ICS 03.100.01
A 02

中华人民共和国国家标准

GB/T 27921—2011

风险管理　风险评估技术

Risk management—Risk assessment techniques

2011-12-30 发布　　2012-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中华人民共和国
国家标准
风险管理 风险评估技术
GB/T 27921—2011
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4.25 字数 125 千字
2012年2月第一版 2012年2月第一次印刷
*
书号:155066·1-44225 定价 57.00 元

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准参考 ISO/IEC 31010:2009《风险管理　风险评估技术》(英文版)编制而成。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由全国风险管理标准化技术委员会(SAC/TC 310)提出并归口。

本标准起草单位:中国标准化研究院、第一会达风险管理科技有限公司、北京理工大学、中国科学院科技政策与管理科学研究所、北京大学。

本标准主要起草人:崔艳武、高晓红、汤万金、杨颖、吕多加、信春华、刘铁忠、李建平、刘新立。

引　言

本标准为依据 GB/T 24353—2009《风险管理　原则与实施指南》开展风险管理的组织提供支持，用于指导组织选择和应用风险评估技术。

各种类型及规模的组织都会面临各种各样的风险，这些风险有可能影响到其目标的实现。应当对组织各项活动中存在的风险进行有效管理。

风险管理主要涉及将逻辑性及系统性的方法应用于以下方面：

——贯穿风险管理过程的沟通和记录；

——明确组织环境信息，以便于识别、分析、评价、应对并监控与任何活动、过程、功能或产品等相关的风险；

——监督和检查风险；

——适当地报告和记录有关结果。

作为风险管理的组成部分，风险评估提供了一种结构化的过程以识别目标如何受各类不确定性因素的影响，并从后果和可能性两个方面来进行风险分析，然后确定是否需要进一步应对。

风险评估工作试图回答以下基本问题：

——会发生什么以及为什么发生？

——后果是什么？

——这些后果发生的可能性有多大？

——是否存在一些可以减轻风险后果或者降低风险可能性的因素？

——风险等级是否可容许或可接受？是否要求进一步的应对？

本标准旨在反映当前风险评估技术选择和应用的良好实践，但并未涉及那些新出现的、尚在发展中的等还未获得专业人员共识的评估技术概念。本标准的资料性附录中介绍了一系列的风险评估技术，在本标准参考的其他标准中对于这些技术的概念和应用有更详细的说明。

风险管理　风险评估技术

1　范围

本标准规定了风险评估技术的选择和应用指南。

本标准并未涉及风险评估的所有技术，标准中未予介绍的技术并不意味着其无效。

本标准适用于指导组织选择合适的风险评估技术，一般性的风险管理标准，以及各种类型和规模的组织。

本标准涉及安全方面的内容参见 GB/T 20000.4—2003。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2009　风险管理　术语(ISO/IEC Guide 73:2002)

GB/T 24353—2009　风险管理　原则与实施指南

3　术语和定义

GB/T 23694—2009 中界定的术语和定义适用于本文件。

4　风险评估概念

4.1　目的和作用

风险评估旨在为有效的风险应对提供基于证据的信息和分析。

风险评估的主要作用包括：

——认识风险及其对目标的潜在影响；

——为决策者提供相关信息；

——增进对风险的理解，以利于风险应对策略的正确选择；

——识别那些导致风险的主要因素，以及系统和组织的薄弱环节；

——沟通风险和不确定性；

——有助于建立优先顺序；

——帮助确定风险是否可接受；

——有助于通过事后调查来进行事故预防；

——选择风险应对的不同方式；

——满足监管要求。

4.2　风险评估和风险管理过程

4.2.1　概述

本标准所指的风险评估是在 GB/T 24353—2009 所描述的风险管理过程内展开的。GB/T 24353—

2009 中界定的风险管理过程包含以下要素：明确环境信息；风险评估（包括风险识别、风险分析与风险评价）；风险应对；监督和检查；沟通和记录。

在风险管理过程中，风险评估并非一项独立的活动，必须与风险管理过程的其他组成部分有效衔接。进行风险评估时尤其应该清楚以下事项：

——组织所处环境和组织目标；

——组织可容许风险的范围及类型，以及如何应对不可接受的风险；

——风险评估的方法和技术，及其对风险管理过程的促进作用；

——实施风险评估的义务、责任及权利；

——可用于风险评估的资源；

——如何进行风险评估的报告及检查；

——风险评估活动如何融入组织日常运行中。

4.2.2 明确环境信息

通过明确环境信息，组织可明确其风险管理的目标，确定与组织相关的内部和外部参数，并设定风险管理的范围和有关风险准则。

风险准则是组织用于评价风险重要程度的标准。因此，风险准则需体现组织的风险承受度，应反映组织的价值观、目标和资源。组织应根据所处环境和自身情况，合理确定本组织的风险准则。

在进行具体的风险评估活动时，明确环境信息应包括界定内外部环境、风险管理环境并确定风险准则。在此过程中，应确定风险评估目标及风险评估程序。

4.2.3 风险评估

风险评估包括风险识别、风险分析和风险评价 3 个步骤。

风险评估活动适用于组织的各个层级，评估范围可涵盖项目、单个活动或具体事项等。但是在不同情境中，所使用的评估工具和技术可能会有差异。

风险评估有助于决策者对风险及其原因、后果和发生可能性有更充分的理解。这可以为以下决策提供信息：

——是否应该开展某些活动；

——如何充分利用时机；

——是否需要应对风险；

——风险应对策略的选择；

——确定风险应对策略的优先顺序；

——选择最适合的风险应对策略，将风险的不利影响控制在可以接受的水平。

4.2.4 风险应对

风险应对是在完成风险评估之后，选择并执行一种或多种改变风险的措施，包括改变风险事件发生的可能性和/或后果。

风险应对是一个递进的循环过程，实施风险应对措施后，应依据风险准则，重新评估新的风险水平是否可以承受，从而确定是否需要进一步采取应对措施。

4.2.5 监督和检查

作为风险管理过程的组成部分，应定期对风险与控制进行监督和检查，以确认：

——有关风险的假定仍然有效；

——风险评估所依据的假定，包括内外部环境，仍然有效；

——正在实现预期结果；

——风险评估的结果符合实际经验；
——风险评估技术被正确使用；
——风险应对是有效的。
组织应确定监督和检查工作的责任。

4.2.6 沟通和记录

成功的风险评估依赖于与利益相关方的有效沟通与协商。
利益相关方参与风险管理过程将有助于：
——沟通计划的制定；
——合理地界定内外部环境；
——确保利益相关方的利益得到充分理解和考虑；
——汇集不同领域的专业知识以识别和分析风险；
——确保风险评价过程中不同的观点也能得到适当考虑；
——确保风险得到充分识别；
——确保风险应对计划得到认可和支持。
利益相关方应当设法促进风险评估与组织其他管理活动的有效融合，例如变革管理、项目和计划管理以及财务管理等。

5 风险评估过程

5.1 概述

通过风险评估，决策者及有关各方可以更深刻地理解那些可能影响组织目标实现的风险，以及现有风险控制措施的充分性和有效性，为确定最合适的风险应对方法奠定基础。风险评估的结果可作为组织决策过程的输入。
风险评估是由风险识别、风险分析和风险评价构成的一个完整过程(见图1)。风险评估活动内嵌于风险管理过程中，与其他风险管理活动紧密融合并互相推动。

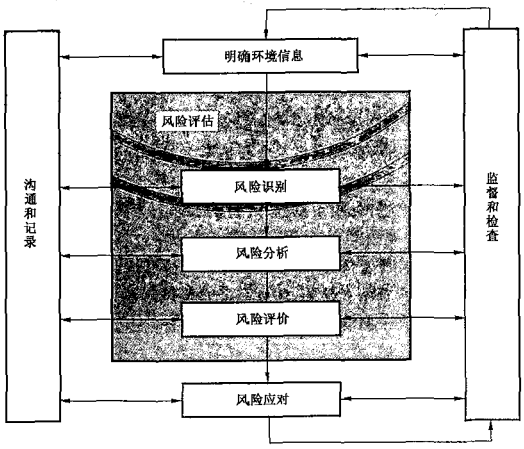

图1 风险评估对风险管理过程的推动作用

考虑到不同类型的风险差异较大，因此风险评估通常涉及到多学科方法的综合应用。风险评估活动的开展形式，不仅依赖于风险管理过程的背景，还取决于所使用的风险评估技术与方法。

5.2 风险识别

风险识别是发现、列举和描述风险要素的过程。

风险识别的目的是确定可能影响系统或组织目标得以实现的事件或情况。一旦风险得以识别，组织应对现有的控制措施(诸如设计特征、人员、过程和系统等)进行识别。

风险识别过程包括对风险源、风险事件及其原因和潜在后果的识别。

风险识别方法可能包括：

——基于证据的方法，例如检查表法以及对历史数据的评审；

——系统性的团队方法，例如一个专家团队遵循系统化的过程，通过一套结构化的提示或问题来识别风险；

——归纳推理技术，例如危险与可操作性分析方法(Hazard and operability study，HAZOP)等。

组织可利用各种支持性的技术来提高风险识别的准确性和完整性，包括头脑风暴法和德尔菲法等。

无论实际采用哪种技术，关键是在整个风险识别过程中要认识到人的因素和组织因素的重要性。因此，偏离预期的人为及组织因素也应被纳入风险识别的过程中。

5.3 风险分析

5.3.1 概述

风险分析是要增进对风险的理解。它为风险评价、决定风险是否需要应对以及最适当的应对策略和方法提供信息支持。

风险分析需要考虑导致风险的原因和风险源、风险事件的正面和负面的后果及其发生的可能性、影响后果和可能性的因素、不同风险及其风险源的相互关系以及风险的其他特性，还要考虑控制措施是否存在及其有效性。附录B提供了一些常用的风险分析方法。对于复杂的应用可能需要多种方法同时使用。

为确定风险等级，风险分析通常包括对风险的潜在后果范围和发生可能性的估计，该后果可能源于一个事件、情景或状况。然而，在某些情况下，如后果很不重要，或发生的可能性极小，这时单项参数的估计可能就足以进行决策。

在某些情况下，风险可能是一系列事件迭加产生的结果，或者由一些难以识别的特定事件所诱发。在这种情况下，风险评估的重点是分析系统各组成部分的重要性和薄弱环节，检查并确定相应的防护和补救措施。

用于风险分析的方法可以是定性的、半定量的、定量的或以上方法的组合。风险分析所需的详细程度取决于特定的用途、可获得的可靠数据，以及组织决策的需求。

定性的风险分析可通过重要性等级来确定风险后果、可能性和风险等级，如“高”、“中”、“低”3个重要性程度。可以将后果和可能性两者结合起来，并对照定性的风险准则来评价风险等级的结果。

半定量法可利用数字评级量表来测度风险的后果和发生可能性，并运用公式将二者结合起来，确定风险等级。量表的刻度可以是线性的，或者是对数的，或其他形式。

定量分析可估计出风险后果及其发生可能性的实际数值，并产生风险等级的数值。由于相关信息不够全面、缺乏数据、人为因素影响等，或是因为定量分析难以开展或没有必要，全面的定量分析未必都是可行的或值得的。在此情况下，由具有专业知识和经验的专家对风险进行半定量或者定性的分析可能已经足够有效。

如果是定性分析，那么应该对使用的术语和概念进行清晰的说明，并记录所有风险准则的设定

基础。

即使已实现全面的定量分析，还应注意到，此时计算获得的风险等级值是估计值，应谨慎地确保其精确度不会与所使用的原始数据及分析方法的精确度存在偏差。

风险等级应当用与风险类型最为匹配的术语表达，以利于进一步的风险评价。在某些情况下，风险等级可以通过风险后果的可能性分布来表述。

5.3.2 控制措施评估

风险的等级水平不仅取决于风险本身，还与现有风险控制措施的充分性和有效性密切相关。

在进行控制措施评估时，需要解决的问题包括：

——对于一个具体的风险，现有的控制措施是什么？

——这些控制措施是否足以应对风险，是否可以将风险控制在可接受范围之内？

——在实际中，控制措施是否在以预定方式正常运行，当需要时，能否证明这些控制措施是有效的？

对于特定的控制措施或一套相关控制措施的有效性水平，可以进行定性、半定量或定量的表述。但在大多数情况下，难以保证高度的精确性。然而，表述和记录测量风险控制效果的有效性是有价值的。因为在改进现有控制措施以及实施不同的风险应对措施时，这些信息有助于决策者进行比较和判断。

5.3.3 后果分析

通过假设特定事件、情况或环境已经出现，后果分析可确定风险影响的性质和类型。某个事件可能会产生一系列不同严重程度的影响，也可能影响到一系列目标和不同利益相关方。在明确环境信息时，就应当确定所需要分析的后果的类型和受影响的利益相关方。

后果分析的形式较为灵活，可以是对后果的简单描述，也可能是制定详细的数量模型等。

影响可能是轻微后果高概率，或严重后果低概率，或某些中间状况。在某些情况下，应关注具有潜在严重后果的风险，因为这些风险往往是管理者最关心的。在其他情况下，同时分析具有严重后果和轻微后果的风险可能是重要的。例如，频繁而轻微的问题可能具有很大的累积或长期效应。另外，处理这两类截然不同的风险的应对措施往往有很大的区别，因此分别分析这两类风险是必要的。

后果分析应包括：

——考虑应对后果的现有控制措施，并关注可能影响后果的相关因素；

——将风险后果与最初目标联系起来；

——对马上出现的后果和那些经过一段时间后可能出现的后果两种情况要同等重视；

——不能忽视次要后果，例如那些影响相关系统、活动、设备或组织的次要后果。

5.3.4 可能性分析

通常主要使用三种方法来估计可能性。这些方法可单独或组合使用，包括：

a) 利用相关历史数据来识别那些过去发生的事件或情况，借此推断出它们在未来发生的可能性。所使用的数据应当与正在分析的系统、设备、组织或活动的类型有关。如果某些事件过去的发生频率很低，则任何可能性的估计都是不确定的。这一点尤其适用于从未发生的事件、情况或环境，人们无法推测其将来是否会发生。

b) 利用故障树和事件树等技术来预测可能性。当历史数据无法获取或不够充分时，有必要通过分析系统、活动、设备或组织及其相关的失效或成功状况来推断风险发生的可能性。

c) 系统化和结构化地利用专家观点来估计可能性。专家判断应利用一切现有的相关信息，包括历史的、特定系统的、具体组织的、实验及设计等方面的信息。获得专家判断的正式方法众多，常用的方法包括德尔菲法和层次分析法等。

5.3.5 初步分析

应对风险进行全面的筛选，以识别出最重大的风险或把不太重要和次要的风险排除，便于进一步的分析，由此确保组织资源能集中于应对最严重的风险。进行筛选时，应注意不要漏掉发生频率低但有重大累积效应的风险。

以上筛选活动应在明确环境信息时所确定的风险准则基础上进行。依据初步分析的结果，组织可能采取以下某个行动方案：

——无需进一步评估，立即进行风险应对；

——搁置暂不需应对的不重要风险；

——继续进行更细致的风险评估。

应记录最初的假定及结果。

5.3.6 不确定性及敏感性

在风险分析过程中经常会涉及到相当多的不确定性。认识这些不确定性对于有效地解释和沟通风险分析结果是必要的。这些不确定性与在风险识别和风险分析时所使用的数据、方法及模型有关。不确定性分析包括明确风险分析结果的方差或不准确性，它们可能来自于用于确定结果的参数和假设的共同偏差。

与不确定性分析密切相关的是敏感性分析。敏感性分析是确定某个参数输入的变化对风险等级的影响。这项分析可用来识别哪些数据是对结果影响较大的，从而更应确保其精确性。

应尽可能充分阐述风险分析的完整性及准确度。如有可能，应识别不确定性的起因，并阐述所使用数据、方法及模型的不确定性。敏感的参数及其敏感性程度应予以说明。

5.4 风险评价

风险评价包括将风险分析的结果与预先设定的风险准则相比较，或者在各种风险的分析结果之间进行比较，确定风险的等级。

风险评价利用风险分析过程中所获得的对风险的认识，对未来的行动进行决策。道德、法律、财务以及包括风险感知在内的其他因素，也是决策的参考信息。

决策包括：

——某个风险是否需要应对；

——风险的应对优先次序；

——是否应开展某项应对活动；

——应该采取哪种途径。

在明确环境信息时，需要做出的决策的性质以及决策所依据的准则都已得到确定。但是在风险评价阶段，需要对以上问题进行更深入的分析，毕竟此时对于已识别的具体风险有更为全面的了解。如果该风险是新识别的风险，则应当制定相应的风险准则，以便评价该风险。

最简单的风险评价结果，是仅将风险分为两种：需要应对与无需应对的。这样的方式无疑简单易行，但是其结果通常难以反映出风险估计时的不确定性，而且两类风险界限的准确界定也绝非易事。

是否以及如何应对风险的决策，也可能取决于承担风险的成本与收益以及实施应对措施的成本与收益。

依据风险的可容许程度，可以将风险划分为如下 3 个区域：

——不可接受区域。在该区域内无论相关活动可以带来什么收益，风险等级都是无法承受的，必须不惜代价进行风险应对；

——中间区域。对该区域内风险的应对需要考虑实施应对措施的成本与收益，并权衡机遇与潜在

后果；

——广泛可接受区域。该区域中的风险等级微不足道，或者风险很小，无需采取任何风险应对措施。

安全工程领域的“最低合理可行”或 ALARP(As Low As Reasonably Practicable)准则即遵循了这一风险分级方式。在中间区域(或称 ALARP 区域)中，对于较低的风险可以直接进行应对措施的成本收益分析：如果增加安全的投入对安全效益的贡献不大，则可认为风险是可容许的；对于其中较高的风险，则需进一步实施应对措施，以使风险尽量向广泛可接受区域靠拢，直至风险降低的成本与获得的安全收益完全不成比例。

