第1章 安全系统工程概论

本章学习目标：

了解系统论的基础知识、系统工程发展简史、安全系统工程发展简史；理解安全、安全系统及安全系统工程的定义；明确安全系统工程的研究对象、研究内容、方法论及分析方法。

本章学习方法：

以了解、理解和分析为主，可借阅系统论方面的经典著作以增加对系统工程基础知识的理解，同时积极思考系统工程、安全系统、安全系统工程之间的区别和联系，思考需要开展安全系统工程研究的各种问题。

试读版本仅供防疫期间线上教学使用

系统工程是系统科学中改造客观世界，并使改造过程合理化的一门技术。它以运筹学、控制论、信息论、系统论中一些具有普遍意义的基本理论为指导，在自然科学、社会科学以及工程建设和管理中发挥作用。近二十多年来，许多学者和科学家一直在探索将系统工程的理论和原理，运用到安全管理方面，并逐步发展为安全系统工程，成为安全科学中的主要分支。

安全系统工程是以系统论、信息论、控制论等为理论基础，以安全工程、系统工程、可靠性工程的原理和方法为手段，以安全管理、安全技术和职业健康为载体，对研究对象中的风险进行辨识、评价、控制和消除，以期实现系统及其全过程安全的新兴学科。

1.1 系统论简介

1.1.1 系统的定义

“系统”的概念，来源于人类社会的实践经验，并在长期的社会实践中不断发展并逐渐形成。一般系统论的创始人奥地利的贝塔朗菲指出：“系统的定义可以确定为处于一定的相互关系中，并与环境发生关系的各组成部分的总体。”我国科学家钱学森对系统的定义为：“把极其复杂的研究对象称为系统，即由相互作用和相互依赖的若干组成部分结合成的具有

特定功能的有机整体，而且这个系统本身又是它所从属的一个更大系统的组成部分。”虽然对于系统概念有多种理解，但其基本意义大致相同，即系统是由相互作用、相互依赖的若干组成部分结合而成的具有特定功能的有机整体。

系统是一种由若干元素组成的集合体，用它来完成某种特殊功能。因此，每一项工作完成都是由人、机器、原材料、方法、环境等许多因素（元素）组成，及相互之间发生作用来完成工作的一个具有特殊功能的体系的总和。

每一个系统中的元素间相互联系、相互渗透、相互促进，彼此间保持着特定的关系，保证系统所要达到的最终目的。一旦相互间特定的关系遭到破坏，就会造成工作被动和不必要的损失。

客观世界都是由大大小小的系统组成的。组成系统的要素或者子系统又由一定数量的元素组成，各有其特定的功能和目标，它们之间相互关联，分工合作，以达到整体的共同目标。例如科学技术系统包括七个基本要素，即机构、法、人、财、物、信息和时间七个子系统。它们集合在一起的共同目标是多出成果，快出人才，推动国民经济向前发展。而科学技术系统又是人类社会经济大系统的一个组成部分，或者说是一个子系统。

任何一个团体、工厂、企业都可称为一个系统，在这个系统中，包含管理机关、运行体系；继续往下分，就又出现一个系统，我们称其为子系统，它们包括班组及其成员等。

1.1.2　系统的分类

按照不同的分类标准可把系统划分成以下类型。

1. 按照系统的起源划分

（1）自然系统。由自然物组成的系统。它是由自然现象发展而来的。如太阳系、银河系、原子结构、山脉系统、河流系统、森林系统、矿产系统等。

（2）人造系统。由人类按一定的目的设计和改造而成的，并由人的智能或机械的动力来完成特定目标的系统。如政府机构、民间团体、交通运输系统、电力传输系统、企业系统等。

2. 按照系统与环境的关系划分

（1）开放性系统。与外界环境发生联系的系统。

（2）封闭性系统。与外界环境隔绝或不受外界环境影响的系统。

3. 按照组成系统的要素存在的形态划分

（1）实体系统。组成系统的元素是实体的、物理方面的存在物的系统。

（2）概念系统。以概念、原理、原则、方法、制度、程序等非物理方面的存在物组成的系统。

4. 按照系统与时间的依赖关系划分

（1）静态系统。决定系统特性的一些因素不会随时间的变化而变化的系统。

（2）动态系统。决定系统特性的因素随时间的变化而变化的系统。

5. 按照物质运动的发展阶段划分

（1）无机系统。如力学系统、物理学系统、化学系统等。

（2）有机系统。如生物系统等。

（3）人类社会系统。如管理系统、经营系统、作业系统等。

试读结束，需要全本PDF请访问

6. 按照系统包含的范围划分

（1）大型系统。如生态平衡系统。

（2）中型系统。如工程系统等。

（3）小型系统。如班组管理系统等。

7. 按照系统的构成划分

（1）简单系统。由性质相近的若干要素组成的系统，如物资系统等。

（2）复杂系统。由人造系统和自然系统相结合的系统，如农业系统、企业系统和武器系统以及社会经济大系统等。

8. 按照系统的功能划分

（1）环境系统。自然系统和人类社会共同组成的大系统，以及与所要研究的系统周围具有一定关系的系统。

（2）军事系统。由军人组成的、保卫国家和本国人民安全以及对世界和平做出贡献的整个系统。

（3）安全系统。由人、机、料、法、环等组成的维持社会团体、机关、企业等安全运行的系统。某些系统的形态并不是一成不变的，它是随着人们认识客观世界的深度，以及改造客观世界的需要，按照人们提出的分类标准进行划分的。在实际工作中这些系统也并非是孤立存在的，有时是相互交叉、相互依存、相互对立和相辅相成的。

1.1.3　系统的特征

从系统的定义可以看出系统具有整体性、目的性、阶层性、相关性、环境适应性、动态性六个基本特征。

（1）整体性。系统是由两个或两个以上相互区别的要素（元件或子系统）组成的整体，而且各个要素都服从实现整体最优目标的需要。构成系统的各要素虽然具有不同的性能，但它们通过综合、统一（而不是简单拼凑）形成的整体就具备了新的特定功能，就是说，系统作为一个整体才能发挥其应有功能。所以，系统的观点是一种整体的观点，一种综合的思想方法。

（2）目的性。任何系统都是为完成某种任务或实现某种目的而发挥其特定功能的。要达到系统的既定目的，就必须赋予系统规定的功能，这就需要在系统的整体的生命周期，即系统的规划、设计、试验、制造和使用等阶段，对系统采取最优规划、最优设计、最优控制、最优管理等优化措施。

（3）阶层性。系统阶层性主要表现在系统空间结构的层次性和系统发展的时间顺序性。系统可分成若干子系统和更小的子系统，而该系统又是其所属系统的子系统。这种系统的分割形式表现为系统空间结构的层次性。另外，系统的生命过程也是有序的，它总是要经历孕育、诞生、发展、成熟、衰老、消亡的过程，这一过程表现为系统发展的阶层性。系统的分析、评价、管理都应考虑系统的阶层性。

（4）相关性。构成系统的各要素之间、要素与子系统之间、系统与环境之间都存在着相互联系、相互依赖、相互作用的特殊关系，通过这些关系使系统各元素有机地联系在一起，发挥其特定功能。即系统的各元素不仅都为完成某种任务而起作用，而且任一元素的变化也都会影响其任务的完成。有些要素彼此关联，有些要素相互排斥，有些要素则互不相

试读结束，需要全本PDF请访问 www.ertongbook.com

干。例如生产班组管理系统的人员增加或减少，就会影响到设备装置、工时安排的改变。

（5）环境适应性。系统是由许多特定部分组成的有机集合体，而这个集合体以外的部分就是系统的环境。一方面，系统从环境中获取必要的物质、能量和信息，经过系统的加工、处理和转化，产生新的物质、能量和信息，然后再提供给环境。另一方面，环境也会对系统产生干扰或限制，即约束条件。环境特性的变化往往能够引起系统特性的变化，系统要实现预定的目标或功能，必须能够适应外部环境的变化。研究系统时，必须重视环境对系统的影响。

（6）动态性。世界上没有一成不变的系统。系统不仅作为状态而存在，而且具有时间性的程序。整个人类社会和自然环境的运行中，系统中的各个元素、子系统，都是随着时间的改变而不断改变的。

1.1.4　系统学原理

系统学是系统科学的基础理论学科，为系统工程提供理论依据。作为系统学原理，可以归纳为以下八条。

1. 整体性原理

现代科学技术的飞速发展，使科学研究的对象和人们对它的认识发生了很大的变化，有机的整体取代了被分割的部分。以前认为最基本的部分，如今看来，实际上也是一个可分的由各个部分组成的有机整体。微观世界呈现出来的整体结构与客观世界出乎意料地相似。世界上一切事物、现象和过程，都是有机的整体，自成系统而又互成系统。客观世界的整体性是系统学整体性原理的来源和依据。

2. 相关性原理

系统学的相关性原理，是辩证法的普遍联系观点的具体体现和实际应用。科学技术发展的全部成就，证明了普遍联系观点的真理性，质量和能量的相互转化和守恒定律，揭示了各种物质的状态及其运动状态之间的普遍联系。细胞的发现和达尔文进化论的创立，揭示了生物界内部的普遍联系以及生物和环境之间的联系。门捷列夫的元素周期表，揭示了曾经被认为互不联系、互不依赖的各种元素之间的关系。客观世界就是一个相互联系的整体。世界上一切事物、现象和过程之间的联系是客观存在的，一种事物离开了它和它周围条件的相互联系和相互作用，就成为不可理解和毫无意义的东西。也就是说，事物总是存在于某种系统之中，亦即处于某种联系之中。如果把某一事物从某个系统中分离出来，它们必然又落入另一个系统。因此，相关性原理要求把任何一个事物作为某个系统的一个要素来研究。传统的科学方法主要研究系统内各子系统（或元素）或子系统与元素之间的联系。诸如系统联系、结构联系、功能联系、起源联系等。客观事物存在的联系是多种多样的，联系的多样性，决定了系统的多样性。各类联系间界线的相对性，导致未知联系向已知联系的转化，形成未知系统向已知系统过渡。科学技术发展到某一阶段人们认为互不联系的东西，可能存在新的未知的联系。某些现在看来不成系统的东西，在进一步深入研究后，可能发现就是一个新的系统。从联系的广泛性，可以知道系统的广泛性。从哲学的高度建立起来的相关性原理，为研究系统结构奠定了基础。

3. 有序性原理

凡是系统都是有序的。系统的有序性，是系统有机联系的反映。稳定的联系构成的结

仅供湖南科技信息学院疫期网线上教学使用

构，保障了系统的有序性；本质的联系，形成了系统发展和变化的规律。在研究事物的联系时，最重要的是把握它的规律性。规律所表现的是现象间在一定条件下所具有的本质的、普遍的、必然的联系。对系统有序性的研究，开辟了发现规律的途径；对有序性原理的运用，将在一定程度上帮助人们按规律办事。

任何一个系统，都和周围环境组成一个较大的系统，因此，任何一个系统都是更高一级的系统的一个要素。同时，任何一个系统的要素本身，通常又是较低一级的系统。以科学体系为例，科学与社会组成一个较大的系统，科学是较高一级的系统——社会的一个组成部分，这就需要研究科学的社会地位和功能。科学本身的两个组成部分——自然科学和社会科学，又分别是较低一级的系统，这就必须研究各门学科的关系及发展的不平衡性。若科学作为一个相对独立的完整体系，则必须研究它的一般规律。

系统的稳定联系构成的系统结构，形成了一个纵横交错的立体网络模式，它既可按垂直方向进行描述，以区分子系统的各种层次和等级，也可按水平方向进行描述，以掌握系统的各个组成部分之间的联系。波兰学者 I. 马列茨基等把现代科学整体化的过程，区分为两类：一类为“纵向整体化，即科学与实践相接近，科学的基础研究与应用研究相接近”；另一类为“横向整体化，即跨课题和跨学科的研究”。这种分类，不仅形象地设计了科学整体化过程的系统模式，而且准确地说明了系统科学和系统方法等学科科学横向整体化的产物，它几乎横贯一切学科，反映一切学科的系统属性。

人类的科学知识，按有序程度的高低，可以分为三类：关于事物的直接知识、系统知识和大系统知识。关于事物的直接知识，有很大的局限性。为了认识事物，不应只看到事物本身，而要把它看作一定种类的代表。因此，关于事物的直接知识必然发展到系统知识。系统知识揭示了事物的现实联系、事物的共同性和某些特殊的规律，它是认识事物较高级的形式和阶段。各门学科的知识大都属于系统知识。大系统知识服从于各种规模的各类系统的组合和相互作用，它揭示了客体的一切现实形态和相互作用，这是知识最高级的形式。

4. 动态性原理

动态是指状态与时间的相关性。动态性原理是研究系统元素间的联系随时间的变化规律。

现代科学研究的对象大都是结构复杂和高度活动的系统，系统学中的动态性原理就是适应这种客观需要产生的。我们不仅要研究各种系统发展变化的方向和趋势、活动的速度和方式，而且要探索它们发展变化的动力、原因和规律，从而主动驾驭这些系统，使之造福于人类。动态性原理反映了辩证法的发展原理。

系统发展变化的动力，来自系统内部对立面的斗争和统一，即内在矛盾。自然界的变化，主要是由于自然界内部矛盾的发展变化。社会的变化，主要是由于社会内部矛盾的发展、生产力和生产关系的矛盾、新和旧的矛盾、正确与错误的矛盾的变化。把科学作为一个相对独立的系统来考察，科学的发展动力直接来自科学能力和科研体制的矛盾运动，社会经济等条件的变化是重要的外部原因。科学的进步必须通过科学研究系统内部科学能力的提高和科研体制的改善来推动。

5. 分解综合原理

分解是将具有比较密切结合关系的要素分组化。对系统来说，分解就是分析出相对独立、层次不同的子系统。综合则是完成新系统的设计过程，即选择具有性能好、适用性强以

试读结束，需要全本PDF请访问

及标准化了的子系统，设计出它们之间的关系，形成具有更广泛价值和特定功能的系统，以达到预期的目的。

系统的分解与综合是系统学的重要原理之一。要设计出新的系统，必须分析已有的系统，已有的系统又是前人分析的综合。可以说不论多大、多复杂的系统，如分解为适当的几个子系统，就能根据过去的经验和知识去处理。如果将这些系统或子系统的特征和性能标准化，并编成程序，运用到计算机中，设计就容易多了。

分解的方法是多种多样的，一般可按结构要素分解，按功能要求分解，按时间序列分解，按空间状态分解等。分解的原则，既要有利于系统设计、可靠，又要便于论证、实施和管理。分解的形式有示意图、关系图、树形图、网络图等。

6. 创造思维原理

管理者的责任在于创造性地工作，工程师的天职在于创造性地设计与施工。创造思维的基本原理有两条：一是把陌生的事物看作熟悉的东西，用已有的知识加以辨别和解决。这是人们惯用的方法，它不只对新的事物给以旧的解释，也能给以新的解释，从而创造出新的理论。二是把熟悉的事物看作陌生的东西，用新的方法、新的原理加以研究，创造出新的理论、新的技术和方法。

创造思维活动极其复杂，它的形式多种多样，并且常常是多种形式互相重叠交错在一起。掌握这条原理，可以克服思维过程中的障碍，通过训练提高创造能力，增强系统设计者的素质，加速系统的综合。

7. 验证性原理

人类的生产活动是最基本的实践活动，是决定其他一切活动的基础。实践是检验真理的唯一标准。人类对于事物的认识，主要依赖于人类社会的生产活动。只有人们的社会实践，也就是验证，才是检验客观世界真理的标准。实际上，在处理系统问题时，无论是管理系统，还是工程系统，要达到预期的目的，只能通过反复的实践、验证、总结，才能产生认识过程的突变，产生新的概念。

一般来说，在处理系统问题时，不能用数学解析式描述系统问题的，总是先提出假设，通过试验对可能出现的故障进行分析判断，为执行者提供数据进行核实和检验，以及通过试验为用户提供验收条件，甚至借助试验验证、修正假设和理论。

8. 反馈原理

反馈是输入的信息和资源经过处理后，将结果（即输出）再送回输入状态的程序，并对新输入信息和资源产生影响的过程。反馈使事物本身与周围环境处于动态的统一之中，构成了新陈代谢运动，架起了原因和结果的桥梁。

反馈按控制结果可分为以下两类。

（1）正反馈。系统的输入与输出的差异是发散的，即加剧该系统正在进行的动态过程，使系统趋于不稳定状态，乃至破坏稳定状态。

（2）负反馈。系统的输入与输出的差异是收敛的，即倾向于反抗系统正在偏离目标的过程，使系统趋于稳定状态。

现代管理系统，是十分复杂的系统，人、财、物的组合关系多种多样，时空变化和环境影响很大，内部运动和结构在不断变化，随机性很大，组织关系错综复杂，使人的思维、信息的动力作用加大，从而使反馈原理在现代管理中处于十分重要的地位。在安全管理系统

试读版权归化学工业出版社所有 仅供试读期间线上浏览使用

中，领导者、安全管理者起着控制作用；信息资料部门起着接收、处理各种安全信息的作用；负责检查工作的部门则起检测作用；执行任务者就起着实现安全目标的关键作用。领导、管理者将安全生产、检修计划指令下达后，必须经常深入基层检查安全措施的执行情况，在职工群众中听取反映，及时根据反馈进行调整、修改安全措施，保证安全生产和检修目标的实现。

1.1.5　系统方法的地位和作用

系统方法是哲学方法和其他科学研究方法之间的中间环节，是唯物辩证法的具体化和实际运用，也是科学理论与实践相结合的工具。它广泛适用于科学研究的各个阶段和各个环节，贯穿于科学研究和人类社会实践的全过程。如今许多传统的研究方法，正在受到和将要受到系统方法的冲击和洗礼。

1. 系统方法是哲学方法和其他科学研究方法之间的桥梁

随着现代科学技术的发展和方法论研究的深入，各种科学的研究方法按照其概括程度和适用范围的不同，分别处于不同的层次。目前，科学方法论按水平方向描述，一般可分为三个层次。

（1）哲学方法。探讨一切科学普遍适用的方法原理，它既指导自然科学的研究，也指导社会科学的研究。

（2）一般科学方法。探讨自然科学和社会科学共同适用或分别适用的一些原则和方法。它具有跨学科性质，能够从一门学科转移到另一门学科。一般科学方法包括数学方法、控制论方法、信息方法、系统方法和基本的逻辑方法，它们是自然科学和社会科学都适用的；观察方法和试验方法等适用于自然科学，社会调查和典型试验等适用于社会科学，这两类方法也列入一般科学方法的范畴。

（3）专门科学方法。探讨各门科学专门的具体方法和技术。例如在安全管理系统中，运用安全系统工程的事故树方法来预测事故发展的规律性等。

系统方法在方法论体系中的地位属于第二层次，发挥一般科学方法的功能。它是在辩证法的指导下形成自己的方法论，在各门学科运用系统方法的基础上概括出一套专门的概念工具。系统方法包含的哲学内容十分丰富，需要认真探讨，这也会促进哲学的发展。

系统方法为科学知识数学化提供中间过渡模式，加快了各门科学数量化的进程。以控制论为理论指导的功能模拟方法，是以事物、机器以及社会现象中所普遍存在的某些功能和行为的相似性为基础，模拟原型的功能和行为的方法。以信息论为基础的信息方法，就是把有目的的运动，看作一个信息的获取、传递、加工和处理的过程，把系统内外各种因素的相互关系，看作信息的交换过程而加以研究的方法。功能模拟方法和信息方法，作为系统方法的研究范围，从其概念可知它们之间的关系是十分密切的。

系统方法在研究社会现象时，比其他任何方法更能把分析和综合、归纳和演绎等方法有机地结合起来，因而为应用数理逻辑方法和现代电子计算机开辟了广阔的道路。

由此可见，系统方法一方面与哲学方法——唯物辩证法直接衔接，另一方面又与其他科学方法紧密结合，它在促进科学方法论知识的整体化，加强哲学与自然科学、技术科学、社会科学的联系方面，发挥着越来越重要的作用。

