系 统 安 全 工 程 学

陈喜山　编　著
撒占友　张永亮　梁晓春　岳丽宏　刘　芳　参　编

中国建材工业出版社

图书在版编目（CIP）数据

系统安全工程学 / 陈喜山主编．—北京：中国建材工业出版社，2006.1
ISBN 7-80227-000-6

Ⅰ.**系**… Ⅱ.**陈**… Ⅲ.**安全工程 - 高等学校 - 教材** Ⅳ.X93

中国版本图书馆 CIP **数据核字（**2005**）第** 153787 **号**

系统安全工程学
陈喜山等编著

出版发行：中国建材工业出版社
地　　址：北京市西城区车公庄大街 6 **号**
邮　　编：100044
经　　销：全国各地新华书店
印　　刷：北京鑫正大印刷有限公司
开　　本：787mm × 960mm　1/16
印　　张：11.75
字　　数：219 **千字**
版　　次：2006 **年** 1 **月第** 1 **版**
印　　次：2006 **年** 1 **月第** 1 **次**
定　　价：21.00 **元**

网上书店：www.ecool 100.com

前　言

随着我国现代化建设的不断深入，生产生活中各个方面的安全问题日益显现出来，爆炸事故、火灾事故、交通事故等各行业领域中的事故已经成为我国社会主义现代化建设事业中经常遇到的问题。为了适应我国现代化建设的高速发展，保证社会主义现代化建设持续健康地向前推进，安全科学技术和安全管理理论也随之迅速发展起来。安全工程科学正是在这个大背景下迅速发展的一门新兴学科。系统安全工程学则是安全工程学科重要的基础理论课程之一。

本书是在以往的安全工程专业的授课教案基础上，经整理、调整、充实、提高、编撰而成。全书力求简明翔实，通俗易懂，一方面，要突出土建、交通等方向；另一方面，立足于夯实基础具有较宽厚的安全科学知识面。

本书定名为《系统安全工程学》主要考虑到安全工作都是针对某一特定系统而言的，从逻辑关系上分析应首先有某一特定的系统过程，然后才涉及该系统的安全问题。

本书的系统可靠性分析部分由撒占友同志编写；安全决策部分由张永亮同志编写；梁晓春同志编写了概论部分，同时对书稿进行了整理等工作；其他部分均由陈喜山同志编写；岳丽宏、刘芳同志对本书做了校对等工作。

在本书的编写中，喜获东北大学陈宝智教授的指导和鼓励，在这里表示衷心的感谢！

由于水平有限，书中若出现问题，敬请广大读者和专家给予批评指正。

编者

2006 年 1 月

目　　录

1 概　　论

1.1 系统安全工程学的产生与发展

二次世界大战以后，全世界范围内的工业技术有了突飞猛进的发展，生产规模不断扩大，核能、航天、石油、化工、冶金等尖端工业和重工业发展迅速。与此同时，工业生产中发生事故的次数也越来越多，公害也越来越严重，造成了很大的社会问题，亟待解决。

20 世纪 50 年代末，前苏联发射了第一颗人造地球卫星后，美国为了迎头赶上，随后进行了多次导弹技术的研究与开发。但是，由于仓促上阵准备不足，在短短不到两年的时间里竟连续四次出现重大事故，每次都造成了数以百万计美元的损失，最后只得推倒重来。

20 世纪 60 年代，美国空军总结了前面失败的教训，应用系统工程学的理论和方法研究导弹系统的安全可靠性。1962 年第一次提出了“弹道导弹系统安全工程”的概念，根据其方法和原理制订了严格的“武器系统安全标准”。1966 年，美国国防部采用这一安全标准，制订了代号为 MIL-S-38130 标准，后来又多次修订，逐步完善并形成了“系统安全程序技术要求”，即 MIL-STD-882B 标准，成为了产业界系统安全工程的重要依据。随后系统安全工程的基本方法在化工和其他工业上开始应用，美国道化学公司针对化工厂的火灾爆炸事故的特点开发并不断完善了“火灾爆炸指数安全评价方法”即称道法。

20 世纪 70 年代，系统安全工程学的基本原理和方法逐步在除军事工业之外的其他工业领域得以广泛应用和进一步完善。围绕原子能工业的安全问题，美国原子能委员会发表的“商用核电站风险评价报告 (WASH-1400)”中成功应用了系统安全分析和评价技术；日本劳工省针对化工生产系统的全过程提出了“六步骤安全评价法”，不仅规定了评价方法和评价技术，同时也规定了生产系统不同阶段的安全评价方法；这期间，在冶金、航空、交通、电子等行业中相继开发出了许多系统安全分析方法和评价方法。系统安全工程学的基本原理和分析方法在各行各业开始全面应用。

20 世纪 80 年代以来，系统安全工程学在世界各国得到广泛重视，国际性学术组织得以发展壮大，出版了许多专著。研究工作逐渐从被动应用其他领域的成果转移到系统安全基本理论和方法研究方面。1983 年在美国 (休斯敦)

召开的第六届国际学术大会上就有 40 多个地区和国家的代表参加，议题涉及国民经济的各行各业。

我国系统安全工程的应用于 20 世纪 80 年代初开始起步，相继成立了相关的学术组织，以系统安全工程为中心，开展开发研究和推广应用等工作。目前，各行各业积极推广应用系统安全工程学的原理和方法，取得了可喜成果。全国有 70 所高校增设了安全工程本科专业、硕士点和博士点。这些都为普及和推广系统安全工程学知识、推进现代安全管理创造了有利条件，同时也为创新出适合我国各行业实际的系统安全工程学的理论和方法打下良好基础。

1.2 系统安全工程学的基本概念

系统安全工程学是 20 世纪中期随着世界经济的发展而发展起来的一门新兴学科，是以系统工程的方法研究和解决工业生产过程中安全问题，运用现代科学和技术手段辨识、控制和消除系统中的危险源，实现系统安全的新学科。在弄清什么是系统安全工程学之前应首先弄清有关的基本概念。

1.2.1 系统、系统工程

系统是由相互作用、相互依赖的若干部分组合而成的具有特定功能的有机整体。

系统无处不在，如由若干个零部件组成的可以完成特定作业的机器设备，由传动、行走等部分组成的车辆，由处室、车间、班组及作业单元组成的工厂，甚至于由星系组成的整个宇宙都是一个系统。

系统应具有如下的基本特征，否则便不称其为系统：

⑴ 具有整体性

系统是能够相互区别的各个部分组成的整体，各个部分都要服从于实现整体最优目标的需要。

⑵ 具有层次性

一个系统可分成许许多多小的部分，这些小的部分本身也是一个有机的整体，具有一定的功能，是原系统的子系统。而子系统又可分成更小的子系统，一直分到不能再分为止。例如一个工厂 （系统） 可以分成若干个车间 （子系统），车间又可以分成若干个班组 （子系统） 等。

由于系统的层次性，在系统安全分析时可以把系统分为若干子系统进行分析。

⑶ 具有目的性

对于整个系统来说，是以完成某种特定的功能，达到某种特定的目标为目的的。

⑷ 具有相关性

系统的相关性是系统内部各部分之间相互联系、相互作用、相互依赖的关系。

⑸ 具有适应性

系统的适应性是指系统通过自我调节适应环境变化的性质，这种适应是通过与环境间进行的能量、物质和信息的交换来实现的。

⑹ 具有动态性

整个系统和系统中的组成部分都是随着时间的改变而不断改变的，不是一成不变的。

系统工程就是运用系统分析的理论，对系统的规划、研究、设计、制造、试验和使用等各阶段进行有效的组织管理的科学技术方法。系统工程是属于组织管理方面的工程技术，是解决工程活动全过程的工程技术，是具有普遍适应性的工程技术。

1.2.2 安全、危险及系统安全

安全是指不发生导致人身伤害、设备或财产损失事故的状态。当某些导致发生上述事故状态的概率是可以接受时，也可视为安全。从工业生产角度上看，安全不仅是人和物不会受到伤害和损失的理想状态，也是满足安全技术指标要求的技术状态。安全工作中还涉及到安全性的概念。安全性是指不发生导致人身伤害、设备或财产损失的可能性，是判断和评价系统安全性能的重要指标。

危险是指导致人身伤害、设备或财产损失的状态。同样，安全工作中还涉及到危险性的概念。所谓的危险性就是表示危险状态发生的可能性。

危险源是指可能导致系统危险状态的不安全因素。任何系统中都不可避免地存在着某些类型的危险源。辨识这些危险源，采取控制或消除措施是系统安全的基本内容。根据危险源的不同性质又分为第一类危险源和第二类危险源。

第一类危险源是指系统中存在的、可能发生意外释放的能量或危险物质的危险源。如爆炸物、有毒有害物质、电力设备、运动车辆等。

第二类危险源是指导致系统中约束、限制能量或有害物质的屏蔽措施失效或破坏的各种不安全因素的危险源。它包括人、物、环境三方面的因素。如人的误操作、防护设施失效、环境温度过高等。

可靠性是指系统在特定的条件下，在规定的时间内完成规定功能的性能，是判断和评价系统性能的重要指标。系统由于可靠性差而不能完成规定功能的现象称为故障。

系统安全是指人们为解决复杂系统的安全性问题而开发、研究的安全理

论、原则和方法体系，是在所研究的系统寿命期间内辨识系统中的危险源并采取控制措施使其危险性最小，从而使该系统在规定的性能、时间和成本范围内达到最佳的安全程度。

1.2.3 系统安全的观念

⑴ 没有绝对的安全

安全是相对的,危险是绝对的。任何事物中都包含有不安全的因素,具有一定的危险性,安全只是一个相对的概念。从此种意义上讲,安全又可以理解为没有超出允许限度的危险。这一允许限度是人们用来判断安全与危险的分界线。

⑵ 安全工作贯穿于系统存在的始终

安全工作贯穿于系统寿命的全过程，是系统安全的基本原则和重要特征。它充分体现了“安全第一，预防为主”的安全工作总方针。在新系统的构思、论证、设计、建造、运行、维护以及直到废弃的各个阶段都要辨识、评价和预防控制系统中的危险源。

⑶ 危险源及危险性的认识

根据道格拉斯的系统安全的三命题，关于危险源及危险性的认识主要有以下三方面：

1) 在某一系统中不可能彻底地消除一切危险源和危险性；

2) 在某一系统中可以采取措施控制危险源，减少现有危险源的危险性；

3) 系统安全是降低系统整体的危险性，而不是只彻底地消除几种选定的危险源及危险性。

⑷ 不可靠是不安全的原因

一般来说，系统的不可靠会导致系统的不安全。当系统发生故障时，不仅影响系统功能的实现，而且还会导致发生事故，造成人员伤亡或财产损失。例如，汽车操纵系统失灵会导致汽车失控，造成伤亡事故。

可靠性着眼于保证实现系统的功能，研究故障发生前直到故障发生为止的系统状态；安全性着眼于防止事故的发生，侧重于研究故障发生后对系统的影响。可见二者的连接点是故障，在防止故障的发生方面二者是一致的，密切关联的。通常，在提高系统可靠性的同时，既可以保证实现系统的功能，又可以提高系统的安全性。

1.3 系统安全工程学及其主要内容

系统安全工程学是运用科学和工程技术手段辨识、消除或控制系统中的危险源，实现系统安全的科学。系统安全工程的基本任务就是辨识、评价和控制

系统的危险源，降低系统的危险性。因此系统安全工程学的主要内容包括了如何辨识危险源，如何评价系统的危险源和危险性，如何控制系统的危险源，降低系统的危险性等方面的任务。

1.3.1 危险源辨识

危险源辨识就是发现和识别系统中的危险源，是安全评价、危险源控制、降低系统危险性的基础。只有准确地找出危险源才能准确地对其进行安全评价，才能有效地采取措施控制危险源，降低系统的危险性。危险源的辨识一般有两种方法：

⑴ 经验对比分析法

它是基于与有关的标准、规范、规程或经验相对比来辨识危险源的方法。由于通常的标准、规范、规程或安全检查表等都是从大量的经验中总结出来的，所以经验对比分析法是一种基于经验的方法，只适用于有以往或类似的经验可供参考的情况。

⑵ 系统安全分析法

系统安全分析法是从安全的角度出发，运用系统工程等分析手段，揭示系统中可导致故障或事故的各种因素及相互关系，从而辨识系统危险源。它既可以用于有经验可寻的危险源辨识，也可以用于无经验可寻的危险源辨识。

1.3.2 安全评价

安全评价（危险性评价）是对系统中的危险源危险性进行的综合评价。它包括对系统危险源自身危险性评价和对危险源控制效果的评价。前者是采取危险源控制措施的基础；后者是采取危险源控制措施后的效果评价。

1.3.3 危险源控制

危险源控制就是利用工程技术和管理手段控制或消除危险源，防止事故发生、人员伤害和财产损失。

危险源控制技术主要包括防止事故发生的安全技术（预防技术）和事故发生后减少或避免损失的安全技术（应急技术）。

管理手段主要是发挥计划、组织、指挥、协调、控制等功能来控制系统中的人、物和环境因素，有效地控制危险源，减小或降低危险性。

实际安全工作中，危险辨识、安全评价和危险源控制并不是严格分阶段独立进行的，而是相互交叉、相互重叠的。一方面，在辨识危险源时，需要进行安全评价，看其对系统安全性的影响程度；另一方面，进行危险源控制时，要对控制措施的效果进行评价；同时，在采取危险控制措施时又可能带来新的危

险源和危险性，因此又需要进一步进行危险源辨识和安全评价。

思　考　题

1. 系统安全工程学的发展状况如何？
2. 何谓安全？何谓危险？二者关系如何？
3. 何谓系统、系统工程和系统安全工程？
4. 系统安全工程学的主要内容有哪些？
5. 系统安全的基本观念有哪些？
6. 何谓第一类危险源？何谓第二类危险源？

2 事故的基本概念及统计预测

2.1 事故的基本概念

要学习掌握系统安全工程学的基本原理和方法，首先应了解和掌握伤亡事故的概念和统计方法，它们是系统安全工程学的基础。

2.1.1 事故概念

事故是指人们在实现某种意图而进行的生产和生活活动中，突然发生的，违反人们意志的，迫使生产和生活活动暂时或永久停止的意外事件。

根据事故统计规则，伤亡事故是指损失工作日达到或超过 1 天的人身伤害或急性中毒的事故。

工伤事故是指在生产过程中发生的伤亡事故。未遂事故是指既没有造成人员伤害，也没有造成财物损失和环境破坏的事故，也称为险兆事故。

失能伤害是指除死亡之外使人体永久或在一定时间内失去某种能力的伤害。分为暂时性失能伤害（受伤害者或中毒者暂时不能从事原岗位工作的伤害）、永久性部分失能伤害（受伤害者或中毒者的肢体或某些器官功能不可逆丧失的伤害）、永久性全失能伤害（受伤害者或中毒者完全残废的伤害）。

2.1.2 事故分类

按事故的性质分为责任事故和非责任事故。责任事故是指本来可以预见、抵御和避免的事故，但由于人为的原因没有采取预防措施从而造成的事故；非责任事故是由于自然灾害造成的事故和由于科技水平所限而无法避免的事故。据统计，责任事故占所发生事故的 90%以上，因此对其应引起足够的认识。

按事故的伤害程度分为轻伤、重伤和死亡。轻伤是指损失工作日低于 105 日的失能伤害；重伤是指损失工作日大于等于 105 日的失能伤害；死亡是指造成死亡的事故。永久性全失能伤害和死亡损失的工作日均为 6000 个。

按事故的严重程度分为轻伤事故、重伤事故和死亡事故。轻伤事故是指只有轻伤，无重伤和死亡的事故；重伤事故是指只有重伤，无死亡的事故；死亡事故是指有死亡的事故。其中，一次事故中死亡 1～2 人的事故称为重大伤亡事故；一次事故中死亡 3 人及超过 3 人的事故称为特大伤亡事故。按事故致伤

原因分为如表 2-1 的 20 类：

表 2-1　事故的致伤原因分类

序　号	类　　别	序　号	类　　别	序　号	类　　别
1	物体打击	8	火　　灾	15	瓦斯爆炸
2	车辆伤害	9	高处坠落	16	锅炉爆炸
3	机械伤害	10	坍　　塌	17	压力容器爆炸
4	起重伤害	11	冒顶片帮	18	其他爆炸
5	触　　电	12	透　　水	19	中毒和窒息
6	淹　　溺	13	放　　炮	20	其　　他
7	灼　　烫	14	火药爆炸		

2.2　事故的统计分析

2.2.1　事故统计分析的作用及概念

⑴ 事故统计分析的作用

事故的统计分析就是运用数理统计的方法对事故的数据进行处理、分析，从而研究事故的发生发展规律，明确安全工作的方向。事故的统计分析在安全工作中具有以下的重要作用：

1）可以用以描述一个企业或部门的安全状况；

2）可以用以作为观察事故发生趋势的依据；

3）可以用以判断和确定事故发生的范围；

4）可以用以作为探查事故原因的依据；

5）可以用以作为制定安全措施的依据；

6）可以用以预测未来事故的依据。

早在 20 世纪 30 年代美国的工程师海因里希运用事故统计分析方法，在对大量的调查数据进行统计分析后发现了，在同一个人发生的 330 起同种事故中，300 起没造成伤害，29 起造成了轻微伤害，只有 1 起造成了严重伤害的重要结论，即著名的 1:29:300 的法则。这一法则的重要性不在于比例数如何精确，而是说明了事故发生的次数（频率）与伤害程度（严重度）之间的随机关系，即每发生一起严重伤害事故就要有大量的无伤害事故和轻微伤害事故的存在。因此全力以赴防止个人发生同种事故是防止严重伤害的关键。这一统计分析结果为我们提供了安全工作的方向和依据。

(2) 事故统计分析的概念

为了便于理解举一具体例子对事故的统计概念加以说明。表 2-2 中列出了某大型建筑企业两年内各月份的事故次数。

表 2-2　某大型建筑企业两年内各月份的事故次数

事故次数 / 月份 / 年份	1	2	3	4	5	6	7	8	9	10	11	12
第一年	6	11	5	2	3	5	6	7	3	2	1	4
第二年	7	4	8	3	2	1	0	4	9	3	4	5

表 2-3 中列出了事故统计的各项参数。

表 2-3　事故的统计参数

在一个月内发生的事故次数 (i)	事故频数 (n_i)	累计事故频数 $\left(N_i = \sum_{j=0}^{i} n_j\right)$	事故频率 $\left(f_i = \frac{n_i}{N_{\geqslant 10}}\right)$	累计事故频率 $\left(F_i = \sum_{j=0}^{i} f_j\right)$
0	1	1	0.04167	0.04167
1	2	3	0.08333	0.12500
2	3	6	0.12500	0.25000
3	4	10	0.16667	0.41667
4	4	14	0.16667	0.58334
5	3	17	0.12500	0.70833
6	2	19	0.08333	0.79167
7	2	21	0.08333	0.87500
8	1	22	0.04167	0.91666
9	1	23	0.04167	0.95833
$\geqslant 10$	1	24	0.04167	1.00000

事故频数 (n_i)，是指在规定的统计范围内某种事故出现的次数 (i)，在本例中是指全年发生 i 次事故的月数 (见表 2-3 中第 2 栏)。事故频数的分布见图 2-1。在某规定值以下某种事故频数之和称为累计事故频数 (N_i)，本例中是指事故频数的累计 (见表 2-3 中第 3 栏)。事故频数的累计分布见图 2-2。

事故频率 (f_i)，是指事故频数与被测的所有事故次数之比 (见表 2-3 中第 4 栏)。在某规定值以下某种事故频率之和称为累计事故频率 (F_i)，本例中是指事故频率的累计 (见表 2-3 中第 5 栏)。同样，事故频率和累计事故频率也可以绘制成类似图 2-1 和图 2-2 的分布图。

事故分布是指事故频数（或频率）在一定时间内的分布状况。由于事故的发生是一种随机现象，所以事故的分布应符合于某种概率分布规律，如泊松分布、正态分布等。

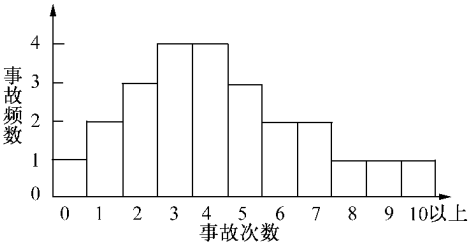


图 2-1　事故频数分布

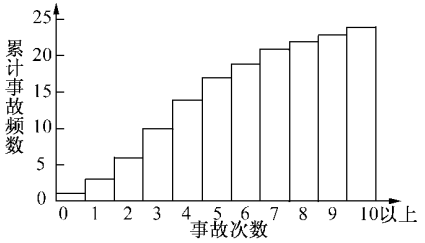


图 2-2　累计事故频数

2.2.2　事故统计分析的数学原理

事故统计分析的基础就是概率论及数理统计这一数学基础。下面结合事故统计的特点加以说明。

(1) 事故发生的随机性质

事故的发生是一种随机的现象。事故随机现象的表现是，在一定条件下可能发生也可能不发生，在个别试验观测中呈现出不确定性，但是在大量的重复试验观测中又具有规律性。

在概率和数理统计中，通过随机变量来描述随机现象。与人们通常接触的函数变量不同，随机变量不能适当地用一个数值来表述，必须用实际数字系统的分布来描述。由于实际分布系统不同，随机变量分为离散型和连续型。在研究事故统计规律时，需要恰当地确定随机变量的类型。例如，一定时期内建筑企业伤亡事故发生次数只能是非负的整数，相应的数字分布是离散型；两次事故之间的时间间隔则应该属于连续型。这是因为与时间相对应的数字分布系统是连续的。

为了描述随机变量分布情况，利用数学期望，即平均值，来描述数值的大小：

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (i = 1,2,3,\cdots,n) \tag{2-1}$$

利用方差来描述统计数据的随机波动性：

$$\sigma^2 = \frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n - 1} \tag{2-2}$$

上述公式中的 x_i 是观测值。

事故频率在一定程度上反映了事故随机现象出现的可能性。在事故统计

中，当观测次数少时，统计的结果将表现出强烈的随机波动性。随着观测次数的增加，事故频率将逐渐趋于一个稳定的常数。此常数称为发生事故的概率，它是事故随机发生可能性的度量。

事故的概率是随着某个自变量（如时间）的变化而变化的。换句话说，事故的概率是某个自变量（如时间）的函数，通常称这个函数为事故概率的密度函数。

(2) 事故的统计分布

在事故统计分析中，经常会遇到如下一些统计分布规律。

1) 均匀分布

对于连续型随机变量。当其事故概率的密度函数具有下述形式时，则称为均匀分布：

$$f(x) = A, \quad \text{当 } x_1 \leqslant x \leqslant x_2 \text{ 时} \tag{2-3}$$

$$f(x) = 0, \quad \text{当 } x < x_1 \text{ 或 } x > x_2 \text{ 时}$$

例如，统计事故损失工时为 0 ~ 100 小时的区段内的事故时，假设在此时间段内任意损失工时的事故发生概率均为 0.01 时，则事故发生的概率密度函数可写为：

$$f(x) = 0.01, \quad \text{当 } 0 \leqslant x \leqslant 100 \text{ 时}$$

$$f(x) = 0, \quad \text{当 } x > 100 \text{ 时}$$

见图 2-3 所示。

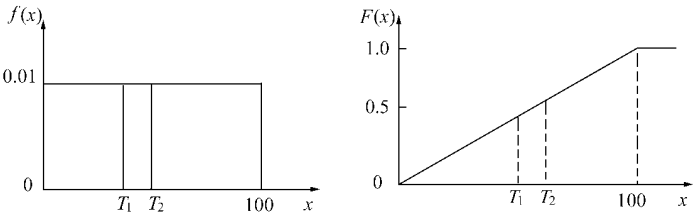


图 2-3 均匀分布

于是，损失工时在 $T_1 \leqslant x \leqslant T_2$ 的区间内的事故发生的概率为：

$$F(x) = \int_{T_1}^{T_2} f(x)\,dx = 0.01 \times (T_2 - T_1)$$

如果给定 T_1 和 T_2 的值，则可计算出相应的概率。

2) 指数分布

指数分布属于连续型随机变量的概率分布，主要用来描述事故发生时间间隔的分布情况。假设单位时间内事故发生的次数，即事故发生率为 λ，则自某

时刻起 t 时间内发生事故的概率为：

$$F(t) = 1 - e^{-\lambda t} \tag{2-4}$$

此式称为事故发生的时间分布，其事故的概率密度函数为：

$$f(t) = \lambda e^{-\lambda t} \tag{2-5}$$

指数分布的数学期望（即平均值）为：

$$\theta = \int_0 t \times f(t)\,dt = \frac{1}{\lambda} \tag{2-6}$$

此式的物理意义为平均事故间隔时间，在安全管理中也称为平均无事故时间，它是事故发生率的倒数。指数分布的方差为：

$$\sigma^2 = \int_0 t^2 \times f(t)\,dt = \frac{1}{\lambda^2} \tag{2-7}$$

3）二项式分布

二项式分布属于离散型随机变量的概率分布，可以用于描述一个企业或部门在一定时期内事故发生次数的概率分布。

设某建筑企业有 n 名职工，且每人每月发生事故的概率相同，均为 p，由二项式分布可知，该企业的每月发生 x 次事故的概率（即概率密度函数）为：

$$f(x) = \frac{n!}{n!(n-x)!}p^n (1-p)^{n-x} \tag{2-8}$$

每月发生事故次数不超过 X 的概率，即发生 X 次及 X 次以下事故的累计概率分布为：

$$F(X) = \sum_{x=0}^{X} f(x) = \sum_{x=0}^{X} \frac{n!}{n!(n-x)!}p^n (1-p)^{n-x} \tag{2-9}$$

二项式分布的数学期望（即平均值）为：$\lambda = n \times p$

二项式分布的方差为：$\sigma^2 = n \times p \times (1-p)$ (2-10)

4）泊松分布

当二项式分布中的 n 值足够大（$n \geqslant 10$），p 值相当小（$p \leqslant 0.1$）时，可以按泊松分布进行近似计算。由于土木建筑、交通运输等企业公司的职工人数较多，而经统计，伤亡事故发生的概率较小，所以按泊松分布计算有足够的精度，可以满足要求。

由泊松分布，一个企业或部门在一定时间内伤亡事故发生 x 次的概率（即概率密度函数）应为：

$$f(x) = e^{-\lambda} \times \frac{\lambda^x}{x!} \tag{2-11}$$

式中，λ 为泊松分布的数学期望，即该时期内伤亡事故的平均次数；当然 λ^2 即为泊松分布的方差。

在一定时间内伤亡事故发生次数不超过 X 次的概率应为：

$$F(X) = \sum_{x=0}^{X} f(x) = \sum_{x=0}^{X} e^{-\lambda} \times \frac{\lambda^x}{x!} \qquad (2\text{-}12)$$

图 2-4 给出了数学期望 λ 得不同值时的泊松分布状况：

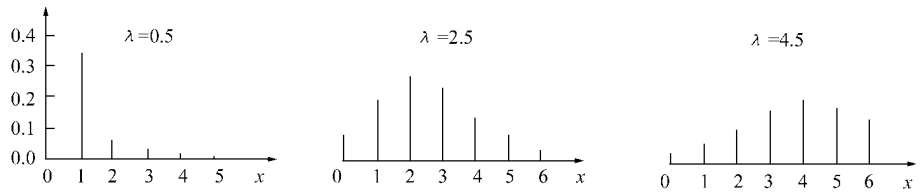


图 2-4　不同 λ 值的泊松分布

【例 2-1】　某大企业集团前两年内共发生伤亡事故 105 次，若安全状况不变，来年每月不发生伤亡事故的概率为多少？每月内伤亡事故次数不超过 3 次的概率为多少？

【解】 每月平均伤亡事故的次数 λ （数学期望）应为：

$$\lambda = \frac{105}{24} = 4.375 \quad (\text{次/月})$$

⑴ 每月不发生伤亡事故的概率为：

$$f(0) = e^{-\lambda} \times \frac{\lambda^0}{0!} = e^{-\lambda} = e^{-4.375} \approx 0.0126$$

⑵ 每月内发生伤亡事故次数不超过 3 次的概率为：

$$F(3) = \sum_{x=0}^{3} f(x) = \sum_{x=0}^{3} e^{-\lambda} \times \frac{\lambda^x}{x!} = e^{-\lambda}\left(1 + \lambda + \frac{\lambda^2}{2!} + \frac{\lambda^3}{3!}\right) \approx 0.3638$$

5）正态分布

生产过程中的事故统计，很多结果服从于正态分布形式。当观测次数非常大时，二项式分布也趋于正态分布。

正态分布是在平均值 $\bar{x}$ （数学期望）附近对称的分布，其概率密度函数为：

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(x-\bar{x})^2}{2\sigma^2}\right] \qquad (2\text{-}13)$$

图 2-5 给出了不同的 σ 值时的正态分布形式。图 2-6 表明了随机变量服从正态分布时，观测值的 68.27%可能落入（$\bar{x} \pm \sigma$）的范围内；94.45%的观测值可能落入（$\bar{x} \pm 2\sigma$）的范围内；99.73%的观测值可能落入（$\bar{x} \pm 3\sigma$）的范围内。

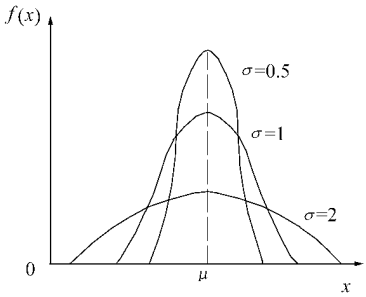


图 2-5　不同 σ 值的正态分布

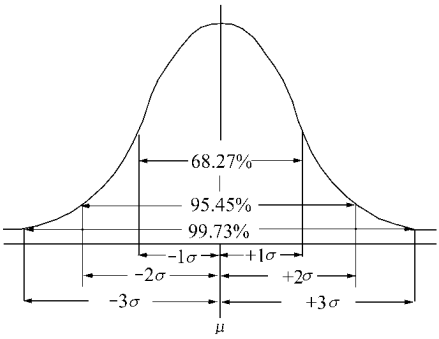


图 2-6　正态分布曲线

(3) 置信度与置信区间

通过试验观测研究随机现象时，通常把研究对象的全体称为总体，把总体中的一部分称为样本，把总体中的一个基本单位叫做个体，把样本中含有的个体数量叫做样本容量。我们希望掌握整体规律，但是有时是十分困难的，甚至不可能做到，因而只能观测一定容量的样本来研究总体分布问题。当通过观测一定容量的样本推断总体情况时，所获的数据也只是总体的近似值。由于近似值并不一定是真值，所以还要估计出一个以区域形式给出的范围，并希望知道该范围包含真值的可靠程度。这便涉及到了置信区间和置信度的概念。

随机地从总体中抽取一个大样本。若关心的是总体的数学期望值（即总平均值），则可以根据样本观测值计算出样本的数学期望值 $\bar{x}$（即样本平均值）。根据总体分布的概率密度函数 $f(x)$ 可以求出 $\bar{x}$ 落入任意两个值 t_1 和 t_2 之间的概率。对于某一特定的概率 $(1-\alpha)$，若有

$$p(t_1 \leqslant \bar{x} \leqslant t_2) = (1-\alpha)$$

则称 t_1 和 t_2 之间（包括 t_1 和 t_2 在内）的所有值的集合为参数 $\bar{x}$ 的置信区间，t_1 和 t_2 分别为置信区间的置信上限和置信下限。特定的概率 $(1-\alpha)$ 称为置信度，α 称为显著性水平。

当正态分布观测值的 95.45% 可能落入 $(\bar{x} \pm 2\sigma)$ 的范围内时，这就相当于置信度为 95.45% 的置信区间为 $(\bar{x}-2\sigma) \sim (\bar{x}+2\sigma)$ 的范围。换句话说，就是当从总体中反复多次抽样时，在每组样本观测值确定的一个区间 $(\bar{x} \pm 2\sigma)$ 中，包含有 $\bar{x}$ 值的概率为 94.45%，不包含 $\bar{x}$ 值的概率为 5.55%。

置信度与置信区间在伤亡事故统计分析中具有重要意义。除了用于推断总体参数之外，还用于估计统计分析的可靠程度。

【例 2-2】　如表 2-4 所示，某大型企业连续三年的事故工亡人数分别为 20 人、15 人和 10 人。单从数据上看，三年中事故工亡人数下降了一半，似乎安

全状况有了很大的改观。但是，从 95%置信度的置信区间去考虑，可以认为该企业的安全状况并没有明显的变化，事故工亡人数的减少也只是偶然现象。

表 2-4　事故工亡人数统计的置信区间

第一年		第二年		第三年	
事故工亡人数 20	95%的置信区间 (13 ~ 29)	事故工亡人数 15	95%的置信区间 (9 ~ 23)	事故工亡人数 10	95%的置信区间 (5 ~ 17)
第二年与第一年相差 5 人			第三年与第二年相差 5 人		

2.2.3　伤亡事故的统计指标

经对伤亡事故进行统计和分析，可以了解和评价企业或生产部门的安全生产状况。为了便于分析过程的通用性，在 1948 年国际劳工会议上，统一了伤亡事故的统计指标，即伤亡事故频率和事故严重率等指标。

(1) 按伤亡事故频率统计

伤亡事故的频率是按下式定义的：

$$a = \frac{A}{N \cdot T} \tag{2-14}$$

式中　a——伤亡事故频率；

A——伤亡事故发生次数；

N——参加生产的职工人数；

T——统计时间间隔。

世界各国的统计指标不尽相同。我国通常是以千人死亡率、千人重伤率和伤害频率等指标来表示 (见 GB 6441—86 中规定)。

1) 千人死亡率

是指某时段内平均每千名职工中工伤事故死亡的人数。

$$\text{千人死亡率} = \frac{\text{死亡人数}}{\text{平均职工数}} \times 10^3 \tag{2-15}$$

2) 千人重伤率

是指某时段内平均每千名职工中工伤事故重伤的人数。

$$\text{千人重伤率} = \frac{\text{重伤人数}}{\text{平均职工数}} \times 10^3 \tag{2-16}$$

3) 伤害频率

是指某时段内平均每百万工时因工伤事故伤害的人数。

$$伤害频率 = \frac{伤害人数}{实际总工时数} \times 10^6 \quad (2\text{-}17)$$

4）千人负伤率

是指某时段内工伤事故的人次数，即我国的工伤事故频率统计指标。

$$千人负伤率 = \frac{工伤事故人次}{在册职工人数} \times 10^3 \quad (2\text{-}18)$$

（2）按事故严重率统计

事故严重率，顾名思义是指事故造成严重程度的统计指标，我国常用的有伤害严重率、伤害平均严重率等。

1）伤害严重率

是指某时段内每百万工时因事故损失的工作日数。

$$伤害严重率 = \frac{总损失工作日数}{实际总工时数} \times 10^6 \quad (2\text{-}19)$$

2）伤害平均严重率

是指受伤害的每人次平均损失工作日数。

$$伤害平均严重率 = \frac{总损失工作日数}{伤害人数} \quad (2\text{-}20)$$

（3）按产品产量统计

1）百万吨钢（或煤）死亡率

$$百万吨钢（或煤）死亡率 = \frac{死亡人数}{实际产量（t）} \times 10^6 \quad (2\text{-}21)$$

2）万立方米木材死亡率

$$万立方米木材死亡率 = \frac{死亡人数}{实际产量（m^3）} \times 10^4 \quad (2\text{-}22)$$

2.2.4 伤亡事故的统计图表

在伤亡事故统计分析中，经常使用各种统计图表来增加直观性和方便性。常用的有柱状图、折线图等。

（1）柱状图

柱状图是以柱状图形表示统计指标数值大小的统计图形。由于绘制容易、表达清晰，所以应用得十分广泛。作为伤亡事故统计图表之一的主次图就是一种柱状图。它把统计指标（通常是事故频率、伤亡人数、伤亡事故频率等）数值绘制成柱状，按从大到小、从左到右依次排列，把各种因素的重要程度直观地表现出来，并以折线表示累计值。图 2-7 绘出了某建筑企业伤亡事故统计分析（表 2-5）中的主次分布状况和累计事故频率。

表 2-5　某建筑企业伤亡事故统计分析

事故类别	频数（n_i）	累计频数（N_i）	频率（f_i，%）	累计频率（F_i，%）
物体打击	26	26	46.4	46.4
机械伤害	18	44	32.1	78.5
起重伤害	6	50	10.7	89.2
高空坠落	3	53	5.4	94.6
车辆伤害	2	55	3.6	98.2
其他伤害	1	56	1.8	100.0

从图中可以看出物体打击和机械伤害事故占事故总数的 78.5%，防止这两项事故的发生应作为企业安全工作的重点。

⑵ 折线图

折线图是将不同时段的统计指标用不间断的折线连接起来绘制成的图表，它可以清晰地表示或分析出事故发生趋势随时间的变化规律。常用的折线图有事故趋势图和事故管理图。

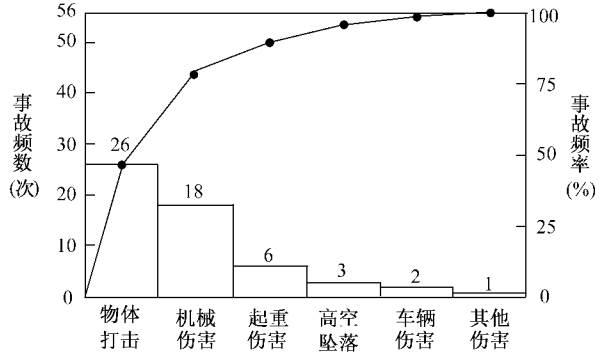


图 2-7　伤亡事故类别主次图

事故趋势图是按时间顺序对事故发生情况进行统计分析后绘制的图表。它既可以展示伤亡事故发生趋势，又可以评价某一时期内企业的安全状况。通常可以用千人负伤率、事故严重度等指标绘制而成。图 2-8 给出了某建筑企业 1990 年至 1999 年间伤亡事故千人负伤率随时间变化的事故趋势图。

由图可以看出，1995 年以前千人伤亡率下降幅度较大，之后呈平稳下降趋势。

⑶ 事故管理图

事故管理图是某企业或部门在实施安全目标管理中，为及时掌握事故发生状况经常使用的统计图表。

在实施安全目标管理时，把作为年度安全目标的伤亡事故指标逐月分解，确定月份的管理目标。通常一个企业或部门的职工人数在短时间内是稳定的，故往往以每月伤亡事故次数作为安全管理的目标值。

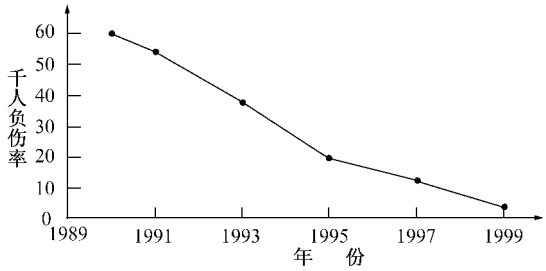


图 2-8　事故发生趋势图

在一定时期内，一个企业和部门每月伤亡事故发生次数的概率基本上服从于泊松分布。通常我们用数学期望来描述每月伤亡事故的平均发生次数（平均事故发生率，即平均单位时间内事故发生次数），用方差来描述每月伤亡事故的随机波动状况。由于泊松分布的数学期望和方差是相等的，均用 λ 来表示。可按下述公式（取置信度为 90% 时）确定围绕安全目标 λ 管理的控制上、下限（即置信度为 90% 的置信区间）：

控制上限为　　$UCL = \lambda + 2\sqrt{\lambda}$　　(2-23)

控制中线为　　$CL = \lambda$　　(2-24)

控制下限为　　$LCL = \lambda - 2\sqrt{\lambda}$　　(2-25)

在实际安全管理工作中，人们最关心的是实际伤亡事故发生次数的平均值是否超过安全目标值。所以，工作中往往不必考虑控制下限，只考虑控制上限即可，力争每个月内的伤亡事故发生次数不超过控制上限。

绘制伤亡事故管理图时，以月份为横坐标、每月的事故次数为纵坐标，用实线绘出管理目标线（即控制中线 CL）、用虚线绘出管理上限（控制上限）和管理下限（控制下限），同时注明数值和符号。在图中将每个月的实际伤亡事故次数的点绘于相应位置上，并用直线连接起来，形成折线图，表明安全状况随时间的总体走势。图 2-9 绘出了四个不同情况的伤亡事故管理图的走势。

正常情况下，各月份的实际伤亡事故发生次数应该控制在管理上限之内，并围绕安全目标值随机波动。如果管理图上出现图 2-9 (a) (b) (c) (d) 四种情况时，就应该认为安全状况发生变化，难以达到预定安全目标，必须查明原因及时整改。

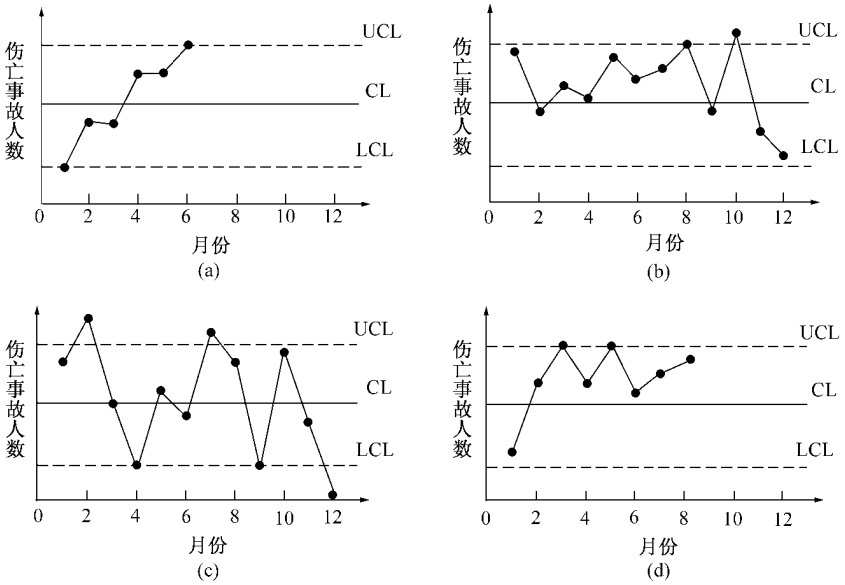


图 2-9　伤亡事故管理图

(a) 个别数据超出了管理上限，说明有新的或突出的不安全因素起了作用；

(b) 连续出现数个点在管理目标之上，说明不仅存在不安全因素，而且在连续起作用；

(c) 多个点连续周期性上升，说明有周期性因素在起作用；

(d) 大多数数据点在管理目标之上，说明安全状况很差，必须整改

(4) 其他分析图

除上述柱状图和折线图之外，通常还用到平面图和玫瑰图等。如图 2-10 所示的平面图，形象地表明了事故原因的分布情况。可见物体打击事故的发生比例最高。如图 2-11 所示的玫瑰图清楚地表示了周期性发生的事故分布状况。图中可见，在 21 时左右事故发生比例最高。

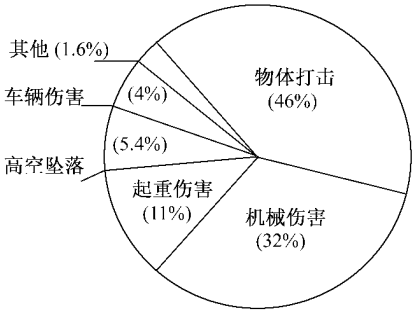


图 2-10　事故分析平面图

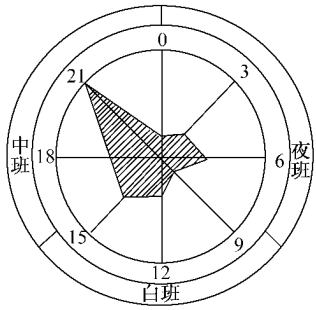


图 2-11　事故分析玫瑰图

2.2.5 伤亡事故统计分析中应注意的问题

⑴ 坚持实事求是的原则

实事求是是一切工作的基本原则和出发点，伤亡事故的统计分析更是如此。发生事故后，必须按国家规定（GB 6441-86、GB 6442-86），根据事故的事实材料，对其性质、类别、原因等做出科学的判断。只有如此才能反映客观实际。

⑵ 保证足够的样本容量

事故的发生是一种随机现象。根据概率统计规律，只有样本容量足够大时，随机现象出现的频率才趋于稳定。样本容量越小，即观测的数据量越少，随机波动越强烈，统计结果的可靠性越差。通常认为，当观测样本低于 20 万工时，统计所得的伤亡事故频率将有明显的波动，往往难以做出正确地判断；当观测样本达到 100 万工时以上时，可以得到较稳定的结果。

⑶ 合理地扩大样本容量

在应用统计分析的方法研究伤亡事故发生规律或利用伤亡事故统计指标评价企业的安全状况时，为获得可靠的统计结果，应该设法增加样本容量。主要可从两方面采取措施。

1）延长观测期间

对于职工人数较少的单位，可以通过适当增加观测期间来扩大样本容量。例如，采用千人负伤率作为统计指标时，如果以月为单位统计，得到的统计结果波动性很大；如果以年为单位统计，则得到的统计结果比较稳定。

2）扩大统计范围

事故的发生具有随机性，事故发生后是否伤害和伤害的严重程度也具有随机性，根据海因里希 1:29:300 法则，越是严重的伤害出现的概率将越小。统计范围越小，也仅能统计一定伤害严重程度的事故，统计结果随机波动性将越大。

一般的伤亡事故统计时，主要统计损失工作日 1 天及 1 天以上的事故。为了扩大样本容量，可以把损失工作日不到 1 天的轻伤事故也统计进去。

2.3 伤亡事故的预测

预测是人们对客观事物发展变化的一种认识和估计。人们通过对已经发生的事故分析、研究，弄清了事故发生的机理，掌握了事故发生和发展规律，就可以对事故在未来发生的可能性及发生趋势做出判断和估计。根据事故统计资料，对事故发生可能性和发生趋势的宏观预测，可以为企业、部门采取具体措

施防止事故再次发生提供依据，为安全目标管理、制定安全工作规划和安全决策提供依据。

常用的统计预测方法有回归预测法、灰色系统预测法、马尔柯夫链预测法、平滑指数法、特尔非法等二三十种之多。这里只介绍回归预测法、灰色系统预测法和马尔柯夫链预测法。

2.3.1 事故的回归预测

(1) 直线趋势的回归

回归预测法是通过以往事故资料回归分析来进行事故预测的方法。回归分析是一种数学方法，即是研究一个随机变量与另一个变量之间相关关系的数学方法。当两变量之间虽然存在着密切关系，但不能用一个变量精确地求出另一个变量时，这种变量间的关系称为相关关系。

两观测变量 (x_i, y_i) 的相关程度用相关系数 r 来表示：

$$r = \frac{L_{xy}}{\sqrt{L_{xx} \cdot L_{yy}}} \tag{2-26}$$

式中

$$L_{xy} = \sum x_i y_i - \frac{1}{n}\sum x_i y_i \text{；}$$

$$L_{xx} = \sum x_i^2 - \frac{1}{n}\left(\sum x_i\right)^2 \text{；}$$

$$L_{yy} = \sum y_i^2 - \frac{1}{n}\left(\sum y_i\right)^2 \text{。}$$

当 $|r| = 1$ 时，表明两变量间完全线性相关；当 $r = 0$ 时，表明两变量完全不相关。通常情况，$0 < |r| < 1$ 之间，$|r|$ 越大，相关性越好。

当 x 和 y 线性相关时，可以用一直线方程加以描述：

$$y' = a + bx \tag{2-27}$$

根据两变量的观测值求得上述直线方程的过程，数学上称为回归。回归的主要步骤是确定参数 a 和 b。

根据最小二乘法的数学原理，使之与观测散点离差平方和为最小的直线是最具有代表性的直线，即：

$$Q = \sum (y_i - y_i')^2 = \sum [y_i - (a + bx_i)]^2$$

对 a 和 b 分别求偏导数，并令其为零，即 $\partial Q/\partial a = 0$；$\partial Q/\partial b = 0$，可分别求得：

$$a = \bar{y} - b\bar{x} \text{；} \quad b = L_{xy}/L_{xx}$$

式中 $\bar{x} = \frac{1}{n}\sum x_i$，$\bar{y} = \frac{1}{n}\sum y_i$；$n$ 为样本数。

根据回归分析得到的直线方程，按外推方式可以求得对应于任意 x 的 y

值。但是，由于变量 x 与 y 之间并不是确定的函数关系而是相关关系，所以实际的 y 值不一定恰好在回归直线上，应处于直线两侧的某一区域内。

可以通过证明得到，当置信度为 $(1-\alpha)$ 时，预测区间为：

$$[y' - \delta(x),\ y' + \delta(x)]$$

其中：
$$\delta(x) = t_{\alpha}(n-2) \cdot S \cdot \sqrt{1 + \frac{1}{n} + \frac{(x-\bar{x})^2}{L_{xx}}} \qquad (2\text{-}28)$$