风险评价的结果应满足风险应对的需要，否则，应做进一步分析。

5.5 文件的归档

风险评估的过程和结果都应进行记录。风险应以可理解的术语来表达，同时风险等级的单位也应得到清晰表述。

风险评估记录文件的内容将取决于评估工作的目标及范围。除非进行很简单的评估，否则，记录文件需包括：

——目标及范围；

——系统相关部分的说明及它们的功能；

——组织的内外部环境描述以及被评估对象与内外环境的关联情况；

——所使用的风险准则及其合理性；

——局限性、假定及假设的合理性；

——评估方法；

——风险识别的结果；

——数据的来源与校验；

——风险分析的结果及评价；

——敏感性及不确定性分析；

——关键的假定和其他需要加以监测的因素；

——结果的讨论；

——结论和建议；

——参考资料。

如果需要风险评估来支持一个连续的风险管理过程，那么对于风险评估的记录工作应在系统、组织、设备或活动的整个生命周期内持续进行。如果出现重要的新信息或者环境发生变化，应根据管理的需要对风险评估进行更新。

5.6 风险评估的监督和检查

风险评估过程强调环境因素和其他因素，这些因素可能会随时间变化，并且可能使风险评估改变或失效。应当识别出这些因素进行持续的监督和检查，以便在必要时更新风险评估的信息。

应当识别和收集为改进风险评估而监测的数据。还应当监测和记录风险控制措施的效果，以便为风险分析提供数据。应当明确证据、文件的建立和检查的责任。

6 风险评估技术的选择

6.1 概述

选择合适的风险评估技术和方法，有助于组织及时高效地获取准确的评估结果。在具体实践中，风

险评估的复杂及详细程度千差万别。风险评估的形式及结果应与组织的自身情况适合。

6.2 技术的选择

6.2.1 概述

一般来说，合适的技术应具备以下特征：

——适应组织的相关情况；

——得出的结果应加深对风险性质及如何应对风险的认识；

——应能按可追溯、可重复及可验证的方式使用。

应从相关性及适用性角度说明选择技术的原因。在综合不同研究的结果时，所采用的技术及结果应是可比较的。

一旦决定进行风险评估并且确定了风险评估的目标和范围，那么就可以依据如下因素，选择一种或多种评估技术：

——风险评估的目标，这对于使用的方法有直接影响；

——决策者的需要：某些情况下做出有效的决策需要充分的评估细节，而某些情况下可能只需要对总体情况进行大致了解；

——所分析风险的类型及范围；

——后果的潜在严重程度；

——专业知识、人员以及所需资源的程度；

——信息和数据的可获得性；

——修改/更新风险评估的必要性：一些评估结果可能在将来需要修改或更新。在这方面，某些方法比其他方法更易于调整；

——法律法规及合同要求等。

只要满足评估的目标和范围，简单方法应优先于复杂方法被采用。

此外，其他几类因素对风险评估技术选择的影响也值得关注，例如资源的可获得性、现有数据和信息中不确定性的性质和程度，以及在应用方面的复杂性。

6.2.2 资源的可获得性

可能影响风险评估技术选择的资源和能力包括：

——风险评估团队的技能、经验及能力；

——信息及数据的可获得性；

——时间和组织内其他资源的限制；

——需要外部资源时的可用预算。

6.2.3 不确定性的性质和程度

组织内外部环境中常常存在着不确定性。可获得的信息和数据并不总是可以对未来的预测提供可靠的基础。不确定性可能产生于信息的质量、数量和完整性，例如较差的数据质量或缺乏基本的、可靠的数据；某些风险可能缺少历史数据；数据收集的方式的有效性；或者是不同利益相关方会对现有数据做出不同的解释。进行风险评估的人员应理解不确定性的类型及性质，同时认识到风险评估结果可靠性的重大意义，并向决策者说明这些情况。

6.2.4 复杂性

风险自身经常具有复杂性的特征。例如，在复杂的系统中进行风险评估时，应对其系统总体进行评

估，而不是孤立地对待系统中的每个部分，并忽视各部分之间的相互关系。在某些情况下，对某一风险采取应对措施可能会对其他活动产生影响。需要认识后果之间的相互影响和风险之间的相互依赖关系，以确保在管理一个风险时，不会导致在其他地方产生另一个不可容忍的风险。理解组织中单个或多个风险组合的复杂性，对于选择适当的风险评估技术和方法至关重要。

6.3 风险评估在生命周期各阶段的应用

许多活动、项目和产品被认为具有生命周期，从最初的概念和定义、实现到最终的完结。风险评估可以应用于生命周期的所有阶段，而且通常以不同的详细程度被应用多次，以便为每一阶段需做出的决策提供帮助。

生命周期各阶段对风险评估有不同的需求，并需要不同的评估技术。例如，在概念和定义阶段，当识别一个机会时，可以使用风险评估来决定是继续还是放弃。在有多个方案可供选择时，风险评估可以用于评价替代方案，帮助确定哪种方案能够提供最好的风险平衡。

在设计和开发阶段，风险评估有助于：

——保证系统风险是可接受的；

——精细化设计过程；

——成本的有效性研究；

——识别在后续阶段可能出现的风险。

在生命周期的其他阶段，可以用风险评估提供必要的信息，以便为正常情况和紧急情况制定程序。

6.4 风险评估技术的类型

为了更清晰地理解各类风险评估技术的特点，可以依据多种方式对这些技术方法进行分类。附录A按适用阶段和影响因素，对常用的风险评估技术进行了分类比较。

在附录B中，对这些常用的风险评估技术和方法展开了进一步的详述介绍，为组织如何在特定情况下选择合适的风险评估技术提供参考。复杂情况下可能需要同时采用多种评估技术和方法。

附 录 A
（资料性附录）
风险评估技术的比较

A.1 适用阶段

本附录描述了各类评估技术如何应用到风险评估过程的每一个阶段。风险评估过程如下所示：

——风险识别；

——风险分析：后果分析；

——风险分析：对发生可能性的定性、半定量或定量分析；

——风险分析：评估现有控制措施的有效性；

——风险分析：风险等级的估计；

——风险评价。

对于风险评估的每一阶段，各类技术的适用性被描述为非常适用、适用或者不适用（参见表 A.1）。

表 A.1 技术在风险评估各阶段的适用性

风险评估技术	风险评估过程					详述
	风险识别	风险分析			风险评价	
		后果	可能性	风险等级		
头脑风暴法	SA	A	A	A	A	B.1
结构化/半结构化访谈	SA	A	A	A	A	B.2
德尔菲法	SA	A	A	A	A	B.3
情景分析	SA	SA	A	A	A	B.4
检查表	SA	NA	NA	NA	NA	B.5
预先危险分析	SA	NA	NA	NA	NA	B.6
失效模式和效应分析	SA	SA	SA	SA	SA	B.7
危险与可操作性分析	SA	SA	A	A	A	B.8
危害分析与关键控制点	SA	SA	NA	NA	SA	B.9
结构化假设分析	SA	SA	SA	SA	SA	B.10
风险矩阵	SA	SA	SA	SA	A	B.11
人因可靠性分析	SA	SA	SA	SA	A	B.12
以可靠性为中心维修	SA	SA	SA	SA	SA	B.13
压力测试	SA	A	A	A	A	B.14
保护层分析法	A	SA	A	A	NA	B.15

表 A.1（续）

风险评估技术	风险评估过程					详述
	风险识别	风险分析			风险评价	
		后果	可能性	风险等级		
业务影响分析	A	SA	A	A	A	B.16
潜在通路分析	A	NA	NA	NA	NA	B.17
风险指数	A	SA	SA	A	SA	B.18
故障树分析	A	NA	SA	A	A	B.19
事件树分析	A	SA	A	A	NA	B.20
因果分析	A	SA	SA	A	A	B.21
根原因分析	NA	SA	SA	SA	SA	B.22
决策树分析	NA	SA	SA	A	A	B.23
蝶形图法(Bow-tie)	NA	A	SA	SA	A	B.24
层次分析法(AHP)	NA	A	A	SA	SA	B.25
在险值法(VaR)	NA	A	A	SA	SA	B.26
均值-方差模型	NA	A	A	A	SA	B.27
资本资产定价模型	NA	NA	NA	NA	SA	B.28
FN 曲线	A	SA	SA	A	SA	B.29
马尔可夫分析法	A	SA	NA	NA	NA	B.30
蒙特卡罗模拟法	NA	NA	NA	NA	SA	B.31
贝叶斯分析	NA	SA	NA	NA	SA	B.32

注 1：SA 表示非常适用。
注 2：A 表示适用；
注 3：NA 表示不适用。

A.2 影响因素

影响风险评估技术选择的因素有多种。在实践过程中，以下因素更应引起关注：

——所需资源的程度，主要涉及时间、专业知识水平、数据需求或评估成本等；

——不确定性的性质及程度；

——问题和所需分析方法的复杂性；

——方法是否可以提供定量结果。

基于以上方面，对各类风险评估技术特征的描述如表 A.2 所示。其中用高、中、低来表示每一种技术与影响因素的联系。

表 A.2 风险评估技术的特征

风险评估方法及技术	说明	影响因素			能否提供定量结果
		资源与能力	不确定性的性质与程度	复杂性	
头脑风暴法及结构化访谈	一种收集各种观点和评价在团队内进行评级的方法。头脑风暴法可由提示、一对一以及一对多的访谈技术所激发	低	低	低	否
德尔菲法	一种综合各类专家观点并促其一致的方法，这些观点有利于支持风险源及影响的识别、可能性与后果分析以及风险评价。需要独立分析和专家投票	中	中	中	否
情景分析	在想象和推测的基础上，对可能发生的未来情景加以描述。可以通过正式或非正式的、定性或定量的手段进行情景分析	中	高	中	否
检查表	一种简单的风险识别技术，提供了一系列典型的需要考虑的不确定性因素。使用者可参照以前的风险清单、规定或标准	低	低	低	否
预先危险分析(PHA)	PHA是一种简单的归纳分析方法，其目标是识别风险以及可能危害特定活动、设备或系统的危险性情况及事项	低	高	中	否
失效模式和效应分析(FMEA)	FMEA是一种识别失效模式、机制及其影响的技术。有几类FMEA：设计(或产品)FMEA，用于部件及产品；系统FMEA；过程FMEA，用于加工及组装过程；还有服务FMEA及软件FMEA	中	中	中	是
危险与可操作性分析(HAZOP)	HAZOP是一种综合性的风险识别过程，用于明确可能偏离预期绩效的偏差，并可评估偏离的危害度。它使用一种基于引导词的系统	中	高	高	否
危害分析与关键控制点(HACCP)	HACCP是一种系统的、前瞻性及预防性的技术，通过测量并监控那些应处于规定限值内的具体特征来确保产品质量、可靠性以及过程的安全性	中	中	中	否
结构化假设分析(SWIFT)	一种激发团队识别风险的技术，通常在引导式研讨班上使用，并可用于风险分析及评价	中	中	任何	否
风险矩阵	风险矩阵(Risk Matrix)是一种将后果分级与风险可能性相结合的方式	中	中	中	是
人因可靠性分析	人因可靠性分析(HRA)主要关注系统绩效中人为因素的作用，可用于评价人为错误对系统的影响	中	中	中	是

表 A.2（续）

风险评估方法及技术	说　明	影响因素			能否提供定量结果
		资源与能力	不确定性的性质与程度	复杂性	
以可靠性为中心的维修	以可靠性为中心的维修(RCM)是一种基于可靠性分析方法实现维修策略优化的技术，其目标是在满足安全性、环境技术要求和使用工作要求的同时，获得产品的最小维修资源消耗。通过这项工作，用户可以找出系统组成中对系统性能影响最大的零部件及其维修工作方式	中	中	中	是
压力测试	压力测试是指在极端情景下(最不利的情形下)，评估系统运行的有效性，发现问题，制定改进措施的方法	中	中	中	是
保护层分析法	保护层分析，也被称作障碍分析，它可以对控制措施及其效果进行评价	中	中	中	是
业务影响分析	分析重要风险影响组织运营的方式，同时明确如何对这些风险进行管理	中	中	中	否
潜在通路分析	潜在分析(SA)是一种用于识别设计错误的技术。潜在通路是指能够导致非期望的功能或抑制期望功能的状态，这些不良状态的特点具有随意性，在最严格的标准化系统检查中也不一定检测到	中	中	中	否
风险指数	风险指数可以提供一种有效的划分风险等级的工具	中	低	中	是
故障树分析	始于不良事项(顶事件)的分析并确定该事件可能发生的所有方式，以逻辑树形图的形式进行展示。在建立起故障树后，就应考虑如何减轻或消除潜在的风险源	高	高	中	是
事件树分析	运用归纳推理方法将各类初始事件的可能性转化成可能发生的结果	中	中	中	是
因果分析	综合运用故障树分析和事件树分析，并允许时间延误。初始事件的原因和后果都要予以考虑	高	中	高	是
根原因分析	对发生的单项损失进行分析，以理解造成损失的原因以及如何改进系统或过程以避免未来出现类似的损失。分析应考虑发生损失时可使用的风险控制方法以及怎样改进风险控制方法	中	低	中	否
决策树分析	对于决策问题的细节提供了一种清楚的图解说明	高	中	中	是
蝶形图法(Bow-tie)	一种简单的图形描述方式，分析了风险从危险发展到后果的各类路径，并可审核风险控制措施。可将其视为分析事项起因(由蝶形图的结代表)的故障树和分析后果的事件树这两种方法的结合体	中	高	中	是

表 A.2（续）

风险评估方法及技术	说　明	影响因素			能否提供定量结果
		资源与能力	不确定性的性质与程度	复杂性	
层次分析法(AHP)	定性与定量分析相结合，适合于多目标、多层次、多因素的复杂系统的决策	中	任何	任何	是
在险值(VaR)法	基于统计分析基础上的风险度量技术，可有效描述资产组合的整体市场风险状况	中	低	高	是
均值-方差模型	将收益和风险相平衡，可应用于投资和资产组合选择	中	低	中	是
资本资产定价模型	清晰地阐明了资本市场中风险与收益的关系	高	低	高	是
FN 曲线	FN 曲线通过区域块来表示风险，并可进行风险比较，可用于系统或过程设计以及现有系统的管理	高	中	中	是
马尔可夫分析法	马尔可夫分析通常用于对那些存在多种状态(包括各种降级使用状态)的可维修复杂系统进行分析	高	低	高	是
蒙特卡罗模拟法	蒙特卡罗模拟用于确定系统内的综合变化，该变化产生于多个输入数据的变化，其中每个输入数据都有确定的分布，而且输入数据与输出结果有着明确的关系。该方法能用于那些可将不同输入数据之间相互作用计算确定的具体模型。根据输入数据所代表的不确定性的特征，输入数据可以基于各种分布类型。风险评估中常用的是三角分布或贝塔分布	高	低	高	是
贝叶斯分析	贝叶斯分析是一种统计程序，利用先验分布数据来评估结果的可能性，其推断的准确程度依赖于先验分布的准确性。贝叶斯信念网通过捕捉那些能产生一定结果的各种输入数据之间的概率关系来对原因及效果进行模拟	高	低	高	是

附 录 B
（资料性附录）
风险评估技术

B.1 头脑风暴法

B.1.1 概述

头脑风暴法(Brainstorming)是指激励一群知识渊博的人员畅所欲言，以发现潜在的失效模式及相关危害、风险、决策准则及/或应对办法。“头脑风暴法”这个术语经常用来泛指任何形式的小组讨论。然而，真正的头脑风暴法包括一系列旨在确保人们的想象力因小组内其他成员的观点和言论而得到激发的专门技术。

在此类技术中，有效的引导非常重要，其中包括：在开始阶段创造自由讨论的氛围；会议期间对讨论进程进行有效控制和调节，使讨论不断进入新的阶段；筛选和捕捉讨论中产生的新设想和新议题。

B.1.2 用途

头脑风暴法可以与其他风险评估方法一起使用，也可以单独使用来激发风险管理过程任何阶段的想象力。头脑风暴法可以用作旨在发现问题的高层次讨论，也可以用作更细致的评审或是特殊问题的细节讨论。

B.1.3 输入

召集一个熟悉被评估的组织、系统、过程或应用的专家团队。

B.1.4 过程

头脑风暴法可以是正式的，也可以是非正式的。正式的头脑风暴法组织化程度很高，其中参与人员需要提前进行充分准备，而且会议的目的和结果都很明确，有具体的方法来评价讨论思路。非正式的头脑风暴法则组织化程度较低，通常针对性更强。

在一个正式的过程中，应至少包括以下环节：

——讨论会之前，主持人准备好与讨论内容相关的一系列问题及思考提示。

——确定讨论会的目标并解释规则。

——引导员首先介绍一系列想法，然后大家探讨各种观点，尽量多发现问题。此时无需讨论是否应该将某些事情记在清单上或是某句话究竟是什么意思，因为这样做会妨碍思绪的自由流动。一切输入都要接受，不要对任何观点加以批评；同时，小组思路快速推进，使这些观点激发出大家的横向思维。

——当某一方向的思想已经充分挖掘或是讨论偏离主题过远，那么引导员可以引导与会人员进入新的方向。其目的在于收集尽可能多的不同观点，以便进行后续分析。

B.1.5 输出

输出取决于该结果所应用的风险管理过程的阶段。例如，在识别阶段，该技术的输出可能是识别出的风险及当前控制措施的清单。

B.1.6 优点及局限

头脑风暴法的优点包括：

——激发了想象力，有助于发现新的风险和全新的解决方案；

——让主要的利益相关方参与其中，有助于进行全面沟通；

——速度较快并易于开展。

局限包括：

——参与者可能缺乏必要的技术及知识，无法提出有效的建议；

——由于头脑风暴法相对松散，因此较难保证过程及结果的全面性；

——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。

B.2 结构化/半结构化访谈

B.2.1 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，但是可以进行更自由的对话，以探讨可能出现的问题。

B.2.2 用途

如果人们很难聚在一起参加头脑风暴讨论会，或者小组内难以进行自由的讨论活动时，结构化和半结构化访谈就是一种有用的方法。该方法主要用于识别风险或是评估现有风险控制措施的效果，是为利益相关方提供数据来进行风险评估的有效方式，并且适用于某个项目或过程的任何阶段。

