能性及其影响，威胁是客观存在的，但对于不同的组织和信息系统，威胁发生的可能性不尽相同。威胁产生的影响与脆弱性是密切相关的。脆弱性越多越严重，威胁产生影响的可能性越大；威胁客体的价值越重要，威胁发生的影响越大；威胁破坏的客体的范围越广泛，威胁发生的影响越大。此外，还要考虑

受影响客体的可补救性也是威胁影响的一个重要方面。

（4） 脆弱性识别

脆弱性是资产自身存在的，如没有被威胁利用，脆弱性本身不会对资产造成损害。脆弱性可以从技术和管理两个方面进行识别。技术方面，可从物理环境、网络、主机系统、应用系统和数据等方面识别；管理方面，可从技术管理脆弱性和组织管理脆弱性进行识别。

脆弱性识别包括：脆弱性的基本特征，时间特征和环境特征的识别。

a. 脆弱性的基本特征包括：

访问路径、访问复杂性、鉴别、保密性影响、完整性影响、可用性影响。

b. 脆弱性的时间特征包括：

可用性、补救级别、报告可信性、脆弱性的环境特征包括。

破坏潜力、目标分布、安全要求。

在识别脆弱性的同时，评估人员应对已采取的安全措施及其有效性进行确认。

脆弱性识别采用的方法主要有：文档查阅，问卷调查，人工核查，工具检测，渗透测试等。

（5） 风险计算

风险评估中涉及到的风险要素为：资产、威胁和脆弱性。其中由威胁和脆弱性确定安全事件发生的可能性，由资产和脆弱性确定安全事件的损失，最后由安全事件发生的可能性和安全事件的损失确定风险值。

表 2.7 风险等级划分表

等级	标识	描述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段

		很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

（6） 矩阵法概述

矩阵法主要适用于由两个要素确定一个要素值的情形。首先确定二位计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 z=f(x,y)，函数 f 可以采用矩阵法。

矩阵法原理如下：

x={x1,x2,...,xi,...,xm},1≦i≦m, xi 为正整数

y={y1,y2,...,yj,...,yn},1≦j≦n, yj 为正整数

以要素 x 和要素 y 的取值构建一个二维矩阵，其中矩阵内 m*n 个值即为要素 z 的取值。

表 2.8 二维矩阵

	y1	y2	y3	...	yj	...	yn
x1	Z_{11}	Z_{12}	Z_{13}	...	Z_{1J}	...	Z_{1n}
x2	Z_{21}	Z_{22}	Z_{23}	...	Z_{2J}	...	Z_{2n}
x3	Z_{31}	Z_{32}	Z_{33}	...	Z_{3J}	...	Z_{3n}
...	...	...	...	...	...	...	...
x_i	Z_{i1}	Z_{i2}	Z_{i3}	...	Z_{iJ}	...	Z_{in}
...	...	...	...	...	...	...	...
x_m	Z_{m1}	Z_{m2}	Z_{m3}	...	Z_{mJ}	...	Z_{mn}

- 对 Zmn 的计算，可以采用具有统一单调性的函数，例如：
- z=x+y
- 或 z=x*y
- 或 z=ax+by

2.2 EVITA 风险评估

2.2.1 概述

EVITA (E-safety vehicle intrusion protected applications) 是欧盟第七框架计划资助项目（2008-2011），旨在为车载网络的体系架构进行设计、验证、形成原型，以防止安全相关的组件被篡改，并保护敏感数据以免受到攻击。这个方法也是目前业界较为推荐的一种方法。

欧盟项目 EVITA 旨在开发一套技术和组件的原型，以确保车载系统硬件、软件和分析方法的安全性。EVITA 仅旨在调查车辆级别的网络安全解决方案。根据需要，设想了不同级别的安全保护。某些资产可能不需要安全措施（低风险）。风险分析旨在确定安全要求的优先级。

基本原理：保护每个威胁的成本太高，因此需要对风险进行分级，以便制定对策。与安全攻击相关的风险取决于影响的严重程度(即对利益相关者的伤害—驾驶员、其他道路使用者、市政当局、智能交通系统运营商、车辆制造商和系统供应商。成功攻击的概率—取决于攻击者的资源、物理安全攻击的性质。物理伤害可能是攻击的目标伤害也可能是意外后果。

2.2.2 评估方法

基于 EVITA 方法学的威胁分析与风险评估流程如下图所示。

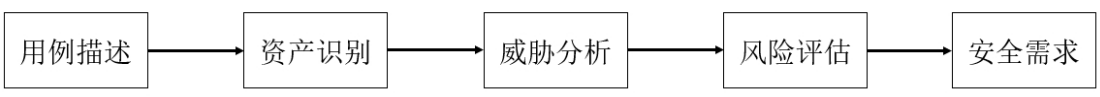

图 2.3 EVITA 分析流程

用例描述具体来讲就是确定在未来可能对安全性产生影响的一系列特定的车辆功能，资产识别是对汽车资产进行识别并对其价值进行赋值，威胁分析是识别威胁，也可以具体解释为建立攻击树模型。这个方法论的不足之处在于，安全威胁识别时繁琐不易操作，成功执行攻击需要时间不确定等。

EVITA 考虑四个方面的安全目标：（1）操控性（operational），维护所有车辆和智能交通系统功能所期望的操作性能；（2）功能安全（safety），确保驾乘人员和路边人员的功能安全；（3）隐私（privacy），保护驾驶人员，以及车辆制造和供应商在知识产权方面的私密性；（4）经济性（financial），保护欺骗性的经济损失和车辆盗窃问题。

对于每个安全目标，EVITA 开展三个阶段的工作：（1）威胁识别（threat identification），使用场景和攻击树识别威胁，并获得安全需求；（2）威胁分类（threat classification），基于威胁的严重性和成功攻击的可能性对威胁进行分类；（3）风险分析（risk analysis），基于威胁的分类，提供建议的措施。

EVITA 风险等级的计算，对于攻击可能性的计算综合了各个不同资产-攻击的可能性。每个具体的资产攻击都具有相应的攻击可能性（综合了成功攻击所需要的时间、专业性、对攻击对象的知识、机会窗口和设备等要素），而攻击目标则决定了攻击后果的严重性（针对汽车电子系统，涉及对其功能安全、操作性、财务和隐私等方面的考量）。根据攻击方法所包含资产攻击的“与”“或”关系，采用不同的方法计算其复合攻击可能性，再结合攻击严重性，计算出针对每一