式中 $t_{\alpha}(n-2)$ ——t 分布值；

S——剩余标准差，$S = \sqrt{\frac{\sum (y_i - y')^2}{n-2}}$。

(2) 曲线趋势的处理

企业伤亡事故发生发展状况随时间的推移而不断变化，这一变化不一定都是直线关系的变化。一般情况下，随着生产技术的不断进步，劳动条件的不断改善和管理水平的不断提高，企业的安全状况也将不断提高。从而使伤亡事故的发生率 (y') 逐渐降低。通常事故发生率随时间 (x) 的推移呈指数下降规律，即：

$$y' = ae^{bx} \qquad (2\text{-}29)$$

将上式两端取对数，并令 $y'_0 = \ln y'$，$a_0 = \ln a$，则得到直线方程：

$$y'_0 = a_0 + bx \qquad (2\text{-}30)$$

在回归预测时，可根据企业历年的伤亡事故数据按上述方法进行预测，得到对应于 x 的 y'_0 的预测值，以及置信度为 $(1-\alpha)$ 时的预测区间 $[y'_0 - \delta(x),\ y'_0 + \delta(x)]$。然后，去掉对数还原到式 (2-29)，求出真正的预测值和预测区间：

$$y' = e^{y'_0}；\ (e^{y'_0 - \delta(x)},\ e^{y'_0 + \delta(x)})。$$

(3) 回归预测实例

【例 2-3】 某大型企业 9 年中的千人负伤率变化情况如表 2-6 所示，试预测第 10 年的千人负伤率。

表 2-6 某企业千人负伤率的情况统计

原始数据		处理后数据				
年份	千人负伤率 $y_i/100$	x_i	$y_0 = \ln y_i$	x_i^2	$x_i \cdot y_0$	y_0^2
第 1 年	56.2	0	4.03	0	0.00	16.24
第 2 年	55.7	1	4.02	1	4.02	16.16
第 3 年	49.5	2	3.90	4	7.80	15.21

续表

原始数据		处理后数据				
年份	千人负伤率 $y_i/100$	x_i	$y_0=\ln y_i$	x_i^2	$x_i \cdot y_0$	y_0^2
第4年	34.6	3	3.54	9	10.62	12.53
第5年	14.4	4	2.67	16	10.68	7.13
第6年	9.5	5	2.25	25	11.25	5.06
第7年	9.0	6	2.20	36	13.20	4.84
第8年	6.5	7	1.87	49	13.09	3.50
第9年	4.1	8	1.41	64	11.28	1.99
Σ		36	25.89	204	81.94	82.66

【解】 如图2-12所示，首先，将原始数据标在直角坐标系内。根据数据分布情况，可以判定该企业的千人负伤率呈指数规律下降分布；然后，将原始数据处理后列于表2-6的右半部分。

根据表内数据计算出所须参数：

$n=9$，$\bar{x}_i=4$，$\bar{y}_0=2.88$，$L_{x_iy_0}=-21.62$，$L_{x_ix_i}=60$，$L_{y_0y_0}=8.18$

计算相关系数和a、b值：

$$r=\frac{L_{x_iy_0}}{\sqrt{L_{x_ix_i}\cdot L_{y_0y_0}}}=\frac{-21.62}{\sqrt{60\times 8.18}}=-0.98$$

可见具有很强的相关性。

$$b=\frac{L_{x_iy_0}}{L_{x_ix_i}}=\frac{-21.62}{60}=-0.36；\ a=\bar{y}_0-b\bar{x}_i=2.88+0.36\times 4=4.32$$

所求直线方程为：

$$y_0=4.32-0.36x$$

如果，外推至第10年（即$x=9$）时，$y_0=1.08$，其预测第10年的千人负伤率应为：

$$y'=e^{y_0}=e^{1.08}=2.9$$

如果，取置信度为：

$$(1-\alpha)=95\%；则\ t_{0.05}(7)=2.262；$$

算得$\delta(x)=0.66$。此时的预测区间应为：

$$(e^{1.08-0.66}，e^{1.08+0.66})=(1.5，5.7)$$

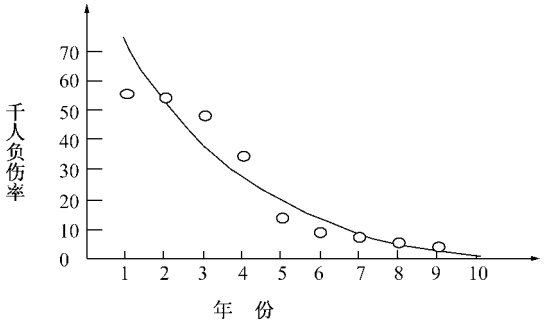


图 2-12 千人负伤率回归预测结果

2.3.2 事故的灰色系统预测

灰色系统理论是近 20 年来发展起来的数学理论，利用灰色系统理论可将没有规律或规律性不强的事物的原始数据变得具有明显的规律性。通常，事物系统的因素有些是清楚的（称为“白色”），有些是不太清楚的（称为“黑色”）。事物系统因素都是清楚的称为“白色系统”；事物系统因素都是不清楚的称为“黑色系统”；而介于清楚和不清楚之间的系统称为“灰色系统”。

（1）灰色系统的数据生成

根据灰色系统理论，处理系统中的“灰色”量是采用数据生成的方法来寻求其中的规律性，而不是采用通常的数理统计的方法。灰色系统数据生成方法主要有累加生成法、累减生成法和映射生成法三种。

所谓的累加生成法是将原始数据列中的各数据项依次累加得到新的数据列，即生成数据列；累减生成法是将原始数据列中的各数据项依次递减得到新的数据列，是累加生成法的逆方法；映射生成法是指除累加生成法和累减生成法之外的数据生成方法。

设有原始数据列如下：

$$x^{(0)} = \{x^{(0)}(k) \mid k = 1,2,3,\cdots,n\} = \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), \cdots, x^{(0)}(n)\} \tag{2-31}$$

令：$x^{(1)}(1) = x^{(0)}(1), x^{(1)}(2) = x^{(0)}(1) + x^{(0)}(2), \cdots, x^{(1)}(n) = x^{(0)}(n-1) + x^{(0)}(n)$。

形成新数据列：

$$x^{(0)} = \{x^{(1)}(1), x^{(1)}(2), x^{(1)}(3), \cdots, x^{(1)}(n)\} \tag{2-32}$$

新数据列的每一项与原始数据列的相应项之间有如下关系：

$$x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i) \tag{2-33}$$

经过累加生成处理后，获得了新的数据列。新数据列的随机波动性将明显减弱，而内在的规律性得以显现。

(2) 灰色系统的数学模型

对于生成后的数据列 $x^{(1)}$ 可以建立起类似于“白色系统”的微分方程，即一阶一个参数的灰色微分方程，记为 GM (1，1)：

$$\frac{dx^{(1)}}{dt} + ax^{(1)} = u \tag{2-34}$$

式中 a 和 u——待定常数。

方程 (2-34) 是一个一阶线性常微分方程，该方程的解为：

$$x^{(1)}(k+1) = \left[x^{(1)}(1) - \frac{u}{a}\right]e^{-ak} + \frac{u}{a} \tag{2-35}$$

该式也称为时间反应方程，其参数列为：

$$a = \begin{bmatrix} a \\ u \end{bmatrix} \quad \text{或} \quad a = (a, u)^T \tag{2-36}$$

可应用最小二乘法求出：

$$a = (B^T B)^{-1} B^T \cdot X_n \tag{2-37}$$

式中

$$B = \begin{bmatrix} -\frac{1}{2}[x^{(1)}(1) + x^{(1)}(2)] & 1 \\ -\frac{1}{2}[x^{(1)}(2) + x^{(1)}(3)] & 1 \\ \vdots & \vdots \\ -\frac{1}{2}[x^{(1)}(n-1) + x^{(1)}(n)] & 1 \end{bmatrix}$$

$$X_n = [x^{(0)}(2), x^{(0)}(3), x^{(0)}(4), \cdots, x^{(0)}(n)]^T$$

将求出的参数 a 和 u 代入时间响应方程中，可以算出生成数据列中的第 k 项和第 k + 1 项的估计值 $\hat{x}^{(1)}(k)$ 和 $\hat{x}^{(1)}(k+1)$。在此基础上，再做累减生成，按下式计算原始数据列中第 k + 1 项的估计值：

$$x^{(0)}(k+1) = x^{(1)}(k+1) - x^{(1)}(k) \tag{2-38}$$

(3) 后验差检验

为了知道灰色系统理论预测结果的可信性，需要对其进行检验。这一检验过程称为后验差检验。原始数据列的实际数据的平均值和方差分析分别为：

$$\bar{x} = \frac{1}{n}\sum_{k=1}^{n} x^{(0)}(k) \quad \text{和} \quad S_1^2 = \frac{1}{n}\sum_{k=1}^{n}[x^{(0)}(k) - \bar{x}]^2 \tag{2-39}$$

把第 k 项数据的原始数据值 $x^{(0)}(k)$ 与计算的估计值 $x^{(0)}(k)$ 之差称为第 k 项的残差：

$$q(k) = x^{(0)}(k) - x^{(0)}(k) \tag{2-40}$$

整个数列所有数据的残差的平均值和方差分别为：

$$\bar{q} = \frac{1}{n}\sum_{k=1}^{n} q(k) \quad \text{和} \quad S_2^2 = \frac{1}{n}\sum_{k=1}^{n}[q(k) - \bar{q}]^2 \tag{2-41}$$

最后，要通过计算后验差比值和小误差频率来进行后验差检验，综合检验灰色系统模型的精度。

1）后验差比值

后验差比值定义为，整个数列所有数据项残差的方差和原始数据列方差的比值：

$$C = \frac{S_2}{S_1} \tag{2-42}$$

实际检验中，后验差比值 C 越小越好，这说明即使原始数据很分散，但是灰色系统模型的估计值且与实际值很接近。

2）小误差频率

小误差频率定义为，整个数据列的残差与残差平均值之差小于给定值 $0.6745S_1$ 的频率，即：

$$P = P\{|q(k) - \bar{q}| < 0.6745S_1\} \tag{2-43}$$

小误差频率值越大说明系统预测模型越接近实际。将后验差比值和小误差频率精度等级制成表 2-7，可以综合评价灰色系统模型的预测精度。

表 2-7　后验差检验的精度等级

精度等级	小误差频率 (P)	后验差比值 (C)
好	> 0.95	< 0.35
合　格	> 0.80	< 0.50
勉　强	> 0.70	< 0.65
不合格	≤0.70	≥0.65

(4) 残差模型

如果根据原始数据列建立的灰色系统模型经过后验差检验不合格时，可以建立残差模型对原模型进行修正，其方法如下：

1）生成残差数据列

首先，应用下式对累加生成数据列的数据项计算残差：

$$q^{(1)}(k) = x^{(1)}(k) - x^{(1)}(k) \tag{2-44}$$

然后，将计算出的各项残差生成残差数据列：

$$q^{(1)} = \{q^{(1)}(1), q^{(1)}(2), q^{(1)}(3), \cdots, q^{(1)}(n_1)\} \tag{2-45}$$

通常，只用部分残差建立残差（即 $n_1 < n$）即可，不需要全部残差。

2）建立残差模型

生成残差数据列后，建立残差模型，即如下形式的一阶微分方程：

$$\frac{dq^{(1)}}{dt} + a_1 q^{(1)} = u_1 \tag{2-46}$$

该方程的解（残差时间反应方程）为：

$$q^{(1)}(k+1) = \left[q^{(1)}(1) - \frac{u_1}{a_1} \right] e^{-a_1 k} + \frac{u_1}{a_1} \tag{2-47}$$

按前述灰色系统求解参数 a 和 u 的方法求出参数 a_1 和 u_1 后，按下式计算原残差数据列第 $k+1$ 项的估计值：

$$q^{(1)}(k+1) = \left[q^{(1)}(1) - \frac{u_1}{a_1} \right] (e^{-a_1(k+1)} - e^{-a_1 k}) \tag{2-48}$$

$$q^{(1)}(1) = q^{(1)}(1) \tag{2-49}$$

3）生成数据列修正

把残差估计值加到前述生成数据列的对应项上，便得到修正后的灰色系统模型。通常，只考虑保证预测精度，仅对生成数据列的最后几个数据进行修正。假如只对生成数据列的第 m 项以后的数据项修正，则修正后的第 $k+1$ 项的估计值应为：

$k > m$ 时，

$$x^{(1)}(k+1) = \left[x^{(1)}(1) - \frac{u}{a} \right] + \frac{u}{a} + \left[q^{(1)}(m) - \frac{u_1}{a_1} \right] (e^{-a_1(k-m+1)} - e^{-a_1(k-m)}) \tag{2-50}$$

$k = m$ 时，

$$x^{(1)}(k+1) = \left[x^{(1)}(1) - \frac{u}{a} \right] + \frac{u}{a} + q^{(1)}(m) \tag{2-51}$$

（5）灰色系统预测举例

【例 2-4】　以【例 2-3】中某大型企业 9 年中千人负伤率变化情况作为原始数据列，应用灰色系统进行预测，见表 2-8。

表 2-8　某企业千人负伤率的情况统计

年　份	原始数据		处理后数据			
	（一）	（二）	（三）	（四）	（五）	（六）
	$x^{(0)}(k)$	k	$x^{(1)}(k)$	$x^{(1)}(k)$	$x^{(0)}(k)$	$q(k)$
第 1 年	56.165	1	56.165	56.165	56.165	0.000
第 2 年	55.650	2	111.815	116.594	60.429	-4.779
第 3 年	49.525	3	161.345	158.215	41.621	7.904
第 4 年	34.585	4	195.925	186.883	28.668	5.917
第 5 年	14.405	5	210.330	206.628	19.745	-5.340
第 6 年	9.525	6	219.855	220.228	13.600	-4.075

续表

年　份	原始数据		处理后数据			
	(一)	(二)	(三)	(四)	(五)	(六)
	$x^{(0)}(k)$	k	$x^{(0)}(k)$	$x^{(1)}(k)$	$x^{(0)}(k)$	q (k)
第 7 年	8.970	7	228.825	229.595	9.367	- 0.497
第 8 年	6.475	8	235.300	236.047	6.452	0.023
第 9 年	4.110	9	238.410	240.491	4.444	- 0.334
第 10 年				243.551	3.060	

【解】

1）将千人负伤率作为原始数据列 $x^{(0)}(k)$ 依次累加成新数据 $x^{(1)}(k)$ 列于表 2-8 的（三）栏之中，得到生成数据列。

2）分别计算出 B 和 X_n 矩阵：

$$B=\begin{bmatrix} -83.990 & 1 \\ -136.578 & 1 \\ \vdots & \vdots \\ -237.355 & 1 \end{bmatrix};\qquad X_n=\begin{bmatrix} 55.650 \\ 49.525 \\ \vdots \\ 4.110 \end{bmatrix}$$

3）求 a 和 u 值。应用方程组 $a=(B^TB)^{-1}B^T\cdot X_n$ 求得：

$$a=[a\quad u]^T=[0.37285\quad 93.33360]^T$$

从而得到 $a=0.37285$ 和 $u=93.33360$。

4）令表 2-8 中 $x^{(0)}(1)$ 作为 $x^{(1)}(1)$，并同求得的 a、u 值代入时间反应方程（2-35）中，建立起的灰色系统模型为：

$$x^{(1)}(k+1)=250.33-194.2e^{-0.37k}$$

将按此式分别计算的数值列于表 2-8 中的（四）栏之中；将应用累减式（2-38）计算得到的还原预测数据 $x^{(0)}(k)$ 列于表 2-8 中的（五）栏之中。

5）将应用（2-44）式计算的原始数据值与估计数据值之间的残差 q (k) 列于表 2-8 中的（六）栏之中。

6）进行后验差检验

计算得到的原始数据平均值和残差平均值分别如下：

$$\bar{x}^{(0)}=\frac{1}{9}\sum_{k=1}^{9}x^{(0)}(k)=26.60;\quad \bar{q}=\frac{1}{9}\sum_{k=1}^{9}q(k)=0.44$$

计算后验差比值：

$$C=\frac{S_2}{S_1}=\sqrt{\frac{\frac{1}{9}\sum_{k=1}^{9}[q(k)-\bar{q}]^2}{\frac{1}{9}\sum_{k=1}^{9}[x^{(0)}(k)-\bar{x}]^2}}=0.20<0.35$$

计算小误差频率：

$$P = P\{|q(k) - \bar{q}| < 0.6745S_1\} = 1 > 0.95$$

对照表 2-7 可以看出，预测精度等级为“好”，不需要进行残差修正。灰色系统模型的预测结果较好地反映了实际情况。

2.3.3 马尔柯夫链预测

如果某事物的发展过程和发展状况只与其当时的状态有关，而与以前的状态无关，则该事物发展变化的一连串过程称为马尔柯夫链。如果系统中的安全状况的发展变化具有马尔柯夫链的特点，从一种状态转变为另一种状态是有规律的，并且又是可知的，那么就可以利用马尔柯夫链对其进行分析和计算，预测以后某特定时刻的安全状态。

依据马尔柯夫链的特点，可用一组随时间而变化的变量来表征一个系统在变化过程中的特性状态。若系统在任何时刻的状态是随机的，则变化过程将是一个随机的过程。当从某时刻 t 变化到下一时刻 t + 1 时，状态变量将从某个值变到另一个值，这样系统便实现了一次状态转移，而这种状态转移的可能性可用转移概率来描述。

设系统初始状态的向量为：

$$S^{(0)} = \{S_1^{(0)}, S_2^{(0)}, \cdots, S_n^{(0)}\} \tag{2-52}$$

状态转移概率的矩阵为：

$$P = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ P_{n1} & P_{n2} & \cdots & P_{nn} \end{bmatrix} \tag{2-53}$$

该转移矩阵是一个 n 阶方阵，并满足下列两个性质，即：

$$0 \leqslant P_{ij} \leqslant 1; \quad \sum_{j=1}^{n} P_{ij} = 1$$

由初始状态向量和状态转移概率矩阵可以求出一次转移矩阵：

$$S^{(1)} = S^{(0)} P$$

同理，可以继续求得二次转移矩阵：

$$S^{(2)} = S^{(1)} P = S^{(0)} P^{(2)}$$

类似地，可以得到 (k + 1) 次转移矩阵，即：

$$S^{(k+1)} = S^{(0)} P^{(k+1)} \tag{2-54}$$

应用上述公式，便可以对某系统的安全状况进行预测。其举例如下：

【例 2-5】 某企业对 1250 名接触矽尘人员进行健康检查，统计出其中各种情况人员的分布状况填入表 2-9 之中。

表 2-9　接尘职工的健康状况

健康状况	健　　康	疑似矽肺	矽　　肺
向量序列	$S_1^{(0)}$	$S_2^{(0)}$	$S_3^{(0)}$
人　　数	1000	200	50

根据统计资料，一年后接尘人员的健康变化规律为：健康者剩 70%；20%变为疑似矽肺；10%变为矽肺，即：

$$P_{11}=0.7；P_{12}=0.2；P_{13}=0.1$$

原来为疑似矽肺的人员一般不可能恢复健康，仍保持原状的为 80%，有 20%被正式确定为矽肺，有：

$$P_{21}=0.0；P_{22}=0.8；P_{23}=0.2$$

矽肺病的人员一般也不可能恢复到疑似矽肺状态，有：

$$P_{31}=0.0；P_{32}=0.0；P_{33}=1.0$$

得到状态概率转移矩阵：

$$P=\begin{bmatrix}0.7 & 0.2 & 0.1\\ 0.0 & 0.8 & 0.2\\ 0.0 & 0.0 & 1.0\end{bmatrix}$$

一年后接尘人员的健康状况，即一次转移向量应为：

$$S^{(1)}=S^{(0)}\cdot P=(S_1^{(0)}，S_2^{(0)}，S_3^{(0)})\cdot\begin{bmatrix}P_{11} & P_{12} & P_{13}\\ P_{21} & P_{22} & P_{23}\\ P_{31} & P_{32} & P_{33}\end{bmatrix}$$

$$=(1000\quad 200\quad 50)\cdot\begin{bmatrix}0.7 & 0.2 & 0.1\\ 0.0 & 0.8 & 0.2\\ 0.0 & 0.0 & 1.0\end{bmatrix}=(700\quad 360\quad 190)$$

一年后接尘人员的健康状况为：健康者为 700 人；疑似矽肺者为 360 人；矽肺病者为 190 人。

思　考　题

1. 何谓事故频数？何谓事故频率？二者有何区别？
2. 何谓置信度和置信区间？意义何在？
3. 何谓事故管理图？有何意义？
4. 某企业五年间发生伤亡事故的次数分别为 16 次，12 次，10 次，13 次和 9 次。如果单位时间内的伤亡事故次数服从泊松分布，求一个月中发生两次

伤亡事故的概率。根据五年间的事故情况确定安全管理目标，求出安全管理上限，画出事故管理图。

5. 某企业 1994 年至 2002 年间，事故伤亡人数分别为 61，77，73，47，46，59，50，31，33 人，试分别用回归预测法和灰色系统预测法预测该企业 2004 年的事故伤亡人数。
6. 某企业接尘人员 125 人，其中健康者 100 人，疑似矽肺者 20 人，矽肺病患者 5 人；一年后健康人员为 75%，疑似矽肺人员为 20%，矽肺患者 5%。原为疑似矽肺的人员中已有 20% 的转变为矽肺病患者；原为矽肺病患者不可能好转，仍为矽肺病患者。求一年后接尘人员的健康状况。

3　事故理论与事故预防

事故是人们在实现其目的的行动中，突然发生的、迫使有目的的行动暂时或永久终止的一种意外事件。事故理论是研究事故为什么发生，如何发生以及如何防制的理论，是指导预防事故工作的基本理论。在与各种工业伤害事故做斗争中，人们不断积累经验，探索伤亡事故发生规律，提出了许多事故理论，为研究事故发生、发展和事故预防提出了不同的途径。

3.1　海因里希 1:29:300 事故法则

20 世纪 30 年代，美国安全工程师海因里希（W.H.Heinrich）在事故发生频率和伤害严重度的研究中，根据大量的事故统计结果发现，在同一个人发生的 330 起同类事故中，有 300 起没有造成伤害，有 29 起造成轻微伤害，1 起导致严重伤害。即，严重伤害、轻微伤害和无伤害的事故件数之比为 1:29:300，见图 3-1 所示。

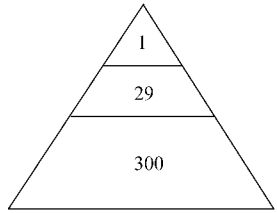


图 3-1　1:29:300 法则

该比例说明，同一种事故其结果可能极不相同，事故能否造成伤害及伤害的严重程度如何具有随机性。

比例 1:29:300 是根据同一个人发生的同类事故的统计资料得到的结果，并以此来定性地表示事故发生频率与伤害严重度间的一般关系。

实际上，不同的人、不同种类的事故导致严重伤害、轻微伤害以及无伤害的比例是不同的。特别是不同工业部门，不同生产作业条件，不同的时期，发生事故造成严重伤害的可能性是不同的。表 3-1 给出了某冶金企业 20 世纪从 50 年代到 80 年代之间不同作业性质的伤亡事故死亡、重伤和轻伤人数的比例关系。

海因里希的 1:29:300 法则的意义不在于比例数本身，而在于揭示了一起死亡事故的出现必然具有发生死亡事故的基础，即大量的未遂事故这一基本规律。这说明在安全管理工作中，要控制和预防死亡事故的发生必须减少大量的未遂事故，即死亡事故的基础。这一点对于死亡事故的预防具有重要的指导意义。

表 3-1　某冶金企业伤亡事故情况

作业性质	死　亡	重　伤	轻　伤
钢铁焦化	1	2.25	138
工业建筑	1	3.48	197
机械制造	1	4.44	408
原材料	1	6.89	430
运　输	1	1.76	73
采　矿	1	1.89	91

3.2　事故因果连锁理论

事故因果连锁理论是一种实际工作中得到广泛应用的事故致因理论。对实际的安全工作具有重要的指导意义。

3.2.1　海因里希事故因果连锁理论

在 20 世纪 30 年代，海因里希还提出了事故因果连锁理论的概念。该理论认为工业伤亡事故的发生是由许多互为因果关系的原因连锁作用的结果。具体即为人员伤亡（图 3-2）5 的发生是由于发生了事故 4；事故的发生是因为人的不安全行为或物的不安全状态（机械或物质的不安全状态）3；人的不安全行为或物的不安全状态是由于人的缺点错误造成的 2；人的缺点起源于不良的环境或先天的遗传因素 1。

所谓人的不安全行为或物的不安全状态，是指那些曾经引起过事故，或可能引起事故的人的行为和物的状态。

人们用多米诺骨牌形象地描述了这一事故因果连锁关系，如图3-2所示。

如果骨牌系列中的第 1 块骨牌（代表不良环境和先天遗传）被碰倒了，则由于连锁作用，其余的骨牌第 2 块（人的缺点错误）、第 3 块（人的不安全行为或物的不安全状态）、第 4 块（发生事故）、第 5 块（伤亡事故）将相继被碰倒，即导致伤亡事故发生。

根据该理论，生产过程中出现的人的不安全行为或物的不安全状态是

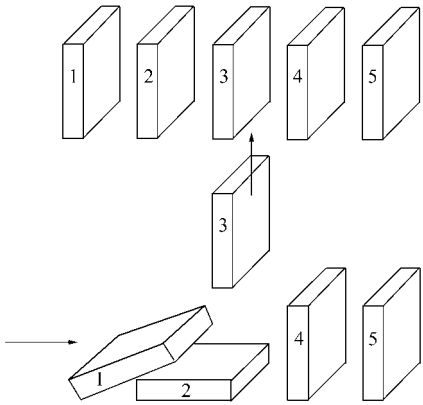


图 3-2　事故因果连锁关系

事故的直接原因。企业安全工作的中心就是防止人的不安全行为，消除物的不安全状态，中断事故连锁过程，避免伤亡事故发生。这相当于移去骨牌系列的中间一块关键的骨牌，使连锁作用被中断，事故过程被中止。

海因里希的事故因果连锁理论虽然对于安全工作具有重要意义，但是它把人的不安全行为和物的不安全状态的产生归咎于人的缺点和错误，过分强调先天遗传因素的作用，反映了海因里希时代的局限性。随着科学技术的不断进步，工业生产的日新月异，在海因里希的理论基础上，提出了能反映现代安全生产观念的事故因果连锁理论。

3.2.2 现代事故因果连锁理论

现代事故因果连锁理论认为，发生在生产现场的人的不安全行为或物的不安全状态作为事故的直接原因是必应加以追究的。但是，它们只是一种表面现象，是间接征兆，是根本原因管理失误的反映。鉴于这一观点，将图 3-2 事故因果连锁关系中的第 1 块骨牌的内容 （不良环境和遗传因素） 换为管理失误，第 2 块骨牌的内容 （人的缺点错误） 换成工作条件和个人原因后，便形成了现代事故因果连锁理论的骨牌排序关系。

在现代事故因果连锁理论中，不安全行为或不安全状态的发生是由于个人原因以及工作条件方面原因造成的。在安全工作中只有找出这些间接原因，采取措施克服它们才能防止不安全行为或不安全状态的出现，才能有效地防止事故的发生。

管理失误是现代事故因果连锁理论中最重要的原因。通常安全管理应是企业管理的一部分。在计划、组织、指导、协调和控制等管理机能中，控制是安全管理的核心。它从对间接原因的控制入手，通过对人的不安全行为和物的不安全状态的控制，达到防止伤亡事故发生的目的。所谓管理失误，主要是指在控制机能方面的欠缺，使得能够导致事故的个人原因和工作条件方面的原因得以存在。按现代事故因果连锁理论，加强企业安全管理是防止伤亡事故的重要途径。

过去，人们认为大多数工业伤害事故的发生都是由于人的不安全行为造成的，把事故的发生归咎于工人的“不注意”。现在，人们逐渐认识到，大多数伤害事故的发生除了存在有人的不安全行为之外，一定还存在有某种物的不安全状态。也就是说，工业伤害事故的发生是由于人的不安全行为和物的不安全状态共同作用的结果。而许多情况下，人的不安全行为和物的不安全状态又互为因果。有时物的不安全状态诱发了人的不安全行为；有时人的不安全行为导致了物的不安全状态的出现。

3.2.3 依据事故因果连锁理论预防事故发生

根据事故因果连锁理论，人的不安全行为和物的不安全状态是事故发生的直

接原因。因此，首先应从消除或控制人的不安全行为和物的不安全状态入手防止事故发生。一般情况下，引起人的不安全行为的原因可以归结为以下四个方面：

1）工作态度不端正。由于对安全生产缺乏正确认识，故意做出不安全的行为；或由于某种心理和精神方面的原因，忽视安全。

2）缺乏安全生产知识。如缺少安全经验；作业不熟练等。

3）生理或健康状况不良。如视力、听力低下；疾病、反应迟钝；醉酒或其他生理机能障碍等。

4）不良的工作环境。如作业场所照明、温度或通风不良；强烈的噪声、振动等；作业空间狭小、物料堆放杂乱；设备、工具缺陷；以及无安全防护装置等。

针对上述问题，可以应用技术的（Engineering）、教育的（Education）和法制的（Enforcement），即 3E 对策加以预防。

技术方面（Engineering）就是利用工程技术手段实现生产工艺、机械设备等生产条件的安全。通过改进生产工艺，采用先进的机械设备、装置，设置有效的安全防护装置等，消除或控制生产中的不安全因素，即使出现了人的不安全行为也不至于酿成事故。为职工创造整洁、安全、卫生的工作环境。这样的生产过程、机械设备、作业环境等生产条件的安全称为本质安全。在实际事故预防工作中，首先应该考虑消除物的不安全状态，实现生产过程、机械设备、作业环境等生产条件的本质安全。

教育方面（Education）就是通过各种形式的安全教育使干部和职工树立“安全第一”的思想理念，掌握安全生产所必需的知识和技能。通过安全教育提高职工的安全意识，增强安全生产的自觉性，变“要我安全”为“我要安全”。通过安全教育和培训增加职工的安全知识，提高生产操作技能。并且，经常注意职工的思想变化，了解职工的生理、心理状况，采取措施减轻他们的精神负担。

法制方面（Enforcement）就是借助于规章制度、法律、法规约束人的行为，实现对不安全行为的有效控制。值得注意的是，人的行为受到各自思想的支配，有较大的行为自由性。一方面，人的行为自由性使人具有搞好安全生产的能动性和一定的应变能力。另一方面，它也能使人的行为偏离规定的目标，产生不安全的行为。由于影响人的行为的因素特别复杂，所以控制人的不安全行为是一件十分困难的工作。

在采取上述 3E 措施过程中，由于受企业实际经济、技术条件等方面的限制，完全地消除生产过程中的不安全因素几乎是不可能的。我们只能是努力减少、控制不安全因素，防止出现不安全状态或一旦出现了不安全状态及时采取措施消除，使得事故不容易发生。因此，在任何情况下，通过科学的安全管理，加强对职工的安全教育及训练，建立健全并严格执行必要的规章制度，规范职工的行为都是非常必要的。

3.3 能量意外释放理论

能量意外释放理论认为，伤亡事故的发生是由于失去控制的，意外释放的过量能量引起的。其导致人员伤害的主要能量形式有机械能（势能和动能）、电能、热能、化学能、电离及非电离辐射、声能和生物能等。建筑工程、交通工程等多数工业领域造成事故的罪魁主要是机械能（势能和动能），其次是电能或化学能。

3.3.1 能量在伤害事故发生中的作用

能量在生产过程中是不可缺少的，人们为了创造物质等方面的需求，在生产过程中必然要利用能量。在正常的生产过程中，能量将受到种种约束和限制，按照人们的意图流动、转换和做功。如果由于某种原因能量失去了控制，超出了人们设置的约束或限制意外逸出或释放，则可以说发生了事故。

如果能量失去控制，意外释放触及人体，并同时超出了人体承受能力，则人员将受到伤害。换句话说，所有伤害的发生都是因为人体接触了超过人体组织抵抗力的某种形式的过量能量，或人体与外界的正常能量交换受到了影响（如窒息、淹溺等）。故此，可以说，各种形式的能量构成了伤害的直接原因。

机械能意外释放造成的伤害事故是建筑工程、交通运输等工程领域中伤害事故的主要形式。建筑工程等领域中的立体作业方式使作业人员、建筑设备及建筑物料具有较高的势能。当作业人员具有的势能意外释放时，将发生高空坠落或跌落事故；当建筑设备和物料具有的势能意外释放时，将发生倒塌、落物打击等事故。

除了势能之外，动能是另一种形式的机械能。在交通运输等工程领域中，使用的各种载人或载物的运输车辆，以及各种机械设备的运动部分均具有较大的动能。作业人员一旦与之接触，则将发生车辆伤害事故或机械伤害事故。

可见，预防由机械能意外释放所导致的伤害事故在建筑工程、交通运输等工程领域具有十分重要的意义。

电力工程为各行各业提供了生产所需的电能，而建筑工程、交通运输等工程领域中要广泛地利用电能。当作业人员意外地接触或接近带电体时，可能发生触电事故而受到伤害。

在交通工程、岩土工程等工程领域中的土石方爆破是一种由炸药的化学能转化为动能和热能的过程，在这一过程中如果控制得不好，能量意外释放的话，将引起爆破伤害事故的发生。

人体对每一种形式能量的作用都具有一定的抵抗能力，或者说具有一定的伤害阈值。当人体与某种形式的能量接触时是否产生伤害以及伤害的严重程度

如何，主要取决于作用人体能量的大小。通常作用于人体的能量越多，造成严重伤害的可能性越大。例如，一个球形弹丸以 4.9N 的冲击力打击人体时，只能轻微地擦破皮肤；以 68.6N 的冲击力打击人头部的重物，会造成头骨骨折。此外，人体接触能量的时间和频率，能量的集中程度，以及接触能量的部位等也对作业人员伤害的严重程度有很大影响。

能量意外释放理论提醒人们要经常注意生产过程中能量的流动、转换以及不同形式能量的相互作用，防止发生能量的意外逸出和释放。

3.3.2 依据能量意外释放理论预防事故发生

经大量的伤亡事故原因分析发现，大多数伤亡事故几乎都是因为过量的能量意外释放引起的，并且无一例外地是，这种过量能量的意外释放都是由于人的不安全行为或物的不安全状态造成的。即人的不安全行为或物的不安全状态使得能量失去了控制，是能量释放的导火索。

从能量以外释放理论出发，预防事故就是要防止能量的意外释放，防止人体与过量的能量相接触。我们把约束和限制能量所采取的措施称为屏蔽，与具体的屏蔽设施不同，此处是广义的屏蔽概念。换句话说，依据能量意外释放理论预防事故发生就是如何设置屏蔽措施。在建筑、交通运输、岩土等工程领域中常用的防止能量意外释放的屏蔽措施有如下几种：

⑴ 安全能源代替危险能源

有的情况下，某种能源的危险性较高，可以用较安全的能源取代。例如，在公路工程或岩土工程爆破凿岩中应用压缩空气动力代替电力，防止触电事故；在运输车辆采用电力驱动代替汽、柴油燃烧驱动，防止燃烧爆炸和环境污染等。应注意的是绝对安全的事物是没有的，只能是结合实际生产过程选用相对安全的能源代替相对危险的能源。

⑵ 限制过量能量

在生产工艺中尽量采用低能量的工艺和设备。例如，公路工程或岩土工程的土石方爆破作业中限制装药量以防止爆破飞石伤人；利用低电压设备，防止电击；限制车辆或设备运行速度，防止动能伤害。

⑶ 预防能量蓄积

能量的蓄积会导致能量的突然释放，因此要及时泄放能量防止能量过量蓄积。例如，通过接地消除危险物质车辆运输中的静电蓄积；利用避雷针放电保护重要设施和建筑物等。

⑷ 缓慢释放能量

尽量缓慢地释放能量降低单位时间内释放的能量，减轻能量对人体的作用，是一种常用的能量屏蔽方法。例如，汽车安全气囊、各种设备减振装置等

可以大幅度减少冲击动能，吸收冲击能量，防止人员伤害。

⑸ 设置屏蔽设施

屏蔽设施是一些防止人员与能量接触的物理实体。它们可以被设置在能源上（例如，安装在机械转动部分外面的防护罩等）；也可以被设置在人员与能源之间（例如，安全围栏、安全网等）；还可以被设置在人员身上（例如，安全帽、防护衣等）。

在生产过程中也有两种或两种以上的能量相互作用引起事故的情况（例如，车辆辗坏电缆等）。为了防止两种能量间的相互作用，可以在两种能量间设置屏蔽设施。

⑹ 信息形式屏蔽

各种警告措施，如警示灯、警示铃、警示牌等，可以阻止人的不安全行为的发生，防止人员接触能量。

⑺ 设置多重屏障

根据可能意外释放能量的大小，可以设置一种形式的多重屏障或多种形式的多重屏障。在生产过程中，应预先设置安全屏障，做到防患于未然。

3.4 事故综合原因理论

事故综合原因理论模型如图 3-3 所示。事故综合原因理论简称综合论，它是综合论述事故原因的现代理论。该理论认为，事故发生绝不是偶然的，而是有其深刻背景原因的，这些原因包括有生产中危险因素的直接原因、管理因素的间接原因和社会因素的基础原因。其生产中的危险因素加上触发因素引起事故发生。

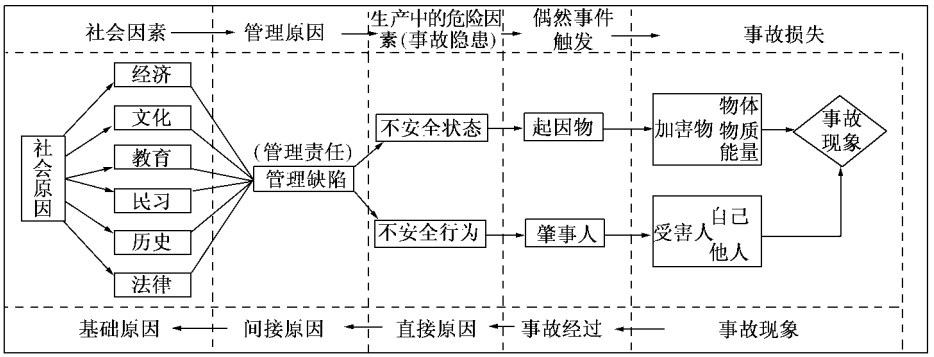


图 3-3 事故综合原因理论模型

事故的直接原因是指不安全状态（物和环境的原因）和不安全行为（人的原因）。这些物质的、环境的以及人的原因构成了生产中的危险因素（或称为事故隐患）；导致事故直接原因的事故间接原因是管理缺陷、管理因素和管理责任；导致事故间接原因的事故基础原因是社会因素（包括经济、文化、教育、习惯、历史和法律）。

简言之，事故的产生过程是：由“社会因素”产生“管理因素”，再由“管理因素”产生“生产中的危险因素”，通过“偶然事件”出发而形成的。

所谓偶然事件出发，是指由于起因物和肇事人的共同作用，造成一定类型事故和伤害的过程。

很显然，该理论全面综合地考虑了所有发生事故的现象和导致事故的因素，因此比较正确地反映了事故发生规律和事故原因，是当今最为流行的事故理论。

3.5 其他事故理论

除了上述事故理论之外，在安全工作中，从不同的侧面还经常会遇到多种不同的事故理论。这些理论从不同的角度出发，具有一定的指导作用。

⑴ 事故频发倾向论

所谓事故频发倾向，是指个别容易发生事故的、稳定的、个人的倾向。按照这一观点，事故频发倾向是由个人内在因素决定的，并且长时间不易改变的，也就是说，有些人的本性就是容易发生事故。具有这种倾向的人被称之为事故频发倾向者，他们的存在被认为是工业事故发生的原因。

20 世纪 40 年代早期，国外曾根据这一理论，通过严格的生理、心理检查，从众多的求职人员中挑选身体条件、智力条件、性格特征以及动作特征等方面均为优秀的人员就业，而把认为可能具有所谓的事故频发倾向的人员拒之门外。一旦发现有事故发生倾向苗头的人便予以解雇。

这一理论一直有所争议。近年来，许多的研究结果认为，事故频发倾向者并不存在。

⑵ 生物节律理论

此理论也称为 PIS 周期学说。生物节律理论认为，人与其他生物一样，是有生理节律的。人从出生之日起，体力 Physical（包括耐力、精力等）、情绪 Sensitive（包括感情、情绪等）、智力 Intellectual（包括记忆力、推理能力等）都是按一定时间呈周期性变化的。它们分别按 23 天（P）、28 天（I）和 33 天（S）为周期进行循环。其节律曲线如图 3-4 所示。

当某人的生物节律曲线由高潮向低潮转化或由低潮向高潮转化时（即通过临界期—临界点前后的相邻两天），人的生理表现很不稳定，发生事故的危险性较大。若某人的三条生物节律曲线同时通过临界点时，则发生事故的危险性最大。每个人的生物节律周期的开始时间不同，危险期也不同，可据此安排不同工作，避免事故发生。

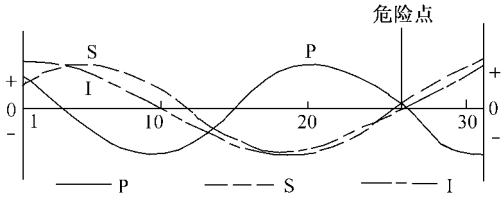


图 3-4　人体生物节律曲线

(3) 事故因果理论

此理论认为，事故的发生是由多个导致事故起因事件的作用引起的。其具体类型有集中型、连锁型和复合型，如图 3-5 所示。

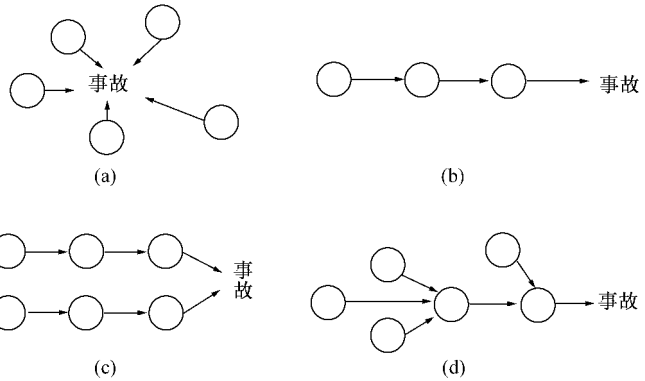


图 3-5　事故因果模型

(a) 集中型；(b) 连锁型；(c) 连锁、集中复合型；
(d) 集中、连锁复合型

海因里希事故因果连锁理论和现代事故因果连锁理论其实就是两种事故因果连锁模型。

(4) 事故扰动起源论

该理论也称为“P”理论。该理论认为，事故形成过程是一组自觉或不自觉的，指向某种预期的或不测结果的相继出现的事件链。这种事件链的发生过程也受到外界条件及其变化的影响。相继事件过程是一种在自动调节的动态平

衡中进行的。

如果行为者的行为得当或受力适中，即可维持能流稳定而不偏离正确的进程，即可实现安全生产的结果；如果行为者的行为不当或发生故障，则对上述平衡产生扰动 (Perturbation)，就会破坏和结束正确的动态平衡而开始导致发生事故的进程，最终造成伤害或损坏。这种伤害和损坏又会依次引起其他变化或能量释放。于是，根据该理论可以把事故看成是从相继的发生事故事件的扰动开始，以伤害或损坏而告终的过程，所以称之为“P”理论。

(5) 事故轨迹交叉论

该理论主要强调了人的不安全行为和物的不安全状态在时间和空间上的相互作用。事故轨迹交叉理论模型如图 3-6 所示。

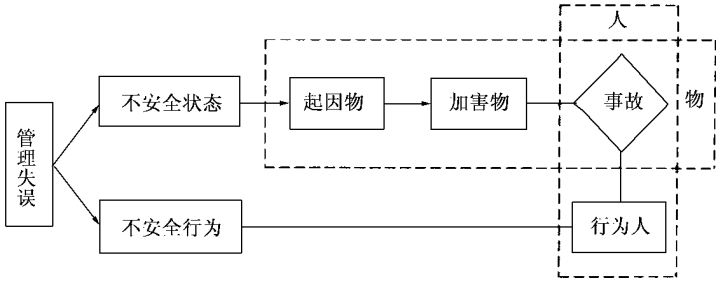


图 3-6　事故轨迹交叉模型

在该模型中，把物的因素进一步划分为起因物和加害物。起因物是引起事故发生的物体，加害物是作用于人体导致人员伤害的物体。模型中明确指出人的不安全行为是指行为人，即事故当事者的不安全行为。

当人与物两系统一旦发生时间和空间上的轨迹交叉时就会造成事故。与事故综合原因理论比较可以看出，它是事故综合原因理论的简化形式。根据这一理论，一方面，应加强安全教育、技术训练和科学管理，从生理、心理和技能上控制人的不安全发生；另一方面，应加强设备管理，提高其安全可靠性，增设安全保护和信号装置，改善作业环境，防止物的不安全状态出现。

除上述事故理论之外，根据具体的情况还有针对特定事故发生原理和不同的出发点提出的事故理论，在此不多加赘述。

3.6　事故预防原理

从管理角度研究预防事故时，主要有以下五个方面的原理可以遵循：

(1) 事故可以预防原理

事故是人灾，不是天灾。因此与天灾不同，人灾是可以预防的。要想防止

事故发生，应立足于防患于未然。对工伤事故不能只考虑事故发生后的对策，必须把重点放在事故发生前的预防对策上。

系统安全工程学把防患于未然作为重点，安全管理强调预防为主就是基于这一原理之上的。通常在事故调查中，常有“事故原因不可抗拒”的字样出现。所谓不可抗拒，只能是对天灾而言，作为人灾的事故，通过采取有效的对策，事故是完全可以避免的。

⑵ 偶然损失的原理

工伤事故包括两层意思：一是发生了意外事件；二是因事故产生损失。所谓损失包括人的损失，即人身事故 (如死亡、致残、有损健康、精神痛苦等) 和物质的损失，即物的事故 (包括设备损坏、原材料损失、产品报废、市场丧失、产量下降等)。

人身事故的伤害不同，其损失各异。根据海因里希的事故法则，事故与损失之间存在有下列关系：一个事故发生后损失的大小和种类是由偶然性决定的。反复发生的同类事故，并不一定造成相同的损失。

也有事故发生后不造成损失的险肇事故。即便危险事件没有造成损失，但如果该危险事件再次发生，会不会造成损失，损失有多大，是由偶然性决定的，而无法预测。

因此，根据这一原理，为了防止由于发生事故造成的重大损失，惟一的办法就是防止事故的再一次发生。

⑶ 继发原因的原理

如前事故理论中所述，事故的发生与其原因有着必然的因果关系，即事故与原因是必然的关系；而事故与损失却是偶然的关系。

所谓继发原因的原理指的是因果关系的继承性。事故综合原因理论很好地表明了这一理论的过程。

损失是由事故引起的，事故是造成损失的原因；事故又是由直接原因 (又称为一次原因) 所导致的，直接原因是事故的近因；直接原因是由间接原因 (又称为二次原因) 引起的，间接原因是直接原因的原因；间接原因是由更深远的基础原因造成的，基础原因又称为远因。

这样便形成了事故原因的继发连锁关系。根据继发原因理论，切断事故原因链，就能够防止事故的发生。欲做到这一点，选择适当的对策，进行正确的事故原因分析是至关重要的。

在事故原因分析中，不仅要强调工人“违章作业”“不小心”“不注意”等的责任，也必须要强调企业管理、教育、文化、历史及法律等方面的基础原因。

⑷ 选择对策的原理

该原理认为，为了预防事故，采取的对策是否切合实际是十分重要的。预防事故的对策应该是在原因分析的基础上得出的。同时，以间接原因和基础原因为对象的对策才是根本的对策。