试读结束，需要全本PDF请访问 教学使用

2. 系统方法既是确定目标的方法，又是实现目标的方法

各种科学研究方法，按照它们在认识过程中的功能一般可分为确定目标的方法和实现目标的方法。实现目标的方法又分为接受信息的方法和加工信息的方法。前者包括观察方法、试验方法以及调查方法；后者包括分析法和综合法、归纳法和演绎法、科学抽象法等。这样，科学方法论体系就形成一种垂直方向的结构。系统方法则横贯并作用于各种科学研究方法，在确定目标和实现目标两个方面，都形成了一些新的专门方法和技术。

系统方法在确定目标方面发挥的重要功能是加强了传统的科学方法论研究中主要关心和侧重实现目标的方法，而较忽视确定目标方法的研究这个比较薄弱的环节。确定目标的过程也是一个认识过程，其中包括接受信息，获得感性材料以及加工信息，整理感性材料，上升到理性认识两个阶段。随着科学技术的进步和社会的发展，人们在现代的科学研究活动中，创造和发展了一系列先进方法，如系统分析，使确定目标的方法程序化、精确化，从而使这种方法的效果达到最佳化。

系统分析要求对特定的问题进行周到和必要的调查，掌握大量数据资料，运用数学方法和计算机进行精确运算，针对目标制定各种可行和适用的方案，提出可行的建议，帮助决策者进行最佳决策。它全面贯彻了系统方法的基本原则。实践证明，这是确定目标和制订计划的现代化的科学方法。

1.2 系统工程简介

系统工程是系统思想在工程上的实践。所谓工程，是将自然科学原理应用到各系统中而形成的各学科的总称，如环境工程、水电工程、管理工程等。系统工程是对系统进行合理规划、研究、设计和运行管理的思想、步骤、组织和技巧等的总称，它是以实现系统最优化为目的的一门基础科学，是一种对所有系统都具有普遍意义的科学方法。这个定义表示：①系统工程属工程技术范畴，主要是组织管理各类工程的方法论，即组织管理工程；②系统工程是解决系统整体及其全过程优化问题的工程技术；③系统工程对所有系统都具有普遍适用性。

系统工程是20世纪50年代发展起来的一门新兴科学，是以系统为研究对象，以现代科学技术为研究手段，以系统最佳化为研究目标的工程学。

系统工程从系统的观点出发，跨学科地考虑问题，运用工程的方法去研究和解决各种系统问题。具体地说，就是运用系统分析理论，对系统的规划、研究、设计、制造、试验和使用等各个阶段进行有效的组织管理。它科学地规划和组织人力、物力、财力，通过最佳方案的选择，使系统在各种约束条件下，达到最合理、最经济、最有效的预期目标。它着眼于整体的状态和过程，而不拘泥于局部的、个别的部分。这是因为系统工程采用了新的方法论，这种方法论的基础就是系统分析的观点，即一种“由上而下”“由总而细”的方法。它不着眼于个别单元的性能是否优良，而是要求巧妙地利用单元间或子系统之间的相互配合与联系，来优化整个系统的性能，以求得整体的最佳方案。

1.2.1 系统工程的发展概况

19世纪后半叶及20世纪初先后出现了电子系统工程学、控制系统工程学、人机系统工

试读结束，需要全本PDF请访问

程学等学科，大大促进了 20 世纪科学技术如航天技术以及计算机技术的发展，同时，也促使军事技术迅速发展，在第一次和第二次世界大战中得到广泛的应用。

20 世纪 30 年代末，英国面临德国的侵略，一批科学家研究雷达系统的运用问题，创造了“运筹学”一词来命名这个应用科学的新分支。在第二次世界大战期间，运筹学逐步推广到军事决策和战争指挥，著名的大西洋潜艇战役和北非登陆战役，都借助于运筹学取得了胜利。这是系统工程的萌芽。

20 世纪 40 年代初，美国贝尔电话公司首先创造了“系统工程”这一学科名称，在发展微波通信网络时，初步运用了系统工程的方法。以后，贝尔公司和丹麦哥本哈根电话公司在电话自动交换机的工程设计中运用了系统方法。美国研制原子弹的曼哈顿计划，采用系统工程方法获得成功，成为典型事例。1940 年，爱因斯坦等科学家提出研制原子弹的建议，美国总统罗斯福采纳后，请理论物理学家奥本海默来组织领导这项军事科研生产计划。他动员了 15000 名科学家和工程师，组织各种专业科技人员进行全面合作。在执行计划的过程中，奥本海默从整体出发，把研究课题逐级分解为许多小课题，组织相应的小组分别从事各个相同或不同课题的研究工作；他非常重视各项课题之间的联系，注意它们的等级和层次，随时进行协调，使所有课题结合起来达到整个计划的最优结构；在生产原子弹材料的中心研究项目方面，他组织大家仔细研究，提出六七千个方案同时试用，在实践中比较优劣。1944 年 5 月，第一颗原子弹爆炸成功，这是大规模地组织起来顺利地完成一项军事科研生产任务的著名实例，是系统工程方法应用的胜利。

1967 年，举世瞩目的美国航天局阿波罗登月计划的实现，是正式运用系统工程的巨大成功。这一规模巨大的载人登月计划，参加的科学家和工程师达 42 万人，投资 300 亿美元，参加单位 2 万多个，历时 11 年完成全部任务。这是科技史上的伟大壮举，它标志着人类在组织管理的技术方面正在走向一个新的时代。由此引发的美苏在航天技术上的相互竞争，促进了各个学科之间的相互渗透，使得系统的原理和方法在实用科学领域的应用和发展出现了前所未有的高潮。同时，世界范围内重大事故频频发生，引起了人们对系统可靠性和安全性的研究和开发的高度重视，出现了运用系统的原理和方法对系统安全进行研究的科学方法。为其他科学领域的飞跃，提供了可靠的理论基础和实践基础。

钱学森教授对系统工程的建立和发展，做出了重大的贡献。首先，他提出了一个清晰的现代科学技术的体系结构，认为从应用实践到基础理论，现代科学技术可以分为四个层次：第一个层次是工程技术；第二个层次是直接为工程技术做理论基础的技术科学；第三个层次是基础科学；第四个层次是通过进一步综合、提炼达到最高概括的马克思主义哲学。整个科学技术包括自然科学、社会科学、系统科学、思维科学和人体科学五大门类。其次，他提出了一个清晰的系统科学结构。作为现代科学技术五大门类之一的系统科学，是由系统工程的工程技术，系统工程的理论方法，像运筹学、控制论和信息论这类技术科学，以及系统的基础理论，像系统学等组成的一个新兴科学技术部门。钱学森教授对系统科学的发展，还表现在他认为系统工程是组织管理的技术，并使之定量化，以便运用数学方法；系统工程是一大类工程技术的总称，而不是一个单一的学科，正如人们传统理解的工程是土木、机械、机电等工程的总称一样。于是便将“人各一词，莫衷一是”的情况澄清为“分门别类，共居一体”。这就给系统工程一个确切的描绘，进而论述了系统工程在整个系统科学体系中所处的地位。

试读结束，需要全本PDF请访问 www.ertongbook.com

系统工程在我国已受到普遍的重视和应用。在全面质量管理、计划评审技术、库存管理、价值工程等方面的应用都取得了显著效果；在生态、区域、能源规划和人口控制、教育系统以及各类工程系统中也得到了较好的应用。

1.2.2　系统工程的定义

系统工程（System Engineering）是为了使系统性能的公认尺度达到最大而进行的关于许多系统元素相互间复杂关系的设计，在设计时对以任何方式和系统相关联的所有因素加以考虑，包括人力的利用以及该系统各个组成部分特性的利用。它是一种管理方法，是一种用于管理系统的规划、研究、设计、制造、实验和使用的科学方法。

系统工程是以系统为研究对象的一门边缘学科。它是根据总体协调的需要，把自然科学和社会科学中的某些思想、理论、方法、策略和手段等有效地结合起来，应用于人类实践，运用系统理论、现代数学、控制论、信息论和计算机等工具，对系统的构成要素、组织机构、信息交换和自动控制等功能进行分析研究，从而达到最优设计、最优控制和最佳管理的目的，是为更加合理地研制和运用系统而采取的各种组织管理技术的总称。也可以简单地定义为：系统工程是组织管理“系统”的规划、研究、设计、制造、试验和使用的科学方法，是一种对所有“系统”都具有普遍意义的科学方法。这个定义，比较明确地表述了三层意思：系统工程属于工程技术，主要是组织管理的技术，是解决工程活动全过程的工程技术，这种技术具有普遍的适用性。

1.2.3　系统工程的理论基础

系统工程是一门边缘学科，涉及很多学科，但究其理论基础，大致可分为两类：共同理论基础和分支理论基础。

共同理论基础是奠定和发展系统工程理论和方法的专业知识。如运筹学、控制论、信息论、计算科学等，其发展为系统工程提供了理论和方法，对系统分析、综合、优化和控制提供了可靠的理论依据和手段。

系统工程的分支理论基础是系统工程实践中所需的专业知识。它是系统工程应用到某一特定领域时所需的特殊理论基础。如安全系统工程是系统工程在安全领域中的应用，应用时，必须以安全工程为其理论基础，才能解决生产过程中的安全问题，并使之达到最优状态。

1.2.4　系统工程的特征

系统工程的基本原理就是用管理工程的办法组织管理整个系统。它以系统为对象，把要组织和管理的事物，用概率、统计、运筹和模拟等方法，经过分析、推理、判断和综合，建成某种系统模型，以最优化的方法，求得最佳化的结果。使系统达到技术上先进、经济上合算、时间上节约、能协调运转的最优效果。因此，它具有以下特征：

（1）优化的方法使系统达到最佳。

（2）与具体的环境和条件、事物本来的性质和特征的密切相关性。

（3）它着眼于整个系统的状态和过程，而不拘泥于局部的、个别的部分，它表现出系统最佳途径并不需要所有子系统都具有最佳的特征。

试读版仅供防疫期间学习使用

（4）它包含着深刻的社会性，涉及组织、政策、管理、教育等上层建筑因素。

（5）它的精华在于，它是软技术，即在科学技术领域，由重视有形产品转向更加重视无形产品带来的效益。

1.2.5　系统工程的基本观点

根据系统工程的特征，在处理问题时，以下一些系统工程的基本观点是值得强调的。

1. 全局的观点

就是强调把要研究和处理的对象看成一个系统，从整个系统（全局）出发，而不是从某一个子系统（局部）出发。例如美国喷气推进实验室早就研究喷气发动机，后来美国陆军希望搞一个“下士”导弹系统，它涉及弹头、弹体、发动机和制导系统等。当时想用该实验室研制的发动机，由于开始没有从总体考虑，只是把已有的东西（各个系统）进行了拼凑，虽然可以使用，但造价昂贵，不便维修，很不成功。后来搞“中士”导弹系统，该实验室提出要参与整个导弹系统的设计，也即对全系统的“特定功能”有所了解，而且要求了解设计、生产、使用的全部过程，结果“中士”导弹系统各个方面的功能大大得以改进。

全局性的观点承认并坚持：凡是系统都要遵守系统学第一定律，即系统的属性总是多于组成它的元素在孤立状态时的属性；在复杂系统内部或这个复杂系统和环境中其他系统之间，存在着复杂的互依、竞争、吞噬或破坏关系；一个系统可以在一定的条件下由无序走向有序，也可以在一定的条件下由有序走向无序；对于非工程系统的研究，必须保证模型和原系统之间的相似性等基本观点。

2. 总体最优化的观点

人们设计、制造和使用系统最终是希望完成特定的功能，而且总是希望完成的功能效果最好。这就是所谓最优计划、最优实际、最优控制和最优管理和使用等。这里需要使用运筹学中的优化方法、最优控制理论、决策论等。值得注意的是近年来关于多目标最优性的讨论，由于考虑的功能很多，有的系统方案在这方面功能较好，而另一方面较差，很难找到一个十全十美的系统。因此在一些互相矛盾的功能要求中，必须有一个合理的妥协和折中，再加上定性目标的研究有时很难做到定量的最优化。因此，近年来有人开始提出“满意性”的观点，也就是总体最优性的观点。

系统总体最优性包含三层意思：一是空间上要求整体最优；二是从时间上要求全过程最优；三是总体最优性是从综合效应反映出来的，它并不等于构成系统的各个要素（或子系统）都是最优。

3. 实践性的观点

系统工程和某些学科的区别是它非常注重实用，如果离开具体的项目和工程也就谈不上系统工程。正如钱学森同志指出的：“系统工程是改造客观世界的，是要实践的。”当然，实践性并不排斥对系统工程理论的探讨和对其他项目系统工程经验的借鉴。

4. 综合性的观点

由于复杂的大系统涉及面广，不但有技术因素，还有经济因素、社会因素等，仅靠一两门学科的知识是不够的，需要综合应用诸如数学、经济学、运筹学、控制论、心理学、社会学和法学等各方面的学科知识；由于一个人所掌握的学科知识有局限性，所以系统工程的研

试读，需要完整PDF请访问：www.ertongbook.com

究需要吸收各方面的专家、领导、工程技术人员乃至有经验的工人参加，组成一个联合攻关和研讨小组开展工作。

5. 定性和定量分析相结合的观点

运用系统工程来研究并解决问题，强调把定性分析与定量分析结合起来。这是因为在处理一些庞大而复杂的系统时，经典数学的精确性与这些大系统的某些因素的不确定性存在着不少矛盾。因此，在对整个系统进行定性分析和定量分析时，必须合理地将定性分析与定量分析有机地结合起来。脱离定性研究来进行定量分析，就只能是数学游戏，不能说明系统的本质问题；同样，只注意对系统进行定性分析，而不进行定量研究，就不可能得到最优化的结果。

1.3 系统分析的基本内涵

系统学原理认为，世界上各种对象都是由具有内在联系的各部分组成的有机整体。整体的效果和功能，不仅取决于其组成部分的效果和功能，而且还取决于它们的相互联系和相互作用，还受到环境条件的限制。系统工程研究的对象主要是复杂系统。这些系统与环境的关系、与子系统的关系以及子系统之间的关系一般说来都非常复杂，不仅涉及工程领域，还涉及社会、经济和政治领域；除有确定的因素外，还存在着许多不确定的矛盾因素。对这些因素能否及时了解、掌握和正确处理，将影响到系统整体功能和目标的完成。系统本身的目标和功能是否合理也需要研究。不明确、不恰当的系统目标和功能，往往会给系统的生存带来严重的后果。因此，不论是组建新系统或是改进现有系统，都必须对系统的目标和功能、环境以及系统内部关系进行认真分析，做出正确的决策，使系统和环境相适应，系统内部相互协调，以保证系统整体功能和目标的完成。系统分析就是完成此项任务的中心环节，在系统工程中起着最重要的作用。

1.3.1 系统分析的概念

关于系统分析的概念有许多说法。一般说来，系统分析就是从系统总体出发，对需要改进的已有系统或准备创建的新系统使用科学的方法和工具，对系统目标、功能、环境、费用效益等进行调查研究，并收集、分析和处理有关资料和数据，据此建立若干备用方案和必要的模型，进行模拟、仿真试验，把试验、分析、计算的各种结果进行比较和评价，并对系统的环境和发展做出预测，在若干选定的目标和准则下，为选择对系统整体效益最佳的决策提供理论和试验。与技术经济分析不同，系统分析从系统总体最优出发，采用各种分析工具和方法，对系统进行定性和定量分析。它不仅分析技术经济方面的有关问题，而且还分析包括政策、组织体制、信息、物流等各有关方面的问题。

系统分析是一种辅助决策工具。借助系统分析，决策者可以获得对问题的综合和整体的认识，既不忽略内部各因素的相互关系，又能顾及外部环境变化带来的影响。特别是系统分析借助各种模型、模拟试验和定量计算，可为决策者提供可靠的数据依据。显然，科学的系统分析会使决策建立在科学的基础上，以最有效的策略解决复杂的问题，顺利地达到系统的各项目标。

系统分析的目的和作用如图 1-1 所示。

此资源仅供清华同方大学教学使用

图 1-1　系统分析的目的和作用

1.3.2　系统分析的特点

（1）以整体为目标。系统分析以发挥系统整体最大效益为准则，而不是局限于个别子系统，以防顾此失彼。系统分析以特定问题为对象。系统分析是一种处理问题的方法，有很强的针对性，其目的在于寻求解决特定问题的最优方案。

（2）运用定量方法。系统分析解决问题不是单凭主观臆断、经验和直觉。在许多复杂情况下，必须以相对可靠的数学资料为分析依据，保证结果的客观性。

（3）凭借价值判断。系统分析不但使用定量方法找出系统中各要素的定量关系，还要依靠直观判断和经验的定性分析，凭借价值判断，综合权衡，以判别由系统分析提供的各种不同策略可能产生的效益优劣，从中选择最优方案。

1.3.3　系统分析的原则

系统的性质取决于系统的要素以及要素之间的相互关系，又受到环境的影响，关系错综复杂，存在着许多矛盾的因素。因此，在系统分析时，必须认真协调和处理好各种因素的相互关系，特别是对复杂系统进行分析时，应遵循下列原则。

（1）外部条件和内部条件相结合。系统的性能不仅取决于系统的内部结构，还受环境条件的制约。在分析一个系统时，应将系统内部、外部各种有关因素结合起来考虑。

（2）当前利益和长远利益相结合。选择一个比较好的方案，不仅要从当前利益出发，而且要考虑到长远利益。只顾当前利益不考虑长远利益的方案是不可取的；对当前不利而对长远有利，也是不理想的；对当前和长远都有利，才是最理想的方案。

（3）局部效益和整体效益相结合。局部效益好并不意味着整体效益也很好，整体效益好往往要求某些局部效益做出一定的牺牲。系统分析要求整体效益最优化。局部效益好但整体效益不好甚至有损失的方案是不可取的；局部效益低而全局效益好的方案才是可取的。

（4）定量分析与定性分析相结合。定量分析是指数量指标的分析，可用实现模型表示，这是评价方案优劣的依据。但绝不能忽视定性因素如某些政治、政策、心理因素、社会效果等。这些因素无法用数学模型表示，只能进行定性分析，即根据经验主观判断和统计分析来解决。此外，定量分析必须以定性分析为指导，不对系统作深入了解，就不能建立探讨定量分析的数学模型。定性和定量两者应结合起来综合分析，或者互相交错进行，才能达到优化的目的。

1.3.4　系统分析的方法和工具

系统分析没有一套特定的普遍适用的技术方法，根据分析对象和分析的问题不同，所使用的具体方法也不同。一般来说，系统分析的各种方法可分为定性和定量的方法两大类。

定量方法主要是运用统计学和运筹学中各种模型化和最优化的方法，如线性规划、动态规划、网络技术、排队论、投入产出分析、决策分析等。定量方法适用于系统机理清楚、收

武汉纺织大学线上教学使用

集到的信息准确、可建立数学模型等情况。如果要解决的问题涉及的机理不清，收集到的信息不准确、模糊不清，或是伪信息，难以形成常规的数学模型，可以采用定性分析方法。定性分析方法有专家调查法、头脑风暴法、冲突分析法、层次分析法等。

系统分析的工具主要是计算机。系统工程的主要研究对象是规模庞大、结构复杂、层次丰富的复杂系统，涉及大量信息的收集、处理、存储、汇总、分析。另外，系统中往往存在着许多不确定的或互相矛盾的因素，为弄清这些因素和系统功能之间的关系，需要建立相应的模型，进行复杂的科学计算、仿真试验。这些都只有借助计算机才能完成。

1.3.5　系统分析的应用范围

系统分析工作的重点应放在系统发展规划方面，系统的发展规划对系统开发的前途、命运起着主导作用。从管理系统来说，主要应用于以下几个方面。

（1）在制定系统规划方案时，应将各种资源资料条件、统计资料以及生产目标要求等，运用规划论的分析方法寻求最优化方案，然后综合其他因素，在保证系统协调一致的前提下，对系统的输入、转变到输出进行均衡，从中选择一个比较满意的规划方案。