个攻击方法的风险等级。对于功能安全相关的威胁，还需要结合可控性来计算风险等级。

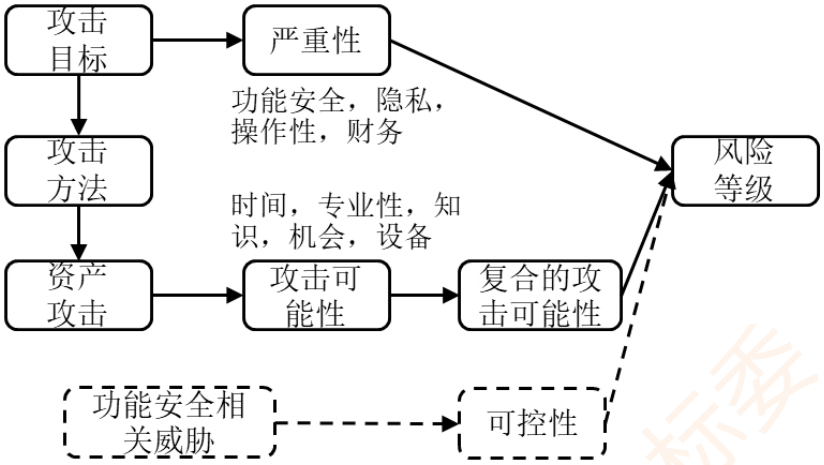

图 2.4　EVITA 基于攻击树方法的威胁分析与风险评估过程

下图展示了这种分析方法的一个实例，在该例中，为了达到攻击目标 1，可能采用攻击方法 1 或攻击方法 2，其中攻击方法 1 为资产攻击 1 和资产攻击 2 的合取（即“与”关系），而攻击方法 2 则为资产攻击 3~5 中的任意一种（即“或”关系）。

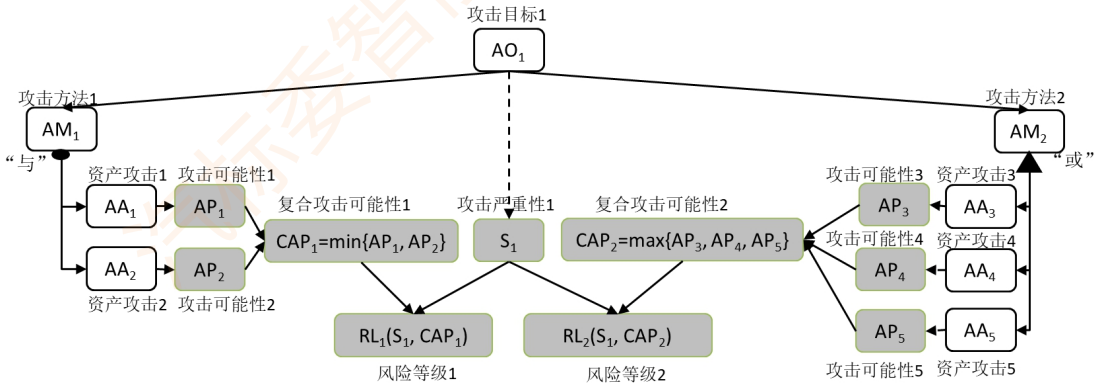

图 2.5 基于攻击树方法的威胁分析与风险评估过程实例

对于每个安全目标，EVITA 把威胁的严重性分为五个等级：S0、S1、S2、S3、S4。其中，S4 的严重性最高。

表 2.9EVITA 危险的严重性等级表

等级	安全性	隐私	经济性	操作性

S0	无伤害	禁止任何未经授权访问数据的行为	没有经济损失	无影响
S1	轻度或者中度伤害	仅限访问匿名数据（无特定驾驶员的数据）	轻度损失（10 美元左右）	对驾驶员无明显影响
S2	严重伤害（可能存活）/由多车引起的轻度或中度伤害	识别车辆或驾驶员数据/多辆车的匿名数据	中度损失（100 美元左右）/对于多辆车的轻度损失	驾驶员意识到了性能下降/对多辆车无明显影响
S3	威胁到生命（不确定能否存活）或致命的伤害/由多车引起的严重伤害	驾驶员或车辆的轨迹信息/识别多车的驾驶员或车辆数据	重度损失（1000 美元左右）/多辆车的中度损失	对操作性能的极大影响/对多辆车有明显影响
S4	由多车引起的的威胁生命或致命伤害	多车的驾驶员或车辆轨迹信息	多辆车的重度损失	对多辆车的极大影响

攻击成功的可能性方面，需要综合考虑多种因素：

- 确定如何攻击和成功执行攻击需要的时间(Elapsed Time)
- 需要的专门技能(Specialist Expertise)
- 需要了解的系统信息(knowledge)
- 需要的机会窗口(Window of opportunity)
- 需要的特殊设备等(Equipment)

表 2.10 攻击潜力和攻击几率评级

数值	**识别和利用攻击场景所需的攻击潜力**	**攻击几率（反映相对攻击性）**
0-9	低	5
10-13	较低	4
14-19	中	3
20-24	高	2

>=25	较高	1

表 2.11 针对私密性、经济性和操作性的网络安全威胁的网络安全风险表

安全风险等级（R）		**攻击可能性组合（A）**				
		A=1	A=2	A=3	A=4	A=5
非功能安全严重性（S_i）	1	R0	R0	R1	R2	R3
	2	R0	R1	R2	R3	R4
	3	R1	R2	R3	R4	R5
	4	R2	R3	R4	R5	R6

表 2.12 安全相关威胁的风险概率图

可控性（C）	**功能安全相关的严重性（S_S）**	**攻击可能性组合（A）**				
		A=1	A=2	A=3	A=4	A=5
C=1	…					
C=2	…					
C=3	S_S	R1	R2	R3	R4	R5
	S_S	R2	R3	R4	R5	R6
	S_S	R3	R4	R5	R6	R7
	S_S	R4	R5	R6	R7	R7+
C=4	…					

表 2.13 安全相关威胁的可控性分类

等级	**含义**
C1	尽管存在操作限制，但在正常的人为反应下，通常可以避免事故的发生
C2	避免事故是很困难的，但是通常可以通过合理的人为反应来避免
C3	避免事故是非常困难的，但在有利的环境下，可以通过有丰富经验的人做出反应来保持控制

C4	人为反应无法影响当前局面

表 2.14 攻击潜能评估表

资产（攻击）	时间	技能	系统信息	机会窗口	设备	所需的攻击潜能	
						数值	评级
车载传感器（传感器输入的外部操作）	0	0	3	0	0	3	低
GPS（干扰）	0	0	0	0	4	4	低
无线通信（干扰）	1	3	0	0	4	8	低
无线通信（有错误的或虚假的消息和信息）	1	3	0	0	4	8	低
车载传感器（停用或拒绝服务）	4	0	0	1	4	9	低

表 2.15 综合分析表

可控性（C）	安全相关的严重性（S_s）	联合攻击概率（A）				
		A=1	A=2	A=3	A=4	A=5
C=1	S_S=1	R0	R0	R1	R2	R3
	S_S=2	R0	R1	R2	R3	R4
	S_S=3	R1	R2	R3	R4	R5
	S_S=4	R2	R3	R4	R5	R6
C=2	S_S=1	R0	R1	R2	R3	R4
	S_S=2	R1	R2	R3	R4	R5
	S_S=3	R2	R3	R4	R5	R6
	S_S=4	R3	R4	R5	R6	R7
C=3	S_S=1	R1	R2	R3	R4	R5
	S_S=2	R2	R3	R4	R5	R6

	S_S=3	R3	R4	R5	R6	R7
	S_S=4	R4	R5	R6	R7	R7+
C=4	S_S=1	R2	R3	R4	R5	R6
	S_S=2	R3	R4	R5	R6	R7
	S_S=3	R4	R5	R6	R7	R7+
	S_S=4	R5	R6	R7	R7+	R7+