通常，在事故预防中普遍采用的是 3E 对策，即技术对策 (Engineering)、教育对策 (Education)、法制对策 (Enforcement)。此 3E 对策被认为是预防事故的三大支柱。

⑸ 危险因素防护原理

此原理具有以下十个方面的原则：

1) 潜在危险防护原则

采用高新技术消除作业环境中的危险和有害因素，从而保证系统最大可能的安全性和可靠性，最大限度地防护潜在的危险因素。

2) 降低危险程度原则

当不能根除危险因素时，应采取降低危险程度和有害因素数量的措施。如加强个体防护、降低粉尘和有毒物质的摄入量等。

3) 安全距离防护原则

一般情况下，生产中的危险因素和有害因素的作用具有随距离的增加而减弱的规律。根据这一规律可根据不同情况设置安全距离，预防事故发生。自动化或遥控操作等技术是安全距离防护原则的发展方向。

4) 缩短时间防护原则

这一原则是使操作人员处于具有危险和有害因素作用环境中的时间缩短到安全限度之内。

5) 安全屏蔽防护原则

这一原则是指在危险和有害因素作用的范围内设置屏障，防止危险和有害因素的伤害。这里的屏蔽是广义的屏蔽，它包括有形的屏蔽和无形的屏蔽。

6) 安全坚固防护原则

增大生产设备、设施等的安全系数，提高结构强度。

7) 有意损坏防护原则

有意利用一些易损部件，使之在危险因素尚未达到危险作用之前预先损坏，增强安全保护。如保险丝、安全阀片等。

8) 不与接近防护原则

此原则是指不许人员接近具有危险和有害因素作用区域，或消除危险物进入人员作业区域。如安全网、安全栏等。

9）安全闭锁防护原则

这一原则是指，当某种作业系统或设备欲发生事故时，其中某一环节强制自锁，使作业系统或设备停止运转，防止事故发生。如电梯的安全过卷装置等。

10）取代人员防护原则

在特殊和极度危险的作业环境下，用机械设备等代替人员作业。如机器人水下作业、自动化设备采矿等。

思　考　题

1. 何谓事故？何谓事故理论？
2. 试说明事故法则的内容和意义。
3. 事故预防的 3E 对策是什么？
4. 应用能量释放理论如何防止脚手架上高空坠落事故的发生？
5. 如果一名危险工种的作业人员出生于 1980 年 9 月 13 日。试计算 2005 年 3 月 20 日他的生物节律状态，分析其是否适合于从事危险工种的作业？
6. 危险因素防护原理中具有哪些防护原则？

4　人为失误及其预防

统计发现，在所发生的伤亡事故中，大多是因为人的失误造成的。由于人为失误所引起的事故占不同类型企业事故比重的50%～90%。因此，对人为失误进行研究，对于在生产实际中努力降低人为失误率，防止事故发生具有重要的实际意义。

4.1　人为失误的定义与分类

人为失误，即人的行为失误，是指工作人员在生产、工作过程中导致实际要实现的功能与所要求的功能不一致，其结果可能以某种形式给生产、工作带来不良影响的行为。换句话说，人为失误就是工作人员在生产、工作中产生的错误或误差。

人为失误可能发生在计划制定、工程设计、制造加工、设备安装、设备使用、设备维修以至于管理工作等各种工作过程之中。人为失误可能导致物的不安全状态或人的不安全行为。其实人的不安全行为本身也就是一种人为失误，所不同的是不安全行为往往是事故直接责任者或当事者的行为失误，是人为失误的特例。另外，管理失误也是一种人为失误，并且是一种更加危险的人为失误。

一般来说，在生产、工作过程中人为失误是难以避免的，但是可以通过管理和技术上的措施降低人的失误率。

按人为失误产生的原因可以分为随机失误、系统失误和偶发失误三种类型。

⑴ 随机失误

它是由于人的动作、行为的随机性质引起的人的失误。例如，手工操作时用力的大小，精确度的变化，操作的时间差，简单的错误或一时的遗忘等。随机失误往往是不可预测的，但是，是不会重复发生的。

⑵ 系统失误

它是由于工作条件设计方面的问题，或人员的不正常状态引起的。系统失误主要与工作条件有关，设计不合理的工作条件很容易诱发人为失误。易于引起人为失误的工作条件大体上分两个方面的问题：其一是工作任务的要求超出

了人的承受能力；其二是规定的操作程序方面的问题，在正常工作条件下形成下意识的行动和习惯使人们不能应付突如其来的紧急情况。

在类似情况下，系统失误可能重复发生，通过改善工作条件及教育训练，能够有效地防止此类失误。

⑶ 偶发失误

它是由于某种偶然出现的意外情况引起的过失行为，或者事先难以预料的意外行为。例如，违反操作规程，违反劳动纪律的行为。

研究认为，人为失误与人的素质和能力具有密不可分的关系。

4.2 人的心理紧张程度与人为失误

人们在工作中，心理的紧张程度直接影响到注意力集中的程度，而注意力集中程度取决于大脑的意识水平 (警觉度)。经研究表明，由于意识水平低而引起对外界信息处理能力的降低是发生人为失误的内在原因。通常大脑的意识水平可分为五个等级：

⑴ 意识丧失

在熟睡、昏迷或癫痫发作等情况下，大脑将完全停止工作。甚至于在身体机能正常状态下，由于过度紧张也可以导致大脑出现无意识的一片空白。

⑵ 反应迟钝

过度疲劳或工作单调，困倦或醉酒，过度紧张可以导致反应迟钝，不能进行任何外界信息的处理。

⑶ 反应被动

长期从事熟悉的、重复性强的工作时，大脑活动易于出现被动状态。

⑷ 反应能动

由于紧张程度适宜，身体机能状态良好，从事相对复杂且不太熟悉的工作时，大脑清晰而高效地工作，积极地发现问题和思考问题，主动进行信息处理。但是，这种状态维持时间较短，随着疲劳出现，意识倦怠，进入反应被动状态。

⑸ 恐慌状态

随着工作任务过重，精神过度紧张或过度恐惧时，不能认真思考问题，以至于信息处理能力降低，信息处理过程中断，大脑出现“空白”现象。

人们在正常的生产过程中，大脑的意识水平经常处在反应能动和反应被动的正常状态下。此时相对信息处理能力较高，失误相对较少；当大脑意识水平处于反应迟钝或恐慌状态时，相对信息处理能力较低，失误相对较多。人的大脑意识水平与心理紧张程度密切相关，而人的心理紧张程度直接影响人的信息

处理能力。图 4-1 绘出了心理紧张程度与信息处理能力之间的关系。从图中可以看出，人在工作时存在有最优的心理紧张程度，此时大脑的意识水平处于能动状态，信息处理能力最高，失误率最低。通常可以将心理紧张程度分为 4 个等级：

1）低级紧张程度。在从事缺少刺激的、过于轻松的工作时，几乎不用脑筋思考；

2）最优紧张程度。在从事较为复杂的、需要思考的工作时，大脑能动地工作；

3）稍高紧张程度。在从事要求迅速行动或一旦发生失误可能出现危险的工作时，心理紧张程度有所升高，易于发生失误；

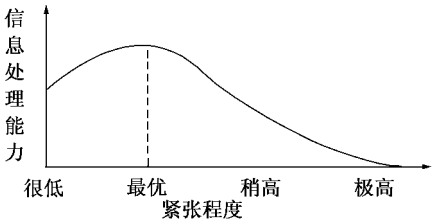


图 4-1　信息处理能力与紧张程度

4）极高紧张程度。在从事危险工作，人员面临生命危险时，大脑处于恐慌状态，很容易发生失误。

除了工作任务引起心理紧张之外，还有如酗酒、疲劳、生理等许多因素增加诸如不安、烦躁、焦虑等心理紧张的程度；工作场所照明不良、温度异常以及噪声等物理因素也可以增加心理紧张的程度；心理紧张程度还与个人的经验、技能等有关。一般来说，缺乏经验及操作不熟练的人心理紧张程度较高。

工作中，合理安排工作任务，消除各种增加心理紧张的因素，以及经常进行训练、教育，是使职工保持最优心理紧张程度的主要途径。

4.3　人的能力与人为失误

在生产作业中，工作人员要经常处理各种有关的信息，同时付出一定的智力和体力来承受工作中的负荷。当工作人员的信息处理能力过低时，容易发生失误。人们处理信息的能力取决于工作人员的硬件状态、心理状态和软件状态。

硬件状态是指人的生理、身体、病理以及药理状态。当人们受到生物节律、倒班、生产作业环境等不利因素的影响，生理状态处于疲劳、睡眠不足、醉酒、饥渴等情况下时，将降低大脑的意识水平，降低信息处理能力；人体的感觉器官的灵敏性、感知范围将影响对外界信息的接受能力；人体不同的身高、力量的大小及运动的速度等将影响动作行为的准确性；人体疾病、心理精神不正常、后遗症等病理状态将影响大脑的意识水平；人们服用某些药剂会大大降低大脑的意识水平。

心理状态是指人心理的稳定状况，它将直接影响到人的心理紧张程度。如心理焦虑、恐慌等状态将妨碍大脑对正常信息的处理；家庭纠纷、忧伤等将引起情绪不安、注意力分散、操作失误；工作任务、工作环境以及人际关系等方面的问题也会影响人的心理状态。

软件状态是指作业人员在生产操作方面的技术水平、知识水平、执行作业规程和程序的能力。在信息处理过程中软件状态对于选择、判断、决策具有重要的影响。随着科学技术的进步，机械化、自动化水平的不断提高，对作业人员的软件状态的要求将越来越高。人的硬件状态、心理状态在短时间内可能会发生很大变化，而软件状态却需经过很长时间的工作实践和经常性的教育、训练才能改变。

4.4 人为失误的预防

本书将着重从预防人为失误的技术措施和管理措施两方面讨论人为失误的预防。

4.4.1 预防人为失误及其危害的技术措施

从预防事故防止损失的角度，如图 4-2 所示，可以从以下三个阶段采取技术措施，防止人为失误，减少人为失误及其损失。

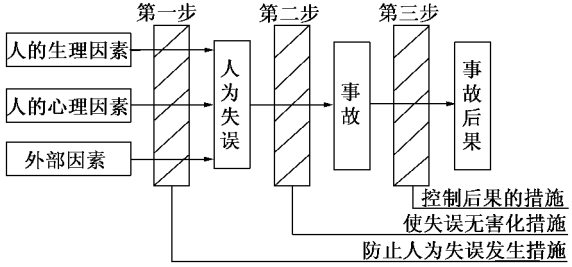


图 4-2 防止人为失误的途径

第一阶段是采取防止人为失误的技术措施。控制、减少可能引起人为失误的各种因素，防止出现人为失误或有效地降低人为失误率。

第二阶段是采取防止人为失误的无害化技术措施。由于人们在生产和工作过程中，产生失误是在所难免的，所以在易于发生人为失误的场合或地点采取有效措施，即使人为失误发生也不至于发生事故，造成损失。使人为失误无害化。

第三阶段是采取控制人为失误的后果技术措施。在因人为失误容易引起事

故的情况下，采取有效措施限制事故的进一步发展，努力减少事故造成的损失。

⑴ 防止人为失误的技术措施

1) 采用机器代替工作人员作业

用机器代替人作业是彻底防止作业中人为失误的最好办法。通常机器的故障率为 $10^{-4} \sim 10^{-6}$之间，而人为失误率在 $10^{-2} \sim 10^{-3}$之间。可见，机器的故障率远远小于人为失误率。

2) 采用冗余系统预防人为失误

冗余就是把若干个元素并联附加于系统基本功能元素上，以提高系统的可靠性。附加的元素称为冗余元素，含有冗余元素的系统称为冗余系统。其具体方法主要有双人操作、人机并行操作、设计审查等。

3) 采取安全设计预防人为失误

在工程或设备的设计中采取安全设计措施，使操作人员不出现人为失误或出现人为失误也不会导致事故发生。具体的方法是，利用不同的形状或规格尺寸预防安装或连接的操作失误；利用连锁或紧急停车装置预防人为失误，或使人为失误无害化；采取强制措施使人员不能发生操作失误。

4) 采取警告措施预防人为失误

警告包括视觉警告（亮度、颜色、信号灯、标志等）、听觉警告（如警铃、警报等）、气味警告（如不同的气味等）和感（触）觉警告（如温度、阻挡物等）。

5) 人、机、环境匹配预防人为失误

主要包括人机动作的合理匹配、机器设备的人机学设计以及生产作业环境的人机学要求等，如显示器的人机学设计、操纵设备的人机学设计、生产环境的人机学设计。

⑵ 防止人为失误无害化的技术措施

为了防止人为失误导致的事故，可以采取如下无害化措施：

1) 设立事故预防装置，保证在人失误的情况下也能确保系统处于安全状态；

2) 设立失误保护系统，当个别部件或子系统发生故障时，仍可保证系统可靠地工作；

3) 设立连锁装置，当操作失误时，设备不能启动。

⑶ 防止人为失误后果的技术控制措施

事故通常是由小到大，由近而远。为了控制由人为失误导致的事故危害范围，对危险作业地点（如易发火的车间）应事先做好准备（如设立自动灭火器），一旦出现事故，将之控制在发生地。

如前所述，由能量释放理论，事故就是失控能量的释放，人为失误引起的事故也不例外。为防止失控释放的能量伤害人员和设备，可采取分流 (如泄压阀)、隔离 (防爆墙)、安全出口或通道、发放自救器材等措施。

4.4.2 预防人为失误的管理措施

预防人为失误的管理措施主要有职业适应性措施、作业标准化措施、安全教育措施和技能训练措施等。

(1) 职业适应性措施

职业适应性是指人员从事某种职业应具备的基本条件。它着重于职业对人员能力的要求。职业适应性措施主要包括以下几个方面：

1) 职业适应性的分析

首先，分析确定特定职业的特性，如工作条件、工作空间、物理环境、使用工具、操作特点、所需训练时间、判断难度、安全状况、作业姿势、体力消耗等特性；然后，在分析了职业特性的基础上，进行人员职业适应性的分析，确定从事该职业人员应具备的条件，如所负责任、知识水平、技术水平、创造能力、灵活性、体力消耗、所受训练和具备的经验等。

2) 职业适应性的测试

职业适应性测试就是指在人们初步选定自己的职业之后，测试其具备的能力，分析是否符合所从事职业的要求。

3) 职业适应性人员的选择

对于特定的职业，选择能力过高或过低的人员都不利于事故的预防。一个人的能力低于操作要求时，可能会由于没有能力正确处理操作中的各种信息而不能胜任，从而出现人为失误；反之，当一个人的能力超过操作水平时，可能会由于心理紧张度过低，产生厌倦和懈怠情绪，从而引发人为失误。

(2) 作业标准化措施

根据对人为失误原因的调查可发现下列三种原因占有很大的比例：

1) 不知道正确的操作方法；

2) 为了省事，省略必要的操作步骤；

3) 按自己的习惯操作。

为了克服这些问题，应积极推广标准化作业，用科学的作业标准来规范人的行为。作业标准化应满足如下要求：

1) 应明确规定操作步骤和程序。例如，关于人力搬运作业中，应具体地规定出如何搬、搬往何处等。

2) 不应给操作者增加负担。例如，对操作者的技能和注意力不能要求过

高，操作尽可能简单化、专业化，尽量减少使用卡具或其他工具的次数，采用自动化设备等。

3）符合现场实际情况。由于同样的生产过程在具体实施中变化很大，所以结合通用标准，针对具体情况制定切实可行的作业标准是十分必要的。

在制定作业标准时，首先把操作过程分解为若干单元，逐一设计各单元的动作，然后相互衔接成为整体。一般地，制定作业标准要考虑人体运动、作业场所布置以及使用的设备、工具等应符合人机学原理。

在制定作业标准时，应该有管理人员、技术人员和操作者共同研究，经反复实践后才可确定。

⑶教育与训练措施

安全教育与技能训练是为了预防操作者不安全行为，预防人为失误的重要途径。首先，能使企业领导和广大职工提高事故预防工作的自觉性和责任感。其次，可以使干部和职工掌握安全技术知识，掌握安全技能和生产技能，保证生产能够安全可靠地进行。

1）教育措施

这里所提及的教育是指安全教育。主要包括三个方面：

①安全知识教育。安全知识教育就是要使操作者掌握有关事故预防的基本知识，使操作者了解和掌握生产操作过程中潜在的危险因素及防范措施等。

②安全技能教育。安全技能教育就是在熟练掌握安全知识的基础上，使操作者学习掌握保证操作安全的基本技能。

③安全态度教育。安全态度教育就是在既掌握了安全知识又掌握了安全技能的基础上，使操作者自觉地运用安全知识和安全技能，变被动的“要我安全”为主动的“我要安全”。

2）训练措施

这里所提及的训练是指技能训练。主要包括两个方面：

①安全技能训练。安全技能训练就是使操作者在学习掌握了安全知识和安全基本技能的基础上，反复实践和实际训练，完全熟练地掌握安全技能的操作要领。保证在作业过程中，遇到安全问题时能果断熟练地运用安全技能采取安全措施。

②生产技能训练。生产技能训练就是使操作者掌握了安全生产知识和安全技能以及安全态度端正的基础上，对其生产技能按标准要求进行严格的训练，使之熟练掌握生产技能。往往具有较高生产技能操作者，也具有较高的安全技能和较好的安全意识。

思　考　题

1. 何谓人为失误？有哪几种类型？
2. 人的心理紧张程度与人为失误有何关系？
3. 人的能力与人为失误关系如何？
4. 如何从技术上预防人为失误？
5. 如何从管理上预防人为失误？

5 系统可靠性分析

5.1 基本概念

可靠性是用来判断和评价系统好坏的重要指标，它主要是采用计算概率的方法来定量描述系统、设备、元件等在规定条件下和预定时间内完成规定功能的性能。

可靠度是指系统、设备、元件等在规定条件下和预定时间内完成规定功能的概率，是可靠性的定量描述，用 R（t）来描述。

故障是指系统、设备、元件等在运行过程中性能低下，不能实现预定功能的状态。故障的发生是人们所不希望的，但是它又是不可避免的。

故障时间是指系统、设备、元件等从投入使用开始到发生故障所经过的时间，用 t 来表示。若故障不能被恢复，则称此故障时间为寿命。

故障率是指正常工作到某时刻的系统、设备和零件等在此后单位时间内所发生事故的比率，用 λ 来表示。它是一个重要指标。特别是在系统安全分析中经常使用这一指标。按系统、设备、零件等故障率随时间减少、不变和增加的三种不同趋势可把故障分为初期故障、随机故障和磨损故障三种类型。通常无论是机械设备、工业装置、元件的故障率，还是人类的死亡率都具有相类似的随时间变化的曲线（如图 5-1），俗称浴盆曲线。

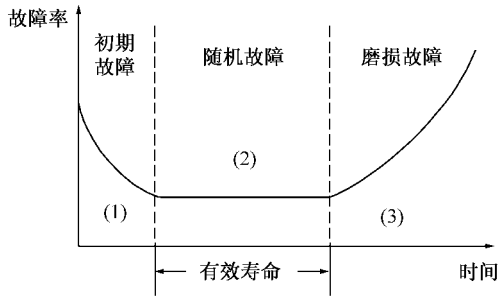


图 5-1 浴盆曲线

人的操作可靠性是把人作为系统中的元素，研究人在执行既定操作时，完成要求功能的可靠性。

人的失误率是用来表征人在操作时发生失误的难易程度量度指标。由于人有思想，而且人的行为又有较大的自由度，所以人的可靠性的研究是一个更加复杂的课题。

5.2 故障发生规律

5.2.1 故障随时间的变化规律

设系统、设备、元件等在 $t = 0$ 时刻开始运行，到 t 时刻发生故障的概率和可靠度分别为如下形式：

故障概率 $$F(t) = P_r(T \leqslant t) \tag{5-1}$$

可靠度 $$R(t) = 1 - F(t) \tag{5-2}$$

当 $F(0) = 0$ 时，$R(0) = 1$

式（5-1）又称为故障时间分布函数，对其进行微分可得到故障概率（或时间）密度函数，将其对时间积分又可以得到故障概率，见式（5-3）和式（5-4）：

故障概率密度函数 $$f(t) = \frac{dF(t)}{dt} \tag{5-3}$$

故障概率 $$F(t) = \int_0^t f(t)\,dt \tag{5-4}$$

通常，故障率函数定义为：

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{5-5}$$

当 dt 很小时，$\lambda(t)\,dt$ 表示到 t 时刻没有发生故障，而在时间间隔 $(t, t + dt)$ 内发生故障的概率。该式也可写成：

$$\lambda(t) = \frac{dF(t)}{dt \cdot \overline{F}(t)} = \frac{dR(t)}{R(t)\,dt} \tag{5-6}$$

将其对时间积分得到：

$$\int_0^t \lambda(t)\,dt = -[\ln R(t)]_0^t = -[\ln R(t) - \ln R(0)] = -1 - \ln R(t)$$

于是，可以得到可靠度 $R(t)$ 和故障发生概率 $F(t)$ 分别与故障率函数 $\lambda(t)$ 之间的如下关系式（5-7）和式（5-8）：

$$R(t) = e^{-\int_0^t \lambda(t)\,dt} \tag{5-7}$$

$$F(t) = 1 - R(t) = 1 - e^{-\int_0^t \lambda(t)\,dt} \tag{5-8}$$

可见，故障率函数 $\lambda(t)$ 决定了故障时间分布函数 $F(t)$ 和可靠度函数 $R(t)$ 的分布形式。

为了更好地理解可靠度函数 $R(t)$、故障时间密度函数 $f(t)$、故障时间分布函数 $F(t)$ 和故障概率函数 $\lambda(t)$ 各类函数的意义，特举例说明。

【例 5-1】 现有某类元件 100 个，同时投入使用。经使用了 7 个不同时间

（可以是年、月、天或小时）时（$t=0$，1，2，3，4，5，6），损坏和完好的情况如表 5-1 所示。

表 5-1　各类函数计算表

经过的时间 t	完好的数量 $N(t)$	损坏的数量 $N(t-1)-N(t)$	可靠度分布 $R(t)$	故障时间密度分布 $f(t)$	故障时间分布 $F(t)$	故障概率分布 $\lambda(t)$
0	100	0	1.00	0.00	0.00	0.00
1	94	6	0.94	0.06	0.06	0.06
2	75	19	0.75	0.19	0.25	0.20
3	32	43	0.32	0.43	0.68	0.57
4	9	23	0.09	0.23	0.91	0.72
5	2	7	0.02	0.07	0.98	0.78
6	0	2	0.00	0.02	1.00	1.00

表中用 $N(t)$ 表示使用到 t 时刻没有发生损坏的元件数量；用 $N(0)$ 表示所使用的元件总数；用 $N(t-1)-N(t)$ 表示时间间隔 $(t-1,\ t)$ 内的损坏元件的数量，那么就有：

可靠度函数　　$$R(t)=\frac{N(t)}{N(0)}$$；

故障时间密度函数　　$$f(t)=\frac{N(t-1)-N(t)}{N(0)}$$；

故障时间分布函数　　$$F(t)=\frac{N(0)-N(t)}{N(0)}$$；

故障率函数　　$$\lambda(t)=\frac{N(t-1)-N(t)}{N(t-1)}$$

当用较小的时间间隔表示故障时间分布时，其各分布函数称为经验分布函数。当元件数无限多，时间间隔无限小时，其各经验分布函数便成为真正的分布函数。

5.2.2　故障随时间的分布形式

（1）指数分布

在随机故障的场合，故障率函数为常数，$\lambda(t)=\lambda$，即为故障率。此时，故障时间的分布变为指数分布，此时的故障发生概率（故障时间分布函数）$F(t)$ 和故障概率密度函数（故障时间密度函数）$f(t)$ 如下：

$$F(t)=1-e^{-\lambda t} \tag{5-9}$$

$$f(t)=\lambda e^{-\lambda t} \tag{5-10}$$

故障率 λ 是指数分布的惟一的分布参数，也是一个最具有实际意义的参

数。它表示单位时间里发生故障的次数。

指数分布的数学期望 $E(x)$ 为：

$$E(x) = \int_0 tf(t)\,dt = \int_0 R(t)\,dt = \int_0 e^{-\lambda t}dt = \frac{1}{\lambda} = \theta \qquad (5\text{-}11)$$

可见，数学期望等于故障率的倒数，记为 θ，称作平均故障时间 (MTTF)。在系统、设备、元件等故障后，经修理被重新使用时称为平均故障间隔时间 (MTBF)。有时，还被统称为平均寿命。

指数分布的方差：

$$V(x) = E\left\{[x - E(x)]^2\right\} = E(x^2) - [E(x)]^2 = \int_0 t^2 f(t)\,dt - \frac{1}{\lambda^2} = \frac{1}{\lambda^2} = \theta^2 \qquad (5\text{-}12)$$

当时间为平均故障时间时，即 $t = \theta$ 时：

发生故障的概率应为：$F(\theta) = 1 - e^{-\lambda\theta} = 1 - e^{-1} = 0.633$；可靠度为：$R(\theta) = 0.367$

【例 5-2】 某设备运转了 7000 小时共发生了 10 次故障。若故障间隔时间服从指数分布，试计算该设备的平均故障间隔时间 θ 和从开机运行到工作 1000 小时后的可靠度 $R(t)$。

【解】 平均故障间隔时间应为：

$$\theta = \frac{1}{\lambda} = \frac{7000}{10} = 700\ (h) \qquad \lambda = \frac{1}{700}$$

工作 1000 小时后的可靠度应为：

$$R(1000) = e^{-1000\lambda} = e^{-\frac{1000}{700}} = 0.239$$

【例 5-3】 某种元件的平均故障时间 $\theta = 5000$ 小时。试计算使用 $t = 125$ 小时后的可靠度。

【解】 因为 $\lambda t = \frac{t}{\theta} = \frac{125}{5000} = 0.025 < 1$，利用级数展开取前两项进行计算可靠度，得：

$$R(t) \approx 1 - \lambda t \text{ 即：} R(125) = 1 - 0.025 = 0.975$$

(2) 韦伯分布

按韦伯分布时，故障时间分布函数和可靠度分别为式 (5-13) 和式 (5-14)：

$$F(t) = 1 - e^{-\frac{t^m}{\eta}} \qquad (5\text{-}13)$$

$$R(t) = e^{-\frac{t^m}{\eta}} \qquad (5\text{-}14)$$

故障时间密度函数和故障率函数分别为式 (5-15) 和式 (5-16)：

$$f(t) = \frac{m}{\eta}t^{m-1}e^{-\frac{t^m}{\eta}} \qquad (5\text{-}15)$$

$$\lambda(t) = \frac{m}{\eta} t^{m-1} \tag{5-16}$$

式中 η——尺度参数；

m——形状参数。

韦伯分布的故障时间密度函数和故障率函数分别如图 5-2 和图 5-3 所示：

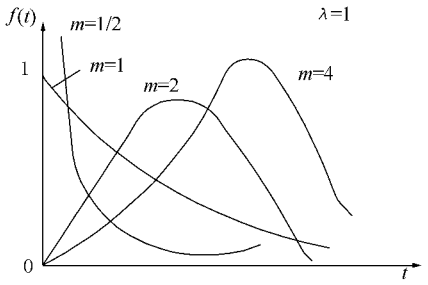


图 5-2 故障时间密度函数分布

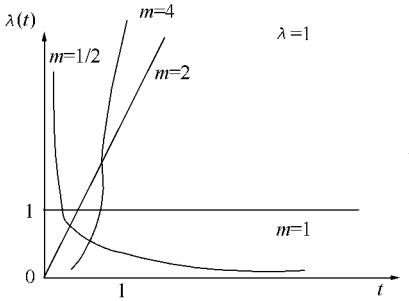


图 5-3 故障率函数分布

在韦伯分布中随着参数 m 的取值不同，具有不同的实际意义：

1) 当 $m < 1$ 时，故障率 $\lambda(t)$ 随时间单调减小，可对应于初期事故；

2) 当 $m = 1$ 时，故障率 $\lambda(t)$ 随时间恒定，变为指数分布，可对应于随机故障；

3) 当 $m > 1$ 时，故障率 $\lambda(t)$ 随时间单调增大，可对应于磨损事故。

韦伯分布的数学期望和方差分别为式 (5-17) 和式 (5-18)：

$$\theta = \eta^{\frac{1}{m}} \Gamma\left(1 + \frac{1}{m}\right) \tag{5-17}$$

$$\sigma = \eta^{\frac{1}{m}} \left\{ \Gamma\left(1 + \frac{2}{m}\right) - \left[\Gamma\left(1 + \frac{1}{m}\right)\right]^2 \right\}^{1/2} \tag{5-18}$$

式中 Γ 符号表示 Γ 分布。

5.2.3 故障次数分布

当故障时间分布服从指数分布，即故障发生率 λ 为常数时，一定时间间隔内故障发生次数 $N(t)$ 服从泊松分布。

自时刻 $t = 0$ 到 t 时刻发生 n 次故障的概率记为：

$$P_n(t) = P_r\{N(t) = n\}, n = 0,1,2,\cdots \tag{5-19}$$

则 $P_n(t)$ 为参数 λt 的泊松分布

$$P_n(t) = (\lambda t)^n e^{-\frac{\lambda t}{n!}} \tag{5-20}$$

到 t 时刻发生不超过 n 次故障的概率：

$$P_r\{n(t) \leqslant n\} = \sum_{k=0}^{n} \frac{(\lambda t)^n}{k!} e^{-\lambda t} \tag{5-21}$$

故障次数 $N(t)$ 的数学期望 $E[N(t)]$ 和方差 $V[N(t)]$ 分别为：

$$E[N(t)] = \sum_{n=0} nP_n(t) = \sum_{n=1} n \frac{(\lambda t)^n}{n!} e^{-\lambda t} = \lambda t \tag{5-22}$$

$$V[N(t)] = E[N^2(t)] - \left\{E[N(t)]\right\}^2 = \sum_{n=0} n^2 P_n(t) - (\lambda t)^2 = \lambda t \tag{5-23}$$

即，故障次数的数学期望和方差都是 λt。

5.3 故障数据处理

故障数据处理是通过对收集的故障数据进行统计处理而弄清故障发生规律的工作。通过专门的试验或观测可以获得故障时间数据；根据获得的故障时间数据可以确定时间分布函数。

故障时间数据通过试验观测获得，这些试验被称作可靠性试验。可靠性试验有多种方式，按试验地点分为现场试验和实验室试验；按试验结束方式分为完整试验和截尾试验，前者进行到全部试件故障为止，后者进行到若干试件故障为止。截尾试验又分为定时截尾方式和定数截尾方式，前者进行到规定的试验时间停止试验；后者进行到规定数目的试件发生故障时停止试验。按试件故障后是否更换又分为更换法和不更换法。各种试验方式都有各自的优点，实际工作中，应根据实际情况进行选择。

由于故障的发生具有随机性质，即使同一批试件在同一条件下工作，故障时间的数据也是不同的，只能利用统计分布来描述。所以，根据概率论中的大数定理，当收集到故障数据的数量（统计学中称样本）相当多时，故障时间分布函数才是一定的。但是，在实际工作中受各方面条件的限制，往往收集到的故障数据很有限。因此，如何应用统计学的方法由较少的故障数据来确定其分布函数就是十分重要的。

当已知统计分布函数的形式时，该分布函数是由一些参数值确定下来的。如果能够确定这些参数值，随即具体的分布函数也可以确定下来。因此，故障数据处理的重要步骤是根据故障时间的数据推断出分布函数中的参数值。另外，还可以通过统计推断方法，由故障时间数据估算出表征故障发生性质的特征量——平均故障时间或平均间隔时间的数值。在不知故障时间分布函数具体形式时，需要用统计检验的方法确定。

统计分布的参数估计包括点估计和区间估计两方面的问题。前者在于推断

出分布参数的一个参数值；后者在于考察该参数值的精确程度，即其真值所在的区间范围。在参数点估计的方法中，以最大似然法和矩法最为常用。在这里只介绍最大似然法。

最大似然法的基本思想是，如果在一次观测中出现了某一个事件，那么我们认为该事件出现的可能性很大。

假设我们获得的 n 个故障时间数据分别是 t_1，t_2，t_3，…，t_n，则首先构造一个 n 变量的函数——似然函数，通过求解该函数的极值来得到分布参数的估计值。

5.3.1 指数分布的参数估计

(1) 完整试验的点估计

当进行完整试验时，观测全部 n 个试件的故障，记录其故障时间 t_1，t_2，t_3，…，t_n。其所构造的似然函数如下：

$$L(t_1, t_2, t_3, \cdots, t_n) = \prod_{i=1}^{n} f(t_i, \lambda) \tag{5-24}$$

式中 $f(t_i, \lambda)$ ——故障时间密度函数，在指数分布的场合：

$$f(t_i, \lambda) = \lambda e^{-\lambda t_i} \tag{5-25}$$

上式可以写成：

$$L(t_1, t_2, t_3, \cdots, t_n) = \prod_{i=1}^{n} f(t_i, \lambda) = \lambda^n e^{-\lambda \sum_{i=1}^{n} t_i} \tag{5-26}$$

为求得使似然函数最大的 λ 的估计值，对该式两端取对数，并令一阶偏导数为零：

$$\ln L(t_1, t_2, t_3, \cdots, t_n) = n \ln \lambda - \lambda \sum_{i=1}^{n} t_i \tag{5-27}$$

得到的参数 λ 的估计值 $\hat{\lambda}$ 和平均故障时间 θ 的估计值 $\hat{\theta}$ 分别为：

$$\hat{\lambda} = n \Big/ \sum_{i=1}^{n} t_i \tag{5-28}$$

$$\hat{\theta} = \frac{1}{\hat{\lambda}} = \sum_{i=1}^{n} t_i \Big/ n \tag{5-29}$$

(2) 截尾试验的点估计

通常情况，定数截尾试验比定时截尾试验得到的估计值更接近真值，因此在此只介绍定数截尾试验方式时的点估计。

设当定数截尾试验进行到 n 个试件中 r 个试件故障时，即停止试验。如果 r 个试件的故障时间分别为 t_1，t_2，t_3，…，t_r。设，第一次故障发生在时刻 t_1，第二次故障发生在时刻 t_2，…，第 r 次故障发生在时刻 $t_r = \tau$。于是，余

下的n - r个试件不发生故障的概率就为：

$$f(t_1;\lambda)\,dt_1 f(t_2;\lambda)\,dt_2\cdots f(t_r;\lambda)\,dt_r\left\{1-F(\tau)\right\}^{n-r}$$

$$=\prod_{i=1}^{r} f(t_i;\lambda)\,dt_i\left\{1-F(\tau)\right\}^{n-r} \tag{5-30}$$

式中 $F(t)$ ——故障时间分布函数，其概率密度为 $f(t;\lambda)$。

考虑到这 r 次故障都发生在 r 个试件上时，其可能的组合数是$\frac{n!}{(n-r)!}$。所以 r 次故障发生在试验的 r 个试件上的概率为：

$$\frac{n!}{(n-r)!}\prod_{i=1}^{r} f(t_i;\lambda)\,dt_i\left\{1-F(\tau)\right\}^{n-r} \tag{5-31}$$

此时，所构造似然函数应为：

$$L(t_1,t_2,\cdots,t_n;\lambda)=\frac{n!}{(n-r)!}\prod_{i=1}^{r} f(t_i;\lambda)\left\{1-F(\tau)\right\}^{n-r}$$

$$=\frac{n!}{(n-r)!}\prod_{i=1}^{r}\lambda e^{-\lambda t_i}\left\{1-F(\tau)\right\}^{(n-r)} \tag{5-32}$$

令，$\partial(\ln L)\Big/\partial\lambda=0$，可得到 λ 的估计值λ：

$$\lambda=r\Big/\left[\sum_{i=1}^{r} t_i+(n-r)\tau\right] \tag{5-33}$$

平均故障时间 θ 的估计值θ即为：

$$\theta=\left[\sum_{i=1}^{r} t_i+(n-r)\tau\right]\Big/r \tag{5-34}$$

(3) 区间估计

虽然，用点估计法可以通过故障数据推断出故障率 λ 或平均故障时间θ 的估计值，但是，要了解近似值的精确程度，还需对其进行误差估计，也就是故障率 λ 或平均故障时间θ 的真值所在的范围，即置信区间。所谓区间估计就是推断在给定置信度下的置信区间。

设危险率为 α，则置信度为 $(1-\alpha)$。在置信度 $(1-\alpha)$ 一定时，截尾试验的平均故障时间 θ 的置信区间为：

$$\left[2T\Big/\chi^2\left(2r;\frac{\alpha}{2}\right),2T\Big/\chi^2\left(2r;1-\frac{\alpha}{2}\right)\right] \tag{5-35}$$

式中 $\chi^2\left(2r;\frac{\alpha}{2}\right)$和 $\chi^2\left(2r;1-\frac{\alpha}{2}\right)$为自由度为 $2r$ 时的χ^2 分布；

$$T=\sum_{i=1}^{r} t_i+(n-r)\tau \tag{5-36}$$

在完整试验时，可将式 (5-36) 中的 r 用 n 代替。

【例 5-4】　已知某种元件的故障时间分布服从指数分布。随机地拿出 15 个试件进行故障试验。规定当故障数达到 5 时即停止试验，得到的故障时间分别为 1410，1872，3138，4218，6971 小时。根据公式（5-36）可算得：

$$T = \sum_{i=1}^{r} t_i + (n - r)\tau =$$
$$(1410 + 1872 + 3138 + 4218 + 6971) + (15 - 5) \times 6971 = 87319 \text{ (h)}$$

再由式（5-34）可算得平均故障时间 θ 的估计值为 $\theta = 17464$ (h)。设置信度为 95%，根据公式（5-35）算得平均故障时间 θ 的置信区间为［8526，5386.7］(h)。

5.3.2　韦伯分布的参数估计

为了较方便地求解韦伯分布时可靠度公式 $R(t) = \exp(-t^m/\eta)$ 中的两个参数 m 和 η，对等式两边取倒数，然后再取两次对数，可得到如下方程：

$$\ln\ln[1/R(t)] = m\ln t - \ln\eta$$

分别令 $Y = \ln\ln[1/R(t)]$；$X = m\ln t$；$B = -\ln\eta$。得到形如下式的直线方程：

$$Y = mX + B \tag{5-37}$$

利用专用的对数坐标纸可以方便地求出分布函数 m 和 η 的估计值 $\hat{m}$ 和 η。求出 $\hat{m}$ 和 η 后，分别应用前面的式（5-17）和式（5-18）计算出平均故障时间 θ（即数学期望）的估计值 θ 和方差值 σ 的估计值 σ。

【例 5-5】　取某种元件 15 个进行故障试验，试验中有 10 个发生了故障，故障时间分别为 190，360，610，800，1100，1340，1570，1790，2240 小时，求分布参数 m、η 和平均故障时间 θ（即数学期望）的估计值 θ。

首先，应用下式求出与各试件故障时间相对应的可靠度，即：

$$R(t) = \frac{\text{没有发生故障的元件数}}{\text{元件总数}} \tag{5-38}$$

在试验元件总数不足 20 个时，用下式计算，即：

$$R(t) = \frac{\text{没有发生故障的元件数}}{\text{元件总数} + 1} \tag{5-39}$$

然后，应用式 $F(t) = 1 - R(t)$ 求出故障发生概率。将上述计算结果分别列于表 5-2 之中。

表 5-2　试验元件的故障时间、可靠度、故障发生概率统计

故障时间　$t\times10^2$，h	1.90	3.60	6.10	8.00	8.50	11.00	13.40	15.70	17.90	22.40
可靠度　R (t)，%	93.7	87.5	81.2	75.0	68.7	62.5	56.2	50.0	43.7	37.5
故障概率 F (t)，%	6.3	12.5	18.8	25.0	31.3	37.5	43.8	50.0	56.3	62.5

将表中数据标在如图 5-4 所示的韦伯概率纸上，可从概率纸上直观地拟合出一条直线。直线与 y 轴的交点 N 的纵坐标应为 $B=-\ln\eta=-3.5$。过点(1，0)作一条与拟合直线相平行的辅助线，该辅助线与 y 轴的交点 M 的纵坐标即为直线的斜率，即：$m=-1.2$。

所以，计算参数 η 的估计值可得：

$$\eta=e^{-B}\times10^{-2m}=8318\ (h)$$

计算平均故障时间 θ (即数学期望) 的估计值可得：

$$\theta=\eta^{\frac{1}{m}}\Gamma\left(1+\frac{1}{m}\right)=1848\times0.939=1735\ (h)$$

计算均方差估计值可得：

$$\sigma=\eta^{\frac{1}{m}}\left\{\Gamma\left(1+\frac{1}{m}\right)-\left[\Gamma\left(1+\frac{1}{m}\right)\right]^2\right\}^{\frac{1}{2}}=1848\times0.78=1441\ (h)$$

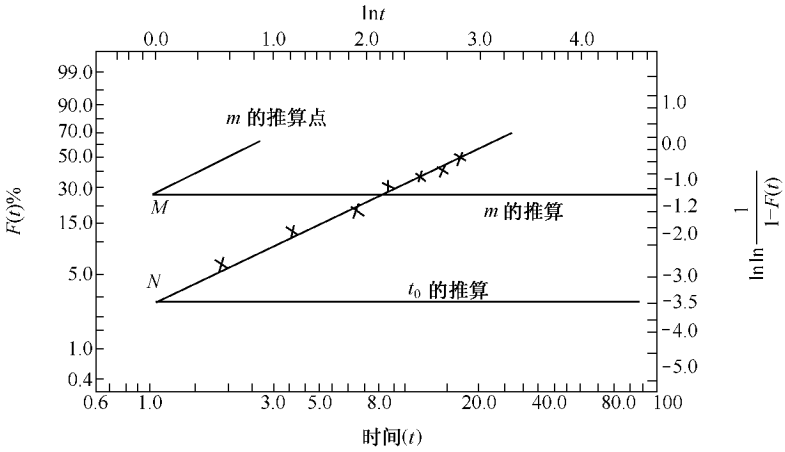


图 5-4　韦伯概率纸求解分布参数

5.3.3　可靠度估计 (非参数估计)

可靠度估计 (非参数估计) 是指当故障时间分布函数形式未知时，直接应

用故障数据推断可靠度和故障发生概率的估算方法。

假定故障时间分布函数 $F(t)$ 在 $[0,1]$ 区间上是均匀分布的，按下述方法估算可靠度和故障发生概率。

(1) 可靠度的点估算

如果用 n 个试件试验到 τ 时刻，有 r 个试件出现故障，其可靠度的点估算值和故障发生概率的点估算值分别按下两式计算：

$$R(\tau) = \frac{n-r}{n} \tag{5-40}$$

$$F(\tau) = 1 - R(\tau) = \frac{r}{n} \tag{5-41}$$

(2) 可靠度区间估算

在定数截尾试验的场合，可靠度的置信度上、下限分别按下列两式估算：

$$R_{上} = 1\Big/\left[1 + \left(\frac{r}{n-r+1}\right) F^{2r}_{2(n-r+1)}\left(1-\frac{\alpha}{2}\right)\right] \tag{5-42}$$

$$R_{下} = 1\Big/\left[1 + \left(\frac{r}{n-r+1}\right) F^{2r}_{2(n-r+1)}\left(\frac{\alpha}{2}\right)\right] \tag{5-43}$$

式中 $F^{2r}_{2(n-r+1)}\left(1-\frac{\alpha}{2}\right)$ 和 $F^{2r}_{2(n-r+1)}\left(\frac{\alpha}{2}\right)$ 为 F 分布，可查有关的表格得到。

5.4 简单系统的可靠性

系统可靠性与构成系统各元素的可靠性具有直接关系。根据构成系统的各元素之间的功能关系，可以把系统划分为简单系统和复杂系统；根据构成系统元素故障与系统故障得到关系，又分为串联系统 (基本系统) 和冗余系统。

串联系统是指系统中任何一个元素出现故障都会导致系统故障的系统，如环环相接的链条系统等。

冗余系统是指系统中的某个 (某些) 元素虽然发生故障也不足以造成系统故障的系统，如并联供水系统等。

冗余方法是指把若干元素或手段附加于系统的元素或组成部分上，即使系统元素或组成部分发生故障也不会造成系统故障的方法。也就是说，从系统功能的角度添加一些看上去似乎多余的东西来提高系统的可靠性，当系统某些元素或组成部分发生故障时起作用，使系统正常运行。冗余方式很多，常见的有以下几种：

(1) 并联冗余方式

并联冗余时附加的元素与原来的元素同时工作，增加系统的可靠性，如元器件的并联。

⑵ 备用冗余方式

备用冗余时元素通常处于备用状态，只有当原来的元素发生故障时才投入工作，保证系统正常运行。按备用的冗余元素所处的状态把备用冗余分为三种：

1) 冷备用：备用元素在完全不工作状态下备用，处于冷备用的元素其故障概率为 0。此时的冗余备用系统称为冷备用系统。

2) 热备用：备用元素与主要元素完全同样地运行，一旦主要元素发生故障则备用元素立即取代它。此时的冗余备用系统称为热备用系统。

3) 温备用：处于冷备用和热备用中间的备用状态。此时的冗余备用系统成为温备用系统。

⑶ 表决冗余方式

表决冗余方式又称 n 中取 k 冗余方式，组成系统的 n 个元素中至少有 k 个正常就能保证系统正常工作。换言之，n 个元素中只有 n - k + 1 或更多个元素故障时系统才出现故障。表决冗余方式多用于在提高安全监控系统的可靠性方面。

在实现冗余时，可以采取附加元素的方法 (元素冗余)，也可以附加系统 (系统冗余)。但是，理论和实践都已经证明，元素冗余比系统冗余效果更好。

5.4.1 简单系统可靠性分析

⑴ 串联系统的可靠性

串联系统是组成系统的元素在实现系统功能方面缺一不可的系统，因此又称作基本系统。这类系统的基本特征是，组成系统的任一元素发生故障都会导致系统故障。系统故障时间 t_s 与元素故障时间 t_1，t_2，…，t_n 之间有如下关系：

$$t_s = \min\ (t_1,\ t_2,\ \cdots,\ t_n) \tag{5-44}$$

即，系统故障时间等于最先发生故障元素的故障时间。

当串联系统的各元素的故障时间相互统计独立时，统计可靠度 R_s (t) 与元素可靠度 R_i (t) 间有如下关系：

$$R_s(t) = \prod_{i=1}^{n} R_i(t) \tag{5-45}$$

同样，系统发生故障概率 F_s (t) 与元素发生故障概率 F_i (t) 之间具有如下关系：

$$F_s(t) = 1 - \prod_{i=1}^{n} [1 - F_i(t)] \tag{5-46}$$

而串联系统的故障率 λ_s (t) 等于各元素故障率 λ_i (t) 之和，即：

$$\lambda_s(t) = \sum_{i=1}^{n} \lambda_i(t) \tag{5-47}$$

很显然，串联系统的平均故障时间 θ_s 必定小于系统中任一元素的平均故障时间 θ_i，并且串联的元素越多越易于发生故障。

(2) 并联系统的可靠性

并联系统是一种常用的冗余系统。其基本特征是，只有组成并联系统的所有元素都发生故障时系统才发生故障。并联系统的故障时间、可靠度、故障概率与元素的故障时间、可靠度和故障概率之间的关系都与串联系统相反，即：

$$t_s = \max\ [t_1, t_2, \cdots, t_n] \tag{5-48}$$

$$R_s(t) = 1 - \prod_{i=1}^{n} [1 - R_i(t)] \tag{5-49}$$

$$F_s(t) = \prod_{i=1}^{n} F_i(t) \tag{5-50}$$

并联系统的故障率与元素的故障率之间的关系较为复杂，很难明确表达，只能根据具体的情况来求解。

一般来说，并联系统随着组成系统元素的增加，系统的平均故障时间也增加，系统的可靠性提高。但是考虑到可靠度的增加幅度、成本和体积等因素，并联系统的元素也不易过多。

(3) 表决系统的可靠性

类似于表决冗余方式，表决系统是指组成系统的 n 个元素中至少有 k 个元素正常时才能保证系统正常运行的系统。串联系统可视为 $k = n$ 的表决系统，即为 n 中取 n 系统；并联系统可视为 $k = 1$ 的表决系统，即为 n 中取 1 系统。