（2）对重大工程项目的组织管理，要运用网络分析方法进行全面的计划协调和安排，以保证工程项目中各个环节相互密切配合，按期完成。

（3）在选择厂址和工厂规模时，应考虑原材料的来源、能源、运输以及市场等客观条件与环境因素，运用系统分析进行技术论证，集思广益，制定出适合我国国情、技术上先进、生产上可行、经济上合理的最优方案。

（4）在设计一个新产品时，应对新产品的使用目的、结构、用料以及价格进行价值分析，再根据分析的结果来确定新产品最适宜的设计性能、结构、用料选择和市场接受的价格水平等。

（5）在资金成本管理中，要做到预算控制，对生产活动的技术改造和技术革新措施，都要进行成本盈亏分析，然后再决定哪一种方案更为经济合理。

（6）厂内的生产布局和工艺路线组织方面，要对人员、物价和设备等各种设施所需要的空间做出最恰当的分配和安排，并使相互间能有效地组合和安全运行，从而使工厂获得较高的经济效益。

（7）在编制生产作业计划时，可以运用投入产出分析方法，使零部件投入产出与生产能力平衡，确定最合理的生产周期、批量标准和在制品的储备周期，并运用调度管理，安排好加工顺序和装配线平衡，实现准时生产和均衡生产。常见的系统分析内容有环境分析、目标分析、功能分析和价值分析等。

（8）对工厂企业安全管理体系进行安全分析时，要了解安全管理现状，分析安全管理目标，实现企业的安全生产目标。

1.3.6　系统分析的要素

系统分析的要素有目标、方案、费用效果、模型和评价基准。

（1）目标。是为了达到一定的目的而对系统对象设计所期望达到的结果和方向，是目的的具体化，是系统分析的出发点。经过分析确定的目标应是具体的、有根据的、可行的。

（2）方案。一般情况下，为达到一定的目的和所期望的目标，可采用多种手段，这些

试读结束，需要全本PDF请访问 www.ertongbook.com

手段为可行性方案。系统分析要求尽量列举各种替代方案，并且估计它们可能产生的结果，以利于分析研究和选择。可行性方案是选优的前提，没有足够数量的可行性方案就没有优化。在列举各种方案时要考虑两点：一是所运用的方法是否可行；二是所采用的方案是否可靠。

（3）费用效果。为实现系统目标就必须投入，其实际支出就是费用。费用有可用货币表示的费用和非货币支出的费用两种。后者如失去的机会、所做的牺牲等。为了某种目的而选择的特定手段，使得一些资源或时间不能用于其他目标，所以会产生牺牲。

效果就是达到目的所取得的成果。它有“效益”和“有效性”两种指标。效益可以用货币表示，而有效性是通过货币以外的指标来衡量的。效益又有直接效益和间接效益之分。

为达到一定的目标，不同的替代方案消耗的资源不同，产生的效果也不同。费用与效果的分析与比较是决定方案取舍的重要标志。在分析和对比时，除考虑货币支出费用和效益外，还必须注意非货币支出的费用和有效性。

（4）模型。模型是对研究对象的某一方面本质属性的简化、模拟和抽象，是分析研究对象的有关因素之间关系和规律的有力工具。因为人和现实系统本身总是十分复杂，特别是在各种替代方案实施之前，尚不能对系统本身进行比较，分析各种方案的优劣。借助模型可进行这种分析比较。通过模型可以预测出各种替代方案的目标、性能、费用与效益、时间等指标情况，以利于方案的分析和比较，模型的优化和评价是方案论证的判断依据。

（5）评价基准。它是衡量可行性方案优劣的指标。由于系统往往是多目标，用单个指标来评价是不充分的，必须用一组互相联系的可以比较的指标来衡量，这就是系统的指标体系。不同的系统可有不同的指标体系，可根据有关要求具体地去确定。有了指标体系，就可以分析各种可行性方案对各项指标的实现程度，并进行综合评价，权衡利弊，确定出各种方案的优劣顺序。

1.3.7　系统分析的步骤

人们在从事系统工程的研究工作中逐步形成了一套科学的工作方法和步骤，这些步骤的划分并不是一成不变的，有的把一个步骤分成几步来做，有的则相反。目前，一般采用美国学者霍尔（A. D. Hall）1969 年提出的系统工程“三维结构体系”作为系统分析步骤的基础。

霍尔将系统工程的活动，按时间顺序分成七个阶段，又把每个阶段按解决问题的逻辑关系分成七个步骤，同时考虑完成各个阶段和步骤所需要的专业知识，组成一个立体空间结构，即时间维、逻辑维和知识维，称为系统工程的三维结构，如图 1-2 所示。它为系统工程提供了一个立体思维方法。

1. 逻辑维

逻辑维是解决问题的思维过程，是系统开发时所经历的工作程序体系。一般把这一过程分为七个步骤。

（1）摆明问题。收集有关信息，摆出问题，并说明问题的症结所在。

（2）指标设计。确定解决问题的目标及评价标准。

（3）系统综合。拟定达到目标可能采取的各种策略和方案，并对其做出必要的评价与说明。

试读版本仅供防火期间试读教学使用

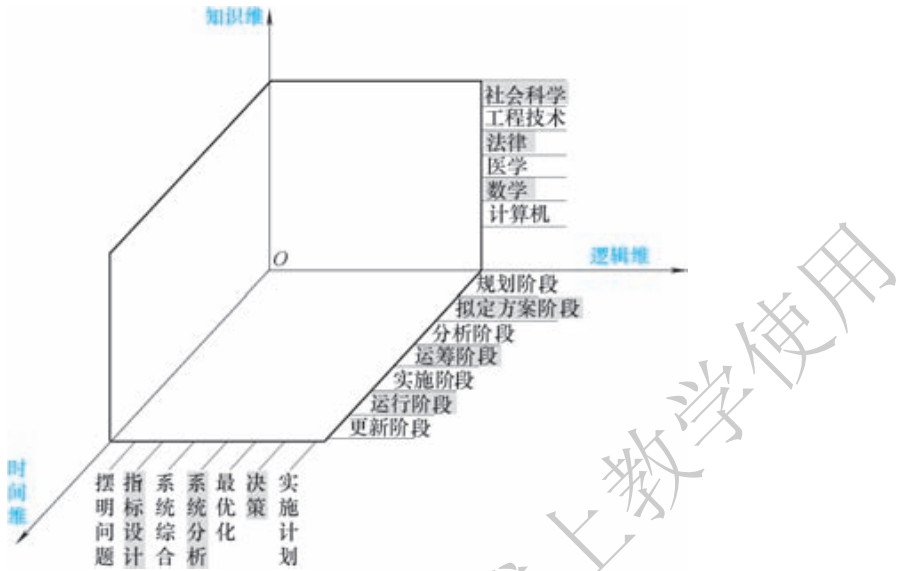

图 1-2　系统工程的三维结构体系

（4）系统分析。建立模型，进行综合研究，对各方案进行比较，为最优化打下基础。

（5）最优化。在系统分析的基础上，选定各个策略参数，使之最优化地满足评价标准。

（6）决策。对各种方案进行分析比较，选择其中最优化方案，做出决策。

（7）实施计划。组织实施已定的决策方案。

2. 时间维

时间维是系统从计划到使用、更新的全过程按时间顺序分工的工作阶段，一般分为七个阶段：

（1）规划阶段：确定系统开发目标和计划阶段。

（2）拟订方案阶段：制定或设计系统开发的方法。

（3）分析阶段：为实现方案进行研究。

（4）运筹阶段：通过具体计算、分析，对方案进行技术修订。

（5）实施阶段：实施确定的方案。

（6）运行阶段：将系统处于运转状态（工作状态）。

（7）更新阶段：对系统中存在的问题进行改善，或系统经过长时间运行后，进行更新改造。

3. 知识维

知识维是在系统分析、综合、优化、实施等过程中所需要的基础和专业知识，除系统工程的理论基础外，还需要用到社会科学、法律、医学、人机工程学等。

从以上分析可以看出，系统工程方法论既把研究对象作为一个整体，又把每个研究过程看作一个整体，如时间维中规划阶段需采用逻辑的思考过程，从整个时间阶段来看也需采用逻辑维的步骤，这就是系统工程方法论的基本指导思想。将上述 7 个逻辑步骤和 7 个时间工作阶段归纳起来，就可以构成系统工程的活动矩阵（见表 1-1）。

试读版本仅供防疫期间线上教学使用

表 1-1　系统工程的活动矩阵

时　间　维		逻　辑　维						
		1	2	3	4	5	6	7
		摆明问题	指标设计	系统综合	系统分析	最优化	决策	实施计划
1	规划阶段	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}
2	拟订方案阶段	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}
3	分析阶段	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}
4	运筹阶段	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	a_{46}	a_{47}
5	实施阶段	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}	a_{56}	a_{57}
6	运行阶段	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	a_{66}	a_{67}
7	更新阶段	a_{71}	a_{72}	a_{73}	a_{74}	a_{75}	a_{76}	a_{77}

从系统工程的“三维结构体系”得到系统分析的基本步骤。

（1）限定问题。问题就是实际情况与理想状态之间的差距。实际情况与人们原来的要求、设想不符，使人们感到不能满意、不能容忍时，就可说是出了问题。系统分析的主要目的是寻求解决特定问题的最优方案。显然，进行系统分析，首先要明确所要解决的问题，弄清问题的实质。问题常常不是一目了然的，往往为一些表面现象甚至假象所掩盖而不易察觉。为了准确地发现问题，需要收集有关资料和数据，掌握对象的历史和现状，预测未来发展趋势，进行纵横比较，甚至组织专家进行诊断。问题发现后，进一步的工作就是限定问题。通常，问题是在一定的外部环境条件下和系统内部发展的需要中产生的，有其本质属性和存在的范围，只有明确了问题的性质和存在的范围，在系统分析时才能有可靠的起点。限定问题就是明确问题的实质和范围，也就是弄清要解决的到底是什么问题，性质如何，严重程度怎么样，涉及哪些因素，应把哪些因素作为系统来研究，环境因素是什么。显然，界限与被研究的问题有很大的关系，问题不同，界限也不同。不能正确地构成问题，或者问题的范围过窄、过宽，或问题的重点和关键不明、不对，就不可能搞好系统分析。

（2）确定目标。弄清并提出为解决问题需要达到的目标。有了明确的目标，系统分析才能有的放矢，才能判断问题能否解决。系统可能只有单一目标，也可能有多个目标，复杂系统都是多目标系统。所确定的目标应明确、具体，应尽可能定量表示（也称指标），以便于定量分析；对那些不能进行定量描述的目标也应用文字说清楚，对这些目标只能进行定性分析。

（3）收集资料，提出方案。系统分析需要有可靠的数据和资料。资料来源包括统计调查资料和预测资料。收集资料可借助于调查、试验、观察、记录以及引用国外资料等方式。收集资料的要求是：第一，具有完整性，切忌盲目性，往往资料很多，但是并不都有用，应对照目标尽可能地收集和整理有关的直接和间接资料；第二，具有可靠性，对说明重要目标的资料必须经过反复核对和推敲。

方案是指达到目标的各种策略，达到同一特定目标可能有多种不同的方案。紧紧围绕所确定的目标，根据收集的资料找出影响目标的诸因素，集思广益，提出能达到目标的各种替代方案。

试读版本仅供预览，非线上教学使用

（4）建立模型。通过构造模型简化系统，确认影响功能和目标的因素及其影响程度、因素之间相互关系及其与环境因素之间的关系，以定量形式表示。

（5）分析效果。通过模型对各种替代方案可能产生的结果和目标能够达到的程度进行分析。比如费用指标，则应考虑投入的人力、设备、资金等，不同方案的输入、输出不同，其结果也不同。当模型复杂、计算工作量大时，应使用计算机进行计算或者模拟。

（6）综合评价。在上述定量分析的基础上，进一步考虑定性因素，以评价基准为尺度，对各种替代方案进行比较，排出优先顺序，最后选出一个或几个可供决策者选择的方案，以供参考。如对选择的方案不满意，可返回到开始步骤，重新分析。

以上只是一般步骤，对实际问题，应根据具体情况，采取不同的具体方法和步骤。

1.4 安全系统及安全系统工程

安全系统工程是运用系统论的观点和方法，结合工程学原理及有关专业知识来研究生产安全管理和工程的新学科，是系统工程学的一个分支。

1.4.1 基本概念

1. 安全与危险

安全和危险是一对互为存在前提的术语，在安全评价中，主要是指人和物的安全和危险。安全，是指免遭不可接受危险的伤害。它是一种使伤害或损害的风险限制处于可以接受的水平的状态。安全程度用安全性指标来衡量。其实质就是防止事故，消除导致死亡、伤害、急性职业危害及各种财产损失发生的条件。危险也是一种状态，指存在引起人身伤亡、设备破坏或降低完成预定功能能力的状态。当存在危险时，就存在产生这些不良影响的可能性。危险性表示危险的相对程度。

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，安全也存在危险，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

仅供学习使用 线上教学使用

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 1-3 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的活动所获得的利益与承受的危险之间的关系，如图 1-4 所示。

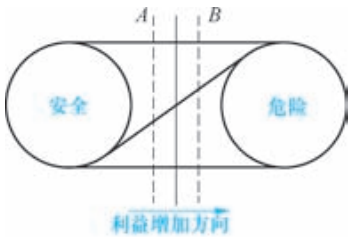

图 1-3　社会允许的危险

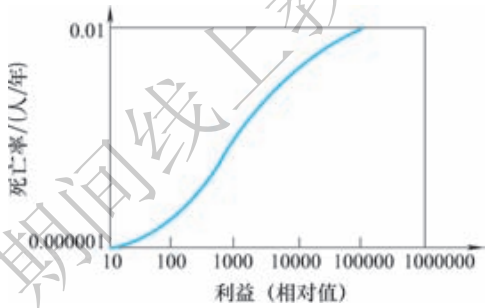

图 1-4　利益与危险关系

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。

在人们的心目中一般认为平均每年中只导致一次死亡 300 人的社会活动比导致平均每天死亡 1 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。

2. 安全标准

安全是一个相对的、主观的概念。评定状态是否安全需要有一个界限、目标或标准，通过与定量化的风险率或危害程度进行比较，判定其是否达到人们所期盼的安全程度。我们把这个标准称为安全标准。受技术、资金等因素的制约，危险是不可能完全杜绝的。安全标准实际上是一个社会各方面可以接受的危险度。

确定安全标准的方法有统计法和风险与收益比较法。对系统进行安全评价时，也可以对评价得到的危险指数进行统计分析，确定使用一定范围的安全标准。

对于有统计数据的行业，常用事故可能造成人员的伤亡或事故可能造成的经济损失作为

试读版本仅供防疫期间线上教学使用

制定安全标准的依据。根据海因利希事故调查报告统计规律：

死亡（重伤）：轻伤：无伤害 = 1：29：300

因而可以通过死亡率来推断伤亡情况，平均死亡率便可作为安全标准制定的依据。例如英国化学工业的 FAFR（工作一亿个小时的死亡率）为 3.5，英帝化学公司（ICI）提案取 0.35 作为安全标准。而美国各公司的安全标准大都取各行业安全标准的十分之一。

1.4.2　安全系统及其特点

1. 安全系统的概念

有了安全和系统的概念就不难给安全系统下定义：安全系统是以人为中心，由安全工程、卫生工程技术、安全管理、人机工程等几部分组成，以消除伤害、疾病、损失，实现安全生产为目的的有机整体，它是生产系统的一个重要组成部分。

2. 安全系统的特点

安全系统的特点可以归纳为如下若干方面：

（1）系统性。与安全有关的影响因素构成了安全系统。因为与安全有关的因素纷繁交错，所以安全系统是一个复杂的巨系统。由于安全系统中各因素之间，以及因素与目标之间的关系多数有一定灰度，所以安全系统是灰色系统。

依据安全问题所涉及范围大小不同，安全系统大小之差可能很悬殊。一般地讲，纯属技术领域的安全系统，比如一台设备、器具，可能只涉及机和物；而对于一个车间甚至一个工厂，考虑安全问题的系统范围，则不只是机和物，肯定要把人—机—环境都考虑进来。实际上，人—机—环境的提法是考虑了安全问题的空间跨度和时间跨度两个方面。如此说来，即便是一台设备，如果把它的制造安全与使用安全考虑进来，也仍然是人—机—环境的复杂系统。

安全系统的目标不是寻求最优解。这是因为安全系统目标的多元化，以及安全目标的极强相对性、时间延滞性与其理想化理念很难协调，所以安全系统的目标解是具有一定灰度的满意解或可接受解。

（2）开放性。安全系统是客观存在的，这是因为安全系统是建立在安全功能构件的物质基础之上的。但同时安全系统总是寄生在客体（另一个系统）中，在处理方法上，如果把客体看成一个黑匣子，安全系统是通过客体的能量源、物流和信息流的流入-流出的非线性变化趋势，确认安全和事故发生的可能性，因此安全系统具有开放性特点。

开放性不仅是安全系统在动态中保持稳定存在的前提，也是安全系统复杂性及安全-事故转换发生的重要机制。

（3）确定性与非确定性。“确定性”是指制约系统演化的规则确定性，不含任何随机性因素。确定性的特征是演化方向及演化结果确定，可精确预测。“非确定性”或者具有演化方向和演化结果不确定，或者具有刻画事物运动特征的特征量不能客观精确地确定的特征，非确定性包括随机性和模糊性。

“随机性”可能有两个方面的来源：一是在不含任何外在的随机影响因素作用下，完全由“确定性”系统演化而产生的随机性（例如产生混沌），这种随机性称为本质随机性。二是系统还可能因其外在影响因素的随机作用而产生随机性行为，从而使系统在一定条件下表

试读版本仅供防疫期间线上教学使用

现了随机的特征（外在随机性）。由于安全系统把环境看成是它的组成部分，所以对安全系统而言，本质随机性和外在随机性的区别不是绝对的。

“模糊性”是指事物的本身不清楚或衡量事物尺度不清楚。对于安全系统，就是指系统的构成及其相互关系，以及组成与目标的关系不清楚。造成这些不清楚的可能来源在于主观和客观两个方面，即具有主观模糊性和客观模糊性。首先，刻画安全运行轨迹的以模糊数学方法建立的数学模型具有主观模糊性。因为数学模型常常不可能“严格地”确定安全系统各因素之间及其与目标之间完整的客观关系。当然，对于自然的技术因素之间的关系尚好一些。而对于社会的因素及其与技术因素的耦合关系将难于量化，因而也将难于建立准确的数学关系。应该强调的是，出现上述问题不完全是由于安全系统本身不清楚，它可能只是人们的安全系统主观模糊性的表现。

另外，对安全系统安全度的评价尺度以及构成安全度等级的评价指标体系也具有客观模糊性，即从事物的本质上无法给出其客观衡量尺度。

（4）安全系统是有序与无序的统一体。序主要反映事物的组成规律和时域。依据序的性质，可分为有序、混沌序和无序。有序通常同稳定性、规则性相关联，主要表现为空间有序、时间有序和结构有序。无序通常与不稳定、无规则相关联。而混沌序则是不具备严格周期和对称性的有序态。现代复杂系统演化理论认为，复杂系统的演化中，不同性质的序之间可以相互转化。安全系统序的转化是否引发灾害或使灾害扩大，取决于序结构的类型及系统对特定序结构下的运动的（灾害意义上的）承受能力。

有序和无序，确定性和非确定性都会在系统演化过程中通过其空间结构、时间结构、功能结构和信息结构的改变体现出来。

（5）突变性或畸变性。安全系统发展过程的突变或畸变，或过程由连续到非连续变化，在本质上还是服从于量变引起质变的哲理。

量变到质变的转化形式可以用畸变、突变或飞跃来描述，但也可通过渐变实现。所以安全系统的渐变也可能孕育着事故，而突变、畸变则肯定对应于灾害故事的启动，是致灾物质或能量的突然释放。