2.3 HEAVENS 风险评估

2.3.1 概述

HEAVENS 安全模型是一个框架，用于识别汽车 EE 系统环境中的安全漏洞和安全要求，并定义方法、流程以及执行安全评估的工具，目的在与提高行业交付安全可靠车辆的能力。此安全模型侧重于汽车行业的威胁分析和风险评估，在概念设计阶段对识别出的资产使用 STRIDE 模型进行威胁分析来帮助研发人员理解每个资产和对应威胁的映射关系，风险评估是指对威胁进行排名，获得每个威胁资产对的安全级别。根据威胁和资产的映射以及安全级别来制定评估对象的安全要求。

HEAVENS 是针对汽车电子电气系统威胁分析和风险评估的方法，同时也提供了完整的评估流程，其目标是提出一种系统方法，以便可以获得汽车电子电气系统的信息安全需求。

HEAVENS 具有四个主要的特点：

（1） 适用性范围广泛，可以适用于乘用车和商用车；

（2） 以威胁为中心，同时采用微软的 STRIDE 方法对汽车电子

电气系统进行威胁评估；

（3） 在威胁分析期间建立了安全属性与威胁之间的直接映射关系，有助于及早评估特定资产对特定技术的影响程度，这种影响程度包括机密性、完整性和可用性；

（4） 将安全目标（例如信息安全、财产、操作、隐私和法规等）与威胁分析期间的影响程度相结合，有助于评估威胁对于相关利益方，比如整车制造商的潜在业务影响。因此 HEAVENS 是一个非常适用于评估整车电子电气系统信息安全风险的评估方法。

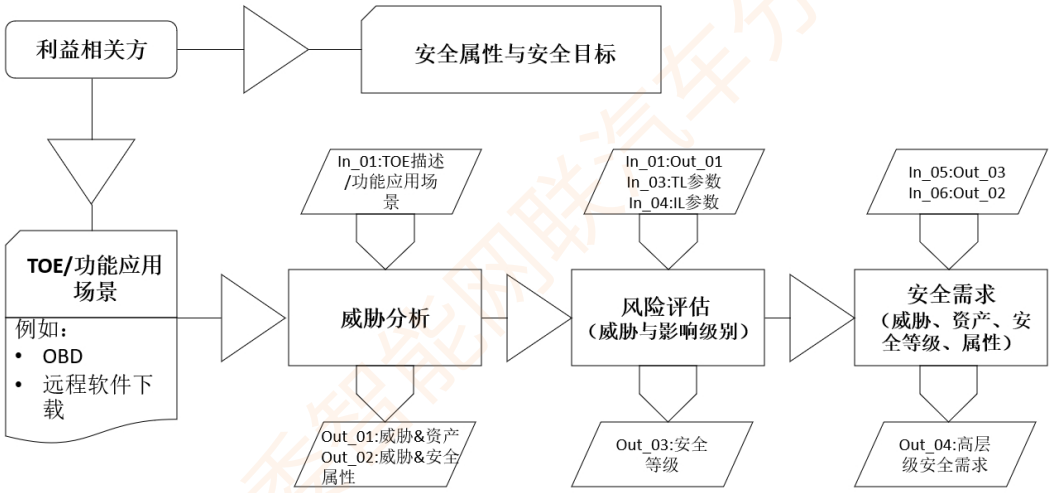

图 2.6HEAVENS 分析流程

2.3.2 评估方法

2.3.2.1 威胁建模

威胁建模是分析已识别出来资产对应的信息安全属性的一种方法，利用系统化和结构化的方法来思考管理资产的风险，帮助设计或测试人员识别、量化和解决与资产相关的安全风险，威胁建模的目的是通过对攻击者可能的攻击面、攻击向量、资产进行系统性分析，从而制定安全要求和防御措施。

STRIDE 模型是由微软提出的一种威胁建模方法，该方法将威胁类型分为 Spoofing（仿冒）、Tampering（篡改）、Repudiation（抵赖）、Information Disclosure（信息泄漏）、Denial of Service（拒绝服务）和 Elevation of Privilege（权限提升）。这六种威胁的首字母缩写即是 STRIDE。威胁类型与安全属性对应的关系如下表：

表 2.16 STRIDE 威胁类型解释

威　　胁	定　　义	对应的安全属性
Spoofing（仿冒）	冒充他人身份	真实性/新鲜性
Tampering（篡改）	修改数据或代码	完整性
Repudiation（抵赖）	否认做过的事情	不可抵赖性
Information Disclosure（信息泄露）	机密信息泄露	机密性/隐私（匿名）
Denial of Service（拒绝服务）	拒绝服务	可用性
Elevation of Privilege（提升权限）	未经授权获得许可	授权

威胁建模步骤：

（1）　分解目标业务场景，绘制数据流图，进行资产识别；

（2）　对数据流中的每个元素可能面临的威胁进行逐个分析，制作威胁列表；

（3）　针对威胁列表制定安全要求并验证安全要求是否消除安全威胁。

2.3.2.2 风险评估

风险评估是指对威胁进行排名，获得每个威胁资产对的安全级别；风险评估包括三个步骤：

（1）　确定威胁等级，即风险的“可能性”部分：

a) 进行攻击所需原理、产品或方法的知识水平；

b) 获取评估目标知识的难易程度；

c) 识别漏洞或发起攻击需要的设备；

d) 对评估目标进行攻击所需的访问类型（物理接触或非物理接触）和访问持续时间（无限制或有限）。

针对这四个参数进行分值评估，每个参数从易到难分为 4 个等级，分值从低到高分为 0，1，2，3，4。如下表所示：

表 2.17 TL 参数分值表

TL 参数值总和	威胁等级（Threat Level）	TL 分值
>9	无	0
7~9	低	1
4~6	中	2
2~3	高	3
0~1	严重	4

（2） 确定影响等级：

a) 安全，借鉴了 ISO 26262-3 概念阶段中 HARA 的评估参数，即严重性（Severity）来实现，从对人身造成的伤害程度，分为 4 个等级，分值分别为 0，10，100，1000。

b) 经济，比如整车厂的财产损失，这个和整车厂的财务实力有关。从风险造成的损失，分为 4 个等级，分值分别为：0，10，100，1000。

c) 隐私和立法，从隐私暴露和合法性的角度，分为 4 个等级，分值分别为 0，1，10，100。

d) 操作性：从隐私暴露和合法性的角度，分为 4 个等级，分值分别为，0，1，10，00。

经过上面的“安全、财产损失、操作性及隐私和法规”这四部分的评估，将所有分值进行相加，可以评估出影响等级（Impact Level），如下表所示。

表 2.18 IL 参数分值表

IL 参数值总和	影响等级（Impact Level）	IL 分值
0	无	0
1~19	低	1
20~99	中	2
100~999	高	3
>=1000	严重	4

（3） 确定安全级别：

安全级别应于最终风险评级，结合威胁级别和影响级别来导出安全级别，当且仅当 TL 和 IL 都具有值 4（“严重”）时，安全级别设置为“严重”。如下表所示：

表 2.19 风险评级表

安全等级（SL）	影响等级 IL					
威胁等级（TL）		0	1	2	3	4
	0	QM	QM	QM	QM	低
	1	QM	低	低	低	中
	2	QM	低	中	中	高
	3	QM	低	中	高	高
	4	低	中	高	高	严重