通常，表决系统的可靠度、故障概率、故障率和平均故障时间与元素的可靠度、故障概率、故障率和平均故障时间的关系随所服从的分布形式的不同有不同的形式，较为复杂。

一般来说，表决系统的平均故障时间小于元素的平均故障时间；表决系统的故障概率介于串联系统和并联系统之间。当元素故障概率较高时，表决系统的故障概率接近于串联系统的故障概率；当元素故障概率较低时，表决系统的故障概率接近于并联系统的故障概率。

(4) 备用系统的可靠性

备用系统是一个主要工作元素和若干个备用元素组成的冗余系统。备用系统工作时一旦主要元素发生故障转换机构则将备用元素投入运行。除了元素故障之外，转换机构故障也会导致系统故障。为简单起见，这里仅讨论主要元素故障时转换机构能够可靠地把备用元素投入运行的理想情况。

1）冷备用系统

若冷备用系统由相同的一个主要元素和 n 个备用元素组成，设各元素的故障率为 λ_0。当故障时间为指数分布时，系统可靠度 $R_s(t)$ 应为：

$$R_s(t) = \sum_{k=0}^{n} \frac{(\lambda_0 t)^k}{k!} e^{-\lambda_0 t} \tag{5-51}$$

冷备用系统的平均故障时间 θ_s 与元素平均故障时间 θ_0 之间关系应为：

$$\theta_s = (n+1)\theta_0 \tag{5-52}$$

2）温备用系统

温备用系统的备用元素在备用期间也处于备用状态，但是备用期间的运行状态和替代主要元素的工作期间的运行状态又不相同，于是，备用元素的故障率可能随着运行状态发生变化。在研究系统故障问题时，温备用系统比冷备用系统复杂得多。

这里仅讨论两个独立元素组成的温备用系统，其中，一个为主要元素，另一个为备用元素。设两个元素的故障时间均服从指数分布，主要元素的故障率为 λ_1；备用元素在备用状态下的故障率为 λ_0，其工作状态下的故障率为 λ_2。则系统可靠度 $R_s(t)$ 应为：

$$R_s(t) = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_2 + \lambda_3}\left[e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_0)t} \right] \tag{5-53}$$

此时，温备用系统平均故障时间应为：

$$\theta_s = \frac{1}{\lambda_1} + \frac{\lambda_1}{\lambda_2(\lambda_1+\lambda_0)} \tag{5-54}$$

5.4.2 可维修系统的可靠性

维修是指系统发生故障后，从诊断故障的部位开始，进行一系列的修理，使系统恢复正常运行的过程。通常，系统运行一段时间后会发生故障，必须经过维修后才能恢复正常运行。

系统的可维修性是指在规定条件下，规定的时间内，按规定的方式维修时可使系统恢复正常运行的可能性。它包括维修度、维修率、平均维修时间和维修可用度等量化指标。

维修度 $M(t)$ 是指可维修系统在规定的条件下，在规定的时间内可以完成维修工作的概率，它是时间的函数。

维修率 $\mu(t)$ 是指维修工作进行到一定时刻之后的单位时间里可以完成维修工作的比率，它也是时间的函数。

维修度和维修率两者之间的关系为：

$$M(t) = 1 - e^{-\int_0^t \mu(t)\,dt} \tag{5-55}$$

维修度的概率密度函数应为：

$$m(t) = \frac{dM(t)}{dt} \tag{5-56}$$

在不考虑维修率随时间变化时，维修率为常量。此时的系统维修度和系统维修概率密度应分别为：

$$M(t) = 1 - e^{-\mu t} \tag{5-57}$$

$$m(t) = \mu e^{-\mu t} \tag{5-58}$$

平均维修时间 MTTR 是指当维修率为常数，维修度随时间呈指数分布时，维修率的倒数，即：

$$MTTR = 1/\mu \tag{5-59}$$

可用度分为瞬时可用度 $A(t)$ 和稳态可用度 $A(\ )$。瞬时可用度 $A(t)$ 是指系统在特定的瞬间能维持正常功能的概率；稳态可用度 $A(\ )$ 是当 $t\rightarrow\ $ 时的可用度。瞬时可用度 $A(t)$ 和稳态可用度 $A(\ )$ 分别与系统的故障率 λ 和系统的维修率 μ 有如下关系：

$$A(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda e^{-(\mu+\lambda)t}}{\mu + \lambda} \tag{5-60}$$

$$A(\ ) = \frac{\mu}{\mu + \lambda} \tag{5-61}$$

5.5 提高系统可靠性的途径

提高元素、设备和系统的可靠性，降低故障率是控制危险防止事故发生的重要工作内容。系统、设备、元件故障的发生，既有其自身的原因，也有外部原因。前者来自设计制造安装等方面的问题，后者包括工作条件方面的问题和时间因素。因此，应该从这些方面的问题入手采取措施提高系统、设备、元素的可靠性。

5.5.1 提高设计可靠性

良好的工程设计是防止故障的一种有效措施，在设计实践中经常采取安全系数、降低额定值、冗余设计、故障-安全设计、耐故障设计、选用高质量的材料、元件、部件等措施，提高系统、设备、元件的可靠性。

(1) 设置安全系数

在设计中设置安全系数是防止机械零部件、建筑结构、岩土工程结构等发生故障的常用方法。设置安全系数的基本思想是，把结构、部件的强度，设计得超出其可能承受的能力的若干倍，这样就可以减少因设计计算误差、制造缺陷、材料老化以及未知因素等造成的破坏或故障。

一般地，安全系数越大，结构部件的可靠性越高，故障率越低。但是，安全系数的增大可能增加结构、部件尺寸，增加成本。合理的确定结构、部件的安全系数是一个很值得研究的问题，大多数情况下主要是根据经验选取。通常，对于一旦发生故障可能导致事故、造成严重后果的结构、部件应选用较大的安全系数。如，汽车、飞机的发动机曲轴的安全系数要达到 40 以上。

⑵ 降低许用值

与设置安全系数方法相类似，在电器电子设备和元件的设计中采用降低许用值的方法，防止故障产生。其具体做法是，选用其功率远大于要求功率的设备或元件，或者采取冷却措施提高设备或元件的承载能力。例如，重要的警告信号灯用低于额定电压的电压供电，以减少故障、增加寿命。

⑶ 采用冗余设计

设计中采用冗余的方式构成冗余系统可以大大提高可靠性，减少故障的发生。在各种冗余方式中，并联冗余和备用冗余最为常用。

当采用并联冗余时，冗余元素与原有元素同时工作，冗余元素越多则可靠性越高。但是，由于并联元素的数量达到一定程度时，并联上去的元素越多所起的作用将越小；同时考虑到体积和成本的限制，实际设计中通常只需把有限的元素并联起来构成冗余系统即可。

在采用备用冗余的原理是，当工作元素发生故障时备用元素接替工作。这一冗余系统增加了平均故障时间，可大大减少系统故障。许多重要的设施设备都采用备用冗余方式，如备用电源、备用电机、备用轮胎等。在设计备用冗余系统时，应该注意备用元素投入工作时转换机构的可靠性问题。如果转换机构发生故障，则在工作元素故障时不能及时将备用元素投入运行，最终也将导致系统故障。

⑷ 故障-安全设计

故障-安全设计是指在系统设备结构的一部分发生故障或破坏的一定时间内，系统能保证安全运行的设计。按系统设备结构在其一部分发生故障后所处的状态不同可有三种方案：

1) 故障-正常方案。系统设备结构在其一部分发生故障后，在采取措施前仍能发挥正常功能。例如，计算机、服务器等应用的 UPS 电源。

2) 故障-消极方案。系统设备结构在其一部分发生故障后，处于最低的能量状态，在采取措施之前不能工作。例如，电路中的保险丝、断电保护器等在过载时熔断或掉闸而断开电路；列车制动系统故障时闸瓦抱紧车轮时列车停止等。

3) 故障-积极方案。故障发生后，在采取措施之前，系统设备结构处于安全的能量状态下，或者维持其基本功能，但是性能（包括可靠性）下降。例

如，在结构设计中将 T 型钢用两根角钢代替，形成分割结构，如果其中一根角钢损坏，另一根角钢仍能承担载荷而不致发生事故。故障-积极方案又称为故障 - 缓和方案，在实际设计中应用较为广泛。

⑸ 耐故障设计

耐故障设计又称容错设计，是指系统中的设备结构在其一部分发生故障或破坏的情况下仍能维持其功能的设计。可以认为耐故障设计是故障-安全设计的一种。耐故障设计方法在防止故障方面得到了广泛应用。如在飞机的结构设计中，为防止疲劳断裂而采用耐破坏设计，即使结构上产生了裂纹，其剩余的强度也足以保证飞机能安全返回地面。

随着计算机在系统控制中的普及，由于计算机软件发生故障而引起的事故越来越受到重视。耐故障设计是防止计算机软件故障的重要措施之一。常用的方法是由两个不同版本的软件同时运行，如果运行结果相同则有效，否则将发出警告。

⑹ 选用高质量的材料、元件和部件

系统、设备、结构是由若干元素、元件和部件组成的。由可靠性高的元素组成的系统，其可靠性也高。选用高质量的材料、元件、部件，可以保证系统元素有较高的可靠性。为此，一些重要的元件、部件要经过严格的筛选后才能使用。

5.5.2 提高系统维修效果

维修是指为了维持或恢复系统、设备、结构正常状态而进行的工作，如保养、检查、故障识别、更换或修理等。

维修可按其与故障发生的时间关系，分为预防性维修和修复性维修两大类。前者是在故障发生之前进行，后者是在故障发生之后进行。

⑴ 预防性维修

预防性维修是指依据平均故障时间等一些可靠性参数确定维修的周期，按预先规定的维修内容有计划地进行维修。工业企业中开展的设备大、中、小维修，均属于预防性维修。一般来说，随着工作时间的增加，系统的可靠性逐渐降低。在进入磨损故障阶段之前进行维修，可以有效地降低故障发生率。

⑵ 修复性维修

修复性维修是指系统、设备、结构发生故障后，查找故障部位，隔离故障更换，修理故障元素，以及校准、校验等，使之尽快恢复正常状态。

为了保证安全，防止可能导致事故的故障发生，做到防患于未然，维修工作应该以预防性维修为主，修复性维修为辅。在预防性维修中，通常有定时维修、按需维修和检测维修等工作方式。

1）定时维修

以平均故障时间为周期进行的周期性维修。这种维修工作方式便于安排维修计划，但是针对性较差、维修工作量大而不经济。

2）按需维修

根据系统、设备、结构的状况决定是否维修。按需维修在定时检查的基础上进行，既可消除潜在故障又可以减少维修工作量，充分利用元素的工作寿命，是一种较好的维修方式。

3）监测维修

在广泛收集、分析元素故障资料的基础上，根据对其运行情况连续监测的结果确定维修时间和内容。它是按需维修的深化和发展，既可以提高系统设备结构的可用度，减少维修工作量，又能发挥元素潜力，是一种理想的预防性维修方式。监测维修设计的故障分析诊断技术、系统状态监测技术，特别适用于随机故障和规律不清楚的故障预防。

5.5.3 提高安全监控系统可靠性

在生产过程中经常利用安全监控系统、监测系统的安全状态参数，以便及时发现问题采取措施，控制这些参数不达到危险水平，以防事故发生。

（1）安全监控系统的种类

安全监控系统种类繁多，图 5-5 是典型的生产过程安全监控系统示意图。图中虚线内的部分是安全监控系统，它由检知、判断和驱动三部分组成。

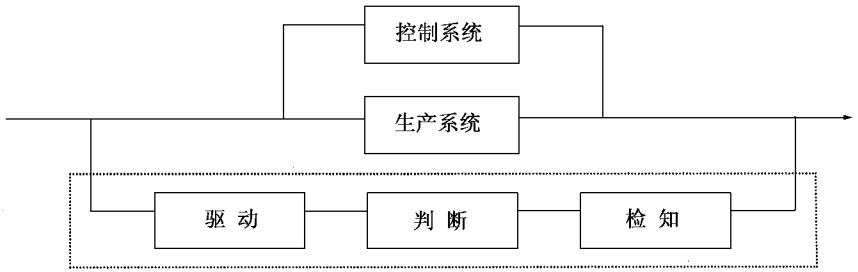


图 5-5 典型的安全监控系统

1）检知部分主要是由传感元件组成，用以感知所监测物理量的变化情况。通常，传感元件的灵敏程度要比人的感觉器官高得多，能够发现人员难以直接觉察的潜在的变化。

2）判断部分是把检知部分获得的物理量参数值与预先设定的值相比较，判断被监控对象的状态是否正常。

3）驱动部分的功能是在判断部分已经判明存在故障、异常，有可能出现危险时，采取适当的安全措施，如停止运转、启动安全装置、发出警告等，让工作人员采取紧急处理措施或及时回避危险。

（2）安全监控系统的形式

安全监控系统基本上有以下三种形式：

1）检测仪表。在此种系统中，只有检知部分的工作是由仪器、设备等来完成的。而将监测到的参数值与预先设定的数值相比较，判断监控对象是否处于正常状态，采取必要的处理措施都是由工作人员来完成的。

2）报警系统。在此种系统中，检知部分和判断部分的工作均由仪器、设备等来完成。驱动部分的功能由工作人员完成。系统检测到异常时发出声、光报警信号，提醒工作人员采取必要的措施。此时，把判定标准的参数值预先设定得低些，可以保证工作人员有充裕的时间做出恰当的决策并采取正确的行动。

3）联锁系统。在此种系统中，检知、判断和驱动部分的工作均由仪器、设备等来完成。当检知部分监测到的数据，经判断部分发现异常时，驱动部分自动采取措施，不必工作人员介入。这是一种高度的自动化系统，适用于短时间内可能发生事故，造成严重后果的情况。

（3）影响安全监控系统可靠性的原因

影响到安全监控系统可靠性原因主要有以下两方面：

1）漏报

漏报是当监测对象出现异常时，安全监控系统没有做出人们所希望的正确的反应（例如报警、紧急停车等）。漏报故障的出现使安全监控系统丧失安全功能，不能阻止事故的发生，其结果可能带来巨大损失。因此，漏报故障属于“危险故障”型故障。

为了防止漏报故障的发生，应该选用高灵敏的传感元件，预先设定较低的标准参照值，确保驱动机构动作可靠。

2）误报

误报是当监测对象没有出现异常时，安全监控系统出现的人们所不希望的错误反应（例如误报警、误停车等）。由于误报不会导致事故发生，故它属于“安全故障”型故障。但是，误报可能带来不必要的生产停顿或经济损失，严重时会使人们产生麻痹思想，不重视安全监控系统，酿成重大事故。为了防止系统的误报发生，安全监控系统应具有较强的抗干扰能力。

经验表明，安全监控系统的三个组成部分中，检知部分发生故障的频率最高。安全监控系统的漏报和误报是性质完全相反的两种类型的故障。提高检知部分的灵敏度虽然可以防止漏报型故障，却容易受外界干扰而产生误报型故

障；反之，抗干扰能力强时虽然可以防止误报型故障，却容易发生漏报型故障。因此，提高安全监控系统可靠性是一件困难且又十分重要的工作，不能忽视。

目前，主要通过两条途径改善安全监控系统（特别是检知部分）的可靠性：

1）选用既有较高灵敏度又有较强抗干扰能力的高性能传感元件；

2）改进系统设计，采用多传感元件系统。

通常情况，采用表决系统既可以提高防止漏报型故障性能，又可以提高防止误报型故障的性能，可以有效地提高安全监控系统的可靠性。

思　考　题

1. 何谓可靠性？何谓可靠度？
2. 何谓故障？故障有几种类型？何谓故障率？
3. 何谓冗余系统？有几种方式？
4. 何谓温备用系统？何谓冷备用系统？两者有何区别？
5. 何谓维修率？维修度？可用度？
6. 用 9 个试件对某产品进行定数截尾实验，截尾试验 $r = 7$，观察到的故障时间分别为 150，450，500，590，600，650，700 小时，试估计平均故障时间。
7. 针对一个你比较熟悉的系统提出改善可靠度的方法。

6　事故树分析

6.1　事故树的概念及分析步骤

事故树（或称故障树）分析（Fault Tree Analysis，简称 FTA）是在系统安全工程中广泛应用的重要的安全分析方法之一。“树”的分析技术属于系统工程的图论范畴。是一个无圈的连通图。事故树则是一种利用布尔逻辑关系从结果到原因表示事故发生过程的逻辑树图。

事故树分析方法可形象明了地反映出事故发生的因果关系。它既可以用于事故后的原因分析，又可以用于系统危险性评价与辨识；既可以用于定性分析，也可以用于定量分析。由于这种分析方法具有形象直观、思路清晰、逻辑性强等特点，因而得到了广泛的应用。

6.1.1　事故树结构及符号意义

⑴ 事故树的基本结构

事故树的基本结构如图 6-1 所示。在事故树中，各事件之间的基本关系是因果逻辑关系，通常用逻辑门来表示。树中以逻辑门为中心，其上层事件是下层事件发生后所导致的结果，称为输出事件；下层事件是上层事件的原因，称为输入事件。

所要研究的特定事故被绘制在事故树的顶端，称为顶上事件，如图 6-1 中 T 表示的事件。导致顶上事件发生的最初的原因事件绘制于事故树下部的各分支的终端，称为基本事件，如图 6-1 中 x_1，x_2，x_3，x_4，x_5，x_6 所表示的事件。处于顶上事件和基本事件中间的事件称为中间事件，它们既

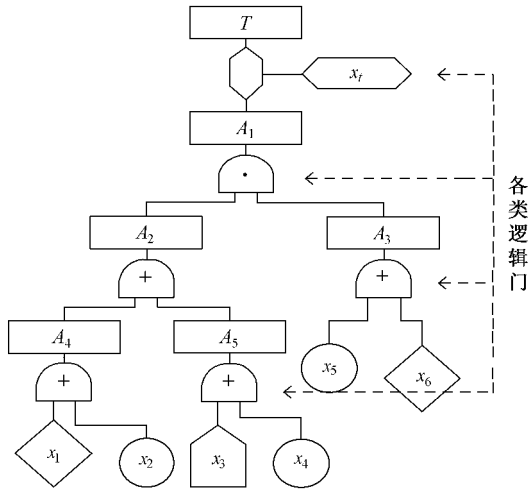


图 6-1　事故树基本结构

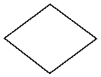
是造成顶上事件的原因，又是由基本事件产生的结果，如图 6-1 中 A_1，A_2，A_3，A_4，A_5 所表示的事件。

⑵ 事故树的符号及其意义

1) 事件符号及意义

矩形符号。表示需要进一步分析的事件,如顶上事件和中间事件。

圆形符号。表示不能再往下分的基本事件。



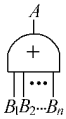
菱形符号。表示目前不能分析或不必要分析的事件，按基本事件处理。

房形符号。表示正常事件，即对输出事件的出现必不可少的事件，按基本事件处理。

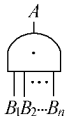
转入符号。表示在别处的部分内容由该处转入 (在符号内标明从何处转入)。

转出符号。表示在此处的部分内容转移到别处 (在符号内标明转移到何处)。

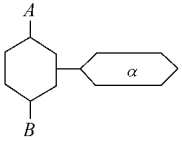
2) 逻辑门符号及意义



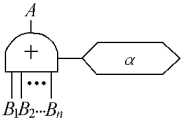
逻辑或门符号。表示 B_1、B_2、…、B_n 中任何一个事件单独发生 (输入) 时，A 事件都可以发生 (输出)。其数学表达形式为：$A = B_1 + B_2 + \cdots + B_n$。



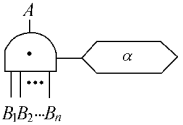
逻辑与门符号。表示 B_1、B_2、…、B_n 之中的事件同时发生 (输入) 时，A 事件才可以发生 (输出)。其数学表达形式为：$A = B_1 \cdot B_2 \cdot \cdots \cdot B_n$。



控制门符号。表示 B 事件发生 (输入) 时，必须满足 α 的条件，A 事件才可以发生 (输出)。其数学表达形式为：$A = B \cdot \alpha$。



条件或门符号。表示 B_1、B_2、…、B_n 中的事件同时发生 (输入) 时,还必须满足 α 的条件,A 事件才可以发生 (输出)。其数学表达形式为：$A = (B_1 + B_2 + \cdots + B_n) \cdot \alpha$。



条件与门符号。表示 B_1、B_2、…、B_n 中任何一个事件单独发生 (输入) 时,还必须满足 α 的条件,A 事件才可以发生 (输出)。其数学表达形式为：$A = (B_1 \cdot B_2 \cdot \cdots \cdot B_n) \cdot \alpha$

(3) 事故树分析法的分析步骤

事故树分析是对所研究系统发生事故的条件、可能导致的灾害性后果，按因果逻辑关系的先后顺序绘制成的分析程序的树状图，它表示了事故与各种事件之间的逻辑关系。事故树分析的基本步骤如下。

1) 熟悉系统

详细了解分析所研究系统的工作状态、工艺过程、运行参数、作业情况以及环境影响程度。

2) 调查事故

广泛收集同类系统的事故资料，进行事故统计，预测所研究系统可能发生的事故。

3) 确定顶上事件

对所要着重研究的事故进行全面的分析，分析它们的损失程度和发生的概率，找出后果严重且易于发生的事故作为顶上事件。

4) 确定顶上事件的控制目标

根据以往事故经验和同类事故的资料，进行统计分析，求出该事故的概率(或频率)。根据这类事故的发生概率及严重程度，确定其发生概率的控制目标。

5) 原因事件调查

从人、机、环境和管理等方面，全面分析、调查与顶上事件 (事故) 有关的原因事件和因素，作为基本事件。

6) 绘制事故树

从顶上事故开始，通过分析逐级找出直接原因事件，按其因果逻辑关系，用逻辑门将上下层事件连接起来，绘出事故树图。

7) 定性分析

运用布尔代数数学工具，对事故树进行简化，求出最小割集和最小径集，确定各基本事件的结构重要度。

8) 求顶上事件 (事故) 的发生概率

确定出所有原因事件 (基本事件) 的发生概率，并利用其求出顶上事件(事故) 的发生概率。

9) 分析比较

将求得的顶上事件发生概率与通常统计分析所得到的概率进行比较。如果两者相互矛盾，需返回到 5)，查看基本事件有无遗漏，逻辑关系是否正确以及所拟订的基本事件发生概率是否合适等。

10) 定量分析

当求得的顶上事件发生概率超过预定目标时，应该从最小割集入手，研究

降低事故概率的各种可能，从中选出最优方案。

原则上列出了事故树分析的十大步骤。由于具体情况不同，有时只需完成其中的若干步骤，就可以达到要求。围绕上述 10 条内容，可根据具体情况灵活运用。

6.1.2 事故树的数学表达

为了对事故树进行详细的分析，在编制出事故树模型后，还要利用波尔代数列出它的数学表达式。布尔代数是完成事故树分析的数学基础。

(1) 布尔代数

布尔代数是集合论数学的组成部分，是一种逻辑运算方法，也称为逻辑代数。布尔代数特别适用于描述只能取两种对立状态的事物变化过程。这正适合于事故树分析的特点。

在布尔代数中，与集合的“并”（即为“∪”）的运算相对应的是逻辑“加”的运算，通常，记为“+”，也称为逻辑“或”；同样，与集合“交”（记为“∩”）的运算对应的是逻辑“乘”的运算，通常，记为“·”，也称为逻辑“与”。

布尔代数的主要运算法则如下：

1) 结合律

$$(a + b) + c = a + (b + c)$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

2) 交换律

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

3) 分配律

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

4) 等幂律

$$a + a = a$$
$$a \cdot a = a$$

5) 互补律

对于元素 a 存在着它的补元素 $\bar{a}$，那么有下述互补律成立。

$$a + \bar{a} = 1$$
$$a \cdot \bar{a} = 0$$

6) 吸收律

$$a + (a \cdot b) = a$$

$$a \cdot (a + b) = a$$

7）对合律

$$\overline{(a)} = a$$

8）对偶律（德·摩根律）

$$\overline{a \cdot b} = \overline{a} + \overline{b}$$
$$\overline{a + b} = \overline{a} \cdot \overline{b}$$

9）重叠律

$$a + b = \overline{a} \cdot b + a$$
$$\overline{a} + \overline{b} = \overline{a} + a \cdot \overline{b}$$

10）存在着元素 0 和 1

则有

$$a + 0 = 0 + a = a$$
$$a \cdot 1 = 1 \cdot a = a$$

（2）事故树的布尔代数表达式

将事故树中连接各事件的逻辑门用相应的布尔代数运算表示，就得到了事故树的布尔代数表达式。

通常，可以自上而下地将事故树逐渐展开后，便得到了布尔表达式。以图 6-1 的事故树为例，其布尔代数表达式及展开过程如下。

$$\begin{aligned} T &= A_1 \cdot x_t = A_2 \cdot A_3 \cdot x_t \\ &= (A_4 + A_5) \cdot (x_5 + x_6) \cdot x_t \\ &= (x_1 + x_2 + x_3 + x_4) \cdot (x_5 + x_6) \cdot x_t \end{aligned}$$

此式还可以继续化简至若干基本事件相“乘”后再相“加”的形式。故障树的布尔代数表达式是事故树的数学描述。对于给出的事故树可以写出相应的布尔代数表达式；相反，给出了布尔代数表达式就可以绘出相应的事故。

（3）事故树的概率函数

事故树的概率函数是指事故树中由基本事件概率所组成的顶上事件概率的计算式。由于每个事故树的结构形式不同，其概率函数（概率计算式）有所不同。

如果，事故树中的基本事件是相互统计独立的，布尔代数表达式中各基本事件逻辑“乘”的概率应为：

$$g(x_1 \cdot x_2 \cdot \cdots \cdot x_n) = q_1 \cdot q_2 \cdot \cdots \cdot q_n = \prod_{i=1}^{n} q_i \qquad (6\text{-}1)$$

各基本事件的逻辑“加”的概率应为：

$$g(x_1 + x_2 + \cdots + x_n) = 1 - (1 - q_1) \cdot (1 - q_2) \cdot \cdots \cdot (1 - q_n) = \prod_{i=1}^{n} (1 - q_i) \qquad (6\text{-}2)$$

式中 q_i ——第 i 个基本事件的发生概率；

$\prod$ ——数学运算符号，求概率积。

利用上述式 (6-1) 和式 (6-2)，求图 6-1 事故树的概率函数，如下式：

$$g(q) = \left[1 - \prod_{i=1}^{4}(1 - q_i)\right] \cdot \left[1 - \prod_{i=5}^{6}(1 - q_i)\right] \cdot q_t$$

式中 q_t ——控制门事件的发生概率。

如果知道了每个基本事件的发生概率，就可计算出顶上事件的发生概率。

(4) 事故树的简化及意义

事故树的简化是应用布尔代数的运算法则来完成的。经简化后的事故树的布尔代数表达式可以除去由于编制事故树时，写入的无关事件。每当事故树形成后都必须对其进行化简，去掉多余的事件，否则将造成分析结果错误。下面的例子给出了某事故树的布尔代数表达式的简化过程。

$$T = x_1 \cdot x_2 \cdot (x_1 + x_3) \qquad \text{(未经简化形式)}$$

$$= x_1 \cdot x_2 \cdot x_1 + x_1 \cdot x_2 \cdot x_3 \qquad \text{(应用分配律展开)}$$

$$= x_1 \cdot x_2 + x_1 \cdot x_2 \cdot x_3 \qquad \text{(应用等幂律去掉多余的 } x_1\text{)}$$

$$= x_1 \cdot x_2 \qquad \text{(应用吸收律去掉多余的 } x_3\text{，达到最简形式)}$$

取事故树中的三个基本事件的发生概率 $q_1 = q_2 = q_3 = 0.1$。未经简化时，事故树的顶上事件的发生概率应为：

$$g(q) = q_1 \cdot q_2 \cdot [1 - (1 - q_1)(1 - q_3)]$$

$$= 0.1 \times 0.1 \times [1 - (1 - 0.1)(1 - 0.1)]$$

$$= 0.0019$$

简化后事故树顶上事件的发生概率应为：

$$g(q) = q_1 \cdot q_2 = 0.1 \times 0.1 = 0.01$$

从计算结果可知，两者相差甚远。由此可见，事故树的简化过程不仅大大减少了运算工作量，同时也避免了运算错误。

6.2 事故树的定性分析

事故树定性分析的目的是根据事故树的结构确定顶上事件的发生模式、起因以及影响程度，为采取有效的预防措施，防止事故发生提供依据。事故树定性分析时，除编制事故树，找出导致顶上事件发生的全部事件之外，还要求出事故树中基本事件的最小割集和最小径集，求出各基本事件的结构重要度，了解其对顶上事件的影响程度。

6.2.1 最小割集及其求法

(1) 最小割集的概念

如果事故树中的全部事件都发生，则顶上事件必然发生。但是，大多数情况下并不是一定要所有基本事件都发生，顶上事件才能发生，而是只要某些基本事件的一起发生就可以导致顶上事件的发生。这些由于同时发生就能够导致顶上事件发生的基本事件的组合称为割集。割集中的基本事件之间是逻辑“乘”(或称为“与”) 的关系。

最小割集是指能够引起顶上事件发生的最低数量的基本事件的组合。最小割集指明了哪些基本事件同时发生，就可以使顶上事件发生的事故模式。

(2) 最小割集的求解方法

1) 观察法

对于一些简单的事故树可以通过观察直接找出最小割集。例如，根据某事故树可得出如下 6 个割集。

(x_1, x_1)　(x_1, x_2)　(x_1, x_3)　(x_1, x_4)　(x_2, x_3)　(x_2, x_4)

应用布尔代数运算法则的等幂律、吸收律对其整理，可得到如下 3 个最小割集。

(x_1)　　(x_2, x_3)　　(x_2, x_4)

2) 布尔代数式化简法

对于一些相对简单的事故树可以利用布尔代数运算法则对布尔代数式进行化简求得最小割集。其求解过程如下面的例子所示。

$$T = A_1 \cdot A_2$$
$$= (x_1 + x_2) \cdot A_2$$
$$= (x_1 + x_2) \cdot (x_1 + x_3 + x_4) \quad \text{(根据逻辑关系展开各中间事件为基本事件)}$$
$$= x_1 \cdot x_1 + x_1 \cdot x_3 + x_1 \cdot x_4 + x_2 \cdot x_3 + x_2 \cdot x_4 \quad \text{(应用分配律进一步展开)}$$
$$= x_1 + x_2 \cdot x_3 + x_2 \cdot x_4 \quad \text{(应用等幂律和吸收律整理简化)}$$

根据逻辑“乘”(或称为“与”) 的关系得到 3 个最小割集为：

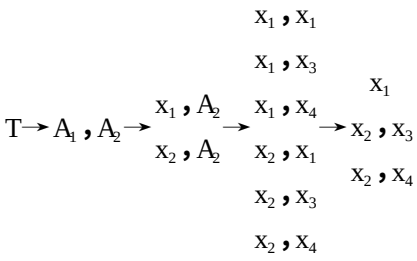
(x_1)　　(x_2, x_3)　　(x_2, x_4)

3) 行列法

对于一些复杂的事故树常用计算机求解最小割集。此式常用的方法为行列法 (又称为福赛尔法)。行列法的求解原理是：从顶上事件开始，按逻辑门顺序用下面的输入事件代替上面的输出事件，逐层展开，直到所有的基本事件全部列出为止。在代替展开过程中，“或”门连接的输入事件纵向列出，“与”门连接的输入事件横向列出，最终得到若干行基本事件组成的割集。对这些割集

应用布尔代数运算法则化简，便得到了所求的最小割集。

以前面的事故树布尔代数表达式为例：



最终得到的最小割集为：

(x_1)　　(x_2, x_3)　　(x_2, x_4)

⑶ 最小割集的作用

最小割集表示了事故树系统的危险性的大小。每个最小割集都是顶上事件发生的一种可能途径。最小割集的数目越多，危险性越大。归纳起来最小割集的作用有如下几种：

1) 表示顶上事件的发生原因。事故发生必然是某个最小割集中的基本事件同时发生的结果。求出事故树的全部最小割集，就可掌握事故发生的各种可能。

2) 每个最小割集代表了一种事故模式。可根据最小割集集合发现事故树系统中的最薄弱环节，判断出最危险的情况。同时，最小割集中的基本事件个数越少，其事故模式的危险性越大。

3) 判断重要度，计算顶上事件发生概率。可以根据最小割集判断基本事件的结构重要度。同时，可以利用其计算事故发生概率。

6.2.2 最小径集及其求法

⑴ 最小径集的概念

如果事故树的全部基本事件都不发生，则顶上事件就一定不会发生。但是，如果事故树中某些基本事件不同时发生，则也可以使得顶上事件不发生。这些不同时发生时，可以使顶上事件不发生的基本事件组合称为径集。

最小径集是指能够使得顶上事件不发生的最低数量的基本事件的组合。最小径集指明了哪些基本事件不同时发生，就可以使顶上事件不发生的安全模式。

⑵ 最小径集的求解

事故树的最小径集是利用布尔代数运算法则的对偶律求得的，其具体步骤是：

1）求解成功树

首先，将所研究的事故树中的事故事件用与其对立的非事故事件代替；其次，将逻辑“与”门用逻辑“或”门代替，逻辑“或”门用逻辑“与”门代替。这样便获得了与原事故树相对偶的成功树，如图 6-2 所示。

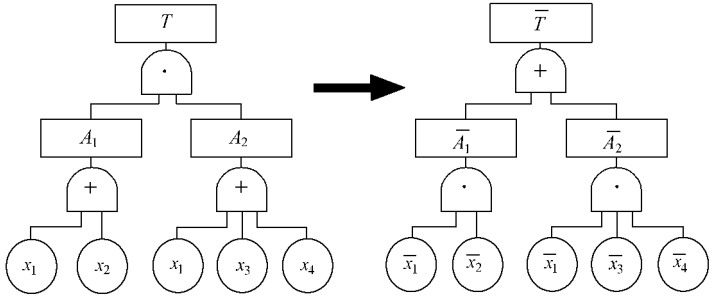


图 6-2　事故树变换为成功树

2）求解成功树的最小割集

求出上述成功树的最小割集为：

$(\overline{x}_1, \overline{x}_2)$　　$(\overline{x}_1, \overline{x}_3, \overline{x}_4)$

3）求解事故树的最小径集

再用事故事件代替成功树中最小割集的非事故事件，便可得到原事故树的最小径集。最后求得的最小径集如下：

(x_1, x_2)　　(x_1, x_3, x_4)

（3）最小径集的作用

1）表示事故树系统的安全性。事故树系统中的最小径集的数量越多，防止顶上事件发生的措施就越多，系统安全性越大。

2）可用于选择最佳的事故控制方案。一般来说，依据基本事件个数少的最小径集选用事故控制措施比依据基本事件个数多的最小径集选用事故控制措施更容易。

3）可以进行结构重要度分析。

6.2.3　基本事件的结构重要度

事故树分析中，导致顶上事件发生的基本事件有很多，而各自对顶上事件的影响程度是不相同的，在采取防止事故发生的措施时应该分出轻重缓急，首先消除或控制那些对顶上事件影响重大的基本事件。在事故树定性分析中，通常用结构重要度来衡量各基本事件对顶上事件的影响程度。

(1) 计算结构重要度系数判定基本事件的排序

在事故树分析中，任何一个基本事件 x_i 都可能呈现出两种状态，一种是发生，记为 $x_i = 1$；一种是不发生，记为 $x_i = 0$。顶上事件是基本事件的状态函数，记为 $\phi(x) = \phi(x_1, x_2, \cdots, x_n)$，又将其称为事故树的结构函数。各基本事件的不同组合又构成了顶上事件的两种不同状态，即 $\phi(x) = 1$ 和 $\phi(x) = 0$。

若基本事件的个数为 n，在第 i 个基本事件 x_i $(i = 1, 2, 3, \cdots, n)$ 的状态由 0 变到 1 (即 $0_i \rightarrow 1_i$) 时，其他 $(n-1)$ 个基本事件的状态保持不变，则顶上事件的状态变化可能有三种情况：

第一种情况：$\phi(0_i, x) = 0 \rightarrow \phi(1_i, x) = 0$，则有 $\phi(1_i, x) - \phi(0_i, x) = 0$；

第二种情况：$\phi(0_i, x) = 0 \rightarrow \phi(1_i, x) = 1$，则有 $\phi(1_i, x) - \phi(0_i, x) = 1$；

第三种情况：$\phi(0_i, x) = 1 \rightarrow \phi(1_i, x) = 1$，则有 $\phi(0_i, x) - \phi(1_i, x) = 0$。

上述分析可知，第一、三种情况时，x_i 从 0 到 1 的变化对顶上事件没有起作用。惟有第二种情况，x_i 从 0 到 1 的变化对顶上事件起了作用。所以第二种情况出现得越多，说明 x_i 越重要。

由于 n 个基本事件的 0 和 1 的两种组合状态共有 2^n 个，所以若将 x_i 作为分子，保持其他基本事件的 2^{n-1} 种状态不变并作为分母，则得出的基本事件 x_i 的结构重要度系数为：

$$I_\phi(i) = \frac{1}{2^{n-1}} \sum [\phi(1_i, x) - \phi(0_i, x)] \qquad (6\text{-}3)$$

下面以图 6-3 所表示的事故树为例，求解事故树中每个基本事件的结构重要度系数。

由图可知，该事故树共有 3 个基本事件，因此其状态组合共有 $2^3 = 8$ 种。为了对比方便，在编制基本事件和顶上事件状态表时，左半部分 x_1 均为 0，右半部分 x_1 均为 1。左右两半部分 x_2，x_3 状态均相同且保持不变。于是作为分母的状态组合数即为 $2^{3-1} = 4$ 种。按上述分析基本事件和顶上事件的状态值见表 6-1。

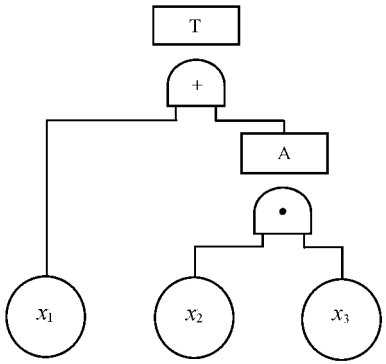


图 6-3　分析结构重要度事故树

表 6-1　基本事件和顶上事件的状态值

x_1	x_2	x_3	$\phi(x)$	x_1	x_2	x_3	$\phi(x)$
0	1	1	1	1	1	1	1
0	1	0	0	1	1	0	1
0	0	1	0	1	0	1	1
0	0	0	0	1	0	0	1

应用公式（6-3），根据表 6-1 所计算的各基本事件的结构重要度系数分别为：

$$I_\phi(1)=\frac{1}{2^{3-1}}\left[(1-1)+(1-0)+(1-0)+(1-0)\right]=\frac{3}{4}$$

$$I_\phi(2)=\frac{1}{2^{3-1}}\left[(1-0)+(0-0)+(1-1)+(1-1)\right]=\frac{1}{4}$$

$$I_\phi(3)=\frac{1}{2^{3-1}}\left[(1-0)+(0-0)+(1-1)+(1-1)\right]=\frac{1}{4}$$

根据所求各基本事件的结构重要度排序应为：

$$I_\phi(1)>I_\phi(2)=I_\phi(3)$$

从上述计算可知，应用此种方法计算基本事件的结构重要度系数是十分麻烦的，对于较为复杂的事故树的计算将带来巨大的困难。

（2）应用最小割（径）集判定基本事件的结构重要度

应用最小割（径）集判定基本事件结构重要度排序的方法虽然精度比前面的方法较低，但是操作简单，因此应用较广。其具体的判定原则如下：

1）包含基本事件越少且互不交叉的最小割（径）集中的基本事件的结构重要度越大。

如在某事故树的最小割集（x_1）；（x_2，x_3）；（x_4，x_5，x_6）之中，各基本事件的结构重要度的排序应为：

$$I_\phi(1)>I_\phi(2)=I_\phi(3)>I_\phi(4)=I_\phi(5)=I_\phi(6)$$

2）仅出现在同一最小割（径）集中的所有基本事件的结构重要度均相等。

例如，在前面例子的基本事件中：

$$I_\phi(2)=I_\phi(3)；I_\phi(4)=I_\phi(5)=I_\phi(6)$$

3）当多个最小割（径）集中的基本事件的个数相等时，在各最小割（径）集中出现次数越多的基本事件的结构重要度越大。

例如，某事故树由 3 个最小割集（x_1，x_2，x_3）；（x_1，x_3，x_4）；（x_1，x_4，x_5）。其 5 个基本事件的结构重要度依次为：

$$I_{\phi}(1) > I_{\phi}(3) = I_{\phi}(4) > I_{\phi}(5) = I_{\phi}(2)$$

4）两个基本事件出现在基本事件个数不等的多个最小割（径）集中时，其结构重要度依次按下列情况确定。

①如果它们在最小割（径）集中出现的次数相等时，则在含基本事件少的最小割（径）集中出现的基本事件的结构重要度大。

例如，某事故树有 4 个最小割集：

(x_1, x_3)；(x_1, x_4)；(x_2, x_4, x_5)；(x_2, x_5, x_6)。在这些割集中的基本事件 x_1，x_2 的结构重要度排序应为：$I_{\phi}(1) > I_{\phi}(2)$。

②如果它们在含基本事件少的最小割（径）集中出现的次数少，在含基本事件多的最小割（径）集中出现的次数多时，或更为复杂的情况，可以用下列近似式分别计算：

$$I_{\phi}(i) = \sum_{x_i \in K_j} \frac{1}{2^{n_j - 1}} \tag{6-4}$$

式中 $I_{\phi}(i)$ ——基本事件 x_i 的机构重要度；

$x_i \in K_j$ ——基本事件 x_i 属于 K_j 最小割（径）集；

n_j ——基本事件 x_i 所在最小割（径）集中包含基本事件的个数。

设某事故树共有 5 个最小割集：(x_1, x_3)；(x_1, x_4)；(x_2, x_4, x_5)；(x_2, x_5, x_6)；(x_2, x_6, x_7)。其应用式（6-4）分别计算的结果如下：

$$I_{\phi}(1) = \frac{1}{2^{3-1}} + \frac{1}{2^{3-1}} = 1；\ I_{\phi}(2) = \frac{1}{2^{3-1}} + \frac{1}{2^{3-1}} + \frac{1}{2^{3-1}} = \frac{3}{4}。$$

因此，可得：$I_{\phi}(1) > I_{\phi}(2)$。

利用上述四条基本原则判断基本事件的结构重要度时，必须严格按顺序进行，否则将出现错误的结果。

至于选用最小割集还是最小径集判断基本事件的结构重要度，其结果都是一样的。通常，选用二者较少的情况比较起来更容易些。

所确定出的基本事件的结构重要度，除可以用于制定事故控制方案之外，也可以用来制定安全检查表，找出日常管理的依据。

6.3 事故树的定量分析

事故树定量分析的基本任务是根据基本事件的发生概率，计算顶上事件的发生概率以及基本事件的概率重要度和临界重要度。

6.3.1 基本事件发生概率的计算方法

在进行事故树定量分析时，首先需要知道基本事件的发生概率。基本事件的发生概率主要包括物的故障率和人的失误率两个方面。由于取得各基本事件发生概率值是非常困难的，要通过大量反复的试验、观测、分析和检验才能得到，而其准确性也受到环境和应用条件的影响，因此，事故树真正意义上的定量分析受到了极大的限制。

下面从理论上，分别给出基本事件的发生概率、顶上事件的发生概率、基本事件的概率重要度和基本事件的临界重要度的求解方法。

(1) 物的故障率

1) 可修复系统单元的故障率

可修复系统的单元包括部件和元件，其故障率 q 的定义为：

$$q = \frac{\lambda}{\lambda + \mu} \tag{6-5}$$

式中 λ ——单元故障率,是指单位时间内故障发生的频率。一般情况下,应为：

$$\lambda = K\lambda_0 \tag{6-6}$$

K——综合考虑温度、湿度、振动及其他条件影响修正系数，一般 K = 1 ~ 10；

λ_0 ——单元故障率的实验值，$\lambda_0 = 1/$ (MTBF)；

MTBF ——平均故障间隔期，是指相邻两故障间隔期内，正常工作的平均时间，计算式为：

$$MTBF = \frac{1}{n}\sum_{i=1}^{n} t_i \tag{6-7}$$

n——各单元发生故障的总次数；

t_i ——第 i - 1 到第 i 次故障的间隔时间。

μ ——单元修复率,是指单位时间内元件修复的频率。$\mu = 1/$ (MTTR)；

MTTR——平均修复时间，是指系统单元出现故障，从开始维修到恢复正常工作所需的平均时间。通常，MTBF >> MTTR，所以 $\lambda << \mu$,则其故障概率为：

$$q = \frac{\lambda}{\lambda + \mu} \approx \frac{\lambda}{\mu} \tag{6-8}$$

2) 不可维修系统的单元故障概率

不可维修系统的单元故障概率为：

$$q = 1 - e^{-\lambda t} \tag{6-9}$$

式中 t——元件的运行时间。

若将 $e^{-\lambda t}$ 按级数展开，略去后面的高阶无穷小，可近似为：

$$q \approx \lambda t \tag{6-10}$$

目前，许多工业发达国家都建立了故障率数据库，用计算机存储和检索，使用方便。我国已有少数行业开始进行艰苦工作，但数据还相当缺乏。因此，应在工程实践中积极统计建立数据库。此外，物的故障率数据也可以从有关产品手册、样本中查得。

(2) 人的失误概率

人的失误是另一种基本事件，是指作业者实际完成的功能与系统所要求的功能之间的偏差。人的失误概率通常是指作业者在一定条件下和规定时间内完成某项规定功能时出现偏差 (或失误) 的概率。因此，人的失误概率也是人的不可靠度。

人的失误率预测方法的分析步骤如下：

1) 调查被分析者的作业程序；

2) 把整个程序分解成单个作业；

3) 再把每个单个作业分解成单个动作；

4) 根据经验和实验，适当选择每个动作的可靠度，见表 6-2；

表 6-2 人的行为可靠度统计

人的行为类型	可 靠 度	人的行为类型	可 靠 度
阅读技术说明书	0.9918	上紧螺母、螺钉和销子	0.9970
读取时间 (扫描记录仪)	0.9921	连接电缆 (安装螺钉)	0.9972
读取电流计或流量计	0.9945	阅读记录	0.9966
确定多处电器开关的位置	0.9957	确定双位置开关	0.9985
在元件位置上标注符号	0.9958	关闭手动阀门	0.9983
分析缓变电压或电瓶	0.9955	开启手动阀门	0.9985
安全垫圈	0.9962	拆除螺母、螺钉和销子	0.9988
分析锈蚀	0.9963	对一个警报器的相应能力	0.9999
记录阅读信息	0.9966	读取数字显示器	0.9990
分析凹陷、裂纹或划伤	0.9967	读取大量参数的打印记录	0.9500
读取压力表数据	0.9969	安装安全锁线	0.9961
安装环状物	0.9965	安装鱼形夹	0.9961
分析老化防护罩	0.9969		

5) 用单个动作的可靠度之积表示每个操作步骤的可靠度。如果各个动作中存在非独立事件，则用条件概率计算；

6) 用各操作步骤可靠度之积表示整个程序的可靠度；

7）用可靠度之补（1 减可靠度）表示每个程序的不可靠度，就是该程序人的失误概率。

人在人机系统中的功能主要是接受信息（输入）、处理信息（判断）和操纵控制机器将信息输出。对于某一个动作，作业人员的基本可靠度为：

$$R = R_1 \cdot R_2 \cdot R_3 \tag{6-11}$$

式中 R_1——与输入有关的可靠度；

R_2——与判断有关的可靠度；

R_3——与输出有关的可靠度。

R_1、R_2、R_3 的参考数值见表 6-3。

表 6-3 R_1、R_2、R_3 的参考数值

类 别	影响因素	R_1	R_2	R_3
简单	变量不超过几个 人机工程上考虑全面	0.9995～0.9999	0.9990	0.9995～0.9999
一般	变量不超过 10 个	0.9990～0.9995	0.9950	0.9990～0.9995
复杂	变量超过 10 个 人机工程上考虑不全面	0.9900～0.9990	0.9900	0.9900～0.9990