综上所述，安全系统虽然与一般系统、非线性系统等有若干共同点，但安全系统的个性还是非常明显的，这是决定它客观存在并区别于其他系统的根本原因。

3. 安全系统的动力学特征

从系统的结构和功能形成看，可把系统分为两类：一类是自组织系统，一类是被组织系统。协同学的创始人哈肯教授曾给自组织下了一个非常经典的定义，他认为，如果系统在获得空间的、时间的或功能的结构过程中，没有外界的特定干预，我们便说系统是自组织的。这里的“特定”一词是指，那种结构或功能并非外界强加给系统的，而且外界是以非特定的方式作用于系统的。可见，自组织与被组织的区别就在于，系统行为是否受外界某种特定干预的影响。显然，自组织的动力在系统内部，是自己运动的结果；而被组织的动力在系统外部，是在外部特定的干预下运动的结果。一般而言，自组织系统因其动力来自系统内部，因而它具有持久永恒的生机和活力；相反，被组织系统因其动力来自系统外部，因而其生机和活力随外部干预状态的变化而变化。

安全系统是物质系统。安全系统既可能是自组织的，也可能是被组织的，也可能两者兼而有之。对安全来说，所谓外界的特定干预主要是指社会属性中的被动因素。它可能有两种

仅供试读，非教学使用

发展形式：一种是非组织的向组织的有序发展过程，其本质组织程度从相对较低向相对较高演化；另一种则是维持相同组织层次，但复杂程度必定相对增加。前一种过程反映了安全系统组织层次跃升过程；后一种过程则标志着安全系统组织结构与功能从简单到复杂的组织水平的提高。

安全系统的自组织的演化过程主要反映了它的自然属性与社会属性共同作用的过程和结果。因为安全系统也是开放系统，它可以不断与外界交换物质、能量和信息，从而出现上述的两种发展形式，即从原有的混沌无序状态转变为一种在时间、空间或功能上的有序状态。

一旦安全过程出现被组织的情况，如不可预见的天灾、地震、战争、纵火、瞎指挥、违规操作等，则会发生灾难或事故。

当然安全系统也是非线性系统，因而也具有非线性系统的共同特征。非线性是系统产生自组织行为的内因，没有这个内因，所谓开放性将不起作用，无序—有序的过程也就不会发生。

1.4.3　安全系统工程简介

1. 安全系统工程的定义

安全系统工程是指应用系统工程的基本原理和方法，辨识、分析、评价、排除和控制系统中的各种危险，对工艺过程、设备、生产周期和资金等因素进行分析评价和综合处理，使系统可能发生的事故得到控制，并使系统安全性达到最佳状态的一门综合性技术科学。

对这个定义，可以从以下几个方面理解：

（1）安全系统工程是系统工程在安全工程学中的应用，安全系统工程的理论基础是安全科学和系统科学。

（2）安全系统工程追求的是整个系统或系统运行全过程的安全。

（3）安全系统工程的核心是系统危险因素的识别、分析，系统风险评价和系统安全决策与事故控制。

（4）安全系统工程要达到的预期安全目标是将系统风险控制在人们能够容忍的限度以内，也就是在现有经济技术条件下，最经济、最有效地控制事故，使系统风险在安全指标以下。

由于安全系统工程从根本上和整体上来考虑安全问题，因而它是解决安全问题的具有战略性的措施，为安全工作者提供了一个既能对系统发生事故的可能性进行预测，又可对安全性进行定性、定量评价的方法，从而为有关决策人员提供决策依据，并据此采取相应安全措施。

2. 安全系统工程的任务

安全系统工程的主要任务有以下几点：

（1）危险源辨识。

（2）分析、预测危险源由触发因素作用而引发事故的类型及后果。

（3）设计和选用安全措施方案，进行安全决策。

（4）安全措施和对策的实施。

（5）对措施效果做出总体评价。

试读版本仅供防疫期间线上教学使用

（6）不断改进，以求最佳效果，使系统达到最佳安全状态。

3. 安全系统工程的步骤

安全系统工程的一般步骤为：

（1）收集资料，掌握情况。

（2）建立系统模型（结构、数学、逻辑模型）。

（3）危险源辨识与分析。

（4）危险性评价。

（5）控制方案与方案比较。

（6）最优化决策。

（7）决策计划的执行与检查。

1.4.4　安全系统工程的研究对象

安全系统工程作为一门科学技术，有它本身的研究对象。任何一个生产系统都包括三个部分，即从事生产活动的操作人员和管理人员；生产必需的机器设备、厂房等物质条件；以及生产活动所处的环境。这三个部分构成一个“人—机—环境”系统，每一部分就是该系统的一个子系统，称为人子系统、机器子系统和环境子系统。

（1）人子系统。该子系统的安全与否涉及人的生理和心理因素，以及规章制度、规程标准、管理手段、方法等是否适合人的特性，是否易于为人们所接受的问题。研究人子系统时，不仅要把人当作“生物人”“经济人”，更要看作“社会人”，必须从社会学、人类学、心理学、行为科学角度分析问题、解决问题；不仅把人子系统看作系统固定不变的组成部分，更要看作自尊自爱、有感情、有思想、有主观能动性的人。

（2）机器子系统。对于该子系统，不仅要从工件的形状、大小、材料、强度、工艺、设备的可靠性等方面考虑其安全性，而且要考虑仪表、操作部件对人提出的要求，以及从人体测量学、生理学、心理与生理过程有关参数对仪表和操作部件的设计提出要求。

（3）环境子系统。对于该子系统，主要应考虑环境的理化因素和社会因素。理化因素主要有噪声、振动、粉尘、有毒气体、射线、光、温度、湿度、压力、热、化学有害物质等；社会因素有管理制度、工时定额、班组结构、人际关系等。

三个子系统相互影响、相互作用的结果就使系统总体安全性处于某种状态。例如，理化因素影响机器的寿命、精度甚至损坏机器；机器产生的噪声、振动、温度又影响人和环境；人的心理状态、生理状况往往是引起误操作的主观因素；环境的社会因素又会影响人的心理状态，给安全带来潜在危险。这就是说，这三个相互联系、相互制约、相互影响的子系统构成了一个“人—机—环境”系统的有机整体。分析、评价、控制“人—机—环境”系统的安全性，只有从三个子系统内部及三个子系统之间的这些关系出发，才能真正解决系统的安全问题。安全系统工程的研究对象就是这种“人—机—环境”系统（以下简称“系统”）。

1.4.5　安全系统工程的内容

安全系统工程是专门研究如何用系统工程的原理和方法确保实现系统安全功能的科学技术。其主要研究内容有系统安全分析、系统安全评价、安全决策与控制。

试读版本仅供防疫期间线上教学使用

1. 系统安全分析

要提高系统的安全性，使其不发生或少发生事故，其前提条件是预先发现系统可能存在的危险因素，全面掌握其基本特点，明确其对系统安全性影响的程度。只有这样，才有可能抓住系统可能存在的主要危险，采取有效的安全防护措施，改善系统安全状况。这里所强调的“预先”是指：无论系统生命过程处于哪个阶段，都要在该阶段开始之前进行系统的安全分析，发现并掌握系统的危险因素。这就是系统安全分析要解决的问题。

系统安全分析有安全目标、可选用方案、系统模式、评价标准、方案选优五个基本要素和程序。

（1）把所研究的生产过程或作业形态作为一个整体，确定安全目标，系统地提出问题，确定明确的分析范围。

（2）将工艺过程或作业形态分成几个单元和环节，绘制流程图，选择评价系统功能的指标或顶端事件。

（3）确定终端事件，应用数学模式或图表形式及有关符号，以使系统数量化或定型化；将系统的结构和功能加以抽象化，将其因果关系、层次及逻辑结构变换为图像模型。

（4）分析系统的现状及其组成部分，测定与诊断可能发生的事故的危险性、灾害后果，分析并确定导致危险的各个事件的发生条件及其相互关系，建立数学模型或进行数学模拟。

（5）对已建立的系统，综合采用概率论、数理统计、网络技术、模糊技术、最优化技术等数学方法，对各种因素进行数量描述，分析它们之间的数量关系，观察各种因素的数量变化及规律。根据数学模型的分析结论及因果关系，确定可行的措施方案，建立消除危险、防止危险转化或条件耦合的控制系统。

系统安全分析是使用系统工程的原理和方法，辨别、分析系统存在的危险因素，并根据实际需要对其进行定性、定量描述的技术方法。

根据有关文献介绍，系统安全分析有多种形式和方法，使用中应注意：

1）根据系统的特点、分析的要求和目的，采取不同的分析方法。因为每种方法都有其自身的特点和局限性，并非处处通用。使用中有时要综合应用多种方法，以取长补短或相互比较，验证分析结果的正确性。

2）使用现有分析方法不能死搬硬套，必要时要根据实用、好用的需要对其进行改造或简化。

3）不能局限于分析方法的应用，而应从系统原理出发，开发新方法，开辟新途径，还要在以往行之有效的一般分析方法基础上总结提高，形成系统性的安全分析方法。

2. 系统安全评价

安全评价的目的是为决策提供依据。系统安全评价往往要以系统安全分析为基础，通过分析，了解和掌握系统存在的危险、有害因素，但不一定要对所有危险、有害因素采取措施；而是通过评价掌握系统的事故风险大小，以此与预定的系统安全指标相比较，如果超出指标，则应对系统的主要危险、有害因素采取控制措施，使其降至该标准以下。这就是系统安全评价的任务。

评价方法也有多种，评价方法的选择应考虑评价对象的特点、规模，评价的要求和目的，采用不同的方法。同时，在使用过程中也应和系统安全分析的使用要求一样，坚持实用和创新的原则。过去20年，我国在许多领域都进行了系统安全评价的实际应用和理论研究，

试读版本仅供预览用，非教学使用

开发了许多实用性很强的评价方法，特别是企业安全评价技术和各类危险源的评估、控制技术。

3. 安全决策与控制

任何一项系统安全分析技术或系统安全评价技术，如果没有一种强有力的管理手段和方法，也不会发挥其应有的作用。因此，在出现系统安全分析的同时，也出现了系统安全决策。其最大的特点是从系统的完整性、相关性、有序性出发，对系统实施全面、全过程的安全管理，实现对系统的安全目标控制。最典型的例子是美国标准《系统安全程序》，美国道（DOW）化学公司的安全评价程序，国际劳工组织、国际标准化组织倡导的《职业安全卫生管理体系》。系统安全管理是应用系统安全分析和系统安全评价技术，以及安全工程技术为手段，控制系统安全性，使系统达到预定安全目标的一整套管理方法、管理手段和管理模式。

安全措施是指根据安全评价的结果，针对存在的问题，对系统进行调整，对危险点或薄弱环节加以改进。安全措施主要有两个方面：一是预防事故发生的措施，即在事故发生之前采取适当的安全措施，排除危险因素，避免事故发生；二是控制事故损失扩大的措施，即在事故发生之后采取补救措施，避免事故继续扩大，使损失减到最小。

1.4.6　安全系统工程的特点

在工业领域内引进安全系统工程的方法是有很多优越性的。安全系统工程使安全管理工作从过去的凭直观经验进行主观判断的传统方法，转变为定性、定量分析。它具有以下五个特点：

（1）通过安全分析，了解系统的薄弱环节及其可能导致事故的条件，从而采取相应的措施，预防事故的发生；通过安全分析，还可以找到事故发生的真正的原因，查找到以前未想到的原因，定性地确定系统的危险程度，定量地分析可能发生事故的大小，采取相应的措施预防事故的发生。

（2）通过安全评价和优化技术的选择，可以找出适当的方法使各个子系统之间达到最佳配合状态，用最少的投资创造最佳的安全效果，大幅度地减少伤亡事故的发生。

（3）安全系统工程的方法不仅适用于工程技术，而且适用于安全管理。在实际工作中已经形成了安全系统工程与安全系统管理两个分支。它的应用范畴可以归纳为发现事故隐患、预测故障引起的危险、设计和调整安全措施方案、实现安全管理最优化、不断改善安全措施和管理方法五个方面。

（4）可以促进各项安全标准的制定和有关可靠性数据的收集。安全系统工程既然需要评价，就需要各种标准和数据。如允许安全值、故障率数据以及安全设计标准、人机工程标准等。

（5）可以迅速提高安全技术人员的管理水平。要搞好安全系统工程，必须熟悉生产的各个环节，掌握各种安全分析方法和评价方法，对提高安全管理工作人员的质量和水平有很大的推动。

1.4.7　安全系统工程的方法论

安全系统工程的方法是依据系统学和安全学理论，在总结过去经验型安全方法的基础上

试读结束，需要全本PDF请访问 www.ertongbook.com

日渐丰富和成熟的。概括起来可以归纳为如下五个方面。

1. 从系统整体出发的研究方法

安全系统工程的研究方法必须从系统的整体性观点出发，从系统的整体考虑解决安全问题的方法、过程和要达到的目标。例如，对每个子系统安全性的要求，要与实现整个系统的安全功能和其他功能的要求相符合。在系统研究过程中，子系统和系统之间的矛盾以及子系统与子系统之间的矛盾，都要采用系统优化方法寻求各方面均可接受的满意解；同时要把安全系统工程的优化思路贯穿到系统的规划、设计、研制和使用等各个阶段中。

2. 本质安全方法

这是安全技术追求的目标，也是安全系统工程方法中的核心。由于安全系统把安全问题中的人—机（物）—环境统一为一个“系统”来考虑，因此不管是从研究内容来考虑还是从系统目标来考虑，核心问题就是本质安全化，就是研究实现系统本质安全的方法和途径。

3. 人—机匹配法

在影响系统安全的各种因素中，至关重要的是人—机匹配。在产业部门研究与安全有关的人—机匹配称为安全人机工程，在人类生存领域研究与安全有关的人—机匹配称为生态环境和人文环境问题。显然，从安全的目标出发，考虑人—机匹配，以及采用人—机匹配的理论和方法是安全系统工程方法的重要支撑点。

4. 安全经济方法

由于安全的相对性原理，所以，安全的投入与安全（目标）在一定经济、技术水平条件下有着对应关系。也就是说，安全系统的“优化”同样受制于经济。但是，由于安全经济的特殊性（安全性投入与生产性投入的渗透性、安全投入的超前性与安全效益的滞后性、安全效益评价指标的多目标性、安全经济投入与效用的有效性等）就要求安全系统工程方法在考虑系统目标时，要有超前的意识和方法，要有指标（目标）的多元化的表示方法和测算方法。

5. 系统安全管理方法

安全系统工程从学科的角度讲是技术与管理相交叉的横断学科，从系统科学原理的角度讲，它是解决安全问题的一种科学方法。所以，安全系统工程是理论与实践紧密结合的专业技术基础，系统安全管理方法则贯穿到安全的规划、设计、检查与控制的全过程。所以，系统安全管理方法是安全系统工程方法的重要组成部分。

1.4.8　安全系统工程的应用

1. 安全系统工程在工业中的应用

安全管理工作和其他工作一样，具有其技术特点。安全系统工程的出现，为安全管理的深入研究和应用提供了坚实的理论基础，几十年的应用和发展又为其提供了可靠的实践经验。

从安全系统工程的发展可以看出，它最初是从研究产品的可靠性和安全性开始的。军事装备的零部件对可靠性和安全性的要求十分严格，否则不仅不能够完成武器的设计，而且制造和使用过程中的各个环节也不安全。后来这种方法发展到对生产系统的各个环节进行安全分析。环节的内容除了包括原料、设备等因素外，还包括了人和环境的因素，这就使安全系统工程的方法在工业安全（即传统的安全工作）领域中得到实际的应用。这个研究开发的

试读版本仅供预览期间线上教学使用

过程大致经历了以下五个阶段：

（1）工业安全和系统安全。工业安全负责工人的人身安全，系统安全负责产品的安全。两者是一种分工合作的关系，保证了生产任务的完成。

（2）工业安全引进系统安全分析方法的阶段。科学技术的发展及重大社会灾害性事故的频繁发生，使得工业安全工作者试图寻求新的解决办法。系统安全分析的方法引起了他们的重视，被引进到工业安全分析中，并在工业安全领域起到了极大的作用。

（3）安全管理对系统工程的引进阶段。工业安全工作者在对人的因素的管理方面引进了系统安全的分析原理和方法，开始综合分析人、机器、原材料、环境等因素，使安全管理工作有了定性、定量分析的可能，并对安全管理工作及其危险性进行安全评价，提高了安全管理工作的系统性、准确性、可靠性和安全性。

（4）安全系统工程的发展阶段。安全系统工程的实践和应用始于美、英等工业发达国家。20 世纪 80 年代，各国广泛地研究和应用，说明这种管理方法已成为完善安全管理工作的发展方向。

（5）安全系统工程向其他领域的渗透。几十年来我国出现了许多研究和应用安全系统工程的科研院校和企业，并取得了很大的成绩。安全系统工程的基本原理和方法已在安全管理、质量管理、环保管理、医疗事故管理等方面得到了应用。

2. 安全系统工程的应用特点

安全系统工程是一门应用性很强的科学技术。几十年来，许多经典的应用范例始终激励人们进行不懈的探索，不断充实和发展其自身的理论体系，以期获得更好的应用效果，这是安全系统工程始终保持快速发展的重要原因。为了进一步促进学科发展，提高其实用性，有必要进一步明确安全系统工程的应用特点，具体如下：

（1）系统性。不论是系统安全分析、系统安全评价的理论，还是系统安全管理模式和方法的应用，都表现了系统性的特点，它从系统的整体出发，综合考虑系统的相关性、环境适应性等特性，始终追求系统总体目标的满意解或可接受解。

（2）预测性。安全系统工程的分析技术与评价技术的应用，无论是定性的，还是定量的，都必须是为了预测系统存在的危险因素和风险水平。它通过这些预测来掌握系统安全状况如何，风险能否接受，以便决定是否应当采取措施控制系统风险。所以，安全系统工程也可称为系统的事故预测技术。

（3）层序性。安全系统工程的应用是按照系统的时空两个跨度有序展开的，管理规范的执行，一般按照系统生命过程有序进行，而且贯彻到系统的方方面面。因此，安全系统工程具有明显的“动态过程”研究特点。

（4）择优性。择优性的应用特点主要体现在系统风险控制方案的综合与比较，从各种备选方案中选取最优方案。在选取控制风险的安全措施方面，一般按下列优先顺序选取方案：设计上消除→设计上降低→提供安全装置→提供报警装置→提出专门规程。因此，冗余设计，安全联锁，有一定可靠的保证的安全系数，是安全系统工程经常采用的设计思想。

（5）技术与管理的融合性。安全系统工程是自然（技术）科学与管理科学的交叉学科，随着科技与经济的发展，人们对安全追求的目标（特别是生产领域）是本质安全。但是，一方面由于新技术的不断涌现，另一方面由于经济条件的制约，对于一时做不到本质安全的技术系统，则必须用安全管理来补偿。所以在相当长的时间内，解决安全问题还必须把技术

此为试读，需要完整PDF请访问：www.ertongbook.com

与管理通过系统工程的方法有机地结合起来。

这些安全系统的应用特点应在该学科的理论研究和实际应用中得到充分重视，使安全系统工程发展更快些，应用效果更明显些。

3. 安全系统工程的优点

从上述介绍可看出，安全系统工程在解决安全问题上与传统的方法不同，它改变了以往凭直接经验和事后处理的被动局面，因而形成了它本身的一些优点。

（1）预测和预防事故的发生，是现代安全管理的中心任务。运用系统安全分析方法，识别系统中存在的薄弱环节和可能导致事故发生的条件；通过定量分析，预测事故发生的可能性和事故后果的严重度，从而可以采取有效措施控制事故的发生，大大减少伤亡事故。这是安全系统工程最大的优点。

（2）现代工业的特点是规模化、连续化和自动化，其生产关系日趋复杂，各个环节和工序之间相互联系、相互制约。安全系统工程通过系统分析，全面地、系统地、彼此联系地以及预防性地处理生产系统中的安全性，而不是孤立地、就事论事地解决生产系统中的安全问题。