B.2.3 输入

输入数据包括：

——明确访谈目标；

——从利益相关方中挑选出被访谈者；

——准备问题清单。

B.2.4 过程

设计相关的访谈提纲以指导访谈者的访谈工作。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，问题最好只涉及一个方面的事务。

接着，将问题提交给访谈对象。在寻求问题的解答时，问题应该是开放式的，应注意不要“诱导”被访谈者。

考虑答复时应具有一定灵活性，以便有机会使访谈对象尽可能地表达其真实观点。

B.2.5 输出

输出结果是利益相关方对于作为访谈主题的问题所形成的看法。

B.2.6 优点及局限

结构化访谈的优点如下：

——结构化访谈可以使人们有时间专门考虑某个问题；

——通过一对一的沟通可以使双方有更多机会对某个问题进行深入思考；
——与只有小部分人员参与的头脑风暴法相比，结构化访谈可以让更多的利益相关方参与其中。
局限如下：
——通过这种方式获得各种观点所花费的时间较多；
——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一大特征——激发想象力。

B.3 德尔菲法

B.3.1 概述

德尔菲法(Delphi)是依据一套系统的程序在一组专家中取得可靠共识的技术。尽管该术语经常用来泛指任何形式的头脑风暴法，但是在形成之初，德尔菲法的根本特征是专家单独、匿名表达各自的观点。即在讨论过程中，团队成员之间不得互相讨论，只能与调查人员沟通。通过让团队成员填写问卷，集结意见，整理并共享，周而复始，最终获取共识。

B.3.2 用途

无论是否需要专家的共识，德尔菲法可以用于风险管理过程或系统生命周期的任何阶段。

B.3.3 输入

达成共识所需的一系列资源。

B.3.4 过程

使用半结构化问卷对一组专家进行提问。专家无需会面，保证其观点具有独立性。
具体步骤如下：
——组建专家团队，可能是一个或多个专家组；
——编制第一轮问卷调查表；
——将问卷调查表发给每位专家组成员，要求定期返回；
——对第一轮答复的信息进行分析、对比和汇总，并再次下发给专家组成员；让专家比较自己同他人的不同意见，修改或完善自己的意见和判断；在此过程中，只给出各种意见，但并不提供发表意见的专家姓名；
——专家组成员重新做出答复；
——循环以上过程，直到达成共识。

B.3.5 输出

逐渐对现有事项达成共识。

B.3.6 优点及局限

德尔菲法的优点包括：
——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看法；
——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；
——便于展开，成员不必一次聚集在某个地方。
局限包括：
——这是一项费力、耗时的工作；

——参与者需要进行清晰的书面表达。

B.4 情景分析

B.4.1 概述

情景分析(Scenario analysis)是指通过假设、预测、模拟等手段,对未来可能发生的各种情景以及各种情景可能产生的影响进行分析的方法。换句话说,情景分析法是类似"如果-怎样"的分析方法。未来总是不确定的,而情景分析使我们能够"预见"将来,对未来的不确定性有一个直观的认识。尽管情景分析法无法预测未来各类情景发生的可能性,但可以促使组织考虑哪些情景可能发生(诸如最佳情景、最差情景及期望情景),并且有助于组织提前对未来可能出现的情景进行准备。

B.4.2 用途

情景分析可用来帮助决策并规划未来战略,也可以用来分析现有的活动。它在风险评估过程的三个步骤中都可以发挥作用。

情景分析可用来预计威胁和机会可能发生的方式,并且适用于各类风险包括长期及短期风险的分析。在周期较短及数据充分的情况下,可以从现有情景中推断出可能出现的情景。对于周期较长或数据不充分的情况,情景分析的有效性更依赖于合乎情理的想象力。

如果积极后果和消极后果的分布存在比较大的差异,情景分析的应用效果会更为显著。

B.4.3 输入

情景分析的必要前提是要构建一支专家团队,其成员了解相关变化的特征(例如,可能的技术进步),同时需要具备丰富的想象力,可以有效预见未来发展。同时,掌握现有变化的文献和数据也很必要。

B.4.4 过程

情景分析的结构可以是正式的,也可以是非正式的。

在建立起团队和相关沟通渠道,同时确定了需要处理的问题和事件的背景之后,下一步就是识别可能出现变化的性质。这就要求研究人员对未来发展趋势及趋势变化的可能时机进行分析。

需要分析的变化可能包括:

——外部情况的变化(例如技术变化);

——不久将要做出的决定,而这些决定可能会产生各种不同的后果;

——利益相关方的需求以及需求可能的变化;

——宏观环境的变化(如政府监管及人口构成等),有些变化是必然的,而有些是不确定的。

有时,某种变化可能归因于另一个风险带来的结果。例如,气候变化的风险正在造成与食物链有关的消费需求发生变化,这样会改变哪些食品的出口会盈利以及哪些食品可能在当地生产。

局部及宏观因素或趋势可以按重要性和不确定性进行列举并排序。应特别关注那些最重要、最不确定的因素。可以绘制出关键因素或趋势的图形,以显示那些情景可以进行开发的区域。

建议使用一系列的情景,关注每个情景参数的合理变化。为每个情景编写一个"故事",讲述你如何从此时此地转向主题情景。这些故事可以包括那些能为情景带来附加值的合理细节。

现在,这些情景可以用来测试或评估最初的问题。这项测试需要考虑到任何重要但可预测的因素,然后通过"假定分析"分析组织现行策略在这种新情景中的"成功"概率。当对每个情景的问题或建议进行评估时,显然需要进行修正,以使其更为全面地反映现状。当情景正在发生变化时,可以找出一些能够表明变化的先行指标,监测先行指标并做出反应,可以为改变计划好的战略提供机会。

由于情景只是可能出现的未来经过界定的“片段”，因此关键是要确定某个特定结果（情景）发生的可能性。例如，对于最佳情景、最差情景以及预期情景，应努力描述或说明每个情景发生的可能性。

B.4.5 输出

识别并描述未来可能发生的各类情景及发展趋势，并针对各类情景制定相应的应对措施。

B.4.6 优点及局限

尽管每个决策人员都希望情报人员能够预测出唯一准确的结果，但由于当前环境的复杂性，更需要情景分析法对几种可能发生的情况进行预测，并针对每种情景进行提前准备，这样更具客观性。

但是，与这种优点相关的缺点是：在存在较大不确定性的情况下，有些情景可能不够现实。如果将情景分析作为一种决策工具，其危险在于所用情景可能缺乏充分的基础，数据可能具有随机性，同时可能无法发现那些将来可能出现、但目前看起来不切实际的结果。

B.5 检查表法

B.5.1 概述

检查表（Check-lists）是一个危险、风险或控制故障的清单，而这些清单通常是凭经验（要么是根据以前的风险评估结果，要么是因为过去的故障）进行编制的。按此表进行检查，以“是/否”进行回答。

B.5.2 用途

检查表法可用来识别潜在危险、风险或者评估控制效果，适用于产品、过程或系统的生命周期的任何阶段。它们可以作为其他风险评估技术的组成部分进行使用。

B.5.3 输入

有关某个问题的事先信息及专业知识，例如可以选择或编制一个相关的、最好是经过验证的检查表。

B.5.4 过程

具体步骤如下：

——组成检查表编制组，确定活动范围；

——依据有关标准、规范、法律条款及过去经验，选择设计一个能充分涵盖整个范围的检查表；

——使用检查表的人员或团队应熟悉过程或系统的各个因素，同时审查检查表上的项目是否有缺失；

——按此表对系统进行检查。

B.5.5 输出

输出结果取决于应用该结果的风险管理过程的阶段。例如，输出结构可以是一个控制措施评估清单或是风险清单。

B.5.6 优点及局限

检查表的优点包括：

——简单明了，非专业人士也可以使用；

——如果编制精良，可将各种专业知识纳入到便于使用的系统中；

——有助于确保常见问题不会被遗漏。

局限包括：

——只可以进行定性分析；

——可能会限制风险识别过程中的想象力；

——鼓励“在方框内画勾”的习惯；

——往往基于已观察到的情况，不利于发现以往没有被观察到的问题。

B.6 预先危险分析(PHA)

B.6.1 概述

预先危险分析(Primary hazard analysis，简称 PHA)是一种简单易行的归纳分析法，其目标是识别危险以及可能给特定活动、设备或系统带来损害的危险情况及事项。

B.6.2 用途

这是一种在项目设计和开发初期最常用的方法。因为当时有关设计细节或操作程序的信息很少，所以这种方法经常成为进一步研究工作的前奏，同时也为系统设计规范提供必要信息。在分析现有系统，从而将需要进一步分析的危险和风险进行排序时，或是现实环境使更全面的技术无法使用时，这种方法会发挥更大的作用。

B.6.3 输入

输入包括：

——被评估系统的信息；

——可获得的与系统设计有关的细节。

B.6.4 过程

通过考虑如下因素来编制危险、一般性危险情况及风险的清单。

——使用或生产的材料及其反应性；

——使用的设备；

——运行环境；

——布局；

——系统组成要素之间的分界面等。

对不良事项结果及其可能性可进行定性分析，以识别那些需要进一步评估的风险。

若需要，在设计、建造和验收阶段都应展开预先危险分析，以探测新的危险并予以更正。获得的结果可以使用诸如表格和树状图之类的不同形式进行表示。

B.6.5 输出

输出包括：

——危险及风险清单。

——包括接受、建议控制、设计规范或更详细评估的请求等多种形式的建议。

B.6.6 优点及局限

PHA 的优点包括：

——在信息有限时可以使用；

——可以在系统生命周期的初期考虑风险。

局限包括：

——只能提供初步信息，其不够全面也无法提供有关风险及最佳风险预防措施方面的详细信息。

B.7 失效模式和效应分析(FMEA)

B.7.1 概述

失效模式和效应分析(Failure mode and effect analysis，简称 FMEA)是用来识别组件或系统是否达到设计意图的方法，广泛用于风险分析和风险评价中。FMEA 是一种归纳方法，其特点是从元件的故障开始逐级分析其原因、影响及应采取的应对措施，通过分析系统内部各个组件的失效模式并推断其对于整个系统的影响，考虑如何才能避免或减小损失。

FMEA 用于识别：

——系统各部分所有潜在的失效模式；

——这些故障对系统的影响；

——故障原因；

——如何避免故障及/或减弱故障对系统的影响。

失效模式、效应和危害度分析(Failure mode and effect and criticality analysis，简称 FMECA)拓展了 FMEA 的使用范围。根据其重要性和危害程度，FMECA 可对每种被识别的失效模式进行排序。如将 FMEA 和 FMECA 联合使用，其应用范围更为广泛。

FMEA 分析通常是定性或半定量的，在可以获得实际故障率数据的情况下也可以定量化。

B.7.2 用途

FMEA 方法大多用于实体系统中的组件故障，但是也可以用来识别人为失效模式及影响。该方法有几种应用：用于部件、产品的设计(或产品)FMEA；用于系统的系统 FMEA；用于制造和组装过程的过程 FMEA；服务 FMEA 和软件 FMEA。

FMEA/FMECA 可以在系统的设计、制造或运行过程中使用。然而，为了提高可靠性，改进在设计阶段更容易实施。FMEA/FMECA 也适用于过程和程序。例如，它被用来识别潜在医疗保健系统中的错误和维修程序中的失败。FMEA 及 FMECA 可以为其他分析技术，例如定性及定量的故障树分析提供输入数据。

FMEA/FMECA 可用来：

——协助挑选具有高可靠性的替代性设计方案；

——确保所有的失效模式及其对运行的影响得到分析；

——列出潜在的故障并识别其影响的严重性；

——为测试及维修工作的规划提供依据；

——为定量的可靠性及可用性分析提供依据。

B.7.3 输入数据

FMEA 及 FMECA 需要有关系统组件的充分信息，以便对各组件出现故障的方式进行详细分析。

信息可能包括：

——正在分析的系统及系统组件的构成图，操作过程步骤的流程图；

——了解过程中每一步或系统组成部分的功能；

——可能影响运行的过程及环境参数的详细信息；

——对特定故障结果的了解；

——有关故障的历史信息，包括现有的故障率数据。

B.7.4 过程

FMEA 的步骤包括：

——确定分析对象；

——组建研究团队；

——将系统分成组件或步骤，确认：

- 各部分出现明显故障的方式是什么？
- 造成这些失效模式的具体机制？
- 故障可能产生的影响？
- 失败是无害的还是有破坏性的？
- 故障如何检测？

——确定故障补偿设计中的固有规定。

对于 FMECA，研究团队需接着根据故障结果的严重性，将每个识别出的失效模式进行分类。可以通过几种方法完成。常用方法包括：

——模式危险度指数；

——风险等级；

——风险优先数(The risk priority number)。

模式危险度是对所考虑的失效模式将导致整个系统发生故障的概率测量，其定义为故障影响率、失效率、系统操作时间三者的乘积。此定义经常应用于设备故障，其中每个术语可以定量地确定，而且失效模式都有同样的后果。

风险等级可通过故障模式后果与失效概率的组合获得。风险等级方法可应用于不同失效模式产生的不同后果，并且能够应用于设备系统或过程。风险等级可以定性地、半定量地或定量地表达。

风险优先数是一种半定量的危害度测量方法，其将故障后果、可能性和发现问题的能力(如果故障很难发现，则认为其优先级较高)进行等级赋值(通常在 1 到 10 之间)并相乘来获得危险度。这个方法经常用于质量保证的应用实践中。

一旦确定失效模式和机制，就可以界定和实施针对更重大失效模式的纠正措施。

失效模式报告记录的内容包括：

——所分析系统的详细说明；

——开展分析的方式；

——分析中的假设；

——数据来源；

——结果，包括完成的工作表；

——危害度(如果完成的话)以及界定危害度的方法；

——有关进一步分析、设计变更或者计划纳入测试计划的特征等方面的建议。

在完成了上述行动之后，可通过新一轮 FMEA 重新评估系统。

B.7.5 输出结果

FMEA 的主要输出结果是失效模式、失效机制及其对各组件或者系统或过程步骤影响的清单(可能包括故障可能性的信息)，也可以提供有关故障原因及其对整个系统影响方面的信息。FMECA 的输出包括对于系统失效的可能性、失效模式导致的风险等级、风险等级和“探测到”的失效模式的组合等方面的重要性进行排序。

如果使用合适的故障率资料和定量后果，FMECA 可以输出定量结果。

B.7.6 优点及局限

FMEA 与 FMECA 的优点包括：

——广泛适用于人力、设备和系统失效模式，以及硬件、软件和程序；

——识别组件失效模式及其原因和对系统的影响，同时用可读性较强的形式表现出来；

——通过在设计初期发现问题，从而避免了开支较大的设备改造；

——识别单点失效模式以及对冗余或安全系统的需要；

——通过突出计划测试的关键特征，为开发测试计划提供输入数据。

局限包括：

——只能识别单个失效模式，无法同时识别多个失效模式；

——除非得到充分控制并集中充分精力，否则研究工作较为耗时，且开支较大；

——对于复杂的多层系统来说，这项工作可能艰难枯燥。

B.8 危险与可操作性分析(HAZOP)

B.8.1 概述

HAZOP 即危险与可操作性分析(Hazard and operability study)，是一种对规划或现有产品、过程、程序或体系的结构化及系统分析技术。该技术被广泛应用于识别人员、设备、环境及/或组织目标所面临的风险。分析团队应尽量提供解决方案，以消除风险。

HAZOP 过程是一种基于危险和可操作性研究的定性技术，它对设计、过程、程序或系统等各个步骤中是否能实现设计意图或运行条件的方式提出质疑。该方法通常由一支多专业团队通过多次会议进行。

HAZOP 与 FMEA 类似，都用于识别过程、系统或程序的失效模式、失效原因及后果。其不同之处在于 HAZOP 团队通过考虑当前结果与预期的结果之间的偏差以及所处环境条件等来分析可能的原因和失效模式，而 FMEA 则先确定失效模式，然后才开始。

B.8.2 用途

HAZOP 技术最初被应用于化学工艺系统的风险评估中。目前该技术目前已拓展到其他类型的系统及复杂的操作中，包括机械及电子系统、程序、软件系统，甚至包括组织变更及法律合同设计及评审。

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。这种方法也广泛地用于软件设计评审中。当用于关键安全仪器控制及计算机系统时，该方法称作 CHAZOP(控制危险及可操作性分析或计算机危险及可操作性分析)。

HAZOP 分析通常在设计阶段开展，因为此时设计仍可进行调整。但是，随着设计的详细发展，可以对每个阶段用不同的导语分阶段进行。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.8.3 输入

HAZOP 分析的主要输入数据是有关计划审批的系统、过程或程序，以及设计意图与效果说明书的现有信息。输入数据可能包括说明书、工艺流程图、逻辑图、布局图、历史数据、操作及维修程序，以及紧急情况响应程序等。对于非硬件系统来说，HAZOP 的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，输入数据可以是组织图或角色说明、合同草案甚至程序草案。

B.8.4 过程

HAZOP依据设计图纸、流程说明、操作程序等对系统各组成部分进行审查，检查是否存在偏离预期效果的偏差、潜在原因以及偏差可能造成的结果。通过使用合适的引导词，对于系统、过程或程序的各个部分对关键参数变化的反应方式进行系统性分析，就可以实现上述目标。可以使用针对某个特殊系统、过程或程序的引导词，也可以使用能涵盖各类偏差的通用词。表B.1举例说明了技术系统常用的引导词。类似的导语如“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。