作业人员单个动作的失误率为：

$$q = k \cdot (1 - R) \tag{6-12}$$

式中 k——修正系数，$k = a \cdot b \cdot c \cdot d \cdot e$；

a——作业时间系数；

b——操作频率系数；

c——危险状况系数；

d——心理、生理条件系数；

e——环境条件系数。

a、b、c、d、e 的取值见表 6-4。

表 6-4 a、b、c、d、e 的取值范围

符 号	项 目	内 容	取值范围
a	作业时间	有充足富裕的时间；没有充足富裕的时间；完全没有富裕时间	1.0；1.0～3.0；3.0～10.0
b	操作频率	频率适当；连续操作；很少操作	1.0；1.0～3.0；3.0～10.0
c	危险状况	即使操作也安全；误操作时危险大；误操作时产生重大灾害的危险	1.0；1.0～3.0；3.0～10.0

续表

符　号	项　　目	内　　容	取值范围
d	心理、生理条件	教育、训练、健康状况、疲劳、愿望等综合条件较好；综合条件不好；综合条件很差	1.0；1.0～3.0；3.0～10.0
e	环境条件	综合条件较好；综合条件不好；综合条件很差	1.0；1.0～3.0；3.0～10.0

6.3.2　顶上事件发生概率的计算方法

(1) 直接计算法

当通过事故树的结构函数得到概率函数后，将各基本事件的发生概率值直接代入，就可以算出顶上事件的发生概率。

在基本事件发生概率很小（$q_i \ll 1$）时，基本事件逻辑“加”的概率和逻辑“乘”的概率可以分别按下述两近似式计算：

$$g(q) = P_r(x_1 + x_2 + \cdots + x_n) \approx q_1 + q_2 + \cdots + q_n = \sum_{i=1}^{n} q_i \qquad (6\text{-}13)$$

$$g(q) = P_r(x_1 \cdot x_2 \cdot \cdots \cdot x_n) \approx q_1 \cdot q_2 \cdot \cdots \cdot q_n = \prod_{i=1}^{n} q_i \qquad (6\text{-}14)$$

当基本事件发生概率很小时，利用上述近似公式计算出结果的误差不会很大。

(2) 最小割集法

当求出事故树的最小割集后，可用其表达事故树的结构函数。由于最小割集包含着基本事件的逻辑“乘”（即逻辑“与”），事故树的结构函数包含着最小割集的逻辑“加”（即逻辑“或”），所以当不同的最小割集中不包含相同的基本事件时，事故树的概率函数可以写成最小割集逻辑“加”的形式：

$$g(q) = P_r(T) = P_r(K_1 + K_2 + \cdots + K_k) = 1 - \prod_{j=1}^{k}(1 - \prod_{i \in K_j} q_i) \qquad (6\text{-}15)$$

式中，$K_i = x_1 \cdot x_2 \cdot \cdots \cdot x_m$（$i = 1, 2, 3, \cdots, k$），$m$ 为第 j 个最小割集 K_j 中包含的基本事件数。

一般情况下，按下述公式（即容斥公式）计算事故树顶上事件的发生概率：

$$g(q) = \sum_{r=1}^{k} \prod_{i \in K_r} q_i - \sum_{1 \leqslant h < j \leqslant k} \prod_{i \in K_h \cup K_j} q_i + \cdots + (-1)^{k-1} \prod_{i=1}^{n} q_i \qquad (6\text{-}16)$$

式中　　i——基本事件的序数；

k——最小割集的个数；

r，h，j——最小割集的序数；

$i \in K_r$——第 i 个基本事件属于第 r 个最小割集；

K——最小割集的符号；

$i \in K_h \cup K_j$——第 i 个基本事件 x_i，或属于第 h 个最小割集，或属于第 j 个最小割集；

$1 \leqslant h < j \leqslant k$——h，j 的取值范围。

例如，某事故树的最小割集为：(x_1, x_2, x_5)；(x_1, x_3, x_5)；(x_1, x_4, x_5)，应用式（6-16）计算顶上事件的概率应为：

$$g(q) = (q_1 q_2 q_5 + q_1 q_3 q_5 + q_1 q_4 q_5) - (q_1 q_2 q_5 q_1 q_3 q_5 + q_1 q_2 q_5 q_1 q_4 q_5 + q_1 q_3 q_5 q_1 q_4 q_5) + q_1 q_2 q_5 q_1 q_3 q_5 q_1 q_4 q_5$$

$$= q_1 q_2 q_5 + q_1 q_3 q_5 + q_1 q_4 q_5 - (q_1 q_2 q_3 q_5 + q_1 q_2 q_4 q_5 + q_1 q_3 q_4 q_5) + q_1 q_2 q_3 q_4 q_5$$

（3）最小径集法

当事故树中逻辑或门较多时，说明最小割集数目较多而最小径集数目较少。此时利用最小径集计算顶上事件的发生概率比较方便。由于最小径集包含着基本事件的逻辑“加”（即逻辑“或”），事故树的结构函数包含着最小径集的逻辑“乘”（即逻辑“与”），所以当不同的最小径集中不包含相同的基本事件时，事故树的概率函数可以写成最小径集逻辑“乘”的形式：

$$g(q) = P_r(T) = P_r(P_1 \cdot P_2 \cdot \cdots \cdot P_k) = \prod_{j=1}^{P} \left[1 - \prod_{i \in P_j} (1 - q_i) \right] \qquad (6\text{-}17)$$

式中　$P_i = x_1 + x_2 + \cdots + x_m$　（i = 1，2，3，…，k），m 为第 j 个最小径集 P_j 中包含的基本事件数。

一般情况下，按下述公式（即容斥公式）计算事故树顶上事件的发生概率：

$$g(q) = 1 - \sum_{r=1}^{p} \prod_{i \in P_r} (1 - q_i) + \sum_{1 \leqslant h < j \leqslant p} \prod_{i \in P_h \cup P_j} (1 - q_i) + \cdots + (-1)^{p-1} \prod_{i=1}^{n} (1 - q_i) \qquad (6\text{-}18)$$

式中　　i——基本事件的序数；

p——最小径集的个数；

r，h，j——最小径集的序数；

$i \in P_r$——第 i 个基本事件属于第 r 个最小径集；

P——最小割集的符号；

$i \in P_h \cup P_j$——第 i 个基本事件 x_i，或属于第 h 个最小割集，或属于第 j 个最小割集；

$1 \leqslant h < j \leqslant p$——h，j 的取值范围。

⑷ 不交化方法

当多个最小割集或最小径集中包含有同样的基本事件时，称这些最小割集或最小径集为“交”集。有“交”的情况存在时，用容斥公式计算事故树的顶上事件发生概率工作量巨大，即使应用计算机进行解算也将十分费时费力。

所谓的不交化方法就是利用布尔代数运算法则使最小割集的交集变为不交集，然后按每个最小割集发生概率的代数和来计算顶上事件的发生概率。不交化方法的基础是布尔代数的重叠律，如图 6-4 所示。

按图 6-4 中的规律可以进一步推广，完全用不交化最小割集表示事故树布尔代数的表达式：

$$T = K_1 + \overline{K}_1 \cdot K_2 + \overline{K}_1 \cdot \overline{K}_2 \cdot K_3 + \cdots + \overline{K}_1 \cdot \overline{K}_2 \cdot \overline{K}_3 \cdots\cdots K_{k-1} \cdot K_k \qquad (6\text{-}19)$$

式中 K_1，K_2，K_3，…，K_k 表示事故树的 k 个最小割集。

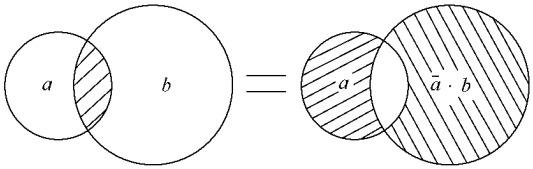


图 6-4 相交集变成不相交集

当求出某事故树的最小割集后，可以直接运用布尔代数的法则及式 (6-16) 将相交集化为不相交集计算。但是，当事故树的结构比较复杂时，应用上式计算也是相当复杂的，而应用布尔代数的不交化之和定理可以简化计算过程。

不同命题的不交化之和定理如下：

1) 若集合 a 和 b 不包含共同的基本事件，则 $\overline{a} \cdot b$ 可以先按对偶律：

$$\overline{a \cdot b} = \overline{a} + \overline{b}\ ;\ \overline{a + b} = \overline{a} \cdot \overline{b}$$

将集合 $\overline{a}$ 变换，然后按重叠率进行不交化处理，最后按分配律将其展开。

2) 若集合 a 和 b 包含共同的基本事件，则有：

$$\overline{a} \cdot b = \overline{a}_0 \cdot b$$

式中 a_0——集合 a 中有的而集合 b 中没有的基本事件的集合。

3) 若集合 a 和 c 包含共同的基本事件，集合 b 和 c 也包括共同的基本事

件，则有：

$$\bar{a}\cdot\bar{b}\cdot c=\bar{a}_0\cdot\bar{b}_0\cdot c$$

式中 a_0——集合 a 中有的而集合 c 中没有的基本事件的集合；

b_0——集合 b 中有的而集合 c 中没有的基本事件的集合。

4）若集合 a 和 c 包含共同的基本事件，集合 b 和 c 也包括共同的基本事件，且 $a\subset b$（a 属于 b），则有：

$$\bar{a}_0\cdot\bar{b}_0\cdot c=\bar{b}\cdot c$$

下面给出了对某事故树结构函数做不交化处理程序的例子：

$$\begin{aligned}T&=x_1+x_2\cdot x_4+x_2\cdot x_3\\&=x_1+\bar{x}_1\cdot x_2\cdot x_4+\bar{x}_1\cdot x_2\cdot x_3\\&=x_1+\bar{x}_1\cdot x_2\cdot x_4+\bar{x}_1\cdot x_2\cdot x_3\cdot\bar{x}_4\end{aligned}$$

假设各基本事件发生概率分别为：$q_1=0.1$，$q_2=0.2$，$q_3=0.3$，$q_4=0.4$。根据此式计算顶上事件发生的概率如下：

$$g(q)=q_1+(1-q_1)q_2q_4+(1-q_1)q_2q_3(1-q_4)=0.2044$$

（5）近似计算法

1）首相近似法

通过对精确计算的容斥公式分析可知，一方面，该公式后面连乘的基本事件概率个数多于前面连乘的基本事件概率个数，而后面基本事件概率连乘项较多的部分都是由于“交”集引起的；另一方面，每个基本事件概率往往较小（$q_i\ll 1$），这使得后面连乘项乘出的数值远远小于前面连乘项乘出的数值。由于在实际应用时，后面交集计算出的概率对顶上事件发生概率值起的作用很小，所以在误差允许的情况下，采用略去交集作用的方法计算顶上事件发生概率，既可以保证实际应用又可以减少计算工作量。

首相近似计算式为：

$$g(q)\approx\sum_{j=1}^{k}\prod_{i\in K_j}q_i \tag{6-20}$$

式中的符号含义同前。

2）平均近似法

平均近似法就是在首相近似法的基础上，加上容斥公式第二项的一半，使得计算结果更加精确。

$$g(q)\approx\sum_{r=1}^{k}\prod_{i\in K_r}q_i-\frac{1}{2}\cdot\sum_{1\leqslant h<j\leqslant k}\ \prod_{i\in K_h\cup K_j}q_i \tag{6-21}$$

3）独立近似法

独立近似法的出发点是，尽管事故树中各最小割、径集彼此包含有相同的

基本事件，但是仍然将其当成为无相同的基本事件处理，即认为最小割、径集的基本事件是相互独立的。

利用最小割集时，计算式为：

$$g(q) \approx \coprod_{j=1}^{k} \coprod_{x_i \in K_j} q_i \tag{6-22}$$

利用最小径集时，计算式为：

$$g(q) \approx \coprod_{j=1}^{p} \coprod_{x_i \in P_j} q_i \tag{6-23}$$

式中 $\coprod$ ——数学运算符号，求概率和。

6.3.3 基本事件的概率重要度和临界重要度

基本事件的概率重要度和临界重要度是事故树定量分析中重要的步骤，分别从量上反映了基本事件的重要程度。

(1) 基本事件的概率重要度

基本事件概率重要度反映了基本事件发生概率的变化对顶上事件发生概率的影响程度。概率重要度的定义为：

$$I_g(i) = \frac{\partial g(q)}{\partial q_i} \tag{6-24}$$

式中 $g(q)$ ——故障树的概率函数；

q_i ——第 i 个基本事件的发生概率。

若知道了故障树对概率函数和各基本事件的发生概率，就可以按上式计算出各基本事件的概率重要度。

例如，某事故树 5 个基本事件的概率分别为：

$$q_1 = 0.01，\ q_2 = 0.02，\ q_3 = 0.03，\ q_4 = 0.04，\ q_5 = 0.05$$

概率函数为：

$$g(q) = 1 - \left\{1 - q_4 \left[1 - (1 - q_3)(1 - q_2 q_5)\right]\right\}\left\{1 - q_1 \left[1 - (1 - q_3)(1 - q_5)\right]\right\}$$

其各基本事件的概率重要度分别为：

$$I_g(1) = \frac{\partial g(q)}{\partial q_1} = 1 - \left\{1 - q_4 \left[1 - (1 - q_3)(1 - q_2 q_5)\right]\right\}\left\{1 - \left[1 - (1 - q_3)(1 - q_5)\right]\right\} = 0.078$$

$$I_g(2) = \frac{\partial g(q)}{\partial q_2} = 0.02；\quad I_g(3) = \frac{\partial g(q)}{\partial q_3} = 0.049；$$

$$I_g(4) = \frac{\partial g(q)}{\partial q_4} = 0.031；I_g(5) = \frac{\partial g(q)}{\partial q_5} = 0.01。$$

于是，各基本事件概率重要度的排序应为：

$$I_g(1) > I_g(3) > I_g(4) > I_g(5) > I_g(2)$$

如果能够有效控制概率重要度大的基本事件，减小其发生概率，则可以有效地防止顶上事件的发生。一般情况下，减小发生概率大的基本事件的发生概率较之容易。

⑵ 基本事件的临界重要度

通常，用顶上事件发生概率的相对变化率与基本事件发生概率的相对变化率的比值表示基本事件的临界重要度。其定义如下式：

$$I_c(i) = \frac{\partial[\ln g(q)]}{\partial(\ln q_i)} = \frac{\partial[g(q)]}{g(q)} \cdot \frac{q_i}{\partial q_i} = I_c(i) \cdot \frac{q_i}{g(q)} \qquad (6\text{-}25)$$

基本事件的临界重要度主要反映了当基本事件发生概率变化时，对顶上事件发生概率变化量的影响程度。

根据前述例子，按此式计算的基本事件临界重要度应为：

$I_c(1) = 0.39$；$I_c(2) = 0.02$；$I_c(3) = 0.74$；$I_c(4) = 0.62$；$I_c(5) = 0.25$

于是，各基本事件的临界重要度的排序应为：

$$I_g(3) > I_g(4) > I_g(1) > I_g(5) > I_g(2)$$

6.4 事故树分析实例

事故树分析主要包括两部分，即根据事故编制事故树；对编好的事故树进行定性和定量分析。

6.4.1 事故树编制的原则

事故树的编制过程是一个严密的逻辑推理过程，应遵循如下原则：

⑴ 危险大的事件作为顶上事件的原则

正确选择顶上事件是事故分析的关键。在系统危险分析时，不希望发生的事件往往不止一个。通常，应当把易于发生且后果严重的事件优先作为顶上事件。当然，也可以把发生频率不高但后果严重的，或后果虽不太严重但发生频繁的事故作为顶上事件。

⑵ 合理确定边界条件的原则

在确定了顶上事件之后，为不使事故树过于繁杂，应明确规定出与其他系统的界限，以及一些必要合理的假设条件。

⑶ 循序渐进的原则

事故树的编制过程是一个逐级展开的演绎过程。首先，从顶上事件开始分析其发生的直接原因、判断逻辑关系，给出逻辑门；其次，找出逻辑门下

的全部输入事件；再分析引起这些事件发生的原因、判断逻辑关系，给出逻辑门；继续逐层分析，直至列出引起顶上事件发生的全部基本事件和上下逻辑关系。

⑷ 逻辑门与逻辑门不直接相连的原则

为了保证逻辑关系的正确性，事故树中任何逻辑门的输出都必须也只能有一个结果事件，不能将逻辑门与逻辑门相连。

⑸ 事故树明确定义的原则

明确事故树定义就是要用简洁明了的语言描述事故的内涵。

6.4.2 事故树分析举例

以高处施工坠落为例进行事故树分析。

⑴ 事故树编制

依据编制原则编制的高处坠落事故树，如图 6-5 所示。

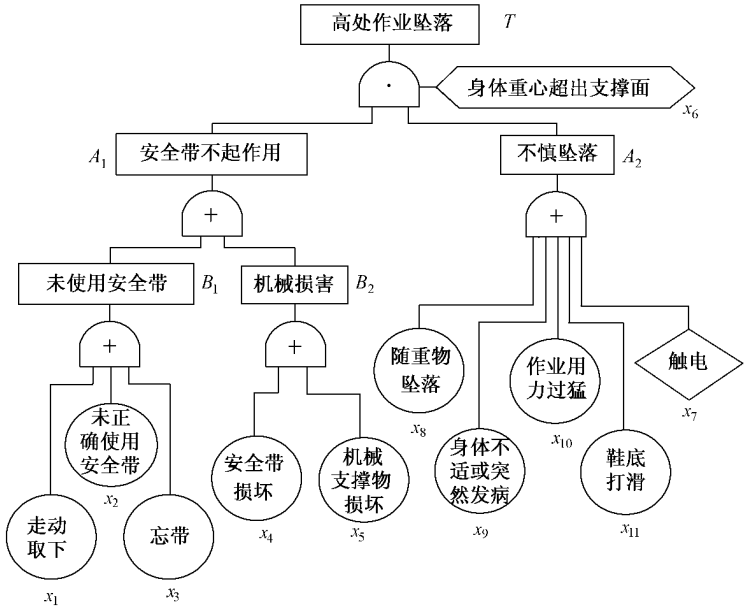


图 6-5 高处作业坠落事故树

⑵ 事故树的定性分析

对事故树结构分析可知，事故树的“或”门（即逻辑“加”）较多，而“与”门（即逻辑“乘”）较少。这说明该事故树的最小割集较多，最小径集较少。因此，应用最小径集对其分析比较方便。

将上述事故树转化成为如下成功树进行分析（图 6-6）：

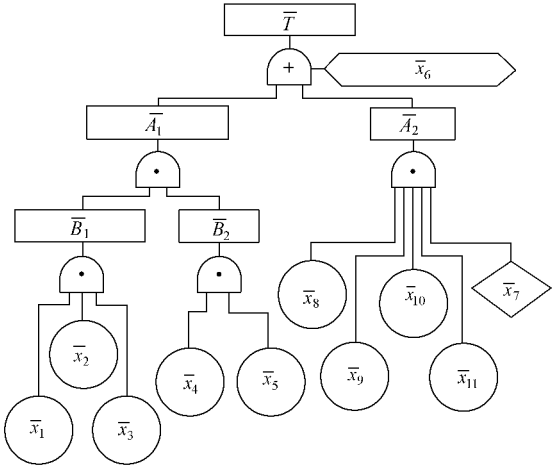


图 6-6　事故树的成功树

写出成功树的布尔代数表达式：

$$\begin{aligned}\overline{T} &= \overline{A}_1 + \overline{A}_2 + \overline{x}_6 \\ &= \overline{B}_1 \cdot \overline{B}_2 + \overline{x}_7 \cdot \overline{x}_8 \cdot \overline{x}_9 \cdot \overline{x}_{10} \cdot \overline{x}_{11} + \overline{x}_6 \\ &= \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \cdot \overline{x}_4 \cdot \overline{x}_5 + \overline{x}_7 \cdot \overline{x}_8 \cdot \overline{x}_9 \cdot \overline{x}_{10} \cdot \overline{x}_{11} + \overline{x}_6\end{aligned}$$

所求出的最小径集分别为：

$$(x_1, x_2, x_3, x_4, x_5)\ ;(x_7, x_8, x_9, x_{10}, x_{11})\ ;(x_6)$$

从最小径集中可以看出 x_6 **最重要，其基本事件的概率重要度的排序应为：**

$$\begin{aligned}I_\phi(6) &> I_\phi(1) = I_\phi(2) = I_\phi(3) = I_\phi(4) = I_\phi(5) \\ &= I_\phi(7) = I_\phi(8) = I_\phi(9) = I_\phi(10) = I_\phi(11)\end{aligned}$$

(3) 事故树的定量分析

事故树中各基本事件发生概率见表 6-5 **所示。**

1) **写出事故树的概率函数，计算顶上事件的发生概率**

事故树的概率函数如下：

$$g(q) = \left[1 - (1 - q_1)(1 - q_2)(1 - q_3)(1 - q_4)(1 - q_5)\right] \cdot q_6 \cdot \left[1 - (1 - q_7)(1 - q_8)(1 - q_9)(1 - q_{10})(1 - q_{11})\right]$$

代入表 6-5 **中的数据计算，得到顶上事件发生概率为：**

$$g(q) = 0.0000143$$

表 6-5　基本事件发生概率取值表

代　　号	基本事件名称	q_i	$1-q_i$
x_1	走动，取下	0.02	0.98
x_2	未正确使用安全带	0.00001	0.99999
x_3	忘带安全带	0.1	0.9
x_4	安全带损坏	0.0001	0.9999
x_5	机械支撑物损坏	0.001	0.999
x_6	身体重心超出支撑面	0.01	0.99
x_7	触　　电	0.000001	0.999999
x_8	随重物坠落	0.001	0.999
x_9	身体不适或突然发病	0.00001	0.99999
x_{10}	作业用力过猛	0.001	0.999
x_{11}	鞋底打滑	0.01	0.99

2）计算基本事件的概率重要度

按式（6-24）和表 6-5 中的数据，计算的基本事件的概率重要度如下：

$I_g(1)=0.000108$；$I_g(2)=0.000106$；$I_g(3)=0.000117$；

$I_g(4)=0.000106$；$I_g(5)=0.000106$；$I_g(6)=0.00143$；

$I_g(7)=0.00119$；$I_g(8)=0.00119$；$I_g(9)=0.00119$；

$I_g(10)=0.00119$；$I_g(11)=0.00120$

基本事件概率重要度排序如下：

$$I_g(6)>I_g(11)>I_g(7)=I_g(8)=I_g(9)=I_g(10)>I_g(3)>I_g(1)>I_g(2)=I_g(4)=I_g(5)$$

3）计算基本事件的临界重要度

按式（6-25）和表 6-5 中的数据，计算的基本事件的临界重要度如下：

$I_c(1)=0.151$；$I_c(2)=0.0000741$；$I_c(3)=0.818$；

$I_c(4)=0.000741$；$I_c(5)=0.00741$；$I_c(6)=1$；

$I_c(7)=0.0000832$；$I_c(8)=0.0832$；$I_c(9)=0.000832$；

$I_c(10)=0.0832$；$I_c(11)=0.839$

基本事件临界重要度排序如下：

$$I_c(6)>I_c(11)>I_c(3)>I_c(1)>I_c(8)=I_c(10)>I_c(5)>I_c(9)>I_c(7)>I_g(2)$$

（4）分析结论

1）从高处作业坠落事故树分析可知，该事故树的“或”门较多，大部分单个基本事件的发生都有输出，只有少数与门有几个基本事件同时发生才发生。

2）由于最小割集较多，造成顶上事件发生的途径较多。因此顶上事件 T 发生的危险性较高。

3）从最小径集分析可知，该事故树只有 3 个最小径集，所以防止顶上事件不发生的途径较少。

4）分析可知，无论是结构重要度、概率重要度还是临界重要度，系统中的基本事件 x_6 都是至关重要的，在实际工作中应注意防范。

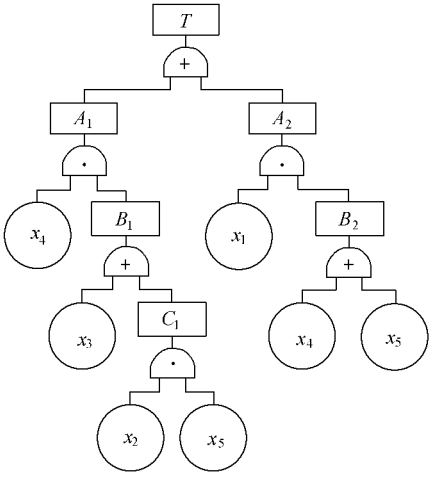
5）降低 x_6，x_{11}，x_7，x_8，x_9，x_{10} 的概率可以大大降低顶上事件的发生概率。

思　考　题

1. 事故树如图所示。要求：

1）写出结构函数，求出最小割集和最小径集，求出各基本事件的结构重要度和排序；

2）设各基本事件的发生概率均为 0.01，计算顶上事件的发生概率，求出各基本事件的概率重要度和临界重要度及其排序。



2. 根据自己所熟悉的系统选择一顶上事件建立事故树，并仿照上题的要求进行分析。

7 系统安全分析

系统安全分析顾名思义是从安全的角度对所研究的系统进行分析，识别系统中导致故障和事故的危险源及其影响因素，找出各影响因素之间的相互关系，以便采取必要的预防措施。

系统安全分析方法有数十种之多，应根据实际的条件选择相适应的分析类型及分析方法。系统安全分析方法具体分为以下几类：

⑴ 按逻辑思维方法分类

按逻辑思维方法可将系统分析方法分为归纳法和演绎法两大类。所谓的归纳法就是从事故发生的原因推论出事故结果的方法，即从个别到一般的方法。主要包括安全检查表法、预先危害性分析、故障类型及影响分析、危险性和可操作性分析等。

所谓的演绎法就是从事故结果推论出事故原因的方法，即从一般到个别的方法。主要包括事件树分析方法、事故树分析方法、系统可靠性分析方法、因果分析方法等。

⑵ 按定性分析和定量分析分类

所谓定性分析就是指对引起系统事故的影响因素进行非量化的分析，即只进行可能性的分析或做出事故能否发生的感性判断。主要包括有安全检查表法、预先危害性分析、故障类型及影响分析、危险性和可操作性分析等。

所谓的定量分析就是在定性分析的基础上，运用数学方法分析系统事故及影响因素之间的数量关系，对事故的危险做出数量化的描述。主要包括事件树分析、事故树分析、系统可靠性分析、因果分析等。

在上述分析方法中，有的既可以用于定性分析，也可以用于定量分析，如事件树分析、事故树分析等。

⑶ 按静态分析和动态分析分类

所谓的动态分析就是指对系统事故危险的分析能够反映出事故过程和环境变化的特点。主要包括有事件树分析、因果分析等。

所谓的静态分析就是指对系统事故危险的分析不能反映出事故过程和环境变化的特点。除动态分析法中的事件树分析和因果分析之外的方法均为静态分析法。

了解系统安全分析的类型之后，有助于针对不同的系统选取不同的系统安

全分析方法。各种不同的系统安全分析方法所适用的情况见表 7-1 所示。

表 7-1　各种系统安全分析方法的适用情况

工作系统 / 分析方法	开发研制	方案设计	样机试验	详细设计	建造投产	日常运行	改造扩建	事故调查	拆除工程
安全检查表分析		√	√	√	√	√	√		√
预先危害（险）分析	√	√	√	√			√		
故障类型及影响分析			√	√		√	√	√	
事件树分析			√			√	√	√	
因果分析			√	√		√	√	√	
危险性与可操作性研究			√	√		√	√	√	
事故树分析			√	√		√	√	√	
系统可靠性分析	√		√	√		√			

表 7-1 中列出了 8 种最常用的系统安全分析方法，其中由于系统可靠性分析法和事故树分析法的内容较多，在前面 5、6 两章中先行进行了讨论，本章不再赘述。

7.1　安全检查表分析

7.1.1　安全检查表及基本格式

安全检查表是一种在对所研究的系统科学分析的基础上，将其存在的各种不安全因素按其重要程度编制成的安全检查专用表格，是实施安全检查和安全诊断的项目明细表，是安全检查结果的备忘录。

安全检查表是一种系统安全的定性分析方法，通常以“是”与“否”或“√”与“×”的方式对所研究系统的不安全因素进行分析。其表述明了，简单易行。

安全检查表的基本格式如表 7-2 所示。

表 7-2　安全检查表的基本格式

序号	检查部位	检查内容	安全要求	标准依据	检查结果 合格（是）不合格（否）	改进措施	负责人

检查时间：　　年　　月　　日　　时　　检查者：

安全检查表在系统安全分析中应用十分广泛。对不同的研究系统，安全检查表的格式虽然有所不同，但是具体的表头内容大同小异。

7.1.2 安全检查表的种类及编制

安全检查表按其用途大致可分为五类，可根据不同用途和要求设计出用于不同系统的安全检查表。

⑴ 设计审查用安全检查表

据统计，有设计不良存在的不安全因素引起的事故约占事故总数的25%～30%。如果在设计时能避免不安全因素的存在，则可以取得事半功倍的效果。大量实践证明，工程投入使用后，再重新补充安全方面的项目，常常是事倍功半。因此，在设计时就要把好安全关。检查表中除以对话方式列入检查项目外，还要列入设计应遵循的有关规程、标准和必要的数据。

设计用安全检查表主要包括选择、平面布置、工艺过程、装置的布置、建筑物与构筑物、安全装置与设备、操作的安全性、危险物品的储藏以及消防设备等方面。

⑵ 厂级的安全检查表

这类安全检查表反映了工厂企业的全面安全状况，主要用于全厂安全性检查，也可作为安全技术措施、防火等系统和部门进行日常检查时使用。其主要内容应包括厂区各个产品的工艺和装置的安全性、要害部位、主要安全装置与设施、危险物品的储藏与使用、消防通道与设施、操作管理、遵章守纪等。

⑶ 车间用安全检查表

供车间进行定期检查和预防性检查使用。其内容包括工艺安全、设备布置、安全通道、通风照明、安全标志、尘毒和有害气体浓度、消防措施、操作和管理等。

⑷ 工段及岗位用安全检查表

供工段和岗位进行自检、互检和安全教育用。其内容根据岗位工艺、设备的抗灾要求而定。要求检查内容具体、易行。

⑸ 专业性安全检查表

由专业机构或职能部门编制和使用，主要用于定期的或季节性的安全检查，如对电气设备、压力容器、特殊装置与设施的专业检查。

安全检查表可以按生产系统、车间、工段和岗位编写，也可以按专题编写，如对重要设备和容易出现事故的工艺流程，应该编制专门的安全检查表。

为了使安全检查表能够指导和检查工作，应该采取专业干部主持，会同有关部门的领导、工程技术人员和工作人员编写，通过实践检验不断修改，使之日趋完善。

编制安全检查表的过程，也是对系统进行安全分析的过程，可以根据有关规程或标准并在总结本单位和吸收外单位经验基础上，完成安全检查表的制定。如果能通过事故树分析找出导致事故发生的基本事件和最小割集，不仅可以列出安全检查表的检查项目和检查重点，而且可以了解它们之间的逻辑关系。

安全检查表的编制过程如图 7-1 所示。

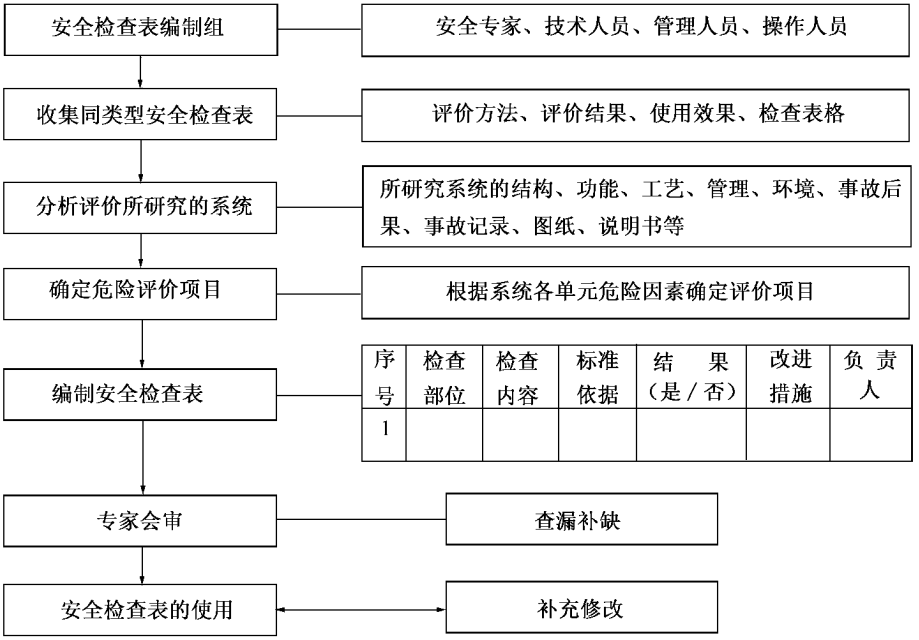


图 7-1　安全检查表的编制过程

7.1.3　安全检查表举例

表 7-3 中给出了某企业厂级安全检查表示例。

表 7-3　某企业厂级安全检查表

项目	序号	检查内容	标准要求	标准依据	检查结果(是/否)	改进措施	负责人
安全管理	1	领导小组成员、不脱产安全员	组织落实	国标			
	2	安全例会每月一次	分管主任主持	省标			
	3	车间领导轮流安全值班	记录为准	企标			
	4	工伤事故按规定上报	及　时	企标			
	5	事故后严格执行“三不放过”原则	分管主任主持	省标			

续表

项目	序号	检查内容	标准要求	标准依据	检查结果(是/否)	改进措施	负责人
安全管理	6	用检查表对班组每月检查一次	分管主任主持	企标			
	7	岗位安全检查表和 ABCDE 卡相符	表卡一致	企标			
	8	隐患整改通知卡 (D 卡) 执行情况	验收签字为准	企标			
安全教育	1	新工人上岗前安全教育	考试合格	国标			
	2	安全板报稿件情况	一月一期一篇	企标			
	3	违章违制人员处罚警告牌	干部工人一样	企标			
	4	厂级安全指标完成情况	100%	企标			
	5	班组安全活动日发言人数	每周一次 50%	企标			
作业场所	1	工作间内人行道不准堆放垃圾杂物	整洁无杂物	企标			
	2	工作场所不准放自行车	自行车放车棚内	企标			
	3	工具箱整齐放置于规定地点	分类放齐	企标			
	4	平台走道不得积水、积油	不影响行走安全	企标			
	5	水沟盖板齐全	不影响行走安全	企标			
	6	生产设备周围不得堆放杂物、备件	不影响操作	企标			
	7	工作区灯具完好	损坏填卡上报	企标			
	8	危险地点安全标志完好	完整齐全	企标			
	9	特殊岗位工人持证上岗	培训合格	国标			
安全技术	1	临时行灯电压	安全电压	国标			
	2	电器线路状况	绝缘、完整	国标			
	3	电器开关状况	绝缘、完整	国标			
	4	高速运转设备安全罩	完好牢固	国标			
	5	起重设备限位	灵敏可靠	国标			
	6	起重设备钢丝绳	一捻距小于 10%	国标			
	7	2m 以上平台栏杆	牢固完好	国标			
	8	高空坠物防护	完好可靠	国标			
	9	氧气瓶与乙炔桶摆放	距明火 10m，两距 5m	国标			
	10	电焊机接线头	安全可靠	国标			

检查日期：×××× 年 ×× 月 ×× 日 ×× 时　　检查者：×××

表 7-4 中给出了某企业起重设备岗位安全检查表示例。

表 7-4　起重设备岗位安全检查表

序号	检查部位及内容	标准要求	标准依据	检查结果 (是/否)	改进措施	负责人
1	操作时电器柜门	完整关严	国标			
2	电　　铃	完好、声音清晰	×× 条			
3	紧急开关	可　　靠	×× 条			

续表

序号	检查部位及内容	标准要求	标准依据	检查结果 (是/否)	改进措施	负责人
4	掉钩限位器	完　好	××条			
5	小车极限	完　好	××条			
6	仓门、栏杆开关	完　好	××条			
7	各部分制动器	完　好	××条			
8	照　明	工作区明亮	国　标			
9	外露传动部分防护罩	完好、可靠	××条			
10	钢丝绳	完　好	××条			
11	走梯、平台、走台栏杆	完　好	国　标			

检查日期：××××年××月××日××时　　检查者：×××

7.2 预先危害 (险) 性分析

7.2.1 基本概念及分析表格

预先危害 (险) 分析方法是在系统开发初期阶段和设计阶段对系统中存在的危险类别、形成条件、事故后果等进行安全分析识别，尽可能在系统付诸实施之前找出预防、改正、补救的措施，消除或控制危险源。

预先危害 (险) 分析方法的优点是：尽可能在系统开发初期和设计阶段识别、控制危险因素，用最小的代价消除或减少系统中的危险源，为制定整个系统运行期间的安全操作规程提出依据。

预先危害 (险) 分析的基本格式如表 7-5 所示。

表 7-5　预先危害 (险) 分析基本格式

事故现象	危险因素	触发事件	事故原因	事故后果	危险等级	防治措施

预先危害 (险) 分析的格式和内容可根据系统的特点作必要的调整。但是，表 7-5 中的事故原因、事故后果、危险等级以及防止措施几项是对新系统分析不可缺少的重要内容。

7.2.2 预先危害 (险) 性分析程序

预先危害 (险) 性分析是一种应用范围较广的定性的系统安全分析方法。

它需要具有丰富知识和实践经验的工程技术人员、操作人员和管理人员经过细致的分析和讨论来实现。

预先危害（险）性分析程序如图 7-2 所示。

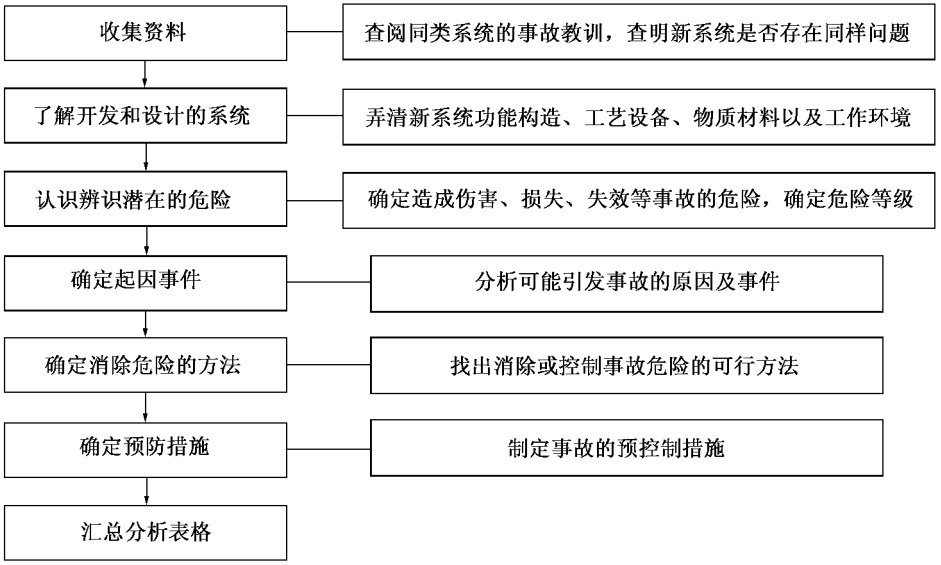


图 7-2　预先危害（险）分析程序

7.2.3　危害（险）性等级划分

在通过对新系统危险源的辨识，研究其产生的原因和可能导致的事故，根据导致事故原因的重要性和后果的严重程度进行分级。通常分为四级，见表 7-6 所示。

表 7-6　危害（险）等级

等级	名　称	特　征　和　要　求
Ⅰ	安全性的危害	不会导致伤害或疾病，系统无损失。可以忽略
Ⅱ	临界性的危害	有导致事故的可能，伤害或疾病轻微，系统损失微小。应注意控制
Ⅲ	危险性的危害	可导致事故，造成严重伤害或疾病，对系统造成较大破坏。采取措施控制
Ⅳ	灾难性的危害	可导致事故，造成死亡和系统报废。必须设法消除

对于辨识出的主要危险源，可以通过修改开发方案和设计、增加安全措施来消除或控制，从而达到新系统安全的目的。

7.2.4 危害（险）性分析应用实例

通常在一些实际系统（工业或民用）设计中，经常需要应用到石油液化气作为燃料或原料。在实际生产生活中石油液化气引起的火灾和爆炸事故时有发生。下面以石油液化气火灾和爆炸事故为例，进行预先危害（险）分析。其分析的结果如表 7-7 所示。

表 7-7 石油液化气火灾、爆炸事故预先危害（险）分析

事故现象	危险因素	触发事件	事故原因	事故后果	危险等级	防治措施
火灾	液化气外溢高温	故障泄漏、运行泄漏、明火、火花、高温物体	漏液遇明火、火花或高温物体	石油液化气损失、人员伤亡、系统严重损坏、严重的经济损失	Ⅳ	控制消除火源、保证质量、加强管理、按规定操作、保证安全设施齐全完好、防止泄漏
爆炸	高温、高压、液化气外溢		储罐遇明火、火花或高温物体		Ⅳ	

在表 7-7 的预先危害（险）分析中，触发事件一栏中概括性地分析出了 5 种触发事件，每个事件可以根据系统的实际情况还可以继续细化至具体事件。

故障泄漏包括：1）储罐、液化气器具、管线、阀门、法兰、密封等破损泄漏；2）超装溢出；3）阀门、管线等安装不当或质量不好泄漏；4）物体撞击造成罐体、阀门、管线等破裂泄漏；5）自然灾害造成破裂泄漏等。

运行泄漏包括：1）超温、超压运行造成破裂泄漏；2）安全附件失灵、损坏或操作不当泄漏；3）骤冷、急热造成罐、器等破裂泄漏等。

明火包括：1）点火吸烟；2）烟火；3）检修违章用火；4）外来人员带火种；5）物体过热着火；6）其他火源等。

火花包括：1）撞击火花；2）电器火花；3）雷击火花；4）短路火花；5）焊、割、摩擦火花等。

同理，在防治措施一栏中也概括性提出了应采取的 5 个方面措施，每项措施也可以根据具体系统的实际情况进行细化直至具体措施。

控制消除火源包括：1）严禁吸烟、携带火种进入；2）需用火时，必须采取有效防范措施；3）使用防爆型电器；4）安装避雷设施并定期检查；5）严禁钢质工具撞击；6）采取防静电措施。

保证质量包括：

1）选用高质量的罐、阀门、管线等设备及配件；2）保证安装质量；

3）定期检查、检验、检测有关设备、设施、电力线路、设备器材；4）定期对报警、监测等系统维护、保养，保持完好状态；5）高温物体、部件采取隔离措施。

加强管理按章操作包括：1）杜绝违章作业、违章指挥、违反劳动纪律现象；2）坚持巡回检查，及时发现问题及时处理；3）维修用火时，做好隔离工作；4）加强培训、教育和考核等工作；5）防止车辆等物体撞击。

安全设施齐全完好包括：1）消防、遥控等设施完好；2）监测、报警等设施完好。

防止液化气及残液泄漏：1）严防故障泄漏；2）严防运行泄漏；3）严防人为泄漏。

7.3 故障类型及影响分析

7.3.1 基本概念及格式

故障是指系统或元素在运行过程中，性能低下不能实现预定功能的状态。通常情况下，研究系统中相同的组成部分和元素发生的故障并不是也不可能是相同的。故障类型是指系统中相同的组成部分和元素所发生故障的不同形式。而系统的组成部分和元素不同的故障类型对系统的影响也是不同的。危险度分析是对系统中组成部分和元素的不同故障类型危险程度（危险度）的分析。通常用不同故障类型发生的概率来衡量其危险程度（危险度）。

故障类型及影响分析就是通过对系统的各个组成部分、元素进行分析，找出其不同的故障类型；分析各种不同的故障类型最终对所研究系统的影响程度；采取必要的措施控制故障影响保证系统的正常运行。它是一种以归纳法为基础的系统安全分析方法。

目前，故障类型及影响分析已由最初的定性分析发展到与故障发生概率和危险度分析结合起来，构成了故障类型及影响和危险度分析方法。从而只要确定了每个元素的故障类型和发生概率，就可以定量地描述故障对所研究系统的影响。

通过对所研究的系统进行故障类型及影响分析后的结果填入表 7-8 中。

表 7-8 故障类型及影响分析

组成的元素	故障的类型	故障的原因	故障的影响	故障的识别	校 正 措 施

对于故障类型及影响和危险度分析法，在编制分析图表时，只需在故障类型及影响分析的图表（表 7-8）之中加上通过分析计算得出的危险程度（危险度）数值和故障发生概率数值两列栏目即可。

7.3.2 故障类型及影响的分析程序

故障类型及影响分析的程序如图 7-3 所示。

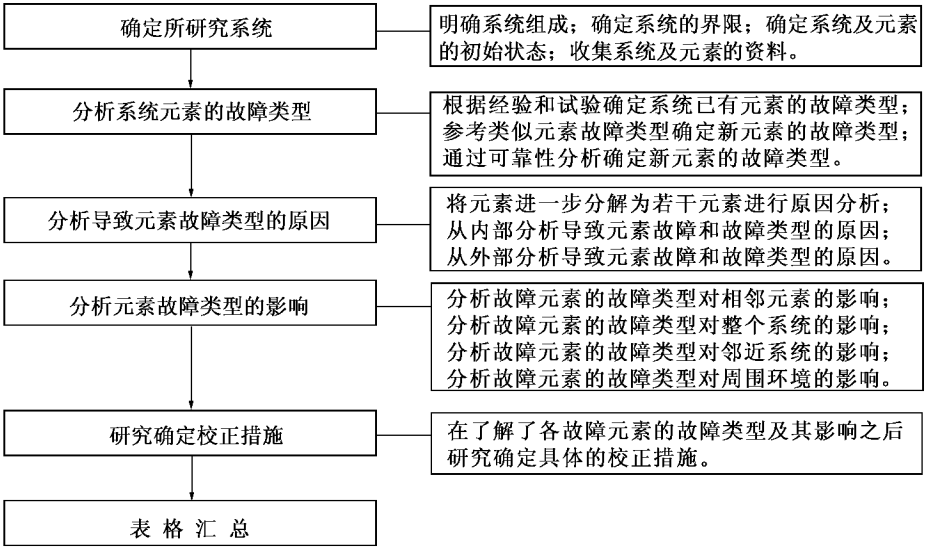


图 7-3 故障类型及影响分析程序

7.3.3 故障类型及其影响分析实例

空气压缩机是在土木工程的道桥工程、地下工程等施工时常用的动力设备。空气压缩机的储气罐属于一种易于出现事故的高压容器，是安全管理工作中的重点设备系统。在此对空气压缩机储气罐的罐体和安全阀两元素的故障类型及影响进行了分析。分析后的结果列于表 7-9 中。

表 7-9 空气压缩机储气罐的故障类型及影响分析

组成元素	故障类型	故障的原因	故障的影响	故障的识别	校正措施
罐 体	轻微漏气	接口不严	能耗增加	漏气噪声、空气压缩机频繁打压	加强维修保养
	严重漏气	焊接裂缝	压力迅速下降	压力表读数下降，巡回检查	停机修理
	破 裂	材料缺陷、受冲击等	压力迅速下降、损伤人员和设备	压力表读数下降，巡回检查	停机修理

续表

组成元素	故障类型	故障的原因	故障的影响	故障的识别	校正措施
安全阀	漏　气	接口不严、弹簧疲劳	能耗增加、压力下降	漏气噪声,空气压缩机频繁打压	加强维修保养
	错误开启	弹簧疲劳折断	压力迅速下降	压力表读数下降，巡回检查	停机维修
	不能安全泄压	由锈蚀污物等造成	超压时失去安全功能，系统压力迅速增高	压力表读数升高，阀门检验	停机检查更换

7.3.4　故障类型及其影响和危险度（致命度）分析

将故障类型及影响分析与危险度分析相结合，便可以从定性分析发展到定量分析，从而形成将故障类型及影响和危险度的系统安全分析方法。

故障类型及影响和危险度分析方法包括两方面的分析内容：

⑴ 故障类型及影响分析

此部分的分析即为前面 7.3.1，7.3.2，7.3.3 三节中讨论的内容。此不赘述。

⑵ 危险度分析

危险度分析的目的在于评价每种组成元素故障类型的危险程度。通常，采用元素故障类型出现的概率和故障后果的严重度两项指标来衡量危险度。表 7-10 和表 7-11 中给出了美国杜邦公司的严重度分级和概率值。