（3）安全系统工程方法，不仅适用于工程，而且适用于管理。实际上已形成安全系统工程和安全系统管理两个分支，其应用范畴可以归纳为五个方面：①发现事故隐患；②预测由故障引起的危险；③设计和调整安全措施方案；④实现最优化的安全措施；⑤不断地采取改善措施。

（4）对安全进行定量分析、评价和优化技术，为安全事故预测提供了科学依据，根据分析可以选择出最佳方案，使各子系统之间达到最佳配合，用最少投资得到最佳的安全效果，从而可以大幅度地减少人身伤亡和设备损坏事故。

（5）促进各项标准的制定和有关可靠性参数的收集。安全系统工程既然包括安全性评价，就需要有各种标准和数据，如许可安全值、故障率、人—机工程标准以及安全设计标准等。

（6）通过安全系统工程的开发和应用，可以迅速提高安全技术人员、操作人员和管理人员的业务水平和系统分析能力，同时为培养新人提供了一套完整的参考资料。

1.4.9　安全系统工程的分析方法

随着安全系统工程学科的发展，出现了许多分析方法，见诸有关文献的分析方法就有数十种，常见的有二十多种。尤其是研究和应用安全系统工程队伍的扩大，使得安全系统工程的分析方法更加多样化。虽然目前还没有形成完整而系统的方法，但是，事故树分析方法以及安全检查表已经得到了广泛应用，并且在工厂的安全管理、安全咨询中介机构的安全评价中发挥了重要的作用。

这些方法都有各自的特点，均在实际生产应用中起到了很大的作用。很难说哪种方法更好，它们之间只能相互补充，而不能相互比较。用一种分析方法也许不能查明系统中所有的危险性因素，达不到分析的目的；而另一种方法却能够给以补充，并揭示它们。安全系统工程分析方法的这种互补性，使得安全系统工程的应用越来越广泛，并大大促进了安全系统工程学科的不断发展。

作为安全系统工程的工作者，或者说安全系统工程分析方法的应用者，应该熟练掌握，

试读版本仅供预览期间线上教学使用

并能够灵活运用几种分析方法。但这并不是说要全部使用这些方法，也不是多使用一种方法就会使分析结果更精确、更有效。

在实际应用中，要具体问题具体分析，对于特定的环境和资源条件，应根据系统的特点，选用不同的分析方法，以提高分析的准确性，有效地消除或控制系统的危险性。

对所有的分析方法进行归类是比较困难的，这些分析方法之间既有联系，又有区别。它们或者分析方法比较相近，或者具有共同的分析特点；有些分析方法既可以划为这一类，又可以划为另一类。按照不同的分类方法，大体上可以划分为以下几类：

（1）按照由初级到高级分为：安全检查表、单点故障分析、意外事故分析、子系统危险性分析、预先危险性分析、故障类型影响分析、致命度分析、事故树分析、事件树分析等方法。

（2）按照逻辑关系分为：归纳分析法、演绎分析法、综合分析法。

1）归纳分析法包括安全检查表、临界异常技术、意外事故分析、子系统危险性分析、故障类型影响分析、作业安全分析、管理监督和风险树分析等。

2）演绎分析法包括潜在回路分析、事故树分析、预先危险性分析等。

3）综合分析法包括故障类型影响分析、子系统危险性分析、网络逻辑分析等。

（3）按数理方法分为：定性分析法、定量分析法。

1）定性分析法包括安全检查表、作业安全分析、操作和后勤危险性分析、流动分析、能量分析、临界异常技术、最大可能的事故分析和最坏条件分析等。

2）定量分析法包括单点故障分析、事故树分析、事件树分析等。

上述分析方法有些既可做定性分析，也可做定量分析。

在实际运用安全系统工程的分析方法时，以上分析方法往往综合采用，并要求分析人员必须熟悉生产系统的各个环节，掌握整个系统各个子系统之间的联系和因果关系，做到对不安全因素了如指掌。系统分析的过程仅仅是系统评价的前提，是系统决策的依据。

1.4.10　安全分析应该遵循的基本原则

安全分析应该遵循以下基本原则：

（1）首先可进行初步的综合性分析，如预先危险性分析、安全检查表等，得出大致的概况，然后根据危险性的大小再进行详细的分析。

（2）根据分析对象的不同，选择相应的分析方法。如分析对象是连续的工艺操作，就要选择单元间有联系的分析方法，如流动分析、交接面分析等；如果分析对象是一个关键的危险性设备，则可选择从零部件开始的故障分析，如故障类型和影响分析等。

（3）如果对新建、改建的设计或限定目标进行分析，可选用静态的分析方法（包括初步分析和详细分析）；如果对运行状态进行分析，则可选用动态的分析方法，如程序分析和逻辑分析等。

（4）如果需要对系统进行反复调整，使之达到较高的安全性水平，可以使用替换分析和逻辑分析等。

（5）各种分析方法可以互为补充，使用一种方法也许不能完全分析出系统的危险性，但用其他方法可以弥补其不足的部分。

（6）进行分析时并不需要使用所有的方法，应该根据实际情况，结合特定的环境和资

试读结束，仅供预览，需要全文请购买

金条件，使分析能够得出正确的评价。

1.5 安全系统工程发展概况

事故给人类带来无数灾难，严重地制约了经济发展和社会进步，甚至对人类生存构成巨大威胁。然而，事故的影响也并非都是消极的，它和其他事物一样，也有积极的一方面。首先，事故具有鲜明的反面教育的作用，它向人们展示了其危害程度，警示人们必须按照科学规律办事。其次，事故是一种特殊的科学试验。一个系统发生事故，说明该系统存在这样那样的不安全、不可靠的问题，从而以事故的形式弥补了设计时应做而没做，或想做而没敢做（没钱做）的试验。人们通过对事故的调查、分析，找出事故原因，研究并采取了有效控制事故的措施，改变了系统工艺、设备，从而提高了系统的性能，发展了专业技术。最后，事故也是诞生新的科学技术的催化剂。事故的强大负面效应对人类产生巨大的冲击作用，从而激发人类以更大的决心和更大的力量研究事故。通过对事故信息和资料的收集、整理、分析、研究，也就是充分开发利用“事故资源”，一个崭新的自然科学学科就在人们这种不懈努力与艰苦卓绝的斗争中诞生了，这就是作用力与反作用力的作用机制。在科学技术发展的历史长河中，几乎每一个学科的诞生都离不开事故这种反作用力的作用。安全系统工程也正是在这种事故的反作用下应运而生的。

1.5.1 国外安全系统工程的发展

安全风险评价起源于20世纪30年代，是随着保险业的发展需要而发展起来的。保险公司为客户承担各种风险，必然要收取一定的费用，而收取的费用多少是由所承担的风险大小决定的。因此，就产生了一个衡量风险程度的问题。这个衡量风险程度的过程就是当时的美国保险协会所从事的风险评价。

安全评价技术在20世纪60年代得到了很大的发展，首先使用于美国军事工业。1962年4月美国公布了第一个有关系统安全的说明书“空军弹道导弹系统安全工程”，此后，系统安全工程方法陆续推广到航空、航天、核工业、石油、化工等领域，并不断发展、完善，成为现代系统安全工程的一种新的理论、方法体系，在当今安全科学中占有非常重要的地位。

安全系统工程产生于20世纪60年代初期美英等工业发达国家。1957年，苏联发射了第一颗人造地球卫星，美国为了夺回空间优势，匆忙进行导弹技术开发，实行研究、设计、施工齐头并进的方法。但由于对系统的可靠性和安全性研究不足，在导弹系统研发过程中仅仅一年半的时间就连续发生四起重大事故，造成惨重损失，从而迫使美国空军以系统工程的基本原理和管理方法来研究导弹系统的安全性、可靠性。1962年美国军方首次公开发表了《空军弹道导弹安全系统工程大纲》，以此作为对民兵式导弹计划有关的承包商提出的系统安全的要求，这是系统安全理论的首次实际应用。1969年美国国防部批准颁布了最具有代表性的系统安全军事标准《系统安全大纲要点》（MIL—STD—822），对完成系统在安全方面的目标、计划和手段，包括设计、措施和评价，提出了具体要求和程序。此项标准于1977年修订为《系统安全程序技术要求》（MIL—STD—822A），1984年又修订为MIL—STD—822B。该标准对系统整个寿命周期中的安全要求、安全工作项目都做了具体规定。

中国煤炭工业出版社教学资源使用

MIL—STD—822B 系统安全标准从一开始实施，就在世界安全和防火领域产生了巨大影响，迅速为日本、英国和欧洲其他国家引进使用。这就是由事故引发的军事系统的安全系统工程。

1961 年美国贝尔电话研究所在系统安全的基础上创造了事故树分析法（FTA）。英国在 20 世纪 60 年代中期成功开发了概率风险评价（PRA）技术，用于计算核电站系统风险大小以及风险是否可以接受。1974 年美国原子能委员会发表了拉斯姆逊教授的“商用核电站风险评价报告”（WASH—1400），从而成功地开发应用了系统安全分析和系统安全评价技术。该报告的科学性和对事故预测的准确性得到了“三哩岛事件”（核电站堆芯熔化造成放射性物质泄漏事故）的证实。这些可称为核工业的安全系统工程。

1964 年美国道（DOW）化学公司根据化工生产的特点，首先开发出“火灾爆炸指数评价法”，用于对化工装置进行安全评价。该法曾多次修订，1994 年已发展到第 7 版。它以单元重要危险物质在标准状态下的火灾、爆炸或释放出危险性潜在能量大小为基础，同时考虑工艺过程的危险性，计算单元火灾爆炸指数（F&EI），确定危险等级，并提出安全对策措施，使危险降低到人们可以接受的程度。目前，安全评价人员使用是道化学（7 版）评价法，该法是在多年使用的基础上逐步修改了一些条款，以便与法规和损失预防原则相一致，同时依据美国消防协会（NFPA）的最新数据给出了物质系数。通过修订，评价程序将更加简明，评价结果直观明了，提出的措施更具有实用价值。由于该评价方法日趋科学、合理、切合实际，在世界工业界得到一定程度的应用，引起各国的广泛研究、探讨，推动了评价方法的发展。1974 年英国帝国化学公司（ICI）蒙德（Mond）部在道化学公司评价方法的基础上引进了毒性概念，并发展了某些补偿系数，提出了“蒙德火灾爆炸毒性指标评价法”。1976 年日本劳动省颁布了“化工厂安全评价六阶段法”，该法采用了一整套系统安全工程的综合分析和评价方法，使化工厂的安全性在规划、设计阶段就能得到充分的保证，并陆续开发了匹田法等评价方法。这些可称为化学工业的安全系统工程。

20 世纪 60 年代正是美国市场竞争日趋激烈的年代，许多民用产品在没有得到保障的情况下就投放市场，造成许多使用过程中的事故，用户纷纷要求厂方赔偿损失，甚至要求追究厂商刑事责任，迫使厂方在开发新产品的同时，寻求提高产品安全性的新方法、新途径。例如，1965 年美国波音公司和华盛顿大学在西雅图召开了安全系统工程的专门学术研讨会，以波音公司为中心对航空工业开展安全性、可靠性分析，取得了很好的效果。这期间，在电子、航空、铁路、汽车、冶金等行业开发了许多系统安全分析方法和评价方法。这些可称为民品工业的安全系统工程。

20 世纪 80 年代以来，安全系统工程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。1983 年在美国休斯敦召开的第六届国际安全系统工程学术大会，有四十多个国家的代表参加，议题涉及国民经济的各行各业。

由于恶性事故常造成严重的人员伤亡和巨大的财产损失，促使各国政府、议会立法或颁布法令，规定工程项目、技术开发项目都必须进行安全评价，并对安全设计提出明确的要求。日本《劳动安全卫生法》规定，由劳动基准监督署对建设项目实行事先审查和许可证制度；美国对重要工程项目的竣工、投产都要求进行安全评价；英国政府规定，凡未进行安全评价的新建生产经营单位不准开工；欧共体 1982 年颁布《关于工业活动中重大危险源的

指令（Seveso Ⅰ)》，1996 年，欧盟颁布《重大事故风险防范指令（Seveso Ⅱ)》欧盟成员国陆续制定了相应的法律；国际劳工组织（ILO）也先后公布了 1988 年的《重大事故控制指南》、1990 年的《重大工业事故预防实用规程》和 1992 年的《工作中安全使用化学品实用规程》，对安全评价提出了要求。2002 年欧盟在未来化学品白皮书中，明确危险化学品的登记注册及风险评价，作为政府的强制性的指令。2012 年欧盟又颁布《重大事件与危险物质风险防控（Seveso Ⅲ)》，明确了危害设施与居民区、公共活动区和特殊敏感或重要区域之间的安全距离，各成员国也相继制定了相应法律法规，确保土地使用安全评估与公共安全的适应性。

1.5.2　我国安全系统工程的发展

在我国，安全系统工程的研究、开发是从 20 世纪 70 年代末开始的。天津东方化工厂应用安全系统工程成功地解决了高度危险企业的安全生产问题，为我国各个领域学习、应用安全系统工程起了带头作用。1982 年北京市劳动保护研究所召开了安全系统工程座谈会，会上交流了国内开展研究和应用的情况，并探讨了在我国开展安全系统工程的方向，研究如何组织分工合作、如何进行学术交流等，这次会议为我国开展安全系统工程的研究与应用打下了良好的基础。1985 年，中国“劳动保护管理科学专业委员会”成立，建立了“系统安全学组”，该学组以安全系统工程为中心，进行开发研究和推广应用等活动，为安全系统工程学科的发展和推进安全管理做出了贡献。其后在机械、冶金、航空、交通运输、水电、汽车、核电等行业和部门借鉴引用国外的系统安全分析方法，对现有系统进行分析评价，取得了较好的效果。

20 世纪 80 年代初期，安全系统工程引入我国，通过吸收、消化国外安全检查表和安全分析方法，机械、冶金、化工、航空、航天等行业的有关生产经营单位开始应用安全分析评价方法，如安全检查表（SCL)、事故树分析（FTA)、故障类型及影响分析（FMFA)、事件树分析（ETA)、预先危险性分析（PHA)、危险与可操作性研究（HAZOP)、作业条件危险性评价（LEC）等。石油、化工等易燃、易爆危险性较大的生产经营单位，还应用美国道化学公司火灾、爆炸危险指数评价方法进行了安全评价。1986 年劳动人事部分别向有关科研单位下达了机械工厂危险程度分级、化工厂危险程度分级、冶金工厂危险程度分级等科研项目。1987 年机械电子部首先提出了在机械行业内开展机械工厂安全评价，1988 年 1 月 1 日颁布了第一个部颁安全评价标准《机械工厂安全性评价标准》。此外，我国有关部门还颁布了《石化生产经营单位安全性综合评价办法》《电子生产经营单位安全性评价标准》《航空航天工业工厂安全评价规程》《兵器工业机械工厂安全性评价方法和标准》《医药工业生产经营单位安全性评价通则》等。

1991 年国家“八五”科技攻关课题中，将安全评价方法研究列为重点攻关项目。由劳动部劳动保护科学研究所等单位完成的“易燃、易爆、有毒重大危险源识别、评价技术研究”，获得了易燃、易爆、有毒重大危险源识别、评价方法的研究成果，填补了我国跨行业重大危险源评价方法的空白，在事故严重度评价中建立了伤害模型库，采用了定量的计算方法，使我国工业安全评价方法的研究初步从定性评价进入定量评价阶段。

1996 年 10 月劳动部颁发了第 3 号令，规定六类建设项目必须进行劳动安全卫生预评价，与之配套的规章、标准还有劳动部第 10 号令、第 11 号令和部颁标准《建设项目（工

程）劳动安全卫生预评价导则》（LD/T 106—1998）。2002 年 6 月 29 日颁布了《中华人民共和国安全生产法》（以下简称《安全生产法》，已于 2014 年修订），规定生产经营单位的建设项目必须实施“三同时”，同时还规定矿山建设项目和用于生产、储存危险物品的建设项目应进行安全条件论证和安全评价。2002 年 1 月 9 日国务院颁布了《危险化学品管理条例》，在规定了对危险化学品各环节管理和监督办法等的同时，提出了“生产、储存、使用剧毒化学品的单位，应当对本单位的生产、储存装置每年进行一次安全评价；生产、储存、使用其他危险化学品的单位，应当对本单位的生产、储存装置每两年进行一次安全评价”的要求。《安全生产法》和《危险化学品管理条例》的颁布，进一步推动了安全评价工作的开展。2007 年国家安全生产监督管理总局发布了《安全评价通则》（AQ8001—2007）、《安全验收评价导则》（AQ8003—2007）、《安全预评价导则》（AQ8002—2007），规范了安全评价工作，提高了企业安全管理水平。近年来，我国安全生产领域的标准化的实施更使安全工作向更广、更深的方向发展。

各行业积极推广应用安全系统工程学的原理和方法，取得了可喜的成果。2011 年 3 月 8 日国务院学位委员会、教育部发布了《学位授予和人才培养学科目录（2011 年）》，将“安全科学与工程”列为研究生教育的一级学科，进一步推进了安全学科与工程专业发展。2012 年教育部颁布《普通高等学校本科专业目录（2012 年）》，将安全科学与工程本科专业升级为一级学科。这些都为普及和推广安全系统工程知识、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发展的安全系统工程理论和方法打下良好人才基础。

综合上述，以系统的观点、方法，对安全系统的理论与方法的产生和发展归纳如下：

（1）安全系统工程是在事故逼迫下产生的。人类在从事社会经济活动中，由于经常发生事故给人们的生命、财产带来了严重的威胁，人们不得不在现有安全工程技术基础上，寻找能够预测、预防、预控事故的科学技术，安全系统工程就是在这样的背景下诞生的。人们开始采用系统安全预先分析、系统安全评价技术，对系统全过程进行安全控制，开展科学的安全管理工程。

（2）现代科学技术的发展为安全系统工程的产生提供了必要条件，20 世纪 40 年代产生了系统可靠性工程，20 世纪 50 年代出现了系统工程，以及这一期间现代数学和计算机技术的迅速发展，使安全系统工程在 20 世纪 60 年代成为科学技术发展的必然产物，也是相关学科相互影响的必然结果。

（3）军事、核工业、化工等行业系统安全分析与评价方法的研究与开发，丰富了安全系统工程的研究内容。20 世纪 60 年代初美国在导弹技术的开发中，深入地研究了系统的安全性和控制系统安全性的手段与方法，从而出现了空军标准“系统安全程序”和“系统安全程序要求”。同一时期，出现了核电站的概率风险评价技术，化工企业的火灾爆炸指数安全评价法以及涉及产品安全的系统安全分析技术，如事故树、事件树、故障类型和影响分析等。这些理论和方法大大丰富了安全系统工程的内容，从而形成一个完整的学科——安全系统工程。

（4）安全系统工程在理论研究和实践中不断完善和发展。安全系统工程以系统工程和安全科学为其理论基础，以人—机—环境为其研究对象，其研究内容不仅包括辨识、分析、评价与控制技术，还包括管理程序、管理方法等管理科学的内容。基于这种思想，迄今国外发表的有关系统安全分析、系统安全评价、系统安全管理技术与方法的论著，都属于安全系

统工程的范畴；各行业预先分析与控制事故、提高系统安全性、倡导安全技术等的实践和研究，也都具有鲜明的系统工程特点。因此，安全系统工程在理论研究和生产实践过程中不断完善和发展。

复　习　题

1. 关于安全的定义很多，请思考什么是安全？
2. 系统、安全系统、安全系统工程的定义是什么？请辨析三者间的区别和联系。
3. 安全系统工程是以安全科学和系统科学为基础理论的综合性学科，请问你认为安全系统工程应遵循的基本观点有哪些？
4. 安全系统工程的基本方法是什么？
5. 请简述安全系统工程的主要研究内容。