2.3.2.3 风险评估示例

蓝牙钥匙功能描述：通过手机 APP 控制车辆开门和启动。

蓝牙钥匙方案描述：车载信息交互系统提供商负责蓝牙钥匙的存储、分发和销毁；手机通过定制 APP 向 TSP 请求数字钥匙；手机通过蓝牙网络向汽车控制端发送数字钥匙；控制端确认钥匙合法通过向车身控制器发送 CAN 命令，解锁车门。

资产识别、威胁分析、风险评估、安全要求如下：

表 2.20 综合分析表

资产	威胁	攻击场景	风险等级	安全要求
TSP	TSP 被仿冒	伪造假的 TSP 骗取用户登录信息类似钓鱼网站的危害	严重	证书认证
	TSP 程序被篡改	应用程序被入侵并置入后门，监控所有车辆数字钥匙状态	严重	服务器安全（隔离、漏扫、配置安全）
Internet	Interne 网络拒绝服务	对 TSP 网络通信进行 Dos 攻击阻止其正常的服务	高	服务器入侵检测、防 dos 攻击
	Interne 流量篡改	攻击者对 TSP 与手机 APP 中的通信进行篡改发送伪造指令	高	加密和信息校验
	Interne 敏感信息泄露	造成用户信息钥匙信息等敏感信息泄露	高	加密
手机	手机被仿冒	攻击者仿冒客户向 TSP 发送请求，获取蓝牙钥匙，从而解锁车门	中	客户身份认证，例如手机号绑定
	手机抵赖	客户端请求钥匙陈工，但是没有记录证明该事件发生，攻击者可以借此逃避追踪，不利于安全审计或攻击溯源工作展开	中	TSP 和车载控制器端应对手机请求事件进行记录
蓝牙信	蓝牙信号被	对蓝牙信息号进行重放解锁	高	加密和信息校验

号	篡改	车门		
	蓝牙敏感信息泄露	蓝牙信号泄露数字钥匙信息	高	加密
	蓝牙信号拒绝服务	攻击者阻塞或干扰蓝牙信号，阻止正常的车门解锁	高	提升蓝牙信号的抗干扰能力
蓝牙接收器	蓝牙接收器被仿冒	攻击者仿冒蓝牙接收器，获取用户信息或钥匙信息	中	认证
车载控制模块	车载控制模块被篡改	固件篡改置入后门使攻击者不用认证随时解锁车门	低	固件加密和混淆
	车载控制模块权限提升	车载控制模块具有接触车载其它权限能力攻击者可以通过入侵该模块进行权限提升，进而接管车内其它控制	低	权限分级、管控、认证
日志	日志被篡改	攻击者篡改日志擦除攻击痕迹	低	日志访问权限控制
	日志信息泄露	日志泄露密钥用户信息等敏感数据	低	日志管理，不可打印敏感信息

2.4 基于 ISO 21434 的风险评估

2.4.1 概述

2020 年 2 月，由 SAE International 和 ISO 联合发布的 ISO/SAE 21434 Road Vehicle-Cybersecurity Engineering 标准 DIS 版正式发布。该标准首次将汽车信息安全提升到与功能安全等同重要或更甚的位置。信息安全旨在避免恶意攻击事件，未来该标准的发布，为 OEM、Tier1、Tier2 解决信息安全问题提供了理论依据和实施指南。

ISO/SAE 21434 标准中规定的评估道路车辆产品网络安全风险的具体方法，目的是在车辆产品开发早期识别潜在的威胁和安全漏洞，

再综合考虑攻击可行性、影响等级等因素，确定系统可能存在的风险及其风险等级，从而得出相应的网络安全目标，为后续形成网络安全需求，输入给设计开发提供基础。风险评估是以往软件开发流程中所没有的一项活动，因此在对项目实施网络安全时，风险评估是一个明确的工作增量。

2.4.2 评估方法

2.4.2.1 资产识别

在资产识别过程中，应将评估对象本身可能涉及信息安全的对象进行列举，并对所列对象的安全属性进行确定。

安全属性应包括保密性、完整性、可用性，可根据实际的安全目标对安全属性进行扩展。

通过分析某个对象的安全属性缺失对评估对象整体的信息安全造成了损害应认定为资产。

在整车系统中，可将汽车资产分为不同类型。

2.4.2.2 威胁场景识别

威胁场景识别是系统的识别和分析可能危及资产网络安全属性的威胁场景的过程。

威胁场景应与相应的资产和损害场景相关联，一个损害场景可对应多个威胁场景。

威胁场景识别可利用头脑风暴、误用案例提取、分类法等方法。

2.4.2.3 影响分析

影响对象应包括道路使用者、其他可能受伤害的人员（例如，维

护人员、制造人员等）、其他实体（例如，业务等）。

影响因子应包括安全、财务、操作、隐私和法律等因子。

如影响因子进行扩展（例如，增加知识产权、品牌形象等），应明确定义扩展参数。

在影响评估中，影响严重等级应分为“极高、高、中、低”四个级别。

影响分析应从安全、财务、操作、隐私等不同类别进行独立评估。

影响分析结果可对最严重的级别作为评定结果。

2.4.2.4 攻击路径分析

攻击路径描述应包含相对应的威胁场景。

（1）自顶向下的分析方法

描述根据已有的输入进行薄弱环节和缺陷检查的方法自顶向下的分析方法，如攻击树、攻击图、基于分类记忆的方法。例如采用STRIDE 模型的分析方法。

a. 在自顶向下（演绎）方法中，根据相似系统和组件中漏洞的历史知识，推断出项目或组件的攻击路径（即理论化、推断、推理、推测）。

b. 当前项目或组件还处于设计未实现的状态，或企图建立攻击假设或攻击路径时，自顶向下的方法在概念和研发阶段是有用的。

注：该方法适用于资产在研发的设计实现前，可通过相似系统或组件的攻击路径进行类似分析，找到安全攻击的路径。在产品开发的早期阶段，攻击路径通常是不完整或不精确的，因为具体的实现细节

还没有足够的详细信息来识别特定的脆弱性。在生命周期中，随着更多信息的可用（例如，在漏洞分析之后），攻击路径可以用更多的细节内容进行补充分析。

（2）自下向上的分析方法

a. 在自下而上（归纳）的方法中，从识别出的网络安全漏洞中为项目或组件构建攻击路径。攻击路径中的每个操作都基于“可利用的弱点”。

b. 当前项目或组件的已设计并实现完成，或者当假设或攻击模型已经建立，待确认时，最常用的是自下而上的方法。

注：该方法适用于资产已经设计实现完成，有成熟的技术架构，成型的产品，或已建立了攻击模型，此时通过安全漏洞的利用方式找到安全攻击的路径。重点是将脆弱性的利用方式和对应威胁结合起来进行评估安全攻击路径。

（3）攻击路径分析结束判定

如果攻击路径分析显示部分攻击路径无法完成威胁场景，则可以截断此部分攻击路径，并在此时停止分析。

2.4.2.5 攻击可行性分析

针对每一条攻击路径进行可行性分析，并给出攻击路径被利用的等级，包括高、中、低和很低四个等级。通常将采用基于攻击潜力方法、基于 CVSS 的方法、基于攻击向量的方法，具体采用哪种方法取决与所处的生命周期的哪个阶段以及可用的分析数据。