HAZOP分析的一般步骤包括：

——确定研究目标及范围；

——成立多专业人员组成的团队开展HAZOP分析；

——建立一系列关键的引导词；

——收集必要的文件。

在研究团队的引导式研讨班上：

——将系统、过程或程序划分成更小的单元/子系统/过程，以进行具体的审核；

——约定各单元/子系统/过程的设计意图，然后对于各元件依次使用引导词，以描述那些会产生不良结果的可能偏差；

——如果发现不良结果，讨论可能的原因及结果，同时就处理方式提出建议，从而减少或消除影响；

——将讨论内容记录在案，同时约定用于处理被识别风险的具体行动。

表B.1 HAZOP引导词的例子

术　语	定　义
“无”或“不”(none)	计划结果根本没有实现或是计划条件缺失
过高(more)	输出结果或运行状况的量值增长
过低(less)	输出结果或运行状况的量值减少
伴随(as well as)	在完成既定要求的同时有多余事件发生
部分(part of)	部分达到设计要求
相逆(reverse)	出现与设计要求完全相反的事件
异常(other than)	出现和设计意图不相通的事件
兼容性(compatibility)	材料、环境等的兼容性能
注：引导词适用于下列参数：材料或过程的物理特征；温度、速度等物理条件；系统或设计组件的规定目的(例如，信息转化)；运行方面。	

B.8.5 输出

对于每个评审点的项目，做好HAZOP会议的会议记录。这包括：使用的引导词、偏差、可能的原因、处理所发现问题的行动以及行动负责人。

对于任何无法纠正的偏差，需要对偏差造成的风险进行评估。

B.8.6 优点及局限

HAZOP的优点包括：

——为系统、彻底地分析系统、过程或程序提供了有效的方法；

——涉及多专业团队，可处理复杂问题；

——形成了解决方案和风险应对行动方案；

——有机会对人为错误的原因及结果进行清晰的分析。

局限包括：

——耗时，成本较高；

——对文件或系统/过程以及程序规范的要求较高；

——主要重视的是找到解决方案，而不是质疑基本假设；

——讨论可能会集中在设计细节上，而不是在更宽泛或外部问题上；

——受制于设计(草案)及设计意图，以及传递给团队的范围及目标；

——过程对设计人员的专业知识要求较高，专业人员在寻找设计问题的过程中很难保证完全客观。

B.9 危害分析与关键控制点法(HACCP)

B.9.1 概述

危害分析与关键控制点法(Hazard analysis and critical control points，简称HACCP)作为一种科学的、系统的方法，应用在从初级生产至最终消费过程中，为识别过程中各相关部分的风险并采取必要的控制措施提供了一个分析框架，以避免可能出现的危险，维护产品的质量可靠性和安全性。HACCP其重点在于预防而不是依赖于对最终产品的测试。

B.9.2 用途

20世纪60年代，美国宇航局最早开展了HACCP，其本意是为了保证太空计划的食品质量。目前，该方法已被广泛应用于食品产业中，在食品生产过程的各个环节识别并采取适当的控制措施防止来自物理、化学或生物污染物带来的风险。HACCP也被用于医药生产和医疗器械方面的危害识别、评价和控制方面。目前，HACCP正逐渐从一种管理手段和方法演变为一种管理模式或者管理体系。

B.9.3 输入

应用HACCP方法，需要了解产品的生产过程流程，以及一切可能影响到产品质量、安全性或可靠性的危险因素的信息。

B.9.4 过程

HACCP包括以下7项原则。

——进行危害分析，识别潜在危害及已有预防性措施；

——确定关键控制点(CCP)；

——确定关键限值，例如每个CCP必须在具体的参数范围内运行，这样才能保证危险得到控制；

——建立一个系统以监测关键控制点的控制情况；

——在监测结果表明某特定关键控制点失控时，确定应采取的纠正行动；

——建立审核程序；

——对于每一步都要实施记录和归档程序。

B.9.5 输出

归档记录包括危害分析工作表及 HACCP 计划。

危害分析工作表包含下列内容：

——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；

——各种危险可能的预防措施；

——该步骤能否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。这项计划包括一个涵盖所有 CCP 并针对各 CCP 的清单：

——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，需要采取的纠正行动；

——核实及记录活动。

B.9.6 优点及局限

HACCP 的优点包括：

——结构化的过程提供了质量控制以及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；

——鼓励在整个过程中进行风险控制，而不是依靠最终的产品检验；

——有能力识别由于人为行为带来的危险以及如何在引入点或随后对这些危险进行控制。

局限包括：

——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，也需要确定相应的控制措施。完成这些工作是为了确定 HACCP 过程中具体的临界控制点及控制参数。同时，还需要其他工具才能实现这个目标。

——如果等到控制参数超过了规定的限值时才采取行动，可能已经错过最佳控制时机。

B.10 结构化假设分析(SWIFT)

B.10.1 概述

最初，结构化假设分析(Structure "What if"，简称 SWIFT)是作为比 HAZOP 更简单的替代性方法推出的。它是一种系统的、团队合作式的研究方法，利用了引导员在讨论会上运用的一系列"提示"词或短语来激发参与者识别风险。引导员和团队使用标准的"假定分析"式短语以及提示词，来调查正常程序和行为的偏差对某个系统、设备组件、组织或程序产生影响的方式。通常，与 HAZOP 相比，SWIFT 用于某个系统的更多层面，同时细节要求较低。

B.10.2 用途

SWIFT 的设计初衷是针对化学及石化工厂的危险进行研究。目前该技术现在广泛地用于各种系统、设备组件、程序及组织的风险评估活动中，可用来分析变化的后果以及新产生的风险。

B.10.3 输入

在开始进行研究之前，必须对系统、设备组件、程序及/或变化进行严格界定。引导员应通过访谈以及对文件、计划和图纸的全面分析建立内外部背景。一般来说，研究涉及的项目、情况或系统应划分成节点或关键要素以便于开展分析过程，而这在 HAZOP 的界定层面中很少涉及。

另一个关键输入，是收集整理经过认真挑选的研究团队的专业知识和经验。其中，所有利益相关方的观点都要得到反映，如果可能的话，应当将其与拥有类似项目经验或情况经历的人员的观点统筹考虑。

B.10.4 过程

一般过程如下所示：

a) 在开展研究之前，引导员应准备一份相关的词语或短语提示单。该清单可以基于一系列标准的词语或短语，也可以是为便于对危险或风险进行综合分析而形成的词语或短语。

b) 讨论并约定项目、系统、变化或情况的内外部背景以及研究范围。

c) 引导员要求参与者提出并讨论：
   - 已知的风险和危险；
   - 以往的经历和事件；
   - 已知和现有的控制及保障措施；
   - 监管要求和限制措施。

d) 使用“假定分析”这样的短语及提示词或主题以形成问题，达到引导讨论的目的。计划使用的“假定分析”短语包括“要是…怎么办…”、“如果…会发生…”、“某人或某事会…”以及“有人或有事曾经…”。其目的是激发研究团队探讨潜在的情景及其原因和后果以及影响。

e) 总结风险，同时团队分析现有的控制措施。

f) 与团队确认风险及其原因、后果和预期控制的描述，并进行记录。

g) 分析控制措施是否充分有效。如果未达到满意的效果，团队应继续界定应采取的控制措施。

h) 在本次讨论中，提出更多的“假定分析”问题，以识别更多的风险。

i) 引导员利用提示单来监督讨论并建议团队讨论其他问题和情景。

j) 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，以确定行动优先级。一般来说，在使用这种风险评估方法时，要考虑现有的控制措施及其效果。

B.10.5 输出

输出结果是一个风险列表，记录了针对不同等级风险的行动或任务。这些任务可构成一个风险应对计划的基础。

B.10.6 优点及局限

SWIFT 的优点包括：

——广泛用于各种形式的物理设备或系统、情况或环境、组织或活动；

——对团队的准备工作要求较低；

——速度较快，同时重大危险及风险在讨论会上可以很快暴露出来；

——通过这项以“系统为导向”的研究，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；

——可用来识别过程及系统改进的机会，通常可用来识别促进成功可能性的活动；

——使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，这样可以增强其责任感；

——可轻松地建立起风险登记表和风险应对计划。

局限包括：

——要求经验丰富、能力较强、工作效率高的引导员；

——需要精心的准备，这样才不会浪费讨论会团队的时间；

——如果讨论团队缺乏足够经验或是提示系统不够全面，那么有些风险或危险可能就无法识别；

——可能无法揭示那些复杂、详细或相关的原因。

B.11 风险矩阵

B.11.1 概述

风险矩阵(Risk matrix)是用于识别风险和对其进行优先排序的有效工具。风险矩阵可以直观地显现组织风险的分布情况，有助于管理者确定风险管理的关键控制点和风险应对方案。一旦组织的风险被识别以后，就可以依据其对组织目标的影响程度和发生的可能性等维度来绘制风险矩阵。

B.11.2 用途

风险矩阵通常作为一种筛查工具用来对风险进行排序，根据其在矩阵中所处的区域，确定哪些风险需要更细致的分析，或是应首先处理哪些风险。

风险矩阵也可以用于帮助在全组织内沟通对风险等级的共同理解。设定风险等级的方法和赋予他们的决策规则应当与组织的风险偏好一致。

B.11.3 输入

需要输入的数据为风险发生的可能性与后果严重程度的评估结果。

对风险发生可能性的高低、后果严重程度的评估有定性、定量等方法。定性方法是直接用文字描述风险发生可能性的高低、后果严重程度，如“极低”、“低”、“中等”、“高”、“极高”等。定量方法是对风险发生可能性的高低、后果严重程度用具有实际意义的数量描述，如对风险发生可能性的高低用概率来表示，对后果严重程度用损失金额来表示。等级标度可以为任何数量的点。最常见的是有3、4或5个点的等级，但各点定义应尽量避免含混不清。如表B.2和表B.3分别列出了某公司对风险发生可能性和对目标的影响程度的定性、定量评估标准及其相互对应关系，供实际操作中参考。

表B.2 风险发生可能性的评价标准

定量方法一	评分	1	2	3	4	5
定量方法二	一定时期发生的概率	10%以下	10%～30%	30%～70%	70%～90%	90%以上
定性方法	文字描述一	极低	低	中等	高	极高
	文字描述二	一般情况下不会发生	极少情况下才发生	某些情况下发生	较多情况下发生	常常会发生
	文字描述三	今后10年内发生的可能少于1次	今后5～10年内可能发生1次	今后2～5年内可能发生1次	今后1年内可能发生1次	今后1年内至少发生1次

表 B.3 风险对目标影响程度的评价标准

适用于所有行业	定量方法一	评分		1	2	3	4	5
	定量方法二	企业财务损失占税前利润的百分比(%)		1%以下	1%～5%	6%～10%	11%～20%	20%以上
	定性方法	文字描述一		极轻微的	轻微的	中等的	重大的	灾难性的
		文字描述二		极低	低	中等	高	极高
		文字描述三	日常运行	不受影响	轻度影响(造成轻微的人身伤害,情况立刻受到控制)	中度影响(造成一定人身伤害,需要医疗救援,需要外部支持才能控制情形)	严重影响(企业失去一些业务能力,造成严重人身伤害,情况失控,但无致命影响)	重大影响(重大业务失误,造成重大人身伤亡,情况失控,给企业致命影响)
			财务损失	较低的财务损失	轻微的财务损失	中等的财务损失	重大的财务损失	极大的财务损失
			企业声誉	负面消息在企业内部流传,企业声誉没有受损	负面消息在当地局部流传,企业声誉轻微损害	负面消息在某区域流传,企业声誉中等损害	负面消息在全国各地流传,对企业声誉造成重大损害	监管机构进行调查,公众关注,对企业声誉造成无法弥补的损害

B.11.4 过程

对风险发生可能性的高低和后果严重程度进行定性或定量评估后,依据评估结果绘制风险图谱。绘制矩阵时,一个坐标轴表示结果等级,另一个坐标轴表示可能性等级。

图 B.1 为一个风险矩阵示例,该矩阵带有 6 点结果等级和 5 点可能性等级。

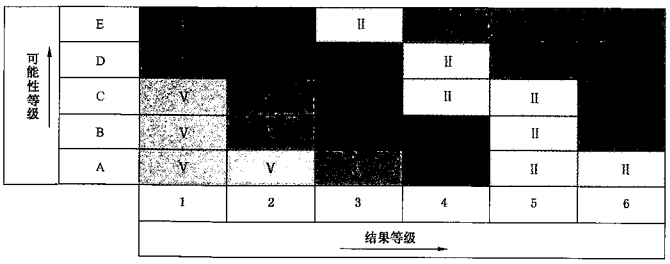

图 B.1 风险矩阵示例

矩阵定义的风险等级与组织的决策规则和风险偏好紧密相关，例如管理层关注度或应对所需的反应时间。

B.11.5 输出

输出结果是对各类风险的等级划分或是确定了重要性水平的、经分级的风险清单。

B.11.6 优点及局限

风险矩阵的优点包括：

——方法简单，易于使用；

——显示直观，可将风险很快划分为不同的重要性水平。

局限包括：

——必须设计出适合具体情况的矩阵，因此，很难有一个适用于组织各相关环境的通用系统；

——很难清晰地界定等级；

——该方法的主观色彩较强，不同决策者之间的等级划分结果会有明显的差别；

——无法对风险进行累计迭加（例如，人们无法将一定频率的低风险界定为中级风险）。

B.12 人因可靠性分析（HRA）

B.12.1 概述

人因可靠性分析（Human reliability analysis，简称 HRA）关注的是人因对系统绩效的影响，可以用来评估人为错误对系统的影响。很多过程都有可能出现人为错误，尤其是当操作人员可用的决策时间较短时。问题最终发展到严重地步的可能性或许不大，但是有时，人的行为是惟一能避免故障最终演变成事故的手段。

HRA 的重要性在各种事故中都得到了证明。在这些事故中，人为错误导致了一系列灾难性的事项。有些事故向人们敲响警钟，不要一味进行那些只关注系统软硬件的风险评估。它们证明了忽视人为错误这种诱因发生的可能性是多么危险的事情。

B.12.2 用途

HRA 可进行定性或定量使用。如果定性使用，HRA 可识别潜在的人为错误及其原因，降低人为错误发生的可能性；如果定量使用，HRA 可以为 FTA（故障树）或其他技术的人为故障提供基础数据。

B.12.3 输入

HRA 分析方法的输入包括：

——明确人们必须完成的任务的信息；

——实际发生及有可能发生的各类错误的经验；

——有关人为错误及其量化的专业知识。

B.12.4 过程

HRA 过程如下所示：

——问题界定：计划调查/评估过程中有哪种类型的人为参与？

——任务分析：如何执行任务？为了协助任务的执行，需要哪类帮助？

——人为错误分析：任务执行失败的原因？可能出现什么错误？怎样补救错误？

——表示：怎样将这些错误或任务执行故障与其他硬件、软件或环境事项整合起来，从而对整个系

统故障的概率进行计算？

——筛查：有不需要细致量化的错误或任务吗？

——量化：人为错误和故障发生的可能性？

——影响程度评估：哪些错误或任务是最重要的？例如，哪些错误或任务最为危害系统可靠性？

——减少错误：如何提高人因可靠性？

——记录：有关 HRA 的哪些详情应记录在案？

在实践中，HRA 会分步骤进行，尽管某些部分（例如任务分析及错误识别）有时会与其他部分同步进行。

图 B.2 给出了过程示意。

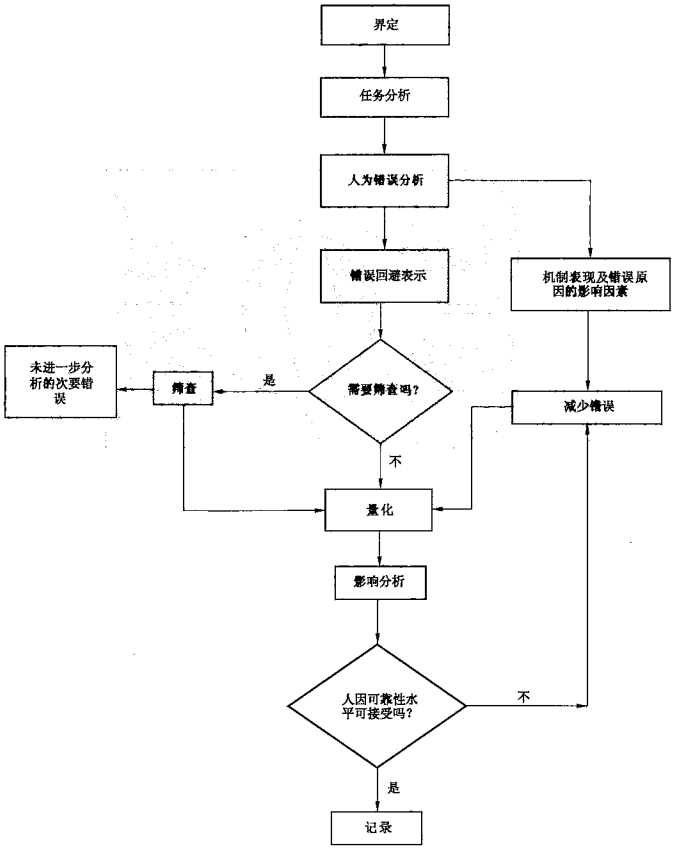

图 B.2 人因可靠性分析

B.12.5 输出

输出包括：

——可能会发生的错误清单以及减少损失的方法(最好通过系统的重新设计)；

——错误模式、错误类型、原因及结果；

——错误所造成风险的定性或定量评估。

B.12.6 优点及局限

HRA 的优点包括：

——HRA 提供了一种正式机制，将人为错误置于系统相关风险的分析中；

——对人为错误的正式分析有利于降低错误所致故障的可能性。

局限包括：

——人的复杂性及多变性导致很难确定那些简单的失效模式及概率；

——很多人为活动缺乏简单的通过/失败模式。HRA 较难处理由于质量或决策不当造成的局部故障或失效。

B.13 以可靠性为中心的维修

B.13.1 概述

以可靠性为中心的维修(Reliability centered maintenance，简称 RCM)是一种识别并确定故障管理策略的方法，目的是高效、有效地实现各类设备必要的安全性、可用性及运行经济性。