表 7-10　危险发生等级和概率标准

发生等级	非常容易发生	容易发生	偶尔发生	不常发生	几乎不发生	很难发生
发生概率	1×10^{-1}	1×10^{-2}	1×10^{-3}	1×10^{-4}	1×10^{-5}	1×10^{-6}

表 7-11　危险等级划分及其校正措施

危险度	大（危险）	中（临界）	小（安全）
校正措施	立即停止作业	及时检修	注意观察

除上述用概率和故障后果两项指标的危险度分析之外，还有只用危险度一项指标来分析评价的情况。此时按下式计算危险度数值 C。它表示元素运行百万小时（次）发生的故障次数。

$$C = \sum_{j=1}^{n} (\alpha \cdot \beta \cdot k_1 \cdot k_2 \cdot \lambda \cdot t \cdot 10^6) \qquad (7\text{-}1)$$

式中 n——导致系统故障或事故的故障类型的数目；

t——元素的运行时间；

λ——元素的基本故障率 ；

$k_1 \cdot k_2$——分别为实际运行状态的修正系数和实际运行环境的修正系数；

α——导致系统故障或事故的故障类型数目占全部故障类型数目的比例；

β——导致系统故障或事故的故障类型出现时，系统发生故障或事故的概率，β 值可参照表 7-12 选取。

表 7-12 β 参考值的选取表

影响程度	实际的损失	可预计的损失	可能出现的损失	没有影响
发生概率（β）	$\beta = 1.00$	$0.10 \leqslant \beta < 1.00$	$0 < \beta < 0.10$	$\beta = 0$

7.3.5 故障类型及影响和危险度（致命度）分析实例

表 7-13 给出了起重机防过卷装置和钢丝绳两组件系统的故障类型及影响和危险度分析的实例。

表 7-13 起重机部分组成元素的故障类型及影响和危险度分析

名称	组成元素	故障类型	故障原因	故障影响	危险程度	发生概率	检查方法	校正措施
防止过卷装置	电器零件 机械部分 制动瓦块	动作不可靠 变形、生锈 间隙过大	零件失修 使用过久 螺丝松动	误动作 损 坏 刹车失灵	大 中 大	1×10^{-2} 1×10^{-4} 1×10^{-3}	通电检查 观察 观察	立即维修 警 惕 及时紧固
钢丝绳	绳 股 钢 丝	变形、扭结 断丝 15%	使用过久 使用过久	绳断裂 绳断裂	中 大	1×10^{-4} 1×10^{-1}	观察 检查	及时更换 立即更换

7.4 事件树分析

7.4.1 事件树的概念

事件树分析是一种按事故发展时间顺序，由初始时间开始推论可能的后果，从而进行危险分析辨识的方法。

事故的发生是由许多原因事件相继发生所引起的结果，而一些事件的发生是以另一些事件预先发生为条件的。

事件树分析过程是以所研究的易于出现故障或事故的系统特定功能作为一个初始事件，找出与其有关的后续事件，分析这些后续事件的安全或危险、成功或失败、正常或故障的两种对立状态，分别逐级推进，直至分析到系统故障或事故为止。由于这一分析过程是用一棵树状的图形直观表述的，故称为事件树。

初始事件是指在一定条件下，事件树系统可能出现故障或事故的特定功能事件，也是最初的原因事件。后续事件是指出现在初始事件之后的一系列可能造成事故的原因事件。

事件树分析源于决策树分析，是一种以归纳法为基础的系统安全分析方法。不仅可以用于事先预测事故，预计事故的可能后果，为采取预防措施提供依据；又可以用于事故发生后的分析，找出事故原因。不仅可以对事故进行定性分析，又可以对事故进行定量分析。

由于该方法直观方便，实用性强，所以在各行各业的实际生产中得到了广泛的应用。

7.4.2 事件树的定性分析

事件树定性分析的基本内容是通过编制事件树，找出系统中的危险源和导致事故发生的连锁关系（发展途径），采取预防措施。事件树定性分析的主要步骤如图 7-4 所示。

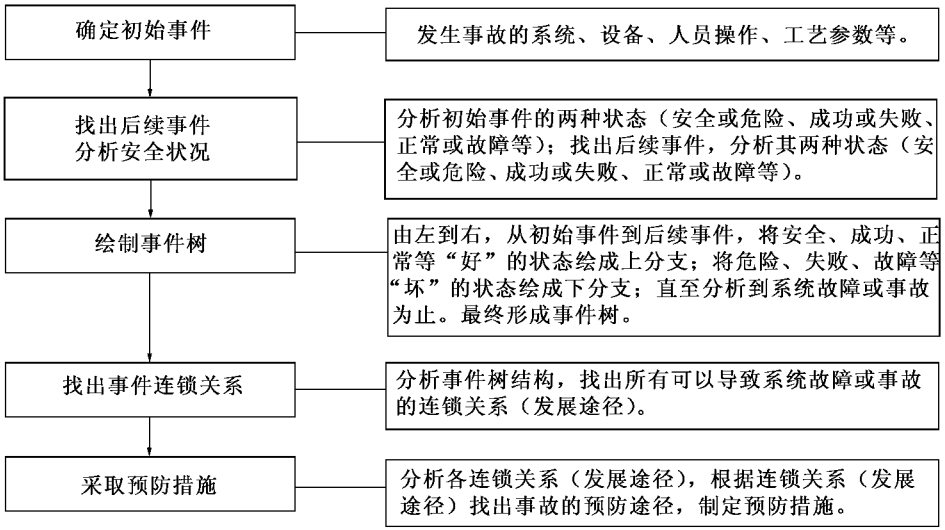


图 7-4 事件树定性分析步骤

根据上述三部分的分析，最终可以得到形如图 7-5 的事件树图。

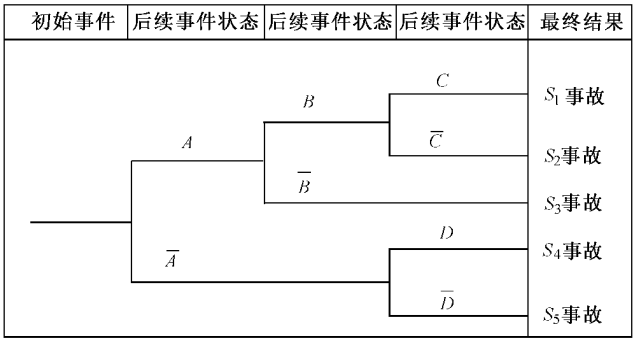


图 7-5　事件树图

在图中，中间事件的安全、成功、正常等“好”的状态均直接用英文字母表示；相反，事件的危险、失败、故障等“坏”的状态在英文字母上部加一横杠表示。

其中，S_1、S_4 为无故障或事故的连锁关系；S_2、S_3、S_5 为发生故障或事故的连锁关系。在实际安全工作中，可以在事件树中 S_2、S_3、S_5 发生故障或事故的连锁关系（发展途径）的基础上，制定和采取预防故障出现和事故发生的措施。

7.4.3　事件树的定量分析

在事件树定性分析的基础上，若能够给出每个中间事件的两种不同状态的概率值，那么根据事件树中的各连锁关系（发展途径）可以计算出各自的发生概率。同样，在各连锁关系（发展途径）概率的基础上，可以计算出所分析系统事故发生的概率。

以图 7-5 为例，各中间事件安全（或成功、正常等）的概率分别为：

$$P[A]，P[B]，P[C]，P[D]$$

各中间事件危险（或失败、故障等）的概率分别为：

$$P[\overline{A}]，P[\overline{B}]，P[\overline{C}]，P[\overline{D}]$$

各连锁关系（发展途径）的发生概率分别应为：

$$P[S_1] = P[A] \cdot P[B] \cdot P[C]$$

$$P[S_2] = P[A] \cdot P[B] \cdot P[\overline{C}]$$

$$P[S_3] = P[A] \cdot P[\overline{B}]$$

$$P[S_4] = P[\overline{A}] \cdot P[D]$$

$$P[S_5] = P[\overline{A}] \cdot P[\overline{D}]$$

所研究系统发生事故的概率应为：

$$\overline{P} = P[S_2] + P[S_3] + P[S_5]$$

所研究系统不发生事故的概率应为：

$$P = P[S_1] + P[S_4]$$

7.4.4 事件树分析应用实例

【例 7-1】 如图 7-6 所示，一台泵和两个串联阀门组成的物料输送系统。根据这一系统绘出的运行事件树如图 7-7 所示。

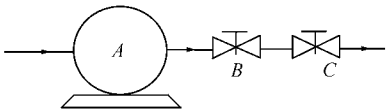


图 7-6 串联输送系统

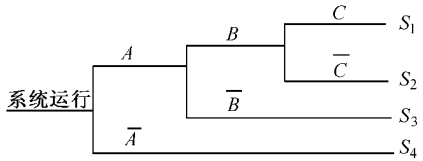


图 7-7 串联输送系统事件树

串联系统中，输送泵 A、阀门 B 和阀门 C 能正常运行的概率分别为：0.95、0.90、0.90，而不能正常运行的概率分别为：0.05、0.10、0.10。

系统能正常运行的连锁关系（发展途径）只有一组 S_1，其概率值应为：

$$P[S_1] = P[A] \cdot P[B] \cdot P[C] = 0.95 \times 0.90 \times 0.90 = 0.7695$$

同时，这也就是整个系统能够正常运行的概率 P 的数值。

系统不能正常运行的连锁关系（发展途径）有三组，即 S_2，S_3，S_4。各自概率值应为：

$$P[S_2] = P[A] \cdot P[B] \cdot P[\overline{C}] = 0.95 \times 0.90 \times 0.10 = 0.0855$$

$$P[S_3] = P[A] \cdot P[\overline{B}] = 0.95 \times 0.10 = 0.095$$

$$P[S_4] = P[\overline{A}] = 0.05$$

整个系统不能正常运行概率应为：

$$\overline{P} = 1 - P = P[S_2] + P[S_3] + P[S_4] = 0.0855 + 0.0950 + 0.05 = 0.2305$$

【例 7-2】 如图 7-8 所示，一台泵和两个并联阀门组成的物料输送系统。根据这一系统绘出的运行事件树如图 7-9 所示。

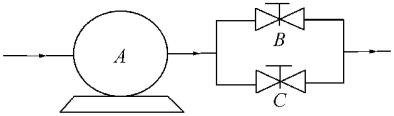


图 7-8 并联输送系统

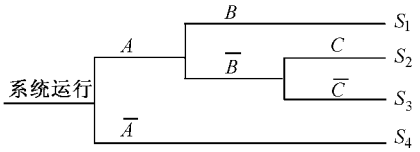


图 7-9 并联输送系统事件树

并联系统中，输送泵 A、阀门 B 和阀门 C 能正常运行的概率分别为：0.95、0.90、0.90，而不能正常运行的概率分别为：0.05、0.10、0.10。

系统能正常运行的连锁关系（发展途径）有两组，即 S_1，S_2。其各自的概率值应为：

$$P[S_1] = P[A] \cdot P[B] = 0.95 \times 0.90 = 0.855$$

$$P[S_2] = P[A] \cdot P[\overline{B}] \cdot P[C] = 0.95 \times 0.10 \times 0.90 = 0.0855$$

整个系统能正常运行的概率即为：

$$P = P[S_1] + P[S_2] = 0.855 + 0.0855 = 0.9405$$

系统不能正常运行的连锁关系（发展途径）也有两组，即 S_3，S_4。其各自的概率值应为：

$$P[S_3] = P[A] \cdot P[\overline{B}] \cdot P[\overline{C}] = 0.95 \times 0.10 \times 0.10 = 0.0095$$

$$P[S_4] = P[\overline{A}] = 0.05$$

整个系统不能正常运行的概率即为：

$$\overline{P} = 1 - P = P[S_3] + P[S_4] = 0.0095 + 0.05 = 0.0595$$

对比串联、并联输送系统的分析计算结果可知，并联系统不正常运行的概率远远小于串联系统；并联系统正常运行的概率远远大于串联系统。

7.5 事故的因果分析

7.5.1 事故因果分析的概念

事故的因果分析法是以事故致因理论的事故因果理论为基础发展起来的系统安全分析方法。目前，在对事故进行因果分析时主要采用了因果分析图法（鱼刺图法）和事件树和事故树结合的原因-结果分析法。根据事故因果理论的原理，本书将这两种方法统归于因果分析法之列。

因果分析图法（鱼刺图法）是把所研究系统中所发生（或预测发生）事故的原因和结果之间的关系，采用简明文字和线条绘制成图进行直观分析的方法。由于所绘制的分析图类似于一副去掉鱼肉的鱼刺，因此也称为鱼刺图法。此法是一种定性分析方法。

原因-结果分析法是由事件树分析法和事故树分析法相结合形成的一种系统安全分析方法。这种方法结合了事件树动态宏观分析的优点和事故树静态微观分析的优点，充分发挥了两者的长处。此法既可以对事故进行定性分析，又可以对事故进行定量分析。

根据事故因果致因理论，事故的发生可分为三种类型，即由多原因导致事故发生的集中型，由一个原因引起另一个原因，直至引起事故发生的连锁型，

以及既有集中作用又有连锁作用的复合型，如图 7-10 所示。通常复合型事故情况较为普遍。

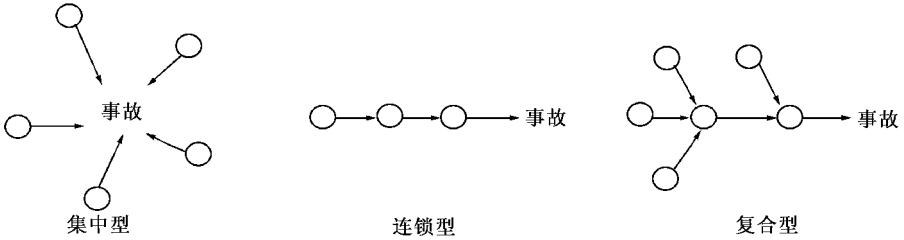


图 7-10　事故因果致因理论的三种类型

7.5.2　事故的因果分析图（鱼刺图）分析法

具体的分析步骤如图 7-11 所示。

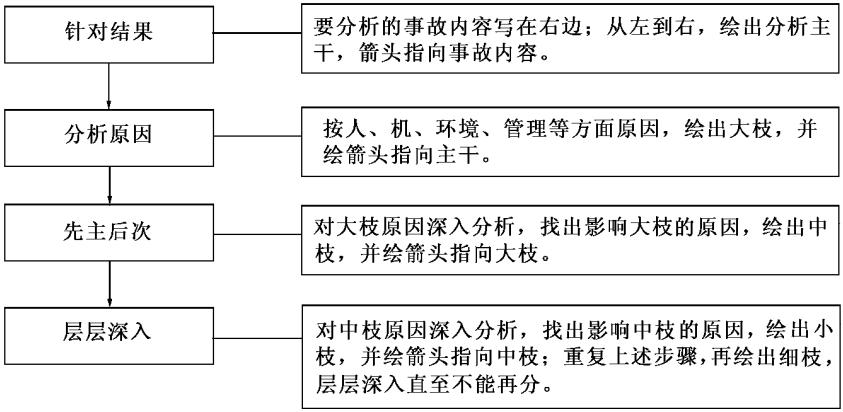


图 7-11　因果分析图法（鱼刺图法）分析步骤

在绘制因果分析图（鱼刺图）时，事故分析应从人、物、环境、管理四个方面着手进行，图 7-12 给出了因果分析图（鱼刺图）基本结构形式。

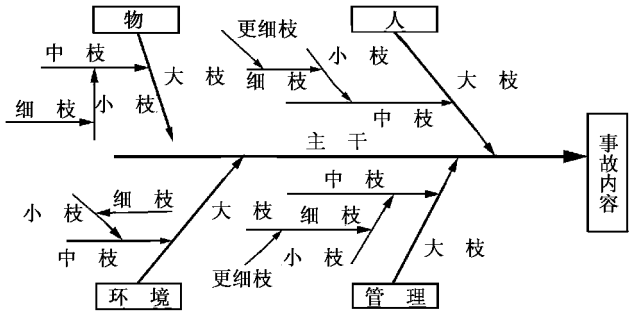


图 7-12　因果分析图法（鱼刺图法）的基本结构图

7.5.3 事故的原因-结果分析法

(1) 原因-结果分析法的分析步骤

1) 根据所研究的事故系统，绘制事件树；

2) 以事件树中的初始事件和处于危险、失败、故障等不利状态的后续事件为事故树的顶上事件，绘制事故树；

3) 将绘制的各故障树与绘制的事件树结合起来，形成原因-结果分析图；

4) 计算故障树顶上事件 (后续事件的不利状态) 发生概率；

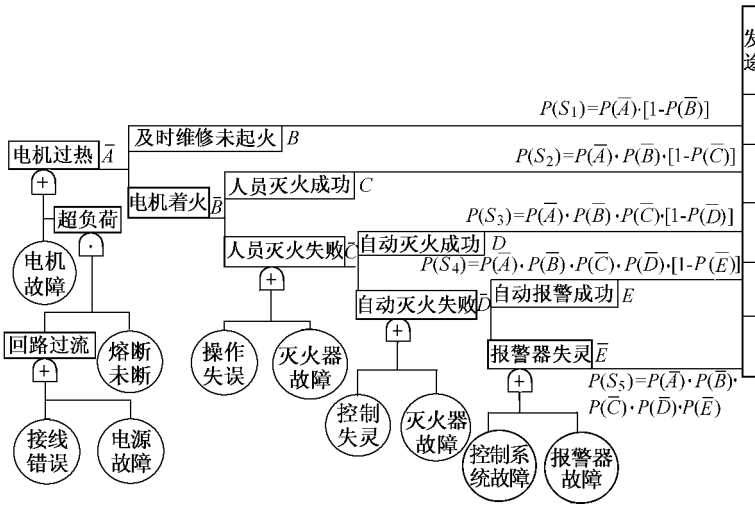
5) 计算事件树中各事故连锁关系 (发展途径) 的发生概率，计算危险程度和事故损失；

6) 根据求得的各事故连锁关系 (发展途径) 的危险程度进行评价。

(2) 原因-结果分析法的应用举例

某企业因电机过热未被及时发现而燃烧，操作人员灭火不及时，自动灭火系统失灵，自动报警系统也失灵，最后导致工作区着火，造成巨大损失。应用原因-结果分析法分析所造成的各种后果和损失。

首先，进行详细的事件树分析，绘出事件树。然后，将后续故障事件作为顶上事件绘制事故树，如图 7-13 所示。



发展途径	发生概率	停工时间	损失千美元/次
S_1	0.172478	2小时	3
S_2	0.003053	24小时	39
S_3	0.000447	720小时	1744
S_4	0.000018	无限期	20000
S_5	0.000001	无限期	50000伤亡10人

图 7-13 电机过热引起火灾的原因 - 结果分析

事件树中的初始事件概率、后续故障事件的概率以及事故树中的基本事件概率见表 7-14 所示。

表 7-14　各种失败事件的发生概率

代　号	失 败 事 件	发生概率 (次/年)
$\overline{A}$	电机过热	0.176
$\overline{B}$	电机着火	0.020
x_5	操作人员失误	0.100
x_6	灭火器失效	0.0365
x_7	自动灭火器控制失灵	0.0219
x_8	自动灭火器故障	0.0219
x_9	报警器控制系统失灵	0.05475
x_{10}	报警器失灵	0.01095

分析计算出的各个后续事件的发生概率如表 7-15 所示。

表 7-15　后续事件发生概率计算表

代　号	计　算　过　程	发　生　概　率
$\overline{C}$	$P(x_5)+P(x_6)-P(x_5)\cdot P(x_6)$	0.13285
C	$1-P(\overline{C})$	0.86715
$\overline{D}$	$P(x_7)+P(x_8)-P(x_7)\cdot P(x_8)$	0.04332
D	$1-P(\overline{D})$	0.95668
$\overline{E}$	$P(x_9)+P(x_{10})-P(x_9)\cdot P(x_{10})$	0.06510
E	$1-P(\overline{E})$	0.93490

7.6　危险性与可操作性研究

危险性与可操作性研究是一种定性的系统危险性分析方法。它应用系统的审查方法审查设计已有生产工艺和工程总图，通过分析装置、设备个别部位的误操作或故障引起的潜在危险，评价其对整个连续性生产系统的影响。通常，危险性与可操作性研究是由包括各相关领域专家的多人小组共同完成的。

7.6.1　危险性与可操作性研究概述

危险性与可操作性研究就是对所研究系统的工艺进行全面地审查，找出可能偏离设计意图的情况，分析其产生原因及造成的后果，采取合适的措施给予控制。在危险性与可操作性研究中，经常用到以下专用术语：

1) 意图

所谓的意图就是所研究系统的工艺的某一部分欲完成的功能。在很多情况

下，这种意图是用流程图描述出来的。

2）偏离

所谓的偏离是指背离设计意图的情况。在分析过程中，需正确地运用引导词系统地审查系统的工艺参数，找出偏离的情况。

3）原因

此处的原因就是引起偏离的原因。这些原因可能是物的故障、人的失误、成分变化等意外的工艺状态和外界的破坏等。

4）后果

所谓的后果就是偏离系统设计意图所造成的结果（如有毒物质泄漏等）。

5）引导词

顾名思义，引导词就是在辨识危险源的过程中，引导、启发人的思维，对设计意图定性或定量描述的简单词语。表 7-16 中列出了危险性与可操作性研究中常用的引导词及其意义。

表 7-16　危险性与可操作性研究的引导词

引导词	意　义	注　释
没有或不	是对意图的完全否定	意图的任何部分都没有达到，也没有其他事情发生
较　多	量的增加	原有量的正增值，或原有活动的增加
较　少	量的减少	原有量的负增值，或原有活动的减少
也，又	量的增加	与某些附加活动一起，达到全部设计或操作意图
部　分	量的减少	只达到一些意图，没达到另一些意图
反　向	与意图相反	与意图相反的活动或物质
不同于	完全替代	没有任何部分达到意图
非		发生完全意外的事情

6）工艺参数

此处是指有关系统工艺的物理和化学的特性。工艺参数即包括如反应、混合、浓度、pH 值等的一般参数，也包括如温度、压力、相态、流量等的特殊参数。

当系统工艺的某个部分或某个操作步骤的工艺参数偏离了设计意图时，则系统的运行状态必然发生变化，甚至造成系统的故障或引起事故。

在对系统进行危险性与可操作性研究时，依次设想所研究部分或操作步骤可能出现的由引导词同工艺参数组合形成的与设计意图的偏离，如“没 + 流量 = 没流量，流量 + 过大 = 流量过大”等组合情况。然后，可以根据组合词的情况详细分析出现偏离的原因，偏离可能造成的后果，从而研究出为了防止出

现偏离采取的措施。

下面列出了设想引导词与工艺参数结合后得到偏离状况的例子。

引导词	+ 工艺参数	= 偏 离
没 有	流 量	没流量
较 多	压 力	压力升高
又	一种相态	两种相态
非	运 行	维 修

危险性与可操作性研究分析方法具有如下特点：

1) 可以探明所分析系统装置和工艺过程存在的危险，并根据危险判断产生的后果；

2) 可以明确所分析系统中的主要危险源，指导安全工作；

3) 可以为事故树对系统进一步深入分析确定“顶上事件”；

4) 既可以用于设计阶段，又可以用于现有的系统装置；

5) 既可以用于连续过程的危险性分析,又可以用于间歇过程的危险性分析；

6) 适合于尚无经验的新技术开发中辨识静态和动态过程的危险性。

危险性与可操作性研究的最终分析表格形式见表 7-17：

表 7-17 × × × 的危险性与可操作性研究

引 导 词	偏 离	可 能 原 因	后 果	修 正 措 施

7.6.2 危险性与可操作性研究的分析程序

(1) 准备工作

准备工作包括如下内容：

1) 确定分析目的、对象和范围

在进行分析前，必须明确目的，确定所研究的对象 (如系统或装置等)。确定目的的工作可以是审查一项设计 (如选择安全的厂址等) 的状况，可以是审查现行的指令、规程的完善情况，也可以是找出工艺过程的危险源等。

在确定研究对象时，要明确其研究边界、研究的深入程度等。

2) 成立研究小组

成立研究小组，充分利用集体的智慧和经验。小组成员以 5 ~ 7 人组成，不能过少，以免知识面较窄，分析结果的可靠性差；也不能过多，以免组织协调困难。小组成员应包括有相关领域的专家、所研究系统的设计者等。

3) 获取必要的资料

资料包括设计图纸、流程图、布置平面图、等比例图和装配图，以及操作指令、设备控制顺序图、逻辑图和计算机程序等。有时还需要企业、设备的操作规程和说明书等。

4) 制定研究计划

在搜集足够资料的基础上，要制定一份可行的研究计划。首先，根据经验确定每个工艺部分或操作步骤所花费的时间，估计全部研究工作所需时间；然后，安排会议次数和每次会议的研究内容。

(2) 会议审查

以会议的形式对工艺的每个部分或每个操作步骤进行审查。组织者应以各种形式提问，启发小组成员对可能出现的偏离、引起偏离的原因、产生的后果以及应采取的措施发表意见。

具体的工作程序如图 7-14 所示。

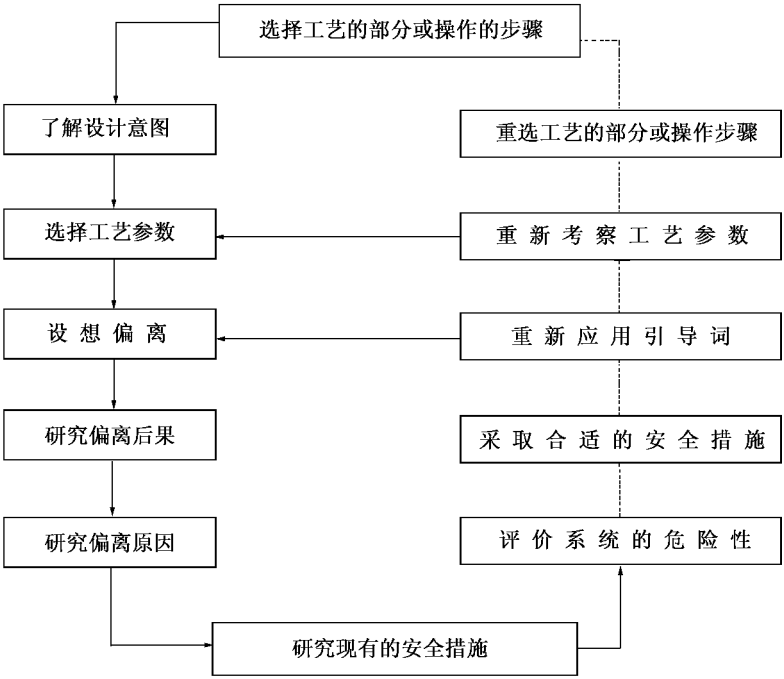


图 7-14 危险性与可操作性研究工作程序

7.6.3 应用举例

针对某燃油锅炉进行了危险性与可操作性研究分析。

分析中采用了“不、多、少、部分、其他”等引导词和“流量、压力、温

度、pH 值”等工艺参数。经调查搜集资料，研究小组按计划进行多次会议讨论审查，制定了修正措施。最后形成了如表 7-18 所示的危险性与可操作性研究结果。

表 7-18　燃油锅炉的危险性与可操作性研究

引导词	偏离	可能原因	后果	修正措施
不	严重缺水	1. 水位超限保护失灵，水位计失灵； 2. 给水系统故障； 3. 排污阀门泄漏； 4. 判断失误（假水位）； 5. 工作失误，操作失误。	爆管，甚至锅炉爆炸	1. 确保自动给水，水位超高超低报警，低水位联动等自动保护装置动作可靠，水位计灵敏可靠； 2. 确保给水系统和排污系统的设备、阀门、管道完好可靠； 3. 提高操作人员技术水平，严格执行操作规程； 4. 杜绝三违（违章作业、违章指挥、违反劳动纪律）现象。
	锅炉灭火	1. 燃油质量低劣或含水太多； 2. 炉膛大量漏风，燃烧不稳定； 3. 燃油雾化不良，影响燃烧； 4. 燃油与空气混合不好； 5. 操作不当或不遵守操作规程； 6. 喷燃器设计或制造不合理。	锅炉灭火，引发炉膛爆炸	1. 燃油应符合设计要求； 2. 炉膛和燃烧器的设计应与使用的燃油特点相适应； 3. 燃油变化范围应符合有关技术标准； 4. 按燃油选择合理的雾化方法，确保燃油雾化效果； 5. 严格按操作规程操作，杜绝三违现象； 6. 安装性能质量好、安全可靠的灭火保护装置和炉膛火焰监控装置； 7. 炉膛装设防爆门，保证炉墙严密不漏风。
多	锅炉超压	1. 安全阀失灵； 2. 压力表故障； 3. 超压报警及连锁保护失灵； 4. 操作不当或不遵守操作规程，脱岗。	爆管，甚至锅炉爆炸	1. 安全阀必须定期校验，定期做排气试验。确保灵敏可靠； 2. 压力表必须定期检查校验，确保灵敏可靠、装置齐全； 3. 确保超压报警及连锁保护装置安全可靠； 4. 安装燃烧自动调节装置，确保可靠燃烧； 5. 严格按规程操作，杜绝三违现象。

续表

引导词	偏离	可能原因	后果	修正措施
多	锅炉漏水	1. 水位超限。报警保护失灵或水位计失灵； 2. 自动供水故障； 3. 判断失误； 4. 工作失误。误操作或违反劳动纪律（脱岗）。	1. 蒸汽管道水冲击； 2. 汽轮机受水冲击。	1. 确保自动给水装置完好，高水位报警装置可靠； 2. 定期冲洗、校验水位计。确保水位计灵敏可靠； 3. 提高职工技术水平，严格执行操作规程； 4. 加强劳动纪律，杜绝三违现象。
	锅炉过热蒸汽超温	1. 蒸汽温度自动调节装置失灵； 2. 超温报警装置失灵； 3. 温度计损坏； 4. 工作失误。误操作或脱岗。	过热器管过热引起爆管	1. 确保蒸汽温度自动调节装置安全可靠； 2. 确保超温报警装置灵敏可靠； 3. 温度计定期校验，确保温度计灵敏可靠； 4. 提高职工技术水平，严格执行操作规程； 5. 加强劳动纪律，杜绝三违现象。
	锅炉严重结垢	1. 炉外处理不合格，入炉水质超标； 2. 炉内处理不当； 3. 没有排污或排污量不够； 4. 生水直接入炉。	锅炉受热面结垢导致过热，爆管	1. 锅炉给水必须经炉外处理合格后才能进入炉内，同时进行炉内水处理； 2. 生水及不合格的水不得进入锅炉； 3. 根据炉水的碱度或含盐量进行排污。
少	锅炉严重腐蚀	1. 没有对锅炉进行定期检修； 2. 因空气潮湿或烟气冲刷，外部腐蚀； 3. 停炉未做保养或方法不当，造成停炉腐蚀； 4. 给水未经除氧，pH 值偏小等造成运行腐蚀。	受热面壁厚变薄，造成爆管。甚至锅炉爆炸	1. 坚持对锅炉定期检查，测定壁厚，制定相应措施； 2. 切实加强停炉保养工作； 3. 按规定控制运行锅炉的炉水碱度，锅炉给水的含氧量必须控制在规定范围之内； 4. 停止运行的锅炉应保持锅炉四周空气干燥，运行时应尽可能少用含硫量较大的燃油，并防止尾部的低温腐蚀。
	供油量不足	1. 油泵数量或排量不够； 2. 油路管道故障； 3. 油箱油量不足。	影响负荷和压力	1. 保证油泵数量和排量； 2. 加强维修检查； 3. 提供充足的油量，足够的油箱。

续表

引导词	偏离	可能原因	后果	修正措施
部分	油系统泄漏	1. 油系统的设备管道阀门的设计、安装、检验、造型、材质等存在缺陷； 2. 误操作或违章操作； 3. 无定期维护、保养。	燃油泄漏，明火或高温引发火灾或爆炸	1. 油系统的设备管道阀门的设计、安装、检验、造型、材质应符合相应的规程、规范、标准，确保严密不漏油； 2. 加强定期维护、保养，发现泄漏应及时处理； 3. 油系统周围的高温管道、设备应严格保温，保证表面温度低于50 ； 4. 严格执行操作规程，加强劳动纪律，杜绝三违现象； 5. 油系统附近严禁烟火。
	噪声	1. 风机、水泵等设备运行产生噪声； 2. 蒸汽排放产生噪声。	听力损伤	1. 选用低噪声设备； 2. 加装消声设施和安装在单独隔声机房中； 3. 蒸汽排放设置消声器； 4. 控制室采用隔声门，双层玻璃的隔声措施。
	机械伤害	无防护罩或防护栏杆	人身伤害	按规定对机械转动设备加防护罩或防护栏杆。
	高温	1. 锅炉及汽、水管道保温不良； 2. 高温汽、水管道泄漏。	灼伤、烫伤	1. 加强汽、水管道维护，确保严密不泄漏，发现泄漏及时处理； 2. 锅炉及汽、水管道加强保温，使其表面温度低于50 。
其他	地震、雷电	自然灾害	危机设备及人身安全	1. 锅炉房厂房根据标准按相应的地震烈度设计； 2. 高层建筑物的顶层、烟囱顶部设置避雷带，保护建筑物； 3. 控制室要防止感应电和雷电侵入。

思 考 题

1. 何谓系统安全分析？系统安全分析方法是如何分类的？有哪些主要方法？
2. 试对所住房间的电气照明系统进行故障类型和影响分析。

3. **一仓库设有火灾检测系统和喷淋系统组成的自动灭火系统。设火灾检测系统可靠度和喷淋系统可靠度皆为** 0.99**，应用事件树分析计算一旦失火时，自动灭火失败的概率。**
4. **简述预先危害（险）性分析、事故类型与影响分析和危险性与可操作性研究。**

8 系统安全评价

8.1 概述

安全评价是系统安全工程的重要组成部分之一，是一种行之有效的安全管理方法。事先对建设工程、生产操作、设备运行等系统开展安全评价工作可以对系统危险性有所认识，提前预防和减少事故的发生。在安全评价过程中，经常提及到安全和危险等基本概念，只有搞清楚安全和危险等基本概念的内涵，了解安全评价的方法才能真正理解安全评价的实际意义。

8.1.1 安全与危险

无论是人类社会还是自然界中都存在着各式各样的危险，人们在生产、生活过程中始终伴随着危险的出现。有的是由于自然灾害所造成的危险（如地震、洪水、飓风等），有的是由于人类活动引起的危险（如交通事故、飞机失事、火灾爆炸等）。

危险是人们所不愿意见到的可以造成人身伤害、环境破坏、财产损失的威胁。人们在现实生活中始终面临着大量的危险（如自然灾害的伤害、生产过程的事故等）。通常人们采用危险性大小来衡量危险程度。危险性是对危险系统的客观描述，说明危险的相对程度。它用危险概率和危险严重度来表示危险可能导致的后果。危险概率是发生危险的可能性。它可用定量的方法来表示，一般用单位时间内危险可能出现的次数来描述。危险严重度是对危险造成结果的评价。

生活在现实世界里的每一个人都要面临大量的危险。面对众多的危险，人们不断努力去追求所谓的安全。按一般的理解，安全是没有伤害、损害或危险，不遭受危害或损害的威胁，或免除了伤害的威胁。然而世界上没有绝对的安全，安全即为没有超过允许限度的危险。按此理解，安全也是一种危险，只不过其危险性很小，人们可以接受它。这种没有超过允许限度的危险被称作可接受的危险。

所谓可接受的危险是来自某种危险源的实际危险，但是它不能威胁有知识而又谨慎的人。例如，在交通拥挤的道路上骑自行车，虽然能发生交通事故，但是人们仍然愿意骑车代步。

被社会公众所接受的危险称为“社会允许危险”。在安全评价中，社会允许的危险是判别安全与危险的标准。

安全是一个相对主观的概念，安全是一种心理状态。对于同一事物是安全还是危险的认识，不同的人是不一样的；即使同一个人当其具有不同的心理状态、不同的立场、不同目的时，对危险的认识也是不同的。

研究表明，有许多因素影响着人们对危险的认识程度。一般来说，当人们进行某项活动时，可能获得的利益越多，所能承受的危险程度越高。如图 8-1 所示，处于 A 处且相对获得的利益较少的人认为是安全的，而处于 B 处且获利较多的人也认为是安全的。美国原子能委员会曾引用它的利益与危险关系图来说明人们从事非自愿地活动所获得的利益与承受的危险之间的关系，如图 8-2 所示。

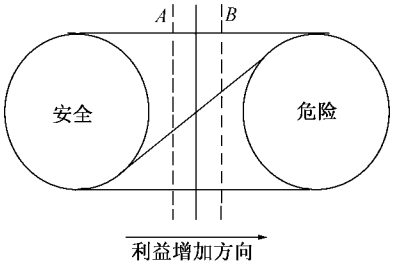


图 8-1　社会允许的危险

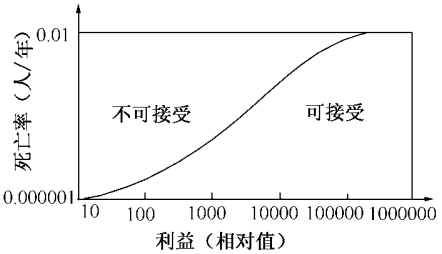


图 8-2　利益与危险关系

影响可接受危险程度的因素还包括人们是否自愿从事某项活动，危险的后果是否立即出现，对危险的认识程度等。

经过研究人们对危险的认识和实际危险之间的关系，容易得到如下结果：

1）人们往往认为疾病死亡人数低于交通事故死亡人数，实际上前者是后者的若干倍；

2）低估了一次死亡人数少，但大量发生的事故的危险性；

3）高估了一次死亡许多人，但很少发生的事故的危险性。

在人们的心目中导致平均每天死亡 1 人的社会活动没有平均每年中只导致一次死亡 300 人的社会活动更加危险，出现这种情况的原因是一些精神的、道义的和社会心理因素起的作用。

8.1.2　安全评价的内容

安全评价是对系统危险程度的客观评价，它通过对系统中存在的危险源和控制措施的评价客观地描述系统的危险程度，指导人们预先采取措施降低系统的危险性。安全评价的内容如图 8-3 所示。

安全评价包括确认危险性和评价危险性两个方面。前者在于辨识危险源，定量来自危险源的危险性；后者在于控制危险源，评价采取措施后危险源存在的危险性是否能被接受。在实际的评价过程中，这两部分工作不是无联系地、孤立地进行，而是相互交叉地、相互重叠地进行。

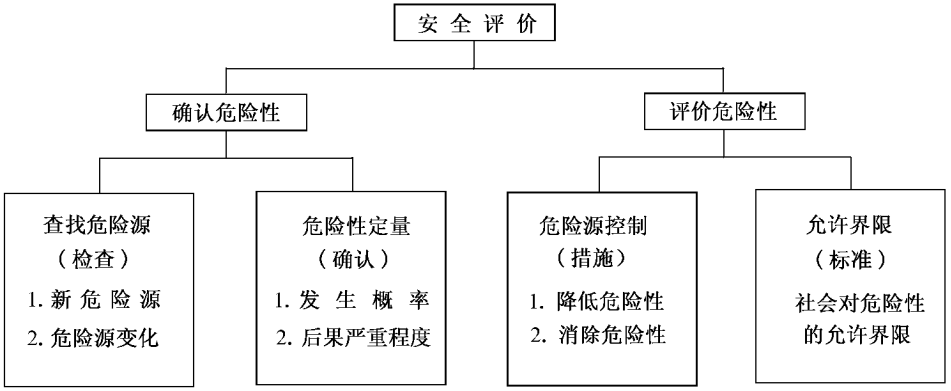


图 8-3　安全评价内容

8.1.3　安全评价的分类

安全评价从不同的角度其分类不同。由于分类的不同，其工作范围、时间阶段以及量化程度都有所不同。

⑴ 安全预评价与现实系统安全评价

根据安全评价对应于系统寿命的相应阶段，区分为安全预评价和现时系统安全评价两大类。

1）安全预评价

安全预评价是指在系统开发、设计阶段，即在系统建成之前进行的危险性评价。安全工作最关心的问题是在事故发生之前是否能够预测到事故的发生、造成伤害或损失的危险性。而系统安全的优越性就在于能够在系统开发、设计阶段预测出系统中的危险源及其导致的事故，根除或减少危险源，使系统的危险性降至最小。

2）现实系统安全评价

现实系统安全评价是指在系统建成以后的运转阶段对系统进行的系统危险性评价。目的在于了解系统的现时危险性，为进一步采取降低危险性的措施提供依据。由于现时系统已经存在，并且根据以往的运行经验对其危险性已经有了一定的了解，所以与系统的安全预评价相比，评价结果将更接近于实际情况。

⑵ 统计评价和预测评价

在现时系统安全评价中又分为统计评价和预测评价两种类型。

1) 统计评价

统计评价是根据系统已经发生事故的统计资料来评价系统的危险性。由于是利用过去的资料进行评价，评价结果是以过去的情况为依据的，所以评价结果主要用于宏观指导事故的预防工作。

2) 预测评价

预测评价是在事故发生之前对系统进行的危险性评价，是在预测系统中可能发生事故的基础上对系统进行的危险性评价。它可以具体地指导事故预防工作。此种安全评价方法与前述的安全预评价方法是相同的，区别在于所评价的系统是处于其寿命期间不同的阶段。

⑶ 定性评价与定量评价

安全评价按其定量的程度，又可以分为定性评价和定量评价。在定量评价之中又分为半定量评价和定量评价。

从本质上说，安全评价是对系统危险性的评价，即回答系统的危险性是可接受的还是不可接受的，系统是安全的还是危险的。如果系统是安全的，则不必采取进一步的控制危险源的措施；否则，必须采取改进措施，以实现系统的安全运行。所谓的定性评价和定量评价、半定量评价是指在实际安全评价时是否将危险性指标进行了量化处理，处理到何种程度。

1) 定性评价

定性评价时，不对危险性进行量化处理而只作定性的比较。其常用的方法有：

①与有关的标准、规范或安全检查表对比，评价系统的危险程度。

②根据同类系统或类似系统以往的事故经验指定危险性分类等级。

定性评价比较粗略，一般用于整个安全评价过程中的初步评价。常用的分析评价方法有安全检查表法、预先危险分析、故障类型与影响分析、事件树分析、事故树定性分析等。

2) 定量评价

定量评价是在危险性量化基础上根据一定的算法和规则按生产过程各因素的赋值，算出确定数值的评价方法。它能够比较精确地描述系统的危险性，因而应用较为广泛。常用的分析评价方法有美国道法，英国蒙德法，日本六段法，我国易燃、易爆、有毒危险源评价法，事件树和事故树定量分析等。

3) 半定量评价

半定量评价是在实际经验的基础上，合理打分，根据分值或概率风险与严重度的乘积进行系统分级评价的方法。由于其可操作性强，且可分析出明确的

等级，得到了更加广泛的应用。适合于系统复杂，不确定性因素太多，具体数值难以估计的场合。常用的分析评价方法有，概率风险评价法、安全检查表打分法等。

安全检查表打分法就是将安全检查表中的结果一栏中的“是/否”，用标准分值和实际得分两栏代替，实现半定量的数字化评价。

8.2 安全评价方法简介

到目前为止,人们结合不同的工业领域和工艺过程已研究开发出了许多种系统安全状况的评价方法。各种评价方法纷繁复杂,大部分针对性较强,通用性较差。在具体的安全评价工作中应根据具体情况,选择合适的安全评价方法。

8.2.1 生产作业条件安全评价

生产作业条件的安全评价是对生产作业单元进行的危险性评价。生产作业单元是生产系统的基本单位，包括人员、设备、物质、星系等系统基本元素，具有系统的基本特征。生产作业条件的危险评价是系统安全评价的基础，其评价方法如下。

(1) LEC 评价法

LEC 评价法是针对在生产作业条件下，发生事故危险性的评价。该方法将发生事故的可能性 L、人员暴露情况 E 和发生事故后果的严重度 C 作为影响生产作业条件危险性的三个要素，分别确定三要素的评价等级分数，并按式(8-1)计算三者分数的乘积，从而得出生产作业条件的危险分值 D。

$$D = L \cdot E \cdot C \tag{8-1}$$

式中 D——生产作业条件危险性计算分值；

L——事故发生的可能性分值；

E——人员暴露情况分值；

C——事故发生的后果严重度分值。

各评价要素的打分情况如下：

1) 事故发生的可能性 L 的分值

事故发生的可能性是表明人们对生产作业中危险源控制程度的重要指标。即使充分控制了生产作业中的各种危险源，而绝对不发生事故的可能性也是不存在的。只能说由于控制措施得当，致使发生事故的可能性很小，以至于事故发生概率接近于零。因此，该方法规定实际不可能发生事故的情况的分值为 0.1；完全意外，极少可能的情况的分值规定为 1；完全可以预料将来某个时候会发生事故情况的分值规定为 10。在此基础上，规定出其他情况的对应分值。

表 8-1 给出了事故发生可能性的分值。

表 8-1 事故发生可能性分值表

事故发生可能性	完全会被预料到	相当可能发生	不经常，但是可能发生	完全意外，极少可能发生	可以设想，但是高度不可能发生	极不可能发生	实际上不可能发生
分值	10	6	3	1	0.5	0．2	0.1

2）人员暴露情况 E 的分值

人员在危险环境中暴露的事件越长，一旦发生事故受到意外释放能量或危险物质作用的机会就越多，受到伤害的可能性就越大，相应的危险性就越大。

根据生产作业所要求的人员在危险环境中出现的情况，规定人员连续出现在危险环境中的分值为 10；每年仅出现几次的情况为 1；其他暴露情况在两者之间取值；将人员非常罕见的出现在危险环境中的数值规定为 0.5，而不是 0。这是由于人员绝对不出现在危险环境中的情况无实际意义。具体分值见表 8-2 中所示。

表 8-2 暴露于危险环境分值表

暴露于危险环境情况	连续暴露于危险环境	逐日暴露于危险环境	每周一次或偶尔暴露于危险环境	每月一次暴露于危险环境	每年几次暴露于危险环境	非常罕见暴露于危险环境
分值	10	6	3	2	1	0.5

3）事故后果严重度 C 的分值

事故造成人员伤害和财产损失严重程度的变化范围较大，从个人的轻伤害到多人的死亡；从很小的损失到重大财产损失。由于范围较大，规定分值为 1 ~ 100 之间，将需要救护的轻微伤害或几乎无财产损失的情况规定为 1；将造成多人死亡或造成重大财产损失的情况规定为 100；其他情况取值均在 1 ~ 100 之间，如表 8-3 所示。

表 8-3 事故后果严重度分值表

事故可能后果	许多人死亡或重大财产损失	数人死亡或很大的财产损失	一人死亡或一定的财产损失	重伤或较小的财产损失	致残或很小的财产损失	需要治疗或不利于基本安全卫生要求
损失价值（万元）	> 500	100 ~ 500	30 ~ 100	20 ~ 30	10 ~ 20	1 ~ 10
分值	100	40	15	7	3	1

4）危险性大小 D 的分值标准

实际应用中将所选定的数据代入公式（8-1）之中，就可以计算出特定的生产作业条件下的危险性。根据经验，计算出的危险性分值在 20 分以下为低危险性，此时比骑自行车通过拥挤的马路去上班的危险性还要低些；计算出的危险性分值在 70～160 之间时，表明有显著的危险性，需要采取措施整改；计算出的危险性分值在 160～320 之间时，表明生产作业的条件是一种必须立即采取措施进行整改的高度危险的条件；计算的危险性分值大于 320 分以上时，表明生产作业条件异常危险，应该立即停止作业，必须彻底整改。危险性等级划分如表 8-4 所示。

表 8-4　危险性等级分值

危险程度	极其危险，不能继续作业	高度危险，需要立即整改	显著危险，需要整改	一般危险，需要注意	稍有危险，可以接受
危险性分值（D）	＞ 320	160～320	70～160	20～70	＜ 20
危险性级别	一级	二级	三级	四级	五级

【例 8-1】　假如工人每天操作一台没有安全防护装置的机器，有时不注意就会把手挤伤，以往曾经发生过这类事故，造成一只手残废，没有人员死亡。对其作业条件进行安全评价。