（1）基于攻击潜力分析方法与等级评估

基于攻击潜力的方法，应根据以下核心因素确定，包括攻击所需要时间、攻击具备的专业知识、被攻击项目或组件的技术知识、攻击机会窗口和攻击所采用设备。

a. 攻击所需要的时间评分依据

攻击所需时间 1 周内，给 0 分；1 个月内，给 1 分；6 个月内，给 4 分；3 年内，给 10 分；3 年以上，给 19 分。

b. 攻击具备的专业知识评分依据

普通人使用公开获取的知识就可攻击，给 0 分；有攻击常识的熟练人员才可攻击，给 3 分；经验丰富的专家才可攻击，给 6 分；多个专业性专家组队才可攻击，给 8 分。

c. 被攻击项目或组件的技术知识的评分依据

从互联网上或公开发布的文档中获取知识就进行攻击，给 0 分；组织机构内部分受限知识才可进行攻击，给 3 分；项目开发的内部团队成员掌握知识才可攻击，给 7 分；项目内部团队中少数人知道的绝密只是才可攻击，给 11 分。

d. 攻击机会窗口的评分依据

无时间约束，可自由访问被攻击组件，给 0 分；有时间约束，在短时间内可访问被攻击组件，给 1 分；有物理和逻辑控制，需要绕过控制才可访问被攻击组件，给 4 分；在有限时间内很难访问被攻击组件，给 10 分。

e. 攻击所采用设备的评分依据

攻击所使用的设备属于普适设备，给 0 分；攻击所使用的设备需

要进行针对性采购或准备，给 4 分；攻击所使用的设备需要定制化设计的，给 7 分；攻击所使用的设备需要定制化设计，在不同阶段采用的定制化设备不同，步骤随攻击层度而改变，给 9 分。

f. 总评分依据及等级对应关系

上述 5 项因素打分后的总分在 0～13 之间，判定为高等级可被攻击，给 4 分；总分在 14～19 之间，判定为中等级可被攻击，给 3 分；总分在 20～24 之间，判定为低等级可被攻击，给 2 分；总分在 25 以上，判定为很低等级可被攻击，给 1 分。

（2）基于 CVSS 的分析方法与等级评估

该方法参考了 CVSS 评级方法，在攻击分析中，重点关注可利用性这个维度，包括攻击向量、攻击复杂度、权限要求和用户交互。

下表给出了攻击可利用性等级的分析方法，见下表。

表 2.21 攻击可用性等级的分析方法

攻击向量（V）	网络/邻居/本地/物理	0.85/0.62/0.55/0.2
攻击复杂度（C）	低/高	0.77/0.44
权限要求（P）	无/低/高	0.85/0.62/0.27
用户交互（U）	不需要/需要	0.85/0.62
攻击可利用率（E）=8.22×V×C×P×U E 在 0.12～1.05 之间，攻击可被利用性为很低，给 1 分； E 在 1.06～1.99 之间，攻击可被利用性为低，给 2 分； E 在 2.00～2.95 之间，攻击可被利用性为中，给 3 分； E 在 2.96～3.89 之间，攻击可被利用性为高，给 4 分。		

（3）基于攻击向量的分析方法与等级评估

攻击向量分析方法，此度量反映了攻击路径利用的可能上下文。

攻击可行性等级越高，攻击者利用攻击路径的远程（逻辑和物理）能力就越强。假设使用 Internet 可以利用漏洞的潜在攻击者的数量大于可以利用需要对项目或组件进行物理访问的攻击路径的潜在攻击者的数量。

参考基于 CVSS 的分析方法的其中一个维度，即攻击向量，见表 2.14。

表 2.22 攻击向量分析方法

攻击向量（V）	网络/邻居/本地/物理	高/中/低/很低
注：对应等级评估分值：4、3、2、1		

2.4.2.6 风险评级及处置

（1）风险值计算

风险是相关损害场景的影响等级以及相应攻击路径的攻击可行性等级的函数。在完成了资产识别、威胁分析后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性，即攻击可行性。综合相关损害场景的影响等级，判断安全事件造成的损失，即安全风险。

根据计算出的相关损害场景的影响等级与相应攻击路径的攻击可行性，计算风险值。评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成损害场景的影响等级和相应攻击路径的攻击可行性之间的二维关系；相乘法通过构造经验函数，将损害场景的影响等级与相应攻击路径的攻击可行性进行运算得到风险值。

（2）风险评级

为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。可将风险划分 5 级，等级越高，风险越高。

评估者应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。

表 2.23 风险等级划分表

等级	标识	描述
5	很高	一旦发生将产生非常严重的人身安全、经济或社会影响，如人员严重伤亡、组织信誉严重破坏、严重影响组织的正常经营，人员伤亡严重、经济损失重大、社会影响恶劣。
4	高	一旦发生将产生较大的人身安全、经济或社会影响，在一定范围内给相关人员、组织的经营和信誉、社会造成损害。
3	中等	一旦发生会造成一定的人身安全、经济、社会或生产经营影响，但影响面和影响程度不大。
2	低	一旦发生造成的影响程度较低，一般仅限于车辆或组织内部，通过一定手段很快能解决。
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补。

（3）风险处置

a. 安全整改建议

应根据安全风险的严重程度、加固措施实施的难易程度、降低风险的时间紧迫程度、所投入的人员力量及资金成本等因素提出整改建议。

对于非常严重、应立即降低且加固措施易于实施的安全风险，应立即采取整改措施并制定应急预案。

对于非常严重、应立即降低且加固措施不便于实施的安全风险，应立即制定安全整改实施方案，尽快实施安全整改；应在整改前对安全隐患进行监控并制定应急预案。

对于比较严重，应降低且加固措施不易于实施的安全风险，应制定限期实施的整改方案，应在整改前对相对安全隐患进行监控。

对于其他不可接受的安全风险，应根据资源及组织实际情况，采取适当可行的整改措施。

b. 评审

应对风险评估相关的报告进行评审。并对评审意见进行记录。风险评估各阶段的验收评审文档如表 2.16 所示。

表 2.24 风险评估项目验收文档

工作阶段	输出文档	文档说明
识别风险	《资产价值分析报告》	资产调查情况，分析资产价值，以及重要资产说明。
	《威胁分析报告》	威胁调查情况，明确存在的威胁及其严重程度，以及严重威胁说明。
	《已有安全措施分析报告》	分析组织或信息系统已部署安全措施的有效性，包括技术和管理两方面的安全管控说明。
影响评估	《影响分析评估报告》	对影响对象、影响类别等进行识别和评估，并对影响程度进行评级。
攻击评估	《安全脆弱性分析报告》	从技术和管理两个层面进行脆弱性分析，针对各应用场景进行薄弱环节分析和缺陷检查。
	《攻击可行性分析报告》	针对脆弱性和攻击分析环节，在明确薄弱环节、缺陷和攻击路径、方法的基础上，依据攻击潜力评价指标和计算方法，给出攻击可行性评级。
风险评级	《风险评估报告》	对资产、威胁、脆弱性等评估数据进行关联计算、分析评价等，应说明风险分析模型、分析计算方法。