现在，RCM 已成为广泛用于各行业内并经过验证而被普遍接受的方法。

RCM 提供了一种决策过程，可以根据设备的安全、运行及经济结果，识别出设备适用且有效的预防性维修要求和退出机制。结束这个过程后，最终可以对执行维修任务或采取其他操作的必要性做出判断。关于使用和应用 RCM 的详细说明可参考 IEC 60300-3-11。

B.13.2 用途

一切任务都离不开人员及环境安全，也离不开关注的运行及经济问题。但是，应该注意的是，考虑的标准将取决于产品的性质及其应用。例如，生产过程在经济上应具有可行性，并且可能对严格的环境因素比较敏感。防护设备则首先应该保证正常运行，而在安全、经济及环境标准方面可能不够严格。通过重点分析故障可能产生严重的安全、环境、经济或运行影响的方面，有利于获得最大的成效。

RCM 用来确保可维护性，主要用于设计和开发阶段，然后在运行和维修阶段实施。

B.13.3 输入

成功地运用 RCM，需要了解设备和结构、运行环境和相关系统、子系统及设备可能的故障以及故障的结果。

B.13.4 过程

RCM 项目的基本步骤如下所示：

——启动和规划；

——功能故障分析；

——任务挑选；

——实施；

——不断完善。

RCM 与风险密切相关，因为它采用的就是风险评估的基本步骤。RCM 与风险评估与失效模式、效应和危害度分析(FMECA)有着相似的类型。

在某些情况下，通过执行维修任务可以消除潜在的故障或是降低其频率及/或结果，而风险识别关注的正是这种情况。这些工作可以通过识别必要的功能及性能标准以及妨碍功能实现的设备和组件故障得以实现。

RCM 的风险分析包括估算无需维修状态下各故障的频率。通过界定失败效果来获得结果。综合故障频率和危险度的风险矩阵有利于对风险进行分级。

随后，通过选择各失效模式适用的故障管理策略来进行风险评价。

整个 RCM 过程应做好大量的记录工作，以供将来参考和检查之用。故障及维修相关数据的采集有助于监督结果并实施改进措施。

B.13.5 输出

维修任务的界定，如状况监控、计划性恢复、计划性替换、故障查找或非预防性维修。这项分析可能带来的其他行动包括重新设计、调整运行或维修程序，或者额外培训。执行任务的时间间隔以及必要的资源都要得到确认。

B.14 压力测试

B.14.1 概述

压力测试是指在极端情景下(例如最不利的情形)，评估系统运行的有效性，及时发现问题和制定改进措施，目的是防止出现重大损失事件。

B.14.2 用途

压力测试广泛应用于各行业的风险评估中，尤其常见于金融、软件等行业。

B.14.3 输入

所需输入数据是：

——界定分析对象；

——召集相关专业人员；

——设想、模拟或试验可能出现的极端情形。

B.14.4 过程

压力测试的具体操作步骤如下：

——针对某一风险管理模型或内控流程，假设可能会发生哪些极端情景。极端情景是指在非正常情况下，发生概率很小，而一旦发生，后果十分严重的事情。假设极端情景时，不仅要考虑本企业或同类企业出现过的历史教训，还要考虑以往不曾出现但将来可能会出现的情形。

——评估极端情景发生时，该风险管理模型或内控流程是否有效，并分析对目标可能造成的损失。

——制定相应措施，进一步修改和完善风险管理模型或内控流程。

以信用风险管理为例。如：某银行拥有一批信用记录良好的客户，该类客户除非发生极端情景，一般不会违约。在日常交易中，该银行只需遵循常规的风险管理策略和内控流程即可。如采用压力测试方法，则设想该批客户在极端情景(如其财产毁于地震、火灾、被盗)下可能会出现违约事故。由此分析一旦出现类似情形，银行可能遭受何种类型和程度的损失。

实施压力测试，一般需要借助敏感性分析、情景分析、头脑风暴法等工具辅助进行。

B.14.5 输出

对潜在风险因素的认识和预防风险的措施建议。

B.14.6 优点及局限

压力测试的优点包括：

——关注非正常情况下的风险情形，是普通风险评估方法的有益补充；

——考虑不同风险之间的相互关系；

——加强对极端情形与潜在危机的认识，预防重大风险的发生。

压力测试不能取代一般的风险管理工具，频繁的进行压力测试并不能解决组织日常的风险管理问题。此外，压力测试的效果取决于是使用者是否可以构造合理、清晰、全面的情景。

B.15 保护层分析(LOPA)

B.15.1 概述

作为一种半定量方法，保护层分析法(Layer protection analysis，简称 LOPA)可估算与不期望事件或危险情景相关的风险，并且将其与风险容许界限比较，以确定现有的控制措施是否合适。

B.15.2 用途

LOPA 典型的应用是在执行了 PHA 之后，以 PHA 的信息为基础进一步考虑安全设计问题。

LOPA 可以定性使用，用来简单分析现有的危害防护措施。LOPA 也可以半定量使用，在应用完 HAZOP 或 PHA 之后进行更为严格的检查。

通过分析各防护措施产生的风险预防效力，LOPA 也可以用来对资源进行合理配置。

B.15.3 输入

LOPA 的输入包括：

——有关风险的基本信息；

——有关现有或建议控制措施的信息；

——原因事件概率、保护层故障、结果措施及可容许风险定义；

——初始原因概率、保护层故障、结果措施及可容许风险定义。

B.15.4 过程

LOPA 可以通过专家团队运用下列程序进行实施：

——识别不良结果的初始原因并查找有关其概率和结果的数据；

——选择一个因果对；

——识别现有的保护层，同时对它们的效力进行分析；

——识别独立保护层(保护层未必都是 IPL)；

——估计每个独立保护层失效的概率；

——保护层的综合影响应与风险承受度进行比较，以确定是否需要进一步的保护。

独立保护层(Independent protection layers，简称 IPL)是一种设备、系统或行动，其能避免某个情景演变成不良结果，并独立于初因事项或任何其他保护层。

IPL 包括：

——设计特点；
——实体保护装置；
——联锁及停机系统；
——临界报警与人工干预；
——事件后实物保护；
——应急反应系统(程序与检查不是 IPL)。

B.15.5 输出

可给出需要进一步采取的控制措施，以及这些控制措施在降低风险方面效果的建议。

B.15.6 优点及局限

LOPA 的优点包括：
——与故障树或其他定量风险分析方法相比，它需要更少的时间和资源，但是比定性的主观判断更为严格；
——它有助于识别并将资源集中在最关键的保护层上；
——它识别了那些缺乏充分安全措施的运行、系统及过程；
——它关注最严重的结果。
局限包括：
——LOPA 每次只能分析一个因果对和一个情景，并没有涉及风险或控制措施之间的相互影响；
——量化的风险可能没有考虑到普通模式的失效；
——LOPA 并不适用于很复杂的情景，例如有很多因果对的情景，或有多种结果影响不同利益相关方的情景。

B.16 业务影响分析(BIA)

B.16.1 概述

业务影响分析(Business impact analysis，简称 BIA)，也称作业务影响评估，旨在分析干扰性风险因素对组织运营的影响方式，同时识别组织是否具备必要的风险管理能力。

具体来说，BIA 可就以下问题达成一致认识：
——识别组织的关键经营过程及其临界状态、职能、相关资源，以及系统组件之间的关键依存关系；
——干扰性事项对组织重要经营目标的实现会产生怎样的影响；
——如何应对干扰因素的影响，以及如何使组织恢复到约定运行水平。

B.16.2 用途

BIA 方法可用来确定干扰性因素的危害性以及过程和相关资源(人员、设备、信息技术)的恢复时间，以确保目标的持续实现。而且，BIA 有助于确定过程、内外部各方以及供应链接口处之间的相互关系。

B.16.3 输入数据

输入包括：
——承担分析并制定计划的小组；
——关于目标、环境及运行和组织的相互依存关系的信息；
——有关组织活动及运行的详情，包括运行过程、辅助资源、与其他组织的关系、外包安排以及利益相关方；

——关键过程的失败造成的财务及运行结果；
——事先准备的调查问卷表；
——组织相关部门的受访者及/或计划联系的利益相关方的名单等。

B.16.4 过程

通过使用调查问卷表、访谈、结构化讨论会或综合运用上述三种方法，可以开展 BIA 活动，识别关键过程，分析这些过程失败可能产生的影响，确定必要的恢复时间范围及辅助资源。

关键步骤包括：
——根据脆弱性分析(Vulnerability assessment)，确认组织的关键过程和输出结果；
——确定在干扰规定的时期内对被识别的关键过程造成的财务及/或运行影响；
——识别关键利益相关方之间的相互依存关系。这可能包括通过供应链说明相互依存关系的性质；
——确定现有资源及干扰过后继续以最低容许水平运行所需的基本资源；
——确定目前使用或计划开发的替代性工作区域和程序。如果在干扰过程中资源或能力无法获得或不够充分，那么可能就要开发替代性的工作区域和程序；
——根据被识别的结果以及职能部门的关键成功因素，确定各过程的最大可容忍故障时间(Maximum acceptable outage time，简称 MAO)，MAO 代表组织所能容忍的能力损失的最大时间段；
——确定任何特定装备或信息技术的目标恢复时间(the recovery time objective，简称 RTO)。RTO 代表组织期望能够恢复运行能力的所需时间；
——确认关键过程的现期准备水平。这可能包括评估过程中的冗余能力(例如备用设备)或替代供应商的存在情况。

B.16.5 输出结果

输出结果包括：
——关键过程及相关依存关系的优先性清单；
——因关键过程失败而带来的财务及运行过程影响的记录；
——用于被识别的关键过程的辅助资源；
——关键过程的故障时间范围以及相关职能的恢复时间范围。

B.16.6 优点及局限

BIA 的优点包括：
——对关键过程的认识，使组织有能力继续实现其既定目标；
——对资源的认识；
——有机会重新界定组织的运行过程，以增强组织的灵活性。

局限包括：
——那些参与完成调查问卷或讨论会的参与人员可能缺乏某些知识；
——小组气氛可能会影响到关键过程的全面分析；
——对恢复要求有简单化或过于乐观的期望；
——难以获得组织运行及活动的足够的认识水平。

B.17 潜在通路分析(SCA)

B.17.1 概述

潜在通路分析(Sneak circuit analysis，简称 SCA)是一种用于识别系统设计错误的方法。潜在状态

不是因部件故障产生的，而是一种可能会抑制预期功能或引起不良事项的潜在硬件、软件或集成的状态。这些状况的特点是具有随意性，在最严格的标准化系统检查中也很难检测出来。潜在状态可能会引起运行不当、系统可用性缺失、程序延时或者甚至造成人员伤亡。

B.17.2 用途

在20世纪60年代后期，潜在通路分析为美国航空航天局(NASA)所开发，用以核实产品设计的完整性及功能实现。潜在通路分析是一种发现非故意电路路径的有效工具，有利于设计出将各功能独立处理的解决方案。随着技术进步，潜在通路分析的工具也一定在发展，潜在分析(Sneak Analysis)是用来描述潜在通路分析扩大范围的术语。潜在分析涵盖并超出了潜在通路分析的范畴。潜在分析可以使用任何技术来确定软硬件问题。潜在分析工具可以将几种分析工具例如故障树、失效模式和效应分析(FMEA)、可靠性估计(Reliability estimates)等整合到一项分析中，从而节省时间和项目成本。

B.17.3 输入

潜在分析是一种独特的设计过程，因为它利用不同的工具(如网络树、网络森林、提示语和问题等，帮助分析者发现潜在状态)来发现具体的问题。网络树和森林是对实际系统进行的拓扑分组。每个网络树代表一种次级功能并显示了可能影响次级功能输出的所有输入数据。将那些促成特定系统输出的网络树结合起来就能建构森林。一个合适的网络森林可以说明系统输出所有相关的输入数据。

B.17.4 过程

开展潜在分析的基本步骤包括：

——数据准备；

——网络树的建构；

——网络路径的评估；

——最终建议与报告。

B.17.5 输出

潜在通路是系统内的意外路径或逻辑流。在特定状况下，意外路径或逻辑流会诱发不良功能或抑制预期功能。路径可能包括硬件、软件、操作人员行为以及这些因素的综合。潜在通路并不是硬件故障的结果，而是因设计疏忽而嵌入系统、通过编码进入软件程序，或者由于人为错误引发的潜在状况。四类潜在状况包括：

——潜在路径：电流、能量或逻辑顺序沿着非预计方向流动的意外路径；

——潜在时序：以意外或相互冲突的顺序发生的事项；

——潜在表述：对系统运行状况含混不清或错误的显示，可能会使系统或操作人员采取不当行为；

——潜在标识：对系统功能进行不正确或不准确的命名，例如，系统输入数据、控制措施及显示总线，可能会造成操作人员对系统的不当操作。

B.17.6 优点及局限

SCA的优点包括：

——潜在分析有利于分析人员识别设计错误；

——与HAZOP(危险与可操作性分析)一起使用时会有最佳效果；

——非常有利于处理那些有多重情况的系统，例如配料车间和半配料车间。

局限包括：

——将其应用于电路、加工厂、机械设备或软件时，分析过程会有所不同；

——使用效果依赖于是否可以建立起正确的网络树。

B.18 风险指数

B.18.1 概述

风险指数(Risk indices)是对风险的半定量测评,是利用顺序尺度的记分法得出的估算值。风险指数可以用来对使用相似准则的一系列风险进行比较。尽管是风险评估的组成部分,风险指数主要用于风险分析。尽管可以获得量化的结果,但风险指数本质上还是一种对风险进行分级和比较的定性方法,使用数字完全是为了便于操作。

B.18.2 用途

如果充分理解系统,可以用指数对与活动相关的不同风险分级。指数允许将影响风险等级的一系列因素整合为单一的风险等级数字。

风险指数可作为一种范围划定工具用于各种类型的风险,以根据风险水平划分风险。这可以确定哪些风险需要更深层次的分析以及可能进行定量评估。

B.18.3 输入

输入数据来源于对系统的分析,或者对背景的宽泛描述。这就要求很好地了解风险的各种来源、可能的路径以及可能影响到的方面。像故障树分析、事件树分析和一般的决策分析工具都可以用来支持风险指数的开发。

由于顺序尺度的选择在一定程度上具有任意性,因此,需要充分的数据来确认指数。

B.18.4 过程

第一步是理解并描述系统。一旦系统得到确认,就要对各组件确定得分,再将这些得分结合起来,以提供综合指数。例如,在环境背景中,来源、途径及接收方将被打分。在有些情况下,每个来源可能会有多种路径和接收方。根据考虑系统客观现状的计划将单个得分进行综合。关键是,系统各部分的得分(来源、途径及接收方)应在内部保持一致,同时保持其正确关系。对风险要素(例如,概率、暴露及后果)或是增加风险的因素打分。

可以设计合适的指数模型对各因素的得分进行加、减、乘及/或除的运算。通过将得分相加来考虑累积效果(例如,将不同路径的得分相加)。严格地讲,将数学公式用于顺序得分是无效的,因此,一旦打分系统得以建立,必须将该模型用于已知系统,以便确认其有效性。确定指数是一种迭代方法,在分析师人员得到满意的确认结果之前,可以尝试几种不同的系统以将得分进行综合。

B.18.5 输出

输出结果是与特定来源有关的一系列数字(综合指数),并可以与为其他来源开发的指数或是按相同方式建模的一系列数字进行比较。

B.18.6 优点及局限

风险指数的优点包括:

——风险指数可以提供一种有效的划分风险等级的工具;

——可以让影响风险等级的多种因素整合到对风险等级的分析中。

局限包括:

——如果过程(模式)及其输出结果未得到很好确认,那么可能使结果毫无意义。输出结果是风险值这一点可能会被误解和误用,例如在随后的成本效益分析中。

——在很多使用风险指数的情况下，缺乏一个基准模型来确定风险因素的单个尺度是线性的、对数的还是某个其他形式，也没有固定的模型可以确定如何将各因素综合起来。在这些情况下，评级本身是不可靠的，对实际数据进行确认就显得尤其重要。

B.19 故障树分析(FTA)

B.19.1 概述

故障树(Fault tree analysis，简称 FTA)是用来识别和分析造成特定不良事件(称作顶事件)的可能因素的技术。造成故障的原因因素可通过归纳法进行识别，也可以将特定事故与各层原因之间用逻辑门符号连接起来并用树形图进行表示。树形图描述了原因因素及其与重大事件的逻辑关系。

故障树中识别的因素可以是与硬件故障、人为错误或其他引起不良事项的相关事项。

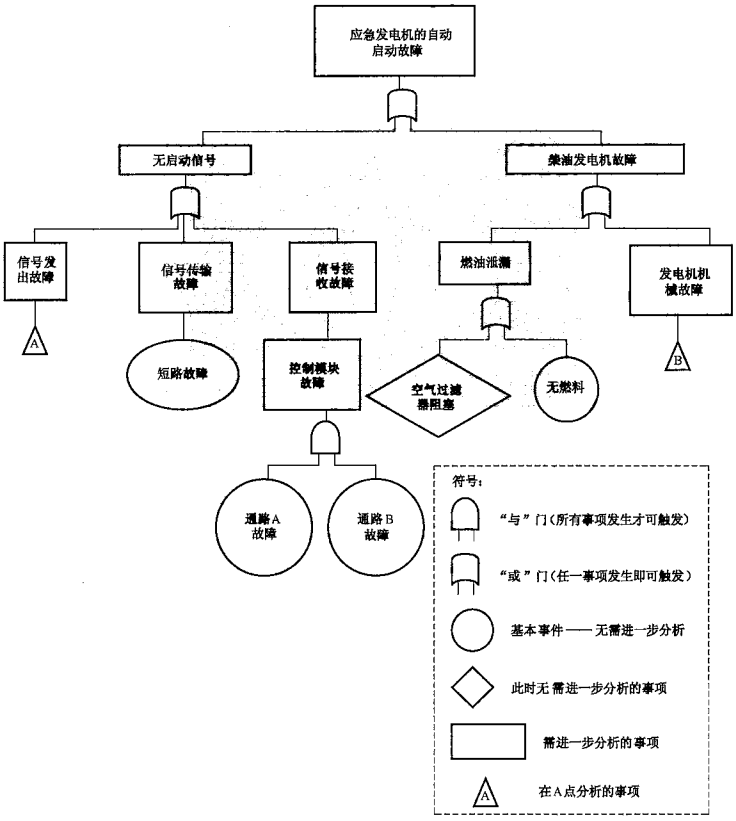

图 B.3 FTA 示例

B.19.2 用途

故障树可以用来对故障(顶事件)的潜在原因及途径进行定性分析,也可以在掌握原因事项概率的相关数据之后,定量计算重大事件的发生概率。图 B.3 是一个 FTA 的应用示例。

