ICS 03.100.01
CCS A 02

中华人民共和国国家标准

GB/T 27921—2023/IEC 31010:2019
代替 GB/T 27921—2011

风险管理　风险评估技术

Risk management—Risk assessment techniques

（IEC 31010:2019,IDT）

2023-08-06 发布　　2023-08-06 实施

国家市场监督管理总局
国家标准化管理委员会　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》的规定起草。

本文件代替GB/T 27921—2011《风险管理　风险评估技术》,与GB/T 27921—2011相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 删除了“风险评估概念”一章(见2011年版的第4章);

b) 增加了“核心概念”一章(见第4章);

c) 增加了“制定风险评估计划”“信息管理和模型开发”等内容(见6.1、6.2),并对“风险评估技术的应用”做了更加详尽的说明(见6.3,附录B);

d) 删除了“风险评估技术的比较”(见2011年版的附录A);

e) 增加了风险评估技术的分类和应用(见附录A)。

本文件等同采用IEC 31010:2019《风险管理　风险评估技术》。

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。

本文件由全国风险管理标准化技术委员会(SAC/TC 310)提出并归口。

本文件起草单位:广东坚美铝型材厂(集团)有限公司、中国标准化研究院、第一会达(北京)数据技术有限公司、安徽华普检测技术有限公司、中国核能电力股份有限公司、浙江吉诚织造有限公司、江苏核电有限公司、工业和信息化部电子第五研究所、中共中央党校(国家行政学院)、北京大学、达信评(北京)风险管理咨询有限公司、国家科技风险开发事业中心、中国矿业大学(北京)、中国计量大学。

本文件主要起草人:陆小伟、高晓红、刘剑、徐涵、张鹏、华春翔、孙友文、施颖、吕多加、崔艳武、游志斌、刘新立、王雷、王兰、张杰军、周玉焕、徐龙辉、宾建伟、刘奕宏、于敏、纪春阳、张月义、陶影海、谢雪萍。

本文件所代替文件的历次版本发布情况为:

——2011年首次发布为GB/T 27921—2011;

——本次为第一次修订。

引　言

本文件提供了各种风险评估技术的选择和应用指导，这些技术可用于帮助改进考虑不确定性的方式，并帮助理解风险。

风险评估技术可用于以下场景：

a) 需要进一步了解存在什么风险或特定风险的源头；

b) 在决策中，对有风险的选项进行比较或优化时；

c) 在需要采取措施应对风险时。

在 ISO 31000 中所述的识别、分析和评价风险的风险评估步骤中，以及在需要了解不确定性及其影响时，通常使用这些风险评估技术。

本文件中描述的风险评估技术，可以在广泛的场景中使用，但大多数技术起源于技术领域。有些技术概念相似，但名称和方法不同，反映了它们在不同领域的发展历史。技术随着时间的推移而不断发展，许多技术可以在其初始应用领域之外的广泛情形下使用。技术可以以新的方式进行调整、组合和应用，或者扩展，以满足当前和未来的需求。

本文件介绍了所选择的风险评估技术，并比较了其可能的应用、优势和局限。它还提供了更为详细的信息来源作为参考。

本文件的潜在使用者是：

a) 参与评估或管理风险的任何人；

b) 参与制定指南的人，该指南规定了如何在特定情况下评估风险；

c) 需要在存在不确定性的情况下做出决策的人员，包括：

——委托或评价风险评估的人员；

——需要了解评估结果的人；

——以及那些必须选择评估技术以满足特定需求的人。

需要为合规或一致性目的进行风险评估的组织，将受益于使用适当正式的和标准化的风险评估技术。

风险管理　风险评估技术

1　范围

本文件为各种情况下风险评估技术的选择和应用提供了指导。这些技术用于支持不确定性情景下的决策，提供有关特定风险的信息，并作为风险管理过程的一部分。本文件提供了一系列技术的总结，并参考了对这些技术进行更详细描述的其他文件。

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。

GB/T 23694—2013　风险管理　术语(ISO Guide 73:2009，IDT)

GB/T 24353—2022　风险管理　指南(ISO 31000:2018，IDT)

3　术语和定义

GB/T 24353—2022、GB/T 23694—2013 界定的以及下列术语和定义适用于本文件。

3.1

可能性　likelihood

某件事发生的概率。

注 1：在风险管理术语中，无论是以客观的或主观的、定性或定量的方式来定义、度量或确定，还是用一般词汇或数学术语来描述(如概率，或一定时间内的频率)，“可能性”都用来表示某件事发生的概率。

注 2：“可能性(likelihood)”这一英语词汇在一些语言中没有直接与之对应的词汇，因此经常用“概率(probability)”这个词代替。不过，在英语中，“概率”常常被狭义地理解为一个数学词汇。因此，在风险管理术语中，“可能性”有着与许多语言中使用的“概率”一词相同的解释，而不局限于英语中“概率”一词的意义。

[来源：GB/T 24353—2022，3.7]

3.2

机会　opportunity

预期有利于目标实现的情形。

注 1：机会是一种积极的情景，在这种情景下，很可能获得收益，并且对其拥有相当程度的控制。

注 2：一方的机会可能对另一方构成威胁。

注 3：抓住或不抓住机会都是风险的来源。

3.3

概率　probability

对事件发生几率的度量，用 0 到 1 之间的数字表示。0 表示不可能发生，1 表示确定发生。

注：见定义 3.1 的注 2。

3.4

风险驱动因素　risk driver；driver of risk

对风险有重大影响的因素。

3.5

威胁　threat

危险、伤害或其他不良结果的潜在来源。

注 1：威胁是一种消极的情景，在这种情景下，很可能会损失，并且对其控制相对较少。

注 2：对一方的威胁可能对另一方构成机会。

4　核心概念

4.1　不确定性

不确定性是一个包含许多基本概念的术语。各界已经对于不确定性的分类做了许多尝试，且将继续完善。不确定性的类别包括：

——一些现象固有的可变性造成的不确定性，这种不确定性不能通过进一步的研究而降低。例如，掷骰子(有时也称为“随机不确定性”)；

——由于缺乏知识而造成的不确定性，这种不确定性可以通过收集更多数据、改进模型、改进抽样技术等方法来降低(有时也称为“认知不确定性”)。

其他常见的不确定性类型包括：

——语言不确定性，指的是口语中固有的模糊性和歧义性；

——决策不确定性，与风险管理策略尤其相关，指的是识别与价值体系、专业判断、企业价值观和社会规范相关的不确定性。

不确定性的例子包括：

——假设条件是否真实的不确定性，包括对人或系统可能行为的假设；

——决策所基于的各项参数的可变性；

——用来预测未来的模型在有效性或准确性方面的不确定性；

——事件(包括环境和条件的改变)的发生、特征和结果的不确定；

——与破坏性事件相关的不确定性；

——系统性问题的不确定性结果，例如缺少合格员工，此类不确定性可能带来无法清晰定义的广泛影响；

——认识到不确定性但没有完全理解时感受到的知识缺乏；

——不可预测性；

——由于人类思维的局限性产生的不确定性，例如，理解复杂数据、预测存在长期影响的情况、作出无偏见的决策等方面。

不是所有的不确定性都能被理解，不确定性的重要性可能很难或不可能被定义或影响。但是，如果认识到在特定情景下存在不确定性，就可以建立预警系统，以主动和及时地发现变化，并作出安排，建立应变能力，以应付意外情况。

4.2　风险

风险包括 4.1 所描述的所有形式的不确定性对目标的影响。不确定性可能带来积极的和/或消极的后果。

风险通常以风险源、潜在事件、其后果和可能性来描述。一个事件可能有多种原因并导致多种后果。后果可能具有多种离散值、或是连续变量、或者未知。起初，后果可能无法识别或度量，但可能会随着时间的推移而累积。风险的来源包括固有的可变性，或与一系列很难预测的因素相关的不确定性，包括人的行为、组织结构、社会影响等。因此，风险不能总是很容易地作为一组事件、其后果和可能性进行列举。

风险评估技术旨在帮助人们了解这种广泛、复杂和多样背景下的不确定性和相关风险，以支持明智的决策和行动。

5 风险评估技术的使用

本文件中介绍的风险评估技术，能够帮助人们理解不确定性及其对决策和行动的影响。

ISO 31000 描述了风险管理的原则，以及有助于管理风险的基础和组织安排。它详述了一个过程，使风险能够根据作为过程的一部分而建立的准则，被识别、理解和调整。风险评估技术可用于这些结构化的方法中，包括建立环境、评估和应对风险，以及持续监督、检查、沟通和咨询、记录和报告。该过程如附录 A 的图 A.1 所示，图中还显示了可在过程中应用的技术示例。

在 ISO 31000 的过程中，风险评估包括风险识别、风险分析，并利用从分析中获得的理解，通过得出风险对于组织目标和绩效阈值的相对重要性的结论，来评价风险。这一过程为决定是否需要应对措施，以及应对措施和旨在应对风险的行动的优先级提供了输入。在实践中，这个过程是循环进行的。

本文件中描述的风险评估技术用于下列场景：

——需要进一步了解存在何种风险、或某一特定风险；

——在需要采取措施应对风险时；

——在决策中，对有风险的选项进行比较或优化时。

具体来说，这些技术可以用于：

——在不确定性的情况下，为决策和行动提供结构化信息；

——明确假设条件对目标的影响；

——当每个选项都存在多种不确定性时，对选项、系统、技术和方法进行比较；

——支持确定切合实际的战略和运营目标；

——支持确定组织的风险准则，例如，风险限额、风险偏好、风险承受能力；

——结合风险，设定或审查优先级时；

——认识并理解风险，包括可能导致极端后果的风险；

——理解哪些不确定性对组织目标最重要，并提供应对这些不确定性的基本依据；

——更有效地识别和利用机会；

——明确导致风险的要素，了解这些要素为什么重要；

——识别有效、高效的风险应对措施；

——确定拟议的风险应对措施的改变效果，包括对风险属性和程度的改变；

——沟通风险及其影响；

——从失败和成功中学习，从而提高风险管理的能力；

——证明自身满足了监管等要求。

评估风险的方式，取决于情况的复杂性和新颖性，以及相关知识和理解的水平。

——在最简单的情况下，这种情况没有任何新的或不寻常的地方，风险得到充分理解，没有重大利益相关者影响或后果不重大，则可能会根据既定的规则和程序，以及之前的风险评估来决定评估的方式。

——在面对非常新颖、复杂或具有挑战性、高度的不确定性和很少的经验的问题时，几乎没有可以作为评估基础的信息，传统的分析技术可能没有用处或没有意义。这也适用于利益相关者持有截然不同观点的情况。在这些情况下，可能会使用多种技术来获得对风险的部分理解，然后根据组织和社会价值以及利益相关者的观点作出判断。

本文件中描述的技术，在上述两种极端之间的情况下具有最大的应用价值，其复杂性适中，并且有一些可用的信息来进行评估。

6 风险评估的实施

6.1 制定风险评估计划

6.1.1 确定风险评估目的和范围

确定风险评估的目的，包括识别相关的决策或行动、决策者、利益相关者、所需输出的时间和性质（例如，是否需要定性、半定量或定量信息）。

确定风险评估的范围、深度和详细程度，并说明包括和排除的内容。确定风险评估中包括的后果类型。指定与评估活动相关的条件、假设、约束或必要资源。

6.1.2 理解背景

在进行风险评估时，相关人员需理解根据其评估作出决策和采取行动所处的大背景，包括理解构成该组织发展背景的内部和外部问题，以及更广泛的社会和环境问题。所有对背景的描述都需审核查实，以确保它是适时和恰当的。在重大复杂情况下，理解大背景尤为重要。

6.1.3 利益相关者的参与

识别利益相关者和可能提供有用知识与相关意见的人员，无论他们是否参与风险评估，都需考虑他们的观点。利益相关者的适当参与，有助于确保风险评估所依据信息的有效性和适用性，确保利益相关者能够理解决策背后的原因。利益相关者的参与，可以：

——提供有助于理解评估背景的信息；

——综合不同领域的知识和专业能力，更有效地识别和理解风险；

——提供使用技术所需的专业知识；

——使利益相关者的利益得到理解和考虑；

——为确定风险是否可接受的过程提供输入，尤其是当利益相关者受到影响时；

——满足知情或咨询人员的相关要求；

——获得对风险评估产生的输出和决策的支持；

——识别在风险评估之前或期间需要弥补的知识缺口。

需考虑如何将风险评估的输出和结果，可靠、准确和透明地传达给利益相关者。

征求利益相关者和专家意见的技术见附录 B 的 B.1。

6.1.4 确定目标

需确定开展风险评估的特定系统或过程的目标，并在可行的情况下进行记录。这将有助于识别风险并理解其影响。

在可行的范围内，目标宜：

——专门针对评估的对象；

——可进行定性或者定量度量；

——在背景的约束范围内是可实现的；

——与组织的整体目标或背景环境相关；

——在规定的时间段内是可实现的。

6.1.5 考虑人员、组织和社会因素

可明确并酌情考虑人、组织和社会因素。人的因素与风险评估有以下关系：

——作为不确定性的来源；

——对技术选择和应用方式的影响；

——对解释和使用信息的方式产生影响(例如，对风险的认知差异)。

人的行为(无论高于或低于预期)是一种风险源，也可能影响控制的有效性。在评估风险时，宜特别考虑到人的行为有可能偏离预期和假设。人的行为通常很复杂，需要专家意见来帮助识别和分析与之相关的风险。

人的因素还会影响到技术的选择和使用，尤其是在需要进行判断或使用小组工作方法的情况下。需要通过熟练的引导，来降低这种影响。同时，还需要处理群体思维和过度自信(例如，在估计和感知方面)等偏见。专家意见宜尽可能以证据和数据为依据，并努力避免或尽量减少认知偏见。

人的个人目标和价值观可能与组织的目标和价值观不同。这可能导致对风险水平的不同认识以及个人决策的不同准则。组织可努力在内部实现对风险的共同理解，并考虑利益相关者的不同意见。

社会方面，包括社会经济地位、种族和文化、性别、社会关系、居住和社区环境等，都会直接或间接地影响风险。这些影响可能是长期的，不会立即显现，宜进行长期规划。

6.1.6 检查决策准则

6.1.6.1 概述

在作出决策时需要考虑的准则，包括风险准则，宜在进行评估之前进行检查。准则可能是定性的、半定量的、或者定量的。在某些情况下，可能没有明确的准则，利益相关者基于自己的判断对分析结果作出回应。

需要检查的准则包括：

——如何决定风险是否可接受；

——如何确定风险的相对重要性；

——如何在选项决策中考虑风险，其中每个选项都与可能产生正面或负面后果的多重风险相关，或两者兼而有之；

——如何考虑风险之间的关系。

6.1.6.2 确定风险是否可接受的准则

确定组织在追求目标时可接受风险的性质和程度的准则，有时被称为风险偏好，可以通过指定一种技术来确定风险的大小，或与风险相关的参数，以及超过该限额的风险变得不可接受。为不可接受的不利风险，设定的限额可能取决于潜在回报。

风险的可接受度，也可通过指定与目标相关的具体绩效指标的可接受变化范围来定义。

根据后果的类型，可以指定不同的准则。例如，组织接受财务风险的准则，可能不同于为人的生命风险定义的准则。

以下是在定义风险是否可接受时，使用的注意事项示例：

——风险承受能力(RBC)(也称为风险容量)：组织的 RBC 通常根据用于吸收风险的不利影响的风险资本来定义。对于商业公司而言，能力可能是指资产覆盖的最大维持能力，或公司在不宣布破产的情况下，可以承受的最大财务损失。宜通过压力测试场景对估计的 RBC 进行合理测试，以提供可靠的置信水平。组织的风险偏好反映了管理层利用其 RBC 的意愿；

——ALARP、ALARA 和 SFAIRP：在某些法域，处理安全相关风险的决策的立法准则，涉及确保伤害或健康不良的风险“尽可能合理降低”(ALARP)、“合理可能尽量低”(ALARA)或证明控制“在合理可行范围内”(SFAIRP)将风险降至最低(见 B.8.2)；

——“至少整体等效”(GALE)：如果可以证明来自其他来源的风险减少了同等或更大的量，则认为

来自特定来源的具有不利后果的风险增加是可以接受的；

——成本/效益准则，如每挽救一条生命的代价或投资回报率(ROI)。

6.1.6.3 评价风险重要性的准则

风险准则(用于确定风险重要性的参考标准)可以通过 6.3.5 和 6.3.7 中描述的风险特征、风险度量方法中的术语来表示。也可能与道德、文化、法律、社会、声誉、环境、合同、财务和其他因素相关。

一个风险与其他风险的相对重要性评价，通常是基于不同风险大小的估计，这些估计来自于与组织目标直接相关的阈值进行的对比。与这些阈值进行比较，可以告知组织宜重点对哪些风险进行应对，这取决于这些风险是否有可能导致结果超出围绕目标设定的阈值。

风险的大小，很少是确定风险重要性的唯一标准。其他相关因素包括可持续性(例如三重底线)和弹性、道德和法律标准、控制的有效性、控制不存在或失败时的最大影响、后果发生的时间、控制的成本和利益相关者的意见。

评价风险重要性的技术，见 B.8。

6.1.6.4 选项间决策的准则

组织将面临很多目标相互冲突的决策，并且需要同时考虑潜在的负面影响和收益。对于这样的决策，可能需要满足几个准则，并且可能需要在相互冲突的目标之间进行权衡。可识别与该决策有关的准则，并确定和说明加权准则或以其他方式进行权衡的方式，并记录和共享信息。在设定准则时，宜考虑到不同利益相关者的成本和收益可能不同。可决定如何考虑不同形式的不确定性。

在选项之间进行选择的技术，见 B.9。

6.2 信息管理和模型开发

6.2.1 概述

在进行风险评估之前和期间，宜收集相关信息。这些信息为统计分析、模型、以及附录 A 和附录 B 中所述技术提供了输入。在某些情况下，决策者无须进一步分析，即可使用这些信息。

每个步骤所需的信息取决于早期信息收集的结果、评估的目的和范围，以及分析使用的一种或多种方法。宜确定收集、存储、提供信息的方式。

宜决定哪些评估结果的记录需要保存，如何制作、存储、更新这些记录，并提供给有需要的人。可妥善维护信息来源。

6.2.2 收集信息

可以通过文献综述、观察和专家意见等渠道来收集信息。数据可以通过测量、实验、访谈和调研来收集或取得。

一般来说，数据直接或间接表示已发生的损失或收益。例如，项目成败、投诉的数量、财务损益、对健康的影响、伤亡等。其他可得的信息还包括失败的原因、投诉的来源、人身伤害的性质等。数据还包括模型和其他分析技术的输出。

宜确定以下问题：

——信息的来源及可信度；

——类型[例如，定性、定量还是两者兼有(见 6.3.7.1)]；

——层次(例如，战略层、战术层、运营层)；

——所需数据的数量和质量；

——收集方法；

——保密级别；

当从抽样中获得待分析数据时，可说明所需的统计置信度，以便收集足够的数据。如果不需要统计分析，则宜予以说明。

如果以前评估的数据或结果可用，宜首先确定背景是否有任何变化，如果有，早期数据或结果是否仍然有用。

宜评估和考虑在风险评估中所使用的信息的有效性、可靠性和局限性：

——信息的年代和相关性；

——信息的来源以及收集方法；

——信息中存在的不确定性和缺失；

——信息、数据集、算法和模型的权威性或来源。

6.2.3 分析数据

通过数据分析，可以：

——了解已发生的后果及其可能性，以便从经验中学习；

——了解趋势和模式，包括周期性，从中了解其对未来的影响；

——获得相关性，这些相关性为进一步验证可能的因果关系提供信息。

要识别和理解数据中的局限性和不确定性。

不能假设过去的数据继续适用于未来，但它们可以向决策者提示未来可能发生的情景。

6.2.4 开发和应用模型

6.2.4.1 概述

模型是对现实的近似表示。其目的是将本质复杂的情形，转化为便于分析的更简单的形式。模型可以帮助人们理解数据的意义、模拟在不同条件下实际中可能发生的情景。模型可以是有形的，也可以是软件中展示的，也可以是一组数学关系。

建模一般包括下列步骤：

——描述问题；

——描述建模的目的，以及预期结果；

——开发该问题的概念模型；

——建立该概念模型的有形、软件或数学表示；

——开发软件或其他工具，来分析模型的表现；

——处理数据；

——通过检查已知情况的输出，来验证或校准模型；

——根据模型得出现实世界问题的结论。

上述所有步骤都可能涉及近似、假设和专家判断，(如有可能)可独立于开发者之外的人员对模型进行验证。宜基于可用信息检查关键假设，从而验证其可信度。

为了在使用模型时获得可靠的结果，宜验证以下内容：

——概念模型充分代表了正在评估的情况；

——模型是在其设计环境的限制条件内使用的；

——充分理解模型和相关计算的理论概念；

——参数的选择和概念的数学表示都是合理的；

——充分理解计算背后的数学原理；

——输入数据准确、可靠，或者该模型的特性考虑了输入数据的可靠性；

——模型按计划运行，没有出现内部错误或缺陷；

——模型很稳定，对关键输入的微小变动不会过分敏感。

上述验证工作可通过下列步骤完成：

——进行敏感性分析，检查模型对输入参数变动的敏感性；

——对模型进行特定场景（往往是极端场景）的压力测试；

——将输出数据与历史数据（而不是模型产生的数据）进行比较；

——验证当模型由不同的人运行时，获得了相似的结果；

——将输出数据和现实情况进行对比。

模型以及建模所依据的理论和假设条件，可进行综合记录并保存，以备模型验证使用。

6.2.4.2 使用软件进行分析

可以使用软件来展示数据、组织数据、或者分析数据。用于建模和分析的软件往往拥有简单的用户界面和快速的输出，但也可能造成用户未注意到无效的结果。出现无效结果的原因可能有：

——用于表示现实情况的算法存在不足之处；

——在软件的设计和模型使用中作出的假设；

——输入数据出现错误，包括误解输入数据的含义；

——使用新软件时，出现数据转换的问题；

——对输出的错误解读。

商用软件一般是黑箱（商业秘密），可能存在上述差错。

在使用新软件测试更复杂的模型之前，宜使用具有已知输出、输入的简单模型测试新软件。宜保留测试细节，以供将来版本更新或新的软件分析程序使用。

可以通过增加或减少输入值确定输出是否按预期响应，来检查开发模型中的错误。这可以应用于各种输入。当改变数据输入时，通常会发现数据输入错误。该方法还提供了有关模型对数据变化的敏感性信息。

建议熟练掌握与特定分析相关的数学原理，从而避免结论出错。不仅可能发生上述错误，还可能选择不合适的软件程序。人们经常会沿着软件程序的设计进行操作，并相信其分析结果是正确的。宜收集证据，检查输出结果是否合理。

6.3 风险评估技术的应用

6.3.1 概述

附录 A 和附录 B 中描述的技术，用于强化对风险的理解作为不确定性情景下的决策的输入，包括关于是否以及如何处理风险的决策。

这些评估技术可用于：

——识别风险（见 6.3.2）；

——确定风险的原因、来源、驱动因素，以及风险的暴露程度（见 6.3.3）；

——评价控制措施的整体有效性，以及计划实施的风险应对措施的改变效果（见 6.3.4）；

——理解风险的后果和可能性（见 6.3.5）；

——分析相互和依赖关系（见 6.3.6）；

——提供进行风险度量的方法（见 6.3.7）。

第 7 章说明了在选择技术以执行上述行为时，需要考虑的因素。

一般情况下，分析可以是描述性的（例如，文献综述报告、情景分析、后果描述等）或定量的分析数据，得出数值。在某些情况下，可以使用排序或评级量表来比较具体风险。

风险评估的方式、输出结果的形式，宜与预设的准则相符。例如，定量准则要求使用定量分析技术，并得出使用正确单位的输出结果。

只有在所选度量指标允许时，才能使用数学运算。一般来说，数学运算不宜与排序量表一起使用。即使进行完全的定量分析，其输入值往往也是估计值。准确度和精度不宜受到与所用数据和方法一致的结果之外的因素的影响。

6.3.2 识别风险

识别风险可以明确考虑不确定性。根据评估的背景环境和范围，不确定性的所有来源，以及有益和有害的影响都可能是相关的。

识别风险的技术，往往会使用多个利益相关者的知识和经验(见 B.1.1)，包括：

——存在哪些不确定性、可能具有什么影响；

——哪些情况和问题(包括有形和无形问题)可能产生未来的后果；

——目前存在及未来可能出现哪些来源的风险；

——目前有哪些控制措施，是否有效；

——可能出现哪些事件和后果，如何、何时、何地、何出现；

——过去发生了什么，以及这可能与未来有何关系；

——可能适用哪些人因和组织因素。

实地调查可能有助于识别风险来源，并对潜在的后果提出早期预警。

识别风险的输出结果可以记录成风险清单，并记录事件、原因和后果，或使用其他合适的格式加以记录。

无论使用何种技术方法，风险识别都可有条不紊地迭代进行，从而彻底、高效地识别风险。宜尽早识别风险，从而留出足够时间来采取行动。但是，在一些情况下，一些风险无法在风险评估的过程中识别。因此，宜建立一种机制，来获取新出现的风险并获得潜在成功或失败的预警信号。

识别风险的技术，见 B.2。

6.3.3 确定风险的来源、原因和驱动因素

通过识别风险的来源、原因和驱动因素，可以：

——帮助预测一个事件或后果的可能性；

——帮助识别有效的应对措施；

——帮助确定早期预警指标及其监测阈值；

——确定常见的风险原因，从而决定风险应对的优先级。

风险的来源包括有利或不利的事件、决策、行动和流程，以及已知存在但结果不确定的情况。4.1 中描述的所有形式的不确定性，都可能是风险的来源。

事件和后果可能存在多个原因或因果链条。

风险通常只能通过调整风险驱动因素来控制。它们影响风险暴露的状态和发展，并且经常影响多个风险。因此，风险驱动因素往往比单个风险来源需要更多和更密切的关注。

有关确定风险来源、原因和驱动因素的技术，见 B.3。

6.3.4 调查现存控制措施的有效性

风险受现有控制措施的总体有效性影响。可考虑控制措施的以下方面：

——控制措施旨在改变风险的机制；

——控制措施是否到位，是否能够按预期运行，并达到预期结果；

——控制设计或应用方式是否存在缺陷；

——控制措施是否存在有缺失；

——控制措施是单独起效，还是需要其他措施的配合；

——是否存在可以降低或消除控制有效性（包括共因失效故障）的因素、条件、漏洞或情况；

——控制措施是否会带来其他风险。

注：一个风险可能需要多个控制措施，而一个控制措施可能同时影响多个风险。

宜区分改变可能性，后果或两者的控制措施，以及改变利益相关者之间如何分担风险的控制措施。例如，保险和其他形式的风险融资，不会直接影响事件或其后果的可能性，但可以通过减少其程度或平滑现金流量，使特定利益相关者更容易容忍某些后果。

在风险分析过程中，对控制措施的实际效果和可靠性作出的任何假设都宜尽可能进行验证，特别要重视假定具有实质性改变效果的单个或组合控制措施。在这方面，宜考虑通过常规监控和检查控制措施的手段得到的信息。

分析控制措施的技术，见 B.4。

6.3.5 理解后果和可能性

6.3.5.1 分析后果的类型、程度和出现的时机

后果分析可以从结果的描述，到详细的定量建模或脆弱性分析。在相关的情况下，宜考虑一种后果导致另一种后果的连续效应（多米诺骨牌或连锁反应）。

风险可能与多种不同类型的后果相关，影响多个不同目标。在进行风险评估的计划时，可确定拟分析的后果的类型。宜检查背景情况说明，保证拟分析的后果类型与风险评估的目的、决策等相符。在评估期间，获得更多信息后，可以回顾背景情况说明。

后果的程度可以定量地表示为点值或分布。在下列情况下，可以用分布来表示：

——后果的值不确定；

——后果因情况而异；

——影响后果的参数各不相同。

考虑一个后果的完整分布，有助于获得完整的信息。可以以点值的形式总结分布，例如期望值（平均）、变化（方差）、尾部或者分布的其他相关部分（百分位数）的百分比。

对于任何获取一个或多个点值来表示后果分布的方法，存在下列假设和不确定性：

——选择适合数据的分布类型（例如连续或离散，正态或高度偏态）；

——将该分布表示为点值的最适合的方式；

——由于产生分布的数据中固有的不确定性，而产生的点估计值。

不宜假设与风险相关的数据一定是正态分布。

在某些情况下，信息可以概括为定性或半定量排序，可用于比较风险。

后果的程度也可能因其他参数而异。例如，暴露于化学品的健康后果，通常取决于人或其他物种暴露的剂量。对于这个例子，风险通常由剂量反应曲线表示，该曲线描绘了指定终点（例如死亡）作为短期或累积剂量的函数的概率。

后果也可能随着时间改变。例如，故障存在的时间越长，其严重性可能越高。可选用合适的技术来考虑这一点。

有时，后果来自多种风险来源：例如，环境或人身健康受到生物、化学、物理和社会心理等风险源的影响。在考虑多重暴露时，宜考虑协同效应的可能性以及暴露持续时间和程度的影响。

6.3.5.2 分析可能性

可能性指事件的可能性或指定结果的可能性。宜明确说明可能性对应的参数，并清晰和准确定义

被陈述可能性的事件或后果。为了充分确定可能性，可能需要包含关于暴露和持续时间的陈述。

可能性可用多种方式进行描述，包括预期的概率、频率、或者使用描述性文字（例如，“可能性较高”）。在使用描述性文字时，描述的意思宜明确。可能性可能存在不确定性，可以表示为将发生特定值的信念程度的值的分布。

如果使用百分比作为可能性的度量，则可说明适用百分比的比率的性质。

示例 1：供应商未能交付的可能性为 5%。这一陈述在时间段和群体两个方面都很模糊。此外，百分比所指代的是 5%的项目还是 5%的供应商，此处也并不清楚。清晰的陈述是“一个或多个供应商在项目生命周期内未能向项目提供所需商品或服务的概率是项目的 5%”。

为了在定性或定量表达可能性时尽量减少误解，有关时间段和群体宜明确，并与特定评估的范围一致。

示例 2：在接下来两个月中，一个或多个供应商未能向交付所需产品或服务的概率是 1%的项目；而在未来六个月中，该概率是 3%的项目。

有许多可能的偏见会影响可能性的估计。此外，可能性估计的解释可根据其背景或环境而变化。宜注意了解个人（认知）和文化偏见的可能影响。

有关理解后果和可能性的技术，见 B.5。

6.3.6 分析相互和依赖关系

风险之间往往存在多种相互和依赖关系。例如，单一原因可能造成多个后果，一个后果可能有多个原因。某些风险的发生可能或多或少地导致其他风险的发生，并且这些因果关系可能形成级联或循环。

在风险之间的因果关系较为突出时，为了得到更可靠的风险分析结果，创建一个因果模型，以某种形式将所有风险都纳入其中是有用的。可以在这些风险信息中发现相同之处，例如，相同的风险起因、相同的驱动因素、相同的后果。

风险之间的相互关系可能对决策造成一系列影响。例如，提高跨越多个相关风险的活动的重要性，或增加一个选项对其他选项的吸引力。风险可能会受到共同应对措施的影响，在某些情况下，宜对某个风险的措施，会对其他风险造成正面或负面的影响。有时可以整合风险应对措施，从而显著减少工作量、更有效地平衡现有资源。在整合应对计划时，宜考虑到上述因素，而不是假设单独应对每个风险。

相互和依赖关系的分析技术，见 B.6。

6.3.7 理解风险度量

6.3.7.1 确定风险度量

在某些情况下，为潜在后果的大小和这些后果的可能性的某种组合，提供一种风险度量是有用的。度量可以是定性、半定量或定量的。

——定性方法往往是基于后果和可能性的描述（类别）或排序（顺序）量表。

——半定量方法包括：

- 一个参数（一般是可能性）为定量描述，另一个参数使用排序量表进行描述；
- 量表被分割为不连续的段，其边界为定量描述。量表中的点往往与数据存在对数关系；
- 数字描述被添加到量表的边界点，其含义被定性描述。

如果不能仔细解释计算的基础，则使用半定量量表可能造成误解。因此，宜验证半定量方法并谨慎使用。

——在定量方法中，后果和可能性以数值（比率）量表的形式表示。如果对一个风险加以定量分析，可在评估过程中持续使用合适的度量单位和维度。

定性和半定量技术，只能用于将风险与使用相同方法度量或使用相同准则的其他风险进行比较。定性和半定量度量不能直接用于汇总或累积风险。并且在存在正面和负面后果，或在风险之间进行权衡的情况下很难使用。

当把后果的定量估计及其可能性作为一个简单的乘积进行组合，以提供风险的大小时，信息可能会丢失。特别是，导致高后果和低可能性的风险，与经常发生的后果低的风险之间没有区别。为了弥补信息损失，可以对结果或可能性进行加权，但此法宜谨慎使用。

使用代表某一特定后果可能性的单个值，不能充分描述或估计风险。此类情况的例子有：

——风险后果最好表示为后果的概率分布；

——一个事件有多个原因，并带来一系列的结果和可能的连锁效应；

——持续暴露于风险源会累积后果；

——风险来源（如系统性问题）是可以识别的，但很难具体说明可能出现的后果的性质和可能性。（在这种情况下，根据可能性和后果估计风险的有效范围变得不可能）。

如果一项风险分布着多种可能的后果，可以将后果的概率加权平均（即预期值）作为风险度量。但此举并不一定可行，因为该度量反映的是该分布的平均结果。这导致了不太可能产生严重后果的信息的丢失，因此对于理解风险很重要。处理极端值的技术不包括在本文件中。