风险处置	《安全整改建议》	对评估中发现的安全问题给予有针对性的风险处置建议。

3 汽车信息安全风险评估实践

3.1 自动紧急刹车系统案例

这个例子展示如何依据自动紧急刹车来做信息安全的风险评估。为简明起见，把感知和决策放在一起。那么整个功能由三个部分组成：

1. 感知和决策系统，判断前方是否有紧急情况，以及车辆应该如何响应。
2. 车内通讯，感知和决策系统通过车内通讯，发送指令给执行系统。
3. 刹车系统，根据感知和决策系统发过来的指令，执行相应的车辆紧急制动。

图 3.1 功能关系示意

表 3.1 资产识别

资产	信息安全属性
感知和决策系统	完整性/真实性
感知和决策系统	可用性
车内通讯	完整性/真实性
车内通讯	可用性
刹车系统	完整性/真实性
刹车系统	可用性

表 3.2 威胁分析

威胁	影响	损害	损害严重程度
感知或决策系统的软件被非法篡改	感知和决策系统的完整性和真实性	错误的感知或者决策，导致系统错误制动，后车追尾	高（刹车系统对于错误的制动请求有门

			限值的限制和监控，所以严重度在一定程度上有所缓解）
		错误的感知或者决策，导致系统未触发，出现碰撞事故	最高
车内通讯被非法篡改或者伪造	车内通讯的完整性和真实性	刹车系统接收到错误的制动请求，导致系统错误制动，后车追尾	高（刹车系统对于错误的制动请求有门限值的限制和监控，所以严重度在一定程度上有所缓解）
		刹车系统未接到制动请求，导致系统未触发，出现碰撞事故	最高
刹车系统被非法篡改	刹车系统的完整性	刹车系统的完整性被破坏，导致系统错误制动，后车追尾	最高（刹车系统对于错误的制动请求有门限值的限制和监控亦可能被破坏）
		刹车系统的完整性被破坏，导致系统该触发时未触发，出现碰撞事故	最高
车内网络的拒绝服务攻击	各系统的可用性	自动紧急刹车系统无法激活，不可用	中

3.1.1攻击路径及可行性

此处可行性的取值基于假设，并非按照实际各系统的分析得来。系统软件被非法篡改，攻击可行性：高（4，3，0，0，0）。

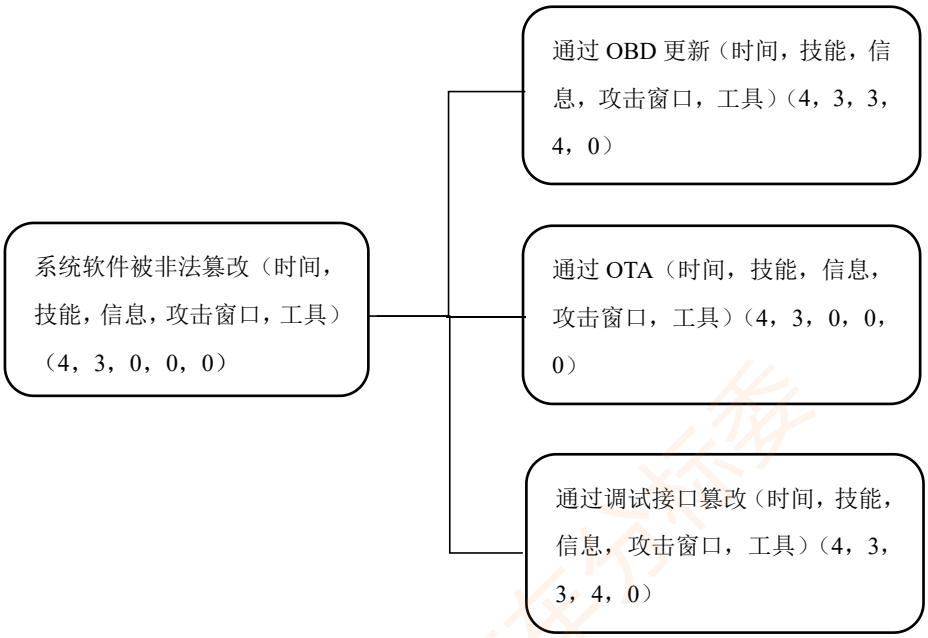

图 3.2 软件篡改攻击可行性分析

车内通讯被非法篡改，攻击可行性：高（4，6，3，0，0）

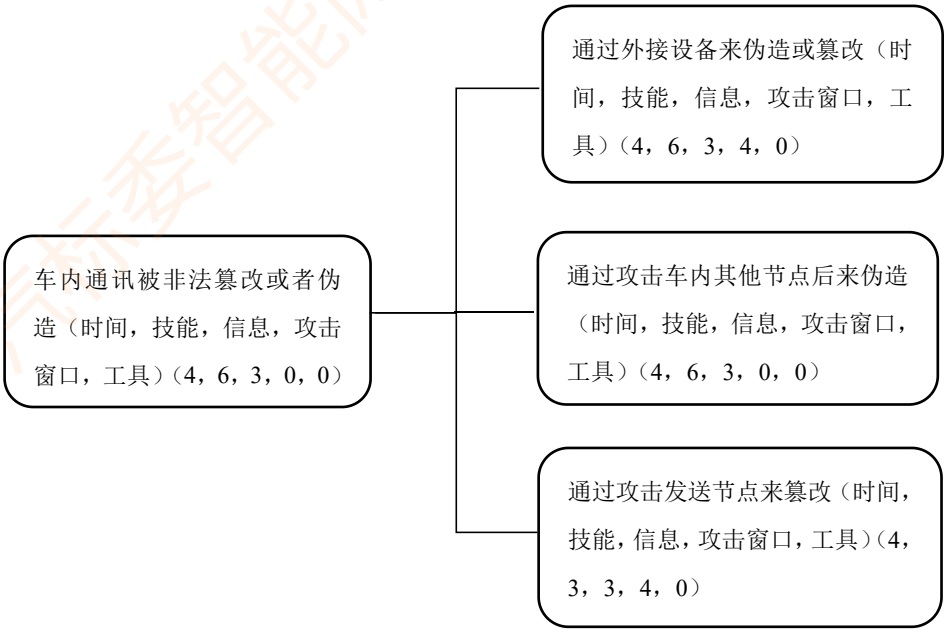

图 3.3 车内通讯篡改攻击可行性分析

表 3.3 威胁分析及影响分析

威胁	损害	损害严重程度	攻击可行性	风险
感知或决策系统的软件被非法篡改	错误的感知或者决策，导致系统错误制动，后车追尾。	高（刹车系统对于错误的制动请求有门限值的限制和监控，所以严重度在一定程度上有所缓解）	高	4
	错误的感知或者决策，导致系统未触发，出现碰撞事故	最高	高	5
车内通讯被非法篡改或者伪造	刹车系统接收到错误的制动请求，导致系统错误制动，后车追尾。	高（刹车系统对于错误的制动请求有门限值的限制和监控，所以严重度在一定程度上有所缓解）	高	4
	刹车系统未接到制动请求，导致系统未触发，出现碰撞事故	最高	高	5
刹车系统被非法篡改	刹车系统的完整性被破坏，导致系统错误制动，后车追尾。	最高（刹车系统对于错误的制动请求有门限值的限制和监控亦可能被破坏）	高	5
	刹车系统的完整性被破坏，导致系统该触发时未触发，出现碰撞事故	最高	高	5