故障树可以在系统的设计阶段使用,以识别故障的潜在原因并在不同的设计方案中进行选择;也可以在运行阶段使用,以识别重大故障发生的方式和导致重大事件的各类路径的相对重要性;故障树还可以用来分析已出现的故障,以便通过图形来显示不同事项如何共同作用造成故障。

B.19.3 输入

对于定性分析,需要了解系统及故障原因、系统失效的方式;对于定量分析,需要了解故障树中各基本事件的故障率或者失效的可能性。

B.19.4 过程

建构故障树的步骤包括:

——界定分析对象系统和需要分析的各对象事件(顶事件);

——从顶事件入手,识别造成顶事件的直接原因或失效模式;

——调查原因事件,对每个原因/失效模式进行分析,以识别造成故障的原因(设备故障、人员失误以及环境不良因素等);

——分步骤地识别不良的系统操作方式,沿着系统自上而下地分析,直到进一步分析不会产生任何成效为止,处于分析中系统最低水平的事项及原因因素称作基本事件;

——定性分析,按故障树结构进行简化,求出最小割集和最小径集,确定各基本事件的结构重要度;

——定量分析,找出各基本事件的发生概率,计算出顶事件的发生概率,计算出概率重要度和临界重要度,对于每个控制节点而言,所有的输入数据都必不可少,并足以产生输出事项。对于故障树中的逻辑冗余部分,可以通过布尔代数运算法则来进行简化。

除了估算顶事件发生的可能性之外,还要识别那些形成顶事件独立路径的最小分割集合,并计算它们对顶事件的影响。除了简单的故障树之外,当故障树存在几处重复事件时,需要使用软件包正确处理计算,并计算最小割集。软件工具有助于保证一致性、正确性和可检验性。

B.19.5 输出

故障树分析的输出结果包括:

——顶事件发生方式的示意图,并可显示各路径之间的相互关系;

——最小分割集合清单(单个故障路径),并说明每个路径的发生概率(如果有相关数据);

——顶事件的发生概率。

B.19.6 优点及局限

故障树(FTA)的优点包括:

——它提供了一种系统、规范的方法,同时有足够的灵活性,可以对各种因素进行分析,包括人际交往和客观现象等;

——运用简单的"自上而下"方法,可以关注那些与顶事件直接相关故障的影响;

——FTA 对具有许多界面和相互作用的分析系统特别有用;

——图形化表示有助于理解系统行为及所包含的因素;

——对故障树的逻辑分析和对分割集合的识别有利于识别高度复杂系统中的简单故障路径。

局限包括:

——如果基础事件的概率有较高的不确定性，计算出的顶事件的概率的不确定性也较高；
——有时很难确定顶事件的所有重要途径是否都包括在内；
——故障树是一个静态模型，无法处理时序上的相互关系；
——故障树只能处理二进制状态（有故障/无故障）；
——虽然定性故障树可以包括人为错误，但是一般来说，各种程度或性质的人为错误引起的故障无法包括在内；
——分析人员必须非常熟悉对象系统，具有丰富的实践经验。

B.20 事件树分析（ETA）

B.20.1 概述

事件树分析（Event tree analysis，简称 ETA）着眼于事故的起因，即初因事件。事件树从事件的起始状态出发，按照一定的顺序，分析初因事件可能导致的各种序列的结果，从而定性或定量地评价系统的特性。由于在该方法中事件的序列是以树图的形式表示，故称事件树。

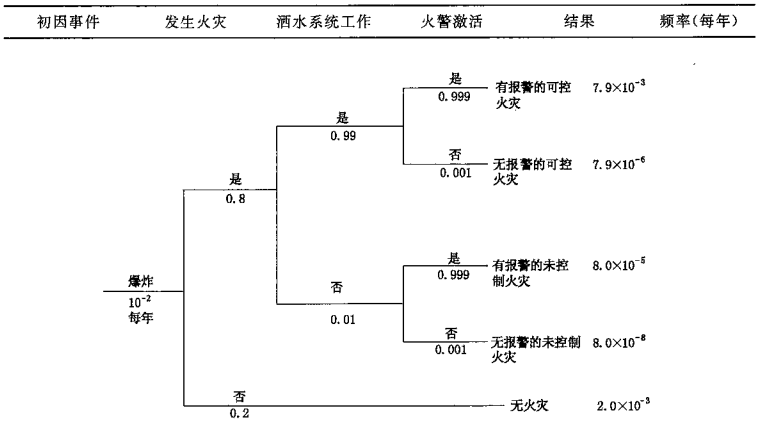

图 B.4 事件树示例

图 B.4 显示了一个事件树的简单示例。

ETA 具有散开的树形结构，考虑到其他系统、功能或障碍，ETA 能够反映出引起初因事件加剧或缓解的事件。

B.20.2 用途

ETA 分析适用于多环节事件或多重保护系统的风险分析和评价，既可用于定性分析，也可用于定量分析。

ETA 可以用于产品或过程生命周期的任何阶段。它可以进行定性使用，有利于群体对初始事件之后可能出现的情景进行集思广益，同时就各种处理方法、障碍或旨在缓解不良结果的控制手段对结果的影响方式提出各种看法。

定量分析有利于分析控制措施的可接受性。这种分析大都用于拥有多项安全措施的失效模式。

ETA 法是从决策树(Decision tree)逐渐演化而来的，用于对可能带来损失或收益的初因事件建立模型。但是，在追求最佳收益路径的情况下，更经常地使用决策树(Decision tree)建立模型。

B.20.3 输入

输入包括：

——相关初始事项清单；

——关于应对、障碍和控制及其失效概率的信息；

——了解最初故障加剧的过程。

B.20.4 过程

事件树首先要挑选初始事件。初始事件可能是粉尘爆炸或是停电这样的事项。那些旨在缓解结果的现有功能或系统应按时序列出。用一条线来代表每个功能或系统的成功或失败。每条线都应带有一定的失效概率，同时通过专家判断或故障树分析的方法来估算这种条件概率。这样，初始事件的不同途径就得以建模。

注意，事件树的可能性是一种有条件的可能性，例如启动洒水功能的可能性并不是正常状况下测试得到的可能性，而是爆炸引起火灾状况下的可能性。

事件树的每条路径代表着该路径内各种事项发生的可能性。鉴于各种事项都是独立的，结果的概率可用单个条件概率与初因事项频率的乘积来表示。

B.20.5 输出

ETA 的输出结果包括：

——对潜在问题进行定性描述，并将这些问题视为包括初始事件、同时能产生各类问题的综合事件；

——对各类事件的发生频率或概率以及事件的发生序列、各类事件的相对重要性的估算；

——降低风险的建议措施清单；

——建议措施效果的定量评价。

B.20.6 优点及局限

ETA 的优点包括：

——ETA 用简单图示方法给出初因事项之后的全部潜在情景；

——它能说明时机、依赖性，以及在故障树模型中很繁琐的多米诺效应。

——它清晰地体现了事件的发展顺序，而使用故障树是不可能表现的。

局限包括：

——为了将 ETA 作为综合评估的组成部分，一切潜在的初因事项都要进行识别。这可能需要使用其他分析方法(如 HAZOP，PHA)，但总是有可能错过一些重要的初因事项；

——事件树只分析了某个系统的成功及故障状况，很难将延迟成功或恢复事项纳入其中；

——任何路径都取决于路径上以前分支点处发生的事项，因此要分析各可能路径上众多从属因素。然而，人们可能会忽视某些从属因素，例如通用组件、公用系统以及操作人员等。如果不认真处理这些从属因素，就会导致风险评估过于乐观。

B.21 因果分析

B.21.1 概述

因果分析(Cause and consequence analysis，简称 CCA)综合了故障树分析和事件树分析。它开始

于关键事件，同时通过结合“是/否”逻辑来分析结果，可识别出所有相关的原因和潜在结果，包括故障可能发生的条件，或者旨在减轻初始事件后果的系统失效。因果分析可应用于产品或系统生命周期的任何阶段；可以定性使用，也可用作定量分析。

最初，因果分析是作为关键安全系统的可靠性工具而开发出来的，可以让人们更全面地认识系统故障。类似于故障树分析（见附录 B.19），它用来表示造成关键事件的故障逻辑，但是，通过对时序故障的分析，它比故障树的功能更强大。这种方法可以将时间滞延因素纳入到结果分析中，而这在事件树分析（见附录 B.20）中是办不到的。

B.21.2 用途

因果分析方法可分析某个系统在关键事件之后可能的各种路径。如果进行量化，该方法可估算出某个关键事件过后各种不同结果发生的概率。由于因果图中的每个序列是子故障树的结合，因此因果分析可作为一种建立大故障树的工具。

B.21.3 输入

与系统及其失效模式和故障情景相关的各类数据。

B.21.4 过程

图 B.5 说明了典型的因果分析过程。

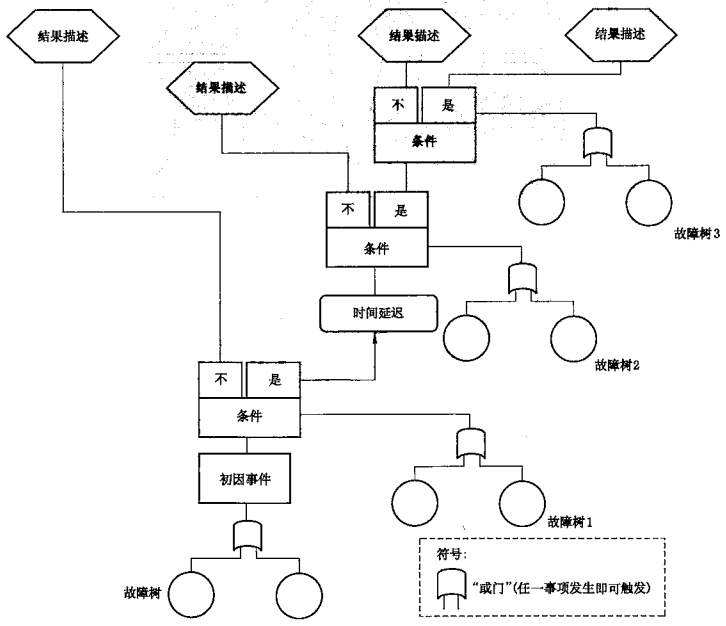

图 B.5 因果分析示例

进行因果分析的步骤包括：

——识别关键事件(或初因事件)(类似于故障树的顶事件及事件树的初因事件)；

——绘制并验证关键事件的故障树；

——确定需考虑条件的顺序。这应该是一种逻辑顺序，例如它们发生的时序；

——建构不同条件下的结果路径。这一点类似于事件树，但事件树路径的划分被表示为贴有适用特定条件的栏；

——如果各条件栏的故障为独立故障，则可以计算各故障的发生概率。要做到这一点，首先是确定条件栏内每个输出结果的概率(如果可以的话，使用相关的故障树)。通过将各次序条件的概率相乘，就可以得出产生特定结果的任一次序的概率，该次序条件结束于上述特定结果。如果一个以上的次序最终有相同的结果，那么各次序的概率应相加。如果某个序列中各条件的故障存在依存关系(例如，停电会造成多个条件出现故障)，那么必须在计算前分析依存关系。

B.21.5 输出

因果分析的结果可用图形表示，对系统故障的原因进行图形表示既可说明原因，也可说明结果。通过对引起关键事件特定条件发生的概率进行分析，我们就可以估算出各潜在结果发生的概率。

B.21.6 优点及局限

因果分析的优点相当于事件树及故障树的综合优点。而且，由于其可以分析随时间发展变化的事项，因果分析克服了那两种技术的局限，提供了系统的全面视角。

局限是该方法的建构过程要比故障树和事件树更为复杂，同时在定量过程中必须处理依存关系。

B.22 根原因分析(RCA)

B.22.1 概述

为了避免重大损失的再次发生，对重大损失进行的分析通常称作根原因分析(Root cause analysis，简称 RCA)或者损失分析(Loss analysis)。RCA 试图识别事故的根本或最初原因，而不是仅仅处理非常明显的表面“症状”。

B.22.2 用途

RCA 适用于各种环境，拥有广泛的使用范围：

——安全型 RCA 用于事故调查和职业健康及安全；

——故障分析 RCA 用于与可靠性及维修有关的技术系统；

——生产型 RCA 用于工业制造的质量控制领域；

——过程型 RCA 关注的是经营过程；

——作为上述领域的综合体，系统型 RCA 主要用于处理复杂系统的变革管理、风险管理及系统分析。

B.22.3 输入

RCA 的基本输入数据是指从故障或损失中搜集的证据。分析中也可以考虑其他类似故障的数据。其他输入数据可以是为了测试具体假设而得出的结果。

B.22.4 过程

识别出 RCA 的需求之后，应指定一群专家开展分析并提出建议。专家的类型主要取决于分析故

障时所需的具体专业知识。

虽然可以使用不同的方法进行分析，但开展 RCA 的基本步骤是相似的，包括以下方面：

——组建团队；
——确定 RCA 的范围及目标；
——搜集有关故障或损失的数据及证据；
——开展结构化分析，以确定根本原因；
——找出解决方案并提出建议；
——执行建议；
——核实所执行建议的成效。

结构化分析方法可以包括下列某一种方法：

——5-why 法，即反复询问“为什么?”，以剥离原因层及次原因层；
——失效模式和效应分析；
——故障树分析；
——鱼骨图(鱼刺图)；
——帕累托分析；
——根原因图。

对可能原因评价经常开始于明显的客观原因，然后是人为的原因，最后是潜在的管理或基本原因。相关各方必须对识别出的事故原因进行控制或消除，以便使纠正行为取得效果并富有价值。

B.22.5 输出

RCA 的输出结果包括：

——记录收集的数据及证据；
——分析假设；
——归纳有关最有可能造成故障或损失的原因；
——纠正行为的建议。

B.22.6 优点及局限

RCA 的优点包括：

——让合适专家在团队环境下工作；
——结构化分析；
——分析各种可能的假设；
——记录结果；
——需要提出最终的建议。

局限性包括：

——未必有所需的专家；
——关键证据可能在故障中被毁或在清理中被删除；
——团队可能没有足够的时间或资源来充分评估情况；
——可能无法充分执行建议。

B.23 决策树分析

B.23.1 概述

考虑到不确定性结果，决策树(Decision tree)以序列方式表示决策的选择和结果，并用树形图的形

式进行表示。类似于事件树，决策树开始于初因事项或是最初决策，考虑随后可能发生的事项及可能做出的决策，它需要对不同路径和结果进行分析。

B.23.2 用途

决策树可用于项目风险管理和其他环境中，以便在不确定的情况下选择最佳的行动步骤。图形显示也有助于决策依据的快速沟通。

B.23.3 输入

包含各个决策点的项目计划、各决策的可能结果、可能影响决策的偶然事件的信息。

B.23.4 过程

决策树开始于最初决策，随着决策的继续，在各个决策点上，不同的事项会发生，通过估算各事项发生的可能性以及相应的成本或收益，使用者可选择最佳决策路径。

B.23.5 输出

输出包括：

——显示可以采取不同选择的风险逻辑分析；

——每一个可能路径的预期值计算结果。

B.23.6 优点及局限

决策树分析的优点包括：

——对于决策问题的细节提供了一种清楚的图解说明；

——能够计算到达一种情形的最优路径。

局限包括：

——大的决策树可能过于复杂，不容易与其他人交流；

——为了能够用树形图表示，可能有过于简化背景环境的倾向。

B.24 蝶形图分析

B.24.1 概述

蝶形图分析(Bow tie analysis)是一种简单的图解形式，用来描述并分析某个风险从原因到结果的路径。该方法可被视为分析事项起因(由蝶形图的结代表)的故障树和分析事项结果的事件树这两种方法的统一体。但是，蝶形图的关注重点是在风险形成路径上存在哪些预防措施及其实际效果。在建构蝶形图时，首先要从故障树和事件树入手，但是，这种图形大都在头脑风暴式的讨论会上直接绘制出来。

B.24.2 用途

蝶形图分析被用来显示风险的一系列可能的原因和后果。如果人们更重视的是确保每个故障路径都有一个障碍或控制，那么就可以使用蝶形图分析。当导致故障的路径清晰而独立时，蝶形图分析就非常有用。

与故障树及事件树相比，蝶形图通常更易于理解，因此，在使用更复杂的技术才能完成分析的情况下，它会成为一种有用的沟通工具。

B.24.3 输入

对于风险的原因和结果以及可能预防风险的障碍及控制措施的认识。

B.24.4 过程

蝶形图的实施步骤如下：

——识别需要分析的具体风险，并将其作为蝶形图的中心结；

——列出造成结果的原因；

——识别由风险源到事故的传导机制；

——在蝶形图左手侧的每个原因与结果之间划线，识别那些可能造成风险升级的因素并将这些因素纳入图表中；

——如果某些因素可有效控制风险原因的升级，用条形框列出这些“控制措施”；

——在蝶形图右侧，识别风险不同的潜在结果，并以风险为中心向各潜在结果处绘制出放射状线条；

——如果某些因素可有效控制风险结果的升级，用条形框列出这些“控制措施”；

——支持控制的管理职能（如培训和检查）应表示在蝶形图中，并与各自对应的控制措施相联系。

在路径独立、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效果的具体数字。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，因此结果并不清晰。更合适的做法是运用FTA及ETA进行定量分析。