注：期望的数值或期望值，相当于将一个分布中所有结果/可能性求和，相当于使用该分布的平均后果。

对风险程度的量化度量举例如下：

——预期发生某项特定后果的频率，例如，某个地区每 1 000 km 行程发生车辆事故的数量；

——关注事件发生的预期间隔时间，例如，某个物品的平均启动时间；

——某个特定的终点在规定的暴露时间段内出现的概率（与后果随着暴露时长积累相关），例如，由于暴露于特定剂量的化学品而在一生中患癌症的概率；

——预期值，例如在投资周期内的预期回报或经济收益，或者以调整残疾生命年计算的每百万人每年的预期公共卫生负担；

——表示后果分布形状的统计数据，例如，某项投资回报的方差或波动；

——后果分布中指定百分位数或以上或以下的值；

示例：某个项目实现利润的概率是 90%；投资组合的风险值（VaR），用于衡量在指定时间段内，以指定概率在投资组合中可能出现的损失；

——与后果分布相关的极端度量，例如，预期的最大后果。

基于后果的度量指标，如最大可信损失或可能的最大损失，主要用于难以确定哪些控制可能失败，或者没有足够的数据来估计可能性。

风险程度依赖于对相关控制措施是否存在、是否有效的假设。固有风险或累积风险（假设可能出错的控制措施实际出错的情况下）、剩余风险或净风险（假设控制措施正常运行的情况），这些是从业者经常使用的术语。但是，很难明确定义这些术语，因此建议始终明确说明有关控制措施的假设。

在定性或定量报告风险程度时，可描述与假设以及输入和输出参数相关的不确定性。

6.3.7.2 累积风险度量

在某些情况下（例如资本分配），将一组风险的值，组合以产生单个值可能是有用的。如果风险只导致单一后果，并使用同样的单位（例如，货币价值）描述，那么原则上可以合并。换言之，只有在定量说明后果和可能性并且单位一致和正确时，它们才能合并。在一些情况下，可以使用效用度量作为统一量表，对使用不同单位的后果进行量化和合并。

将一系列复杂的风险合并成一个累积值，这种做法会丢失单个风险的信息。此外，除非十分小心，否则该累积值可能不准确，甚至造成误导。所有将多个风险整合为单一值的做法，都有相应的假设条件，宜先理解这些假设条件再进行整合。宜分析数据，了解可能影响风险整合的相关性和依赖性。用于产生总体风险水平的建模技术宜得到情景分析和压力测试的支持。

如果模型包含分布的计算，则宜以适当的方式纳入这些分布之间的相关性。如果相关性没有得到适当的考虑，结果将是不准确的，可能会严重误导。通过简单相加的方式来累积风险，得出的结果不能

作为决策的可靠依据，并且会带来负面结果。可以通过蒙特卡罗模拟来累积分布（见 B.5.10）。

定性或半定量的风险度量不能直接累积。同样，基于风险水平变化的定性或半定量度量，只能对控制的相对有效性做出一般的定性陈述。

不同风险的相关数据可以通过多种方式进行汇总，来帮助决策者。可以根据专家意见进行定性汇总，在此过程中，可考虑更详细的风险信息。在进行风险的定性汇总时，使用的假设和信息都宜明确阐述。

6.3.7.3 社会风险

当人群暴露于风险中时，一般来说，如果将个体面临的风险程度，简单地乘以暴露人群的数量，这样的累积数据不足以表示后果的真实影响。例如，在发生溃坝事故时，一个个体的死亡风险和一群人的整体风险，其考虑方式是不同的。

一般情况下，可以通过一个后果发生的频率（F）和承受该后果的人数（N）之间的关系来表示和评价社会风险（见 B.8.3）。

风险度量的技术，见 B.7。

6.4 检查分析结果

6.4.1 核查和验证分析结果

在可行的情况下，可核查和验证分析结果。核查是指检查是否正确完成分析。验证是指检查是否执行了正确的分析以实现预期的目标。在某些情况下，可执行独立的检查流程，以完成核查和验证。

验证可能包括：

——检查分析的范围是否符合既定目标；

——检查所有的关键假设，确保根据已有信息，这些关键假设是可信的；

——检查是否使用了合适的方法、模型和数据；

——使用多种方法、近似值、敏感性分析来测试和验证结论。

核查可能包括：

——检查数学运算和计算的正确性；

——检查分析结果是否对数据或结果的显示或呈现方式不敏感；

——将分析结果与存在数据的历史经验进行比较，或与发生后的结果进行比较；

——确定分析结果是否对数据或结果的显示或呈现方式敏感，并确定对评估结果有重大影响的输入参数；

——将分析结果与历史经验或未来的实际结果进行对比，包括随时间推移明确获得的反馈。

6.4.2 不确定性和敏感度分析

风险分析人员可了解分析中的不确定性，并了解其对结果可靠性的影响。宜与决策者沟通这些不确定性及其影响。

由于下列原因，风险分析的输出中可能出现的不确定性：

——分析的系统存在可变性；

——数据来源不可靠、不一致、不充分。例如，收集的数据类型或收集方法发生了改变；

——可能存在歧义，如定性词语的描述或理解方式；

——分析方法不能充分代表系统的复杂性；

——高度依赖人的专家意见或判断；

——相关数据可能不存在或组织可能未收集所需数据；

——由于背景或实际情况发生改变，以往数据不足以支持对未来进行可靠的预测；

——所做的假设存在不确定性或近似值。

如果在分析过程中发现缺少可靠的数据，则宜在可行的情况下收集进一步的数据。这可能涉及实施新的监控安排。或者，可调整分析过程以考虑数据限制。

可以执行敏感性分析，评价分析数据和假设条件中的不确定性的显著性。在进行敏感性分析时，可确认由于个别输入参数改变而对最终结果造成的相对改变。该项分析用于了解哪些数据必须保证准确、而哪些数据的敏感性较低因而对整体准确性的影响较小。经分析发现敏感性较高的参数以及该参数的敏感度宜恰当陈述。

对于风险评估有关键作用和可能发生变化的参数，宜持续监控，以便更新风险评估，并在必要时重新决策。

6.4.3 监督和检查

在下列情况下，宜进行监督：

——将实际结果和风险评估的预测结果进行比较，据此优化未来的评估工作；

——寻找在评估中识别出的潜在后果的先兆或预警指标；

——收集深入理解风险所需的数据；

——检查发现需要更新风险评估的新风险和意外改变。

如果在敏感性分析中发现一些参数对分析结果尤为重要，则宜考虑进行监控。

宜定期检查风险评估过程，从而发现是否出现了改变，包括背景和假设的改变、或者是否有新的信息或新方法可用。

6.5 使用评估结果支持决策

6.5.1 概述

风险分析的结果为所需作出的决策和采取的行动提供了输入。

注：即使没有遵循明确的决策程序，对风险的理解也可以为行动提供信息。

在制定决策时要考虑的因素和任何具体准则，都宜被确定为建立评估背景的一部分（见 6.1.6）。

可区分下列两种决策类型：

——对风险重要性、以及是否采取风险应对措施和如何应对风险的决策；

——对含有不确定性的多个选项进行对比的决策（例如，在多个机会中选择一个）。

6.5.2 针对风险重要性的决策

从风险识别和分析中得到的信息，可用于决定风险是否可接受，以及风险相对于组织目标和业绩阈值的重要性。这些信息是对于风险是否可接受、是否需要应对、应对优先等级等决策的输入。

一些风险可能在有限时间内可接受（例如，留出时间等待实施应对措施）。评估者宜清晰了解暂时接受风险的机制，以及后期复议的流程。

往往基于风险程度，来确定风险应对、监控、详细分析等的优先级。风险程度的数据来自典型后果及其概率的综合数据，且通过后果/可能性矩阵进行展示（见 B.10.3）。这一方法有一定局限性（见 B.10.3.5 和 6.3.7.1）。在决定优先级时，风险程度之外的下列要素也可考虑：

——与风险相关的其他度量，例如，控制措施的最大或预期后果，以及控制措施的有效性；

——事件及其可能后果的定性特征；

——利益相关者的观点和感知；

——与获得的改善相比，进一步风险应对的成本和可行性；

——风险之间的相互关系，包括应对措施对其他风险的作用。

一旦评价了风险并确定了应对措施，就可以重复实施风险评估过程，以检查拟议的应对措施是否产

生额外的负面风险，以及经应对后剩余的风险，是否在组织的风险偏好之内。

评价风险重要性的技术，见 B.8。

6.5.3 选择选项的决策

选择选项的决策，一般涉及权衡各个选项潜在的优缺点，并考虑下列不确定性：

——与选项的潜在结果、成本和收益估计等相关的不确定性；

——可能影响结果的潜在事件和事态发展；

——不同利益相关者对待成本和收益的不同价值观；

——根据风险分析的输出所做判断的不确定性，包括考虑诸如目标和准则未来是否将维持不变。

这种类型的决策，通常是根据对相关选项和与之相关风险分析的理解，使用专家判断作出的，并考虑到：

——在相互冲突的目标之间进行取舍；

——组织的风险偏好；

——利益相关者的不同态度和信念。

用于对比含有不确定性的选项的技术，见 B.9。

6.6 记录和报告风险评估过程及结果

风险评估的结果、所使用的方法、假设条件的基本依据以及其他建议都宜妥善记录。并就需要传达的信息和传达给谁作出决定。宜明确检查和更新记录的方法。

记录的目的是：

——与决策者和包括监管方在内的其他利益相关者传达风险信息；

——对所做决策的基本原理提供记录和证明；

——保留评估结果，以备未来使用和参考；

——跟踪绩效和趋势；

——确保风险得到理解和恰当的管理；

——支持对评估的验证；

——提供审计记录。

任何文件和记录宜及时提供，并且其形式宜便于阅读者理解。文件还可为验证提供必要的技术深度，并记录足够的细节以备未来使用。文件和记录中的信息，宜足以支持接下来对流程和流程结果进行检查和验证。假设条件、数据和方法的局限性、提出建议的原因等，都宜清晰记录。

风险宜以便理解的术语描述，用于表示定量度量的单位宜明确且正确。

提交风险评估结果的人员，宜重点说明其个人或其团队对结果的准确度和完整性的信心。可充分沟通说明不确定性，以确保报告所表达的确定性不会高于实际。

有关用于记录和报告的技术，详见 B.10。

7 选择风险评估技术

7.1 概述

本章描述了为特定目的选择一种或多种技术时可考虑的因素。附录 A 和附录 B 列出并进一步解释了一些常用技术。它们描述了每种技术的特点及其可能的应用范围，以及其固有的优缺点。

本文件中描述的很多技术，原本是由某些行业开发，用于管理某些类别的负面结果。有几项技术是相似的，但使用了不同的术语，这反映了这些技术在不同行业中为了类似的目的而独立开发的过程。随着时间的推移，很多技术的应用范围扩大了，例如，从技术工程领域应用扩大到金融或管理领域，或者可以同时兼顾正面和负面结果。新技术已经出现，而旧技术则适应了新的场景。这些技术及其应用场景不断演变。将这些技术用于其原始设计范围之外的场景，可以增强人们对风险的理解。附录 A 和附录 B 说明了可用于确定技术的应用场景的技术特征。

7.2 选择技术

对于技术的选择和应用方式，宜根据具体的背景环境和用途决定，并且以利益相关者需要的类型和形式提供信息。总体来说，所选技术方法的数量和类型，宜与决策的重要程度相符，并考虑时间和其他资源的限制以及机会成本。

在选择定性技术或定量技术时，可考虑的主要准则是利益相关者最方便使用的输出形式，以及数据的可获得性和可靠性。如果定量技术要提供有意义的结果，通常需要高质量的数据。在数据不足的情况下，虽然定量技术的计算结果可能存在不确定，但它对数据的严格要求能提高人们对风险的理解。

在选择技术时，往往会考虑既定环境。可能需要选择多个技术，使用多个技术有时能够帮助加深理解。随着更多信息可用，可以采用不同的技术。

在选择一个或多个技术时，宜考虑下列要素：

——评估的目的；

——利益相关者的需求；

——法律、监管、合同要求；

——运行环境和场景；

——决策的重要性(例如，决策失误的后果)；

——既定决策准则及其形式；

——在决策的最后期限前的剩余时间；

——现有信息和可获得信息；

——情况的复杂程度；

——可用或可获得的专业知识。

表 A.1 中列出了与上述要求相关的技术特征。表 A.2 提供了根据这些特征分类的技术列表。

随着背景环境的不确定性、复杂性和模糊性增加，咨询更多利益相关者的需求也会增加，这将对所选技术的组合产生影响。

注：例如，IEC TR 63039:2016[50]指导人们将 ETA、FTA，以及马尔可夫技术配合使用，从而高效完成对复杂系统的风险分析。

本文件中描述的一些技术不仅可以用于风险分析，还可以用于 ISO 31000 风险管理过程中的一些步骤。这些技术在风险管理过程中的应用如图 A.1 所示。表 A.3 说明了其在评估中的具体应用。

附录 B 综述了各种技术、用途、输入和输出条件、优势和局限，并在适用的情况下，提供了参考，以了解更多细节。该附录根据技术在风险评估过程中的主要用途进行分类，具体包括：

——从利益相关者和专家处获取意见(B.1)；

——识别风险(B.2)；

——确认风险的来源、原因和驱动因素(B.3)；

——分析现有的控制措施(B.4)；

——理解后果和可能性(B.5)；

——分析依赖关系和相互作用(B.6)；

——提供风险度量(B.7)；

——评价风险的重要性(B.8)；

——选择备选项(B.9)；

——记录和报告(B.10)。

在每个类别内，技术的顺序是按照字母表安排的，并不代表其重要性。

附件 B 中是大部分技术，都假设可以识别风险及其来源。同时，也有一些技术可以通过分析现有的控制措施和需求，间接评估剩余风险(例如，IEC 61508 [36])。

虽然本文件讨论并提供了示例技术，但所描述的技术并非详尽无遗，对于任何给定技术在任何给定情况下的有效性，没有提出任何建议。在选择任何技术时都宜小心，以确保其在给定环境中是适当、可靠和有效的。

附 录 A
（资料性）
技 术 分 类

A.1 技术分类简介

表 A.1 解释了可选择使用的一种或多种技术的技术特征。

表 A.1 技术特征

特征	描述	详细信息(例如,功能指标)
应用	该技术如何用于风险评估(参见 B.1 至 B.10 的标题)	引出观点、识别、分析原因、分析控制措施等
范围	适用于组织层面、部门或项目层面、单个流程或设备层面的风险	组织(组织) 项目/部门(部门) 设备/流程(设备/流程)
时间范围	着眼于短期、中期或长期风险,或适用于任何时间范围	短;中;长;任何
决策层级	适用于战略、战术或运营层级的风险	战略(1),战术(2),运营(3)
起始信息/数据需求	所需起始信息或数据的需求	高,中,低
专业知识	正确使用所需的专业知识水平	低:直觉或一到两天的培训 中:两天以上的培训课程 高:需要大量培训或专业知识
定性-定量	该方法是否是定性、半定量或定量	定量(quant) 定性(qual) 半定量(semi-quant) 可用于定性或定量(两者之一)
应用所需资源	应用技术所需的时间和成本	高,中,低

A.2 技术分类的应用

表 A.2 列出了根据这些特征分类的一系列技术。所描述的技术代表了研究手头问题的结构化方法;事实表明,这些方法在特定环境中有用。该列表的目的不在于全面,而是涵盖了一系列来自各个领域的常用技术。为简单起见,这些技术按字母顺序列出,没有任何优先级。

每种技术在附录 B 中有更详细描述,参见表 A.2 第 1 列。

表 A.2　技术和指标性特征

条款号	技术	描述	应用	范围	时间范围	决策层级	起始信息/数据需求	专业知识	定性/定量/半定量	应用所需资源
B.8.2	ALARP/SFAIRP	确定风险重要性的准则和评价风险承受能力的准则	评价风险	1	任何	1/2	高	高	定性/定量	高
B.5.2	贝叶斯分析	一种利用贝叶斯定理推断模型参数的方法，该定理能够将经验数据纳入对概率的先验判断	分析可能性	任何	任何	任何	中	高	定量	中
B.5.3	贝叶斯网络/影响图	使用概率表示的变量及其因果关系的图形模型。基本贝叶斯网络具有表示不确定性的变量。称为影响图扩展版本包括代表不确定性的变量、后果和行动	识别风险评估风险在选项之间作出决定	任何	任何	任何	中	高	定量	中/高
B.4.2	蝶形图分析	用来描述并分析某个风险从原因到结果的路径以及审查控制措施的图解方式	分析风险分析控制措施描述风险	2/3	短/中	任何	低	低/中	定性/半定量	低
B.1.2	头脑风暴	以讨论小组的方式鼓励思维的碰撞	引出观点	任何	任何	任何	无	低/中	定量	低
B.5.4	业务影响分析	BIA 流程分析破坏性事件对组织的影响，这确定了组织产品和服务的恢复优先级，进而确定活动以及提供这些活动的资源的优先级	分析结果分析控制措施	1	短/中	2	中	低	定量/定性	中
B.6.1	因果图	表示事件、原因和影响及其关系的网络图	分析原因	2/3	任何	2/3	中	中	定量	中
B.2.2	检查表、分层分类法	基于经验或基于可用于帮助识别风险或控制措施的概念和模型的列表	识别风险或控制措施	2/3	任何	任何	开发需求高，使用需求低	低/中	定性	低/中
B.3.2	辛迪尼克方法(cindynic)	考虑利益相关者的目标、价值观、规则、数据和模型，识别不一致、模糊、遗漏和疏忽。这些构成风险的系统性来源和驱动因素	识别风险驱动因素	1/2	短或中	1	低	中	定性	高

表 A.2　技术和指标性特征（续）

条款号	技术	描述	应用	范围	时间范围	决策层级	起始信息/数据需求	专业知识	定性/定量/半定量	应用所需资源
B.7.3	条件风险价值（CVaR）	也称为损失期望值（ES），是衡量金融投资组合在最差情况下的预期损失的指标	风险度量	任何	短/中	3	高	高	定量	中
B.10.3	后果/可能性矩阵	通过选择结果/可能性因素，并将它们显示在矩阵上来比较单个风险，其中一个轴是结果，另一个轴是可能性	报告风险；评估	任何	任何	任何	中	使用要求低，开发要求中等	定性/半定量/定量	低
B.9.2	成本-效益分析	用金钱作为衡量正面和负面、有形和无形的后果的尺度	对选项作比较	任何	短/中	任何	中/高	中/高	定量	中/高
B.6.2	交叉影响分析	评估一组给定事件的发生概率随其中一个事件的实际发生而发生的变化	分析可能性和原因	任何	短/中	任何	从低到高	中/高	定量	中/高
B.9.3	决策树分析	使用树状的显示或决策模型及其可能的后果；结果通常以金钱或效用来衡量决策树的另一种表示是影响图（见 B.5.3）	对选项作比较	任何	任何	2	低/中	中	定量	中
B.1.3	德尔菲技术	通过一组问卷收集判断；人们专家单独、匿名表达各自的观点，收集意见，整理并共享	引出观点	任何	任何	任何	无	中	定量	中
B.5.6	事件树分析（ETA）	对给定初始事件的可能结果和控制状态进行建模，从而分析各种可能结果的频率或概率	分析结果和控制措施	2/3	任何	任何	低/中	中	定性/定量	中
B.5.7	故障树分析（FTA）	使用布尔（Boolean）逻辑分析焦点事件的原因，描述故障组合。变化的方面是，包括需要顶部事件的成功树和用于历史事件的原因树	分析可能性分析原因	2/3	中	2/3	用于定量分析的需求高	取决于复杂性	定性/定量	中/高

表 A.2　技术和指标性特征（续）

条款号	技术	描述	应用	范围	时间范围	决策层级	起始信息/数据需求	专业知识	定性/定量/半定量	应用所需资源
B.2.3	故障模式和影响（和临界）分析 FME(C)A	考虑系统的每个组件可能发生故障的方式以及故障原因和影响。实施 FMEA 后，可进行关键性分析，定义每种故障模式的重要性（FMECA）	识别风险	2/3	任何	2/3	取决于应用	中	定性/半定量/定量	低/高
B.8.3	频率/数量（F/N）图	使用定量后果/可能性图来考虑人类生命风险的承受度的特定情形	评估风险	1	任何	任何	高	高	定量	高
B.9.4	博弈论	研究战略决策制定，模拟参与博弈的不同参与者决策的相互影响。基于风险的定价可作为应用领域的示例	在选项之间作出决定	1	中	1/2	高	高	定量	中/高
B.4.3	危害分析和关键控制点法（HACCP）	分析各不同保护层可实现的风险降低程度	分析控制措施监测	2/3	短/中	2/3	中	中	定量	中
B.2.4	危险和可操作性分析（HAZOP）	对计划的或现有的流程或操作进行结构化和系统检查，识别和评估可能对人员或设备造成风险或妨碍高效运行的问题	识别和分析风险	3	中/长	2/3	中	人：高；参与者：中	定性	中/高
B.5.8	人因可靠性分析（HRA）	可以用来评估人为错误对系统的影响的技术	分析风险和风险来源	2/3	任何	2/3	中	高	定性/定量	中到高
B.1.5	采访	结构化或半结构化的一对一对话以引出观点	征求观点	任何	任何	任何	无	中	定性	高
B.3.3	石川分析（鱼骨图）	识别对已定义结果（想要的或不想要的）的促成因素。促成因素通常划分为预先定义的类别，并以树状结构或鱼骨图的形式显示	分析风险来源	任何	任何	任何	低	低/中	定量	低

表 A.2　技术和指标性特征（续）

条款号	技术	描述	应用	范围	时间范围	决策层级	起始信息/数据需求	专业知识	定性/定量/半定量	应用所需资源
B.4.4	保护层分析法（LOPA）	分析各不同保护层可实现的风险降低程度	分析控制措施	3	任何	2/3	中	中/高	定性/定量	中/高
B.5.9	马尔可夫分析	计算有能力处于多种状态之一的系统在未来时间 t 处于特定状态的概率	分析可能性	3	任何	2/3	中/高	高	定量	中
B.5.10	蒙特卡罗分析	通过使用随机变量运行多个模拟来计算结果的概率	分析可能性	任何	任何	任何	中	高	定量	中/高
B.9.5	多标准分析（MCA）	以明确权衡的方式比较选项；提供成本/收益分析的替代方案，不需要为所有投入匹配货币值	在选项之间作出决定	任何	任何	任何	低	中	定量	低/中
B.1.4	名义小组技术	通过征求尚未互动交流的小组成员的意见，然后进行小组讨论	引出观点	任何	任何	任何	无	低	定量	中
B.8.4	帕累托图	帕累托原则（80-20 法则）指出，对于许多事件，大约 80％的结果来自 20％的原因	设定优先级	任何	任何	任何	中	缓	半定量/定量	低
B.5.11	（PIA/DPIA）隐私影响分析/数据保护影响分析	分析事件和活动如何影响个人隐私（PI），确定并量化管理它所需的能力	分析风险源头后果分析	任何	任何	1/2	中	中/高	定量	中
B.8.5	以可靠性为中心的维修（RCM）	一种用于确定系统及其组件的预防性维修需求的风险评估方法	评估风险决定控制措施	2/3	中	2/3	中	对人要求高；使用要求中等	定性/半定量/定量	中/高
B.8.6	风险指数	根据应用于被认为会影响风险大小的因素的评级，对风险的重要性进行评级	对风险进行比较	任何	任何	任何	中	使用要求低，开发要求中等	半定量	低
B.10.2	风险登记表	一种记录风险信息和跟踪行动的方法	记录和报告风险；监测和审查	任何	任何	任何	低/中	低/中	质量	中

表 A.2　技术和指标性特征（续）

条款号	技术	描述	应用	范围	时间范围	决策层级	起始信息/数据需求	专业知识	定性/定量/半定量	应用所需资源
B.10.4	S 曲线	一种显示后果及其可能性之间关系的方法，绘制为累积分布函数(S 曲线)	显示风险评估风险	任何	任何	2/3	中/高	中/高	定量/半定量	中
B.2.5	情景分析	在想象和建模推测的基础上，对可能发生的未来情景加以描述。然后考虑这些情景中的每一个风险	识别风险；后果；分析	任何	中或长	任何	低/中	中	定量	低/中
B.1.6	调查	基于纸质或计算机的问卷调查，旨在征求观点。来得出结论	征求观点	任何	中/长	2/3	低	中	定量	高
B.2.6	结构化假设分析技术(SWIFT)	比 HAZOP 更简单的替代性方法，进行“假设”提示，识别与预期的偏差。运用的一系列“提示”词或短语来激发参与者识别风险	识别风险	1/2	中/长	1/2	中	低/中	定量	低/中
B.7.1	毒理学风险评估	为衡量因接触化学品而对人类或生态系统造成的风险而采取的一系列步骤	风险度量	3	中/长	2/3	高	高	定量	高
B.7.2	风险价值(VaR)	一种风险财务度量，在稳定的市场条件下使用假定的损失概率分布，计算在定义的时间跨度内以特定概率发生的损失的价值。在未来特定的一段时间内的最大可能损失	风险度量	任何	短/中	3	高	高	定量	中

A.3　ISO 31000 过程中技术的使用

表 A.3 列出了每种技术适用于风险评估不同阶段的程度：即，风险识、风险分析和风险评估。一些技术也用于整个过程的其他步骤，见图 A.1。

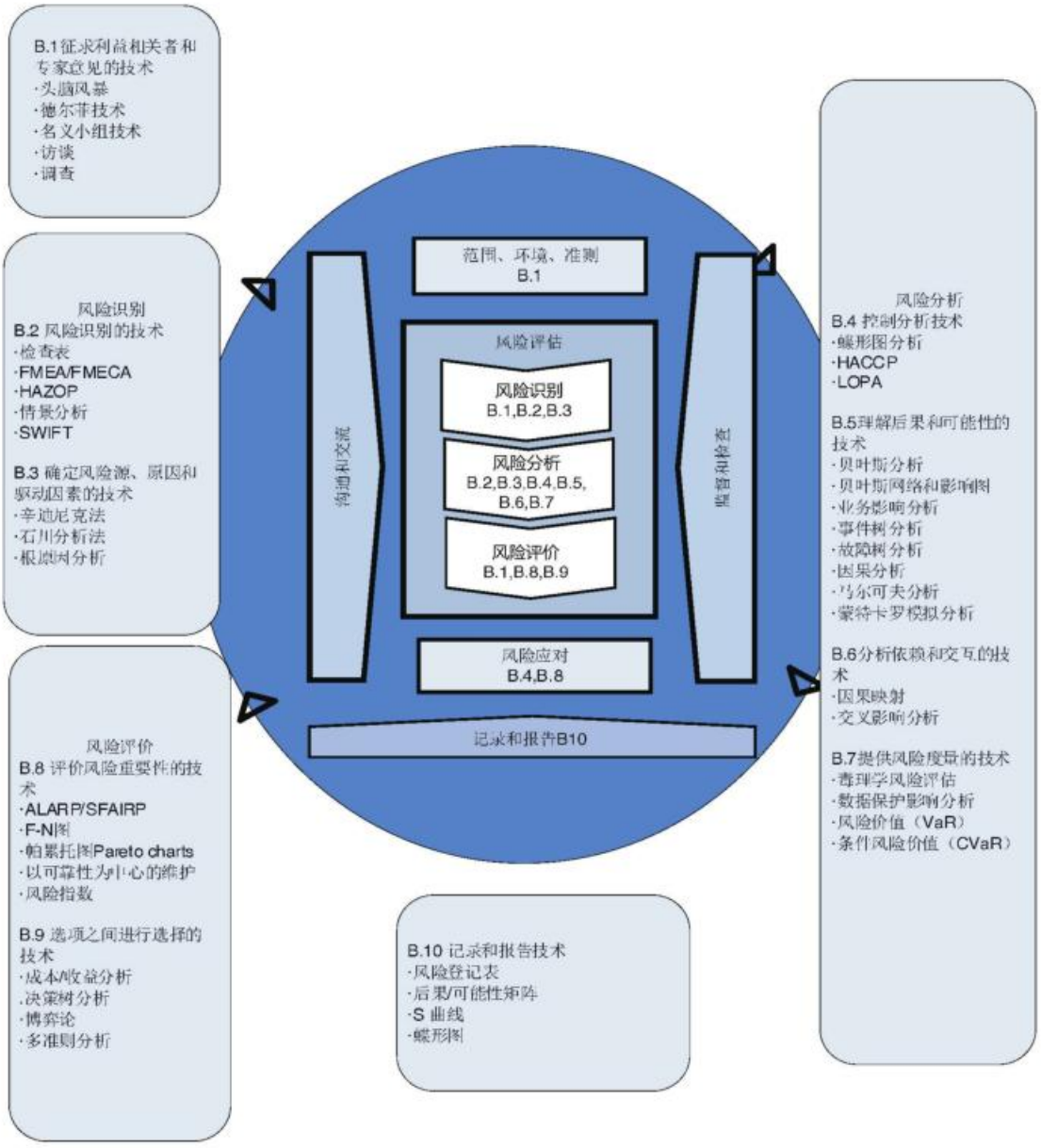

图 A.1　ISO 31000 风险管理过程中的技术应用

注：图 A.1 旨在提供一个概述，并不是在每个步骤中均可以使用列表的所有技术。

表 A.3　技术对 ISO 31000 流程的适用性

工具和技术	风险评估流程					条款号
	风险识别	风险分析			风险评价	
		结果	可能性	风险等级		
ALAR，PALARA 和 SFAIRP	NA	NA	NA	NA	SA	B.8.2
贝叶斯分析	NA	NA	SA	NA	NA	B.5.2
贝叶斯网络	NA	NA	SA	NA	SA	B.5.3

表 A.3　技术对 ISO 31000 流程的适用性（续）

工具和技术	风险评估流程					条款号
	风险识别	风险分析			风险评价	
		结果	可能性	风险等级		
蝶形图分析	A	SA	A	A	A	B.4.2
头脑风暴	SA	A	NA	NA	NA	B.1.2
业务影响分析	A	SA	NA	NA	NA	B.5.4
因果图	A	A	NA	NA	NA	B.6.1
因果分析	A	SA	SA	A	A	B.5.5
检查表、分层分类法	SA	NA	NA	NA	NA	B.2.2
辛迪尼克方法	SA	NA	NA	NA	NA	B.3.2
后果/可能性矩阵	NA	A	A	SA	A	B.10.3
成本-效益分析	NA	SA	NA	NA	SA	B.9.2
交叉影响分析	NA	NA	SA	NA	NA	B.6.2
决策树分析	NA	SA	SA	A	A	B.9.3
德尔菲技术	SA	NA	NA	NA	NA	B.1.3
事件树分析	NA	SA	A	A	A	B.5.6
故障模式和影响分析	SA	SA	NA	NA	NA	B.2.3
故障模式和影响以及危害性分析	SA	SA	SA	SA	SA	B.2.3
故障树分析	A	NA	SA	A	A	B.5.7
F-N 图	A	SA	SA	A	SA	B.8.3
博弈论	A	SA	NA	NA	SA	B.9.4
危害和可操作性研究(HAZOP)	SA	A	NA	NA	NA	B.2.4
危害分析和关键控制点法(HACCP)	SA	SA	NA	NA	SA	B.4.3
人因可靠性分析	SA	SA	SA	SA	A	B.5.8
石川分析(鱼骨图)	SA	A	NA	NA	NA	B.3.3
保护层分析（LOPA）	A	SA	A	A	NA	B.4.4
马尔可夫分析	A	A	SA	NA	NA	B.5.9
蒙特卡罗模拟	NA	A	A	A	SA	B.5.10
多标准分析（MCA）	A	NA	NA	NA	SA	B.9.5
名义小组技术	SA	A	A	NA	NA	B.1.4
帕累托图	NA	A	A	A	SA	B.8.4
隐私影响分析/数据隐私影响评估(PIA/DPIA)	A	SA	A	A	SA	B.5.11
以可靠性为中心的维护	A	A	A	A	SA	B.8.5
风险指数	NA	SA	SA	A	SA	B.8.6

表 A.3　技术对 ISO 31000 流程的适用性（续）

工具和技术	风险评估流程					条款号
	风险识别	风险分析			风险评价	
		结果	可能性	风险等级		
S 曲线	NA	A	A	SA	SA	B.10.4
情景分析	SA	SA	A	A	A	B.2.5
结构化或半结构化访谈	SA	NA	NA	NA	NA	B.1.5
结构化假设分析技术（SWIFT）	SA	SA	A	A	A	B.2.6
调查	SA	NA	NA	NA	NA	B.1.6
毒理学风险评估	SA	SA	SA	SA	SA	B.7.1
风险价值（VaR）	NA	A	A	SA	SA	B.7.2
A：适用；SA：非常适用；NA：不适用。						

附 录 B
（资料性）
技 术 说 明

B.1 征求利益相关者和专家意见的技术

B.1.1 概述

B.2～B.7 中描述的相关技术包括利益相关者和专家提供的意见，以及丰富的专业知识，并允许利益相关者参与。利益相关者和专家的意见包括信息披露、个人建议表达或创新想法，可采用访谈调研、头脑风暴法、名义小组法或德尔菲技术获得。B.1 描述了一些可用于引出信息或达成共识的技术。