试读版本仅供防疫期间线上教学使用

第2章

系统安全定性分析

本章学习目标：

了解系统安全分析方法的分类，掌握安全检查表、预先危险分析、故障类型及影响分析、危险与可操作性研究等典型的定性系统安全分析方法，理解各方法的原理和适用范围，并具有运用以上方法开展系统安全分析的实践能力。

本章学习方法：

在分析、理解各类方法原理的基础上，可将每一类方法的特点、基本步骤、基本分析要素进行归纳和总结，明确各类方法的适用范围，并注重理论联系实际。

试读版仅供防疫期间线上教学使用

系统安全分析是安全系统工程的核心内容，也是安全评价的基础。通过这个过程，人们可以对系统进行深入、细致的分析，充分了解系统存在的危险性，估计事故发生的概率和可能产生伤害及损失的严重程度，为确定出哪种危险能够通过修改系统设计或改变控制系统运行程序来进行预防提供依据。所以，分析结果的正确与否，关系整个工作的成败。

系统安全分析方法有数十种，对所有的分析方法进行归类是比较困难的，这些分析方法之间既有联系，又有区别。它们或者分析方法比较相近，或具有共同分析特点；有些分析方法既可以划为这一类，又可以划为另一类。从定性和定量分析角度可以将其分为定性分析方法和定量分析方法。定性分析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。定性分析主要包括安全检查表、预先危险性分析、危险性可操作性研究分析、鱼刺图分析、作业危害分析等。定量分析方法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，对事故的危险性做出数量化的描述。定量分析主要包括事件树分析、事故树分析、系统可靠性分析等。在上述分析方法中，事件树分析和事故树分析既可用于定性分析，也可用于定量分析。

本章从定性角度出发，对系统安全定性分析方法进行阐述。

2.1 安全检查表

安全检查表（Safety Check List，简记为 SCL）是进行安全检查，发现潜在危险，督促各

项安全法规、制度、标准实施的一个较为有效的工具。它是安全系统工程中最基本、最初步的一种形式。

2.1.1　安全检查表的介绍

1. 检查表的定义

安全检查表是20世纪30年代工业迅速发展时期的产物。当时，由于安全系统工程尚未出现，安全工作者为了解决生产中遇到的日益增多的事故，运用系统工程的手段编制了一种检验系统安全与否的表格。系统工程广泛应用以后，安全系统工程开始萌芽，安全检查表的编制逐步走向理论阶段，使得安全检查表的编制越来越科学、全面和完善。它们的内容基本相同，不同的是编制的依据和方法不同，前者运用系统工程手段，后者源于安全系统工程的科学分析。

因此，安全检查表的定义为：运用安全系统工程的方法，发现系统以及设备、机器装置和操作管理、工艺、组织措施中的各种不安全因素，列成表格进行分析。

2. 安全检查表的特点

安全检查表对有计划地解决安全问题是很有效的。其主要特点如下：

（1）安全检查表能够事先编制，可以做到系统化、科学化，不漏掉任何可能导致事故的因素，为事故树的绘制和分析做好准备。

（2）可以根据现有的规章制度、法律、法规和标准规范等检查执行情况，容易得出正确的评估。

（3）通过事故树分析和编制安全检查表，将实践经验上升到理论，从感性认识到理性认识，并用理论去指导实践，充分认识各种影响事故发生的因素的危险程度（或重要程度）。

（4）安全检查表按照原因事件的重要顺序排列，有问有答，通俗易懂，能使人们清楚地知道哪些原因事件最重要，哪些次要，促进职工采取正确的方法进行操作，起到安全教育的作用。

（5）安全检查表可以与安全生产责任制相结合，按不同的检查对象使用不同的安全检查表，易于分清责任，还可以提出改进措施，并进行检验。

（6）安全检查表是定性分析的结果，是建立在原有的安全检查基础和安全系统工程之上的，简单易学，容易掌握，符合我国现阶段的实际情况，为安全预测和决策提供坚实的基础。

（7）只能作定性的评价。

（8）只能对已经存在的对象评价。

3. 安全检查表的适用范围

安全检查表适用于对系统生命周期的各个阶段进行安全分析，适用范围涉及生产、工艺、规程、管理等多方面，对检查内容的列举过程即为危险辨识的过程。

该方法适用范围较广，分析精度相对较低，且检查表的质量受编制人员的知识水平和经验影响，生产中安全检查表需要在实践中不断修改完善。

2.1.2　安全检查表的编制

1. 编制安全检查表的主要依据

安全检查表应列举需查明的所有能导致工伤或事故的不安全状态和行为。为了使检查表在

试读结束，需要全本PDF请访问www.ertongbook.com

内容上能结合实际、突出重点、简明易行、符合安全要求，应依据以下四个方面进行编制。

（1）有关标准、规程、规范及规定。为了保证安全生产，国家及有关部门发布了各类安全标准及有关的文件，这些是编制安全检查表的一个主要依据。为了便于工作，有时将检查条款的出处加以注明，以便能尽快统一不同意见。

（2）事故案例和行业经验。收集国内外同行业及同类产品行业的事故案例，从中发掘出不安全因素，作为安全检查的内容。国内外及本单位在安全管理及生产中的有关经验，自然也是一项重要内容。

（3）通过系统分析，确定的危险部位及防范措施，都是安全检查表的内容。

（4）研究成果。在现代信息社会和知识经济时代，知识的更新很快，编制安全检查表必须采用最新的知识和研究成果，包括新的方法、技术、法规和标准。

2. 安全检查表的格式

安全检查表的格式，没有统一的规定，可以根据不同的要求，设计不同需要的安全检查表。原则上应条目清晰、内容全面，要求详细、具体。总体上讲，目前应用较多的有两种形式，即提问式和对照式安全检查表。

（1）提问式。提问式检查表的检查项目内容采用提问方式进行，其一般格式见表 2-1。

表 2-1 ×××安全检查表（提问式）

序号	检查项目	检查内容要点	是“√” 否“×”	备注
1				
2				
……	……	……		
检查人		时间	直接负责人	

这种格式适用于企业非安全专业的生产人员实施自行检查，只需要按检查表内容和生产实际情况符合性填“√”或“×”，确定当日或较短时期内安全情况。

（2）对照式。对照式检查表的检查项目内容后面附上合格标准，检查时对比合格标准作答。对照式检查表的一般格式见表 2-2。

表 2-2 ×××安全检查表（对照式）

序号	检查项目	国家技术标准规定项	检查结果	备注
1				
2				
……	……	……		
检查结论				

这种格式适用于企业安全管理或安全监管机构的专业人员，按照行业安全技术标准，对

试读版本仅供防疫期间线上教学使用

照企业生产条件和设备、工艺配置情况设计对应的检查表，填写表格检查结果时需要使用安全术语或相应的数据对比等来明确实际生产状况和安全技术标准或法规间的差距，从而起到准确判断和辅助决策的作用。

此外，在安全标准化实施过程中，也有在安全检查表中增加分值评判等表格项的新格式。总之，安全检查表是应用最广泛、使用最便捷、效果较显著的一种系统性安全分析评价方法，其形式也比较多样。

3. 编制安全检查表的程序

编制安全检查表和对待其他事物一样，都有一个处理问题的程序。图 2-1 是编制安全检查表的程序框图。

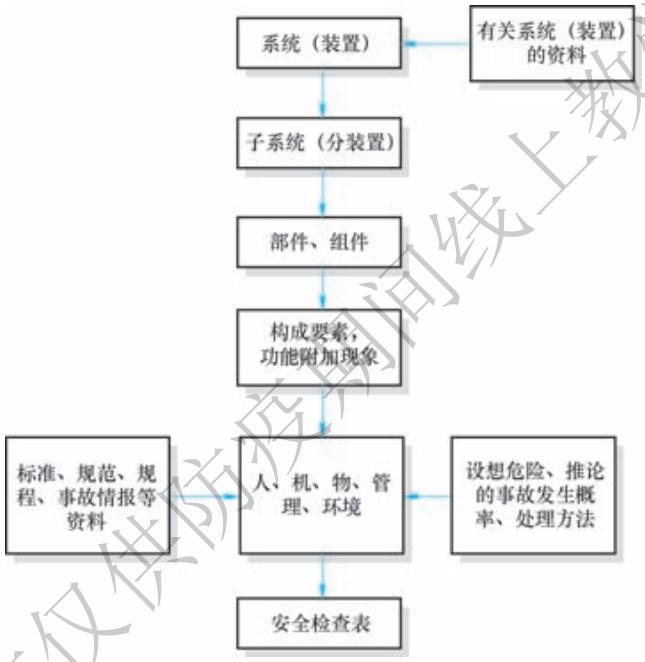

图 2-1　编制安全检查表的程序框图

（1）系统的功能分解。一般工程系统（装置）都比较复杂，难以直接编制出总的检查表。我们可按系统工程观点将系统进行功能分解，建立功能结构图。这样既可显示各构成要素、部件、组件、子系统与总系统之间的关系，又可通过各构成要素的不安全状态的有机组合求得总系统的检查表。

（2）人、机、物、管理和环境因素。如以生产车间为研究对象，生产车间是一个生产系统，车间中的人、机、物、管理和环境是生产系统中的子系统。从安全观点出发，不只是考虑“人—机系统”，应该是“人—机—物—管理—环境系统”。

（3）潜在危险因素的探求。一个复杂的或新的系统，人们一时难以认识其潜在危险因素和不安全状态，对于这类系统可采用类似“黑箱法”原理来探求，即首先设想系统可能存在哪些危险及其潜在部分，并推论其事故发生过程和概率，然后逐步将危险因素具体化，最后寻求处理危险的方法。通过分析不仅可以发现其潜在危险因素，而且可以掌握事故发生的机理和规律。

试读版本仅供防疫期间线上教学使用

4. 编制安全检查表应注意的问题

（1）编制安全检查表的过程，实质是理论知识、实践经验系统化的过程，一个高水平的安全检查表需要专业技术的全面性、多学科的综合性和对实际经验的统一性。为此，应组织技术人员、管理人员、操作人员和安全技术人员深入现场共同编制。

（2）按照查找隐患要求列出的检查项目应齐全、具体、明确，突出重点，抓住要害。为了避免重复，尽可能将同类性质的问题列在一起，系统地列出问题或状态。另外应规定检查方法，并有合格标准。防止检查表笼统化、行政化。

（3）各类检查表都有其适用对象，各有侧重，是不宜通用的。如专业检查表与日常检查表要加以区分，专业检查表应详细，而日常检查表则应简明扼要，突出重点。

（4）危险性部位应详细检查，确保一切隐患在可能发生事故之前就被发现。

（5）编制安全检查表应将安全系统工程中的事故树分析、事件树分析、预先危险性分析和可操作性研究等方法结合进行，把一些基本事件列入检查项目中。

2.1.3 安全检查表的内容要求

安全检查表应该能够列举所有需查明的能导致工伤事故或其他事故的不安全状态和行为。这就需要有正确而全面的事故树分析结果。同时，对事故树无法绘出的因素，也要通过传统的安全检查表和其他形式的安全检查表，进行综合分析，罗列清单，分清轻重缓急，编制正确而全面的安全检查表。这也正是安全检查表的强大生命力之所在。

一般来说，安全检查表有以下一些内容。在实际应用过程中，要综合采用传统的安全检查表和采用事故树分析法编制的安全检查表。下面是一些有关的检查内容，仅供参考。

1. 防止人受到伤害的安全检查的内容

（1）厂址选择。厂区附近火灾、噪声、爆炸、大气污染和水质污染危险；铁路、公路交叉口和急转弯的防护措施；各种标志。

（2）建筑物。楼梯、地坪、装卸地点按标准进行设计；出入口和紧急撤离口合理，安全通道有防护措施；照明装置适当；门和窗户不影响出入；钢结构的棱角应磨圆。

（3）操作地点。蒸气、水、空气等的工艺管线、电源软管和电线不妨碍职工操作和通路；有害气体、蒸气、粉尘等的通风换气良好；新鲜空气的进口远离排气口；原材料与产品的放置地点应合理；有火灾爆炸等潜在危险的车间或厂房应为独立建筑物；厂房应有安全通道；主要设备应有防爆装置；应有必要的装置检修的地坪面积和空间；要有利于进行清扫和维修；加热表面的防护；操作地点的位置和空间；动力装置的防护；人工操作的阀门和开关以及控制设备有安全的操作地点；有毒有害液体的排放要符合防止污染的标准，不会对职工、附近居民和财物造成危险；起重机械的行程限位器和其他安全装置；电梯的自动联锁和其他安全装置；尽量以机械作业代替人工作业；配备必要的紧急淋浴和冲眼设备；可燃（易燃）的危险化学品的储存场所与生产设备和建筑物的安全距离；消除噪声的设施和措施；停车时要能顺利切断电源。

（4）厂区。厂内道路应适于运输急救物品的车辆行驶；卷扬机的钢丝绳和制动安全可靠；可燃物品的装卸地点应有接地装置、安全的装卸位置、空间操作地点、场所的安全空间和安全标志；厂区照明要足够。

试读版本仅供防疫期间线上教学使用

2. 防止装置和设备发生事故的安全检查内容

（1）原料。明确工厂有哪些原料是危险和有毒的，其危险性的敏感度和毒性如何，发生异常反应的后果如何；工艺过程的危险性如何，应有各种控制措施和设施；操作过程中的注意事项及紧急救援事项；储存设备或设施的防护措施；对原料进行妥善管理的措施；生产过程中原料的短缺会发生什么严重后果；工厂的消防设施，发生火灾时的紧急措施。

（2）反应。对潜在性的危险反应，采取适当的隔离措施；工艺参数是否接近危险的界限值；会产生的危险反应、不良的介质流动和环境污染的防护措施；明确正常状态与异常状态的反应速度及其发生的后果；正常生产过程中的换热措施；了解工艺过程的化学反应；装置发生异常或剧烈反应及制止剧烈反应的措施；装置发生故障时，应有紧急停车措施和防止造成事故的防护装置。

（3）装置。与大气相通的系统是否有潜在的危险及其位置是否合理，不应影响生产装置；化工生产的水封；设备外发生事故，对设备内的影响；主要设备的安全阀、防爆板及其位置；储存区的安全管理措施；易燃易爆场所的灭火装置和灭火器材的位置；液面计、液位计的防护措施；紧急开关和阀门在事故状态下应易于接近；锅炉、压力容器的登记、检验和检测，并建立档案；检修时，应有必要的检修手续，对现场危险性有正确的判断及检修的质量；易燃易爆场所的防静电措施；易燃易爆场所的屏蔽或隔离措施；压力表、安全阀的定期检验。

（4）仪表。仪表的动力电源发生故障会有什么危险；对仪表进行维修和检修时，会对生产产生什么影响，有什么保证安全的措施；有关安全的仪表反应速度；对重要的仪表和装置，有无备用品；设计时应把工艺的安全作为生产过程的一个环节考虑；异常天气的温度、湿度对仪表的影响；表盘刻度是否容易读取；仪表的防护罩；仪表的定期检验和检测。

（5）操作。操作规程的检查和研究；职工对操作法的熟悉程度，特别是开车、停车、紧急停车和处理的熟悉程度和训练；工艺流程和工艺指标的经常性检查；开车前的装置处理和全面检查；针对不同事故的具体操作程序；产品的灌装和堆放的安全措施和防护装置；日常维修和检修作业的危险性；环境保护的“三废”排放要求；惰性气体的供应及其危险性；变更设计、改建、扩建、扩大生产、提高质量等，对安全生产的影响。

（6）公用工程。公用工程（指水、电、汽、燃气）发生问题时的安全保证及应急措施；通风、采暖、自控等能满足生产工艺技术的要求；考虑故障情况下的最坏的后果；燃气泄漏的可能性及其危险性，检测报警和安全防护装置的可靠性。

（7）平面布置。各种装置的间距，是否便于维护检修；个体的泄漏对整体的影响及防护措施；在管理上采取的措施。

另外，对于专业的安全检查表，如电器安全检查表、锅炉和压力容器安全检查表，它们都具有各自具体详细的内容，这里不再介绍。

安全检查的内容还包括：查领导，即查各级领导在工作中是否把安全工作放在应有的地位，在决策中是否考虑安全生产的要求，是否能够保证安全生产必要的投入；查思想，即检查各级生产管理人员对安全生产的认识，对安全生产的方针政策、法律、法规和各项规章制度的贯彻执行情况；查管理，即查安全管理的各项具体工作的执行情况，如安全生产责任制和其他安全管理规章制度是否健全，安全技术措施、安全教育、事故管理等的实施情况；查隐患，即检查劳动条件、生产设备、安全卫生设施是否符合安全卫生条件的要求，职工在生产中的不安全行为的情况等；查整改，即查曾经检查出的隐患是否进行了相应的整改或采取

了相应的措施。

2.1.4 实用举例

【例 2-1】 矿山企业综合检查表，见表 2-3。

表 2-3 矿山企业安全现状综合检查表

序号	检查内容	依据		结果	备注
1	矿山、建筑施工单位和危险物品的生产、经营、储存单位，应当设置安全生产管理机构或者配备专职安全生产管理人员	《安全生产法》	第 19 条		
2	危险物品的生产、经营、储存单位以及矿山、建筑施工单位的主要负责人和安全生产管理人员，应当由有关主管部门对其安全生产知识和管理能力考核合格后方可任职		第 20 条		
3	生产经营单位应当对从业人员进行安全生产教育和培训，保证从业人员具备必要的安全生产知识，熟悉有关的安全生产规章制度和安全操作规程，掌握本岗位的安全操作技能。未经安全生产教育和培训合格的从业人员，不得上岗作业		第 21 条		
4	生产经营单位进行爆炸、吊装等危险作业，应当安排专门人员进行现场安全管理，确保操作规程的遵守和安全措施的落实		第 35 条		
5	生产经营单位必须为从业人员提供符合国家标准或者行业标准的劳动防护用品，并监督、教育从业人员按照使用规则佩戴、使用		第 37 条		
6	矿山必须有与外界相通的、符合安全要求的运输和通信设施	《矿山安全法》	第 11 条		
7	矿山企业必须对下列危害安全的事故隐患采取预防措施： ① 冒顶、片帮、边坡滑落和地表塌陷 ② 爆炸器材和爆炸作业发生的危害		第 18 条		
8	矿山企业必须建立、健全安全生产责任制		第 20 条		
9	矿山企业必须对职工进行安全教育、培训；未经安全教育、培训的，不得上岗作业；矿山企业安全生产的特种作业人员必须接受专门培训，经考核合格取得操作资格证书的，方可上岗作业		第 26 条		
10	矿长必须经过考核，具备安全专业知识，具有领导安全生产和处理矿山事故的能力；矿山企业安全工作人员必须具备必要的安全专业知识和矿山安全工作经验		第 27 条		
11	矿山企业必须向职工发放保障安全生产所需的劳动防护用品		第 28 条		
12	矿山企业必须制定矿山事故防范措施，并组织落实		第 30 条		
13	矿山企业应当建立由专职或者兼职人员组成的救护和医疗急救组织，配备必要的装备、器材和药物		第 31 条		