B.24.5 输出

输出结果是一个简单的图表，说明了主要的故障路径以及预防或减缓不良结果或者刺激及促进期望结果的现有障碍。一个蝶形图示例如图B.6所示。

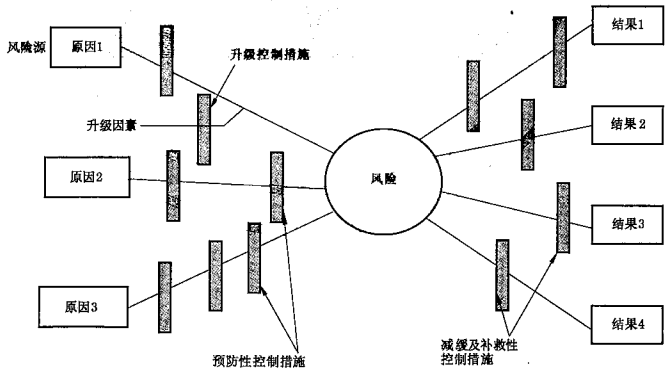

图 B.6 不良结果的蝶形图

B.24.6 优点及局限

蝶形图分析的优点：

——用图形清晰表示问题，便于理解；

——关注的是为了到达预防及减缓目的而确定的障碍及其效力；
——可用于期望结果；
——使用时不需要较高的专业知识水平。
局限包括：
——无法描述当多种原因同时发生并产生结果时的情形(例如，故障树中有“闸”这个概念来描述蝶形图的右手侧)；
——可能会过于简化复杂情况，尤其是在试图量化的时候。

B.25 层次分析法

B.25.1 概述

在进行社会、经济以及科学领域问题的系统分析中，常常面临由相互关联、相互制约的众多因素构成的复杂而往往缺少定量数据的系统。层次分析法(Analytic hierarchy process，简称 AHP)为这类问题的决策和排序提供了一种新的、简洁而实用的建模方法，它特别适用于那些难于完全定量分析的问题。

B.25.2 用途

层次分析法以其系统性、灵活性、实用性等特点特别适合于多目标、多层次、多因素的复杂系统的决策，在目标因素结构复杂且缺乏必要数据的情况下使用更为方便，同时它也被广泛应用于社会、经济、科技、规划等很多领域的评价、决策、预测、规划等。

B.25.3 输入

对任意两因素的相对重要性进行比较判断，给予量化。为保证输入的比较值真实可信，通常可以用德尔菲法、头脑风暴法等进行操作。

B.25.4 过程

运用层次分析法建模，大体上可按下面四个步骤进行：
——建立递阶层次结构模型；
——构造出各层次中的所有判断矩阵；
——层次单排序及一致性检验；
——层次总排序及一致性检验。
其中后二个步骤在整个过程中需要逐层地进行。

B.25.5 输出

各种方案相对于总目标的重要排序。

B.25.6 优点及局限

AHP 法较好地体现了系统工程学定性与定量分析相结合的思想。在决策过程中，决策者直接参与决策过程，并且其定性思维过程被数学化、模型化，而且还有助于保持思维过程的一致性。

层次分析法的局限性，主要表现在：
——很大程度上依赖于人们的经验，主观因素的影响很大，它至多只能排除思维过程中的严重非一致性，却无法排除决策者个人可能存在的严重片面性；
——比较、判断过程较为粗糙，不能用于精度要求较高的决策问题。

B.26 在险值法(VaR)

B.26.1 概述

在过去的几年里,一些银行和监管部门普遍地运用在险值法(Value at Risk,简称 VaR)衡量风险。在险值法又被称为"风险价值"或"在险价值",是指在一定的置信水平下,某一金融资产(或证券组合)在未来特定的一段时间内的最大可能损失。与传统风险度量手段不同,VaR 完全是基于统计分析基础上的风险度量技术,它的产生是 JP 摩根公司用来计算市场风险的产物,随后逐步被引入信用风险管理领域。目前,VaR 已成为国外大多数金融机构广泛采用的衡量金融风险大小的方法。

在实际工作中,对于 VaR 的计算和分析可以使用多种计量模型,如参数法、历史模拟法和蒙特卡罗模拟法。参数法是 VaR 计算中最为常用的方法。以下以参数法为例介绍该方法的大致特点。

B.26.2 用途

利用 VaR 法可以比较全面地描述和评估风险。许多风险度量方法,只能用来度量一类资产的风险或一类特定的风险,而 VaR 法不依赖个别风险的特性或受资产种类的限制,具有整体性。因其适用于各种风险,所以 VaR 法可提供一个基准单位,用来比较不同的风险。比如,企业可以用 VaR 法统一度量其面临的市场风险、信用风险等。另外,VaR 法可以对企业管理层的资源配置和投资决策起到参考作用,如衡量公司各产品业绩、调整交易员的收益行为、实施风险限额和头寸控制等。

VaR 法也可以应用于投资组合之中,投资者可以通过成分 VaR 来判断投资组合中哪笔交易对投资组合的风险暴露起到了对冲效果,从而优先把新投资投向该交易。在险值的概念还可以用来衡量诸如企业现金流和盈利的风险。这就是所谓的现金流在险值和收益在险值。

B.26.3 输入

使用参数法计算 VaR 仅需要将市价、当前头寸面临的风险和风险数据三种数据相结合,因此比较易于操作。

B.26.4 过程

参数法利用资产组合的价值函数与市场因子间的近似关系、市场因子的统计分布(方差-协方差矩阵)简化 VaR 计算。

参数法的主要计算步骤包括:

——列出各种风险因素;

——对投资组合中所有金融工具的线性风险进行映射;

——汇总不同金融工具的风险;

——估计风险因子的协方差矩阵;

——计算总体投资组合风险。

由于在使用参数法时,一般假定资产收益率服从正态分布,这对于股票、债券、商品等基础资产以及外汇远期等线性衍生产品而言是恰当的,但对期权等非线性衍生品而言,由于它们的收益分布是非正态的,即使假设标的资产收益率正态分布,经过非线性收益型态转换后,仍有巨大的偏移。因此,该方法仅适用于线性资产和线性衍生品。

VaR 基本模型见式(B.1):

$$\mathrm{VaR} = E(\omega) - \omega^{*} \qquad \cdots\cdots(\mathrm{B.1})$$

式中:

$E(\omega)$——资产组合的预期价值;

ω ——资产组合的期末价值；

ω^* ——置信水平 α 下投资组合的最低期末价值。

又设

$$\omega=\omega_0(1+R) \qquad \cdots\cdots(B.2)$$

式中：

ω_0——持有期初资产组合价值；

R ——设定持有期内(通常一年)资产组合的收益率。

$$\omega^*=\omega_0(1+R^*) \qquad \cdots\cdots(B.3)$$

式中：

R^* ——资产组合在置信水平 α 下的最低收益率。

根据数学期望值的基本性质，将式(B.2)、式(B.3)代入式(B.1)，有

$$\mathrm{VaR}=\omega_0[E(R)-R^*] \qquad \cdots\cdots(B.4)$$

式(B.4)即为该资产组合的 VaR 值，根据式(B.4)，如果能求出置信水平 α 下的 R^*，即可求出该资产组合的 VaR 值。

在估计 VaR 值时，置信区间和时间段的选取依赖于我们的管理需要和风险本身的特性。例如，商业银行通常采用 95%或 99%的置信区间，国际银行业监管机构的巴塞尔协议则规定商业银行应使用 99%的置信区间和 10 天的时间段。

B.26.5 输出

VaR 法可以给出特定持有期内、一定置信水平下资产组合面临的最大损失，有效描述资产组合的整体市场风险状况。

B.26.6 优点及局限

VaR 法的优点包括：

——过程简单，结果简洁，非专业背景的投资者和管理者也可以通过 VaR 值对风险进行评判；

——可以事前计算风险，不像以往风险管理的方法都是在事后衡量风险大小；

——不仅能计算单个金融工具的风险，还能计算由多个金融工具组成的投资组合风险。

局限包括：

——过分依赖统计数据和模型，当统计数据不足时难以支持可信赖的 VaR 模型，比如一次性投资决策的数据；

——VaR 方法衡量的主要是市场风险，如单纯依靠 VaR 方法，可能会忽视其他风险；

——VaR 值表明的是一定置信度内的最大损失，但并不能排除高于 VaR 的损失发生的可能性；

——VaR 值描述的是正常的市场条件下的情景。在极端情景下，VaR 可能就会失去作用。因此，在使用 VaR 值时，要结合其他的方法去进一步考虑这些极端的情形，例如使用情景分析和压力测试的分析方法。

B.27 均值-方差模型

B.27.1 概述

均值-方差模型(Mean-Variance Model)是组合投资理论研究和实际应用的基础，由美国经济学家马柯维茨(Markowitz)提出，因此又称为 Markowitz 模型。证券及其他风险资产的投资者们面对着两个核心问题：即预期收益与风险，他们期望尽可能高的收益率和尽可能低的不确定性。如何测定组合投

资的风险与收益，并平衡这两项指标进行资产分配，是市场投资者迫切需要解决的问题。均值-方差模型即可用于这一场合。从所有可能的证券组合中选择一个最优的组合，使收益和风险这两个相互制约的目标达到最佳平衡。对于给定的收益水平，利用该模型可以求出方差意义下最小风险的组合。

均值-方差模型揭示了"资产的期望收益由其自身的风险的大小来决定"这一重要结论，即资产（单个资产和组合资产）由其风险大小来定价，单个资产价格由其方差或标准差来决定，组合资产价格由其协方差来决定。

B.27.2 用途

该方法常用于实际的证券投资和资产组合决策。

B.27.3 输入

预期收益率及各项目的风险概率信息。

B.27.4 过程

均值-方差模型如下所示。

目标函数：$\min\sigma^2(R_p)=\sum\sum x_i x_j \mathrm{cov}(R_i,R_j)$，其中 $R_p=\sum x_i R_i$。

限制条件：$\sum x_i=1$

$x_i\geqslant 0, i=1,2,\cdots,n$

其中 R_p 为组合收益，R_i 为第 i 只股票的收益，x_i、x_j 为证券 i、j 的投资比例，$\sigma^2(R_p)$ 为组合投资方差（组合总风险），$\mathrm{cov}(R_i,R_j)$ 为两个证券之间的协方差。

上式表明，在限制条件下如何使组合风险 $\sigma^2(R_p)$ 最小，可通过拉格朗日目标函数求得。其经济学意义是，投资者可预先确定一个期望收益，通过上式可确定投资者在每个投资项目（如股票）上的投资比例（项目资金分配），使其总投资风险最小。不同的期望收益就有不同的最小方差组合，这就构成了最小方差集合。

B.27.5 输出

在给定收益率下的最小风险组合或预定风险下的最大收益组合。

B.27.6 优点及局限

均值-方差模型通过数理方法描绘出了资产组合选择的最基本、最完整的框架，具有开创性，是目前投资理论和投资实践的主流方法。

该模型的局限在于没有考虑到收益的非正态分布，而多数实证研究表明证券收益率不一定服从正态分布；另一方面该方法计算复杂，特别是运用于多个项目的投资组合问题时，这种计算量更为庞大。

B.28 资本资产定价模型

B.28.1 概述

资本资产定价模型（Capital asset pricing model，简称 CAPM），是在投资组合理论和资本市场理论基础上形成发展起来的，主要研究证券市场中资产的预期收益率与风险资产之间的关系，以及均衡价格是如何形成的。该模型运用一般均衡模型刻划所有投资者的集体行为，揭示在均衡情况下证券风险与收益之间关系的经济本质。目前，资本资产定价模型被公认为是金融市场现代价格理论的主干，使丰富的金融统计数据可以得到系统而有效的利用。此模型亦被广泛用于实证研究并因而成为不同领域中决

策的重要基础。

该理论的前提假设包括以下几点：市场是均衡的，并不存在摩擦；市场参与者都是理性的；不存在交易费用；税收不影响资产的选择和交易；投资总风险可以用方差或标准差表示，系统风险可用 β 系数表示；非系统性风险可通过多元化投资分散掉，不发挥作用，只有系统性风险发挥作用。

B.28.2 用途

CAPM 理论广泛应用于投资决策及公司理财领域，一般用于评估已经上市的不同证券价格的合理性；帮助确定准备上市证券的价格；能够估计各种宏观和宏观经济变化对证券价格的影响。

B.28.3 输入

输入数据主要包括预期回报率和无风险利率等相关信息，以及当前市场背景的宽泛描述。

B.28.4 过程

资本资产定价理论认为，一项投资所要求的必要报酬率取决于以下 3 个因素：

a) 无风险报酬率，即将国债投资（或银行存款）视为无风险投资；

b) 市场平均报酬率，即整个市场的平均报酬率，如果一项投资所承担的风险与市场平均风险程度相同，该项报酬率与整个市场平均报酬率相同；

c) 投资组合的系统风险系数即 β 系数，是某一投资组合的风险程度与市场证券组合的风险程度之比。

CAPM 见式(B.5)：

$$E(R_i)=R_f+(R_m-R_f)\beta_i \qquad \cdots\cdots(B.5)$$

$E(R_i)$ 表示投资组合 i 的期望收益率，R_f 是无风险资产的报酬率，R_m 是市场均衡组合的报酬率，β 是投资组合 i 的 β 系数。β 越大，系统性风险越高，要求的报酬率越高；反之，β 越小，要求的报酬率越低。

CAPM 是通过比较一项资本投资的回报率与投资于整个股票市场的回报率，来衡量该投资的风险贴水。如果该资产是股票，其 β 通常可以用统计数据估算出来。但当资产是一家新工厂时，确立 β 比较困难。许多公司因此利用公司的资本成本作为正常的贴现率，公司资本成本是公司股票的预期回报率（取决于该股票的 β）和它偿付债务的利息率的加权平均数。只要有关的资本投资对整个公司是有代表性的，这一方法可以使用。

B.28.5 输出

CAPM 模型说明了单个证券投资组合的期望受益率与相对风险程度间的关系。

B.28.6 优点及局限

CAPM 模型是金融是市场价格理论的经典模型，作为第一个不确定性条件下的资产定价的均衡模型，具有重大的历史意义。由于股票等资本资产未来收益的不确定性，CAPM 的实质是讨论资本风险与收益的关系。该模型合理简明的表达了这一关系，即：高风险伴随着高收益。

CAPM 模型由于其严格的理论假设和对现实环境的高度抽象，影响和限制了其应用范围和效果。

B.29 FN 曲线

B.29.1 概述

FN 曲线(FN Curves)表示的是人群中有 N 个或更多的人受到影响的累积频率(F)。FN 曲线最初

用于核电站的风险评价中，其采用死亡人数 N 与事故发生频率 F 之间关系的图形来表示，目前广泛用于社会风险接受准则的制定。在大多数情况下，它们指的是出现一定数量伤亡出现的频率。

B.29.2 用途

FN 曲线可用于系统或过程设计，或是用于现有系统的管理。

FN 曲线是表示风险分析结果的一种手段。很多风险都具有轻微结果高概率或是严重后果低概率的特点，FN 曲线用区域块来表示风险，而不是用表示后果和概率组成的单点表示风险。FN 曲线可用来比较风险，例如将风险与 FN 曲线规定的标准相比，或是将风险与历史数据相比，或是与决策准则相比。

B.29.3 输入

所需输入数据是：

——特定时期内成套的可能性/后果对；

——定量风险分析的数据结果，估算出一定数量伤亡的可能性；

——历史记录及定量风险分析中得出的数据。

B.29.4 过程

将现有数据绘制在图形上，以伤亡人数(一定程度的伤害，例如死亡)作为横坐标，以事故发生频率作为纵坐标。由于数值范围大，两个轴通常都离不开对数比例尺。

FN 曲线可以使用过去损失的“真实”数字进行统计上建构，或者通过模拟模型进行计算。使用的数据及假定意味着这两类 FN 曲线可以传递出不同的信息，应单独用于不同目的。一般来说，理论 FN 曲线对于系统设计非常有用，而统计 FN 曲线对现有的特定系统的管理非常有用。

两种归纳法可能会很耗时，因此，将两种方法综合运用较为常见。接着，实证数据将形成已准确掌握的伤亡人数(在规定时间范围内已知事故/事项中发生的伤亡人数)，以及通过外插法或内插法提供其他观点的定量风险分析。对于低频率事故的分析工作，需要收集较长时间跨度范围内的数据。

B.29.5 输出

可与现有风险决策准则进行比较的一个风险区域。

B.29.6 优点及局限

FN 曲线是一种有效描述风险信息的手段，能以便于理解的形式来表示频率及后果信息。管理人员和系统设计师可通过 FN 曲线，更有效地做出风险及安全水平方面的决策。

FN 曲线适用于具有充分数据且背景类似的情况下的风险比较。

FN 曲线的局限性是，它们无法说明影响范围或事项结果，而只能说明受影响人数，并且无法识别引发伤害发生的方式。FN 曲线并不是风险评估方法，而是一种表示风险评估结果的方法。作为一种表示风险评估结果的明确方法，它们需要那些熟练的分析师进行准备，经常很难为专家以外的人士所理解和使用。

B.30 马尔可夫分析

B.30.1 概述

如果事物每次状态的转移只与互相接引的前一状态有关，而与过去的状态无关，则称这种无后效性的状态转移过程为马尔可夫过程。具备这种时间离散、状态可数的无后效随机过程称为马尔可夫链。

马尔可夫分析(Markov analysis)通常用来分析那些存在时序关系的各类状况的发生概率。该方法可用于生产现场危险状态、市场变化情况的预测,但是不适宜于系统的中长期预测。通过运用更高层次的马尔可夫链,这种方法可拓展到更复杂的系统中。类似于 Petri 网分析,马尔可夫分析也能监督并观察系统状态,但是两者存在差异,因为前者能同时处于多重状态下。

马尔可夫分析是一项定量技术,可以是不连续的(利用状态间变化的概率)或者连续的(利用各状态的变化率)。虽然马尔可夫分析可以手工计算进行,但是当前其更依存于计算机程序。