在某些情况下，利益相关者具有特定的专业知识和角色，并且几乎没有意见分歧。有时利益相关者的观点可能会显著不同，并且可能会有权力结构和其他因素影响相互之间的互动方式，进而影响所用方法的选择。此外，需要咨询的利益相关者数量、时间限制以及同时召集所有必要人员的可行性也将会影响方法的选择。

当使用小组面对面的方法时，一位经验丰富且技术娴熟的负责人对于获得良好结果很重要。负责人或协调者的角色是：

——组织团队；

——在会议/合作前获取和共享相关信息和数据；

——为会议/合作准备有效的框架和形式；

——激发创造性思维，从而加强理解，激发想法；

——确保结果准确，尽可能没有偏差。

源自分层和分类法的检查表可用作该过程的一部分（见 B.2.2）。

任何依赖人们看法和观点而获取信息的方法都有可能不可靠，并且会受到各种主观因素的影响，例如可得性偏差（倾向于高估刚刚发生事情的可能性）、聚类错觉（倾向于高估大样本中小集群的重要性）或从众效应（因为其他人做或相信同样的事情，而倾向于做或相信某件事）。

EN12973[4]中给出了功能分析指南，可用于减少主观因素的影响，并将创造性思维集中在影响最大的方面。

对于作出判断或假设所依据的信息，宜进行汇报。

B.1.2 头脑风暴

B.1.2.1 概述

头脑风暴（Brainstorming）是一种激发和鼓励一群人生发出关于任何性质的一个或多个主题的想法的过程。“头脑风暴”这个词经常被宽泛地用来指任何类型的小组讨论，但有效的头脑风暴需要有意识地努力确保小组中其他人的想法被用作激发每个参与者创造力的工具。对想法的任何分析或批评要与头脑风暴分开进行。

当一位专家能够提供必要的刺激但不限制思考，这种情况下，运用该技术可获得最佳结果。支持人鼓励小组尽可能涵盖所有相关领域，并确保捕捉过程中的想法以供后续分析。

头脑风暴可以是结构化，也可以是非结构化的。对于结构化的头脑风暴，人将要讨论的问题分解为多个部分，并在其中一个主题穷尽时及时使用准备好的提示来激发关于新主题的想法。非结构化的头脑风暴通常不太正式。两种情况下，人都会开启一个思路，每个人都可产生自己的想法。保持步调一致，让想法激发横向思维。当一个思路已经用尽或讨论偏离太远时，协调人可以建议一个新的方向，或

者采用一个不同的创造性思维工具。目标是收集尽可能多的不同想法，以供后续分析。

实践表明，在实践中，团队产生的想法少于一个人单独工作时的想法。例如：

——在一个团队中，成员的想法趋同而非多样化；

——等待轮流发言时，时间的延迟往往会阻碍想法产生；

——成员在一个团队中往往心理上倾向于不够努力工作。

——可以通过以下方式减少这些趋势：

——为成员提供部分独自工作的机会；

——使团队多元化，不断更新团队成员；

——结合其他方法使用，如名义小组法(B.1.4)或电子头脑风暴等方法。这些方法鼓励更多个人参与，可以设置为匿名形式，从而避免个人政治和文化问题。

B.1.2.2 用途

头脑风暴法可以应用于组织的任何层级讨论中，用于识别不确定性、成功或失败的原因、后果、决策准则或应对方案。该方法可用于定量分析，采用结构化形式，确保充分考虑偏差，尤其在涉及所有利益相关者的情况下。

头脑风暴法可以激发创造力，在进行创新设计、创新性产品及创新性流程讨论时非常有效。

B.1.2.3 输入

头脑风暴法引导小组成员各抒己见，与其他方法相比，对数据或外部信息的需求较少。小组成员宜具备解决问题的专业知识、经验和观点，同时充分发挥头脑风暴法的作用需要经验熟练的人。

B.1.2.4 输出

输出是小组讨论时产生的所有想法以及想法呈现时形成的思路列表。

B.1.2.5 优势和局限

头脑风暴的优势包括：

——激发想象和创造，有助于识别新的风险和新的解决方案；

——在数据很少或没有数据，以及需要新技术或新解决方案的情况下，该方法很有用；

——主要利益相关者参与其中，有助于进行全面沟通；

——速度较快并易于开展。

局限性包括：

——很难证明小组讨论过程是全面的；

——与单独工作的个人相比，团队产生的想法更少；

——可能会出现特殊的小组状况，导致某些有重要观点的人保持沉默而其他人成为讨论的主角，这可以通过有效的引导来解决；

——鼓励创造性思维和新想法可能意味着讨论未专注于正在思考的问题，从而占用会议时间。

B.1.2.6 参考资料

[5] PROCTOR, A.(2009).Creative problem solving for managers

[6] GOLDENBERG, Olga, WILEY, Jennifer. Quality, conformity, and conflict: Questioning theassumptions of Osborn's brainstorming technique

B.1.3 德尔菲技术

B.1.3.1 概述

德尔菲技术(Delphi)是依据一套系统的程序在一组专家中取得可靠共识的方法。该方法通过调查问卷收集和整理对特定主题的判断方法。德尔菲法的一个基本特征是,随着过程的推进,专家们可以独立、匿名地表达他们的意见,同时可以获知其他专家的观点。

为专家组成员单独提供需要审议的一个或多个问题,通过让团队成员填写问卷,汇总意见,整理并共享,周而复始,最终获取共识。如果一名专家组成员或少数专家组成员始终维持各自答复,则可能表明他们持有重要观点或信息。

B.1.3.2 用途

德尔菲技术用于解决复杂的不确定性问题,其不确定性需要专家来判断。该方法可用于预测分析和政策制定,并用于达成共识或调解专家之间的分歧;可用于识别风险(正面和负面影响)、威胁和机遇,并就未来事件的可能性和后果达成共识;可应用于战略或战术层面;其最初应用是对长时间框架的预测,也可应用于任何时间框架。

B.1.3.3 输入

该方法依赖于参与者的知识以及在一定时间跨度内的持续合作,该时间跨度可以天、周、月甚至年为计算单位。

参与者的数量可以从几到几百人不等。问卷调查可以采用纸笔形式,也可以使用电子通信工具(包括电子邮件和互联网)分发和反馈。技术系统的使用有助于确保每个周期信息汇编的及时性和精确性。

B.1.3.4 输出

对审议中的事项达成共识。

B.1.3.5 优势和局限

优势包括:

——由于观点是匿名的,因此成员更有可能表达出那些不受欢迎的想法;

——所有观点都获得相同的重视,以避免某一权威占主导地位和话语权的问题;

——实现了对结果的共识;

——成员不必同时聚集在某个地方;

——成员有时间对问题做出深思熟虑的回答;

——该过程往往意味着专家将全部精力投入到任务上。

局限性包括:

——耗费时间和精力;

——参与者要能进行清晰的书面表达。

B.1.3.6 参考资料

[7] ROWE,G.WRIGHT,G.The Delphi technique: Past, present, and future prospects. Technological forecasting and social change 2011, 78, Special Delphi Issue

B.1.4 名义小组技术

B.1.4.1 概述

名义小组法(nominalgroup),如同头脑风暴法,旨在收集专家想法。首先在小组成员没有互动情况下,单独寻求个人意见,然后进行小组讨论。

过程如下:

——主持人向每个小组成员提供要考虑的问题。

——小组成员安静、独立地写下想法。

——在小组成员表达其想法的阶段,不进行讨论;如果小组讨论意味着某些意见比其他意见更有分量,则可匿名将想法传递给主持人,进而参与者可寻求进一步澄清。

——小组讨论想法,给出共识意见。

——小组成员对想法进行私下投票,并根据投票做出小组决策。

B.1.4.2 用途

名义小组法可以作为头脑风暴法的替代,也可用于确定小组内想法的优先级。

B.1.4.3 输入

参与者的想法和经验。

B.1.4.4 输出

根据需要提出想法、解决方案或决定。

B.1.4.5 优势和局限

名义小组法的优势包括:

——当团队中的某些成员比其他成员更有发言权时,其提供了比头脑风暴法更平衡的观点;

——如果所有或部分小组成员是团队的新成员,或者问题具有争议性,或者团队之间存在权力不平衡或冲突,通常会促使参与更平衡;

——结果表明其比头脑风暴法能产生更多想法;

——减少了小组的适应性压力;

——可以在相对较短时间内达成共识。

局限性包括:

——限制不同想法的相互激发;

——相同的想法可能会以很多不同方式呈现,难以整理。

B.1.4.6 参考资料

[8] MCDONALD,D,BAMMER,G,andDEANE,P,Research Integration Using DialogueMethods

注:本参考文献还提供了一系列其他方法的详细信息,其中一些也在本文档中进行了讨论。

B.1.5 结构化或半结构化访谈

B.1.5.1 概述

在结构化访谈(Structured Interviews)中,访谈者会依据事先准备好的提纲向访谈对象提问一系列准备好的问题,从而获取访谈对象对某问题的看法。半结构化访谈(Semi-structured Interviews)与结

构化访谈类似，但可进行更自由的对话，能够有更多机会涉及其专业领域，以探讨出现的问题。

问题应该是明确而简单的，利于访谈对象理解。也要准备可能的后续问题，用来补充说明该问题。为了保证访谈质量，问题应该只涉及一个主题。

问题应先由与访谈对象背景相似的人测试，以检查问题是否含糊不清，是否能被正确理解，答案是否涵盖了预期内容，应注意不要“诱导”访谈对象。

B.1.5.2 用途

结构化和半结构化访谈是一种从团队中的个人获取深入信息和意见的手段。如必要，访谈对象的回答可以保密。由于个人不会因团队其他成员的观点产生偏见，访谈可以提供深入信息。

如果很难将成员同时聚集在同一个地方，或者小组内难以进行自由的讨论活动时，则结构化和半结构化访谈就是一种有用的方法。与调查或研讨会相比，还可以在采访中获得更详细的信息。该方法可用于组织的任何级别。

B.1.5.3 输入

输入包括对所需问题的清晰理解，以及已被试点小组测试过的一组准备好的问题。

设计访谈问题需要技巧，以获取不受访谈对象自身偏见影响的良好且有效的答复。

B.1.5.4 输出

输出是访谈对象对于访谈主题的问题所形成的看法。

B.1.5.5 优势和局限

结构化采访的优势包括：

——可以使人们有时间专门考虑某个问题；

——相比小组讨论方式，一对一的沟通可以使双方有更多机会对某个问题进行深度思考；

——与面对面的小组讨论相比，结构化访谈可以让更多的利益相关者参与其中。

结构化采访的局限性包括：

——访谈的设计、反馈和分析非常耗时；

——需要具备一定专业知识设计问题，避免访谈对象对问题回复的偏见；

——访谈对象的观点可能会存有偏见，因其没有通过小组讨论加以消除；

——无法实现头脑风暴法的重要特征——激发想象力；

——半结构化采访中，访谈对象的回复会生成很多信息，可能难以将其明确地归类到易于分析的某种形式。

B.1.5.6 参考资料

[9] HARRELL，M.C. BRADLEY，M.A. 2009，Data collection methods-A training Manual-Semi structured interviews and focus groups

[10] GILL，J.JOHNSON，P.2010，Research methods for managers

B.1.6 调查法

B.1.6.1 概述

调查法通常比访谈涉及更多人，会提出更多限制性问题。调查采用电子或纸质问卷形式，问题通常提供是或否答案、评分量表选择或多项选择。调查针对结果进行统计分析，是这种方法的重要特征。调

查可包括主观问答题，由于分析困难，其数量受到限制。

B.1.6.2 用途

调查法对于在大范围内咨询利益相关者是有效的，特别是大量人员所需提供的信息相对较少时。

B.1.6.3 输入

将预先完成测试、明确的问题发送给愿意参与调查的具有广泛代表性的样本人员。宜具备专业知识设计调查问卷，从而获取有效结果，进而对其进行统计分析。宜有足够的调查问卷返回数量，以便提供有效的统计。（调查问卷返回数量通常很低，意味着需要发放很多问卷。）

B.1.6.4 输出

输出是对来自大量个人观点的分析，通常以图形形式体现。

B.1.6.5 优势和局限

调查的优势包括：

——相对于访谈，参与人员更多，提供更有效的信息；

——调查的运行成本相对较低，特别是能够借助于在线统计分析软件的情况下；

——可以提供统计意义上的有效信息；

——结果易于制表与理解；通常可以以图表形式输出；

——提供调查报告相对容易。

调查的局限性包括：

——问题的性质宜要简单和明确的限制；

——通常需要获取一些人员统计信息以解释结果；

——如果预期获得足够数量的回复，则涵盖的问题数量会受到限制；

——提出问题的人无法解释，因此调查对象对问题的解释可能与预期不同；

——很难设计出不引导调查对象找到特定答案的问题；

——问卷往往会包含可能无效的基本假设；

——可能很难获得良好且公正的回复率。

B.1.6.6 参考资料

[11] SAUNDERS，M. LEWIS，P. THORNHILL，A. 2016，Research Methods for Business Students

[12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13，Conducting surveys

B.2 风险识别的技术

B.2.1 概述

风险识别技术包括：

——基于证据的方法，例如检查表法以及对历史数据的审查；

——实证分析方法，包括测试和建模，以确定在特定情况下可能发生的情况；

——认知调查，广泛征求有经验专家的意见；

——其他技术，即将所考虑的问题分成更小的元素，使用提出假设问题的方法依次对每个元素进行分析；

示例：HAZOP(B.2.4)、FMEA(B.2.3)和 SWIFT(B.2.6)。

——鼓励采用对未来可能性进行富有想象力思考的技术，例如情景分析法(B.2.5)；

——基于过去数据或理论模型的检查表或分层分类法(B.2.2)。

B.2 中描述的技术是一些风险识别的结构化方法示例。结构化方法可能比非结构化或半结构化讨论更全面，更容易体现风险识别方面的尽职调查。

使用包括自上而下和自下而上方法在内的多种技术，支持全面的风险识别。挑战风险识别结果的方法(例如红队策略)也可用于帮助检查，确保未忽略任何相关风险。

注：红队策略是从竞争对手的角度看待问题的做法[13]。

所描述的技术可能涉及多个利益相关者和专家，用来以个人或小组方式引出观点的方法描述，参见 B.1。

B.2.2 检查表、分层分类法

B.2.2.1 概述

风险评估可采用检查表法，便于理解背景、识别风险，以及针对不同目的对风险进行分组。还可用于管理风险，例如，对风险控制和处理方式进行分类，明确问责机制和责任，进行风险汇总和信息传递。

检查表可以基于过去失败和成功的经验，形成更为正规的风险类型和分类标准，根据共同属性对风险进行归类或分类。从形式来看，归类法是“自上而下”的概念上派生的分类方法，而分类法是“自下而上”的经验或理论上派生的分类方法，两者混合称之为混合方法。

风险分层分类法主要确保相互独立和全面详尽(即避免重叠和遗漏)。该方法侧重于对特定类别的风险进行分类并仔细检查。

分层分类法涵盖多个分类级别。分类法均宜分层，且被细分的级别越来越精细，有助于维护和管理类别数量，同时也满足足够的维度。

B.2.2.2 用途

检查表、分层分类法可应用于战略或操作层面，通过问卷、访谈、结构化讨论会或三者组合，采用面对面或基于计算机的方法进行实施。

在战略层面使用的检查表、分层法或分类法示例包括以下内容。

——SWOT 分析用于识别内部环境中的优势和劣势因素，外部环境中的机会和威胁因素，在考虑风险情况下帮助设定目标和制定策略；

——PESTLE、STEEP、STEEPLED 等方法代表了确定情景或识别风险时要考虑的因素类型的首字母缩略词[14]，代表政治、经济、社会、技术、环境、法律、道德和人口统计。可以选择与特定情况相关的类别，并为每个类别下的示例创建检查表；

——考虑战略目标实现的关键成功因素和风险驱动因素，并为风险驱动因素制定风险控制措施和预警指标。

在操作层面，风险检查表用于危险源辨识分析(HAZID)和预先危险性分析(PHA)[15]，是初步的安全风险评估，通常在项目的早期设计阶段进行。

风险的一般分类包括：

——按风险源：市场价格、交易对手违约、欺诈、安全隐患等；

——按结果、目标或绩效维度。

预先识别的风险类别可用于大范围风险分析，很难确保这些类别是全面的。此外，通过预先定义的方式细分风险，思维会沿着特定的路径进行，而忽视风险的重要方面。

本文件中描述的其他技术使用了检查表、分层法和分类法；例如，危险和可操作性分析 HAZOP

B.2.4 中的关键词和石川分析(B.3.3)中的类别。IEC 62740:2015[16]中给出了识别风险时可用于考虑人为因素的分类法。

一般来说,检查表越具体,其使用就越局限于它所创建的特定环境中。识别风险时,提供一般提示的词汇在鼓励创造性水平方面通常更有成效。

B.2.2.3 输入

输入是用于创建有效检查表、分层分类的数据或模型。

B.2.2.4 输出

输出如下:

——检查表、提示或类别以及分类方法;

——使用后对风险的理解,包括(在某些情况下)风险清单和风险分类。

B.2.2.5 优势和局限

检查表、分层分类法的优势包括:

——促进利益相关者对风险的理解;

——如果设计得当,能够将大量专业知识融入非专家也易于操作的系统中;

——一旦创建,后续几乎不需要专业知识;

局限性包括:

——其使用仅限于没有相关历史的新情况,或与其发展过程不同的情况;

——解决已知或想象的问题;

——通常是通用的,可能不适用于正在考虑的特定情况;

——复杂性会阻碍相互关系的识别(例如,互连和替代分组);

——缺乏信息会导致重叠和/或差距(例如,计划并非相互独立,并非完全穷尽);

——会鼓励"勾选框"类型的行为,而不是对想法的探索。

B.2.2.6 参考资料

[17] BROUGHTON, Vanda, Essential classification

[18] BAILEY, Kenneth, Typologies and taxonomies: An introduction to classification techniques

[19] VDI 2225 Blatt 1, Konstruktionsmethodik-Technisch-wirtschaftliches Konstruieren—Vereinfachte Kostenermittlung, 1997 Beuth Verlag

B.2.3 故障模式和影响分析(FMEA)、故障模式、影响和危害性分析(FMECA)

B.2.3.1 概述

故障模式和影响分析(FMEA)将硬件、系统、过程或程序细分为元素,对于每个元素,明确其可能故障的方式、故障的原因和影响。FMEA 完成后可进行关键性分析,明确每种故障模式的重要性(FMECA)。

对于每个元素,记录以下内容:

——功能;

——可能发生的故障(故障模式);

——可能产生这些故障模式的机制;

——如果故障确实发生，后果的性质；

——故障是无害的还是破坏性的；

——如何以及何时可以检测到故障；

——应对故障的现有内在规定。

对于 FMECA，研究团队根据其严重程度对每个已识别的故障模式进行分类，可以使用几种不同的危害性方法。最常用的是定性、半定量或定量后果/可能性矩阵(B.10.3)或风险系数(RPN)。危害性的定量测量也可以从实际故障率和已知后果的定量测量得出。

注：RPN 是一种指数方法(B.8.6)，它对故障的后果、故障的可能性和检测问题的能力(检测)进行评级。如果故障难以检测，则给予更高的优先级。

B.2.3.2 用途

FMEA/FMECA 可以在物理系统的设计、制造或操作过程中应用，以改进设计、选择设计备选方案或计划维护方案。它还可以应用于过程和程序，例如医疗程序和制造过程。它可以在系统从框图到系统的详细组件或流程的步骤任何级别中执行。

FMEA 可用于为故障树分析等分析技术提供信息。它可以为根本原因分析提供一个起点。

B.2.3.3 输入

输入包括待分析的系统、系统元素的足够详细的信息，以便可以对每个元素可能失败的方式以及失败的后果进行有意义的分析。所需的信息可以包括图纸和流程图、系统运行环境的详细信息以及有关故障的历史信息。

FMEA 通常由对所分析系统具有专业知识的跨职能团队执行，并由受过培训的主持人领导。涵盖团队所有相关的专业领域是非常重要的。

B.2.3.4 输出

FMEA 的输出是：

——包含故障模式、影响、原因和现有控制的工作表；

——测试每种故障模式(如果是 FMECA)的临界程度以及用来定义它的方法；

——任何推荐的措施，例如，后续分析、设计变更或待纳入测试方案的特征。

FMECA 通常对故障模式的重要性进行定性排序；不过，如果使用合适的故障率数据和定量结果，则可以给出定量输出。

B.2.3.5 优势和局限

FMEA/FMECA 的优势包括以下方面。

——可广泛应用于系统、硬件、软件和程序的人为和技术模式；

——它识别故障模式、其成因以及它们对系统的影响，并以易于阅读的格式进行呈现；

——通过在设计过程的早期识别问题，避免了在使用中进行昂贵的设备修改的需要；

——通过突出显示待监控的关键特性，为维护和监控程序提供输入信息。

局限性包括以下方面。

——FMEA 只能用于识别单一故障模式，而不是故障模式的组合；

——除非得到充分控制和重点关注，否则研究可能既耗时，成本又高；

——对于复杂的多层系统，实施 FMEA 可能困难、繁琐。

B.2.3.6 参考资料

[20] IEC 60812, Failure modes and effects analysis (FMEA and FMECA)

B.2.4 危险和可操作性(HAZOP)分析

B.2.4.1 概述

HAZOP(HazardandOperabilitystudies)分析是对计预期或现有过程、程序或体系进行的结构化和系统性检查,涉及识别出与设计意图的潜在偏差,并检查其潜在原因和后果。

在引导式研讨会上,该分析团队:

——将体系、过程或程序细分为更小的元素;

——同意每个元素的设计意图,包括定义相关参数(例如物理体系中的流量或温度);

——将引导词连续应用于每个元素的每个参数,并假设可能偏离设计意图,从而产生不良后果;

注:并非所有的引导词参数组合都有意义。

——同意每个案例的原因和后果,建议如何处理;

——记录讨论情况,同意可能采取的措施来应对已识别的风险。

表 B.1 提供了技术系统常用指导语的示例。类似的引导词,如"过早""过迟""过多""过少""过长""过短""错误方向""错误目的""错误行动",可以用来标明人为错误的模式。

引导词适用于以下参数,如:

——材料或过程的物理特征;

——温度、速度等物理条件;

——时机;

——系统组件或设计的特定意图(例如信息传输);

——操作方面。

表 B.1 基本引导语示例及其通用含义

引导语	含义
无或不	计划结果根本没有实现,或计划条件缺失
更多(更高)	量值增加
过少(过低)	量值减少
伴随	定性修改/增加(例如,附加材料)
部分	定性修改/减少(例如,混合物中只有两种成分中的一种)
相逆/相反	与设计意图逻辑相反(例如,反向流动)
异常	完全替代,完全不同的事情发生(例如,错误的材料)
早	相对于时钟时间
晚	相对于时钟时间

B.2.4.2 用途

HAZOP 分析最初用于分析化学工艺系统,但目前已扩展到其他类型的系统,包括机械、电子和电力系统、软件系统、组织变更、人为活动和法律合同设计和评审。

HAZOP 过程可以处理由于设计、部件、计划程序和人为活动的缺陷所造成的各种形式的对设计意图的偏离。它最常用于改进设计或识别与设计变更相关的风险。它通常在详细设计阶段开展,此时可以获得预期过程的完整图表和配套设计信息,同时设计变更仍然可行。不过,它可以分阶段进行,随着

设计的详细发展，每个阶段使用不同的引导语。HAZOP 分析也可以在操作阶段进行，但是，该阶段的变更可能需要较大成本。

B.2.4.3 输入

输入包括计划审核系统的现有信息，以及设计意图和性能规范的现有信息。对于硬件，这可以包括图纸、规格表、流程图、过程控制和逻辑图以及操作和维护程序。对于非硬件相关的 HAZOP，输入数据可以是描述所分析的系统或程序的功能和因素的任何文件；例如，组织图和角色说明、或合同草案、或程序草案。

HAZOP 分析通常由一个多学科团队实施，该团队宜包括系统的设计者和操作者，以及未直接参与被审核的设计或系统、过程或程序的人员。分析的领导者/引导员宜接受过培训，在实施 HAZOP 分析方面有经验。

B.2.4.4 输出

输出包括 HAZOP 会议记录，其中涵盖每个评审点的偏差记录。记录宜包括所使用的指导语，以及造成偏差的潜在原因。它们还可以包括解决已识别问题的措施，以及该措施的负责人员。

B.2.4.5 优势和局限

HAZOP 的优势包括以下内容：

——提供了系统地检查一个系统、过程或程序的方法，以确定未能实现其目的的原因。

——由多学科团队进行详细而彻底的检查；

——在流程的设计阶段识别潜在的问题；

——产生解决方案和风险应对行动；

——适用于广泛的系统、流程和程序；

——允许明确考虑人为错误的原因和后果；

——创建了整个过程的书面记录，可用于证明尽职调查。

局限性包括以下方面：

——详细的分析会很耗时，因此成本较高；

——该技术趋于重复，多次发现相同的问题；因此很难保持专注；

——详细的分析需要高水平的文档或系统/流程和程序规范；

——可以专注于寻找详细的解决方案，而不是挑战基本假设（然而，这可以通过分阶段举措缓解）；

——讨论可以集中在设计的细节问题，而不是更广泛的或外部的问题；

——受到设计（草案）和设计意图的约束，受到团队被赋予的范围和目标的约束；

——这个过程在很大程度上依赖于设计师的专业知识，他们可能会发现很难足够客观地在设计中寻找问题。

B.2.4.6 参考资料

[21] IEC 61882，Hazard and operability studies (HAZOP studies)-Application guide

B.2.5 情景分析

B.2.5.1 概述

情景分析（ScenarioAnalysis）是一系列技术的名称，这些技术涉及开发出预测未来如何发展的模

型。一般而言,它包括定义一个合理的场景,并根据各种可能的未来发展研究可能发生的情况。

在相对较短的时间尺度内,情景分析可能涉及从过去发生的事情进行推断。在相对较长的时间尺度内,情景分析可能涉及构建一个虚构但可信的情景,然后探索该情景中风险的性质。它最常由一群具有不同兴趣和专业知识的利益相关者应用。情景分析涉及详细定义要考虑的一个或多个情景,并探索该情景的影响和相关风险。通常宜考虑的变化包括:

——技术变化;

——可能产生多种结果的潜在未来决策;

——利益相关者的需求以及需求可能的变化;

——宏观环境的变化(监管、人口统计等);

——物理环境的变化。

B.2.5.2 用途

情景分析最常用于识别风险和探索后果。它可以在战略和运营层面使用,也可以用于整个组织或组织的一部分。

长期情景分析试图帮助规划未来的重大转变,例如过去 50 年来在技术、消费者偏好、社会态度等方面发生的转变。情景分析无法预测此类变化的可能性,但可以考虑后果并帮助组织发展适应可预见变化所需的优势和弹性。它可用于预测威胁和机会的发展趋势,并可用于所有类型的风险。

短时间框架情景分析用于探索起始事件的后果。可能的情景可以从过去发生的事情或模型中推断出来。此类应用程序的示例包括针对紧急情况或业务中断进行规划。如果没有数据,则使用专家的意见,但在这种情况下,尽最大程度关注专家对其意见的解释是非常重要的。

B.2.5.3 输入

为了进行情景分析,需要有关当前趋势和变化以及未来变化相关观点的数据。对于复杂或非常长期的场景,需要技术方面的专业知识。

B.2.5.4 输出

输出可以是每个场景的“故事”,告诉人们如何从现在转向主题场景。所考虑的影响既可以是有益的,也可以是有害的。这些故事可以包括那些能为情景带来附加值的合理细节。

其他输出可能包括:政策或计划对各种可能发生的未来的可能影响的理解,计划中未来发生可能出现的风险清单,以及在某些应用中,上述风险的主要指标清单。

B.2.5.5 优势和局限

情景分析的优势包括以下内容:

——考虑了一系列可能的未来。相比较传统依赖预测的方法更可取,即假设未来事件可能会继续遵循过去趋势。如果对当前知之甚少,难以据此进行预测;或考虑长期风险,这两种情况下,情景分析方法很重要;

——支持思维的多样性;

——鼓励对变化的主导指标进行监测;

——针对识别出的风险作出决定,这有助于为发生的任何事情建立弹性。

——局限性包括以下方面:

——使用的场景可能缺乏充分的基础,例如数据可能是随机性的。这可能会产生可能不被认可的

不切实际的结果；

——几乎没有证据表明，针对为远期未来探索的情景实际会发生。

B.2.5.6 参考资料

[22] RINGLAND, Gill. Scenarios in business

[23] VanderHEIJDEN, Kees. Scenarios: The art of strategic conversation

[24] CHERMACK, ThomasJ. Scenario planning in organizations

[25] MUKULPAREEK, Using Scenario analysis for managing technology risk

B.2.6 结构化假设分析技术(SWIFT)

B.2.6.1 概述

SWIFT 是一种高级别风险识别技术，可以独立使用，也可以作为分阶段方法的一部分使用，使 HAZOP 或 FMEA 等自下而上的方法更有效。SWIFT 在引导式的研讨会中使用结构化的头脑风暴(B.1.2)，其中将一组预先确定的引导语(时间、数量等)与参与者提出的提示相结合，这些提示通常以诸如“假设?”或“怎么可能?”等短语开头。它类似于 HAZOP，但应用于系统或子系统而不是设计者的意图。

在研究开始之前，主持人准备一份提示清单，以便对风险或风险源进行全面审查。在研讨会开始时，讨论了 SWIFT 的背景、范围和目的，并阐明了成功的准则。使用指导语以及“假定分析”式提示，主持人要求参与者提出和讨论以下问题：

——已知风险；

——风险源和驱动因素；

——以往的经验、成功和事件；

——已知的和现有的控制；

——监管要求和限制。

引导员使用提示列表来监控讨论并建议团队讨论的其他问题和场景。团队考虑控制是否充分，如果不充分，则考虑潜在的应对方法。在这个讨论中，进一步提出“假定分析”式问题。

在某些情况下，可以识别特定风险并记录风险描述、其原因、后果和控制措施。此外，还可以识别出关于风险、控制问题或系统性问题的更加共性的来源或驱动因素。

生成风险列表时，通常要使用定量或半定量风险评估方法来将行动进行等级划分。这通常会考虑现有的控制措施及其有效性。

B.2.6.2 用途

该技术通常可以应用于系统、工厂项目、程序和组织。特别是，它用于检查更改的后果以及由此变更或新出现的风险。可以考虑积极和消极的结果。它还可用于确定某系统或流程，这些系统或流程值得投入资源获取更详细的 HAZOP 或 FMEA。

B.2.6.3 输入

宜清楚地了解系统、程序、工厂项目和/或变更以及外部和内部环境。这是通过访谈、召集多功能团队以及协调人对文件、计划和图纸的研究来确定的。通常，待分析系统被分成多个元素以推进分析过程。尽管协调员需要接受实施 SWIFT 方面的培训，但这通常可以很快可以完成。

B.2.6.4 输出

输出包括一个风险登记册，其中记录了针对不同等级风险的行动或任务。

B.2.6.5 优势和局限

SWIFT 的优势包括以下几点：

——它广泛适用于所有形式的物理设备或系统、情况或环境、组织或活动；

——它对团队的准备工作要求较低；

——速度较快，重大危险及风险源在研讨会上可以很快凸显出来；

——该研究是“系统导向的”，参与者可以分析系统对偏差的反应，而不只是分析组件故障的后果；

——它可用来识别过程及系统改进的机会，通常可用来识别导致并促进成功可能性的活动；

——那些参与现有控制和进一步风险应对行动的人员参与到讨论会中，这样可以增强他们的责任感；

——它轻松创建风险登记表和风险应对计划。

局限性包括以下方面：

——如果讨论会团队缺乏足够丰富的经验或是如果提示系统不够全面，那么有些风险或危险可能就无法识别；

——该技术的高级应用可能不会揭示复杂、详细或相关的原因；

——建议通常是广泛的，例如，如果不进行进一步分析，该方法对稳健详细的控制措施起不到支持作用。

B.2.6.6 参考资料

[26] CARD，AlanJ.WARD，JamesR.和 CLARKSON，P.John. Beyond FMEA：The structured what-if technique（SWIFT）

B.3 确定风险源、原因和驱动因素的技术

B.3.1 概述

对潜在事件的原因和风险驱动因素的了解可用于设计预防不利后果或增强积极后果的策略。在获知根本原因之前，通常存在具有多个层次的原因层次结构。一般来说，对原因进行分析，直到行动可以被确定和证明。

因果分析技术可以在一组预先确定的标题下探索对原因的看法，例如石川方法（见 B.3.3），或者可以采用更具逻辑导向的方法，如故障树分析和成功树分析（见 B.5.7）。