试读版本仅供防疫期间线上教学使用

（续）

序号	检查内容	依据		结果	备注
14	矿山企业必须按照国家有关规定对职工经常进行安全教育，搞好技术培训	《矿山安全条例》	第7条		
15	所有爆炸材料库不得超量储存，不得发放、使用变质失效或外部破损的爆炸材料		第45条		
16	矿山企业必须建立爆炸材料领退制度		第46条		
17	进行爆炸作业，必须明确规定警戒区范围和岗哨位置以及其他安全事项。爆炸后留下的盲炮（瞎炮），应当由现场作业指挥人和爆炸工组织处理。未处理妥善前，不许进行其他作业		第47条		
18	新工人入矿前，必须经过健康检查，不适于从事矿山作业的，不得录用		第57条		
19	矿山企业应当建立、健全下列安全生产责任制： ① 行政领导岗位安全生产责任制 ② 职能机构安全生产责任制 ③ 岗位人员的安全生产责任制	《矿山安全法实施条例》	第28条		
20	爆炸工、信号工、电工、金属焊接（切割）工和矿内机动车驾驶员等特种作业人员应当接受专门技术培训，经考核合格取得操作资格证书后，方可上岗作业		第37条		
21	具备采矿许可证、爆炸物品使用证、营业执照	《安全生产规定》	第4条		
22	凡从事爆炸作业的人员，必须由矿场主管部门审查和专业训练，经所在地的县（市）公安局考核合格，获得爆炸员作业证，方准作业		第10条		
23	爆炸作业必须严格执行国家标准《爆炸安全规程》的规定： ① 严格爆炸器材的管理，爆炸器材必须储存在专用的仓库或储存室内。使用爆炸器材必须建立严格的领取、清退制度。当班剩余的爆炸器材必须及时清点退回库房保管。严禁乱放、乱扔、私存和转让他人 ② 工作面遇有瞎炮时，必须及时处理。处理瞎炮时，禁止掏出或拉出起爆药包。严禁打残眼		第11条		
24	爆炸作业必须实行定时爆炸制度，在规定的时间进行。禁止在雷雨天、夜间和雾天进行爆炸作业		第12条		
25	对矿场产尘作业点必须采取有效的防尘措施，坚持湿式作业。粉尘浓度要达到国家工业卫生标准的要求。爆炸后和装卸矿岩时，应进行喷雾洒水。确无水源时，应采取干式捕尘措施 接触粉尘作业人员应戴防尘口罩		第13条		

试读版本仅供防疫期间线上教学使用

（续）

序号	检查内容	依据		结果	备注
26	爆炸器材必须储存在专用的仓库、储存室内，并设专人管理，不准任意存放	《民用爆炸物品管理条例》	第13条		
27	储存爆炸器材的仓库、储存室，必须做到： ① 建立出入库检查、登记制度 ② 库房内储存的爆炸器材数量不得超过设计容量。性质相抵触的爆炸器材必须分库储存。库房内严禁存放其他物品 ③ 严禁无关人员进入库区		第16条		
28	需用爆炸器材时，应当报经上级主管部门审查同意，向所在地县、市公安局申请领取爆炸物品购买证，凭证向指定的供应点购买		第19条		
29	购买爆炸器材，需要运输的，应当在申请领取“爆炸物品购买证”的同时，申请领取“爆炸物品运输证”		第22条		
30	建立、健全主要负责人、分管负责人、安全生产管理人员、职能部门、岗位安全生产责任制；制定安全检查制度、职业危害预防制度、安全教育培训制度、生产安全事故管理制度、重大危险源监控和重大隐患整改制度、设备安全管理制度、安全生产档案管理制度、安全生产奖惩制度等规章制度；制定作业安全规程和各工种操作规程	《非煤矿矿山企业安全生产许可证实施办法》	第5条		
31	安全投入符合安全生产要求，按照有关规定提取安全技术措施专项经费		第5条		
32	设置安全生产管理机构，配备专职安全生产管理人员		第5条		
33	主要负责人和安全生产管理人员的安全生产知识和管理能力经考核合格		第5条		
34	依法参加工伤保险，为从业人员缴纳工伤保险费		第5条		
35	制定边坡坍塌等各种事故以及采矿诱发地质灾害等事故的应急救援预案		第5条		
36	建立事故应急救援组织，配备必要的应急救援器材、设备；生产规模较小可以不建立事故应急救援组织的，应当指定兼职的应急救援人员，并与邻近的事故应急救援组织签订救护协议		第5条		
37	有具有资质的设计单位设计的开采设计和附图。附图包括地质地形图、采场工程平面布置图和采场剖面图		第9条		
38	爆炸器材管理、爆炸安全距离和爆炸作业符合《爆炸安全规程》规定		第9条		

试读版本仅供防疫期间线上教学使用

【例2-2】　举例说明工程施工安全管理检查评分表，具体内容及样式见表2-4。

表2-4　安全管理检查评分表

序号		检查项目	扣分标准	应得分数	扣减分数	实得分数
1	保证项目	安全生产责任制	未建立安全责任制，扣10分 各级各部门未执行责任制，扣4～6分 经济承包中无安全生产指标，扣10分 未制定各工种安全技术操作规程，扣10分 未按规定配备专职安全员，扣10分 管理人员责任制考核不合格，扣5分 无安全日志，每少一天，扣2分	12		
2		施工组织设计	施工组织设计中无安全措施，扣10分 施工组织设计未经审批，扣10分 专业性较强的项目，未单独编制专项安全施工方案，每缺一项，扣8分 未按规范对专项施工方案进行专家论证审批，扣5分 安全措施不全面，扣2～4分 安全措施无针对性，扣6～8分 安全措施未落实，扣8分	12		
3		分部（分项）工程安全技术交底	无书面安全技术交底，扣10分 交底针对性不强，扣4～6分 交底不全面，扣4分 交底未履行签字手续，扣2～4分	12		
4		安全检查	无定期安全检查制度，扣5分 安全检查无记录，扣5分 检查出事故隐患，整改做不到定人、定时间、定措施，扣6分 对事故隐患整改通知书所列项目未如期完成，扣5分	12		
5		安全教育	无安全教育制度，扣10分 新入厂工人未进行三级安全教育，扣10分 无具体安全教育内容，扣6～8分 变换工种时未进行安全教育，扣10分 每有一人不懂本工种安全技术操作规程，扣2分 每有一人未通过入场安全教育和考核上班，扣3分 施工管理人员未按规定进行年度培训，扣5分 专职安全员未按规定进行年度培训考核或考核不合格，扣5分	12		
		小计		60		

试读版本仅供防疫期间线上教学使用

（续）

序号		检查项目	扣分标准	应得分数	扣减分数	实得分数
6	一般项目	班前安全活动	未建立班前安全活动制度，扣10分 班前安全活动无记录，缺一次，扣2分 班前教育活动无针对性，扣5分	10		
7		特种作业持证上岗	无特殊作业人员管理制度，扣5分 每有一人未经培训从事特种作业，扣4分 每有一人未持操作证上岗，扣2分	10		
8		工伤事故	工伤事故未按规定报告，扣6分 工伤事故未按事故调查分析规定处理，扣10分 未建立工伤事故档案，扣4分	10		
9		安全标志	无现场安全标志布置总平面图，扣5分 现场未按安全标志总平面图设置安全标志，扣5分	10		
		小计		40		
项目合计				100		

检查部位：

检查人：

注：1. 每项最多扣减分数不大于该项应得分数。

2. 保证项目有一项不得分或保证项目小计得分不足40分的，检查评分表记零分。

【例2-3】 高处作业现场安全检查表，见表2-5。

表2-5 高处作业安全检查表

检查单位： 检查时间： 年 月 日

检查项目	序号	检查内容	检查结果	备注
施工人员	1	无高血压、心脏病、精神病等不适于高处作业的病症		
	2	正确穿戴安全帽、软底鞋等防护用品		
	3	井、孔口、临空面边缘不准休息和停留		
	4	不准向下抛丢物体、材料		
	5	不准沿绳、立杆攀爬		
	6	作业前检查安全绳的牢固程度，不准使用不合格的安全绳		
架子平台	7	按设计施工、牢固可靠		
	8	定期检查排架损伤、腐朽、松动情况，及时维护		
	9	井、孔口、预留口加盖板或设围栏		
	10	平台脚手板铺满钉牢、临空面有护身栏杆，不准有探头板		
	11	栈道栈桥通道有扶手栏杆，扶梯固定牢固，通道外侧下部为道路或作业场所时边缘有10cm以上的挡板		
	12	堆物整齐、稳固，不准超负荷		
	13	废物废渣及时清理，不得乱丢乱堆		

试读版本仅供防疫期间线上教学使用

（续）

检查项目	序号	检查内容	检查结果	备注
临空边缘悬空作业	14	悬挂合格的安全网或搭设其他防护设施		
	15	正确拴挂安全网		
	16	使用工具和易下落的物体，有绳子拴牢，不能下掉		
	17	下方为通道或其他工作场所，应有防护棚或专人监护		
其他	18	六级以上大风、暴雨、浓雾等恶劣天气，停止作业		
	19	雪天、冰冻天气应清除雪、霜、冰和采取防滑措施		
	20	夜间有足够的照明		
	21	石棉瓦等简易轻型屋顶作业有相应的安全防护措施		
	22	带电体附近作业应保持规定的安全距离或采取防护隔离措施		
	23	登高作业，电杆立杆等埋设固定牢靠，登高工具合格		

2.2 预先危险性分析

2.2.1 基本含义

预先危险性分析（Preliminary Hazard Analysis，简记为PHA），又称为预先危险分析，是一种定性分析系统内危险因素和危险程度的方法。

预先危险性分析是在每项工程活动之前，如设计、施工、生产之前，或技术改造后，即制定操作规程和使用新工艺等情况之后，对系统存在的危险性类型、来源、出现条件、导致事故的后果以及有关措施等，做概略分析。其目的是辨识系统中存在的潜在危险，确定其危险等级，防止这些危险发展成事故。预先危险性分析也是对固有系统中采取新的操作方法、接触新的危险性物质、工具和设备时进行的分析。这种方法是一种简单易行、经济、有效的定性分析方法。预先危险性分析的目的是防止操作人员直接接触对人体有害的原材料、半成品、成品和生产废弃物，防止使用危险性工艺、装置、工具和采用不安全的技术路线；如果必须使用时，也应从工艺上或设备上采取安全措施，以保证这些危险因素不致发展成为事故。

2.2.2 分析内容与其优点

系统安全分析的目的不是分析系统本身，而是预防、控制或减少危险性，提高系统的安全性和可靠性。因此必须从确保安全的观点出发，寻找危险源（点）产生的原因和条件，评价事故后果的严重程度，分析措施的可能性、有效性，采取切合实际的对策，把危害与事故发生率降低到最低程度。

1. 预先危险性分析的内容

根据安全系统工程的方法，生产系统的安全必须从人—机—环境系统进行分析，而且在进行预先危险性分析时应持这种观点：即对偶然事件、不可避免事件、不可知事件等进行剖

试读版不允许在试读期间线上教学使用

析，尽可能地把它变为必然事件、可避免事件、可知事件，并通过分析、评价控制事故发生。

分析的内容可归纳几个方面：

（1）识别危险的设备、零部件，并分析危险发生的可能性条件。

（2）分析系统中各子系统、各元件的交接面及其相互关系与影响。

（3）分析原材料、产品、特别是有害物质的性能及储运。

（4）分析工艺过程及其工艺参数或状态参数。

（5）人、机关系（操作、维修等）。

（6）环境条件。

（7）用于保证安全的设备、防护装置等。

2. 预先危险性分析的主要优点

（1）分析工作做在行动之前，可及早采取措施排除、降低或控制危害，避免由于考虑不周造成损失。

（2）对系统开发、初步设计、制造、安装、检修等进行分析的结果，可以提供应遵循的注意事项和指导方针。

（3）分析结果可为制定标准、规范和技术文献提供必要的资料。

（4）根据分析结果可编制安全检查表以保证实施安全，并可作为安全教育的材料。

3. 预先危险性分析的适用范围

预先危险性分析适用于固有系统中采取新的方法，接触新的物料、设备和设施的系统安全分析。预先危险性分析既可用于对整个系统的分析，又可用于对某个子系统、某项设备或某项操作的分析，该分析法一般在项目的发展初期使用。当只希望进行粗略的危险和潜在事故情况分析时，也可用 PHA 对已建成的装置进行分析。

预先危险性分析是一种常用的定性分析方法，大多数情况下能辨别出系统中存在的主要危险，但随着系统设计的深入，还会有新的危险出现，故 PHA 常与其他方法结合使用。

2.2.3 分析步骤及应注意的问题

1. 分析的一般步骤

分析的一般程序，如图 2-2 所示。

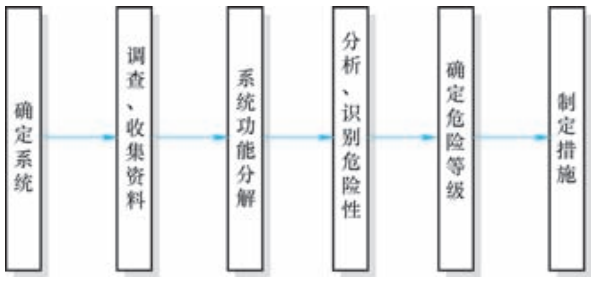

图 2-2 预先危险性分析的程序

（1）确定系统。明确所分析系统的功能及分析范围。

（2）调查、收集资料。调查生产目的、工艺过程、操作条件和周围环境。收集设计说

试读版本仅供预览期间线上教学使用

明书、本单位的生产经验、国内外事故情报及有关标准、规范、规程等资料。

（3）系统功能分解。一个系统是由若干个功能不同的子系统组成的，如动力、设备、结构、燃料供应、控制仪表、信息网络等。其中还有各种连接结构，同样，子系统也是由功能不同的部件、元件组成的，如动力、传动、操纵和执行等。为了便于分析，按系统工程的原理，将系统进行功能分解，并绘出功能框图，表示它们之间的输入、输出关系，功能框图示例如图2-3所示。

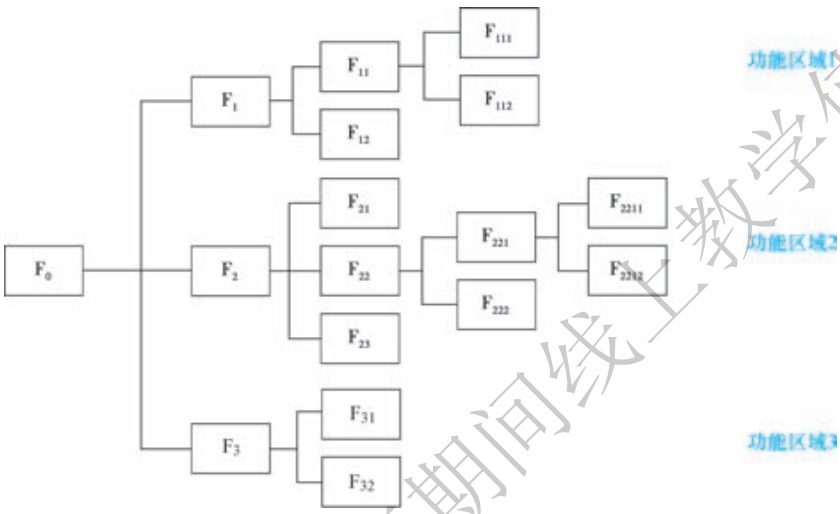

图2-3　功能分解图示例

（4）分析、识别危险性。确定危险类型、危险来源、初始伤害及其造成的危险性，对潜在的危险点要仔细判定。

（5）确定危险等级。在确认每项危险之后，都要按其效果进行分类。

（6）制定措施。根据危险等级，从软件（系统分析、人机工程、管理、规章制度等）、硬件（设备、工具、操作方法等）两方面制定相应的消除危险性的措施和防止伤害的办法。

2. 预先危险性分析应注意的问题

（1）由于在新开发的生产系统或新的操作方法中，对接触到的危险物质、工具和设备的危险性还没有足够的认识，因此为了使分析获得较好的效果，应采取设计人员、操作人员和安技干部三结合的形式进行。

（2）根据系统工程的观点，在查找危险性时，应将系统进行分解，按系统、子系统、系统元件一步一步地进行。这样做不仅可以避免过早地陷入细节问题而忽视重点问题的危险，而且可以防止漏项。

（3）为了使分析人员有条不紊地、合理地从错综复杂的结构关系中查出深潜的危险因素，可采取以下对策。

1）第一，迭代。对一些深潜的危险，一时不能直接查出危险因素时，可先做一些假设，然后将得出的结果作为改进后的假设，再进一步查危险因素。这样经过一步一步地试析，向更准确的危险因素逼近。

2）第二，抽象。在分析过程中，对某些危险因素常忽略其次要方面，首先将注意力集

试读版本仅供防疫期间线上教学使用

中于危险性大的主要问题上。这样可使分析工作能较快地入门，先保证在主要危险因素上取得结果。

另外也可以运用控制论的观点来探求，如图 2-4 所示。输入是一定的，技术系统（具体结构）也是一定的，问题是探求输出哪些危险因素。

（4）在可能条件下，最好事先准备一个检查表，指出查找危险性的范围。

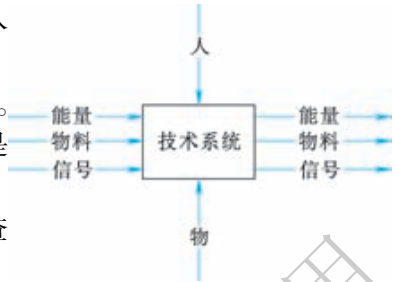

图 2-4　分析系统

2.2.4　危险性辨识

生产现场包含着来自人、机（物）和环境三方面的多种隐患，为确保安全生产，就必须分析和查找隐患，并及早消除，将事故消灭在发生之前，做到预防为主。因此，识别危险性是首要问题。

造成事故必须有两个因素，一是有引起伤害的能量，二是有遭受伤害的对象（人或物），两者缺一不可。而且这两个因素必须相距很近，伤害能量能够作用到对象，才能造成事故。如人的不安全行为和机械或物质危险是人—机“两方共系”中能量逆流的两个系列，其轨迹交叉点就会造成事故。

潜在的危险性只有在一定条件下才能发展成为事故。为了迅速地找出危险源（点），除需具有丰富的理论基础和实践知识外，还可以从能量的转换等几方面入手。

生活和生产都离不开能源，在正常情况下，能量通过做有用功制造产品和提供服务，其能量平衡式为：

$$\text{输入能} = \text{有用功（做功能）} + \text{正常耗损能}$$

但在非正常运行状态下，其能量平衡式为：

$$\text{输入能} = \text{有用功} + \text{正常耗损能} + \text{逸散能}$$

这个逸散能作用在人体上就是伤害事故，作用在设备上则损坏设备。因此，从预防事故来看，关键是查找出生产现场能量体系中潜在的危险因素。

能够转化为破坏能力的能量有：电能、原子能、机械能、势能和动能、压力和拉力、燃烧和爆炸、腐蚀、放射线、热能和热辐射、声能、化学能等。

另一种表示破坏能量的因素及事件也可作为参考：加速度、污染、化学反应、腐蚀、电（电击、电感、电热、电源故障等）、爆炸、火灾、热和温度（高温、低温、温度变化）、泄漏、湿度（高湿、低湿）、氧化、压力（高压、低压、压力变化）、辐射（热辐射、电磁辐射、紫外线辐射、电离辐射）、化学灼伤、结构损害或故障、机械冲击、振动与噪声等。

为便于分析，应了解能量转换过程，为此有必要进一步叙述能量失控情况。一般说来，能量失控情况可分为两种模式：物理模式和化学模式。各类生产企业中，机械设备很多，因此从事故数量上来看，物理模式的能量失控引起的事故占大多数。

1. 物理模式

物理能可分为势能和动能两种形式。以势能的形式出现的，如处于高处的物体（如落体、坠落、倒塌、崩垮、塌方、冒顶等）、受压的弹性元件、储存的热量、电压等。以动能的形式出现的有运动的机械、行驶的车辆、电流、流动的液体等。势能是静止的、潜在的，人们对其危险性的认识往往不敏感。然而由于某种原因，势能转换为动能时，危险性就可能

试读版本仅供防疫期间线上教学使用

急剧增大。动能凭人的视觉能感觉到它的存在，危险性可以一目了然，但是静止的人会被运动物体所撞伤，人与物体相互运动也可能受伤，行动的人碰到静止物体也会受伤，这些危险都是无法预料的。另外，还要注意有些物体同时具有两种能量，如电动机既有电能，又有机械回转能。

（1）物理爆炸。物理爆炸是纯粹物理现象产生的冲击波，它常常是因压力容器的破坏而产生，受压气体突然释放，能够产生很大的破坏力，如空压机储气罐、液化气储气罐、各种气瓶等。