车内网络的拒绝服务攻击	自动紧急刹车系统无法激活，不可用	中	高	3

3.2 汽车网关案例

针对零部件——网关的风险评估流程，从该零部件的功能出发，如网关的功能有车内 CAN/LIN 报文高速传输、车内以太网高速传输模式、车内网络行为管理、 FOTA（Firmware Over-The-Air 空中下载软件升级）、 TSP（车载信息服务系统服务）服务-远程诊断等。

按照风险评估的流程及网关功能的划分，本文针对网关的 FOTA 功能进行网关风险评估的流程示范。

3.2.1功能概述

网关（GW）的作用就是为在不同的通信协议和不同的传输速度的计算机或模块之间进行通信时，建立连接和信息解码，重新编译，并将数据传输给其他系统。

FOTA 是指通过云端升级技术，为具有连网功能的设备提供固件升级服务。车载电子设备，如 T-Box，车载信息娱乐系统，或其他一些有升级需求的 ECU，在连网后采用 FOTA 方式进行固件系统升级。

3.2.2资产识别

根据项目涉及的资产，列出资产清单，并进行用例描述，分析已有的安全机制。网关 FOTA 功能资产识别示例如下。

表 3.4 资产识别

功能	资产 ID	资产类型	资产名称	用例描述	已有的安全机制
Fn_01 FOTA	As_001	网关-芯片（如 MPU）	MPU-NXP xxxxG	收到软件数据包，写入网关，通过网关内部各个模块协作进行，将数据传送至各系统 ECU。	1.安全启动 2.回滚机制 3.安全漏洞 4.安全日志

根据资产信息，首先进行威胁分析：进行安全属性识别，建立 STRIDE 威胁

模型（包括：欺骗、篡改、抵赖、信息泄露、拒绝服务、提权），并分析出损害场景及潜在的车辆威胁场景、攻击路径；然后进行风险评估：包括威胁分析及威胁等级计算，影响分析及影响等级计算。

3.2.3威胁分析

进行威胁分析要从安全属性出发，安全属性有真实性、完整性、不可抵赖性、机密性、可用性、权限、时效性、隐私 8 个属性。基于安全属性的划分，分别分析损害场景、建立 STRIDE 威胁模型、分析潜在的车辆威胁场景及攻击路径。

如对应 FOTA 功能的“真实性”的安全属性，可能存在的损害场景为破坏网关 MPU 的安全性能，通过发送自制的软件升级包舞蹈 MPU 对转向 ECU 进行错误更新，导致车辆在行驶中意外转向。该损害场景及安全属性对应的 STRIDE 模型为“欺骗”，对应的潜在的车辆威胁场景为：攻击者使用伪造的软件升级数据，破坏 MPU 的安全性能，导致 GW 进行错误更新，通过发送自制的软件升级包误导 GW 对转向 ECU 进行错误更新，导致车辆行驶中意外转向。存在的攻击路径为：攻击者攻入汽车企业 APN 专网，明确车辆信息后，穿透 Tbox 安全机制，向车辆发送 FOTA 流程。

3.2.4风险评估

（1） 威胁评估

威胁评估根据威胁分析得出的威胁情况，从专业水平、对目标的知识度、机会窗口、设备的角度进行威胁评估，并得出各方面的指标值。

如要实现上节所述的攻击路径，需要的专业水平为“Expert”，因为伪造数据需要满足接口特征，该方面对应的指标值为 2；需要的对目标的知识度为“Sensitive”，因为需要对升级接口有深入了解，对应的指标值为 2；需要的机会窗口为“Critical”，因为网关属于半开放接口，对应的指标值为 0；设备水平为“Bespoke”，因为需要定制设备，对应的指标值为 2。

（2） 威胁等级计算

威胁计算时可根据实际情况换算，本文中威胁水平参数值等于各指标值相加。

$$TV=2+2+0+2=6$$

威胁等级评估规律如下表所示：

表 3.5 威胁等级评估表

威胁水平参数总值	威胁等级	威胁等级值
>9	无	0
7-9	低	1
4-6	中	2
2-3	高	3
0-1	严重	4

根据上表的对应关系可以得出威胁等级为中等，威胁等级值为 2。

3.2.5影响分析

根据威胁分析的结果，对损害场景所造成的影响从安全、经济、操作、隐私和法律（SFOP）四个方面进行分析，并得出每个影响的指标值。

如损害场景所造成的影响，在安全方面为“S3”级，因为车辆行驶中意外转向，会威胁生命安全，并且伤害不确定是否会生存，是否会有致命伤害，所以对应的指标值为 1000；造成的经济损失为“Medium”，因为所造成的损害会导致重大的财务损失，但不会威胁到组织的生存，所以指标值为 100；对车辆运转造成的影响为“High”，应为未能满足安全或监管要求，所以指标值为 100；在隐私和法律角度造成的影响为“High”，因为违反了法律，所以对应的指标值为 100。

3.2.6影响等级计算

影响计算时可根据实际情况计算，本文中影响参数值等于各指标值相加。

$$IV=1000+100+100+100=1300$$

影响等级评估规律如下表所示：

表 3.6 影响等级评

影响参数总值	影响等级	影响等级值
0	无	0
1-19	低	1
20-99	中	2
100-999	高	3
>=1000	严重	4

根据上表的对应关系，可知影响等级为严重，影响等级值为 4。

3.2.7风险处置决策

当进行威胁评估与影响分析之后，需要对两者的结果进行汇总，得出整体的安全等级。根据安全等级决定风险处置决策，并得出安全目标或高级别安全要求，对于未选择风险降级的风险处理决策，涵盖理由和结论在内的信息安全声明应被视为项目的安全参照。对于安全等级的评价本文使用矩阵法，如下表所示：

表 3.7 安全等级评估矩阵

安全等级	影响等级					
威胁等级		0	1	2	3	4
	0	无	无	无	无	低
	1	无	低	低	低	中
	2	无	低	中	中	高
	3	无	低	中	高	高
	4	低	中	高	高	严重

如对上述的威胁等级值为 2，影响等级值为 4，根据矩阵法对应的安全等级为高，风险处置决策为：风险缓解，安全目标/高级别安全要求为：设置完整性校验如写入代码签名，具备强安全校验以保证安全性；配置访问控制列表，为外来信息授予权限，缓解由于以太网欺骗而导致的车辆安全风险。

3.2.8威胁等级参数

表 3.8 威胁等级参数表

参数	等级	指标说明	值
Expertise 专业水平	Layman 外行	与没有在某一技术领域有深入研究的专家或工程师相比，所谓的外行对于专业的涉猎是较浅的，例如，包括只会遵从可用工具或设备附带的简单的指导书的指导而去进行简单的攻击的工程师，一旦指导书或工具未按照预期的进行，就无法开展后续的工作。	0
	Proficient 熟练的	“精通”是指工程师具有安全领域的专业知识，并参与过业务，例如，车间的技术人员。 知道简单且被熟知的攻击手段的专业人士。 他/她们能够进行攻击，例如，使用可用的工具调整里程表的参数，或者安装假冒的零部件，具备快速的设计和开发攻击脚本以达到预期效果的能力。	1