蝶形图分析（见 B.4.2）可用于以图形方式表示原因和后果，并显示其被控制的方式。

IEC 62740[16]中描述的几种技术可用于主动分析未来可能发生的事件以及已发生的事件的可能原因。这些技巧在此不再赘述。

B.3.2 辛迪尼克（Cindynic）方法

B.3.2.1 概述

辛迪尼克的字面意思是关于危险的科学。辛迪尼克方法确定了可能导致许多不同后果的无形风险源和驱动因素。特别是，它识别和分析以下方面：

——不一致、模棱两可、遗漏、一无所知（称为缺陷）；

——利益相关者之间的分歧(称为不协调)。

辛迪尼克方法首先收集关于作为研究主题的系统或组织的信息,以及由地理、时间和空间和一组利益相关者网络或群体这些综合因素设定的情况。

然后使用半结构化访谈(见 B.1.5)在不同时间(t_1、t_2、……、t_i)收集关于各利益相关者的知识状态和心理状态的信息,其与辛迪尼克方法以下五个的准则相关:

——目标(组织的主要目的);

——价值(利益相关者高度重视的价值观);

——规则(管理其成就的权利、标准、程序等);

——数据(决策的基础);

——模型(技术、组织、人员等在决策中使用数据)。

注:可以根据辛迪尼克方法五个准则将表征内部和外部环境的元素放在一起。

该方法既考虑了看法,也考虑了事实。

一旦获得了这些信息,就要分析要达到的目标与辛迪尼克五个准则之间的一致性,建立表格,列出缺陷和不一致部分。

B.3.2.2 用途

辛迪尼克方法旨在了解:为什么尽管采取了所有控制措施来预防灾害,但它们仍然发生。此方法已扩展到提高组织的经济效率。该技术在组织内寻找可能导致影响广泛的后果的系统性风险源和驱动因素。它应用于战略层面,还可用于识别系统实现新目标演变过程的各因素,这些因素以有利或不利的方式发挥作用。

还可用于验证任何项目的一致性,尤其适用于复杂系统的研究。

B.3.2.3 输入

信息如上所述。分析通常涉及一个多学科团队,其中包括具有实际操作经验的团队以及将采取应对措施解决已识别风险源的团队。

B.3.2.4 输出

输出是各种表格,标明利益相关者之间的不协调和缺陷,如下示例所示。表 B.2 列举了一个矩阵,表明各利益相关者对五个分析准则(目标、价值、规则、模型和数据)所持的缺陷。通过比较不同时间t_1、t_2、……、t_i 情况下获取的输入信息,可以识别不同情况之间的缺陷。

表 B.2 每个利益相关者的缺陷

利益相关者	分析准则				
	目标	价值	规则	数据	模型
S1		专注于有限数量的值	没有参考程序	没有参考测量	没有参考模型
S2	目标与规则不一致	值之间缺乏排列	规则之间缺乏排列	其他国家的经验和反馈一无所知	特定型号一无所知
S3	目标与标准不一致	专注于特定值(例如,就业)	规则之间缺乏排列	未注意特定数据,如,工伤)	选择模型时缺乏优先级

表 B.3 是一个矩阵，其中相关利益相关者在两个轴上都表示，利益相关者之间的观点差异（所谓的不一致）显示在矩阵单元格中。这些表格能够促使设立减少缺陷和失调的计划。

表 B.3　利益相关者之间的分歧表

利益相关者	利益相关者			
	S1	S2	S3	S4
S1		S1 和 S2 的目标不同	S1 和 S3 的值不同	S1 和 S4 不共享相同的测量系统
S2			S2 和 S3 对程序的解释未达成一致	S2 和 S4 在数据上不一致
S3				S3 和 S4 对规则的解释存在分歧
S4				

B.3.2.5　优势和局限

辛迪尼克方法的优势包括以下几点：

——是一种系统的、多维的和多学科的方法；

——提供了系统潜在风险状态及其一致性的知识；

——考虑了任何责任级别风险的人和组织因素；

——整合了空间和时间的概念；

——产生了降低风险的解决方案。

局限性包括以下方面：

——并不优先考虑风险或风险源；

——最近才开始在行业中传播。因此，不会像传统方法那样受益于过去的发展获得的成熟度；

——根据所涉及的利益相关者的数量，可能需要大量的时间和资源。

B.3.2.6　参考资料

[27] KERVERN，G-Y.Elements fondamentaux des cindyniques

[28] KERVERN，G-Y.Latest advances in cindynics

[29] KERVERN，G-Y.&BOULENGER，P.Cindyniques-Concepts et mode d'emploi

B.3.3　石川分析（鱼骨）法

B.3.3.1　概述

石川分析使用团队方法来确定任何可取或不受欢迎的事件、影响、问题或情况的可能原因。可能的促成因素分为大类，涵盖人为、技术和组织上原因。信息在鱼骨图（也称为石川图）中描述（见图 B.1）。执行分析的主要步骤如下。

——建立要分析的“效果”，放在一个框内作为鱼骨图的头部。“效果”可以是积极的（目标），也可以

是消极的(问题)。

——就主要的原因类别达成一致。常用类别的示例包括:

- 6Ms,如,方法、机器、管理、材料、人力、金钱;
- 材料、方法和过程、环境、设备、人员、测量。

注:可以使用适合正在分析的情况的任何一组已定的类别。图 B.1 说明了另一种可能性。

——问"为什么?"和"这怎么会发生?"反复探索每个类别的原因和影响因素,将每个因素添加到鱼骨图的骨骼中。

——检查所有分支以验证一致性和完整性,并确保原因适用于主效果。

——根据团队的意见和现有证据确定最重要的因素。

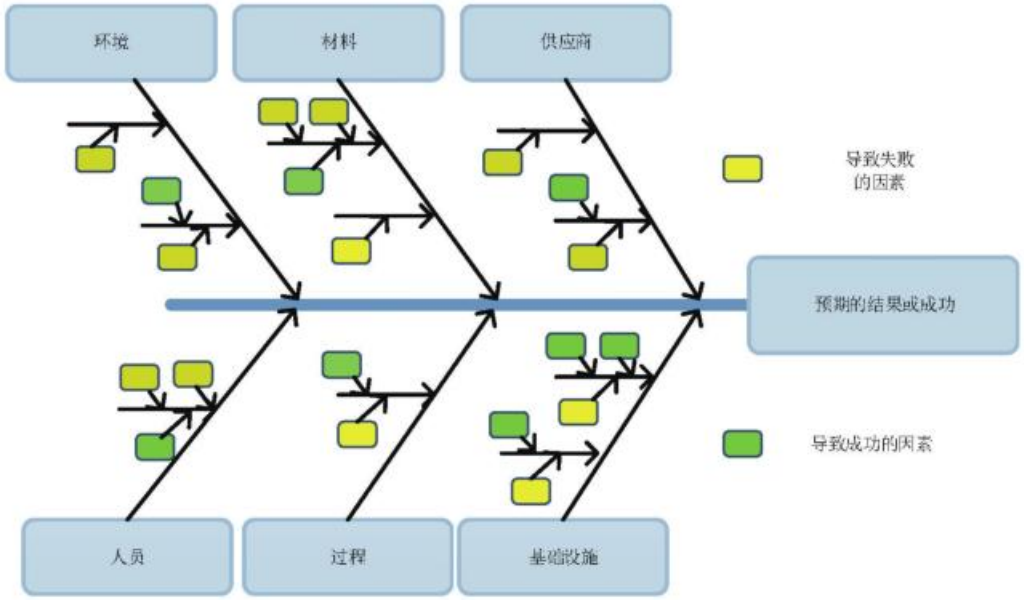

图 B.1 石川(鱼骨)图示例

该图通常是在研讨情景中创建。

B.3.3.2 用途

石川分析可用于对已发生的事件进行根本原因分析,或识别可能导致尚未发生的结果的因素。该方法可用于检查组织中任何级别、任何时间范围内的情况。

这些图表通常用于定性。根据对其相关性的置信度,可以将概率分配给一般原因,并进一步分配给子原因。然而,促成因素经常相互作用并以复杂的方式促成"效果",并且可能存在不明原因,使得量化无效。

B.3.3.3 输入

输入是参与者的专业知识和经验以及对所审查情况的理解。

B.3.3.4 输出

输出是被分析的效果的感知原因,通常显示为鱼骨图或石川图。鱼骨图的结构是将主要类别表示

为鱼骨干上的主要骨骼，并带有分支和子分支，这些分支和子分支描述了这些类别中更具体的子原因。

B.3.3.5 优势和局限

石川分析技术的优势包括以下内容：

——鼓励参与并利用团队知识；

——为头脑风暴或类似的识别技术提供了一种集中的方法；

——适用范围广；

——通过易于阅读的图形，提供了结构化的原因分析；

——允许人们在中立的环境下汇报问题；

——可以用来识别想要的和不需要的“效果”的促成因素；

注：积极的关注可以鼓励更多的主人翁意识和参与。

局限性包括以下方面：

——在分析开始时将因果因素分为主要类别意味着可能没有充分考虑类别之间的相互作用；

——对于未涵盖在所选类别内的因素的潜在原因，未予说明。

B.3.3.6 参考资料

[30] ISHIKAWA，K.Guide to Quality Control

了解其他因果分析技术，另请参阅 IEC 62740[16]。

B.4 控制分析技术

B.4.1 概述

B.4 中的技术可用于检查控制是否适当和充分。

蝶形图分析(B.4.2)和保护层分析法(B.4.4)确定风险源与其可能后果之间的障碍，可用于检查障碍是否足够。

危害分析和关键控制点法(B.4.3)寻找过程中的点，当有迹象表明条件发生变化时，可对条件进行监控并引入控制。

通过计算不同控制对后果概率的影响，事件树分析(B.5.6)也可以用作控制分析的定量手段。

任何原因分析技术都可以用作检查每个原因是否受到控制的基础。

B.4.2 蝶形图分析

B.4.2.1 概述

蝶形图是对从事件的原因到其后果的路径的图形描述。它显示了改变事件可能性的控制，以及事件发生时改变后果的控制。它可以被视为故障树或成功树(分析事件的原因)和事件树(分析后果)的简化表示。蝶形图可以从故障树和事件树开始构建，但更经常由团队在研讨会情景中直接绘制。

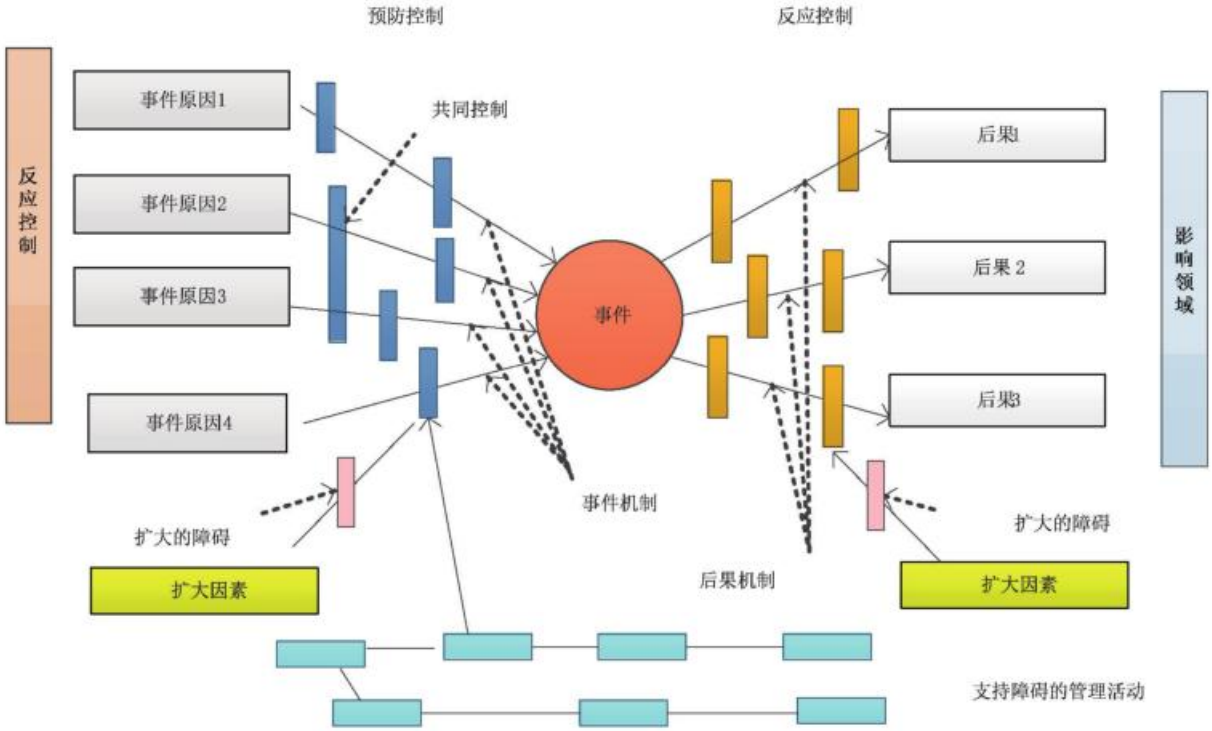

图 B.2　蝶形图示例

蝶形图绘制如下：

——目标事件由蝶形图的中心结表示，见图 B.2；

——风险源（或安全情境中的危险/威胁）列在蝶形图结的左侧；将导致事件发生的风险源通过线条连接到蝶形图的结上，这些线条代表风险源作用的不同机制；

——每个机制的障碍或控制显示为跨国线条的垂直条；

——在蝶形图结的右侧，向各潜在结果处绘制出放射状线条；

——事件发生后，竖线代表改变结果的反应性控制或障碍；

——添加了可能导致控制失败的因素（升级因素），以及针对升级因素的控制；

——支持控制（例如培训和检查）的管理功能可以显示在蝶形图下并链接到相应的控制。

在路径独立、某特定结果的可能性已知的情况下，可以对蝶形图进行一定程度的量化，同时可以估算出控制故障的可能性。然而，在很多情况下，路径和障碍并不独立，控制措施可能是程序性的，因此，其有效性并不确定。更适合的做法是使用故障树分析（B.5.7）和事件树分析（B.5.6）或 LOPA（B.4.4）进行量化。

B.4.2.2　用途

蝶形图分析用于在事件具有一系列可能的原因和后果的情况下显示和传达有关风险的信息。可用于探索事件的原因和后果，这些事件以简单形式记录在风险登记表（B.10.2）中。它特别用于分析后果更严重的事件。在评估控制措施时使用蝶形图，检查从原因到事件、事件到后果的每个途径是否具有有效的控制措施，并且可以识别可能导致控制措施失效（包括管理系统失败）的因素。对于不符合风险登记表的简单线性表示的风险，它可以用作记录相关信息方法的基础。它可以用于主动考虑潜在事件，也可以回顾性地对已经发生的事件进行建模。

当情况不能保证完整的故障树分析和事件树分析的复杂性，但比单一的原因-事件-结果路径所示更复杂时，可以使用蝶形图。

在某些情况下，可以创建级联蝶形图，其中一个事件的后果成为下一个事件的原因。

B.4.2.3 输入

输入包括关于预定义事件的原因和后果的信息，以及可能改变事件的控制。该信息可以从风险识别和控制的相关技术输出中获取，也可以从个人经验中获取。

B.4.2.4 输出

输出是一个简单的图表，显示了主要风险路径、现行控制以及可能导致控制失效的因素。它还显示了潜在的后果，以及在事件发生后可以采取的改变这些后果的措施。

B.4.2.5 优势和局限

蝶形图分析的优势包括以下内容：

——易于理解，并清晰地描绘了事件及其原因和后果；

——把注意力集中在可落实的控制及其有效性上；

——可适用于理想的结果以及不想要的结果；

——不需要高水平的专业知识来使用。

局限性包括以下方面：

——蝶形图不能描述从原因到事件的路径不独立的情况(即，故障树中存在“和”的情况)；

——可能过度简化复杂的情况，尤其是在尝试量化的情况下。

B.4.2.6 参考资料

[31] LEWIS，S. SMITH，K.，Lessons learned from real world application of the bow-tie method.

[32] HALE，A. R，GOOSSENSL.H.J.，ALE，B. J. M.，BELLAMYL.A. POSTJ.Managing safety barriers and controls at the workplace

[33] MCCONNELL，P.和 DAVIES，M.Scenario Analysis under Basel Ⅱ

B.4.3 危害分析和关键控制点法(HACCP)

B.4.3.1 概述

最初创建危害分析和关键控制点(HACCP)是为了确保 NASA 太空计划的食品安全，不过，也可用于非食品加工或活动。该技术提供了一种结构，用于识别风险源(危害或威胁)并在流程的所有相关部分实施控制进行防止。HACCP 用于操作级别，虽然其结果可以支持组织的整体战略。HACCP 旨在通过整个过程的监控和控制，而不是通过在过程结束时的检查，确保将风险降至最低。

HACCP 包括以下七项原则：

a) 识别危害、影响风险的因素和可能的预防措施；

b) 确定过程中的控制点，这些点可以进行监控、控制并将威胁最小化(关键控制点(CCP))；

c) 为要监控的参数建立关键限值，即每个 CCP 宜在特定参数内运行，以确保风险得到控制；

d) 建立程序，以规定的时间间隔监控每个 CCP 的关键限值；

e) 制定过程超出既定限制时要使用的纠正措施；

f) 建立验证程序；

g) 每一步都要实施记录和归档程序。

B.4.3.2 用途

HACCP是大多数国家/地区从事食物链中从收获到消费的任何缓解运营的组织的要求，以控制物理、化学或生物污染物的风险。

它已扩展用于制药、医疗器械制造以及其他领域，这些组织有其固有的生物、化学和物理风险。

该技术的原理是识别与过程输出的质量相关的风险源，并在该过程中确定可以监控的点，这些点的关键参数可以监控，风险源可以控制。这可以推广到许多其他流程，例如财务流程。

B.4.3.3 输入

输入包括：

——基本流程图或过程图；

——有关可能影响产品或过程输出的质量、安全或可靠性的风险源的信息；

——过程中可以监控指标、引入控制的控制点的信息。

B.4.3.4 输出

输出包括记录，包括危害分析工作表和HACCP计划。

危害分析工作表列出了该过程的每个步骤：

——某个步骤中可能引入、控制或加剧的危害；

——危险是否会带来严重的风险（通过经验、数据及技术文献等综合因素对结果和可能性进行分析）；

——对严重性做出判断；

——各种危险可行的预防措施；

——该步能否可使用监控或控制措施（例如，它是CCP吗?）。

HACCP计划说明了后续程序，以确保对具体设计、产品、过程或程序的控制。该计划包括一个涵盖所有CCP的清单；针对各CCP，清单内容如下：

——预防措施的关键限值；

——监控及继续控制活动（包括开展监控活动的内容、方式及时机以及监控人员）；

——如果发现与关键限值存在偏差，宜采取的纠正行动；

——验证和记录活动。

B.4.3.5 优势和局限

HACCP的优势包括以下内容：

——HACCP是一个结构化的过程，提供了质量控制并识别和降低风险的归档证据；

——重点关注流程中预防危险和控制风险的方法及位置的可行性；

——提供了整个过程的风险控制，而不是依于最终产品的检验；

——提请注意人类行为引入的风险，以及如何在引入点或随后对这些危险进行控制。

——局限性包括以下方面。

——HACCP要求识别危险、界定它们代表的风险并认识它们作为输入数据的意义。还需要确定适当的控制措施。HACCP可能需要与其他工具结合来提供这些输入；

——仅当控制参数超过规定的限值时才采取行动，这可能会错过控制参数的逐渐变化，而这些变化在统计上很重要且可采取行动。

B.4.3.6 参考资料

[34] ISO 22000, Food safety management systems—Requirements for any organization in the

food chain

[35] Food Quality and Safety Systems—A Training Manual on Food Hygiene and the Hazard-Analysis and Critical Control Point (HACCP) System

B.4.4 保护层分析法(LOPA)

B.4.4.1 概述

LOPA 对实施一组控制后实现的风险降低进行分析。它可以被视为事件树(B.5.6)的一个特例,有时作为危险和可操作性分析研究(B.2.4)研究的后续行动进行。

从已识别的风险列表中选择一个因果对,识别其独立保护层(IPL)。IPL 是一种机制、系统或操作,能够避免某个情景演变成不良结果。每个 IPL 可独立于初因事件,或与场景相关的任何其他保护层,并且是可审计的。IPL 包括:

——设计特点;

——实物保护装置;

——联锁和停机系统;

——临界报警与人工干预;

——事后实物保护;

——应急响应系统。

标准程序和/或检查不会直接增加失效的障碍,因此通常不宜被视为 IPL。估计每个 IPL 的失效概率,并进行数量级计算,以确定整体保护是否足以将风险降低到可容忍的水平。

通过将引发原因的频率与每个 IPL 的失效概率相结合,并考虑任何条件修改,可以发现非预期结果的发生频率。(条件修改的一个例子是一个人是否会在场并可能受到影响。)数量级用于频率和概率。

B.4.4.2 用途

LOPA 可以用于定性地审查因果要素和结果之间的保护层。还可以用于通过对每一层保护所产生的低风险的分析,定量地分配资源进行处理。它可以应用于具有长期或短期时间范围的系统,通常用于处理操作风险。

LOPA 还可以定量用于仪表系统的 IPL 和安全完整性等级(SIL 等级)的规范,如 IEC 61508(所有部分)和 IEC 61511(所有部分)中所述,并证明实现了指定的 SIL。

注:SIL 是一个离散级别(可能的四个中的一个),用于规定安全相关系统所需的可靠性。级别 4 具有最高等级的安全完整性,级别 1 具有最低级别。

B.4.4.3 输入

LOPA 的输入包括:

——事件来源、原因和结果的基本信息;

——有关现有控制或建议处理的信息;

——因果事件的频率、保护层失效的概率、结果措施和可容忍风险的定义。

B.4.4.4 输出

输出是对任何进一步处理和剩余风险估计的建议。

B.4.4.5 优势和局限

LOPA 的优势包括以下内容:

——比事件树分析或完全定量的风险评估需要更少的时间和资源，但比主观定性判断更严格；
——有助于确定资源并将资源集中在最关键的保护层上；
——确定了保障措施不足的操作、系统和过程；
——侧重于最严重的后果。

LOPA 的限制包括以下内容：

——一次侧重一对因果关系和一个场景；不包括风险之间或控制措施之间的复杂相互作用。
——当定量使用时，它可能无法解释共模失效。
——不适用于非常复杂的场景，其中存在许多因果对，或者存在影响不同利益相关者的各种结果。

B.4.4.6 参考资料

[36] IEC 61508(allparts), Functional safety of electrical/electronic/programmable electronic-safety-related systems

[37] IEC 61511(allparts), Functional safety—Safety instrumented systems for the processin-dustry sector

[38] Layer of protection analysis—Simplified process risk assessment

B.5 理解后果和可能性的技术

B.5.1 概述

B.5 中描述的技术旨在提供对结果及其可能性的更好理解。一般来说，可以通过以下方式探讨结果：

——实验，例如细胞研究，以探讨暴露于毒素的后果，并将结果应用于人类和生态健康风险；
——对过去事件的研究，包括流行病学研究；
——建模以确定在某些起因随后结果发展的方式，以及其如何取决于适当的控制。这可以包括数学或工程模型和逻辑方法，例如事件树分析(B.5.6)；
——鼓励想象力思维的技术，如情景分析(B.2.5)。

事件或特定结果的可能性可以通过以下方式估计：

——从历史数据推理(假设有足够的相关历史数据使分析在统计上有效)。这尤其适用于零发生，即人们不能假设由于过去没有发生过的事件或后果，它在不久的将来也不会发生；
——从与系统组件的失效或成功率相关的数据中进行综合：使用例如事件树分析(B.5.6)、故障树分析(B.5.7)或因果分析(B.5.5)之类的技术；
——模拟技术，例如，生成由于老化和其他退化过程导致的设备和结构失效的概率。

可以要求专家在考虑相关信息和历史数据的情况下就可能性和结果发表意见。有许多形式化的方法可以引出专家意见，能够让意见变得可见和明确(见 B.1)。

结果和可能性可以结合起来给出风险等级。这可用于通过将风险等级与可接受性标准进行比较来评估风险的重要性，或将风险按等级排序。

组合结果和可能性的定性值的技术包括指数方法(B.8.6)和结果/可能性矩阵(B.10.3)。风险的单一度量也可以从结果的概率分布中产生(参见例如 VaR(B.7.2)和 CVaR(B.7.3)以及 S 曲线(B.10.4))。

B.5.2 贝叶斯分析

B.5.2.1 概述

遇到既有数据又有主观信息的问题是很常见的。贝叶斯分析使两种类型的信息都可以用于决策。贝叶斯分析基于托马斯·贝叶斯牧师(1760)的定理。简而言之，贝叶斯定理为根据新证据改变观点提

供了概率基础。一般用公式(B.1)表示：

$$Pr(A \mid B)=\frac{Pr(B \mid A)Pr(A)}{Pr(B)} \quad \cdots\cdots(B.1)$$

式中：

$Pr(A)$ ——是 A 概率的先验评估；

$Pr(B)$ ——是 B 概率的先验评估；

$Pr(A \mid B)$——是给定 B 发生时 A 的概率(后验评估)；

$Pr(B \mid A)$——是给定 A 发生时 B 的概率。

贝叶斯定理可以扩展到包含特定样本空间中的多个事件。

例如，假设我们有一些数据 D，我们希望用它来更新我们之前对风险的理解(或缺乏)。我们希望使用这些数据来评估多个(N)竞争和非重叠假设的相对优势，我们将其表示为 H_n(其中 $n=1$、2、…、N)。然后可以使用贝叶斯定理来计算第 j 个假设的概率，见公式(B.2)：

$$Pr(H_j \mid D)=Pr(H_j)\left[\frac{Pr(D \mid H_j)}{\sum Pr(H_n)Pr(D \mid H_n)}\right] \quad \cdots\cdots(B.2)$$

式中：

$j=1$、2…、n。

这表明，一旦考虑到新数据，假设 j 的更新概率[即 $Pr(H_j \mid D)$]是通过将其先验概率 $Pr(H_j)$乘以括号中的分数获得的。

如果第 j 个假设为真，则该分数的分子是获得这些数据的概率。分母来自“总概率定律”——如果每个假设都为真，则获得这些数据的概率。分母是标准化因子。

如果将贝叶斯概率视为一个人对某个事件的信任程度，而不是基于物理证据的经典概率，则可以更容易地理解贝叶斯概率。

B.5.2.2 用途

贝叶斯分析是一种从数据推理的手段，包括判断性和经验性。可以开发贝叶斯方法，为特定环境下开发的风险模型中的参数提供推理；例如，事件的概率、事件的发生率或事件发生的时间。

贝叶斯方法可用于提供基于主观信任的关注参数的先验估计。先验概率分布通常与主观数据相关，因为它代表知识状态的不确定性。可以仅使用主观数据或使用来自类似情况的相关数据来构建先验。先验估计可以提供事件可能性的概率预测，并且对于没有经验数据的风险评估很有用。

然后可以通过贝叶斯分析将观察到的事件数据与先验分布相结合，以提供关注的风险参数的后验估计。

贝叶斯定理用于将新证据纳入到先验信任中，以形成更新的估计。

贝叶斯分析可以为关注的参数提供点和区间估计。这些估计体现了与可变性和知识状态相关的不确定性。这与经典频率论推理不同，它代表了关注变量的统计随机变化。

支持贝叶斯分析的概率模型取决于应用。例如，泊松概率模型可用于事故、不合格或延迟交货等事件，或者二项式概率模型可用于一次性项目。建立概率模型以贝叶斯网络(B.5.3)的形式表示变量之间的因果关系越来越普遍。

B.5.2.3 输入

贝叶斯分析的输入是构建和量化概率模型所需的判断和经验数据。

B.5.2.4 输出

与经典统计学一样，贝叶斯分析为关注的参数提供单个数字和区间的估计，并且可以应用于广泛的

输出。

B.5.2.5 优势和局限

优势如下：

——推理性陈述易于理解；

——它提供了一种对问题使用主观信任的机制；

——它提供了一种将先验信任与新数据相结合的机制。

局限性如下：

——它可以产生很大程度上依赖于先验选择的后验分布；

——解决复杂问题可能涉及高计算成本和密集劳动。

B.5.2.6

[39] GHOSH, J., DELAMPADY, M. 和 SAMANTA, T. An introduction to Bayesian analysis, New York Springer-Verlag, 2006

[40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. Prior Distribution Elicitation

B.5.3 贝叶斯网络和影响图

B.5.3.1 概述

贝叶斯网络(Bayes'net 或 BN)是一种图形模型，其节点代表随机变量(离散和/或连续)(图 B.3)。节点通过有向弧连接，这些有向弧表示变量之间的直接依赖关系(通常是因果关系)。

指向节点 X 的节点称为它的父节点，表示为 pa(X)。变量之间的关系由与每个节点关联的条件概率分布(CPDs)量化，表示为 P(X|pa(X))，其中子节点的状态取决于父节点值的组合。在图 B.3 中，概率由点估计表示。

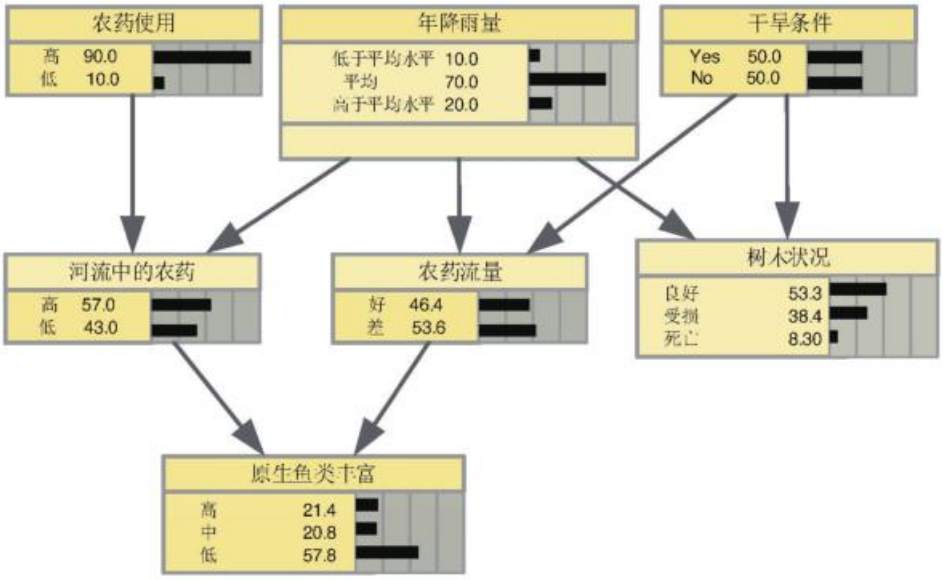

图 B.3 真实生态问题的简化版本：模拟澳大利亚维多利亚的本地鱼类种群

B.5.3.2 用途

基本 BN 包含代表不确定事件的变量，可用于估计可能性或风险，或推理导致特定结果的关键风险驱动因素。

BN 可以扩展为包括决策行动和评估以及不确定性，在这种情况下，它被称为影响图，可用于评估风险控制/缓解的影响或评估干预选项。

BN 模型可以构建为利益相关者对问题的定性表示，然后使用相关数据进行量化，包括判断（例如药品配送中心风险分析），或者 BN 模型只能从经验数据中学习（例如网络搜索引擎、金融风险）。无论 BN 的形式如何，底层推理机制都基于贝叶斯定理，并具有贝叶斯分析（B.5.2）的一般特性。

BN 的应用范围很广：包括环境决策、医疗诊断、关键基础设施寿命延长、供应链风险、新产品和过程开发图像建模、遗传学、语音识别、经济学、太空探索和网络搜索引擎。

一般来说，BN 提供可视化模型，支持问题的表达和利益相关者之间沟通。BN 模型允许进行敏感性分析，以探索“如果？”情况。使用因果映射（B.6.1）可以支持定性 BN 结构的构建，BN 可以与情景分析（B.2.5）和交叉影响分析（B.6.2）结合使用。

在存在高度不确定性和利益相关者意见分歧的情况下，BN 可用于获得利益相关者的意见和决策一致性。尽管需要专业知识来制作它，但这种表示很容易理解。

通过提高假设和过程的透明度以及以数学上合理的方式处理不确定性，BN 可用于为非技术利益相关者绘制风险分析图。

B.5.3.3 输入

BN 的输入需要了解系统变量（节点）、它们之间的因果关系（有向弧）以及这些关系的先验概率和条件概率。

在影响图的情况下，还需要评估（例如经济损失、伤害等）。

B.5.3.4 输出

BN 在图形输出中提供条件分布和边际分布，通常被认为是易于解释的，至少与其他黑盒模型相比是这样。BN 模型和数据可以很容易地修改，可使关系轻松地可视化，并探索参数对不同输入的敏感性。

B.5.3.5 优势和局限

BN 的优势包括以下几点：

——有易于使用和理解的现成软件；

——他们有一个透明的框架，能够快速运行场景并分析输出对不同假设的敏感性；

——可以包括对问题的主观信任以及数据。

局限性包括以下方面：

——定义复杂系统的所有交互是困难的，并且当条件概率表变得太大时在计算上可能变得难以处理；

——BN 通常是静态的，通常不包括反馈回路。然而，动态 BN 的使用是在增加的；

——设置参数宜了解很多条件概率，这些条件概率通常由专家判断提供。BN 只能根据这些假设提供答案（这是其他建模技术常见的限制）；

——用户可以输入错误，但输出可能仍然给出可信的答案；检查极值有助于定位错误。

B.5.3.6 参考资料

[41] NEIL, Martin andFENTON, Norman. Risk Assessment and Decision Analysis with

Bayesian Networks CRC Press, 2012

[42] JENSEN, F. V., NIELSENT. D. Bayesian Networks and Decision Graphs, 2nd ed. Springer, New York, 2007

