在现实物联网环境下，域间资源在进行跨域调度时需要考虑的不仅仅是信任度，还需要考虑到数据资源传输时所付出的代价和获得收益。各域的域管理服务器在进行了综合判定和比较后可以分析出，在不同上下文环境下与其他域进行资源调度时本域所能获得收益情况。由于域间信息交互都是理性且处于利己因素考虑的，所以在物联网环境下域间交互的信任推荐决策可以借助信任博弈的理论进行分析，以保证达到最优交易的博弈均衡，资源交互双方均获益。

软件开发失败的风险是客观存在的。因此，风险分析对于软件项目管理是决定性的。风险分析实际上就是贯穿在软件工程过程中的一系列风险管理步骤，其中包括：风险识别、风险估计、风险管理策略、风险解决和风险监督等。

风险因素：

① 产品大小。实践经验表明项目风险和产品的大小成正比。公认产品大小度量单位是以代码行或功能点计。

② 技术相关。未曾使用过的新技术都存在风险。包括未使用过的新型硬件、支持软件，缺乏标准与规范的非传统的开发方法等。技术过时也是风险。技术风险一般难于改正。

③ 开发环境。适用的开发工具不足、不可靠、使用不方便等因素，都会降低开发效率。

④ 组织规模和人员经验。

⑤ 客户因素。表现在客户需求经常矛盾，不了解客户的特殊需要，客户不了解项目中采用的新技术，且双方又难于沟通等。

风险分析：

风险通常是指由于当事者主观上不能控制的一些因素的影响，使得实际结果与当事者的事先估计有较大的背离而带来的经济损失。这些背离产生的原因，可能是当事者对有关因素和未来情况缺乏足够情报而无法作出精确估计，也可能是由于考虑的因素不够全面而造成预期效果与实际效果之间的差异。进行风险分析，有助于确定有关因素的变化对决策的影响程度，有助于确定投资方案或生产经营方案对某一特定因素变动的敏感性。若一种因素在一定范围内发生变化，但对决策没有引起很大影响，则所采取的决策对这种因素是不敏感的；若一个因素的大小稍有变化就会引起投资决策的较大变动，则决策对这一因素便是高度敏感的。了解在给定条件下的风险对这些因素的敏感程度，有助于正确地作出决策。

风险分析是找出行动方案的不确定性（主观上无法控制）因素，分析其环境状况和对方案的敏感程度；估计有关数据，包括行动方案的费用，在不同情况下得到的收益以及不确定性因素各种机遇的概率，计算各种风险情况下的经济效果；作出正确判断，等等。

风险分析技术：

风险因素分析法：

风险因素分析法是指对可能导致风险发生的因素进行评价分析，从而确定风险发生概率大小的风险评估方法。其一般思路是：调查风险源→识别风险转化条件→确定转化条件是否具备→估计风险发生的后果→风险评价。

风险评价：

风险评价，又称安全评价，是指在风险识别和估计的基础上，综合考虑风险发生的概率、损失幅度以及其他因素。得出系统发生风险的可能性及其程度

风险评估：

风险评估就是量化测评某一事件或事物带来的影响或损失的可能程度。

从信息安全的角度来讲，风险评估是对信息资产（即某事件或事物所具有的信息集）所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估。作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

风险评估过程注意事项

在风险评估过程中，有几个关键的问题需要考虑。

首先，要确定保护的对象（或者资产）是什么？它的直接和间接价值如何？

其次，资产面临哪些潜在威胁？导致威胁的问题所在？威胁发生的可能性有多大？

第三，资产中存在哪些弱点可能会被威胁所利用？利用的容易程度又如何？

第四，一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？

最后，组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？

解决以上问题的过程，就是风险评估的过程。

进行风险评估时，有几个对应关系必须考虑：

每项资产可能面临多种威胁

威胁源（威胁代理）可能不止一个

每种威胁可能利用一个或多个弱点

风险评估的主要任务包括：

识别评估对象面临的各种风险

评估风险概率和可能带来的负面影响

确定组织承受风险的能力

确定风险消减和控制的优先等级

推荐风险消减对策

风险矩阵法

根据风险矩阵法可以辨识出每个作业单元可能存在的风险问题，并判定这种风险问题可能产生的后果及产生这种后果的可能性，二者相乘，得出所确定问题的风险值。然后进行风险分级，根据不同级别的风险，采取相应的风险控制措施。风险的数学表达式记为：



其中：R表示风险值；L表示发生问题的可能性；S表示发生问题后果的严重程度。

本章从交互成功率、恶意攻击、实体状态、网络环境状态、模型性能五个方面对物联网环境下跨域实体间进行交互活动过程中风险出现的可能性（L）进行评价取值，取五项得分的最高的分值作为其最终的L值。从问题从未发生，极少发生，偶尔发生，多次发生以及频繁发生五个方面对后果的严重程度（S）进行评价取值，取得五项最高的分值作为其最终的S值。确定了S和L值后，根据R＝L×S计算出风险度R的值。分析过程如表4.2

表4.2

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 后果及严重性 | | | | |  | 可能性 | | | | |
| 风险分类 | I | A | S | E | M | A | B | C | D | E |
| 交互成功率 | 恶意攻击 | 实体状态 | 网络环境 | 模型性能 | 从未发生 | 极少发生 | 偶尔发生 | 多次发生 | 频繁发生 |
| 1 | 无失败 | 无攻击 | 状态稳定 | 环境稳定 | 性能稳定 | 1 | 2 | 3 | 4 | 5 |
| 2 | 极少失败 | 极少攻击 | 极少故障 | 极少异常 | 极少异常 | 2 | 4 | 6 | 8 | 10 |
| 3 | 偶尔失败 | 偶尔攻击 | 偶尔故障 | 偶尔异常 | 偶尔异常 | 3 | 6 | 9 | 12 | 15 |
| 4 | 多次失败 | 多次攻击 | 多次故障 | 多次异常 | 多次异常 | 4 | 8 | 12 | 16 | 20 |
| 5 | 全部失败 | 经常攻击 | 经常故障 | 停止使用 | 停止工作 | 5 | 10 | 15 | 20 | 25 |

其中：

|  |  |  |  |
| --- | --- | --- | --- |
| 特高风险区 | 需要立即停止一切交互活动，排除风险因素 | 20-25 |  |
| 高风险区 | 需要采取有效的控制措施 | 15-19 |  |
| 中风险区 | 需要进行有限的风险管理 | 7-14 |  |
| 低风险区 | 需要进行跟踪监控 | 1-6 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| p | a | s | e | m |
| 交互失败率 | 恶意攻击 | 实体状态 | 网络环境 | 模型性能 |