	Experts 专业的	技术专家需熟悉底层的算法，协议，硬件设计，架构，安全机制，安全技术的原理，加密技术的原理，定义新出现的攻击事件所用到的技术手段和工具，针对不同产品的经典攻击手段，例如已实现的针对某类产品或系统的攻击。	2
	Multiple Expert 多专家	此处需考虑对于一个真实完整复杂的攻击过程，攻击链路各节点需涉及不同领域专业人士的专家进行研究设计。	3
Knowledge about TOE 对目标的知识度	Public 公开的	指可以从网络，纸质书，或无保密协议限制的信息中取得。	0
	Restricted 受限的	指在组织开发人员内部共享，或在有保密协议的组织之间共享。	1
	Sensitive 敏感的	指在组织开发人员内部各团队之间共享的信息，访问权限仅限于指定团队的成员。	2
	Critical 关键的	指只有少数几个人掌握的信息，严格的控制在核心技术人员和管理人员的范围内。	3
Window of opportunity 机会窗口	Low 低	可用性低，例如，通过复杂的操作才可接触式的访问，通过零部件的拆解才可进入车辆内部发起攻击	3
	Medium 中	可用性中，例如，虽然物理或逻辑访问受到限制，但无需任何特殊设备即可打开例如打开机盖接入电线。	2
	High 高	可用性高，例如，存在逻辑或远程访问的接口，无需接触式的访问。	1
	Critical 严重的	可用性极高，无需接触，仅通过公共/不受信任的网络进行逻辑或远程访问，无限制的访问内部资产，例如，无线或蜂窝接口。	0
Equipment 设备	Standard 普通的	指攻击者可以随时使用的公开设备或开源工具，利用漏洞，进行攻击。此设备可能是系统本身的一部分，例如操作系统中的调试器。或通过网络下载，轻松获得的工具，例如，攻击脚本。或一些简单的诊断设备，测试设备。	0
	Specialized 专业的	指需要购买但操作相对简单的设备。包括购买适量的设备，例如电源分析工具，需数百台电脑搭建的复杂的网络环境。或开发量较大的攻击脚本或程序，例如车内通讯设备，昂贵的车间诊断设备。	1
	Bespoke 需定制的	指不容易为公众使用，需要专门设计，制作例如非常复杂的软件的设备。或者因为其专业性而存放条件严格受限的设备。	2

		或者，极端昂贵的设备。	
	Multiple Bespokes 需多面定制	此处需考虑对于一个真实完整复杂的攻击过程，攻击链路各节点需涉及不同的专业设备进行攻击的实际情况。	3

3.2.9影响等级参数

表 3.9 影响等级参数表

参数	指标		指标说明	指标值
Safety 安全	S0		无伤害	0
	S1		轻度的/中度的伤害	10
	S2		严重的/威胁生命的伤害	100
	S3		威胁生命的/致命的伤害	1000
Financial 经济损失	No Impact 无影响		无明显的影响/后果	0
	Low 低		财产损失在可接收的范围内	10
	Medium 中		所造成的损害会导致重大的财务损失，但不会威胁到组织的生存	100
	High 高		经济损失会威胁到组织的生存	1000
Operational 车辆运转	No Impact 无影响	无破坏效果	无明显的影响	0
	Low 低	轻微破坏	车辆的外观受到了影响或在车辆运转时发出现非预期的噪音车辆在此状态下运转时，会出现令人不悦的情况，影响超过 25%的车辆用户	1
			车辆的外观受到了影响或在车辆运转时发出现非预期的噪音车辆在此状态下运转时，会出现令人不悦的情况，影响超过 50%的车辆用户	
		中等破坏	车辆的外观受到了影响或在车辆运转时发出现非预期的噪音车辆在此状态下运转时，	

			会出现令人不悦的情况，影响超过 75%的车辆用户	
	Medium 中	中等破坏	非核心功能受到影响车辆仍可操作，但舒适性或便利性功能无法满功率运转	10
			非核心功能无法工作车辆仍可操作，但舒适性或便利性功能无法运转	
		严重破坏	核心功能受到影响车辆仍可操作，但核心功能如 ADAS 无法满功率运转	
	High 高	极严重破坏	核心功能无法工作车辆仍可操作，但核心功能如 ADAS 无法运转	100
			由于未充分遵从政府的法律规定，潜在的风险影响了整车的运行	
		不满足安全法规的基本要求	由于政府的法律规定未加以说明和规范，潜在的风险影响了整车的运行	
Privacy and legislation 隐私及法律法规	No Impact 无影响		未违反隐私保护和法律的相关规定	100
	Low 低		-侵犯特定利益相关者如车主，驾驶员的隐私，但未导致隐私信息的滥用如假冒受害者实施犯罪活动 - 侵犯其它利益相关者如主机厂，车队所有者的隐私，但不会造成财务或运营的严重问题，例如主机厂受到了侵犯，但未遭受数目较大的经济罚单	
	Medium 中		-侵犯特定利益相关者如车主，驾驶员的隐私，导致隐私信息的滥用如假冒受害者实施犯罪活动，并受到了媒体的报道 -侵犯其它利益相关者如主机厂，车队所有者的隐私，造成财务或运营的严重问题丢失极大的市场份额	

	High 高	- 侵犯多个利益相关者如车主，驾驶员的隐私，但未导致隐私信息的滥用如假冒受害者实施犯罪活动，近而导致广泛的媒体报道，并给主机厂所有者的市场份额，业务运营，信任，声誉和财务损失造成严重损失。 - 侵犯其它利益相关者如主机厂，车队所有者的隐私，造成财务或运营的严重问题丢失极大的市场份额，巨额的罚款等，以及广泛的媒体报道	

3.2.10 风险处置建议

表 3.10 风险处置

风险处置办法	描述
风险缓解	通过引入，删除或更改安全控制选项来管理风险级别，以便可以将剩余风险重新评估为可接受的水平
风险保留	根据风险评估的结果，保留风险而不采取进一步措施的决定
风险规避	避免引起特定风险的活动或行为
风险转移	根据风险评估的结果，将风险与最有效管理特定风险的另一方共享

4 结论及建议

汽车信息安全风险评估有助于发现汽车存在的安全问题及隐患，是保障汽车全生命周期信息安全的必要措施。通过上述信息安全风险评估方法对比研究分析汽车信息安全风险评估标准化及应用的建议如下：

第一，基于 ISO/SAE 21434 标准中汽车风险评估的方法指导，融合了 EVITA 和 HEAVENS 的方法特点，成为行业认可的汽车信息安全评估的方法论。国内，汽标委智能网联汽车分标委下设汽车信息安全标准工作组，正在进行国际标准转化，形成推荐性国家标准 GB/T 《道路车辆 信息安全工程》，可以用于指导汽车全生命周期的风险评估相关活动及流程，目前暂时不建议单独编制一个汽车信息安全风险评估标准，对汽车风险评估进行统一要求。

第二，风险评估方法有多个，不同方法各有侧重点，相关企业可以参考现有标准的方法论的指导，根据企业及产品自身的特点选用具体的评估方法，进行风

险分析，最终得出风险处置决策方案。

第三，风险评估在实践应用时会遇到很多细节问题，由于汽车产品智能化、网联化、电动化、共享化进程不断推进，汽车产品在不断更新迭代，汽车信息安全风险评估在遵循现有标准指导的基础上，根据汽车发展的情况进行调整，以将方法灵活的应用于新技术新产品的分析。