[43] NICHOLSON, A., WOODBERRYO 和 TWARDYC, The "Native Fish" Bayesian networks. Bayesian Intelligence Technical Report 2010/3, 2010

[44] NETICA TUTORIAL

B.5.4 业务影响分析(BIA)

B.5.4.1 概述

业务影响分析就事件和活动如何影响组织的运营进行分析,并识别和量化管理这种影响所需的能力。具体而言,BIA 提供了对以下方面的一致理解:

——关键业务流程、功能和相关资源的重要性以及组织存在的关键相互依存关系;

——中断事件将如何影响实现关键业务目标的能力;

——管理中断因素影响和恢复到商定的运营水平所需的能力和性能。

BIA 可以使用问卷调查、访谈、结构化研讨会或结合三者进行。

B.5.4.2 用途

BIA 可用于确定流程和相关资源(例如人员、设备和信息技术)的关键性和恢复时间框架,以对中断事件进行适当的规划。BIA 还能帮助确定流程、内部和外部各方以及任何供应链之间的相互关系。

当考虑中断事件的结果时,它还可以用作结果分析的一部分。

BIA 提供的信息可帮助组织确定和选择适当的业务连续性策略,以实现对中断事件的有效响应和恢复。

B.5.4.3 输入

输入包括:

——有关组织的目标、战略方向、环境、资产和相互依存关系的信息;

——概述组织的业务产品和服务及其与业务流程的关系;

——对以往管理审查的优先事项的评估;

——组织活动和运营的详细信息,包括流程、资源、与其他组织的关系、供应链、外包安排和利益相关者;

——能够评估关键流程损失的财务、法律和运营结果的信息;

——事先准备的问卷或其他收集信息的方式;

——与中断事件结果相关的其他风险评估和关键事件分析的输出;

——将要联系的相关领域的组织和/或利益相关者的名单。

B.5.4.4 输出

输出包括:

——组织产品和服务的优先列表;

——作为输入收集的详细说明信息的文件;

——关键流程和相关依存关系的优先列表;

——记录关键流程损失的影响,包括财务、法律、环境和运营影响;

——有关重建关键流程所需的支持资源和活动的信息;

——短期、中期和长期不提供产品和服务的影响评估；
——考虑不提供产品和服务造成的影响变为不可接受的时间点，并在规定的最低水平上恢复提供产品和服务的优先时间框架；
——关键流程的中断时间框架和相关的信息技术恢复时间框架。

B.5.4.5 优势和局限

BIA 的优势包括：
——深入了解使组织能够实现其目标的关键流程，并可以指明业务改进的领域；
——规划组织应对中断事件所需的信息；
——了解发生中断时所需的关键资源；
——有机会重新定义组织的运营流程，以帮助提高组织的韧性。
局限性包括以下方面：
——BIA 依赖于参与完成问卷调查或进行访谈或研讨会的参与者的知识和认知。这可能导致对恢复要求的期望过于简单或过于乐观。
——群体动态会对关键流程的完整分析产生不利影响；
——对恢复要求的预期可能过于简单化或过于乐观；
——很难对组织的运营和活动有充分的了解。

B.5.4.6 参考资料

[45] ISO TS 22317, Societal security—Business continuity management systems—Guidelines for Business Impact Analysis

[46] ISO 22301, Societal security—Business continuity management systems—Requirements

B.5.5 因果分析(CCA)

B.5.5.1 概述

在某些情况下，可以通过故障树分析的事件由 CCA 可以更好地解决。例如：
——如果建立事件序列比因果关系更容易；
——如果故障树分析可能变得非常大；
——是否有单独的团队处理分析内容的不同部分。
在实践中，首先定义的通常不是顶事件，而是功能领域和技术领域之间的接口处的潜在事件。

例如，考虑航天器任务中“机组人员或车辆损失”事件。与其基于此项顶事件构建大型故障树，不如将点火故障或推进故障等中间不良事件定义为顶事件，并作为单独的故障树进行分析。然后，这些顶事件将依次用作事件树的输入，以分析操作结果。

根据分析部分情景的相关性，可以区分两种类型的 CCA。当需要详细的原因，但更一般的结果描述可以接受时，则分析的故障树部分可以扩展，并将该分析称为 CCA-SELF(小事件树大故障树)。当需要对结果进行详细描述但可以不太详细地考虑原因时，该分析称为 CCA-LESF(大事件树小故障树)。图 B.4 显示了一个典型的因果分析的概念图。

B.5.5.2 用途

与故障树分析一样，CCA 用于表示导致关键事件的故障逻辑，但它通过允许分析时间顺序故障来增加故障树的功能。该方法还允许将时间延迟纳入到结果分析中，而这在事件树中是不可能的。它根据特定子系统(例如应急响应系统)的行为，分析系统在发生关键事件后可能采取的各种路径。

如果量化，因果分析将给出对关键事件后不同可能结果的概率的估计。

因果图中的每个序列都是子故障树的组合，因此可以使用因果关系分析来构建大型故障树。

由于这些图的制作和使用是复杂的，当故障的潜在结果的严重程度证明需要加强力度时，往往会应用该技术。

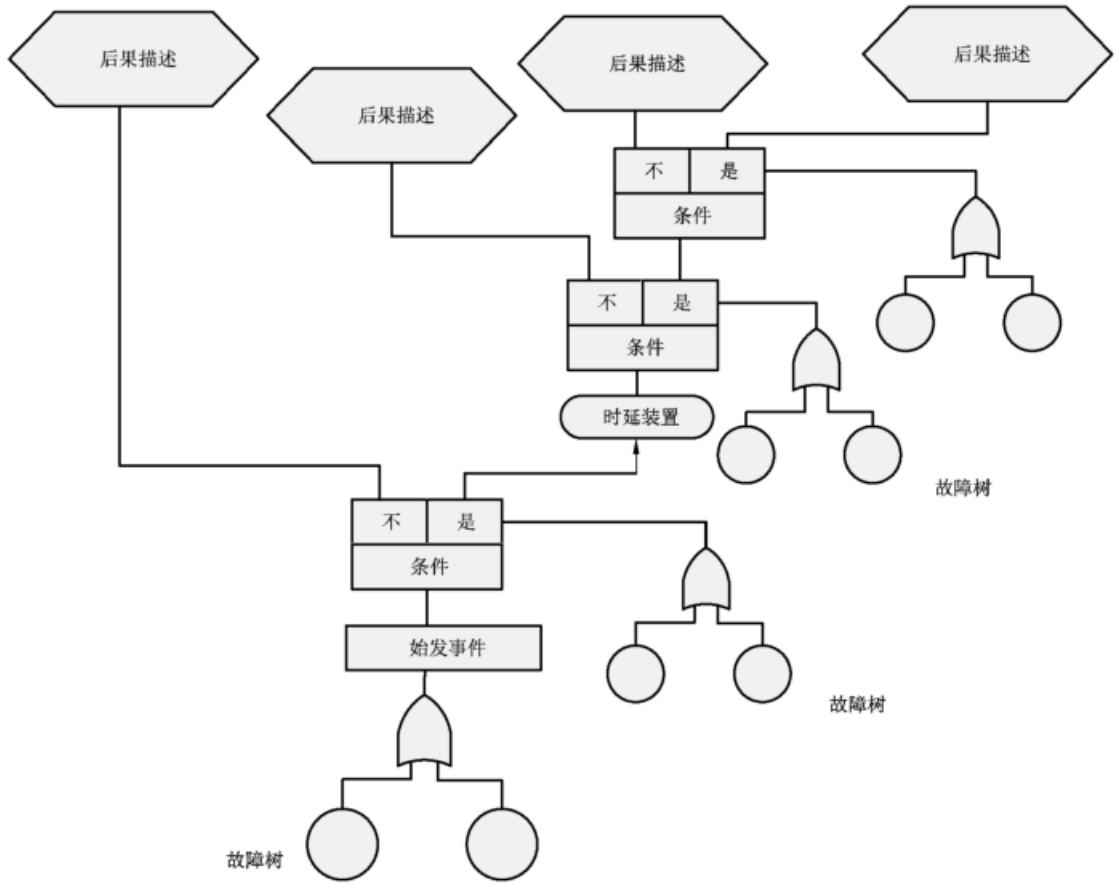

图 B.4　因果图示例

B.5.5.3　输入

宜了解系统及其故障模式和故障场景。

B.5.5.4　输出

CCA 的输出是：

——一个系统如何发生故障的图示，同时显示原因和结果；

——基于对关键事件之后特定条件下发生概率的分析，对每个潜在结果发生概率做出估计。

B.5.5.5

除了故障和事件树的优势之外，CCA 比这些技术能够更好地同时表示焦点事件和时间依赖关系的原因和结果。

局限性则是无论是在构造上还是在量化处理相关性上，CCA 比故障树和事件树分析更复杂。

B.5.5.6　参考资料

[47]　ANDREWSJ. D，RIDLEYL. M2002.Application of the cause-consequence diagram method

to static systems

[48] NIELSEND.S.The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis

B.5.6 事件树分析(ETA)

B.5.6.1 概述

ETA 是一种图形技术,它根据各种系统是否能够改变结果,来表示在初始事件之后可能出现的相互排斥的事件序列。事件树分析可以被量化来提供不同可能结果的概率(见图 B.5)。

事件树从初始事件开始,然后为每个控制线绘制代表其成功或失败的线。通过专家判断、数据或单个故障树分析,可以为每个控制分配失败或成功的概率。概率是条件概率。例如,某项功能的概率不是从正常条件下的测试中获得的概率,而是在初始事件条件下的功能概率。

假设各种事件是独立的,不同结果的频率由个体条件概率与初始事件的概率或频率的乘积表示。在图 B.5 中,假设初始事件的概率为 1。

B.5.6.2 用途

ETA 可以定性地用于帮助分析初始事件后的潜在场景和事件序列,并探索各种控制对结果的影响。它可以应用于组织的任何级别和任何类型的初始事件。

定量 ETA 可用于考虑控制的可接受性以及不同控制对整体风险等级的相对重要性。定量分析要求控制要么有效要么无效(即它不能说明降级的控制)并且控制是独立的。这主要是操作问题的情况。ETA 可用于模拟可能带来损失或收益的初始事件。然而,在追求优化增益路径的情况下,更常使用决策树(B.9.3)建模。

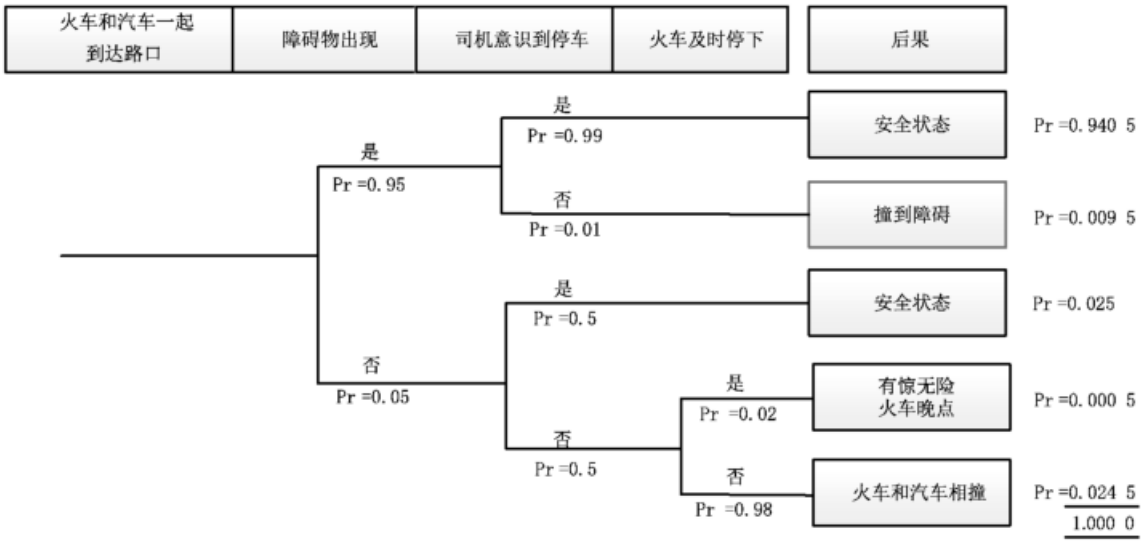

图 B.5 事件树分析示例

B.5.6.3 输入

输入包括:

——特定的初始事件;

——有关障碍和控制的信息,以及用于定量分析其失效概率的信息;

——了解可能的场景。

B.5.6.4 输出

ETA 的输出包括以下内容：

——初始事件的潜在结果的定性描述；

——事件发生率/频率或概率的定量估计以及各种故障序列和促成事件的相对重要性；

——控制有效性的定量评估。

B.5.6.5 优势和局限

ETA 的优势包括以下内容：

——分析初始事件后的潜在场景，并以清晰的图表方式显示控制成功或失败的影响，如果需要，可以量化；

——识别了可能无法预见的最终事件；

——可以识别潜在的单点故障、系统脆弱性区域和低回报对策，因此可用于提高控制效率；

——考虑了在故障树中难以建模的时间和多米诺骨牌效应。

局限性包括以下方面：

——为了进行全面分析，宜确定所有潜在的初始事件。总是有可能遗漏一些重要的启动事件或事件序列；

——只处理系统的成功和失败状态，并且很难将部分操作控制、延迟成功或恢复事件合并在一起；

——任何路径都以在路径上的前一个分支点发生的事件为条件。因此，可能路径上的许多依赖关系都得到了解决。然而，一些依赖关系，例如公共组件、公用系统和运营商，可能会被忽略，从而导致对特定结果的可能性的乐观估计；

——对于复杂的系统，事件树很难从头开始构建。

B.5.6.6 参考资料

[49] IEC 62502，Analysis techniques for dependability—Event tree analysis

[50] IEC TR 63039，Probabilistic risk analysis of technological systems—Estimation of finalevent rate at a given initial state

B.5.7 故障树分析(FTA)

B.5.7.1 概述

FTA 是一种用于识别和分析导致特定不良事件(称为“顶事件”)的因素的技术。顶事件的分析首先要确定其直接和必要的原因。这些可能是硬件或软件故障、人因错误或任何其他相关事件。这些原因之间的逻辑关系由多个门表示，例如与(AND)门和或(OR)门。然后以相同的方式逐步分析每个原因，直到进一步的分析变得无效。结果在树形图(见图 B.6)中以图形方式表示，树形图是布尔方程的图形表示。

B.5.7.2 用途

FTA 主要用于运营层面和中短期问题。它用于定性地识别顶事件的潜在原因和形成途径，或定量计算顶事件的概率。对于定量分析，必须遵循严格的逻辑。这意味着与(AND)门输入的事件必须是导致事件的必要和充分条件，或(OR)门上的事件代表事件的所有可能原因，其中任何一个原因都可能是唯一原因。使用基于二进制决策图或布尔代数的技术来说明重复的故障模式。

FTA 可在设计期间用于在不同选项之间进行选择，或在运营期间用于识别重大故障如何发生以及

不同路径对顶事件的相对重要性。

与之相关的技术是原因树，它用于回顾性地分析已经发生的事件，以及顶事件是一个成功事件的成功树。故障树则用于研究成功的原因，以实现未来的成功。

成功树中的概率往往高于故障树，并且在计算顶事件的概率时，宜考虑事件可能不相互排斥的可能性。

B.5.7.3 输入

故障树分析的输入如下：

——宜了解系统以及失败或成功的原因，以及对系统在不同情况下的行为方式的技术理解。详细的图表有助于分析；

——对于故障树的定量分析，所有基本事件都需要有关故障率的数据，或处于故障状态的概率，或故障频率和相关的修复/恢复率等；

——对于复杂的情况，建议使用软件并了解概率论和布尔代数，以便正确输入软件。

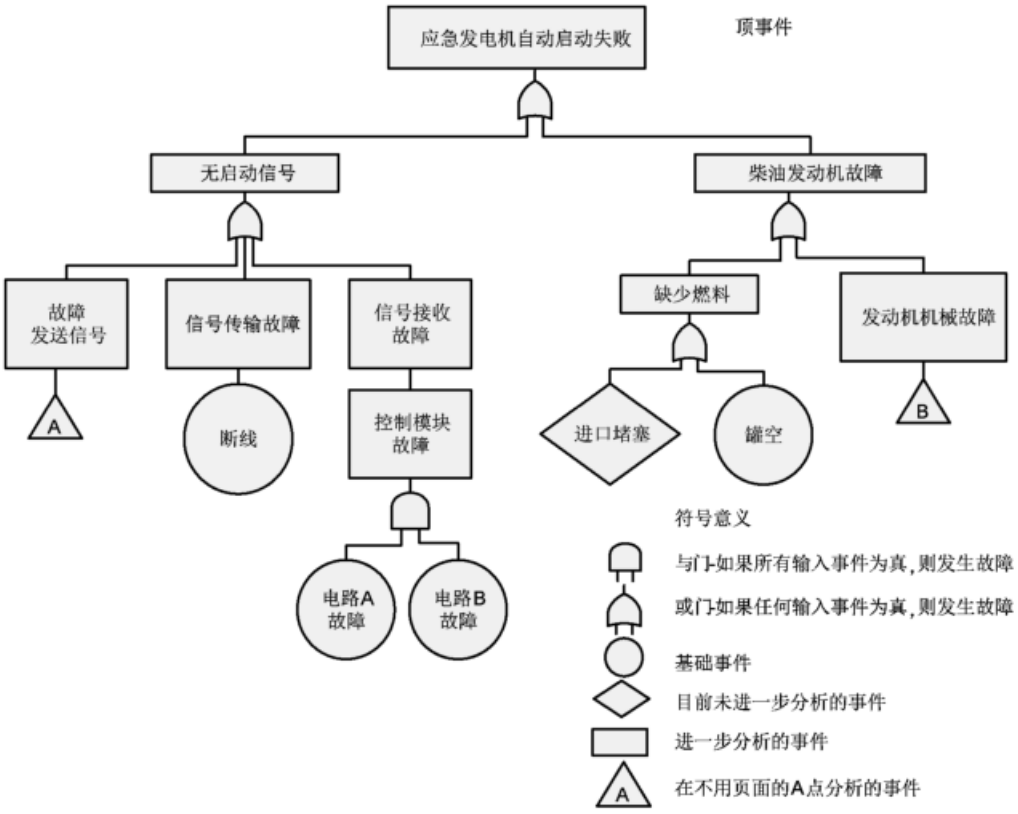

图 B.6 故障树示例

B.5.7.4 输出

故障树分析的输出包括：

——顶事件如何发生的图形表示，它显示了交互路径，每个路径都涉及两个或多个（基础）事件的发生；

——如果数据可用，一个有每个割集发生的概率的最小割集列表（单个失效路径）；

——在定量分析的情况下，顶事件的概率和基本事件的相对重要性。

B.5.7.5 优势和局限

FTA 的优势包括以下几点：

——这是一种高度系统化的规范方法，但同时又足够灵活，可以分析各种因素，包括人际交往和物理现象；

——对于分析具有许多接口和交互的系统特别有用；

——提供了一种图形表示，可以更容易地理解系统行为和所包含的因素；

——故障树的逻辑分析和割集的确定对于识别复杂系统中的简单故障路径非常有用，尤其是在该系统中，导致顶事件和事件序列的特定组合可能被忽略；

——可以适应简单或复杂的问题，工作量取决于复杂性。

局限性包括以下方面：

——在某些情况下，很难确定是否包括所有通往顶事件的重要途径；例如，在火灾分析中包括所有点火源。在这些情况下，无法计算顶事件的概率；

——时间相关性没有得到解决；

——FTA 只处理二进制状态（成功/失败）；

——虽然人因错误模式可以包含在故障树中，但此类故障的性质和程度可能难以定义；

——FTA 只分析一个顶事件，它不分析次要或偶然故障；

——对于大型系统，FTA 可能会变得非常大。

B.5.7.6 参考资料

[51] IEC 61025，Fault tree analysis (FTA)

[16] IEC 62740，Root cause analysis (RCA)

B.5.8 人因可靠性分析（HRA）

B.5.8.1 概述

HRA 是指一组旨在通过识别和分析不当操作的可能性来评估个人对系统可靠性和安全性贡献的技术。虽然最常用于在安全环境中降低操作者的操作水平，但类似的方法也可用于提高操作水平。HRA 在战术层面上应用于正确执行至关重要的特定任务。

首先执行分层任务分析，识别活动中的步骤和分步骤。通常使用一组关键字提示（例如太早、太晚、错误对象、错误操作、正确对象）来识别每个子步骤潜在的错误机制。

这些错误的来源（例如分心、可用时间太短等）可以被识别，并且可以使用信息来减少任务中出现错误的可能性。个人、组织或环境中影响错误概率的因素（绩效塑造因素（PSF））也同样能被识别。

错误动作的概率可以通过多种方法来估计，包括使用类似任务的数据库或专家判断。通常，任务类型的名义错误率首先被定义，然后应用乘数来表示增加或减少故障概率的行为或环境因素。目前，多种方法已经被开发来应用这些基本步骤。

早期的方法非常强调估计失效的可能性。最近的定性方法侧重于人的行为变化的认知原因，且更多地分析外部因素改变行为的方式，而不是试图计算失败概率。

B.5.8.2 用途

定性 HRA 可用于：

——在设计过程中，使系统的设计尽量减少操作者出错的可能性；

——在系统修改期间，查看人的操作是否可能受到任一方向的影响；
——改进流程以减少错误；
——协助识别和减少环境或组织安排中的错误诱发因素；
——定量 HRA 用于提供人的行为数据，作为逻辑树方法或其他风险评估技术的输入。

B.5.8.3 输入

输入包括：
——定义人们可执行的任务信息；
——实践中发生的错误类型或异常行为的经验；
——关于人的行为及其影响因素的专业知识；
——要使用的技术方面的专业知识。

B.5.8.4 输出

输出包括：
——可能发生的错误或异常行为的列表以及可以通过重新设计系统使之增强的方法；
——人的行为方式、类型、原因和结果；
——对行为差异带来的风险进行定性或定量评估。

B.5.8.5 优势和局限

HRA 的优势包括以下内容：
——在考虑与人能发挥重要作用的系统到相关风险时，提供了一个包括人类表现的正式机制；
——基于对认知机制的理解，正式考虑人的行为模式和机制，有助于确定修正风险的方法。
——局限性包括以下方面：
——这些方法最适合在受控良好的环境中执行的日常任务。它们对于复杂的任务或必须基于多个且可能相互矛盾的信息源的行动不太有用；
——许多活动没有简单的通过/失败模式。HRA 难以处理对行动的部分影响，如动作或决策的质量；
——因为可用的验证数据很少，量化往往严重依赖专家意见。

B.5.8.6 参考资料

[51] IEC 62508，Guidance on human aspects of dependability
[52] BELLJulie，HOLROYDJustin，Review of human reliability assessment method
[53] OECD，Establishing the Appropriate Attributes in Current Human Reliability AssessmentTechniques for Nuclear Safety

B.5.9 马尔可夫分析

B.5.9.1 概述

马尔可夫分析是一种定量技术，可以应用于任何可以用一组离散状态和它们之间的转换来描述的系统，前提是从其当前状态的演变不依赖于其过去任何时间的状态。

通常假设状态之间的转换以指定的间隔发生，并具有相应的转换概率(离散时间马尔可夫链)。在实践中，如果定期检查系统以确定其状态，则最常出现这种情况。在某些应用中，转换由具有相应转换

率(连续时间马尔可夫链)的指数分布随机时间控制。这通常用于可靠性分析,请参阅 IEC 61165。

状态及其转换可以用马尔可夫图表示,如图 B.7 所示。图中圆圈代表状态,箭头代表状态之间的转换及其相关的转换概率。此示例只有四种状态:良好(S1)、一般(S2)、差(S3)和故障(S4)。假设每天早上,系统都会被检查并分类为这四种状态之一。如果系统出现故障,总是当天得以修复并恢复到良好状态。

该系统也可以用表 B.4 中所示的转换矩阵来表示。请注意,在此表中,每一行的总和为 1,因为这些值表示每种情况下所有可能转换的概率。

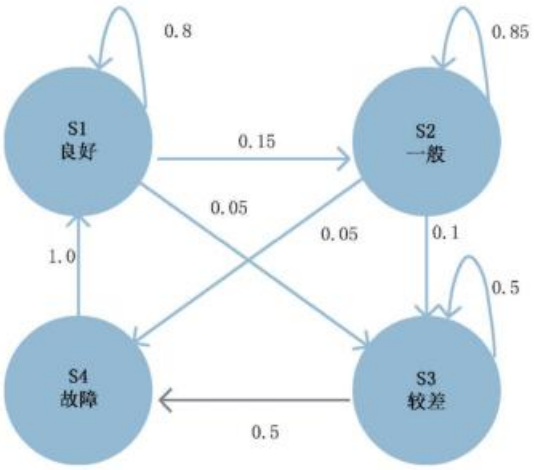

图 B.7　马尔可夫图示例

表 B.4　马尔可夫矩阵示例

		转换后的下一个状态			
		S1,良好	S2,一般	S3,差	S4,故障
当前状态	S1,良好	0.8	0.15	0.05	0
	S2,一般	0	0.85	0.1	0.05
	S3,差	0	0	0.5	0.5
	S4,故障	1	0	0	0

B.5.9.2　用途

马尔可夫分析可用于估计:

- 系统处于指定状态的长期概率;例如,这可能是生产机器按要求运行、组件出现故障或供应水平低于临界阈值的可能性;
- 复杂系统首次失效的预期时间(第一次通过时间),或系统恢复到指定状态前的预期时间(重现时间)。

表 B.5 中提供了不同领域的系统、状态和转换示例。

表 B.5　可以应用马尔可夫分析的系统示例

系统	状态	转换
技术系统	机器状况	变质、故障、维修
生产	生产水平	操作、清洁、复位
营销	购买的品牌	品牌忠诚，品牌转换
会计	应收账款状况	付款、核销、延期
医疗	患者状态	感染、康复、治疗、复发
水库	水量	流入、流出、蒸发
人力资源	工作类别	在工作类别和退出之间转移

B.5.9.3　输入

马尔可夫分析的输入是系统可以占据的一组离散状态、对需要建模的可能转换的理解以及对转换概率或转换率的估计(在连续时间马尔可夫链的情况下-CTMC)。

B.5.9.4　输出

马尔可夫分析生成系统处于任何指定状态的概率估计。它支持有关管理者在复杂系统中可能进行干预的多种类型的决策(例如，修改系统状态以及它们之间的转换)。

B.5.9.5　优势和局限

马尔可夫分析的优势包括以下内容：

——可用于对动态、多状态系统进行建模；

——状态转换图提供简单且易于交流的结构。

局限性包括以下内容：

——假设可能不适用于所有关注的系统，特别是随着系统的退化或适应，状态之间的转移概率或转移率会随时间而变化；

——准确的建模可能需要大规模数据收集和验证；

——太多的数据会降低答案的平均值。

B.5.9.6　参考资料

[54]　IEC 61165，Application of Markov techniques

[55]　OXLEY，ALAN.Markov Processes in Management Science

B.5.10　蒙特卡罗模拟分析

B.5.10.1　概述

分析风险时进行的一些涉及分布的计算。但是，使用分布进行计算并不容易，除非分布具有明确指定的形状，并且仅在可能不现实的限制和假设下，否则通常不可能导出解析解。在这些情况下，蒙特卡罗模拟分析等技术提供了一种进行计算和得出结果的方法。模拟通常涉及从每个输入分布中获取随机样本值，执行计算来导出结果值，然后通过一系列迭代重复该过程建立结果分布。结果可以作为值的概率分布或某些统计量(例如平均值)给出。

可以使用电子表格和其他传统工具来开发系统，也可以使用更复杂的软件工具来帮助满足更复杂

的需求。

B.5.10.2 用途

一般来说，蒙特卡罗模拟分析可以应用于任何系统：

——一组输入相互作用以定义输出；

——输入和输出之间的关系可以表示为一组依赖关系；

——分析技术无法提供相关结果或当输入数据存在不确定性时。

蒙特卡罗模拟可以作为风险评估的一部分用于两个不同的目的：

——传统分析模型的不确定性传播；

——当分析技术不起作用或不可行时的概率计算。

除其他外，应用包括建模和财务预测、投资绩效、项目成本和进度预测、业务流程中断和人员配备要求中的不确定性评估。

B.5.10.3 输入

蒙特卡罗模拟的输入是：

——包含不同输入之间以及输入和输出之间关系的系统模型；

——关于要表示的输入类型或不确定性来源的信息；

——所需的输出形式。

根据不确定性的程度，具有不确定性的输入数据可表示为分布或者分布的随机变量。均匀分布、三角分布、正态分布和对数正态分布通常用于此目的。

B.5.10.4 输出

输出可以是单个值，也可以表示为概率或频数分布，也可以是模型中对输出影响最大的主要函数的识别。

一般来说，蒙特卡罗模拟的输出要么是可能出现的结果的整个分布，要么是分布的关键度量，例如：

——出现既定结果的概率；

——不会超过问题所有者设置有一定置信的结果值。例如，超过的可能性小于10%的成本或超过80%的持续时间。

对输入和输出之间关系的分析可以揭示输入值不确定性的相对重要性，并确定影响结果不确定性的目标。

B.5.10.5 优势和局限

蒙特卡罗分析的优势包括以下内容：

——原则上，该方法可以适应输入变量中的任何分布，包括从相关系统的观察中得出的经验数据；

——模型开发相对简单，可以根据需要进行扩展；

——可以表示任何影响或关系，包括条件依赖等影响；

——可以应用敏感性分析来识别强弱影响；

——模型易于理解，因为输入和输出之间的关系透明；

——提供了结果准确性的度量；

——软件随时可用。

局限性包括以下方面：

——解决方案的准确性取决于可以执行的模拟次数；

——该技术的使用依赖于能够通过有效分布来表示参数中的不确定性；

——很难建立一个充分代表情形的模型；

——大型和复杂的模型可能对建模者构成挑战，并使利益相关者难以参与到过程中；

——该技术倾向于淡化高影响/低概率风险。

蒙特卡罗分析认识到所有结果不太可能在风险组合中同时发生，从而防止对不太可能的、后果严重的结果给予过多的重视。但这可能会产生将极端事件排除在外的效果，尤其是在考虑大型投资组合的情况下。这会给决策者带来无根据的置信。

B.5.10.6 参考资料

[56] ISO/IEC Guide 98-3:2008/Suppl 1: Uncertainty of measurement—Part 3: Guide to theexpression of uncertainty in measurement (GUM 1995)—Propagation of distributionsusing a Monte Carlo method

B.5.11 隐私影响分析(PIA)/数据保护影响分析(DPIA)

B.5.11.1 概述

隐私影响分析(PIA)(也称为隐私影响评估)和数据保护影响分析(DPIA)方法分析事件和活动如何影响个人隐私(PI)，并确定和量化管理它所需的能力。PIA/DPIA 是评估建议的过程，以确定对个人隐私和个人数据的潜在影响。

PIA 和 DPIA 可帮助组织识别、评估和处理与数据处理活动相关的隐私风险。当引入新的数据处理流程、系统或技术时，它们尤为重要。PIA 和 DPIA 同时是采用隐私设计方法的一个组成部分。

DPIA 还帮助组织遵守数据保护监管机构(例如欧盟通用数据保护条例，GDPR)的要求，并证明已采取适当措施来确保合规性。

具体流程如下：

——分析侵犯个人隐私的潜在后果(基本风险筛查)；

——考虑在发生隐私事件时处理个人信息是否具有高风险；

——对处理个人身份数据进行深入的风险分析。

PIA/DPIA 可以使用问卷调查、访谈、结构化研讨会或三者的结合进行，可利用欧盟第 29 条工作组的指导以及由 ICO(英国)、CNIL(法国)、NOREA(荷兰)等公司开发的几个模板。

B.5.11.2 用途

PIA/DPIA 用于确定流程和相关资源(例如人员、设备和信息技术)中的高风险结果，以限制因信息处理方式对人们隐私造成的潜在负面影响。

当更普遍地考虑信息处理的结果时，PIA/DPIA 也可以用作结果分析的一部分。

B.5.11.3 输入

输入包括：

——有关组织的目标、战略方向、环境、资产和相互依存关系的信息；

——对先前基本风险筛查的优先次序进行评估；

——处理个人信息时组织的活动和运营的详细信息，包括流程、资源、与其他组织的关系、供应链、外包安排和利益相关者；

——能够评估财务、法律和个人信息泄露或丢失造成的运营后果的信息(尤其是高度敏感的个人信息)；

——准备好的问卷或其他收集信息的方式；

——与相关事件结果相关的其他风险评估和关键事件分析的输出(尤其是数据泄露或数据丢失事件以及其他可能对预期数据处理产生影响的信息安全事件);
——将要联系的相关领域的组织和/或利益相关者的名单。

B.5.11.4 输出

输出包括:
——详细记录输入收集的信息的文件;
——关键信息过程和相关的相互依存关系的优先列表;
——按预期处理个人数据的风险较高的一组场景;
——个人信息泄露或丢失对自然人造成影响的记录;
——有关限制对数据主体潜在产生后果所需的支持资源和活动的信息;
——组织所涉及的产品和服务的优先列表;
——评估随时间变化的影响,对数据主体,不保证(高风险)个人数据的机密性、完整性和可用性的方式和后果;
——为遏制和/或信息恢复而采取行动的中断时间框架,向有关当局声明,在某些情况下,向数据主体声明。