首先，确定各评价要素的分值：

事故发生的可能性属于“相当可能发生”，所以选取 L = 6；

人员暴露情况属于“逐日暴露于危险环境”，所以选取 E = 6；

发生事故后果的严重度属于“致残”，所以选取 C = 3。

于是，此种生产作业条件的危险性分值为：

$$D = L \cdot E \cdot C = 6 \times 6 \times 3 = 108$$

对照表 8-4 可知，属于显著危险性，等级为三级。需要整改。

该安全评价方法也可以用来评价多个不同生产作业条件下的危险性，以作为对不同生产作业条件采取改进措施轻重缓急的依据。

为了实际应用方便，根据前面的表格和公式做出如图 8-4 所示的安全评价诺模图。使用时，首先，按选出的各要素的分值在图上找出相应的点；再通过事故发生可能性分值点和暴露情况分值点做出直线交于辅助线上做一辅助点；最后通过该辅助点与事故后果严重度分值点做直线交于危险分数线的交点即为要求解的危险性得分值。在图 8-4 上危险分值线的右侧列出了危险性的评价结果。

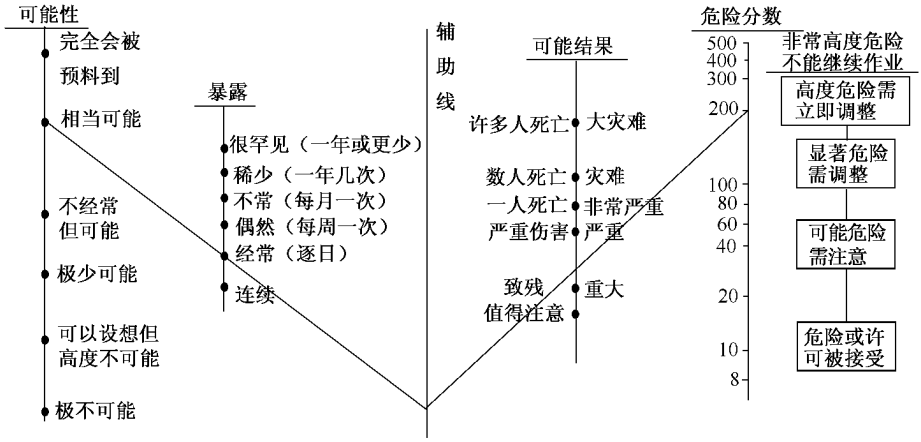


图 8-4　生产作业条件安全评价诺模图

(2) MES 评价法

MES 评价法是对 LEC 评价法的改进。该方法将 LEC 评价法中的事故发生可能性 L 改为了控制措施的状态 M，将事故后果的严重度要素 C 中的人员伤害程度、设备财产损失情况进行了调整并将其用 S 表示，同时增加了职业病发病状况、环境影响状况两项影响因素，制定了其取分标准，将 LEC 评价法的危险分值 D 的评价标准进行了改进并用字母 R 来表示之。经改进后的计算公式为：

$$R = M \cdot E \cdot S \tag{8-2}$$

式中　R——生产作业条件的危险程度计算分值；

M——控制设备状态的分值；

E——人员暴露情况分值；

S——事故后果严重程度分值。

各要素的打分情况如下：

1）控制措施的状态 M

其打分标准如表 8-5 所示。

表 8-5　控制措施状态分值表

控制措施的状态	无控制措施	有减轻后果的应急措施，包括报警系统	有预防措施，如机器防护装置等
分值标准	5	3	1

2）人员暴露情况 E

其打分标准与 LEC 评价法相同，此不赘述。

3）事故后果严重程度 S

其打分标准如表 8-6 所示。

表 8-6　事故后果严重程度分值表

环境影响程度	有重大环境影响的不可控排放	有中等环境影响的不可控排放	有较轻环境影响的不可控排放	有局部环境影响的可控排放	无环境影响
财产损失状况	> 1 亿元	1000 万 ~ 1 亿元	100 万 ~ 1000 万元	10 万 ~ 100 万元	< 10 万元
职业病状况		职业病（多人）	职业病（1 人）	职业性多发病	身体不适
人身伤害情况	有多人死亡	有 1 人死亡	永久失能伤害	需治疗，缺工	轻微，仅需救护
分值标准	10	8	4	2	1

4）生产作业条件的危险程度 R

其打分标准如表 8-7 所示。

表 8-7　危险等级分值

单纯财产损失事故	30 ~ 50	20 ~ 24	8 ~ 12	4 ~ 6	< 3
有人身伤害事故	> 180	90 ~ 150	50 ~ 80	20 ~ 48	< 18
分级标准	一级	二级	三级	四级	五级

（3）MLS 评价法

MLS 评价法是对 MES 评价法和 LEC 评价法的进一步改进。经与 MES 评价法、LEC 评价法相比较，该方法的评价结果更接近于实际情况。该评价方法的计算公式为：

$$R = \sum_{i=1}^{n} M_i L_i \left(S_{i1} + S_{i2} + S_{i3} + S_{i4}\right) \qquad (8\text{-}3)$$

式中　R——生产作业条件的危险程度计算分值；

n——危险因素的个数；

M_i——对第 i 个危险因素的控制与监控措施 $M_i = M_{i1} + M_{i2}$，其具体取值见表 8-8：

表 8-8　第 i 种危险因素的控制与监控状态 M_i

分数取值	检测措施（M_{i1}）	控制措施（M_{i2}）
5	无监测措施或被监测到的概率 < 10%	无控制措施
3	有高于 50%的事故可以被监测到	有减轻后果的应急措施，包括警报系统
1	肯定能被监测到	有行之有效的控制措施

L_i ——作业区域的第 i 种危险因素发生事故的频率，其具体取值见表 8-9：

表 8-9　第 i 种危险因素的事故发生频率 L_i

分数取值	暴露于危险环境的频率	分数取值	暴露于危险环境的频率
365	约每天发生 1 次	2	约半年发生 1 次
52	约每周发生 1 次	1	约一年发生 1 次
12	约每月发生 1 次	1/n	n 年发生 1 次

S_{i1} ——第 i 种危险因素发生事故可能造成的一次性人员伤亡损失（死亡 1 人按 20 万元计算，重伤 1 人按 10 万元计算，轻伤 1 人按 3500 元计算，再少时按实际损失计算）；

S_{i2} ——第 i 种危险因素存在带来的职业病损失（不管发生事故与否，按在工作单元内 1 年中用于该种职业病的费用总和）；

S_{i3} ——第 i 种危险因素诱发的事故造成的财产损失；

S_{i4} ——第 i 种危险因素诱发的环境累计污染及一次性事故的环境破坏造成的损失。

MLS 评价法充分考虑了待评价区域的生产作业条件及各种危险因素和所造成事故的严重度；在考虑了危险源固有的危险性之外，还反映了事故监控和控制措施的指标；在事故严重度计算中考虑了可能造成的人员伤亡、财产损失、职业病情况、环境破坏的总的影响。

MLS 评价法的评价分级见表 8-10。

表 8-10　MLS 评价法危险分级

危险分级	一级危险	二级危险	三级危险
分级数值	R > 30	R > 15	R > 5

8.2.2　危险物质加工处理安全评价

易燃易爆、有毒有害危险物质（其中包括大量的化学物质）具有较高的危险性，在加工处理、运输储存的过程中为保证安全必须采取严格的控制措施。危险物质加工处理的安全评价将为采取危险源有效控制措施提供可靠的依据。

(1) 火灾爆炸指数评价法（道法）

火灾爆炸指数评价方法的评价程序如图 8-5 所示。火灾爆炸指数评价法是美国道化学公司开发的一种在世界范围内有广泛影响的危险物质加工处理安全

评价方法，也称为道法。

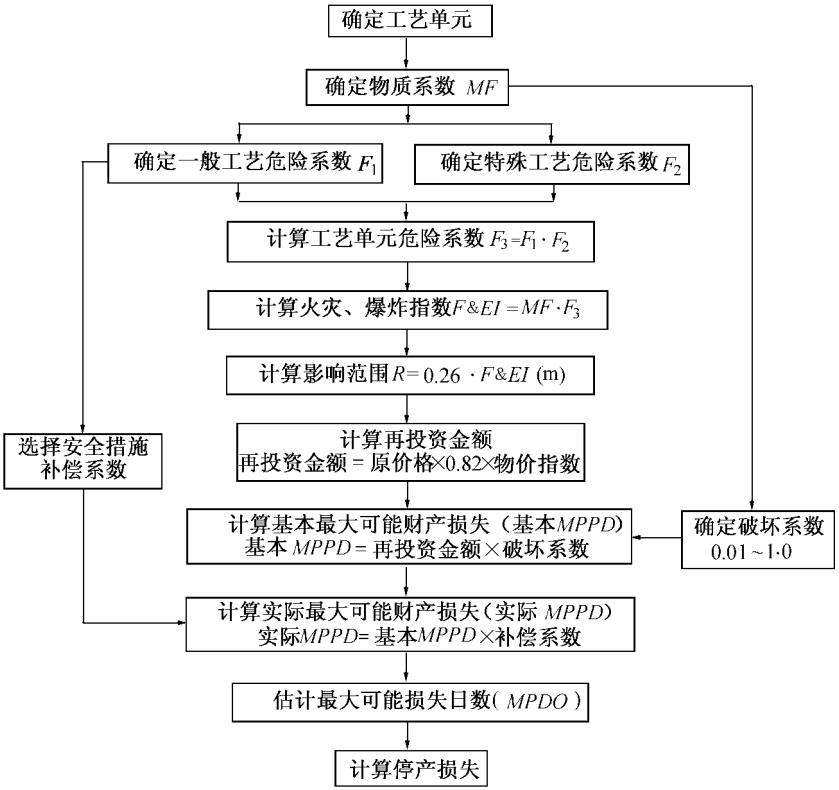


图 8-5　美国道法安全评价程序

在应用道法进行安全分析评价时，需准备如下资料：

1）装置系统的设计方案；

2）装置系统的工艺流程图；

3）道法评价时的所有安全评价表格，它们包括：

①火灾爆炸指数计算表。该表对一般工艺和特殊工艺中的危险物质指定了危险系数范围，具体数据参照选取。

②安全措施补偿系数表。该表对工艺控制安全补偿系数、物质隔离安全补偿系数、防火设施安全补偿系数的补偿范围给出了参考值。总补偿系数是上述三者之积。

③工艺单元危险分析汇总表。此表中需填写出工艺单元的火灾爆炸指数、暴露半径、暴露面积、暴露区内财产价值、危害系数、基本最大可能财产损失、安全措施补偿系数、实际最大可能财产损失、最大可能停工天数、停产损失数据。

④生产装置危险分析总汇总表。在此表中，对各工艺单元的危险损失进行汇总。

⑤工艺设备及安全成本计算表。

同时，国际劳工组织推荐了道法的简化法，即单元危险性快速排序法。由于该方法与道法相类似，在这里不再赘述。

(2) 火灾爆炸毒性指数法 (蒙德法)

在道法基础上，由英国帝国公司蒙德部进行了补充，开发出了另一种火灾爆炸毒性指数安全评价法，简称蒙德法。其评价程序如图 8-6 所示。

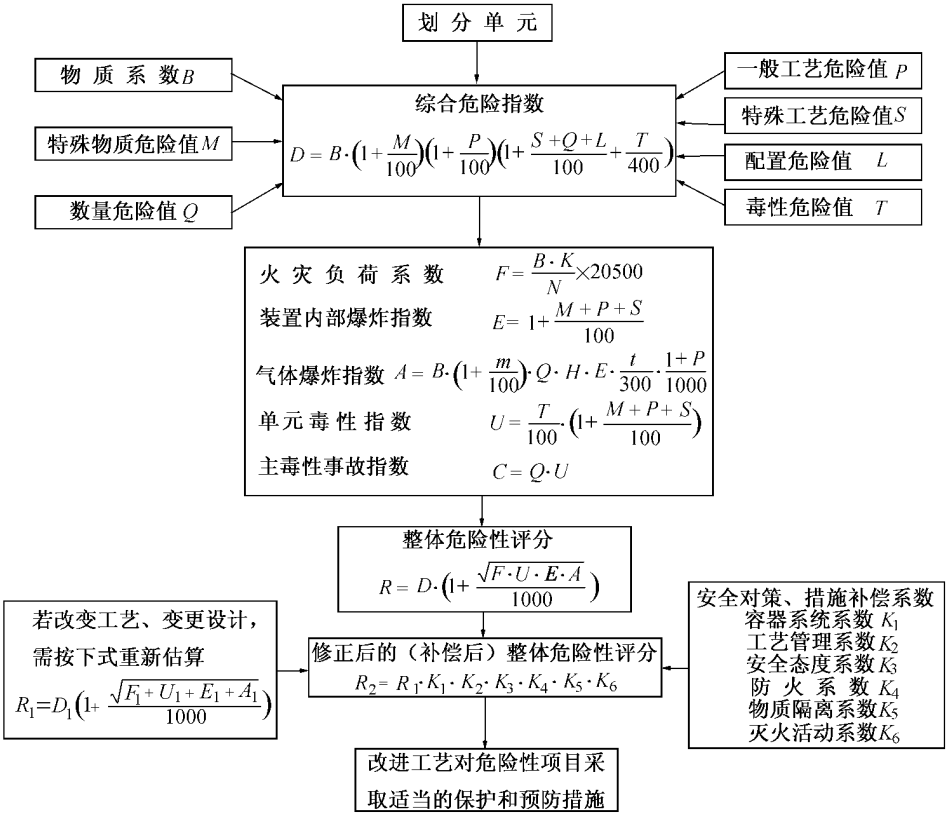


图 8-6 英国蒙德法安全评价程序

火灾爆炸毒性指数法 (蒙德法) 所计算的指标包括：总评价指标、火灾潜在性评价指标、爆炸潜在性评价指标 (包括内部单元爆炸指标、地区爆炸指标)、毒性危险性评价指标以及总危险性系数指标。各指标的评价标准见表 8-11 ~ 表 8-17 所示。

表 8-11　总指标 D 的范围及危险性

D 值范围	0 ~ 20	20 ~ 40	40 ~ 60	60 ~ 75	75 ~ 90	90 ~ 115	115 ~ 150	150 ~ 200	> 200
整体危险性	缓和的	轻度的	中等的	稍重的	重　的	极端的	非常极端的	潜在灾难性	高度灾难性

表 8-12　火灾负荷 F 及火灾持续时间

火灾负荷 F （$Btu \cdot ft^{-2}$）	危险性程度	预计火灾持续时间 （h）	备　注
$0 \sim 5 \times 10^4$	轻	1/4 ~ 1/2	
$5 \times 10^4 \sim 10^5$	低	1/2 ~ 1	住宅
$10^5 \sim 2 \times 10^5$	中等	1 ~ 2	工厂
$2 \times 10^5 \sim 4 \times 10^5$	高	2 ~ 4	
$4 \times 10^5 \sim 10^6$	非常高	4 ~ 10	建筑物
$10^6 \sim 2 \times 10^6$	强的	10 ~ 20	橡胶仓库
$2 \times 10^6 \sim 5 \times 10^6$	极端的	20 ~ 50	
$5 \times 10^6 \sim 10^7$	非常极端的	50 ~ 100	

注：$1 Btu \cdot ft^{-2} = 11.36\ kJ \cdot m^{-2}$

表 8-13　内部单元爆炸指标值 E 及其分类

E 值	0 ~ 1	1 ~ 2.5	2.5 ~ 4	4 ~ 6	> 6
程度	轻微	低	中等	高	非常高

表 8-14　地区爆炸指标值 A 及其分类

A 值	0 ~ 10	10 ~ 30	30 ~ 100	100 ~ 500	> 500
程度	轻	低	中等	高	非常高

表 8-15　单元毒性指标值 U 及其分类

U 值	0 ~ 1	1 ~ 3	3 ~ 6	6 ~ 10	> 10
程度	轻微	低	中等	高	非常高

表 8-16　主毒性事故指标值 C 及其分类

C 值	0 ~ 20	20 ~ 50	50 ~ 200	200 ~ 500	> 500
程度	轻	低	中等	高	非常高

表 8-17　总危险性系数 R 及其分类

R 值	0 ~ 20	20 ~ 100	100 ~ 500	500 ~ 1100	1100 ~ 2500	2500 ~ 12500	12500 ~ 65000	> 65000
分类	缓和	低	中等	高 1 类	高 2 类	非常高	极端	非常极端

与火灾爆炸指数法（道法）一样，在用火灾爆炸毒性指数法（蒙德法）评价之前也必须准备一批特定的数据取值表和系统资料，同时评价人员应具有丰富的专业知识和良好的判断能力。

(3) 六阶段安全评价法

六阶段安全评价法是日本劳动省研究开发的一种针对危险物质加工处理的危险性评价方法。该方法将评价过程分成六个阶段，故简称为六阶段法。其评价的步骤如下：

1) 有关资料整理和讨论

为了进行事先评价，必须将有关资料整理并讨论。这些资料主要包括建厂条件、物质的物理化学特性、工程系统图、各种设备情况、操作要领、人员配备、安全教育计划等。

2) 定性评价

对设计和运转的各个部分进行定性评价，设计部分共包括有 29 个评价项目，运转部分共包括了 34 个评价项目。

3) 定量评价

将评价系统分成几道工序，再将每道工序中各单元的危险度定量，以其中最大的危险度作为本工序的危险度。

单元的危险度由物质、容量、温度、压力和操作 5 个项目确定。其每个项目的危险度分为：0、2、5、10 四个分值。对各个项目赋以分值，最后按照各项目赋以的分值相加便可得到单元的危险度等级，如下式所示。

$$\{\text{危险性 R}\} = \left\{\begin{matrix}\text{物质 E}\\ 0\sim10\end{matrix}\right\} + \left\{\begin{matrix}\text{容量 F}\\ 0\sim10\end{matrix}\right\} + \left\{\begin{matrix}\text{温度 C}\\ 0\sim10\end{matrix}\right\} + \left\{\begin{matrix}\text{压力 H}\\ 0\sim10\end{matrix}\right\} + \left\{\begin{matrix}\text{操作 I}\\ 0\sim10\end{matrix}\right\} \tag{8-4}$$

计算出的数值与分级表 8-18 相对比，得到危险性 R 的等级。

表 8-18　危险度分级

危险情况	高度危险	中度危险	低度危险
分值范围	$R\geqslant16$	$11\leqslant R\leqslant15$	$1\leqslant R\leqslant10$
分　级	1	2	3

4）安全措施

根据各道工序评价出的危险度等级，从设备上和管理上采取相应的措施。其中，设备方面的措施有 11 种安全装置和防火装置，管理方面的措施有人员安排、教育训练、维护检修等内容。

5）由事故案例进行再评价

按照第四步讨论了安全措施之后，再参照同类系统以往的事故案例评价其安全性。必要时，再进行安全措施的讨论。属于 2、3 级危险度的系统，到此评价完毕。

6）用事故树进行再评价

属于第 1 级危险度的系统，进一步应用事故树进行再评价。

通过安全性的再评价过程，如果发现还需要改进时，采取必要的措施后再投入建设。

（4）化工企业安全评价法

此种方法是用企业的危险指数和企业安全系数共同评判企业的危险状况的方法。具体评价过程如下：

1）企业危险指数 D

$$D = \frac{1}{n}\sum_{i=1}^{n} D_i \qquad (8\text{-}5)$$

式中 D_i——某单元危险性指数，取决于燃烧爆炸、毒性和机械伤害危险性。

2）企业安全系数 C

$$C = \frac{S}{D} \times 100 \qquad (8\text{-}6)$$

式中 S——企业安全指数，取决于单元安全指数、综合管理安全系数。

3）企业危险等级划分

见表 8-19。

表 8-19 危险等级划分

危险等级	1 级	2 级	3 级	4 级	5 级
取值范围	D≥600	600 > D≥450	450 > D≥250	250 > D≥50	50 > D

4）企业安全等级划分

见表 8-20。

表 8-20 安全等级划分

安全等级	1 级	2 级	3 级	4 级	5 级
取值范围	C≥95	95 > C≥80	80 > C≥65	65 > C≥50	50 > C

⑸ 易燃、易爆、有毒重大危险源安全评价法

该评价方法是从物质危险性、工艺危险性入手分析了重大事故发生的原因、条件后，对系统发生事故的影响范围、伤亡人数和经济损失进行的评价。在该方法中从工艺设备、人员素质和安全管理三个方面出发，设定了 107 项指标，组成了评价指标体系。该评价方法的数学模型如下：

$$A = \left\{ \sum_{i=1}^{n} \sum_{j=1}^{m} (B_{111})_i \cdot W_{ij} \cdot (B_{112})_j \right\} \cdot B_{12} \cdot \prod_{k=1}^{3} (1 + B_{2k}) \qquad (8\text{-}7)$$

式中 $(B_{111})_i$ ——第 i 种危险物质的事故易发生系数；

$(B_{112})_j$ ——第 j 种工艺过程的事故易发生系数；

W_{ij} ——第 i 种危险物质的危险性与第 j 种工艺过程危险性的相关系数；

B_{12} ——事故后果的严重程度；

B_{2k} ——危险性抵消因子。

危险性抵消因子主要依据三个方面的因素取值：

1) 工艺、设备、容器与建筑物的状况；

2) 人员的素质；

3) 安全管理的水平。

易燃、易爆、有毒重大危险源安全评价法的评价流程如图 8-7 所示。

用该方法评价时，可较准确地评价出系统内的危险物质、工艺过程危险程度、危险等级及事故后果的严重程度。

8.2.3 概率危险性安全评价

概率危险性安全评价是以某种伤亡事故或财产损失事故的发生概率为基础进行的系统危险性评价方法。该方法主要采用定量的系统分析方法中的事件树分析、事故树分析等方法，计算系统事故发生的概率，确定安全目标，然后将所计算的事故发生的概率与所确定的目标值相比较，从而评价系统的危险性。

由于此种评价方法需耗费大量人力、物力和时间，所以较适合于那些不允许发生事故的系统、安全性受到世人瞩目的系统、会造成多人死亡的系统以及严重污染环境的系统。

⑴ 概率危险性安全评价的程序

关于概率危险性安全评价的评价程序如图 8-8 所示。

整个评价过程包括了系统内危险源的辨识、估算事故发生的概率、推算事故后果、计算危险度、与事先所设定的安全目标值相比较等一系列的工作。

在概率危险性评价中，广泛应用事件树分析和事故树分析等系统定量安全分析方法分析辨识危险源，计算系统事故发生概率。

应用后果分析方法推测重大危险源导致事故后果的严重程度。通常概率危

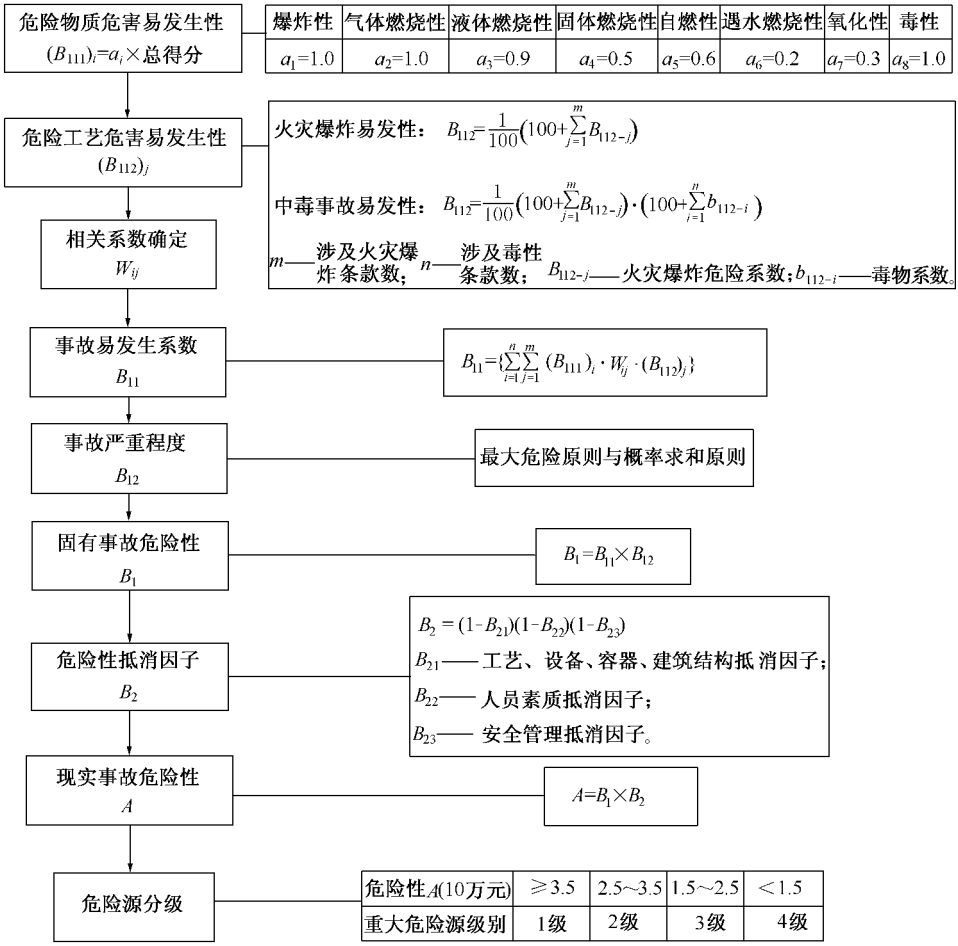


图 8-7　易燃、易爆、有毒重大危险源安全评价流程

险性评价包括计算危险度和设定安全目标两项主要工作。前者在于定量描述系统的危险性，后者在于确定可接受的危险水平。

⑵ 危险性的量化

应用概率危险性安全评价时，往往以危险度作为衡量指标类，客观地描述系统的危险程度。通常危险度定义为事故发生概率与事故后果严重度的乘积，即：

$$D = P \cdot C \tag{8-8}$$

式中　D——系统的危险程度，称为危险度；

P——给定时间间隔内系统事故发生的概率；

C——事故后果的严重程度，称为严重度，可以用经济损失金额、反映人员伤害严重程度的损失工作日数以及伤亡人数表示。

值得注意的是，对于相同的危险度数值，可能会有许多种事故发生概率与事故后果严重度的组合乘积。如前所述，某企业每年发生死亡 1 人的事故 10 起和每年发生死亡 10 人的事故 1 起，分别按上式计算的危险度是相同的。但是，人们主观上将更重视后者。

为了强调事故后果严重度的社会心理影响，常取下式计算系统危险度：

$$D = P \cdot C^k \qquad (k > 1) \tag{8-9}$$

式中 k——社会心理影响指数，是一个大于 1 的数，当社会影响力越大时，该指数值越大。

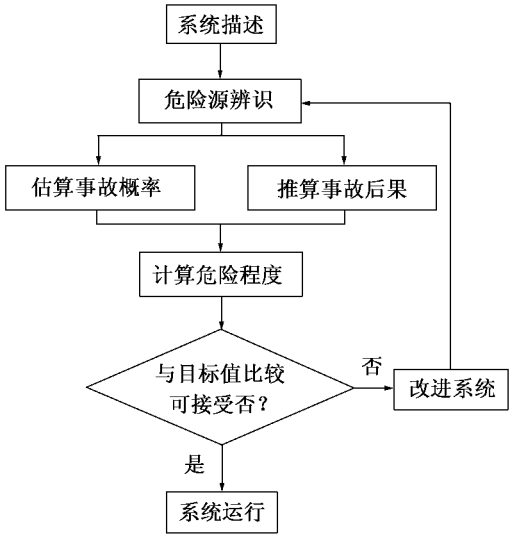


图 8-8 概率危险性安全评价程序

系统事故可能带来不同形式和不同严重度的后果，并且各种形式后果及其不同严重度相应地有不同的发生率。在这种情况下，用累积概率分布函数或危险曲线来描述危险性更符合实际，更容易比较。

设在给定的时间间隔内，严重度在 x_i 和 $x_i + dx_i$ 之间的第 i 类后果的事故发生概率为 $R(x_i)$，则严重度不超过 x_i 的第 i 类后果的事故发生累积概率为：

$$D(\leqslant x_i) = \int_0^{x_i} R(x_i)\,dx_i \tag{8-10}$$

各种严重度的第 i 类后果的事故发生累积概率为：

$$D_i = \int_0 R(x_i)\,dx_i \tag{8-11}$$

如果事故可能带来 n 类结果，则各种严重度的所有种类后果事故发生累积概率为：

$$D = \sum_{i=1}^{n} a_i \int_0 R(x_i)\,dx_i \tag{8-12}$$

式中 a_i——累计因子，用以将不同种类的后果（人员伤亡、财产损失、

环境污染）折算成统一的指标。

（3）安全目标的确定

在进行概率危险性评价时，确定安全目标是非常困难的工作。目前确定安全目标的方法有如下三种。

1）根据可接受的个人危险或集体危险来确定安全目标

在确定安全目标时，要划定可接受的危险和不可接受的危险之间的界限。按社会对危险性的认识，可以把危险分为三类：

①过渡性的危险。必须立即采取措施降低其危险性。

②正常性的危险。只要经济上合理、技术上可能，就可以采取措施降低其危险性。

③可接受的危险。如果采取措施降低其危险性显得有些浪费。

在考虑可接受的危险时，往往以疾病或其他灾害的死亡率作为参考值。通常，可接受的危险应低于疾病的死亡率而高于自然灾害的死亡率。

2）根据经济性确定安全目标

系统安全的目标是使系统在规定的功能、成本、时间范围内具有的危险性最小。因此，在系统的危险性和经济性之间有个最协调、最优化的数值。根据经济性确定安全目标是把个人或企业承担的危险与获得的利益相比较，考虑每项活动的得失，优化财力分配，使系统的危险性减小到合理的程度。

当把危险性用个人或企业从事某项有危险的活动获得的效益表示，确定安全目标的方法称作为“危险-效益”法；当把降低危险性的成本用所期望获得的效益表示，确定安全目标的方法称作为“成本-效益”法。

当评价一项减少事故发生概率或减轻事故后果严重度所采用的安全措施时，可按下式计算其成本-效益率：

$$B = \frac{M}{D - D'} \tag{8-13}$$

式中 M——所采取安全措施的成本；

D——采取安全措施前的危险度；

D′——采取安全措施后的危险度。

该式的意义应为，采取措施减少每个危险度所消耗的成本。

3）根据事故统计结果确定安全目标

根据统计数据确定安全目标的方法在实际的安全评价中得到了广泛的应用。一般情况下，根据以往的事故统计资料，依据经济上合理、技术上可行的原则来确定安全目标。

我国确定安全评价的目标时，是以本地区、本行业前三年到前五年的事故

统计平均值为基准，然后遵照国家和上级的要求，参照其他地区和行业的状况制定。

例如，按我国规定，若晋升为国家级企业其各行业的死亡率指标应为：化工生产企业≤0.10；钢铁生产企业≤0.090；林业采伐运输≤0.150～0.300；石油化工企业≤0.070；石油天然气油田企业及油田勘探企业≤0.130；国有统配煤矿2.8人/百万吨；地方国营煤矿6.5人/百万吨。

8.2.4 模糊安全评价

模糊安全评价法是利用模糊数学这一工具，对所研究的系统进行危险性分析，对其安全状况进行评价的方法。

任何一个系统的安全状况都要受许多因素的影响。如一个企业的安全状况可用其伤亡事故的多少，安全管理水平的高低，安全教育效果的好坏，安全技术装备的优劣，生产环境和劳动卫生条件的完善与不完善等因素进行综合评价。而这些因素还要由一系列子因素决定，如伤亡事故情况可用千人负伤率，千人重伤率，千人死亡率，百万吨产量死亡率等指标来衡量；安全管理水平则需要用企业领导安全意识的高低，专业人员的素质等子因素来评价。这些因素和子因素不仅数量众多、作用不同，而且多数都很难用经典的数学方法进行描述。又如企业领导的安全意识，安全工作的重视程度，只能用很重视、比较重视、一般、重视不够和忽视一类的模糊概念进行描述。

在系统安全评价过程中，存在着大量的模糊概念和模糊的量需要分析研究。模糊数学的发展为系统安全分析与评价提供了有力的工具。

(1) 模糊安全评价的数学模型

模糊安全评价的基本程序如下：

1) 建立综合因素的评价集合

将表明某系统安全状况且具有特定属性的因素（V_1，V_2，…，V_n）的全体称作综合因素评价集合 V：

$$V = \{V_1, V_2, \cdots, V_n\}$$

2) 分配各评价因素的权重

每个因素都从某一方面表达了系统的安全状况，但各因素对系统的影响程度且有所不同。根据各因素的影响程度，对其配以不同的权重：

设系统中各因素为：V_1，V_2，…，V_n

则各自分配的权重为：a_1，a_2，…，a_n　　$(0 \leqslant a_i \leqslant 1)$

$$\sum_{1}^{n} a_i = 1$$

设 A 为综合权重分配集合，则：

$$A = \{a_1, a_2, \cdots, a_n\}$$

3）建立子因素的评价集合 V_i

由于因素 V_i 还受到各子因素 v_1，v_2，…，v_k 的影响，所以子因素评价集合写成：

$$V_i = \{v_{i1}, v_{i2}, \cdots, v_{ik}\}$$

4）分配各子因素的权重

应根据子因素的影响大小，对其分配权重。

假设各子因素为：v_1，v_2，…，v_k

各子因素分配的权重为：u_1，u_2，…，u_k

则有子因素权重分配集合为：

$$u = \{u_1, u_2, \cdots, u_k\}$$

5）建立评价矩阵

请专家对各子因素状况进行评价。如有 100 位专家对因素 V_i 按下列五个分级进行评价，其结果如表 8-21：

表 8-21　评分等级表

评价等级	好	较好	中等	较差	差	总计
投票人数	10	20	50	15	5	100
比例 r_{ij}	$r_{11}=0.1$	$r_{12}=0.2$	$r_{13}=0.5$	$r_{14}=0.15$	$r_{15}=0.05$	1.00

设评价矩阵为 R_i，则：

$$R_i = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{k1} & r_{k2} & \cdots & r_{km} \end{bmatrix}$$

6）求综合评价矩阵 B_i

$$B_i = A_i \cdot R_i$$

7）求总评价矩阵 B

$$B = [B_1 \quad B_2 \quad \cdots \quad B_n]^T$$

8）求总评价矩阵 C

$$C = A \cdot B$$

式中　A——综合权重分配集合。

9）求系统的总得分 f

$$f = C \cdot S^T$$

式中 S^T——综合评价集合 V 的级别分值。

10）综合评价系统的安全等级 （表 8-22）

表 8-22 安 全 等 级

系统安全得分	> 80	70 ~ 79	60 ~ 69	50 ~ 59	40 ~ 49	< 40
安全等级	很好	好	良好	中等	较差	差

（2）模糊安全评价的实例

某企业利用模糊安全评价法对本企业的安全状况进行了评价。按前述步骤评价过程和得到的结果如下：

1）建立综合因素评价集合 V

选择六个因素作为综合评价因素：

$V = \{V_1, V_2, V_3, V_4, V_5, V_6\}$

= {伤亡事故，安全管理，安全教育，安全技术，生产环境，劳动卫生}

2）各因素的权重分配

按各因素的影响程度分配的权重值为：

$$A = \{a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6\}$$

$$= \{0.30，0.20，0.15，0.15，0.10，0.10\}$$

3）建立评价矩阵 R_i

根据专家投票得各因素 V_i 的评价矩阵 R_i，如表 8-23 中的第 9 项所示。

4）求各因素评价矩阵

$$B_i = A_i \cdot B_i$$

其结果如表 8-23 中的第 10 项所示。

5）归一化处理

结果如表 8-23 中的第 11 项所示。

6）建立总评价矩阵 B

$$B = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{bmatrix} = \begin{bmatrix} 0.375 & 0.25 & 0.25 & 0.125 & 0 \\ 0.286 & 0.286 & 0.286 & 0.143 & 0 \\ 0.313 & 0.313 & 0.25 & 0.125 & 0 \\ 0.111 & 0.222 & 0.333 & 0.222 & 0.111 \\ 0.133 & 0.133 & 0.266 & 0.333 & 0.133 \\ 0.316 & 0.316 & 0.263 & 0.105 & 0 \end{bmatrix}$$

7）求系统评价矩阵 C

$$C = A \cdot B$$

因　　素　V_1，V_2，V_3，V_4，V_5，V_6

权重分配　0.30，0.20，0.15，0.15，0.10，0.10

$$A = \{a_1, a_2, a_3, a_4, a_5, a_6\} = \{0.3, 0.2, 0.15, 0.15, 0.1, 0.1\}$$

代入式中得：

$$C = [0.3, 0.2, 0.15, 0.15, 0.1, 0.1] \times \begin{bmatrix} 0.375 & 0.25 & 0.25 & 0.125 & 0 \\ 0.286 & 0.286 & 0.286 & 0.143 & 0 \\ 0.313 & 0.313 & 0.25 & 0.125 & 0 \\ 0.111 & 0.222 & 0.333 & 0.222 & 0.111 \\ 0.133 & 0.133 & 0.266 & 0.333 & 0.133 \\ 0.316 & 0.316 & 0.263 & 0.105 & 0 \end{bmatrix}$$

通过矩阵计算得：

$$C = \{0.3, 0.25, 0.25, 0.15, 0.133\}$$

对其进行归一化处理：

因为　　$0.3 + 0.25 + 0.25 + 0.15 + 0.133 = 1.083$

$$C = \left\{\frac{0.3}{1.083}, \frac{0.25}{1.083}, \frac{0.25}{1.083}, \frac{0.15}{1.083}, \frac{0.133}{1.083}\right\}$$

$$= \{0.277, 0.231, 0.231, 0.138, 0.123\}$$

8）求系统总得分

上式表明，对系统的安全状况按五个等级评价时，所得结果的分布情况。如对各种等级都按表 8-24 以百分制打分，则可求得系统的总得分 f。

表 8-24　安全等级得分

分　　数	95	80	65	45	30
安全级别	好	较好	中	较差	差

$$f = C_1 S_1 + C_2 S_2 + C_3 S_3 + C_4 S_4 + C_5 S_5$$

$$= 0.277 \times 95 + 0.231 \times 180 + 0.231 \times 65 + 0.138 \times 45 + 0.123 \times 30$$

$$= 69.71$$

所以，该企业的安全情况属于“良好”等级。

8.2.5　人工神经网络安全评价法简介

该方法是借助于人工神经网络技术研究开发的安全评价方法。人工神经网

络技术是由人工建立的以有向图为拓扑结构的动态系统，它通过对连续或断续的信息输入作动态响应而实现信息处理。人工神经网络安全评价主要采用了多层结构的 BP 人工神经网络技术。

(1) BP 人工神经网络技术用于危险性评价的优点

1) 利用其并行结构和并行处理的特点，可以全面地评价系统的安全状况和多因素共同作用下的安全状况；

2) 利用其知识分布于整个系统的存储方式和自适应性的特点，可以补充学习样本，将过去的经验和新的知识结合，动态地评价系统的安全状况；

3) 利用其可容错的特点，通过适当的传递函数和数据结构，可以处理非数值性指标，对系统安全状态进行模糊评价。

BP 人工神经网络的安全评价过程如图 8-9 所示。

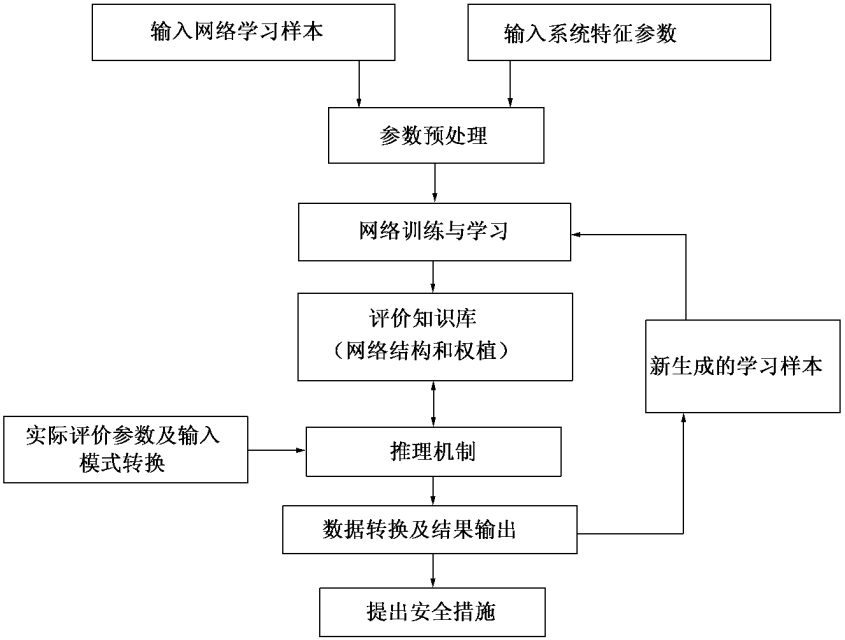


图 8-9 BP 人工神经网络安全评价过程框图

(2) BP 人工神经网络技术系统安全评价的步骤

1) 建立合适的多层网络结构；

2) 制定所评价系统的指标体系以及特征参数和状态参数；

3) 确定适宜的学习样本，建立合理的网络学习模式；

4) 确定合理的网络传递函数的形式；

5）建立系统危险性评价知识库；

6）运用系统危险性评价知识库的数据，通过神经网络推理评价系统的安全状况，得出评价结果。

7）评价结果又可作为神经网络的学习样本，进一步丰富系统危险性评价的知识库。

8.3 安全评价方法的比较

不同的安全评价方法具有不同的特点和不同的应用范围，在进行安全评价时，应根据评价系统的具体情况，选择适宜的安全评价方法。必要时，也可采用两种或两种以上的评价方法对某一特定的系统进行评价，做到互相弥补、互相验证，使评价结果更接近实际，提高系统安全评价的可靠性。

表 8-25 中归纳出了本章讨论的主要评价方法及其特点和应用范围，供选择时参考。

表 8-25 安全评价方法比较

评价方法	评价目标	定性/定量	特　　点	适用范围	基础要求	优缺点
LEC 法和 MES 法	生产作业条件的危险性等级	半定量	按标准给系统事故发生可能性、人员暴露情况、危险程度赋分，经计算评定危险等级	各类生产作业条件	熟悉系统，有生产和安全知识，实践经验	简单使用，易受主观因素的影响
MLS 法	生产作业条件的危险性等级	半定量	除危险源固有危险外，综合考虑监控与控制设施后计算评定危险性等级	各类生产作业条件	熟悉系统，有生产和安全知识，实践经验	简单使用，易受主观因素的影响
道法	危险物质加工处理的火灾、爆炸危险性指数、等级，事故损失	定量	计算火灾、爆炸指数，判定采取措施前后的系统整体危险性，计算系统整体经济损失	生产、储存、处理易燃、易爆、化学物质的工艺过程等	熟悉系统，有生产和安全知识，良好判断能力。有各类损失的控制目标值	图表简单明了，参数取值范围宽，受主观因素影响，系统整体评价

续表

评价方法	评价目标	定性/定量	特　　点	适用范围	基础要求	优缺点
蒙德法	危险物质加工处理的火灾、爆炸、毒物和系统整体危险性等级	定量	计算火灾、爆炸、毒性的危险指数，判定采取措施前后的系统整体危险性指数，评定各类危险性等级	生产、储存、处理易燃、易爆、化学有毒物质的工艺过程等	熟悉系统，有生产和安全知识，良好判断能力	图表简单明了，参数取值范围宽，受主观因素影响，系统整体评价
六阶段法	危险物质加工处理的危险等级	半定量	检查表定性评价，局部单元定量评价，类比资料复评，一级危险单元用事件树和事故树再评价	化工系统和有关单元装置	熟悉系统，有生产和安全知识，有类比资料	综合几种方法反复评价，准确性高，工作量大
化工企业评价法	危险物质加工的化工生产系统的危险等级和安全等级	半定量	根据燃烧爆炸危险性、毒物危险性、机械伤害危险性确定企业危险性指数，根据生产单元、管理安全系数确定企业安全系数。对照标准确定等级	各类化工企业	熟悉企业生产系统，有生产和安全知识，有类比资料	两指标分类，综合评价，工作量较大
易燃易爆有毒重大危险源评价法	重大危险源危险性等级	定量	从物质危险性和工艺危险性出发，分析重大危险源事故发生的原因、条件，评价事故影响范围和损失，提出预防、控制措施	生产、储运、加工易燃、易爆、有毒物质的工艺系统等	熟悉系统，有生产和安全知识，有相关数据	较为准确，计算量较大

续表

评价方法	评价目标	定性/定量	特　　点	适用范围	基础要求	优缺点
概率危险性评价法	计算系统危险度和确定安全目标	定量	应用事件树和事故树定量分析，辨识危险源，求算系统发生概率，推测事故后果严重程度，确定系统安全目标	世人瞩目的、不许发生事故的、出事多人伤亡或巨大污染的系统	熟悉系统，有生产和安全知识，有相关统计资料和数据基础	计算准确，工作量很大
模糊评价法	综合评价系统的危险等级	定量	将模糊行为的因素定量化、数字化，评价整个系统的安全状况，分出危险性等级	企业、生产单位等整体系统	熟悉系统，有生产和管理方面的安全知识，有专家的评定分值数据	结果准确，权重设置受主观因素影响，计算量较大
神经网络评价法	综合评价系统的危险性	半定量	仿照人脑动态分析，知识加工学习，思维推理，及时纠错，提出安全措施的能力	企业、生产单位等整体系统	熟悉系统，有生产和管理方面的安全知识，有专家的评定分值数据	结果准确，计算推理工作量较大，应用微机

思　考　题

1. 何谓可接受的危险？影响因素有哪些？
2. 什么是安全评价？主要内容有哪些？又是如何分类的？
3. 道法和蒙德法有何不同？
4. 六段评价法程序如何？
5. 选择一熟悉的加工工艺过程，应用生产作业条件安全评价的 LEC 法对其进行安全评价。

9 安全决策

9.1 概述

事件的发生受许多确定和不确定因素的影响，这时决策就起了重要的作用。决策在人们生活、工作中随时都会遇到。有些决策是简单的、容易的，例如出门利用哪种交通工具；到商店买何种式样、颜色、价钱的商品等。有些决策是复杂的、困难的，例如能源资源开发、经济发展战略和计划等。

什么是决策？决策可以理解为对拟订的若干个欲采用方案的选择，以期达到优化的目标。简单地说，决策就是作决定，决定策略和方法。既然决策就是作决定，那么从多个为达到同一目标的可行方案中选定最优方案时，就要求人们的选择和判断尽可能地符合客观实际。要做到这一点，决策者应尽可能真实地了解问题背景、环境和发展变化规律，占有详细的信息资料和正确地掌握决策方法。决策学是为决策提供科学的理论和方法，以支持和方便人们做决策的科学；是自然科学与社会科学并涉及人类思维的新兴交叉学科。

9.1.1 安全决策的概念及意义

所谓安全决策就是针对生产活动中需要解决的特定安全问题，根据安全标准、规范和要求，运用现代科学技术知识和安全科学的理论与方法，提出各种安全措施方案，经过分析、论证与评价，从中选择最优方案并予以实施的过程。

广义的决策，都是在价值判断的基础上做出选择，它的基本准则就是效用，离开了效用准则，决策是非理性的、盲目的。首先，安全的价值或效用是不容置疑的，可以说安全本身就是价值。其次，安全是相对的，所以安全的价值具有比较特性。另外，安全的价值是客观的，虽然，安全的社会效用、精神效用难以量化，但是安全的经济效用是可度量的。所以，安全决策同样是建立在安全价值判断基础上。

“管理就是决策”现代安全管理主要就是解决安全决策的问题。在现代安全管理中，面对许多安全生产问题，要求领导者能统观全局，立足改革，不失时机地做出可行和有效的决策，以期实现安全生产的目标。

9.1.2 安全决策的类型

在安全管理决策中，由于决策目标的性质、决策的层次和要求的差别，决策的类型很多。为了便于决策，必须确定在什么层次上进行，也就是说，一定要划定决策者与被决策对象的范围以及它们相互作用构成的决策系统与外界的联系(即与外界的物质、能量和信息的交换)。下面介绍几种常见的安全决策类型。