B.30.2 用途

马尔可夫分析技术可用于各种系统结构(无论是否需要维修),包括:

——串联系统中相互独立的部件;

——并联系统中相互独立的部件;

——负荷分载系统;

——备用系统,包括发生转换故障的情况;

——降级系统。

马尔可夫分析技术也可以用于计算设备可用度,包括考虑需要维修的备件。

B.30.3 输入

马尔可夫分析的关键输入数据如下所示:

——系统、子系统或组件可能处于的各种状况的清单,例如,全运行、部分运行(降级状况)以及故障状况等;

——状态的可能转移。例如,如果是汽车轮胎故障,那就要考虑备胎的状况,还要考虑检查频率;

——某种状况到另一种状况的变化率,通常由不连续事项之间的变化概率来表示,或者连续事项的故障率(λ)及/或维修率(μ)来表示。

B.30.4 过程

马尔可夫分析技术主要围绕"状态"这个概念(例如,现有状态及故障状态)以及基于常概率的状态间的转移。随机转移概率矩阵可用来描述状态间的转移,以便计算各种输出结果。

为了说明马尔可夫分析技术,不妨分析一种仅存在于三种状态的复杂系统。功能、降级和故障将分别界定为状态 S1、状态 S2 以及状态 S3。每天,系统都会存在于这三种状态中的某一种。表 B.4 说明了系统明天处于状态 Si 的概率(i 可以是 1、2 或 3)。

表 B.4 马尔可夫矩阵

		今天状态		
		S1	S2	S3
明天状态	S1	0.95	0.3	0.2
	S2	0.04	0.65	0.6
	S3	0.01	0.05	0.2

该概率阵称作马尔可夫矩阵,或是转移矩阵。注意,每栏数值之和是 1,因为它们是每种情况一切可能结果的总和。

这个系统可以用马尔可夫图来表示，见图 B.7。其中，圆圈代表状态，箭头代表相应概率的转移。

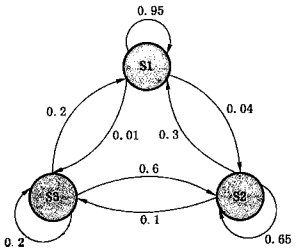

图 B.7　系统马尔可夫图

从某个状态返回自身的箭头通常并不绘出，但是为了完整性也显示在图 B.7 所示的例子中。

P_i 代表系统处于状态 i（i 可以是 1、2 或 3）的概率，那么需要解决的联立方程包括：

$$P_1 = 0.95P_1 + 0.30P_2 + 0.20P_3 \quad \cdots\cdots(\text{ⅰ})$$

$$P_2 = 0.04P_1 + 0.65P_2 + 0.60P_3 \quad \cdots\cdots(\text{ⅱ})$$

$$P_3 = 0.01P_1 + 0.05P_2 + 0.20P_3 \quad \cdots\cdots(\text{ⅲ})$$

这 3 个方程并非独立的，无法解出 3 个未知数。因此，下列方程必须使用，而上述方程中有一个方程可以弃用。

$$1 = P_1 + P_2 + P_3 \quad \cdots\cdots(\text{ⅳ})$$

状态 1、2 和 3 的答案分别是 0.85、0.13 和 0.02。该系统只在 85%的时间里能充分发挥功效，13%的时间内处于降级状态，而 2%的时间存在故障。

再来考虑平行运行的两个组件。其中，系统要发挥功能，其中一组件必须正常运行。这些组件可能是正常或故障的，系统的可用性依赖于组件的整体状态。

状态可以视为：

状态 1：两个项目能发挥正常功能；

状态 2：一个项目已出现故障并正在进行维修，而另一个项目运行正常；

状态 3：两个项目都已出现故障且都在进行维修。

如果假设各项的故障率为 λ，维修率为 μ，那么状态转移图如图 B.8 所示：

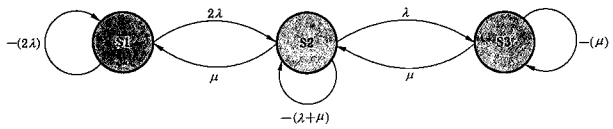

图 B.8　状态转移图

注意，从状态 1 到状态 2 的转移为 2λ，因为这两项中任一项的故障都会使系统进入状态 2。

设定 $P_i(t)$ 为 t 时系统处于初始状态 i 的概率；

设定 $P_i(t+\delta t)$ 为 $t+\delta t$ 时系统处于最终状态 i 的概率。

转移概率矩阵就变成表 B.5 的结果。

表 B.5 最终马尔可夫矩阵

		最初状态		
		$P_1(t)$	$P_2(t)$	$P_3(t)$
最终状态	$P_1(t+\delta t)$	-2λ	μ	0
	$P_2(t+\delta t)$	2λ	$-(\lambda+\mu)$	μ
	$P_3(t+\delta t)$	0	λ	$-\mu$

值得关注的是，如果无法从状态 1 转移到状态 3 或是由状态 3 转移到状态 1，那么就会出现零值。而且，在规定比率时，各栏总和为零。

联立方程变为：

$$dP_1/dt = -2\lambda P_1(t) + \mu P_2(t) \quad \cdots\cdots(\text{V})$$

$$dP_2/dt = 2\lambda P_1(t) + [-(\lambda+\mu)]P_2(t) + \mu P_3(t) \quad \cdots\cdots(\text{Vi})$$

$$dP_3/dt = \lambda P_2(t) + (-\mu)P_3(t) \quad \cdots\cdots(\text{Vii})$$

为了简单起见，我们假设所需的可用度为稳定状态可用度。

当 δt 趋向无限时，dP_i/dt 会趋于零，方程式的求解会变得更容易。

B.30.5 输出

马尔可夫分析的输出结果是处于各种状态下的各种概率，因此，可以估算出故障概率及/或可用度（系统的关键组件之一）。

B.30.6 优点及局限

马尔可夫分析的优点是能够计算出系统未来处于各状态的概率。

马尔可夫分析的局限包括：

——假设状态变化的概率是固定的；

——所有事项在统计上具有独立性，因此未来状态独立于一切过去的状态，除非两个状态紧密相接；

——需要了解状态变化的各种概率；

——有关矩阵运算的知识；

——计算结果很难与非技术人员进行沟通。

B.31 蒙特卡罗模拟分析(Monte Carlo simulation)

B.31.1 概述

蒙特卡罗模拟方法(Monte Carlo simulation)又称随机模拟法，广泛用于计算各种领域的风险，是预测和估算失事概率常用的方法之一。该方法的主要思路是：按照概率定义，某事件发生的概率可以用大量试验中该事件发生的频率估算。因此，可以先对影响其失事概率的随机变量进行大量随机抽样，获得各变量的随机数，然后将这些抽样值一组组地代入功能函数式，确定系统失效与否，统计失效次数，并计算出失效次数与总抽样次数的比值，此值即为所求的失事概率。蒙特卡罗法就是依靠上述思路求解系统失效概率的，该方法处理手段是计算机模拟与仿真。

B.31.2 用途

蒙特卡罗模拟通常用来评估各种可能结果的分布及值的频率，例如成本、周期、吞吐量、需求及类似的定量指标，其应用范围包括财务预测、投资效益、项目成本及进度预测、业务过程中断、人员需求等领域的风险评估。

蒙特卡罗模拟法可以用于两种不同用途：

——传统解析模型的不确定性的分布；

——解析技术不能解决问题时进行概率计算。

B.31.3 输入

进行蒙特卡罗模拟分析时，需要构建一个可以很好地描述系统特性的模型。模型中各变量的输入数据需要依据其分布随机产生。为此，均匀分布、三角分布、正态分布和对数正态分布经常被使用。

B.31.4 过程

过程如下：

——确定尽可能准确代表所研究系统特性的模型或算法；

——用随机数将模型运行多次，产生模型(系统模拟)输出。模型以方程式的形式提供输入参数与输出之间的关系；

——在每一种情况下，计算机以不同的输入运行模型多次并产生多种输出。这些输出可以用传统的统计方法进行处理，以提供均值、方差和置信区间等信息。

下面给出一个模拟例子。两组设备平行运行，而系统的正常运行只需要一个设备即可。第一个项目的可靠性为0.9，而另一个项目的可靠性为0.8。现求整个系统的可靠性。

可以构建如表B.6所示的电子表格。

表 B.6 模拟数据

模拟数	项目1		项目2		系统运行情况
	随机数	功能状态	随机数	功能状态	
1	0.577 243	是	0.059 355	是	1
2	0.746 909	是	0.311 324	是	1
3	0.541 728	是	0.919 765	否	1
4	0.423 274	是	0.643 514	是	1
5	0.917 776	否	0.539 349	是	1
6	0.994 043	否	0.972 506	否	0
7	0.082 574	是	0.950 241	否	1
8	0.661 418	是	0.919 868	否	1
9	0.213 376	是	0.367 555	是	1
10	0.565 657	是	0.119 215	是	1

随机数生成器生成了0到1之间的数字，用来与各项的概率进行比较，以便确定系统是否正常运行。仅凭10次运行，0.9这个结果不会成为准确的结果。常见的方法是在计算器内建模，当模拟程度达到了所需精度时，再比较总结果。在这个例子中，经过20000次迭代，我们就得出了0.9799这个结果。上述模型可以通过多种方式进行拓展。例如：

——通过拓展模型本身(例如,只有在首项出现故障的情况下,才考虑第二项);
——当概率无法准确确定时,通过改变某个变量的固定概率拓展(三角分布是个很好的例子);
——使用故障率外加一个随机函数生成器去推导出故障时间(指数分布、Weibull 分布或其他合适的分布)并建立维修时间;

B.31.5 输出

输出结果可能是单个数值,例如上例确定的单个数值;它也可能是表述为概率或频率分布的结果。一般来说,蒙特卡罗模拟可用来评估可能出现的结果的整体分布,或是以下分布的关键测评:
——期望结果出现的概率;
——在某个置信概率下的结果值。
对输入数据与输出结果之间关系的分析可以说明目前正发挥作用的因素的相对重要性,同时可识别那些旨在减少结果不确定性的工作的有用目标。

B.31.6 优点及局限

蒙特卡罗模拟的优点包括:
——从原则上讲,该方法适用于任何类型分布的输入变量;
——模型便于开发,并可根据需要进行拓展;
——实际产生的任何影响或关系都可以进行表示,包括微妙的影响,例如条件依赖;
——敏感性分析可以用于识别较强及较弱的影响;
——模型便于理解,因为输入数据与输出结果之间的关系是透明的;
——提供了一个结果准确性的衡量;
——软件便于获取且成本较低。
局限包括:
——结果准确性取决于可执行的模拟次数(随着计算机运行速度的加快,这一限制越来越小);
——依赖于能够代表参数不确定性的有效分布;
——大型复杂的模型可能对建模者具有挑战性,很难使利益相关方参与到该过程中;
——由于抽样效率的限制,该方法对于组织最为关注的严重后果/低概率的风险事件预测效力不足。

B.32 贝叶斯统计及贝叶斯网络

B.32.1 概述

贝叶斯统计学是由英国学者贝叶斯提出的一种系统的统计推断方法。其前提是任何已知信息(先验)可以与随后的测量数据(后验)相结合,在此基础上去推断事件的概率。贝叶斯理论的基本表达式见式(B.6):

$$P(A|B)=\{P(A)P(B|A)\}/\sum_i P(B|E_i)P(E_i) \quad \cdots\cdots(B.6)$$

式中:
事件 X 的概率表示为 $P(X)$;
在事件 Y 发生的情况下,X 的条件概率表示为 $P(X|Y)$
E_i代表第 i 个事项。
式(B.6)的最简化形式为式(B.7):

$$P(A/B)=\{P(A)P(B\mid A)\}/P(B) \quad \cdots\cdots(B.7)$$

与传统统计理论不同的是，贝叶斯统计并未假定所有的分布参数为固定的，而是设定这些参数是随机变量。如果将贝叶斯概率视为某个人对某个事项的信任程度，那么贝叶斯概率就更易于理解了。相比之下，古典概率取决于客观证据。由于贝叶斯方法是基于对概率的主观解释，因此它为决策思维和建立贝叶斯网络(信念网、信念网络及贝叶斯网络)提供了现成的依据。

贝叶斯网络是基于概率推理的数学模型，它是基于概率推理的图形化网络，使用图形模式来表示一系列变量及其概率关系。网络中节点表示随机变量的，节点间的结有向边代表了节点间的互相关系，这里母节点是一个直接影响另一个(子节点)的变量，用条件概率进行表达关系强度，没有父节点的用先验概率进行信息表达。贝叶斯网络对于解决复杂系统中不确定性和关联性引起的故障有较大优势，由此在多个领域中获得广泛应用。

B.32.2 用途

近年来，归功于目前越来越多现成的软件计算工具，贝叶斯理论及贝叶斯网络的运用非常普及。贝叶斯网已用于各种领域：医学诊断、图像仿真、基因学、语音识别、经济学、外层空间探索，以及今天使用的强大的网络搜索引擎。对于任何需要利用结构关系和数据来了解未知变量的领域，它们都被证明行之有效。贝叶斯网可以用来认识因果关系，以便了解问题域并预测干预措施的结果。

B.32.3 输入

其输入数据接近蒙特卡罗模拟的输入数据。每个贝叶斯网络应采取的步骤如下所示：

——界定系统变量；

——界定变量间的因果联系；

——确定条件及先验变量；

——增加证据；

——进行信念更新；

——获取后验信念。

B.32.4 过程

分析下列贝叶斯网络(图 B.9)：

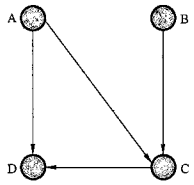

图 B.9 贝叶斯网络样图

借助于确定的先验概率，计算结 C、结 D 的条件概率，见表 B.7～表 B.9。其中 Y 表示正值，N 表示负值。

表 B.7 结 *A* 与结 *B* 的先验概率

$P(A=Y)$	$P(A=N)$	$P(B=Y)$	$P(B=N)$
0.9	0.1	0.6	0.4

表 B.8 在明确结 *A* 与结 *B* 的情况下，结 *C* 的条件概率

A	*B*	*P*(*C*=*Y*)	*P*(*C*=*N*)
Y	*Y*	0.5	0.5
Y	*N*	0.9	0.1
N	*Y*	0.2	0.8
N	*N*	0.7	0.3

表 B.9 在明确结 *A* 与结 *B* 的情况下，结 *D* 的条件概率

A	*C*	*P*(*D*=*Y*)	*P*(*D*=*N*)
Y	*Y*	0.6	0.4
Y	*N*	1.0	0.0
N	*Y*	0.2	0.8
N	*N*	0.6	0.4

为了确定 $P(A|D=N,C=Y)$的后验概率，首先要计算出 $P(A,B|D=N,C=Y)$。

使用贝叶斯规则，可以确定 $P(D|A,C)P(C|A,B)P(A)P(B)$，如表 B.10 所示。同时，最后一栏表示正态概率，其和为上列得出的 1(结果四舍五入)。

表 B.10 在明确结 *C* 与结 *D* 的情况下，结 *A* 与结 *B* 的后验概率

A	*B*	$P(D\|A,C)P(C\|A,B)P(A)P(B)$	$P(A,B\|D=N,C=Y)$
Y	*Y*	0.4×0.5×0.9×0.6=0.110	0.4
Y	*N*	0.4×0.9×0.9×0.4=0.130	0.48
N	*Y*	0.8×0.2×0.1×0.6=0.010	0.04
N	*N*	0.8×0.7×0.1×0.4=0.022	0.08

要得出 $P(A|D=N,C=Y)$，*B* 的所有值必须求和。

表 B.11 在明确结 *D* 与 *C* 的情况下，结 *A* 的后验概率

$P(A=Y\|D=N,C=Y)$	$P(A=N\|D=N,C=Y)$
0.88	0.12

表 B.11 表明，$P(A=N)$的先验概率已由 0.1 增加到后验的 0.12，此变化较小。同理，通过计算可以得知，$P(B=N/D=N,C=Y)$已由 0.4 增加到 0.56，这个变化更明显。

B.32.5 输出

贝叶斯方法与传统统计方法有着相同的应用范围，并会产生大量的输出结果，例如得出点估算结果的数据分析以及置信区间。贝叶斯方法最近颇为流行，而这与可以产生后验分布的贝叶斯网络密不可分。图形结果提供了一种便于理解的模式，可以轻松修正数据来分析参数的相关性及敏感性。

B.32.6 优点及局限

贝叶斯统计及贝叶斯网络的优点包括：

——仅需有关先验的知识；

——推导式证明易于理解；

——确应考虑贝叶斯规则；

——它提供了一种利用客观信念解决问题的机制。

局限包括：

——对于复杂系统，确定贝叶斯网中所有节点之间的相互作用是相当困难的；

——贝叶斯方法需要众多的条件概率知识，这通常需要专家判断提供。软件工具只能基于这些假定来提供答案。

参 考 文 献

[1] GB/T 7826—1987 系统可靠性分析技术 失效模式和效应分析(FMEA)程序

[2] IEC 61511 Functional safety—Safety instrumented systems for the process industry sector

[3] IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems

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

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

[6] ISO/IEC Guide 51 Safety aspects—Guidelines for their inclusion in standards

[7] IEC 61649 Weibull analysis

[8] IEC 61078 Analysis techniques for dependability—Reliability block diagram and Boolean methods

[9] IEC 61165 Application of Markov techniques

[10] ISO/IEC 15909(all parts) Software and systems engineering—High-level Petri nets

[11] IEC 62551 Analysis techniques for dependability—Petri net techniques 3

[12] IEC 61025 Fault tree analysis (FTA)

[13] IEC 60300-3-9 Dependability management—Part 3: Application guide—Section 9: Risk analysis of technological systems

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

[15] ISO/IEC Guide 98-3:2008, Uncertainty measurement—Part 3: Guide to the of uncertainty in measurement (GUM:1995)

GB/T 27921-2011

书号:155066·1-44225

定价: 57.00 元