B.5.11.5 优势和局限

PIA/DPIA 的优势包括它提供:
——深入了解在组织内部或代表组织处理(敏感)个人信息的关键流程;
——通过设计和默认原则评估隐私的实施;
——规划组织对个人数据事件的响应所需的信息;
——了解个人数据泄露或丢失时所需的关键资源;
——有机会重新定义和重新考虑组织对个人数据的操作处理;
——法律义务(例如欧洲通用数据保护条例)的情景下,在个人数据的高风险处理开始之前通知数据保护管理机构的文件。

局限性包括以下方面:
——在初始阶段(隐私影响筛选),对个人隐私的潜在风险严重程度的计算可能过于简化或低估风险;
——PIA/DPIA 依赖于参与完成问卷调查或进行访谈或研讨会的参与者的知识和认知;
——团队动态和时间压力会对关键流程的完整分析产生不利影响;
——在处理个人数据时,可能难以充分了解组织的运营和活动。

B.5.11.6 参考资料

[57] EU: General Data Protection Regulation (European Union Official Journal, 04.05.2016)
[58] ICO (UK): Data protection impact assessments
[59] CNIL (FR), Privacy Impact Assessment (PIA)

B.6 分析依赖和交互的技术

B.6.1 因果映射

B.6.1.1 概述

因果映射以论证链的形式将个人认知捕获到适合检查和分析的指向图中。事件、原因和后果可以

在映射中进行描述。

通常，映射是在研讨会环境中开发的，来自不同学科的参与者承担着获取、构建和分析材料的任务。在适当的情况下，认知通过文件的信息得以增强。输入可以从便利贴到专门的小组决策支持软件的各种工具来捕获。后者允许直接输入问题，并且可以成为一种高效的工作方式。所选工具可允许匿名捕获问题，以便创建一个开放和非对抗性的环境，以支持对因果关系的重点讨论。

通常，该过程从产生影响或导致与所考虑问题相关的事件的贡献开始。然后根据内容对它们进行聚类，此后再进行探索以确保全面覆盖。

参与者然后考虑每个事件可能对彼此产生的影响。这使得离散事件能够链接在一起，在映射中形成因果推理路径。该过程旨在促进对不确定事件的共同理解，并通过强制解释过程触发进一步的贡献，这对于建立一个事件如何影响另一个事件的论证链是必要的。对于捕获代表事件的节点和关系有明确的规则，以确保稳健和全面的建模。

一旦事件网络形成一个完整的映射，就可以对其进行分析以确定对风险管理有用的属性：例如，确定中心节点，即哪些事件的发生是中心事件，并且可以产生实质性的系统性影响；或确定反馈回路，这可能导致动态和破坏性行为。

B.6.1.2 用途

因果映射可识别风险列表中风险与主题之间的联系和相互作用。

可用于取证，为已发生的事件（例如项目超限、系统故障）开发因果映射。司法鉴定因果映射可以揭示触发因素、后果和动态。它们允许确定因果关系，这可能对索赔至关重要。

因果映射还可以主动用于捕捉对事件场景的全面系统评价。然后可以检查映射以进行深度学习，并形成风险定量分析的基础，以帮助确定优先级。

它们使综合处理计划得以制定，而不是单独考虑每种风险。

因果分析研讨会可以定期举办，以确保认识到风险的动态性质并适当地管理。

B.6.1.3 输入

用于制定因果映射的数据可以来自一系列不同的来源，例如来自个人访谈，其中生成的映射深入描述了发生或可能发生的情况。数据也可以从报告、索赔材料等文件中提取。这些数据可以直接使用，也可以用于为研讨会参与者分析与事件相关的论证链的过程提供信息。

B.6.1.4 输出

输出包括：

——因果映射，能够提供风险事件和这些事件之间的系统关系的可视化表达；

——因果映射的分析结果，用于识别由中心地位、反馈循环等引起的突发事件集群、关键事件；

——一份将映射翻译成文本并报告关键结果的文件，并解释参与者的选择和用于开发映射的过程。

输出宜提供与风险管理决策相关的信息以及用于生成此信息的过程的审计跟踪。

B.6.1.5 优势和局限

因果映射的优势包括以下内容：

——从参与者的多个角度考虑与问题相关的风险；

——过程的发散性和开放性允许探索风险，减少忽视关键事件或关系的机会；

——该过程允许有效且高效地捕获事件之间的交互关系，并提供对其关系的理解；

——确定形成映射的事件网络的过程，可以建立对有效风险管理的重要共同语言和共识。

局限性包括以下方面：

——映射的过程并不容易学习，因为它不仅需要掌握映射技术，还需要拥有在使用映射工具的同时具有管理组群的能力；

——映射本质上是定性的，在需要量化的情况下，映射需要用作其他适当模型的输入；

——映射的内容由来源决定，因此仔细考虑参与者的构成至关重要，否则可能会忽略重要区域。

B.6.1.6 参考资料

[60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. Visible thinking unlocking causal mapping for practical business results

[61] ACKERMANN, F, HowICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view ofrisks

B.6.2 交叉影响分析

B.6.2.1 概述

交叉影响分析是一系列技术的总称，旨在评估一组给定事件的发生概率随其中一个事件的实际发生而发生的变化。

交叉影响分析涉及构建一个矩阵，以显示不同事件之间的相互依存关系。行中列出了一组可能发生的事件或趋势，列中列出了可能受行事件影响的事件或趋势。然后需要专家估计：

——在给定时间范围内每个事件（独立于其他事件）发生的概率；

——假定每个其他事件发生，每个事件的条件概率，即专家估计的 i/j 对事件：

- $P(i/j)$—如果 j 发生，i 的概率；
- $P(i/\text{not}j)$—如果 j 不发生，i 的概率。

将其输入计算机进行分析。

有几种不同的方法可以在考虑所有其他事件的情况下计算一个事件的概率。不管这是如何完成的，通常的程序是执行蒙特卡罗模拟，其中计算机模型系统地选择一致的事件集合并迭代多次。随着计算机运行次数的增加，每个事件将产生新的后验概率。

敏感性分析是通过选择初始概率估计值或条件概率估计值进行的，其中存在不确定性。改变这个判断，再次运行矩阵。

B.6.2.2 用途

交叉影响分析用于预测研究，并作为预测不同因素如何影响未来决策的分析技术。它可以与场景分析（B.2.5）相结合，以确定最有可能产生的场景。当存在多个交互风险时，例如在复杂项目中或在管理安全风险时，可以使用它。

交叉影响分析的时间范围通常是中长期的，可以是从现在到五年，也可以是到未来 50 年。宜明确说明时间范围。

即使没有从分析中计算出的概率，事件矩阵及其相互依赖性也可以作为一般背景为决策者所用。

B.6.2.3 输入

该方法宜熟悉所研究问题，有能力预测未来的发展，能够现实地估计概率的专家。

可支持软件来计算条件概率。如果用户想要了解软件如何处理数据，则该技术需要特定的建模知识。开发和运行模型通常需要大量时间（几个月）。

B.6.2.4 输出

输出是可能的未来场景及其解释的列表。模型的每次运行都会生成一个合成的未来历史或场景，其中包括某些发生的事件和其他未发生的事件。在特定交叉影响模型的基础上，输出场景尝试生成最可能的场景，或一组统计上一致的场景，或从整个场景集合中生成一个或多个似是而非的场景。

B.6.2.5 优势和局限

交叉影响分析的优势包括以下内容：

——进行交叉影响问卷调查相对容易；

——将注意力转移到因果关系链(a 影响 b；b 影响 c，等)；

——可以澄清和增加对未来发展的知识；

——有助于探索假设以及找到共同点和分歧点。

局限性包括以下方面：

——可以包含的事件数量在实践中受到软件和专家所需时间的限制。所需的运行次数和估计的条件概率的数量随着所包括事件数量的增加而迅速增加(例如，对于一组十个事件，专家宜提供 90 次条件概率判断)；

——一项现实的研究需要专家进行大量的工作，而且经常会遇到很高的中途退出率；

——难以界定要包括的事件，任何未包括在事件集合中的影响都将被完全排除在研究之外；相反，包含的不相关的事件可能会不必要地使结果的最终分析复杂化；

——与其他基于获取专家知识的技术一样，该方法依赖于调查对象的专业水平。

B.6.2.6 参考资料

[62] JOINT RESEARCH CENTRE, EUROPEAN COMMISSION, Cross impact analysis, [viewed 2017-9-14]

B.7 提供风险度量的技术

B.7.1 毒理学风险评估

B.7.1.1 概述

在暴露于一系列环境危害对植物、动物、生态领域和人类造成风险的背景下进行的风险评估包括以下步骤：

对植物、动物、生态领域和人类的风险可能是由于物理、化学和/或生物制剂导致 DNA 损伤、先天缺陷、疾病传播、食物链污染和水污染。对此类风险的评估可能要在以下步骤中应用一系列技术。

a) 问题制定：这涉及通过定义评估的目的、目标群体的范围和关注的危害类型来确定评估的背景。

b) 危害识别和分析：这涉及在研究范围内识别对目标群体造成伤害的所有可能来源，并了解危害的性质及其与目标的相互作用。例如，在考虑人类接触化学品时，所考虑的后果可能包括破坏 DNA、或导致癌症或先天缺陷的可能性。危害识别和分析通常依赖于专业知识和文献回顾。

c) 剂量反应评估：目标群体的反应通常是暴露水平或剂量的函数。剂量反应曲线通常由动物试验或组织培养等实验系统得出。对于微生物或引入物种等危害，可根据现场数据和流行病学研究确定剂量反应曲线。在可能的情况下，确定产生效果的机制。图 B.8 显示简化的剂量反应曲线。

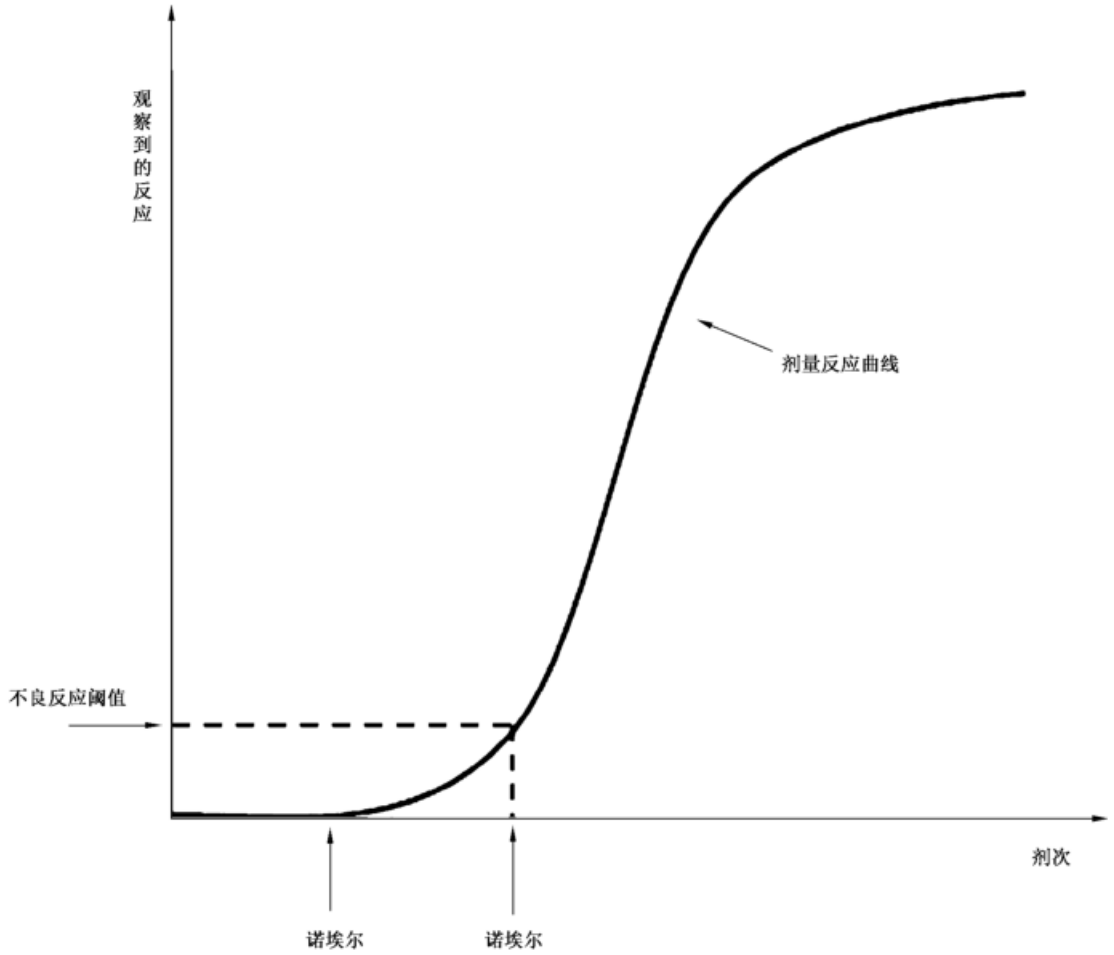

图 B.8　剂量反应曲线示例

关键词

NOEL　无可见作用限度

LOAEL　最低可见副作用水平

d) 暴露评估：估计目标群体在实践中将经历的剂量。这通常涉及路径分析，该分析考虑危险可能采取的不同途径、可能阻止其到达目标的障碍以及可能影响暴露水平的因素。例如，在评估化学品喷洒的风险时，暴露分析将考虑喷洒了多少化学品和在什么条件下，是否有人类或动物的任何直接接触，有多少可能作为残留物留在植物上，任何农药到达地面的环境影响，是否会在动物体内蓄积，是否进入地下水等。

e) 风险表征：将来自先前步骤的信息汇集在一起，以估计综合所有途径的影响后产生特定后果的可能性。

B.7.1.2　用途

该方法提供了对人类健康或环境风险程度的衡量标准。可用于环境影响报告中，表明特定暴露的风险是否可接受。它还用作定义可接受风险限度的基础。

B.7.1.3　输入

输入包括有关毒理学危害、关注的生态系统（包括人类健康）以及所涉及可能的相关机制的信息。

通常，需要进行物理测量来估计暴露量。

B.7.1.4 输出

输出是对人类或生态健康风险的估计，可以定量表示，也可以混合提供定性和定量信息。输出可能包括用于定义环境中危害的可接受限值的限值，例如不可见副作用限值(见图 B.8)。

B.7.1.5 优势和局限

这种分析形式的优势包括以下几点：

——提供了对风险性质和增加风险的因素的详细理解；

——路径分析是一个非常有用的工具，通常用于所有风险领域，以确定如何以及在何处改进控制或引入新的控制；

——该分析可以形成关于可接受暴露的简单规则的基础，这些规则可以普遍应用。

局限性包括以下方面：

——得到可能无法立即获得的可靠数据。因此可能需要进行大量研究；

——需要高水平的专业知识才能应用；

——剂量反应曲线和用于开发它们的模型的不确定性通常较高；

——如果目标是生态而不是人类，并且危害不是化学的，可能就不能很好的理解所涉及的系统。

B.7.1.6 参考资料

[63] WORLD HEALTH ORGANISATION, Human health risk assessment toolkit-chemical hazards

[64] US EPA, Guidelines for ecological risk assessment

B.7.2 风险价值(VaR)

B.7.2.1 概述

风险价值(VaR)在金融部门中被广泛使用，以提供在给定置信水平内特定时间段中金融资产投资组合可能损失金额的指标。大于 VaR 的损失只有在特定的小概率下才会发生。

损益的分配通常通过以三种方式之一得出。

——蒙特卡罗模拟(见 B.5.10)用于模拟投资组合中的可变性驱动因素并推导出分布。这种方法特别有用，因为它提供了有关分布尾部风险的信息，并且允许测试相关性假设。

——历史模拟模型在回顾观察到的结果和分布的基础上做出预测。这是一种简单的方法，但如果未来的发展与过去的经验不一致，则可能会产生很大的误导，这是市场压力时期的一个重大缺陷。

——分析方法基于潜在市场因素具有多元正态分布的假设。如此，就可以确定同样呈正态分布的损益。

许多金融组织使用这些方法的组合。

某些部门要求根据压力市场和高波动性条件计算 VaR，以提供一组可信的“最坏情况”结果。

VaR 的常用度量与一天和两周范围内的损失有关，损失的概率为 1%和 5%。按照惯例，VaR 报告为正数，尽管它指的是损失。

例如，图 B.9 显示了金融资产组合在一段时间内的价值分布，分布以累积形式显示。图 B.10 显示了投资组合遭受损失的区域，1%时的 VaR 值为 160 万(损失概率为 0.01)，5%时为 28 万(损失概率为 0.05)。

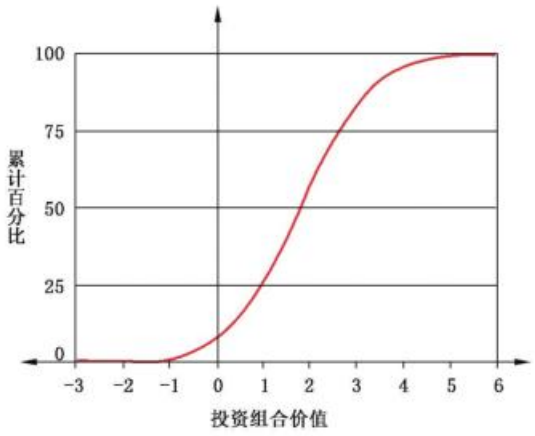

图 B.9 价值分布

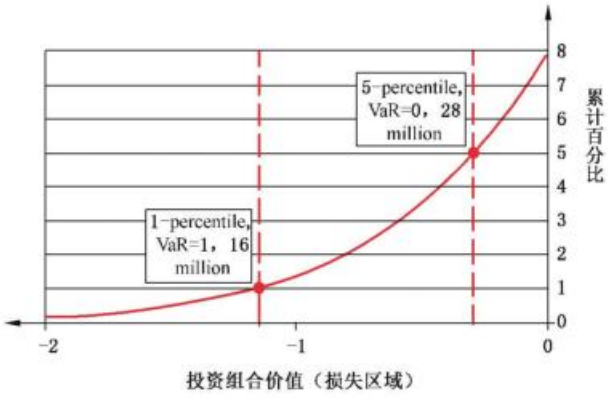

图 B.10 损失区域 VaR 值详细信息

B.7.2.2 用途

VaR 具有三个参数：潜在损失量、该损失量的概率以及损失可能发生的时间段。用于以下目的：

——在约定的风险承受能力或风险偏好范围内，为投资组合经理设定投资组合的最大损失限额；

——监控某个时间点资产组合的“风险”和风险趋势；

——确定可能需要为特定投资组合预留多少经济、审慎或监管资本；

——向监管机构报告。

B.7.2.3 输入

输入是影响投资组合价值的市场因素，例如汇率、利率和股票价格。通常，通过将投资组合中的工具分解为与基本市场风险因素直接相关的更简单工具，然后将实际工具解释为更简单工具的投资组合来识别这些工具。在评估输入变量时，出资者和监管机构可能要求采用特定的方法。

B.7.2.4 输出

在指定的时间段内，VaR 以指定的概率计算金融资产组合的潜在损失。该分析还可以提供指定损失量的概率。

B.7.2.5 优势和局限

优势包括以下方面：

——该方法简单明了，并为金融监管机构所接受(或要求)；

——如果需要，可以用于每天计算经济资本需求。

提供了一种根据约定的风险偏好设定交易组合限额的方法，并根据这些限额监控绩效，继而支持治理。

局限性包括以下方面：

——VaR 是一个指标，而不是对可能损失的具体估计。从 VaR 分析得出的损失可能性为 1%或 5%的 VaR 对应的单个数字来看，任何给定情况下的最大可能损失并不明显；

——VaR 有许多不合需要的数学特性：例如，当基于椭圆分布(如标准正态分布)时，VaR 是一种连贯的风险度量，但在其他情况下则不然。分布尾部的计算通常不稳定，并且可能取决于关于分

布形状和相关性的特定假设，这些假设很难证明是合理的，并且在市场压力时期可能不成立；

——模拟模型运行可能很复杂且耗时；

——组织可能需要复杂的 IT 系统，以易于使用的形式及时获取市场信息，以用于 VaR 计算；

——有必要假设一组参数的值，然后为模型确定这些值。如果情况发生变化，因此这些假设不相关，则该方法将不会给出合理的结果。换言之，这是一个无法在不稳定条件下使用的风险模型。

B.7.2.6 参考文件

[65] CHANCE,D., BROOKS, R. (2010).An introduction to derivatives and risk management

[66] THOMASJ.and PEARSONNeilD.Value at risk. Financial Analysts Journal 2000 56,47-67

B.7.3 条件风险价值(CVaR)或损失期望值(ES)

B.7.3.1 概述

条件风险价值(CVaR)，也称为损失期望值(ES)，是衡量金融投资组合在 a%最差情况下的预期损失的指标。这是与 VaR 类似的风险计量技术，但它对投资组合价值分布的尾部风险更为敏感。CVaR(a)指那些仅在特定时间发生损失的预期损失。例如，在图 B.10 中，当 a 为 5 时，CVaR(5)是指垂线左侧 5%处的曲线所表示的损失预期值，即所有损失的平均值大于 28 万。

B.7.3.2 用途

CVaR 技术已应用于信用风险计量，能够使贷款方更深入了解自金融危机爆发以来各行业极端风险的变化。图 B.11 最能说明风险投资组合中 CVaR 和 VaR 之间的差异。

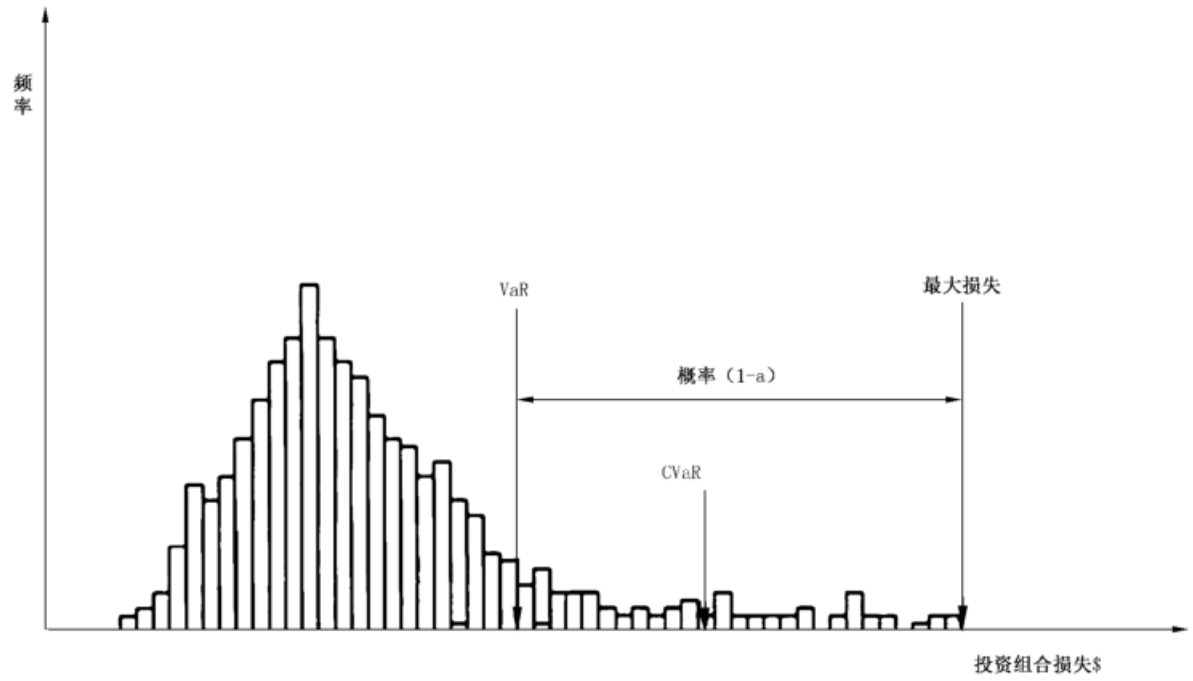

图 B.11 可能损失组合的 VaR 和 CVaR

B.7.3.3 输入和输出

参见 B.7.2 中对在险值法(VaR)的描述。

B.7.3.4 优势和局限

优势包括以下方面：

——CVaR 对尾部分布的风险比 VaR 更敏感；

——CVaR 避免了 VaR 的一些数学限制；

——CVaR 比 VaR 更保守，因为它关注的是会造成最大损失的结果。

局限性包括以下方面：

——CVaR 是一个潜在损失的指标，而不是对最大可能损失的估计；

——与 VaR 一样，CVaR 对资产价值波动的基本假设很敏感；

——CVaR 依赖于复杂的数学计算，需要大量的假设。

B.7.3.5 参考文件

[67] CHOUDHRY, M. An introduction to Value at Risk

[68] Value at Risk. New York University. [viewed 2017-9-14]. Available at: http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf

B.8 评价风险重要性技术

B.8.1 总论

B.8 中讨论的技术可用于如何风险应对的整个过程。其中一些可用于确定某一风险是否可以容忍或接受，另一些可用于表明某一风险的相对重要性或按优先顺序排列风险。

B.8.2 最低合理可行(ALARP)和在合理可行范围内(SFAIRP)

B.8.2.1 概述

ALARP 和 SFAIRP 是“合理可行”原则的首字母缩写词。它们代表了风险可接受性或可容忍性的检验准则，即采取更多措施降低风险是否合理可行。ALARP 通常要求将风险水平降低到合理可行的最低水平。SFAIRP 通常要求在合理可行的范围内确保安全。部分国家的立法或判例法已对合理可行原则进行了界定。

SFAIRP 和 ALARP 准则旨在获得相同的结果，但它们在一个语义点上有所不同。ALARP 通过将风险降低到合理可行的级别来实现安全，而 SFAIRP 则没有涉及风险级别。一般将 SFAIRP 解释为一个准则，通过该准则评估管控措施，以确定是否有可能进行进一步处理；若有可能，评估是否实际可行。在成本与收益严重不相称的基础上，ALARP 和 SFAIRP 都允许对风险处理进行贴现，但是其适用程度取决于所在管辖区。例如，在某些管辖区，成本效益研究(见 B.9.2)可支持已实现 ALAR 或 SFAIRP 的论点。

ALARP 概念最初由英国卫生与安全执行局提出，如图 B.12 所示。在某些司法管辖区，量化的风险水平位于不可容忍区、ALARP 区和广泛可接受区之间。

B.8.2.2 用途

作为确定是否需要对风险进行处理的准则。经常用于安全相关的风险，在某些司法管辖区，立法者也会使用 ALARP 和 SFAIRP。

ALARP 模型可将风险分为以下三类：

——不可容忍的风险类别，除非在特殊情况下，否则该风险不可接受；

——广泛可接受的风险极低的风险类别，无须考虑进一步降低风险（但如切实可行及合理，可予以实施）；

——介于以上风险之间的区域（即 ALARP 区域），即在合理可行的情况下，宜进一步降低风险。

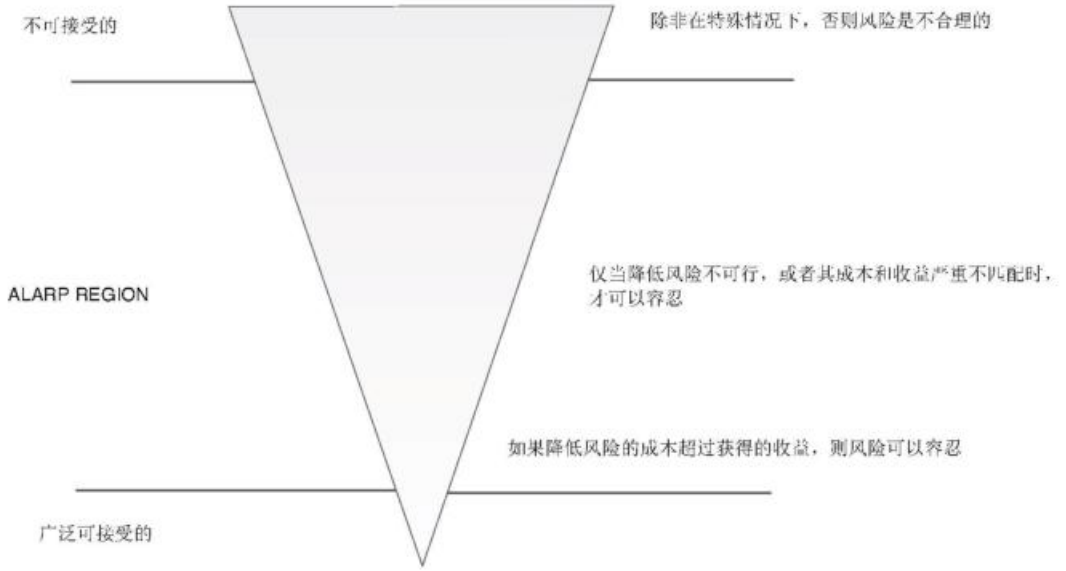

图 B.12 可能损失组合的 VaR 和 CVaR

B.8.2.3 输入

相关信息：

——风险来源及相关风险；

——ALARP 区域的限制准则；

——现有控制措施，以及可能实施的其他控制措施；

——潜在后果；

——这些后果发生的可能性；

——可能的处理措施所需的成本。

B.8.2.4 输出

可给出是否需要处理的决定以及处理的方式。

B.8.2.5 优势和局限

ALARP/SFAIRP 的优势包括：

——能够在判例法和立法的基础上制定统一的处理标准，支持公平原则，即所有个人都有权获得同等程度的保护，而不是其组织认定的可容忍或接受的风险；

——支持效用原则，降低风险所需的成本不宜超过合理可行的范围；

——允许非规定性目标设定；

——支持风险最小化目标的持续改进；

——通过利益相关者协商讨论和确定可接受或可容忍的风险，并提供透明、客观的处理方法。

局限性包括以下方面：

——对 ALARP 或 SFAIRP 的诠释具有挑战性，因为它要求组织必须了解合理可行原则的背景，并对该背景做出判断。

——将 ALARP 或 SFAIRP 应用于新技术可能会出现问题，因为尚不清楚或不了解风险及其可行的处理措施。

——对规模较小的组织来说，在经济上可能无法承担 ALARP 和 SFAIRP 设定的统一处理标准，从而会导致项目风险或终止。

B.8.2.6 参考文件

[69] HSE，2010a，HID'S Approach To'As Low As Reasonably Practicable'（ALARP）Decisions

[70] HSE，2010b，Guidance on（ALARP）decisions in control of major accident hazards（COMAH）

[71] HSE，Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable

B.8.3 频率-数量（F-N）图

B.8.3.1 概述

F-N 图是定量后果/可能性矩阵的特例（B.10.3）。X 轴表示累计死亡人数，Y 轴表示死亡发生的频率。轴上的刻度均为对数，以符合典型数据。风险准则通常显示为直线，其中斜率越高，死亡人数越高。

B.8.3.2 用途

F-N 图可用于记录涉及人员死亡的事件的结果，也可与可接受性预定准则进行比较，显示生命损失风险的定量分析结果。

图 B.13 显示了标记为 A 和 A-1 以及 B 和 B-1 的两个准则示例。它们将风险划分为了不可接受区域（A 或 B 之上）、普遍接受的区域（A-1 和 B-1 以下）以及当风险降低到尽可能低的允许风险区域（ALARP 区域）（B.8.2）。B 准则显示了更高的斜率（即对多人死亡事故的容忍度较低）和更保守的总体限值。曲线 C 上还显示了六个点，代表了与准则进行比较的风险定量分析的结果。