(1) 系统安全管理决策

是指解决全局性重大问题的高层决策，只要解决安全方针、政策、规划、安全管理体制、法规、监督监察及推进安全事业发展等方面的决策。

这类决策是基础性的决策，涉及的范围广、沿用的时间长，影响的面也比较大。

(2) 解决工程项目建设问题的决策

为了保证新建、改建、扩建的工程项目能安全地投入生产，对工程项目设计进行安全论证、审核与安全评价方面的决策。这里涉及厂址选择、厂房布局、厂房结构、工艺过程、设备布置、物资储运、防火防爆等一系列问题，必须对其一一做出决策。

(3) 企业安全管理决策

主要是为健全、改善和加强企业安全管理所进行的计划、组织、协调、控制以及预测和预防事故等方面的决策。这方面的决策不只是安全部门本身的事，它涉及企业的各个方面，应与企业的发展规划、生产任务、组织机构、工程计划、人员素质的提高等各方面综合加以考虑。

预测和预防事故是安全管理决策的主要课题之一。导致事故发生的直接原因是设备的不安全状态、人的不安全行为和作业的不良环境。预防事故的对策是采取有效的技术措施，加强安全教育和加强安全管理。人、机、环境是分析的对象和决策的依据，技术、教育、管理是预防事故的保证，它们之间因果联系如图 9-1 所示。

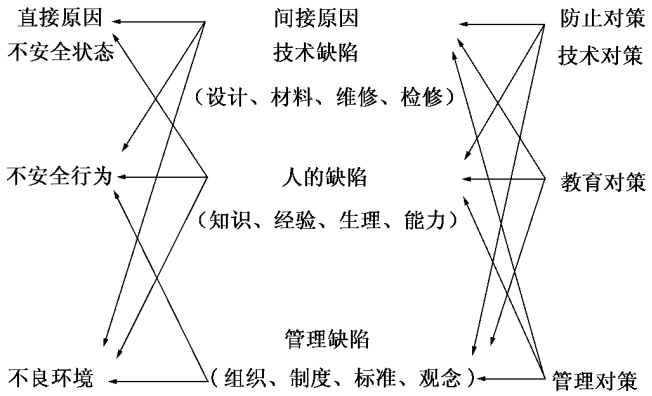


图 9-1 人、机、环境与技术、教育、管理对策的关系

⑷ 处理事故的决策

主要是在事故发生后采取的调查、分析、处理及改善与改进的对策。也就是发生事故时，做出如何抢救现场人员和控制事故发展并将之制止的决策。这样的决策必须迅速、果断，虽不可能万无一失，但也要尽可能完善，因为一秒之差就可能使灾害扩大，稍有失误也许会使更多的人伤亡和损失。

9.2 安全决策分析的任务和决策要素

9.2.1 决策分析的任务

找到了问题产生的根源不是目的，我们的目的是在调查研究、分析问题基础上，找到解决问题的方法与对策，即制定出最佳的决策与对策，这是管理人员日常最感困难而又最为繁重的工作。

对一个大的复杂问题，由于涉及面较广，因而需要慎重考虑、细致分析和认真比较。要做到这一点，一般来说，必须慎重考虑和回答下列问题：①制定对策，解决问题，希望达到哪些目标；②在这些目标中，哪些目标是主要的而必须达到，哪些目标是希望达到；③有多少可行方案可用于达到目标；④哪些方案可能达到决策目标；⑤哪些方案可能发生不良后果。

9.2.2 决策要素

决策的要素有：决策单元、准则体系、决策结构和环境、决策规则等。

⑴ 决策单元和决策者

决策者是指对所研究问题有权利、有能力做出最终判断与选择的个人或集体。其主要责任在于提出问题，规定总任务和总需求，确定价值判断和决策规划，提供倾向性意见，抉择最终方案并组织实施。所谓决策单元常常包括决策者及共同完成决策分析研究的决策分析者，以及用以进行信息处理的设备。他们的工作是接受任务、输入信息、生成信息和加工成智能信息，从而产生决策。

⑵ 准则（指标）体系

对一个有待决策的问题，必须首先定义它的准则。在现实决策问题中，准则常具有层次结构，包含有目标和属性两类，形成多层次的准则体系。

准则体系最上层的准则只有一个，一般比较宏观、笼统、抽象，不便于量化、测算、比较、判断。为此要将总准则分解为各级子准则，直到相当具体、直观，并可以直接或间接地选用具体的决策方案为止。在层次结构中，下层的准则比上层的准则更加明确具体并便于比较、判断和测算，它们可作为达到上层准则的某种手段。下层子准则的集合一定要保证上层准则的实现，子准则之

间可能一致，亦可能相互矛盾，但要与总准则相互协调。

⑶ 决策结构和环境

决策结构和环境属于决策的客观态势（情况）。为阐明决策态势，必须尽量清楚决策问题（系统）的组成、结构和边界条件，以及所处的环境。它需要标明决策问题的输入类型、数量，决策变量（包括各种备选方案）以及测量类型，决策变量（方案）和属性间以及属性与准则间的关系。

决策变量亦称可控（受控）变量，它是决策（评价）的客观对象。在自然系统中，决策变量常以表征系统主要特征的一组性能、参数形式出现，由它们可以组合出无限多个备选方案，其范围由一组约束条件所限制。决策变量又分为两种类型，即连续型和离散型。

决策的环境条件可以区分为确定性和非确定性两大类。确定性环境条件是指出现可能性很大的环境条件；非确定性环境条件是指出现可能性很小的环境条件。

⑷ 决策规则

在做出最终抉择的过程中，要按照方案结果进行择优排序。这种促使方案完全序列化的规则，便称为决策规则。

然而在多准则决策问题中，各种方案是不完全有序的，准则之间往往存在矛盾，如各准则的量纲不统一等。所以，各个准则均为最优的方案通常是不存在的。因而，决策者只能按独有的判断规则和以往的经验确定最终方案。

9.3 安全决策分析的基本程序

决策本身是一个过程。要做出科学的、正确的决策，应遵循必要的程序和步骤。安全决策与通常的决策过程一样，应按照一定的程序和步骤进行。不同的是，在进行安全决策时，应根据安全问题的特点，确定各个步骤的具体内容。

⑴ 确定目标

决策过程首先需要明确目标，也就是要明确需要解决的问题。决策目标就是所需要解决的问题，正确地确定目标是决策分析的关键。对安全而言，从大安全观出发，安全决策所涉及的主要问题就是保证人们的生产安全、生活安全和生存安全。但是，这样的目标所涉及的范围和内容太大了，以至于无法操作，应进一步界定、分解和量化。安全问题寓于生产过程之中，因此安全决策所涉及的主要问题就是保证安全生产，即防止事故发生、消除职业病和改善劳动条件三个基本目标。

例如：生产安全是一个总目标，它可以分解为预防事故发生、消除职业病

和改善劳动条件。而且，对已分解的目标，还应根据行业不同、现实条件不同（例如，经济保证、技术水平）、边界约束条件不同区分目标的实现层次及内涵。

另外，对于决策目标应有明确的指标要求；对于技术问题，应有风险率、严重度、可靠度系数以及事故率、时间域和空间域等具体量化指标；对于难以量化的定性目标，则应尽可能加以具体说明。

⑵ 区分目标

安全生产是一个总的目标，对一个具体行业或具体单位来讲，安全生产问题是多方面的。决策目标在尽可能详尽地列出后，应把所有目标区分为必须目标和期望目标。也就是说，哪些目标必须达到，哪些目标希望达到，必须区分清楚。

在区分目标时，应把边界划清，即划定安全与危险的边界、可行与不可行的边界以及确定现实条件（经济保证、技术保证）。也就是说，要把需要解决的问题的性质、种类、范围、时间、部位、约束条件等弄清楚，权衡整体的利弊得失，从而确定出先后顺序。

⑶ 制定对策

在目标确定之后应进行技术性的论证，其目的是寻求对实施手段与途径提出战术性的决策。在这个过程中，决策人员应用现代科学理论与技术对达到目标的手段进行调查研究、预测分析，进行详细的技术设计，拟出几个可供选择的方案。

⑷ 分析和权衡对策方案

各种对策方案制定出以后，就可根据目标进行分析。首先根据总目标和指标将那些不能完成必须目标的方案舍弃掉，对那些能够完成目标的方案保留下来，再用期望目标去权衡。考虑到每个方案达到的每个期望目标的程度，可用加权法来划分，求出每个方案的期望值权重，期望值权重大者，应为最优先的备选方案。

⑸ 备选决策提案

能够达到目标，并且对完成期望目标取得最大权重数的对策方案，称为备选决策提案。备选决策提案不一定是最后决策方案，需要经过技术评价和潜在问题分析（主要是不良影响分析），做进一步的慎重研究。

⑹ 技术评价与潜在问题分析

技术评价一般要考虑所选决策提案对自然和社会环境各种影响所导致的安全对策问题，应侧重在安全评价，对系统中固有的或潜在的危险及其严重程度进行分析和评价。对备选决策方案，决策者要向自己提出“假如采用这个方案，将要产生什么样的结果；假如采用这个方案，可能导致哪些不良后果和错

误”等问题，从这些可能产生的后果中进行比较，以决定方案的取舍。

对安全问题，考虑其决策方案后果，应特别注意如下一些潜在问题：

1）人身安全方面，能否造成工伤危险，是否有中毒危险，有无生命危险，有无导致疾病留下后遗症的危险，是否会加重人的疲劳，是否会带来精神紧张等。

2）人的精神和思想方面，是否会造成人的思想观念的变化，是否会造成人的兴趣爱好和娱乐方式的变化，是否会造成人的情绪和感情方面的变化，是否会加重人的疲劳，带来精神紧张，是否对个人生活和家庭生活产生影响，导致不安全和束缚感等。

3）人的行动方面，能否造成人的生活规律、生活方式的变化（多样化或单一化），能否影响生活的时间划分（劳动时间、休息时间、学习时间、家庭生活时间）等。

总之，对备选决策方案，决策者要向自己提出“假如采用这个方案，将要产生什么样的结果”“假如采用这个方案，可能导致哪些不良后果和错误”等问题。从一连串的提问中，发现各种可行方案的不良后果，把它们一一列出，并进行比较，以决定取舍。一旦选定决策方案，就决策过程而言，分析问题决策过程已告完结，但是要把解决问题的决策付诸实施，可以说还没有完成。

⑺ 实施与反馈

决策是为了实施，为了使决策方案在实施中取得满意的效果，决策方案在实施过程中应注意执行时要制定规划和进程计划，健全机构，组织力量，落实负责部门与人员，及时检查与反馈实施情况，使决策方案在实施中趋于完善并达到预期效果。

9.4 潜在问题分析

在决策方案确定之后和执行过程中，还要随时分析研究可能遇到的问题，以免影响方案的顺利执行。潜在问题分析就是预测所选择的方案和实施计划可能遇到的问题，同时找出问题的原因，制定预防措施、应变措施以及出现问题时的补救措施。在进行潜在问题分析时，应不断地提出几个问题：①未来可能发生哪些问题将影响决策目标？②发生这些问题的可能原因是什么？③有哪些预防措施可以消除产生这些问题的原因？④有哪些应变措施可以减少对决策目标的影响？⑤需要哪些情报资料来决定应变措施的实施？⑥如何反馈执行方案的进度？

潜在问题分析的基本程序与步骤：

1）预测潜在问题

应用预测方法预测未来可能发生哪些问题。任何管理人员在制定实施计划时，都希望这个计划能够顺利地完成。所以在制定计划时，对一些要素、单位、活动或步骤需要特别注意，以免出问题影响整个计划的进行。这些应该注意的地方，叫做“关键区域”。例如很复杂的生产装置、以前没有过先例的作业、操作人员没有经验、时间紧迫等万一失败产生后果严重的环节都叫做“关键区域”。管理人员找出这些关键区域之后，对区域内的一切活动，必须一一提出“哪些将会发生偏差”，并逐一做出确切的回答。根据这些答案，便可发现许多潜在的问题。

2）评价威胁性

要评价每个潜在问题对整个计划的威胁性，包括问题发生的可能性和影响的严重性，一般可用高、中、低三种程度来衡量。

3）制定预防措施

在确认了对整个计划威胁性比较大，而不希望将来会发生那些潜在问题之后，对其分析研究、采取措施。首先要找出出现问题的可能原因，再针对这些原因，进行重点分析研究，制定出相应的预防措施和应变措施。

4）指导实施心中有数

决策目标具体明确，完成目标的实施计划井然有序，潜在问题分析准确，应变措施周密、充足，只有这样，决策者对解决问题才能做到心中有数。但是，对于复杂的重大问题，决策者并非都能亲临现场进行指导和实践，这就是一个信息交流问题。首先，决策者应向下级管理人员指出执行这一计划的“关键区域”和其“关键点”。在执行计划达到“关键点”之前，要及时地将与预防措施和应变措施有关资料提供给执行计划的管理人员，指导其采取适当的措施。

一般情况下可按表 9-1 格式填写潜在问题分析的内容。

表 9-1　潜在问题分析表

项　　目	内 容 记 载
潜在问题	
可 能 性	
严 重 性	
责任及责任人	
潜在后果	
可能原因	

续表

项目		内容记载
预防措施		
应变措施		
进度计划	需要采取的应变措施	
	计划执行关键	

9.5 安全决策的方法

安全决策是一门交叉学科，它既含有从运筹学、概率论、控制论、模糊数学等引入的数学方法，也有从安全心理学、行为科学、计算机科学、信息科学引入的各种社会、技术科学。

根据决策环境，考虑属性量化程度，可以把多属性决策（MADM）问题区分为确定性和非确定性两类，相应的决策方法就有确定性多属性决策方法、定性与定量相结合的决策方法和模糊多属性决策方法。在安全决策中，针对所决策问题的性质、条件、风险性大小的不同，可以运用多种方法。

9.5.1 确定性多属性的决策方法

一种多属性决策方法就是一个对属性及方案信息进行处理选择的过程。该过程所用的基础数据主要是决策矩阵 A、属性 f_i（$j \in M$）和/或方案 x_i（$i \in N$）的偏好信息（倾向性）。决策矩阵 A 一般是由决策分析人员给出，它提供了分析决策问题的基本信息。需要指出的是，A 的元素形式上并非是定量化的，它们也可以是定性的，甚至是模糊的。但对于确定性多属性决策，则矩阵 A 是定量化的，f_j（$j \in M$）和/或 x_i（$i \in N$）的倾向性信息的量化一般是由决策者给出。根据决策者对决策问题提供信息的过程及充分程度的不同，可将确定多属性的决策方法归纳为：无倾向性信息的决策方法、属性倾向性信息的决策方法和方案倾向性信息的决策方法三类。鉴于安全决策问题的复杂性，本书只介绍几种无倾向性信息的决策方法，即筛选方案的方法。

（1）优势法

该方法的操作过程是，从备选方案集合 $R = \{x_1, x_2, \cdots, x_n\}$ 中任取两个方案，（记为 $\tilde{x}_1$ 和 $\tilde{x}_2$），若决策者认为 $\tilde{x}_1$ 劣于 $\tilde{x}_2$，则剔去 $\tilde{x}_1$，保留 $\tilde{x}_2$；若无法区分两者的优劣时，皆保留。将留下的方案与 R 中的第三个方案 $\tilde{x}_3$ 作比较，如果它劣于 $\tilde{x}_3$，则剔去前者，如此进行下去，经 n - 1 步后便确定了非劣

方案的解集合 $R^{\#}$。

(2) 连接法 (满意法)

该方法要求决策者对表征方案的每个属性提供一个可接受的最低值，称为切除值。只有当一个方案的每个属性值均不低于对应的切除值时，该方案才能保留。若方案 x 被接受，即有：

$$f_j(x) \geqslant f_j^0 \quad (j \in M,\ x \in R) \tag{9-1}$$

式中 f_j^0 —— j 个属性的切除值。

可见，切除值的规定是这个方法的关键所在，如果定得过高，将淘汰过多方案；定得太低，又会保留过多方案，可按下列方式来确定切除值。令 r 为被淘汰方案的比例，P_c 为任一随机选出的方案的概率。设两者的关系为 $r = 1 - P_c^m$，则有：

$$P_c = (1 - r)^{1/m} \tag{9-2}$$

例如：若 $m = 6$，$r = 0.75$，则 $P_c = (1 - 0.75)^{1/6} = 0.79$。即对每个属性所设定的切除值应保证有至少 79% 的方案数对应的属性值超过该切除值。另外，也可以用迭代法由低到高逐步提高切除值，直到得到所希望保留的方案数为止。

(3) 分离法

该方法用来筛选方案时仍要对每个属性设定切除值，但和连接法不同的是，并不要求每个属性值都超过这个值，只要求方案中至少有一个属性值超过切除值就被保留。按此原则方案 x，即满足：

$$f_j(x) \geqslant f_j^d \quad (\text{当 } j = 1 \text{ 或 } 2 \text{ 或} \cdots \text{或 } m,\ x \in R) \tag{9-3}$$

式中 f_j^d ——规定的切除值。

总起来看，分离法保证了凡在某一属性上占优势的方案皆被保留，而连接法则保证了凡在某一属性上处于劣势的方案皆被淘汰。显然，它们虽不宜用于方案排序，但却可以保证经上述两种方法筛选后，方案集合 R 中所剩的方案已基本上是非劣方案。

【例 9-1】 设某生产线，安全技术改造方案所涉及的各种因素的集合见表 9-2。

表 9-2 安全技术改造方案集合

备选方案 x_i	属性 (f_j)					
	最大生产量 f_1	多品种生产性 f_2	可靠性 f_3	自动化程度 f_4	安全技术改造费 f_5/元	风险率 f_6
x_1	20	中	中等	中等	900 万	10^{-6}

续表

备选方案 x_i	属　性 (f_j)					
	最大生产量 f_1	多品种生产性 f_2	可靠性 f_3	自动化程度 f_4	安全技术改造费 f_5/元	风险率 f_6
x_2	25	低	低	低	1200 万	10^{-3}
x_3	18	高	高	高	1000 万	10^{-4}
x_4	22	中	中等	中等	950 万	10^{-4}

该安全技术改造问题决策矩阵为：

$$A=\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}\begin{array}{c} \begin{array}{cccccc} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \end{array} \\ \begin{bmatrix} 20t & 中 & 中 & 中 & 900\text{ 万元} & 10^{-6} \\ 25t & 低 & 低 & 低 & 1200\text{ 万元} & 10^{-3} \\ 18t & 高 & 高 & 高 & 1000\text{ 万元} & 10^{-4} \\ 22t & 中 & 中 & 中 & 950\text{ 万元} & 10^{-4} \end{bmatrix} \end{array}$$

【解】

⑴ (采用优势法) 在多准则决策问题中，定义：设 $\bar{x}\in R$，若不存在 $x\in R$ 满足 $F(x)\geqslant F(\bar{x})$，则称 $\bar{x}$ 为多准则决策问题的非劣解。(其中：R 为备选方案的集合)

我们用此概念去考察这 4 个方案，并不存在 $F(x)\geqslant F(\bar{x})$ 的情况，所以 x_1，x_2，x_3，x_4 均为非劣解。

若假设 $f_1(x_1)=f_1(x_4)$，则可导出 $x_1>x_4$，此时 x_4 是劣解，应予以剔除。

⑵ (采用连接法) 若设定切除值：

$$F^c=[f_1^c,f_2^c,\cdots,f_6^c]^T=[18,中,中,中,1000,低]$$

则可接受的方案集合 R_c 为：

$$R_c=\bigcap_{j=1}^{m}\{x\mid f_j(x)\geqslant f_j^c,x\in R\}=\{x_1,x_3\}$$

⑶ (采用分离法) 设定 $F^d=[20,中,中,中,1000,低]^T$，则可接受方案的集合 R_d 为：

$$R_d=\bigcup_{j=1}^{m}\{x\mid f_j(x)\geqslant f_j^d,x\in R\}=\{x_1,x_3,x_4\}$$

9.5.2 智力激励法

智力激励法也称为头脑风暴法或集思广益法，是一种运用集体智慧的

方法。由于每个人所掌握的知识和经验是有局限性的，所以集中一批富有个性的人在一起讨论，将每人的知识和经验、掌握的材料、观察问题的角度和分析问题的方法通过相互讨论与交流，可以激励出更多的想法与对策。

⑴ 专家评审法

这种方法的特点是邀集一批同行专家，针对所要采取对策的问题召开会议，敞开思想，各抒己见，畅所欲言。为了做到这一点，还须符合如下要求：①与会者没有上下级之分，要平等相待；②允许胡思乱想；③不回避矛盾；④不允许否定和批评别人意见；⑤可对别人的意见做补充和发表相同意见。这种做法不仅适用于对重大问题的决策，也适用于对一个车间、一个班组的安全问题的决策。

⑵ 德尔菲法

德尔菲法也称专家预测法。组织者针对要采取对策的问题，首先编写出一个意见征询表，将问题及要求函寄给专家们，要求他们限期寄回书面回答；然后将所得看法或建议加以概括，整理成一份综合表；再将综合表和意见征询表寄回给专家，征询第二次书面意见，使专家们在别人意见的启发下提出新的设想，或对自己的意见加以补充或修改。根据情况需要，经过几次反馈后，意见逐步集中和明确，从中可得到较好的预测和决策方案。

9.5.3 评分法

评分法就是根据预先规定的评分标准对各方案所能达到的指标进行定量计算比较，从而对各个方案排序。评分法根据预先规定标准用分值作为衡量抉择的优劣尺度，对抉择方案进行定量评价。如果有多个决策（评价）目标，则先分别对各个目标评分，再经处理求得方案的总评分。

⑴ 评分标准

一般按5分制评分：优、良、中、差、最差。“理想状态”取最高分（5分），“不能用”取最低分（1分），“中间状态”分别取4分（良好）、3分（可用）、2分（勉强可用）。当然也可按7个等级评分，这要视决策方案多少及其之间的差别大小和决策者的要求而定。

⑵ 评分方法

评分方法多数是采用专家打分的办法，即以专家根据评价目标对各个抉择方案评分，然后取其平均值或除去最大、最小值后取的平均值作为分值。

⑶ 评价指标体系

评价指标一般应包括三个方面的内容：技术指标、经济指标和社会指标。对于安全问题决策，要解决某个安全问题，若有几个不同的技术决策方案，则其评价指标体系的技术指标大致有：技术先进性、可靠性、安全性、维修性、可操作性等；经济指标大致有：成本、质量可靠性、原材料、周期、风险率等；社会指标大致有：劳动条件、环境、精神习惯、道德伦理等。当然要注意指标因素不宜过多，否则不但难于突出主要因素，而且会造成评价结果不符合实际。

⑷ 加权系数

由于各评价指标其重要性程度不一样，必须给每个评价指标一个加权系数。为了便于计算，一般取各个评价指标的加权系数 g_i 之和为 1。加权系数值可由经验确定或用判断表法计算，其判断表见表 9-3。

判断表法是将评价目标的重要性两两比较，同等重要各给 2 分；某一项重要者则分别给 3 分，另一项给 1 分；某一项比另一项重要得多，则分别给 4 分，另一项给 0 分。将上述对比的给分填入表中。

计算各评价指标的加权系数公式为：

$$g_i = k_i \Big/ \sum_{i=1}^{n} k_i \tag{9-4}$$

式中 k_i ——各评价指标的总分；

n ——评价指标的个数。

表 9-3 加权系数判别计算表

被比较者 / 比较者	A	B	C	D	k_i	g_i
A		1	0	1	2	0.083
B	3		1	2	6	0.250
C	4	3		3	10	0.417
D	3	2	1		6	0.250
重要程度排序 C > B，D > A					$\sum_{i=1}^{4} k_i = 24$	$\sum_{i=1}^{4} g_i = 1.0$

当指标较多时，比较过程应十分细致，否则会引起混乱，出现自相矛盾的现象。

另一种办法是对多个指标不一对一地逐个对比，而是只依次对两个目标做

一次比较。如表 9-4 所示，按从上到下的顺序，对上下两个相邻指标进行比较。先比较目标 A 和 B，认为 A 的重要性是 B 的 2 倍，而 B 的重要性是 C 的一半，这样一直进行到底。

表 9-4　重要程度比较表

目　　标	暂定重要程度	修正重要程度	加权系数
A	2.0	1.0	0.235
B	0.5	0.75	0.176
C	1.5	1.5	0.353
D	—	1.0	0.235
重要程度排序 C > A = D > B		$\sum_{i=1}^{n} k_i = 4.25$	$\sum_{i=1}^{n} g_i = 1.0$

若把最后一项目标 D 的数值假定为 1.0，因为它上面的目标 C 是 D 的 1.5 倍，因此，修正的重要程度即为原来的 1.5 倍 （D × C = 1 × 1.5 = 1.5）。目标 C 上面的目标 B 是 C 的一半，故修正的重要程度为 0.75 （C × B = 1.5 × 0.5 = 0.75）。目标 B 上面的目标 A 是 B 的 2 倍，故修正的重要程度为 1 （B × A = 0.5 × 2 = 1.0）。由此看出，目标 C 最重要，其次是 A、D 同等重要，最不重要的是 B。

最后求各修正程度系数之和并除以各修正重要程度系数即得到各目标的加权系数。这种方法较上述方法可用较少的判断次数来确定重要程度，但主观因素的影响也更大些。

(5) 定性指标的定量处理

有些指标如美观、舒适等，很难定量表示，一般只能用很好、好、较好、一般、差，或是优、良、中、及格、不及格等定性语言来表示。这时可规定一个相应的数量等级，如很好或优给 5 分，好或良给 4 分，差或不及格给 1 分。

但应注意，诸如美观、舒适之类指标，不同的人有不同的感受。如操作座椅，对形体高大的人认为舒适，而对形体矮小的人感觉可能相反。对美观更是如此。因此，他们对同一事物可能给出不同的评分。这时可用概率决策方法来处理，求其所期望的价值 E （V）。

$$E(V) = \sum_{i=1}^{n} P_i \cdot V_i \qquad (9\text{-}5)$$

式中 V_i——第 i 个目标可能有的价值；

P_i——第 i 个目标价值的发生概率；

n——指标个数。

(6) 计算总分

计算总分也有很多种方法，如表 9-5 所示，可根据具体情况选用。总分或有效值高者为较佳方案。

表 9-5 总分计算方法

方 法	公 式	备 注
分值相加法	$Q_1 = \sum_{i=1}^{n} k_i$	计算简单，直观
分值相乘法	$Q_2 = \prod_{i=1}^{n} k_i$	各方案总分相差大，便于比较
均值法	$Q_3 = \frac{1}{n}\sum_{i=1}^{n} k_i$	计算较简单，直观
相对值法	$Q_4 = \frac{\sum_{i=1}^{n} k_i}{nQ_0}$	$Q_4 \leqslant 1$，能看出与理想方案的差距
有效值法 (加权计分法)	$N = \sum_{i=1}^{n} k_i g_i$	总分中考虑各评价指标的重要度

表中公式 Q——方案总分值；

N——有效值；

n——评价指标数；

k_i——各评价指标的评分值；

g_i——各评价指标的加权系数；

Q_0——理想方案总分值。

9.5.4 决策树法

决策树法是决策过程的一种有序的概率图解表示方法。因此，决策树分析方法又称概率分析决策方法，是风险型决策中的基本方法之一。决策树法是一种演绎性方法，即是一种有序的概率图解法，它将决策对象按其因果关系分解成连续的层次与单元，以图的形式进行决策分析，由于这种决策图形似树枝，故称“决策树”。

⑴ 决策树形态

决策树的结构如图 9-2 所示。

图中，方块表示决策点，从它引出的分枝叫方案分枝，分枝个数即为可能的行动方案个数。

圆圈表示方案节点（也称自然状态点），从它引出的分枝叫概率分枝，每条分枝的上面注明了自然状态（客观条件）及其概率值，分枝个数即为可能出现的自然状态个数。

三角表示结果点（也称“末梢”），它旁边的数值是每一个方案在相应状态下的收益值。

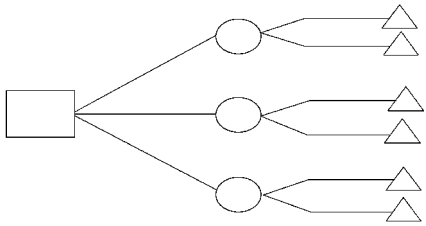


图 9-2　决策树示意图

⑵ 决策步骤

首先根据问题绘制决策树；然后由右向左逐一进行分析，根据概率分枝的概率值和相应结果节点的收益值，计算各概率点的收益期望值，并分别标在各概率点上；最后再根据概率点期望值的大小，选择最优方案。

⑶ 决策树分析法的优点

1）决策树能显示出决策过程，不但能统观决策过程的全局，而且能在此基础上系统地对决策过程进行合理分析，集思广益，便于做出正确决策。

2）决策树显示把一系列具有风险性的决策环节联系成一个统一的整体，有利于在决策过程中周密思考，能看出未来发展的几个步骤，易于比较各种方案的优劣。

3）决策树法既可进行定性分析，也可进行定量分析。

⑷ 应用举例

【例 9-2】　应用上述决策方法对某企业计划自行研制一种新的安全装置的事件进行决策，选择合理方案。具体条件如下：

⑴ 决定研制项目是否需要评审。若评审，则需评审费 5000 元。由于这是一个主观抉择环节，决策者完全可以决定。如果决定评审，评审通过概率为 0.8，不通过的概率为 0.2。这种不能由决策者自身抉择的环节称为客观随机抉择环节。

⑵ 是采取“本厂独立完成”形式还是和“外厂协作完成”形式来研制此安全装置。也是主观环节，决策者可以独立决定。

⑶ 如果研制成功，能有 6 万元收益。若“本厂独立完成”研制费为 2.5

万元，成功概率为 0.7，失败概率为 0.3。

⑷ 若与“外厂协作”研制（包括先评审），需支付研制费 4 万元，成功概率为 0.99，失败概率为 0.01。

【解】

⑴ 先画出决策树，如图 9-3 所示。

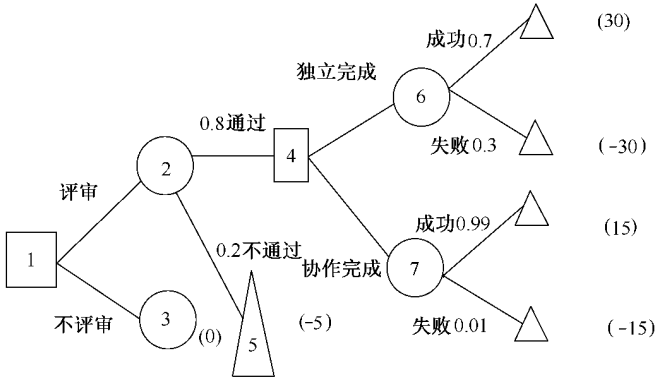


图 9-3　决策树

⑵ 根据上述数据计算各节点的收益（收益 = 效益 - 费用）

独立研制成功的收益：60 - 5 - 25 = 30（千元）

独立研制失败的收益：0 - 5 - 25 = - 30（千元）

协作研制成功的收益：60 - 5 - 40 = 15（千元）

协作研制失败的收益：0 - 5 - 40 = - 45（千元）

按照期望值公式计算独立研制成功的期望值：

$$E(V_6) = \sum_{i=1}^{2} P_{6i} \cdot V_{6i} = 0.7 \times 30 + 0.3 \times (-30) = 12$$

协作研制成功的期望值：

$$E(V_7) = \sum_{i=1}^{2} P_{7i} \cdot V_{7i} = 0.99 \times 15 + 0.01 \times (-45) = 14.4$$

⑶ 根据期望值决策准则，若决策目标是收益最大，则采用期望值最大的行为方案；如果决策目标是使损失最小，则选定期望值最小的方案。本例选用的是期望值最大者，即选用协作完成形式。

上报评审环节的期望值：

$$E(V_2) = \sum_{i=1}^{2} P_{2i} \cdot V_{2i} = 0.8 \times 14.4 + 0.2 \times (-5) = 10.52$$

(5) 决策树分析法的优点

1) 决策树能显示出决策过程，形象具体，便于发现问题。

2) 决策树能把风险决策的各个环节联系成一个统一的整体，有利于决策过程中的思考，易于比较各种方案的优劣。

3) 决策树法既可以进行定性分析，也可以进行定量分析。

9.5.5 技术经济评价法

技术经济评价法是对抉择方案进行技术经济综合评价时，不但考虑评价指标的加权系数，而且所取的技术评价和经济评价都视为相对于理想状态的相对值。这样更便于决策判断、方案筛选和方案改进。

(1) 技术评价

技术评价步骤如下：

1) 确定评价的技术项目和评价指标集。

2) 明确各技术指标的重要程度。在指标集的众多技术指标中，要明确哪些是必须满足的，即所谓固定要求，低于或高于该指标就不合格；要明确哪些是可以给出一个允许范围的，也即有一个最低要求；还要明确哪些是希望达到的。

3) 分别对各个技术指标评分。

4) 进行技术指标总评价。在各个技术指标评分的基础上，进行总的评分，即求出各技术指标的评分值与加权系数乘积之和与最高分 (理想方案) 的比值：

$$W_t = \frac{\frac{1}{n}\sum_{i=1}^{n} V_i q_i}{V_{max}\sum_{i=1}^{n} g_i} = \frac{\sum_{i=1}^{n} V_i}{nV_{max}} \tag{9-6}$$

式中 W_t——技术价；

V_i——各技术评价指标的评分值；

n——技术评价指标个数；

g_i——各技术评价指标的加权系数，取 $\sum_{i=1}^{n} g_i = 1$；

V_{max}——各技术评价指标的最高分 (对理想方案，5 分制的 5 分)。

技术价 W_t 越高，方案的技术性能越好。理想方案的技术评价为 1，$W_t <$

0.6 表示方案不可取。

(2) 经济评价

经济评价的步骤如下：

1) 按成本分析的方法，求出各方案的制造费用 C_i。

2) 确定该方案的理想制造费用。

通常理想的制造费用是允许制造费的 0.7 倍。允许制造费 C 可按下列公式计算：

$$C = \frac{C_{M,\min}}{\rho} \tag{9-7}$$

$$\rho = \frac{C_S}{C_i} = \frac{\text{标准价格}}{\text{制造费用}}$$

式中 $C_{M,\min}$ ——合适的市场价格；

C_S ——标准价格，是研制费、制造费、行政管理费、销售费、盈利和税金的总和。

3) 确定经济价。确定经济价的公式：

$$W_w = \frac{C_I}{C_i} = \frac{0.7C}{C_i} \tag{9-8}$$

经济价 W_w 值越大，经济效果越好。理想方案的经济价为 1，表示实际生产成本等于理想成本。W_w 的许用值为 0.7，此时，实际生产成本等于允许成本。

(3) 技术经济综合评价

可以通过计算法和图法进行技术、经济综合评价。

1) 相对价 W 法

①均值法 $$W = 0.5\ (W_t + W_w) \tag{9-9}$$

②双曲线法 $$W = \sqrt{W_t + W_w} \tag{9-10}$$

相对价 W 值越大，方案的技术经济综合性能越好，一般应取 $W > 0.65$。当 W_t，W_w 两项中有一项数值较小时，用双曲线法能使 W 值明显变小，更便于对方案的抉择。

2) 优度图法

优度图如图 9-4 所示。图中横坐标为技术价 W_t，纵坐标为经济价 W_w。每个方案的 W_{ti}、W_{wi} 值构成点 S_i，而 S_i 的位置就反映了此方案的优度。当 W_t、W_w 值均等于 1 时的交点为 S_I，此时就为理想优度，表示技术经济综

合指标的理想值。0—S_I 连线称为“开发线”，线上各点 $W_t = W_w$。S_i 点离 S_I 点越近，表示技术经济综合指标越高；离开发线越近，说明技术经济综合性能越好。

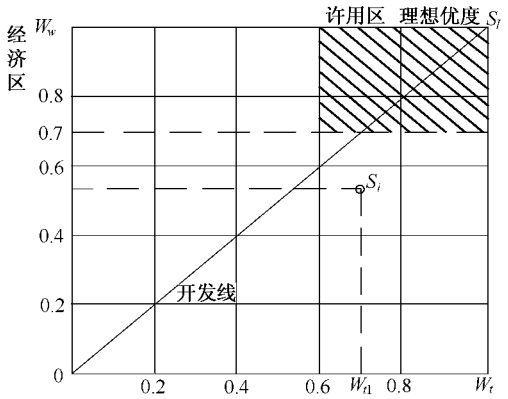


图 9-4　优度图

9.5.6　A B C 分析法

ABC 分析法又叫 ABC 管理法、主次图法、排列图、巴雷托图等。该法是由巴雷托法则转化而来的。该方法反映了“在社会现象中，少数事物（10% ~ 20%）对结果有 90% 的决定作用，而大部分事物只对结果有 10% 以下的决定作用”，即“关键的少数与次要的多数”原理。ABC 方法在企业中已成为提高经济效益的重要手段并得到广泛的应用。

ABC 分析方法运用在安全管理上，就是应用“许多事故原因中的少数原因带来较大的损失”的规律，根据统计分析资料，按照不同的指标和风险率进行分类与排列，找出其中主要危险或管理薄弱环节，针对不同的危险特性，实行不同的管理方法和控制方法，以便集中力量解决主要问题。

ABC 分析法用图形表示（巴雷托分布图），如图 9-5 所示。该图是一个坐标曲线图，其横坐标为所要分析的对象，如某一系统中各组成部分的故障模式，某一失效部件的各种原因等，纵坐标即横坐标所标示的分析对象的量值，如失效系统中各组成部分事故相对频率、某一失效系统和部件的各种原因的时间或财产损失等。

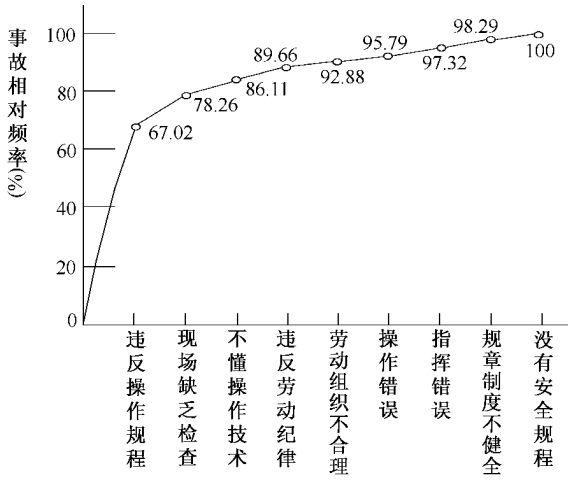


图 9-5　安全管理项目的巴雷托分布图

图 9-5 中的数据见表 9-6 所示。

表 9-6　系统安全管理不利出现的事故类型统计

事故类型	事　故　数	相对频率 (%)
违反操作规程	6258	67.02
现场缺乏检查	1050	11.24
不懂操作技术	735	7.87
违反劳动纪律	329	3.53
劳动组织不合理	301	3.22
操作错误	272	2.91
指挥错误	143	1.53
规章制度不健全	137	1.47
没有安全规程	113	1.21
总　　计	9338	100

根据图 9-5 中的巴雷托曲线对应（纵坐标）的百分比，就可查找出关键因素和部位。通常将占累加百分数 0%～90%的部分或因素称为主要因素或主要部位；其余 10%（即 90%～100%）部分称为次要因素或次要部位；0%～80%的部分或因素称为关键因素或关键部位，即 A 类（如图中违反操作规程和现场缺乏检查两项）；80%～90%的部分或因素划为 B 类（即图中不懂操作技术

和违反劳动纪律两项）；余下部分或因素划为 C 类。

在安全管理上，若不作分析图，也可参考表 9-7 来划分 A、B、C 的类别。

表 9-7　划分 ABC 类别的参考因素

类别 / 因素	A	B	C
事故严重度	可造成人员死亡	可能造成人员严重伤害、严重职业病	可能造成轻伤
对系统影响程度	整个系统或两个以上子系统损坏	某子系统损坏或功能丧失	对系统无多大影响
财产损失	可能造成严重的损失	可能造成较大的损失	可能造成轻微的损失
事故概率	容易发生	可能发生	不大可能发生
对策的难度	很难防止或投资很大，费时很多	能够防止，投资中等，费时不很多	易于防止，投资不大，费时少

9.5.7　稀少事件的风险评估

⑴ 稀少事件的概念

当决策者要在多种抉择方案中作决策时，可能会遇到某种稀少事件是否值得考虑，或者在用智力激励法进行风险辨别时，稀少事件如何估计的问题。

稀少事件是指那些发生的概率非常小的事件，对它们很难用直观的方法进行研究，因为它们不但“百年不遇”，而且“不重复”。在稀少事件中有两种不同的风险估计：一类是称外围“零至无穷大”的风险，指的是那些发生的可能性很小（几乎为零）而后果却十分严重（几乎是无穷大）的事故，例如核电站的重大事故。另一类是发生概率很小，但涉及的面或人数却很广，而它们的后果却不像前一类明显，并且被一些偶然的因素、另外一些风险、与它们的作用相同或相反的种种其他作用因素所掩盖，如水质污染与癌症发病率的关系。水质污染不是特别严重的情况下，很难确定与癌症发病率之间的关系。前一类情况主要涉及明显事故的估计与评价，后一类情况则主要是对潜在危险进行测量和估计。

对稀少事件很难给出一个严格定义，就第一类事故情况来说，一般采用如下的定义：即 100 年才可能发生一次事故称为稀少事件。其数学表达式如下：

$$nP < 0.01/\text{年} \tag{9-11}$$

式中　n——试验次数；

P——事故发生的概率。

⑵ 稀少事件的风险度

稀少事件一般服从二项式分布，它们相互独立，发生的概率为 P，在 n 次试验中，有 m 次成功的概率 P（m）为：

$$P(m) = C_n^m P^m (1-P)^{n-m} \tag{9-12}$$

其中：m = 0，1，…，n

其均值（期望值）：

$$E(X) = nP \tag{9-13}$$

其方差值：

$$D(X) = nP(1-P) \tag{9-14}$$

风险度 R 为：

$$R = \frac{D(X)}{E(X)} = \frac{\sqrt{nP(1-P)}}{nP} \tag{9-15}$$

对于稀少事件，发生概率 $P \ll 1$，故有：

$$\left.\begin{aligned} D(X) &\approx nP \\ R &= \frac{1}{\sqrt{nP}} \end{aligned}\right\} \tag{9-16}$$

(3) 绝对风险与对比风险

概率估计只有当概率不太大和不太小时才比较准确，因而以期望值（均值）为基础的统计数据对稀少事件分析已失去效用，需要引入对比风险的概念。对比风险与绝对风险可定义如下。

绝对风险：是对某一可能发生事件的概率及其后果的估计，也就是我们通常所讨论的风险概念。

对比风险：可分为两种情况，一种是对于发生概率相似的事件，比较其发生的后果；另一种是对于两种后果及大小相似的事件，比较其发生的概率。图 9-6 是绝对风险与对比风险的适用区域示意图。

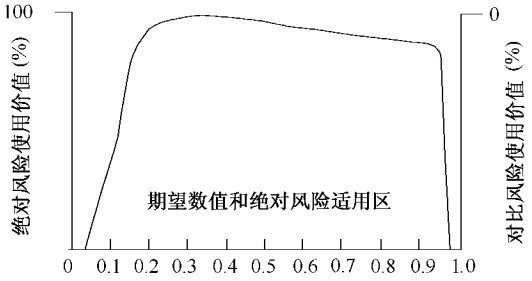


图 9-6　绝对风险与对比风险的适用区域示意图

(4) 稀少事件风险估计的应用

当决策者要在多种抉择方案中作决策时，首先会遇到某种稀少现象（事件）是否值得考虑，或者在用智力激励法进行风险辨识时，人们提出的许多应考虑的因素是否都要认真考虑和估计等问题。下面举一例说明。

某企业存在一种有害物质，拟有两种存放方案：一种是简单的浅埋，另一

种是放在专门建造的地窖中。浅埋比价经济，但在发生水灾时会大量溢散。水灾的发生是稀少事件。现在需要决定，是否需要考虑浅埋溢散的影响？设有害物质的保护期 100 年。当发生水灾时，浅埋方案会造成 100%的有害物质溢散，而专建地窖方案有 10%的溢散。因专建的地窖是按要求建造的，溢散 10%是可以接受的。

假定一个对风险持中性态度的人，等价水平 $P = 0.01/100$ 年（即 100 年中发生溢散的概率为 0.01 与埋在专建地窖中等价），决策者为更保险，将此又降低两个数量级，即认为等价水平是 $P = 10^{-6}$/年，然后就要对水灾发生的概率进行估计。如果概率小于 10^{-6} 年，就可以采用浅埋方案，否则，则用专建地窖的方案。

9.6 各种决策方法中的共性问题

前面介绍了 7 种常见的安全决策方法，加上安全评价中的模糊评价法（也可以用于安全决策）共计 8 种。每种方法都有各自的优点，基本上涵盖了日常生活、生产中需要的安全决策情况。但从各种决策方法中，我们也可看到一些值得注意的共性问题。

1）决策中存在主观因素

决策是由决策者做出的，决策者的主观因素必然影响决策过程。虽然我们研究摸索出了多种科学的分析方法，但其中许多因素要由决策者做出判断和决定的，所以在决策过程中，决策者的主观估计要尽可能符合客观实际。要达到这一点，这就要设法能使决策者在做出决定时尽可能少地带有主观随意性。具体地说，就是要设法能比较客观地决定各目标的相对重要程度，或者是加权系数的数值大小。

2）决策结果不可能是最理想的答案

多指标决策，很难简单地满足一个要求而不使别的方面的要求受到损失。因此，任何设计方案几乎总是包括有不十分理想的成分，不会是十全十美的。因为受到时间、投资和技术的限制，不可能提出客观存在的无穷多个方案，再加上加权系数和诸指标的目标值本身就不是十全十美的。所以多指标决策不能获得最优解，所获得的只能是一种满意解。问题是在允许的条件下如何使所获得的解能相对地更为令人满意。

3）决策的目的在于作方案比较

无论哪种决策方法，最终目的是为了综合评价时便于方案优劣比较。因此，实际工作中，在提出的各种方案之前，应首先通过定性比较，分出相对的优劣，然后再进行定量的处理，这样的过程更为科学。在工程上进行方案选择，大多采用加权处理，以便将诸指标值汇成总指标值，以利比较。

思 考 题

1. 简述确定型决策和风险型决策分别应具备哪些条件。
2. 安全决策主要有哪几种类型？
3. 安全决策分析主要程序有哪些？在进行潜在问题分析时，通常存在哪些问题？
4. 安全决策方法都有哪些？各有什么特点？
5. 非确定型安全决策一般有哪几种方法？
6. 某人欲投资钢铁生意，如进行市场调查，则需调查费 1 万元，如不进行市场调查，则可省去这笔费用。如果进行调查，则决定投资的概率为 0.7，决定不投资的概率为 0.3。如果与其他人合作，则进行较大的生意额，需投入成本 6 万元，成功的可能性为 0.9，失败的可能性为 0.1，如成功则可获利 12 万；如果单独投资，则进行小额投资，只需投入成本 3 万元，成功的可能性为 0.7，失败的可能性为 0.3，如成功则可获利 7 万。试用决策树法对其分析，做出合理的决策。

参 考 文 献

1 黄祥瑞编著．可靠性工程．北京：清华大学出版社，1990

2 中国现代设计法研究会编．决策管理现代设计法．北京：中国建筑工业出版社，1990

3 沈斐敏等编著．安全系统工程基础与实践．北京：煤炭工业出版社，1991

4 肖爱民编著．安全系统工程学．北京：中国劳动出版社，1992

5 王金波等编著．系统安全工程．沈阳：东北工学院出版社，1993

6 冯兆瑞等编著．安全系统工程．北京：冶金工业出版社，1993

7 陈宝智编著．安全原理．北京：冶金工业出版社，1995

8 陈宝智编著．危险辨识控制及评价．成都：四川科学技术出版社，1996

9 汪元辉等编著．安全系统工程．天津：天津大学出版社，1999

10 孙连捷等编著．安全科学技术百科全书．北京：中国劳动社会保障出版社，2003

11 李海泉等编著．系统可靠性分析与设计．北京：科学出版社，2003

12 罗云等编著．风险分析与安全评价．北京：化学工业出版社，2004

13 蒋军成等编著．安全系统工程．北京：化学工业出版社，2004

14 Roland H E & Moriarty B. System Safety Engineering and Management. USA：J. Wiley Co.，1990

15 Kumamoto & Henley. Probabilistic Risk Assessment and Management for Engineers and Scientists. IEEE. Press，1996