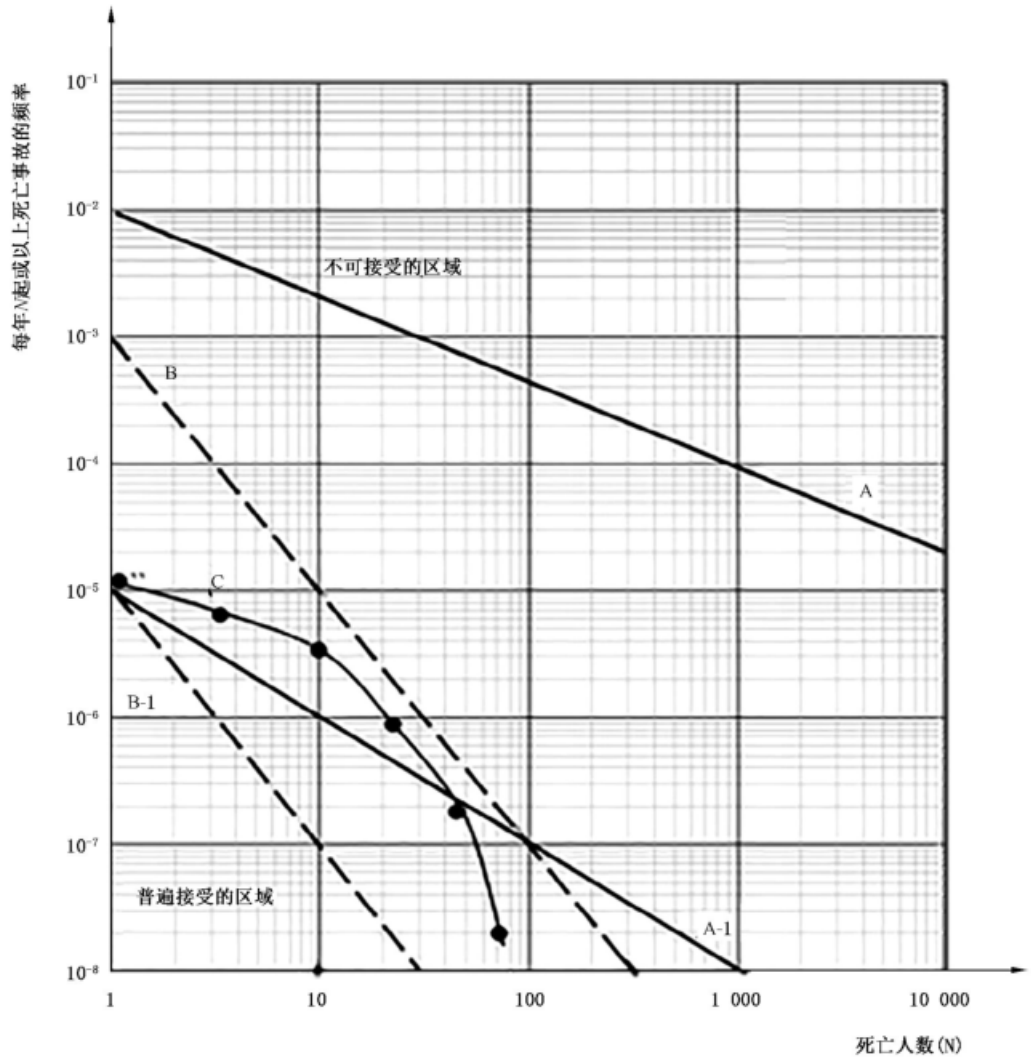

图 B.13　F-N 图示例

该方法广泛运用于土地使用规划或类似安全评估影响的特定重大危险场所的社会风险。

注：社会风险是指由于单一事件中发生多人死亡而引起的社会问题。

B.8.3.3　输入

来自事故或预测死亡概率的定量风险分析的数据。

B.8.3.4　输出

与预先设定的准则相比较并以图表形式显示的数据。

B.8.3.5　优势和局限

F-N 图的优势包括：

——提供的输出易于理解，并可以作为决策的基础；

——开发 F-N 图所需的定量分析有助于理解风险及其原因和后果。

局限性包括以下方面：

——图表的计算较为复杂，存在诸多不确定性；

——全面分析需要分析所有潜在的重大事故情景。比较耗时并且需要较高水平的专业知识；

——在排名时，F-N 图不利于进行相互比较（例如，决定哪种发展会导致更高的社会风险）。

B.8.3.6 参考文件

[72] Understanding and using F-N Diagrams, Annex in Guidelines for Developing Quantitative-Safety Risk Criteria

[73] EVANS, A. Transport fatal accidents and FN-curves

B.8.4 帕累托图

B.8.4.1 概述

帕累托图（见图 B.14）是一种选择有限数量任务来产生显著整体效果的工具。它采用帕累托原则（也称为二八法则），即 80％的问题是由 20％的原因所造成的，或者说做 20％的工作可以产生 80％的收益。

绘制帕累托图来选择要解决原因的步骤如下：

——识别并列出问题；

——识别每个问题的原因；

——按原因将问题归为一组；

——将每组的分数相加；

——绘制一个柱状图，首先显示得分较高的原因。

帕雷托原则只考虑问题的数量，而不考虑其重要性。换而言之，严重后果问题可能与不严重后果问题的最常见原因无关。可以根据结果对问题进行评分，来提供权重分配。帕累托分析是一种自下而上的方法，可以提供定量结果。虽然不用复杂的工具，也不需要特殊的培训或能力来使用这项技术，但一些经验对于避免常见的限制和错误非常有帮助。

注：数字 80％和 20％是说明性的——帕累托原则说明了投入的工作和取得的成果之间往往缺乏对称性。例如，13％的工作可以产生 87％的回报。或者 70％的问题可以通过处理 30％的原因来解决。

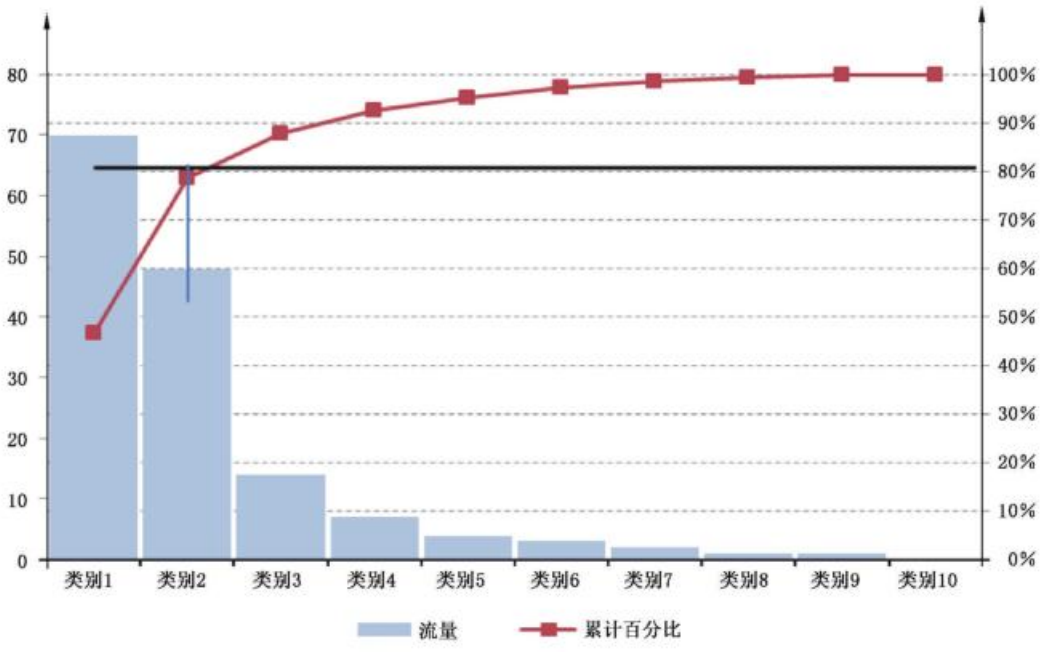

图 B.14 帕累托图示例

B.8.4.2 用途

当出现众多可能的行动方案时，帕累托分析在操作层面很有用。不管需要哪种形式的优先级排序，都可以使用帕累托分析。例如，它可以帮助确定哪些原因最需要解决或哪些风险处理措施最有益。

条形图是一种显示帕累托分析的典型示例，其中横轴代表类别（例如材料类型、尺寸、废料代码、加工中心），而不是连续的刻度（例如从 0 到 100）。这些类别通常是“缺陷”、缺陷来源或流程输入。纵轴代表某种类型的计数或频率（例如，发生次数、事件、部分、时间）。此后可绘制累积百分比的折线图。

累积百分比与 80％线相交处的左侧部分是已处理的部分。

B.8.4.3 输入

需要分析的数据，例如与过去的成功和失败及其原因相关的数据。

B.8.4.4 输出

帕累托图的输出，有助于说明哪些类别最为重要，以便将精力集中在可以进行最大改进的领域。它有助于直观地确定哪些类别构成“至关重要的极少数”，哪些构成“微不足道的大多数”。虽然是定量的分析，但是输出的是问题、原因等分类，比如，按重要性排序。

若第一个分析包含许多小的或不常见的问题，则可以将它们合并到“其他”类别中。显示在帕累托图的最后（即使它不是最小的柱线）。累积百分比贡献线（每个类别贡献的总和作为总数的一部分）也可以得到显示。

B.8.4.5 优势和局限

帕累托分析的优势包括：

——帕累托分析着眼于个体风险的常见原因，并将其作为处理措施的基础；

——直观地显示可以取得最大收益的地方；

——可以以较少或中等的时间及成本来取得成果。

局限性包括以下方面。

——没有考虑到处理每个潜在原因的成本或相对困难性；

——需要提供适用于所分析情况的数据；

——数据需要分类并且符合二八法则，才能使方法有效；

——数据不足时，难以构建相对权重；

——通常只考虑历史数据，不考虑潜在变化。

B.8.4.6 参考文件

[74] ParetoChart，ExcelEasy

[75] Pareto Chart

B.8.5 以可靠性为中心的维修（RCM）

B.8.5.1 概述

以可靠性为中心的维修（RCM）是一种基于风险的评估技术，用于为系统及其组件确定适当的维护策略及任务，以便高效、有效地实现各类设备所需的安全性、可用性和运行经济性。它包含了执行风险

评估的所有流程步骤，包括风险识别、风险分析和风险评价。

RCM 程序的基本步骤是：

——启动和规划；

——功能失效分析；

——维修任务选择；

——执行；

——持续改进。

RCM 中的功能分析最常通过执行故障模式、影响分析和危害性分析(FMECA，B.2.3)来进行，重点关注可通过进行维修任务来消除或减少潜在故障频率和/或后果的情况。通过定义故障影响来确定后果，在不进行维护的情况下，估计每个故障模式的频率来分析风险。风险矩阵(B.10.3)允许建立风险级别的类别。

然后为每个故障模式选择适当的故障管理策略。通常采用标准的任务选择逻辑来选择最合适的任务。

制定计划以执行建议的维修任务，包括确定详细的任务内容、任务间隔、所涉及的程序、所需的备件及执行维修工作所需的其他资源。示例如表 B.6 所示。

整个 RCM 过程都要全面详尽记录下来，以备将来参考和审查。收集与故障和维修相关的数据可以监测结果及其改进措施的执行情况。

B.8.5.2 用途

RCM 用于实现适用且有效的维修。通常应用于系统的设计和开发阶段，然后在运行和维护阶段实施。针对故障会对安全、环境、经济或操作产生严重影响的情况进行分析来获取最大利益。

在高危害性分析识别宜确定维修任务的设备和系统后，启动 RCM 程序。这可能发生在初始设计阶段，也可能发生在后期使用过程中(如果之前没有以结构化的方式完成，或是需要审查或改进维护)。

B.8.5.3 输入

RCM 的成功应用宜充分了解设备和结构、运行环境和相关系统、子系统和设备项目，以及可能的故障和故障后果。

该应用过程需要一个具备必要知识和经验的团队，并且由训练有素、经验丰富的人来控制。

B.8.5.4 输出

对是否需要执行维修任务或其他操作(例如更改操作)做出判断。

针对每种故障模式给出合适的故障管理策略，例如状态监控、故障查找、计划恢复、基于时间间隔(如日历、运行小时数或周期数)的更换或故障维修。能从分析中得出的其他可能行动，包括重新设计、更改操作或维护程序或额外培训。示例如表 B.6 所示。

制定计划以执行建议的维修任务。详细说明了执行维护任务所需的任务、任务间隔、涉及的程序、所需的备件和其他资源。

表 B.6　RCM 任务选择示例

功能故障-无法提供压缩机保护和停机							
设备	故障模式	故障间隔（小时）	故障检测	原因	任务类型	任务描述	以小时为单位的任务间隔
压力变送器-压缩机油压	输出不准确	80 000	明显	未校准	时间导向	检验校准	16 000
振动传感器-压缩机振动	无法提供正确的输出	40 000	明显	探测器/传感器故障	条件导向	若发生振动变化，请验证精度	在控制面板上连续不断
液位开关-低压缩机油位	无法按需更改状态	80 000	隐性	探测器/传感器故障	故障查找	液位开关功能测试	8 000
传感器和接线-压缩机油温	输出高	160 000	明显	开路	时间导向	检查连接是否松动	8 000
液位变送器-乙二醇罐	输出不准确	40 000	隐性	未校准	时间导向	在确认乙二醇填充水平之前先校准变送器	8 000
压力变送器-压缩机吸入/排出压力	输出不准确	80 000	明显	未校准	时间导向	检验校准	16 000
传感器和接线-压缩机吸入/排出温度	输出高	160 000	明显	开路	时间导向	检查连接是否松动	8 000
振动传感器-冷却器振动	无法提供正确的输出	40 000	明显	探测器/传感器故障	条件导向	若发生振动变化，请验证精度	在控制面板上连续不断

B.8.5.5　优势和局限

优势包括以下方面：

——可以利用风险的量级来做出维护决策；

——任务取决于它们是否适用，即它们是否会达到预期结果；

——能对任务进行评估以确保其具有成本效益且值得实施；

——能以适当的理由取消不必要的维护操作；

——过程和决策记录在案，有利于之后审查。

局限性包括以下方面：

——若要该过程发挥作用，需要花费大量时间；

——该过程非常依赖于训练有素且经验丰富的专业人员；

——团队必须具备所有必要的专业知识和维护经验，才能使决策有效；

——在过程中可能会有走捷径的倾向，从而影响决策的有效性；

——一些考虑在内的潜在任务会受到现有技术知识的限制（如状态监测技术）。

B.8.5.6 参考文件

[76] IEC 60300-3-11，Dependability management—Part 3-11：Application guide-Reliabilitycentred maintenance

B.8.6 风险指数

B.8.6.1 概述

风险指数提供了通过评分方法和顺序量表得出的风险度量。使用一种方程式来表示识别、评分影响风险大小的因素。在最简单的公式中，将增加风险水平的因素相乘，然后除以降低风险水平的因素。若有可能，量表及其组合方式要基于证据和数据。

重要的是，系统每个部分的分数在内部要保持一致并保持正确的关系。

数学公式不能应用于顺序量表。因此，一旦开发了评分系统，可将其应用于一个很好理解的系统来验证模型。

建立索引是一种迭代方式，宜尝试使用几个不同的系统来组合分数，以验证该方法。

B.8.6.2 用途

风险指数本质上是一种定性或半定量的方法，用于对风险进行排序和比较。可用于有限范围或扩展范围的内部或外部风险。它们通常针对的是特定类型的风险，用于比较不同的风险发生情况。虽然使用了数字，但这只是为了便于操作。在基础模型或系统不为人所知或无法表示的情况下，最好使用更明显的定性方法，该方法不意味着使用顺序量表无法达到的精度水平。

示例 1：考虑到风险因素与疾病之间的关联强度，疾病风险指数通过综合流行病学研究中确定的各种已知风险因素的得分，用于估计个人感染某种特定疾病的风险。

示例 2：从湿度、风力、景观干燥度和燃料负荷等预测条件，丛林火灾危险等级比较了不同日期的火灾风险。

示例 3：贷方使用代表其金融稳定性组成部分的指数来计算客户的信用风险。

B.8.6.3 输入

输入源于对系统的分析。这需要充分了解所有风险来源，以及后果会如何产生。

可以使用诸如 FTA(B.5.7)、ETA(B.5.6)和 MCA(B.9.5)等工具以及历史数据来支持风险指数的开发。

由于所采用的顺序量表在某种程度上是任意选择的，因此需要足够的数据来验证指数。

B.8.6.4 输出

输出是得出与特定风险相关的一系列数字（复合指数），可与同一系统内为其他风险制定的指数进行比较。

B.8.6.5 优势和局限

风险指数的优势：

——可以提供一个简单易用的工具来对不同的风险进行排名；

——可以将影响风险水平的多个因素合并到一个单一的数字分数中。

局限性包括以下方面：

——如果过程(模型)及其输出没有得到很好的验证,其结果可能毫无意义;
——输出的是风险的数值这一事实可能会被误解和误用,例如在随后的成本/收益分析中;
——在许多使用该指数的情景下,没有基本模型来定义风险因素的单个量表是线性、对数还是其他形式,也没有一个模型来确定如何将各种因素结合起来。在这些情况下,评级本质上是不可靠的,所以对真实数据的验证就尤为重要。
——通常很难获得足够的证据来验证量表。
——使用数值可能造成一种无法证明的准确程度。

B.8.6.6 参考文件

[77] MACKENZIECameronA.Summarizing risk using risk measures and risk indices

B.9 选项之间进行选择的技术

B.9.1 概述

B.9 中的技术可帮助决策者在涉及多种风险的选项和必须进行权衡的选项之间作出决定。这些技术有助于提供逻辑基础来证明决策理由。由于这些方法具有不同的理念,因此使用多种方法来研究选项是很有价值的。

基于预期财务损益的决策树分析和成本效益分析。允许对不同的准则进行加权和权衡的多标准分析。情景分析(见 B.2.5)也可用于探索不同的选择可能产生的后果。这种方法在不确定度高的情况下特别有效。决策问题也可以使用影响图(B.5.3)建模。

B.9.2 成本/收益分析(CBA)

B.9.2.1 概述

成本/收益分析以货币形式衡量选项的总预期成本与其总预期收益,以做出最有效或最有利益的选择。它可以是定性的,也可以是定量的,或者是定量和定性元素的组合,并且可以应用于组织的任何级别。

确定可能付出成本或获得收益(有形或无形)的利益相关者会被识别,以及每个利益相关者的直接和间接收益及成本。

注:直接成本是与行动直接相关的成本。间接成本指额外的机会成本,例如效用损失、管理时间的分散或资本从其他潜在投资转移。

在定量 CBA 中,货币价值被分配给所有有形和无形的成本和收益。若发生成本发生在短时间内(例如一年),而收益会持续很长时间的情况。则有必要对成本和收益进行折现,将它们变成“今天的钱”,以便在成本和收益之间进行有效的比较。所有利益相关者的所有成本现值(PVC)和收益现值(PVB)可以结合起来产生净现值(NPV):NPV=PVB−PVC。

正的 NPV 意味着该行动可能是一个合适的选择。NPV 最高的选项不一定是最有价值的选项。NPV 与成本现值的最高比率是最佳价值选项的有用指标。基于 CBA 的选择应与满意方案之间的战略选择相结合,满意方案可单独提供最低成本治疗、最高可承受效益或最佳价值(最有利润的投资回报)。在政策和操作层面都可能需要这种战略选择。

通过计算净收益的加权平均概率(预期净现值或 ENPV)可以考量成本和收益中的不确定性。在该计算中,假设用户对发生概率高的小收益和发生概率低的大收益不关心,只要两者具有相同的期望值。NPV 计算也可以与决策树(B.9.3)相结合,以模拟未来决策及其结果的不确定性。在某些情况下,可以推迟一些成本,直到获得有关成本和收益的更好信息。这样做可能有一个值,可以使用实物期权分析进行估计。

在定性CBA中，没有试图去寻找无形成本和收益的货币价值，也不是提供一个总结了成本和收益的单一数字，而是定性的考虑了不同的成本和收益之间的关系和权衡。

一种相关的技术是成本效益分析。假设需要某种利益或结果，并且有几种替代方法可以实现它。该分析仅着眼于成本，并试图确定实现效益的最廉价方式。

虽然无形价值通常是通过给予其货币价值来处理的，但也可以对其他成本应用加权系数，例如更重视安全利益而不是经济利益。

CBA的一个变体——成本/收益风险分析(CBRA)——则更加强调风险。CBA使用点或二进制分布，而CBRA的风险值也可以考虑负面和正面结果的全概率分布[78]。

B.9.2.2 用途

CBA可用于操作和战略层面，帮助决策者在选项之间作出决定。在大多数情况下，这些选择具有不确定性。在计算中宜考虑成本和收益的预期现值的可变性以及意外事件的可能性。因此可以运用敏感性分析或蒙特卡罗分析(B.5.10)。

CBA还可用于做出有关风险及其处理措施的决策，例如：

——为是否可处理风险提供建议；

——确定风险处理的最佳形式；

——比较长期和短期的处理方案。

B.9.2.3 输入

输入包括与利益相关者相关的成本和收益有关的信息以及这些成本和收益的不确定性信息。宜考虑有形和无形的成本和收益。成本包括可能消耗的任何资源，包括直接和间接成本、可归属的间接费用和负面影响。收益包括积极影响和成本规避(这可能是风险处理的结果)。已经支出的沉没成本不属于分析的一部分。简单的电子表格分析或定性讨论不需要大量工作，但应用于更复杂的问题时需要大量时间来收集必要的数据和估算无形资产的适当货币价值。

B.9.2.4 输出

成本/收益分析的输出是关于不同选择或行动的相对成本和收益的信息。这可以定量表示为净现值(NPV)、最佳比率(NPV/PVC)或收益现值与成本现值的比率。

定性输出的通常是比较不同类型成本和收益的成本和收益的表格，并注意权衡。

B.9.2.5 优势和局限

CBA的优势包括：

——CBA允许使用单一指标(通常是货币)来比较成本和收益；

——提供了用于决策的信息的透明度；

——鼓励收集有关该决定所有可能方面的详细信息(这在揭示无知和交流知识方面很有价值)。

局限性包括以下方面：

——CBA宜对可能的收益有充分的理解，因此它不适合具有高度不确定性的新场景。

——定量CBA可以产生截然不同的数字，这取决于给非经济和无形利益赋予经济价值的假设和方法。

——在某些应用中，很难为未来的成本和收益确定一个有效的贴现率。

——很难估计大量人口所获得的利益，特别是那些与不在市场上交换的公共品有关的利益。不过，当与“支付或接受意愿”相结合时，它就可以解释这些外部或社会利益。

——依赖于所选择的贴现率，贴现为现值的做法意味着在长期未来获得的收益对决策的影响可以

忽略不计，因此会阻碍长期投资。

——CBA 不能很好地处理成本和收益发生时间的不确定性或未来决策的灵活性。

B.9.2.6 参考文件

[79] The Green book, Appraisal and Evaluation in Central Government

[80] ANDOSEH, S., et al. The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects

B.9.3 决策树分析

B.9.3.1 概述

决策树对必须做出的初始决策(例如，是继续进行项目 A 还是项目 B)之后的可能路径进行建模。随着这两个假设项目的进行，可能会发生一系列事件，宜做出不同的可预测决策。这些以树格式表示，类似于事件树。事件发生的概率可以与每个路径最终结果的预期值或效用一起进行估计。

关于最佳决策路径的信息在逻辑上是会产生最佳期望值的信息，该值是路径上的所有条件概率与结果值的乘积。

B.9.3.2 用途

决策树可用于构建和解决序贯决策问题，当问题的复杂性增加时尤其有用。它使组织能够量化决策的可能结果，从而帮助决策者在结果不确定时选择最佳行动方案。图形显示还可以帮助传达决策原因。

决策树还可用于评估决策，通常对事件概率进行主观估计，并帮助决策者克服对成功或失败的固有认知偏见。它可用于操作或战略层面的短期、中期和长期问题。

B.9.3.3 输入

构建决策树需要一个项目计划，其中包含决策点、关于决策可能结果的信息以及可能影响决策的偶然事件。宜具备专业知识，特别是在复杂情况下。

根据树的构造，需要定量数据或充足的信息来证明专家对概率的意见。

B.9.3.4 输出

输出包括：

——决策问题的图形表示；

——计算每条可能路径的期望值；

——根据预期值或建议宜遵循的路径，列出可能结果的优先次序。

B.9.3.5 优势和局限

决策树分析的优势包括：

——为决策问题的细节提供了清晰直观的图形表示；

——开发树的练习可以提高对问题的洞察力；

——鼓励清晰的思考和规划；

——能够计算出一种情况下的最佳路径和及其预期结果。

局限性包括以下方面：

——大型决策树可能过于复杂，不利于沟通；

——树状图可能存在将情况过度简化的趋势；
——所依赖的历史数据可能不适用于所建模的决策；
——简化了决策问题，并将其离散化，从而导致了极值的消除。

B.9.3.6 参考文件

[81] KIRKWOOD Craig, Decision Tree Primer

B.9.4 博弈论

B.9.4.1 概述

B.9.4.1.1 总论

博弈论可以针对未来可能出现的多种情况，对不同可能决策的后果进行模拟。未来的情况可以由不同的决策者(例如竞争对手)或外部事件(例如技术或测试的成功或失败)决定。例如，假设任务是根据不同决策者(称为博弈者)在不同时间可能做出的不同决策来确定产品的价格。可以计算与相关时间段相关的参与博弈的每个博弈者的收益，并为每个玩家选择具有最佳收益的策略。博弈论也可用于确定其他参与者的信息价值或不同的可能结果(如技术的成功)。

有不同类型的博弈，例如合作/非合作、对称/非对称、零和/非零和、同时/序贯、完全信息和不完全信息、组合博弈、随机结果。

B.9.4.1.2 交流与合作/非合作博弈

一个重要的因素是博弈者之间的交流是否可能或被允许。如果玩家能够形成具有约束力的承诺，则该博弈是合作博弈。而在非合作博弈中，这种情况不可能发生。混合博弈包含合作和非合作元素。例如，在合作博弈中形成了玩家联盟，但这些联盟时以非合作的方式进行。

博弈者之间没有交流的博弈经典例子就是“囚徒困境”。它表明，在某些情况下，每个参与者不考虑其他人而改善自己结果的行为可能会给双方造成最糟糕的情况。这类博弈已被用于分析两个博弈者之间的冲突与合作，缺乏沟通可能会导致不稳定的情况，而这可能会给双方玩家带来最坏的结果。在囚徒困境博弈中，假设两个人一起犯罪。但他们被隔开，不能交流。警方提供了一个协议，如果每个囚犯都承认自己有罪并指证对方，他将获得较轻的刑罚，但另一个囚犯将被判重刑。如果一个囚犯不坦白和指证，但是另一个囚犯做了，那么前者将受到最大的处罚。因此，为了改善他们的处境，双方都试图坦白和指证，但在这种情况下，他们都将受到最高的处罚。他们最好的方法就是拒绝协商并且不承认任何事情。在这种情况下，双方都将获得最低处罚。

B.9.4.1.3 零和/非零和对称/非对称博弈

在零和博弈中，一个玩家得到什么，另一个玩家就会失去什么。在非零和博弈中，结果的总和可能随决策而变化。例如，降低价格可能会使一个参与者的成本高于另一个参与者，但可能会增加两者的市场容量。

B.9.4.1.4 同时博弈与序贯博弈

在某些博弈中，只针对博弈者之间的一次互动进行计算。但在序贯博弈中，玩家会进行多次交互，并且可能会在一个博弈到下一个博弈之间改变他们的策略。

例如，已经开展了模拟博弈调查作弊在市场中的影响。每个博弈者有两种可能。供应商可以交付或不交付，客户可以付款或不付款。可能会出现四种情况，正常情况是双方都能收益(供应商及时交付，客户正常付款)。供应商未交付，客户未付款，这种情况会引起机会丢失。最后两种可能性是供应商

(客户不付款)或客户(供应商不交付)的损失。通过模拟得出各种不同的策略,例如始终保持诚实、一直作弊或随机作弊。已确定的最佳策略是在第一次互动中保持诚实,在下一次互动中根据其他交易方上次的表现来做出行动判断(诚实或作弊)。

注:在实际情况中,供应商很可能会识别出作弊的客户并停止与他们交易。

B.9.4.2 用途

博弈论允许在以下情况中做出风险评估,例如许多决策结果取决于另一个博弈者(如竞争对手)的行为,或取决于许多可能的结果(如新技术是否可行)。下面的例子说明了可以通过博弈分析获得信息。

表 B.7 说明该公司可以选择三种不同技术,但利润将取决于竞争对手的行动(行动 1、2 或 3)。竞争对手采取什么行动不得而知,但其采取各种行动的概率能被估计。表格中利润以百万为货币单位(MU)计算。

表 B.7 博弈矩阵示例

	竞争者			预期利润	担保利润	最大的回归
	行动一	行动二	行动三			
概率	0.4	0.5	0.1			
技术一	0.10	0.50	0.90	0.38	0.10	0.50
技术二	0.50	0.50	0.50	0.50	0.50	0.40
技术三	0.60	0.60	0.30	0.57	0.30	0.60

可以通过表格得出以下信息来支持该决定。

显然技术三是最优,预期利润为 57 万 MU。宜考虑竞争对手行动的敏感性。担保利润一栏说明了独立于竞争对手的给定技术利润。此处表明技术二最优,保证利润为 50 万 MU。宜考虑是否值得选择仅能获得 7 万 MU 的技术三,同时冒着损失 20 万 MU 的风险。

还需要进一步计算可能出现的最大回归,即选择给定技术的利润与已知竞争对手行为利润之间的差异。这样通过对竞争对手决策的了解而带来了货币收益。

这可以通过谈判或其他法律手段来实现。在这个例子中,技术三的增量信息价值最大。

B.9.4.3 输入

要实现完全定义,一个博弈宜至少确定以下元素作为输入元素:

——博弈的参与者或替代者;

——每个参与者在每个决策点可用的信息和行动。

B.9.4.4 输出

输出是博弈中每个选项的收益,通常用来表示单个参与者的效用。在建模情况下,收益代表货币,但其他结果也可能出现(例如,市场份额或项目延迟)。

B.9.4.5 优势和局限

博弈论的优势包括以下几点:

——开发了一个包含多种可能决策的分析决策的框架,但结果取决于另一个参与者的决策或未来事件的结果;

——开发了一个考虑到不同组织所作决定的相互依赖性的分析决策框架;

——提供了几个鲜为人知的概念见解，这些概念出现在利益冲突的情况下，例如，描述和解释了讨价还价和结盟的现象；

——至少在两个组织的零和博弈中，博弈论概述了一种科学的量化技术，参与者可以加以利用得出最佳策略。

局限性包括以下方面：

——假设博弈者了解自身收益，而其他人的行为和收益可能不切实际；

——解决涉及混合策略的博弈技术（特别是在大收益矩阵的情况下）非常复杂；

——不是所有的竞争问题都可以借助博弈论来分析。

B.9.4.6 参考文件

[82] MYERSON，ROGERB.，Game Theory：Analysis of Conflict

[83] MARYNARD，SMITHJOHN，Evolution and Theory of Games

[84] ROSENHEAD，J.and MINGER，J.（Eds），Rational Analysis for a Problematic World Revisited

B.9.5 多标准分析（MCA）

B.9.5.1 概述

MCA 使用一系列标准对一组选项的整体性能进行透明地评估和比较。通常，目标是生成一组选项的优先顺序。该分析涉及开发一个选项和标准矩阵，通过对矩阵排序和汇总，得出每个选项的总分。这些技术也称为多属性或多目标决策。这种技术有许多变体，可支持许多软件应用程序。

通常情况下，个人或一群知识渊博的利益相关者会完成以下流程：

——定义目标；确定与每个目标相关的属性（标准或功能绩效措施）；

——将属性构造为必要的有理想要求的层次结构；

——确定每个标准的重要性并为每个标准分配权重；

——在加权层次结构上获得利益相关者的共识；

——根据标准评估备选方案（这可以表示为分数矩阵）；

——将多个单属性分数组合成一个整体加权的多属性分数；

——评估每个选项的结果；

——通过执行敏感性审查来评估更改属性层次权重，从而评估选项排名的可靠性。

可以通过不同的方法得出每个标准的权重，以及将每个选项的标准分数加权为单个多属性分数的不同方法。例如，分数可以加权为总和或乘积或使用层次分析流程（一种基于成对比较的权重和分数的激发技术）。所有这些方法都假设对任何一个标准的偏好不依赖于其他标准值。如果此假设无效，则使用不同的模型。

由于分数呈主观性，敏感性分析对于检查权重和分数影响选项之间整体偏好的程度很有用。

B.9.5.2 用途

MCA 可用于：

——比较多个选项以进行首次分析确定首选项和不合适的选项；

——比较存在多个且有时相互冲突的标准的选项；

——在不同利益相关者的目标或价值观存在冲突的情况下，就决策达成共识。

B.9.5.3 输入

输入是一组基于目标的分析和标准选项，可用于评估选项的性能。

B.9.5.4 输出

结果可以表示为：

——呈现最优到最不喜欢的选项排名顺序；

——一个矩阵，其中矩阵的轴是标准权重和每个选项的标准分数。

以矩阵形式呈现结果允许剔除不符合高加权标准或不符合必要标准的选项。

B.9.5.5 优势和局限

MCA 的优势包括：

——为有效的决策制定、假设和结论的呈现提供简单的结构；

——制定更易于管理的复杂决策问题，这些决策问题不适合成本/收益分析；

——帮助理性考虑宜权衡的问题；

——当利益相关者有不同的目标并因此有不同的价值观和标准时，能够帮助利益相关者达成一致。

局限性包括以下方面：

——MCA 可能会受到偏见和决策标准选择不当的影响。

——加权算法根据明确的偏好或加权不同的观点来计算标准权重，可能会模糊决策的真实基础。

——评分系统可能会过度简化决策问题。

B.9.5.6 参考文件

[85] EN 16271:2012, Value management-Functional expression of the need and functionalperformance specification—Requirements for expressing and validating the need to besatisfied within the process of purchasing or obtaining a product

注：EN 16271:2012 规定了协调冲突利益相关者需求的方法、可用于导出功能性能要求方法，以及在比较选项之前设置多标准分析粒度指南。

[86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, Multi-criteria analysis: a manual 2009

[87] RABIHAHMHD.SUM(2001), Risk Management Decision Making

[88] VELASQUEZ, M., HESTER, P. An Analysis of Multi-criteria Decision Making Methods

B.10 记录和报告技术

B.10.1 概述

B.10 涵盖了用于报告和记录有关风险的一般信息的技术。6.6 中涵盖了对详细报告的要求。

报告和记录风险信息的常用方法是在风险登记册中输入每个风险的基本信息，例如电子表格或数据库(见 B.10.2)。与传统风险登记册登记内容相比，某些风险可能需要更复杂的描述。例如，描述可能需要包括导致单个事件的多个风险来源、单个事件或来源产生的多种可能结果、连锁效应和潜在的控制失效。领结图是一种用于组织和传达此类信息的工具示例(见 B.4.2)。

有关风险程度的信息可以通过多种不同方式进行报告。最常用的方法是使用后果/可能性矩阵(见 B.10.3)。除了由矩阵中位置显示的可能性、后果和风险水平外，还可以通过标记风险点的大小或其颜色提供额外信息，例如控制的性质、已实施的处理程度等。

后果/可能性矩阵要求风险可以由单个后果/可能性组合表示。如果不是这种情况，风险有时可以用概率分布函数或累积分布函数表示(见 B.10.4)。

B.10.2 风险登记表

B.10.2.1 概述

风险登记表汇集了有关风险的信息，以告知面临风险的人和负责管理风险的人。它可以是纸质或

数据库格式，通常包括：

——风险的简短描述（例如名称、后果和导致后果的事件顺序等）；

——关于后果发生可能性的声明；

——风险的来源或原因；

——目前正在采取什么措施来控制风险。

风险可以分为不同的类别进行报告（B.2.2）。

风险通常作为单独的事件单独列出，但宜标记相互依存关系。

在记录有关风险的信息时，宜明确风险（可能发生事情的潜在影响）和风险源（如何或为什么会发生）和可能失败的控制之间的区别。指示事件可能即将发生的早期预警信号效果很好。

许多风险登记表还包括对风险重要性的一些评级、风险是否被认为是可接受或可容忍的指示，或者是否需要进一步处理以及做出此决定的原因。如果根据后果及其可能性对风险应用重要性评级，则宜考虑控制失败的可能性。不宜给控制失败分配风险级别，宜将其视为作独立风险。

具有正面后果的风险可以与具有负面后果的风险记录在同一文件中或单独记录。机会（即可以利用的情况或想法而不是偶然事件）通常进行单独记录，并以考虑成本、收益和任何潜在负面后果的方式进行分析。有时可以称为价值和机会登记表。

B.10.2.2 用途

风险登记表用于记录和跟踪有关个人风险及其控制方式的信息。它可用于向利益相关者传达有关风险的信息，并突出特别重要的风险。它可用于跟踪公司、部门、运营和项目等不同级别众多风险的控制和处理。来自风险登记册的信息可以进行整合以提供给最高管理层。

风险登记表可用作跟踪应对措施实施情况的基础，因此可以包含有关措施及其实施方式的信息，或参考其他文件或包含此信息的数据库。（此类信息可以包括风险所有者、行动、行动所有者、行动业务案例摘要、预算和时间表等）。在某些情况下，可以强制要求做出一种形式的风险登记册。

B.10.2.3 输入

风险登记表的输入通常是风险评估技术的输出，如 B.1 至 B.4 所述，并辅以失败记录。

B.10.2.4 输出

输出是关于风险的信息记录和报告。

B.10.2.5 优势和局限

风险登记表的优势包括以下内容：

——有关风险的信息以一种可以识别和跟踪所需行动的形式汇集在一起；

——关于不同风险的信息以一种可比较的格式呈现，这可用来指示优先级，并且比较容易查询；

——风险登记表的构建通常涉及许多人，宜提高对风险管理必要性的普遍认识。

局限性包括以下内容：

——风险登记表中捕获的风险通常基于事件，这使得难以准确描述某些形式的风险（见 4.2）；

——表面上的易用性可能会给信息带来错误的置信度，因为很难一致地描述风险，而且人们经常将风险的来源、风险本身和风险控制的弱点混淆；

——描述风险的方式有很多种，任何分配的优先级将取决于描述风险的方式和问题的分解程度；

——宜付出极大的努力才能确保风险登记册保持最新（例如，所有提议的应对措施一旦列出就应列为当前控制措施，新风险宜不断添加，并删除不再存在的风险）；

——风险通常单独记录在风险登记表中，这令整合信息以制定整体应对计划变得困难。

B.10.2.6 参考文件

没有此技术的参考文件。

B.10.3 后果/可能性矩阵(风险矩阵或热图)

B.10.3.1 概述

后果/可能性矩阵(也称为风险矩阵或热图)是一种根据风险的后果和可能性来显示风险并结合这些特征来显示风险重要性评级的方法。

后果和可能性定义为矩阵的轴。量表可以有任意数量的点——最常见的是三、四或五点量表——并且可以是定性、半定量或定量的形式。如果用数字描述定义量表,它们宜与现有数据一致,并给出相应单位。一般来说,为了与数据保持一致,两个尺度上的每个尺度点都需要比之前的一个大一个数量级。

结果量表(或多个量表)可以描述积极或消极的后果。量表可与组织的目标直接相关,并且宜从最大的可信结果扩展到最低的利益结果。图 B.15 显示了不利后果的部分示例。

评分	经济	健康和安全	环境和社区	等等
a	最大可信损失 ($)	多次致命	不可逆转的重大伤害;社区愤怒	
b	⋮	⋮	⋮	⋮
c	⋮	⋮	⋮	⋮
d	⋮	⋮	⋮	⋮
e	最低利息 ($)	只需要急救	轻微的临时损坏	

图 B.15 定义后果等级表的部分示例

注:由于部分示例的使用,因此不能直接使用这些示例来强调宜始终自定义比例。

根据上下文,可以使用更多或更少的结果类别,并且量表可以具有少于或多于五个点。结果评级栏可以填写单词、数字或字母。

可能性量表宜涵盖与要评级风险数据相关的范围。图 B.16 显示了一个可能性量表的部分示例。

评分	描述符	描述符含义
5	可能	预计在数周内发生
4	⋮	⋮
3	⋮	⋮
2	⋮	⋮
1	不太可能	理论上可能,但实际上极不可能

图 B.16 可能性量表的部分示例

可能性评定量表的分数可能多于或少于 5 分,评分可以使用单词、数字或字母表示。

可能性量表宜根据情况量身定制,可能需要涵盖不同范围的积极或消极结果。在某种低可能性下可容忍,那么在可能性量表上的最低步骤宜代表最高定义的结果接受的可能性(否则,所有具有最高结

果的活动都被定义为不可容忍的，也不能使其成为可容忍的）。在确定单个结果高风险的可容忍可能性时，可考虑多种风险可能导致相同后果的事实。

绘制一个矩阵，其结果在一个轴上，可能性在另一个轴上对应于定义的尺度。可以将优先评级链接到每个单元格。此处提供的示例中有五个优先级，用罗马数字表示。通常，将单元格着色以指示风险的大小。决策规则（例如管理层的关注程度或响应的紧迫性）可以与矩阵单元格相关联。这些将取决于量表的定义和组织对风险的态度。设计宜使风险的优先级基于风险导致的结果超出组织为其目标定义的绩效阈值。

矩阵可以设置为对结果（如图 B.17 所示）或可能性给予额外的权重，也可以呈对称性，具体情况取决于应用程序。

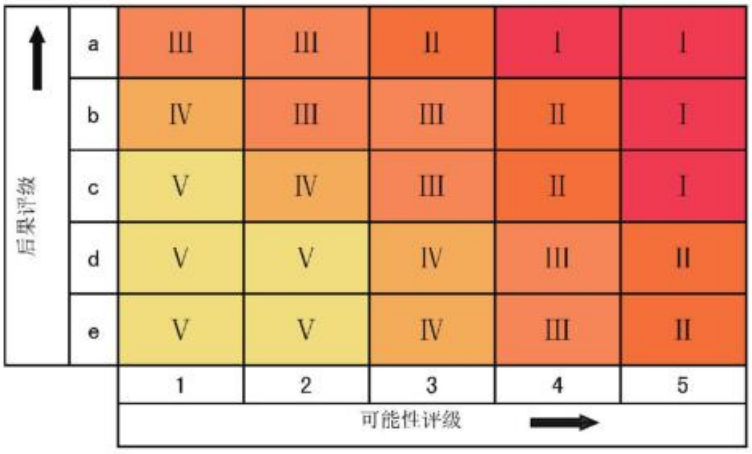

图 B.17　结果/可能性矩阵示例

B.10.3.2　用途

结果/可能性矩阵可用于评估和沟通风险的相对大小，其基础通常与重点事件的后果/可能性匹配相关。

为了对风险进行评级，用户首先宜找到最适合情况的结果描述符，然后定义认为出现结果的可能性。在组合这些值的框内设定一个点，并从矩阵中读取风险级别和相关的决策规则。

潜在的高风险结果通常是决策者最关心的问题，即使出现可能性非常低，但其频繁程度所带来的低风险也可能会造成过多累积或者形成长期结果。如有必要可以分析这两种风险，因为其相关的风险处理方式可能大不相同。

如果一个事件可能产生一系列不同的结果值，则任何特定结果的可能性将不同于产生该结果事件的可能性。通常使用指定结果的可能性。在所有比较的风险中应对可能性的解释和使用方式宜保持一致。

该矩阵可用于比较具有不同类型潜在结果的风险，并适用于组织的任何级别。当已识别出许多风险时，它通常用作筛选工具，例如定义哪些风险需要提交给更高级别的管理人员。它还可用于帮助确定给定的风险是否能够被广泛接受，或者根据它在矩阵上所处的区域是不可接受的。它可以用于缺乏足够数据做详细分析的情况，或者不需要时间和精力进行更详细或定量分析的情况。一种形式的结果/可能性矩阵可用于 FMECA（B.2.3）中的关键性分析或根据 HAZOP（B.2.4）或 SWIFT（B.2.6）设置优先级。

B.10.3.3　输入

宜开发一个结果/可能性矩阵以适应上下文。这需要一些可用的数据来建立真实的量表。矩阵草

案宜进行测试，以确保矩阵建议的行动与组织对风险的态度相匹配，并且用户正确理解了量表的应用。

使用矩阵需要人们（最好是一个团队）了解被评级的风险以及可用于帮助判断后果及其可能性的数据。

B.10.3.4 输出

输出是一个显示，说明了不同风险的相关结果可能性和风险水平以及每个风险的重要性评级。

B.10.3.5 优势和局限

优势包括以下方面：

——比较容易使用；

——提供了将风险快速分级为不同重要级别的方法；

——按风险的结果、可能性或水平，清晰直观地显示了风险的相关重要性；

——可用于比较具有不同结果类型的风险。

局限性包括以下方面：

——需要良好的专业知识去设计有效的矩阵；

——定义适用于与组织相关的一系列环境通用量表有一定难度；

——很难明确地定义尺度以使用户能够加权结果和可能性保持一致；

——风险评级的有效性取决于量表的开发和校准情况；

——需要一个单一的指示值来定义结果，而在许多情况下，结果值的范围有多种可能，风险的排名取决于自己的选择；

——准确校准的矩阵将涉及非常低的可能性水平的个体风险，难以概念化；

——方法的使用是非常主观的，不同的人通常对相同的风险分配持有不同的评级。这使它容易受到操纵；

——风险不能直接加权（例如，不能定义特定数量的低风险，或识别特定次数的低风险是否等同于中等风险）。

——很难将不同类别结果的风险水平进行合并或比较；

——有效的排名需要使用一致的风险公式（这很难实现）；

——每个评级将取决于描述风险的方式和给出的详细程度（即识别越详细，记录的场景数量越多，每个情景的可能性越低）。在描述风险时将情景组合在一起的方式宜保持一致，并在排名之前给出定义。

B.10.3.6 参考文件

[89] ELMONSTRI，Mustafa，Review of the strengths and weaknesses of risk matrices

[90] BAYBUTT，Paul，Calibration of risk matrices for process safety

B.10.4 S 曲线

B.10.4.1 概述

如果风险可能具有一系列结果值，可以显示为结果的概率分布（PDF）。例如，参见图 B.18 中的立体曲线。数据也可以绘制为累积分布（CDF），有时称为 S 曲线（图 F.18 中的虚线）。PDF 可以是参数化或非参数化。

结果超过特定值的概率可以直接从 S 曲线中读取。例如，图 B.18 表明结果有 90% 的概率不会超过结果值 C。

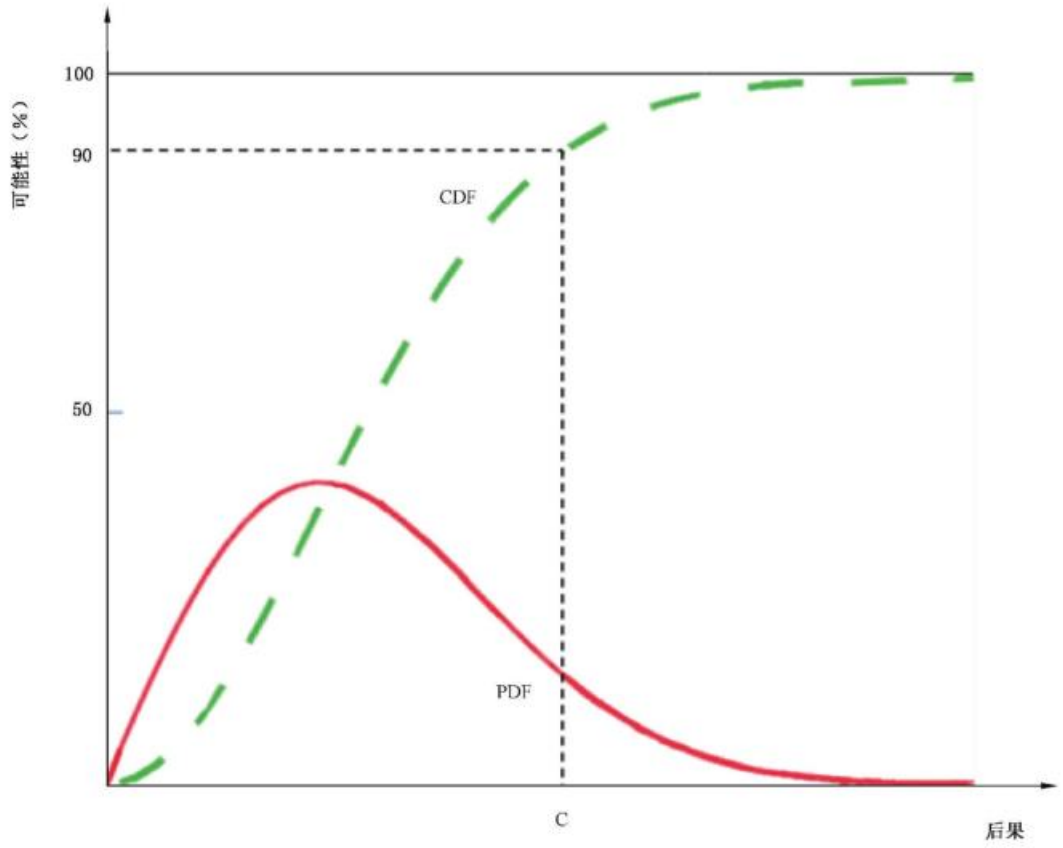

图 B.18　概率分布函数和累积分布函数

在某些情况下，分布的形状在理论上是已知的。在其他情况下，分布的形状可以从数据中获得，或者是通过模型输出。

也可以经过专家判断来估计结果范围的低点、可能出现的中间点和最高点。然后可以使用多种公式来确定结果和方差的平均值，并且可以根据这些信息绘制一条曲线。

B.10.4.2　用途

pdf 以视觉形式表示不同结果值的概率，能够显示最可能的值、可变化的程度以及发生极端事件可能性的程度。

在某些情况下，从概率分布中获取单个代表值可能很有用，例如与评估准则进行比较。通常，期望值（相当于平均值）最适合用于表示对结果大小的估计。（这相当于曲线所表示的概率和结果的乘积之和）其他度量包括分布的方差或某个百分位范围，例如四分位间距（由第 25 个和第 75 个百分位数包围的尺度宽度）或第 5 个和第 95 个百分位数（例如参见 VaR B.7.2）。然而，这些措施可能仍然没有充分强调极端结果的可能性，而这对做出的决定可能至关重要。例如，在选择投资时，既要考虑预期收益，也要考虑收益的波动；在规划如何应对火灾时，宜考虑极端事件以及预期后果。

在讨论代表可接受风险的结果值时，S 曲线是一项有效的工具。它是一种呈现数据的方式，可以更容易地看出结果超过特定值的概率。

B.10.4.3　输入

生成 S 曲线需要数据或判断，从中可以生成有效的分布。虽然通过判断可以用很少的数据来产生分布，但可用的数据越多，分布的有效性和从中获得的统计数据就会越大。

B.10.4.4 输出

输出是决策者在考虑风险可接受性时可以使用的图表，以及可以与准则进行比较分布的各种统计数据。

B.10.4.5 优势和局限

优势包括以下方面：

——该技术表示存在后果分布风险的大小；

——专家通常可以判断结果的最大值、最小值和最可能的值，并对可能的分布形状做出合理的估计。将其转换为累积分布的形式使非专业人士更容易使用此信息。随着更多可靠输入数据使用率的提高，S 曲线的准确性也会提高。

局限性包括以下方面：

——该方法给人留下非常准确的印象，但这种印象无法通过生成分布的数据确定性水平加以证明；

——对于获得一个或多个点值来表示结果分布的任何方法，都存在以下基本假设和不确定性：

- 分布的形式（例如正态、离散或高度偏态）；
- 将该分布表示为点值的最恰当方式；
- 由于派生数据的固有不确定性，点估计值也无法确定。

——基于经验或过去数据的分布及其统计仍然较少提供未来事件发生可能性的信息，这些事件具有极端结果但发生可能性很小。

B.10.4.6 参考资料

[91] GARVEY, P., BOOKS. A., COVERTR. P. Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective

参 考 文 献

总体参考

[1] Principe "GAME" (Globalement au moins équivalent) Methodologie de demonstration, Les guides d'application. Systèmes de transport public guidés urbains de personnes.2011

[2] FEKETE ISTVAN, Integrated Risk Assessment for supporting Management decisions Scholars Press, Saarbrücken, Germany 2015

[3] PEACE, C. The reasonably practicable test and work health and safety-related risk assessments New Zealand Journal of Employment Relations. 2017, 42(2), 61-78.

征求利益相关者和专家意见的技术

[4] EN 12973, Value Management

[5] PROCTOR, A. Creative problem solving for managers. Abingdon: Routledge

[6] GOLDENBERG, Olga, WILEY, Jennifer. Quality, conformity, and conflict: Questioning the assumptions of Osborn's brainstorming technique, The Journal of Problem Solving. 2011, 3 (2), 96-108 [viewed 2019-02-13] available at: http://docs. lib. purdue. edu/cgi/viewcontent. cgi?article=1093&context=jps

[7] ROWE, G. WRIGHT, G. The Delphi technique: Past, present, and future prospects. Technological forecasting and social change 2011, 78, Special Delphi Issue

[8] MCDONALD, D. BAMMER, G. and DEANE, P. Research Integration Using Dialogue Methods, ANU press Canberra. 2009 Chapter 3 Dialogue methods for understanding a problem: integrating judgements. Section 7 Nominal Group Technique [viewed 2019-02-13]. Available at http://press.anu.edu.au/node/393/download

[9] HARRELL, M.C. BRADLEY, M.A. 2009, Data collection methods-A training Manual-Semi structured interviews and focus groups, RAND National defence research Institute USA [viewed 2019-02-13]. Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf

[10] GILL, J. JOHNSON, P. Research methods for managers 4th ed. 2010 London: Sage Publications Ltd

[11] SAUNDERS, M. LEWIS, P. THORNHILL, A. 2016, Research Methods for BusinessStudents7th ed. 2016 Harlow: Pearson Education Ltd.

[12] UNIVERSITY OF KANSAS COMMUNITY TOOL BOX Section 13 Conducting surveys: [viewed 2019-02-13]. Available at: https://ctb. ku. edu/en/table-of-contents/assessment/assessing-community-needs-andresources/conduct-surveys/main

风险识别的技术

[13] MATHERLY, Carter The Red Teaming Essential: Social Psychology Premier for Adversarial Based Alternative Analysis. 2013 [viewed 2019-02-13]. Available at: https://works. bepress. com/matherly/6/download/

[14] Pestle analysis Free Management eBooks [viewed 2019-02-13]. Available at: http://www.free-management-ebooks.com/dldebk/dlst-pestle.htm

[15] POPOV, G., LYON, B., HOLLCROFT, B., Risk Assessment: A Practical Guide to

Assessing Operational Risks. Hoboken, NJ: Wiley, 2016

[16] IEC 62740, Root cause analysis (RCA)

[17] BROUGHTON, Vanda. Essential classification. Facet Publishing 2015

[18] BAILEY, Kenneth. Typologies and taxonomies: An introduction to classification technique. Quantitative applications in the social sciences Series 7,102 1994 Sage publications

[19] VDI 2225 Blatt 1,Konstruktionsmethodik—Technisch-wirtschaftliches Konstruieren—Vereinfachte Kostenermittlung, 1997 Beuth Verlag

[20] IEC 60812, Failure modes and effects analysis (FMEA and FMECA)

[21] IEC 61882,Hazard and operability studies (HAZOP studies)—Application guide

[22] RINGLAND, Gill. Scenarios in business, Chichester: John Wiley, 2002

[23] Van der HEIJDEN, Kees. Scenarios: The art of strategic conversation, Chichester: JohnWiley, 2005

[24] CHERMACK, Thomas J. Scenario planning in organizations, San Francisco: Berrett Koehler publishers Inc. 2011

[25] MUKUL PAREEK, Using Scenario analysis for managing technology risk: [viewed 2019-02-13]. Available at: http://www.isaca.org/Journal/archives/2012/Volume-6/Pages/Using-Scenario-Analysis-for-Managing-Technology-Risk.aspx

[26] CARD, Alan J. WARD, James R. and CLARKSON, P. John. Beyond FMEA: The structured what-if technique (SWIFT) Journal of Healthcare Risk Management, 2012,31, (4) 23-29

确定风险源、原因和驱动因素的技术

[27] KERVERN, G-Y. Elements fondamentaux des cindyniques, Editions Economica 1995

[28] KERVERN, G-Y. Latest advances in cindynics, Editions Economica,1994

[29] KERVERN, G-Y. & BOULENGER, P. Cindyniques—Concepts et mode d'emploi, Edition Economica 2007

[30] ISHIKAWA, K. Guide to Quality Control, Asia Productivity Organization, 1986

控制分析技术

[31] LEWIS, S. SMITH, K., Lessons learned from real world application of the bow-tie method. 6th AIChE. Global Congress of Process Safety, 2010, San Antonio, Texas [viewed 2019-02-13]. Available at: http://risktecsolutions.co.uk/media/43525/bowtie%20lessons%20learned%20-%20aiche.pdf

[32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. Managing safety barriers and controls at the workplace. In Probabilistic safety assessment and management. Editors SPITZER C, SCHMOCKER, U, DANG VN, Berlin: Springer; 2004.pp. 608-13

[33] MCCONNELL, P. and DAVIES, M. Scenario Analysis under Basel II. [viewed 2019-02-13]. Available at http://www.continuitycentral.com/feature0338.htm

[34] ISO 22000,Food safety management systems—Requirements for any organization in the food chain

[35] Food Quality and Safety Systems-A Training Manual on Food Hygiene and the Hazard Analysis and Critical Control Point (HACCP) System [viewed 2019-02-13]. Available at http://www.fao.org/docrep/W8088E/w8088e05.htm

[36] IEC 61508(allparts),Functional safety of electrical/electronic/programmable electronic-

safety-related systems

[37] IEC 61511(allparts),Functional safety—Safety instrumented systems for the processindustry sector

[38] CENTRE FOR CHEMICAL PROCESS SAFETY OF THE AMERICAN INSTITUTE OF CHEMICAL ENGINEERS New York 2001. Layer of protection analysis-Simplified process risk assessment

理解后果和可能性的技术

[39] GHOSH, J., DELAMPADY, M. 和 SAMANTA, T. An introduction to Bayesian analysis, New York Springer-Verlag, 2006

[40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. Prior Distribution Elicitation. In: Encyclopaedia of Statistics in Quality and Reliability. Wiley. 2008 ISBN 9780470018613

[41] NEIL, Martin andFENTON, Norman. Risk Assessment and Decision Analysis with Bayesian Networks CRC Press, 2012

[42] JENSEN, F. V., NIELSENT. D. Bayesian Networks and Decision Graphs, 2nd ed. Springer, New York, 2007

[43] NICHOLSON, A., WOODBERRYO 和 TWARDYC, The "Native Fish" Bayesian networks. Bayesian Intelligence Technical Report 2010/3, 2010

[44] NETICA TUTORIAL Introduction to Bayes Nets: What is a Bayes Net? [viewed 2019-02-13]. Available at https://www.norsys.com/tutorials/netica/secA/tut_A1.htm

[45] ISO TS 22317,Societal security—Business continuity management systems—Guidelines for Business Impact Analysis(BIA)

[46] ISO 22301,Societal security—Business continuity management systems—Requirements

[47] ANDREWS J. D, RIDLEY L. M. 2002. Application of the cause-consequence diagram method to static systems, Reliability engineering and system safety 75(1) 47-58; also at https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/695/1/01-22.pdf[viewed 2019-02-13]

[48] NIELSEN D.S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis, Danish Atomic Energy Commission, RISO-M-1374, May 1971

[49] IEC 62502,Analysis techniques for dependability—Event tree analysis

[50] IEC TR 63039, Probabilistic risk analysis of technological systems—Estimation of finalevent rate at a given initial state

[51] IEC 61025,Fault tree analysis (FTA)

[52] BELL Julie, HOLROYD Justin, Review of human reliability assessment methods. Healthand Safety Executive UK, HMSO 2009, [viewed 2019-02-13]. Available at: http://www.hse.gov.uk/research/rrpdf/rr679.pdf

[53] OECD Establishing the Appropriate Attributes in Current Human Reliability Assessment-Techniques for Nuclear Safety, NEA/CSNI/R 2015 [viewed 2019-02-13] Available at: http://www. oecd. org/officialdocuments/publicdisplaydocumentpdf/? cote = NEA/CSNI/R (2015) 1&-docLanguage=En

[54] IEC 61165,Application of Markov techniques

[55] OXLEY, ALAN. Markov Processes in Management Science, published by Applied Probability Trust, 2011 [viewed 2019-02-13]. Available at: https://studylib. net/doc/8176892/markov-

processes-in-management-science

[56] ISO/IEC Guide 98-3:2008/Suppl 1: Uncertainty of measurement—Part 3: Guide to theexpression of uncertainty in measurement (GUM 1995)—Propagation of distributionsusing a Monte Carlo method

[57] EU: General Data Protection Regulation (European Union Official Journal, 04.05.2016)

[58] ICO (UK): Conducting privacy impact assessments code of practice [viewed 2019-02-13] Available at:

https://ico.org.uk/media/about-the-ico/consultations/2052/draftconducting-privacy-impact-assessments-code-of-practice.pdf

[59] CNIL (FR), Privacy Impact assessment (PIA) [viewed 2019-02-13]. Available at: https://www.cnil.fr/en/privacy-impact-assessment-pia

分析依赖和交互的技术

[60] BRYSON, J. M., ACKERMANN, F., EDEN, C., & FINN, C. (2004). Visible thinking unlocking causal mapping for practical business results. Chichester: John Wiley & Sons

[61] ACKERMANN, F, HOWICK, S, QUIGLEY, J, WALLS, L, HOUGHTON, T. Systemic risk elicitation: Using causal maps to engage stakeholders and build a comprehensive view of risks, European Journal of Operational Research 2014, 238(1), 290-299

[62] JOINT RESEARCH CENTRE, EUROPEAN COMMISSION, Cross-impact analysis [viewed 2019-02-13] Available at: http://forlearn.jrc.ec.europa.eu/guide/2_design/meth_cross-impact-analysis.htm

[63] WORLD HEALTH ORGANISATION Human health risk assessment toolkit-chemical hazards. 2010 [viewed 2019-02-13]. Available at: http://www.inchem.org/documents/harmproj/harmproj/harmproj8.pdf

[64] US EPA Guidelines for ecological risk assessment 1998 [viewed 2019-02-13]. Available at https://www.epa.gov/sites/production/files/2014-11/documents/eco_risk_assessment1998.pdf

[65] CHANCE, D., BROOKS, R. An introduction to derivatives and risk management, (9th ed.). Published Mason, Ohio: South-Western Cengage Learning 2013

[66] THOMASJ.and PEARSONNeilD.Value at risk. Financial Analysts Journal 2000 56,47-67

[67] CHOUDHRY , M. An introduction to Value at Risk, Ed. 5, John Wiley and Sons,Chichester UK, 2013

[68] Value at Risk. New York University. [viewed 2017-9-14]. Available at: http://people.stern.nyu.edu/adamodar/pdfiles/papers/VAR.pdf

评价风险重要性技术

[69] UK HEALTH AND SAFTY EXECUTIVE, 2010a: HID'S Approach To'As Low As Reasonably Practicable' (ALARP) Decisions [viewed 2019-02-13] available at: http://www.hse.gov.uk/risk/theory/alarpglance.htm

[70] UK HEALTH AND SAFTY EXECUTIVE, 2010b: Guidance on (ALARP) decisions in control of major accident hazards (COMAH), [viewed 2019-02-13] available at: http://www.hse.gov.uk/foi/internalops/hid_circs/permissioning/spc_perm_37/

[71] UK HEALTH AND SAFTY EXECUTIVE, 2014: Principles and guidelines to assist HSE in its judgments that duty-holders have reduced risk as low as reasonably practicable [viewed

2019-02-13] available at: http://www.hse.gov.uk/risk/theory/alarp1.htm

[72] AMERICAN INSTITUTE FOR CHEMICAL ENGINEERS: Understanding and using F-N Diagrams: Annex A in Guidelines for Developing Quantitative Safety Risk Criteria. New York. John Wiley 2009

[73] EVANS, A. Transport fatal accidents and FN-curves: 1967-2001. Health and Safety Executive Research Report RR 073 [viewed 2019-02-13]. Available at: http://webarchive.nationalarchives.gov.uk/20101111125221/http://www.railreg.gov.uk/upload/pdf/rr073.pdf

[74] Pareto Chart, Excel Easy [viewed 2019-02-13]. Available at: http://www.exceleasy.com/examples/pareto-chart.html

[75] Pareto Chart [viewed 2019-02-13]. Available at: http://www.uphs.upenn.edu/gme/pdfs/Pareto%20Chart.pdf

[76] IEC 60300-3-11, Dependability management—Part 3-11: Application guide—Reliability-centred maintenance

[77] MACKENZIE Cameron A. Summarizing risk using risk measures and risk indices. RiskAnalysis, 34,12 2143-2163 2014

选项之间进行选择的技术

[78] KHOJASTEH, P, (2016). Application of benefit-cost-risk formula and key change indicators to meet project objectives [viewed 2019-02-13]. Available at https://www1.bournemouth.ac.uk/sites/default/files/asset/document/Mon%205.1%20Kh ojasteh%20Pejman%20Risk.pdf

[79] The Green book, Appraisal and Evaluation in Central Government; 2011 Treasury Guidance LONDON: TSO London

[80] ANDOSEH, S., et al. The case for a real options approach to ex-ante cost-benefit analyses of agricultural research projects. Food policy 44, 2014, 218-226 [viewed 2019-02-13]. Available at: http://pdf.usaid.gov/pdf_docs/pnaec758.pdf

[81] KIRKWOOD, CRAIG . Decision Tree Primer University of Arizona in Decision Analysis and System Dynamics resources 2002 [viewed 2019-02-13]. Available at: http://www.public.asu.edu/~kirkwood/DAStuff/decisiontrees/

[82] MYERSON, ROGER B., Game Theory: Analysis of Conflict, Harvard University Press,1991

[83] MARYNARD, SMITH JOHN Evolution and Theory of Games, Cambridge University Press 1982

[84] ROSENHEAD, J. and MINGER, J. (Eds), Rational Analysis for a Problematic World Revisited, 2nd ed. Wiley, Chichester UK, 2001

[85] EN 16271:2012, Value management—Functional expression of the need and functionalperformance specification—Requirements for expressing and validating the need to besatisfied within the process of purchasing or obtaining a product

[86] DEPARTMENT FOR COMMUNITIES AND LOCAL GOVERNMENT, Multi-criteria analysis: a manual 2009 [viewed 2019-02-13]. Available at:https://www.gov.uk/government/publications/multi-criteria-analysis-manual-for-makinggovernment-policy

[87] RABIHAH MHD. SUM, Risk Management Decision Making, 2001 [viewed 2019-02-13].Available at: http://www.isahp.org/uploads/47.pdf

[88] VELASQUEZ, M., HESTER, P. An Analysis of Multi—Criteria Decision Making Methods. International Journal of Operations Research, 10 (2), 55-66, 2013 [viewed 2019-02-13]. Available at: http://www.orstw.org.tw/ijor/vol10no2/ijor_vol10_no2_p56_p66.pdf

记录和报告技术

[89] ELMONSTRI, Mustafa, Review of the strengths and weaknesses of risk matrices, Journal of Risk Analysis and Crisis Response, 4 (1), 49-57, 2014 [viewed 2019-02-13]. Available at http://www.atlantis-press.com/php/download_paper.php? id=11718

[90] BAYBUTT, Paul, Calibration of risk matrices for process safety. Journal of Loss Prevention in the Process Industries, 38, 163-168, 2015

[91] GARVEY, P., BOOK S.A., COVERT R.P. Probability Methods for Cost Uncertainty Analysis: A Systems Engineering Perspective, Ed 2 Annex E Unravelling the S curve. CRC 2016