（2）锅炉爆炸。锅炉是工业生产中用得较多的设备，又是比较容易发生灾害性事故的设备。锅炉爆炸比单纯的受压气体爆炸的破坏性更大，因为在相同压力下，蒸汽比同等体积的气体的能量大很多倍。另外，锅炉的过热水由于锅炉破坏而闪蒸成蒸汽，使蒸汽中所含的热量进一步增多。引起锅炉爆炸的主要事件是锅炉体结垢、炉壁腐蚀、缺水和超压运行。所有的蒸汽发生器、冷却水夹套、烧沸水的设备、家用水暖设备等，都有可能发生锅炉型爆炸。

（3）机械失控。机械把一种形式的能量转换为另一种形式的能量，如把水的势能转换为电能，或把机械能转换成压缩、成形、挤压、破碎、切削等有用功。正在运转的机器有很大的动能，它们不断地有次序地进行能量转换工作或做有用功。由于机械设计不良、强度计算有误或超负荷运转，都可能造成机械失控，对机器本身或其附近目标做破坏功。例如，离心机由于超速运行而发生爆炸。

（4）电气失控。电动机和发电机是转换能量的装置，输电线和变压器、配电设备等则是传输电能的装置，而且前者同时具有电能和机械能。将电能转换为机械能的设备系统或元件若不完善或超负荷运行就可能发生电气失控，电能有逆流到人体的潜在危险，同时也会造成火灾或其他损失。

（5）其他物理能量失控。一些物理因素如热辐射、核污染、噪声和次声、电场和磁场、微波、激光、红外和紫外辐射等，如果失控，都会引起人员伤亡和财产损失。

2. 化学模式

化学模式危险性所产生的破坏力和物理模式不同，它是通过物质化合和分解等化学反应产生的能量失控而造成火灾或爆炸。其过程是静态化学能通过化学反应转变为物理能，由物理能对目标施加破坏力。化学爆炸的起因是由于化学反应失控，瞬时产生大量高温气体，该气体受到约束时可具有极大的压力，高压气体产生冲击波，对周围目标造成破坏。化学模式通常有三种情况。

（1）直接火灾。当可燃性物质和氧气共存时，遇到火源就有可能发生火灾。但是，应该注意某些非可燃性物质也有发生直接火灾的可能性，如各类粉尘，包括有机塑料粉尘，染料粉尘，某些金属如镁、铝等粉尘，煤及谷物粉尘等，它们能和空气充分结合，有些还有吸附空气的能力。这些粉尘在加工、运输、储存过程中，容易造成粉尘爆炸，产生严重后果。

在石油和易燃液体加工过程中，一般都注意到尽可能减少与空气接触。但是在储存过程中，如石油储罐都装有呼吸阀，当环境温度高时（中午）排出多余的油气，若油气受到空间的约束，达到爆炸极限时，遇火就会发生爆炸；当环境温度低时（晚上或雨后），则会吸入周围空气，如遇到静电火花也会发生爆炸。

（2）间接火灾。间接火灾是指受外力破坏引起本身发生火灾的情况，如设备或容器遭

试读结束，仅供防疫期间线上教学使用

受外来事故的波及、易燃物质外泄、遇火源发生爆炸等。因此，在设计布局时要注意设备之间、装置之间、工厂之间的距离，避免间接火灾发生。

（3）自动反应。有些化学反应物体本身带有含氧分子团，不需外部供氧就能发生氧化反应。如炸药、过氧化物等，性质极不稳定，遇到冲击振动或其他刺激因素就能发生火灾爆炸。另外，有些化合物本身聚合（不饱和烃类）和分解（乙炔），受到温度、压力或储存时间的影响会自动发生反应，造成火灾爆炸。

3. 有害因素

很多化学物质如氰化物、氯气、光气、氨、一氧化碳等，都会对人体造成急性或慢性的毒害。因此，国家为了保护职工身体健康，规定了这些有害物质在操作环境中的最高允许浓度，超过了规定的允许值则被认为存在着危险性。

要注意惰性气体等对人的危害性，如氮气会使人窒息致死。

生物性有害因素会使人致病，如致病微生物（细菌、病毒、真菌、原生物、螺旋体等）。

4. 外力因素

外力是指受到外界爆炸而产生的冲击波、爆炸碎片的袭击等和地震、洪水、雷击、飓风等自然现象，对生产设备或房屋外施加很大的能量而造成的损坏和人身伤亡。

5. 人的因素

在人—机系统中，人子系统比机械子系统可靠性低很多。因为人具有自由性，再加上构成劳动集体的每个成员的精神素质和心理特征不同，易受环境条件所造成的心理上的影响，从而造成误操作。为了防止事故的发生就必须对人加强教育训练，提高其可靠性、适应能力和应变能力，同时加强人机工程学的研究，使机器能适应人的操作，减少误差。

6. 环境因素

在生产现场，除机器设备能构成不安全状态和人的不安全行为能造成事故外，生产所用的原材料、半成品、成品、工具以及工业废弃物等，若放置不当也会形成不安全状态，因为这些物体具有潜在的势能。还有粉尘、毒气、恶臭、照明、温度、湿度、噪声、振动、高频、微波、放射性等危害。环境危害不只限于在操作点上发生，而是发生在一定的范围内，影响面大。

2.2.5　危险性等级划分与确定

1. 危险性等级的划分

在危险性查出之后，应对其划分等级，排列出危险因素的先后次序和重点，以便分别处理。由于危险因素发展成为事故的起因和条件不同，因此在预先危险性分析中仅能作为定性评价，其等级见表2-6。

表2-6　危险性等级分布表

级　别	危险程度	可能导致的后果
1级	安全的	不会导致伤害或疾病，系统无损失，可以忽略
2级	临界的	处于事故的边缘状态，暂时还不会造成人员伤亡和系统的损坏，但应予排除或控制
3级	危险的	会造成人员伤亡和系统损坏，要立即采取措施控制
4级	破坏性的	破坏性的，会造成死亡或系统报废，必须设法消除

试读版本仅供防疫期间线上教学使用

2. 危险性等级的确定方法

当系统中存在很多危险因素时，如何分清其严重程度，因人而异，带有很大的主观性。为了较好地符合客观性，可集体讨论或多方征求意见，也可采取一些定性的决策方法。下面介绍一种矩阵比较法，其基本思路是：如有很多大小差不多的圆球放在一起，很难一下分出哪个最大，哪个次之。若将它们一对一比较，则较易判明。

其具体方法是列出矩阵表。设某系统共有6个危险因素需要进行等级判别，可分别用字母A、B、C、D、E、F代表，画出一个如图2-5a所示的方阵。

按方阵图中顺序，比较每一列因素的严重性，用“×”号表示在列里严重、在行里不严重的因素。例如比较因素A和B，A比B严重，则在第一列第二行空格内画“×”号。再比较因素A和C，A比C不严重，在第一列第三行空格内不画“×”号。照此方法，依次一一对应比较后，可得出每一列画“×”号的总和。图2-5a中结果是因素E画“×”号的总和为5，因素A、B、C画“×”号的总和均为3，因素F总和为1，因素D则为零。这样就可得出各危险因素的严重性次序为：E、A、B、C、F、D。其中因素A、B、C具有同等的严重性。

	A	B	C	D	E	F
A			×		×	
B	×				×	
C		×			×	
D	×	×	×		×	×
E						
F	×	×	×		×	
Σ	3	3	3	0	5	1

a)

	A	B	C	D	E	F
A			×		×	
B	×		1		×	
C		1			×	
D	×	×	×		×	×
E						
F	×	×	×		×	
Σ	3	2.5	3.5	0	5	1

b)

图2-5　危险因素严重程度比较矩阵表

在这种情况下，可以承认A、B、C三因素具有同等严重性。为了分得细一些，也可在方阵图中增加一个“1”符号，以它代表严重性的1/2，如图2-5b所示，在两者有关的行和列各画一个“1”符号。这样处理后，对A、B、C三个因素进行比较，可看出，因素C画“×”号和“1”符号为3.5，因素A为3，因素B为2.5。这样，6个因素的严重性的顺序是：E、C、A、B、F、D。需要指出的是，当因素较多时，这样一一对比会引起混乱，陷入自相矛盾的境地，为此要求在比较时应十分冷静、细致。

2.2.6　危险性控制

危险性识别和等级划分后，就可采取相应的预防措施，避免它发展成为事故。采取预防措施的原则首先是采取直接措施，即从危险源（或起因）着手。其次，则是间接措施，如隔离、个人防护等。其主要方法如下所述。

（1）限制能量或采用安全能源代替危险能源，如限速装置、低电压设备、安全设备、限制生产能量等。

（2）防止能量外泄，如自动温度调节器、熔丝、气体检测器、地面装卸作业、锐利工

试读版本仅供阅读期间线上浏览使用

具等。

（3）防止能量散逸，如放射性物质的铅储器、绝缘材料、安全带等。

（4）在能量的放出路线上和放出的时间上采取措施，如排尘装置、安全禁止标志、防护性接地、安全连锁装置等。

（5）能量放出缓冲装置，如爆炸板、安全阀、保险带、冲击吸收装置等。

（6）在能量源上采取防护措施，如防护罩、喷水灭火装置、禁入栅栏、防火墙等。

（7）在能量和人与物之间设立防护措施，如玻璃视镜、过滤器、防噪声装置等。

（8）对人体采取防护措施，如防尘眼镜、安全靴、头盔、手套、呼吸器、防护用具等。

（9）提高耐受能力，选用适应性强的人和耐久性材料。

（10）降低损害程度的措施，如紧急冲浴设备、配置低放射线、救援活动和急救治疗等。

1. 防止能量的破坏性作用

（1）限制能量的集中与蓄积。一定量的能量集中于一点要比大面散开所造成的伤害程度更大。有一些具有能量的物体本身就是工厂的产品或原料，如炼油厂的原油及其成品汽油和轻油，发电厂的电以及一些化工企业原料用轻油等。对这样一些工厂要根据原料或产品的储量和周转量规定限额来限制能量集中。对某些机械能可采用限制能量的速度和大小，规定极限量，如限速装置。对电气设备采用低电压装置，如使用低压测量仪表以及熔丝、断路器和使用安全电压等。

防止能量蓄积，如温度自动调节器、控制爆炸性气体或有害气体浓度的报警器、应用低势能（如地面装卸作业）等。

（2）控制能量的释放。具体如下：

1）防止能量的逸散，如将放射性的物质储存在专用容器内，电气设备和线路采用良好的绝缘材料以防止触电，高空作业人员使用安全带及建筑工地张挂安全网。

2）延缓能量释放，如用安全阀、逸出阀、吸收机械振动的吸振器以及缓冲装置等。

3）另辟能量释放渠道，如接地电线、抽放煤层中的瓦斯、排空管等。

（3）隔离能量。具体如下：

1）在能源上采取措施，如在运动的机件上加防护罩、防冲击波的消波器、防噪声装置等。

2）在能源和人与物之间设防护屏障，如防火墙、防水闸墙、辐射防护屏以及安全帽、安全鞋和手套等个体防护用具等。

3）设置安全区、安全标志等。

（4）其他措施。为提高防护标准，可采用双重绝缘工具、低压电回路、连续监测和遥控等；为提高耐受能力，可挑选适应性强的人员，选用耐高温、高寒以及高强度材料。

2. 采取降低损失程度的措施

事故一旦发生，应马上采取措施，抑制事态发展，减轻危害的严重性，如设置紧急冲浴设备、开展快速救援活动和急救治疗等。

3. 防止人的失误

人的失误是人为地使系统发生故障或发生使机件不良的事件，是违反设计和操作规程的错误行为。人的可靠性比机械、电器或电子元件要低很多，特别是情绪紧张时容易受作业环

试读版本仅供防疫期间线上教学使用

境影响，失误的可能性更大。为了减少人的失误，应为操作人员创造安全性较强的工作条件，设备要符合人机工程学的要求，重复操作频率大的工作应用机械代替手工，变手工操作为自动控制。

建立健全规章制度、严格监督检查、加强安全教育也是有力措施。

2.2.7　实用实例

预先危险分析的记录结果一般采用表格的形式列出。表格的格式和内容可根据实际情况确定。表2-7～表2-9为几种基本的预先危险分析表（PHA）的表格格式。

表2-7　PHA工作表

单元：　　编制人员：　　日期：

危　险	原　因	后　果	危险等级	改进措施/预防方法

表2-8　PHA工作的典型格式表

地区（单元）：　　会议日期：

图号：　　小组成员：

危险/意外事故	阶　段	原　因	危险等级	对　策
事故名称	危险发生的阶段，如生产、试验、运输、维修、运行等	产生危害的原因	对人员及设备的危害	消除、减少或控制危险的措施

表2-9　PHA表通用格式

系统：1　　子系统：2　　状态：3　　制表者：

编号：　　日期：　　制表单位：

潜在事故	危险因素	触发事件	发生条件	触发事件	事故后果	危险等级	防范措施	备注
4	5	6	7	8	9	10	11	12

注：1——所分析子系统归属的车间或工段的名称；

2——所分析子系统的名称；

3——子系统处于何种状态或运行方式；

4——子系统可能发生的潜在危害；

5——产生潜在危害的原因；

6——导致产生“危险因素5”的那些不希望事件或错误；

7——使“危险因素5”发展成为潜在危害的那些不希望发生的错误或事件；

8——导致生产“发生条件7”的那些不希望发生的事件及错误；

9——事故后果；

10——危害等级；

11——为消除或控制危害可能采取的措施，其中包括对装置、人员、操作程序等几方面的考虑；

12——有关必要的说明。

试读版本仅供防疫期间线上教学使用

PHA 的表格中应该有以下内容：①了解系统的基本目的、工艺工程、控制条件及环境因素等；②划分整个系统为若干子系统（单元）；③参照同类产品或类似的事故教训及经验，查明分析单元可能出现的危害；④确定危害的起因；⑤提出消除或控制危险的对策，在危险不能控制的情况下，分析最好的预防损失的方法。

【例 2-4】　表 2-10 是根据某液化石油气新建项目，做出的预先危险性分析，并提出了可行的防范措施，对表格中存在的事故发生原因进行分析。

表 2-10　液化石油气火灾、爆炸预先危险性分析

危险因素	液化石油气及其残液泄漏，压力容器爆炸
触发事件一	（1）故障泄漏 ① 储罐、汽化器、管线、阀门、法兰等泄漏或破裂 ② 储罐等超装溢出 ③ 机、泵破裂或转动设备、泵密封处泄漏 ④ 罐、器、机、泵、阀门、管道、流量计、仪表等连接处泄漏 ⑤ 罐、器、机、泵、阀门、管道等因质量不好（如制造加工质量、材质、焊接等）或安装不当泄漏 ⑥ 撞击（如车辆撞击、物体倒落）或人为破坏造成罐、器及管线等破裂而泄漏 ⑦ 由自然灾害造成的破裂泄漏，如雷击、台风等 （2）运行泄漏 ① 超温、超压造成破裂、泄漏 ② 安全阀等安全附件失灵、损坏或操作不当 ③ 垫片撕裂造成泄漏 ④ 骤冷、急热造成罐、器等破裂、泄漏 ⑤ 液化石油气瓶等压力容器未按有关规定及操作规程操作 ⑥ 转动部分不洁摩擦产生高温及高温物件遇易燃物品
发生条件	（1）液化石油气浓度达到爆炸极限 （2）液化石油气及其残液遇明火 （3）存在点火源、静电火花、高温物体等引燃、引爆能量
触发事件二	（1）明火 ① 点火吸烟 ② 烟火 ③ 抢修、检修时违章动火，焊接时未按“十不烧”及有关规定动火 ④ 外来人员带入火种 ⑤ 物质过热引起燃烧 ⑥ 其他火源，如电动机不洁、轴承冒烟着火 ⑦ 其他火灾引发二次火灾等 （2）火花 ① 穿带钉皮鞋 ② 击打管道、设备产生撞击火花 ③ 电气线路陈旧老化或受到损坏产生短路火花，以及因超载、绝缘烧坏引起明火 ④ 静电放电 ⑤ 雷击（直接雷击、雷电二次作用，沿着电气线路或金属管道侵入）

试读版本仅供防疫期间线上教学使用

（续）

危险因素	液化石油气及其残液泄漏，压力容器爆炸
触发事件二	⑥ 进入车辆未带阻火器等（一般要禁止驶入） ⑦ 焊、割、打磨产生火花等
事故后果	液化石油气跑损、人员伤亡、停产、造成严重经济损失
危险等级	Ⅳ
防范措施	（1）控制与消除火源 ① 严禁吸烟、携带火种、穿带钉皮鞋进入易燃易爆区 ② 动火必须严格按动火手续办理动火证，并采取有效防范措施 ③ 易燃易爆场所使用防爆型电器 ④ 使用不发火的工具，严禁钢质工具敲打、撞击、抛掷 ⑤ 按规定安装避雷装置，并定期进行检测 ⑥ 按规定采取防静电措施 ⑦ 加强门卫，严禁机动车辆进入火灾、爆炸危险区，运送液化石油气的车辆必须配置完好的阻火器，正确行驶，杜绝发生任何故障和车祸 （2）严格控制设备质量及其安装 ① 罐、器、管线、机、泵、阀等设备及其配套仪表要选用质量好的合格产品，并把好质量关和安装关 ② 管道、压力容器及其仪表等有关设施要按要求进行定期检验、检测、试压 ③ 对设备、管线、机、泵、阀、仪表、报警器、监测装置等要定期进行检查、保养、维修，保持完好状态 ④ 按规定安装电气线路，定期进行检查、维修、保养，保持完好状态 ⑤ 有液化石油气泄漏的场所，高温部件要采取隔热、密闭措施 （3）防止液化石油气及其残液的跑、冒、滴、漏 （4）加强管理，严格工艺纪律 ① 禁火区内根据“170号公约”和危险化学品安全管理条例张贴作业场所危险化学品安全标签 ② 杜绝“三违”（违章作业、违章指挥、违反劳动纪律），严守工艺纪律，防止生产控制参数发生变化 ③ 坚持巡回检查，发现问题及时处理，如液位报警器、呼吸阀、压力表、安全阀、防寒保温、防腐、联锁仪表、消防及救护设施是否完好，液位报警器是否正常，储罐、管线、截止阀、自动调节阀等有否泄漏，消防通道、地沟是否畅通等 ④ 检修时，特别是液化石油气及其残液储罐，必须做好与其他部分的隔离（如安装盲板等），并且要彻底清理干净，分析合格后，在有现场监护及通风良好的条件下，方能进行动火等作业 ⑤ 检查有否违章、违纪现象 ⑥ 加强培训、教育、考核工作 ⑦ 防止车辆撞坏管线等设施 （5）安全设施要齐全完好 ① 安全设施（如消防设施、遥控装置）齐全并保持完好 ② 储罐安装高、低液位报警器 ③ 易燃、易爆场所安装可燃气体检测报警装置

试读版本仅供防疫期间线上教学使用

【例 2-5】 对某新建化工码头项目进行劳动卫生预评价，对码头装卸作业进行预先危险分析并提出了防范措施，分析结果见表 2-11。

表 2-11 码头装卸作业 PHA 分析

危险、有害因素	触发事件	现象	形成事故原因事件	事故模式	事故后果	危险等级	措施
化学性爆炸：苯、苯乙烯等易燃易爆物料泄漏	运行泄漏： ① 码头设备运行泄漏 ② 接卸结束时，接卸臂洒漏 ③ 阀门、法兰等泄漏 ④ 泵破裂或泵、转动设备等动密封处泄漏 ⑤ 阀门、泵、管道、流量计、仪表连接处泄漏 ⑥ 阀门、泵、管道等因质量或安装不当泄漏 ⑦ 撞击或人为破坏等造成管道等破裂而泄漏 ⑧ 由自然灾害造成的破裂泄漏，如雷击等	① 易燃易爆物料蒸气浓度达到爆炸极限 ② 易燃易爆物料泄漏	火花： ① 穿带钉皮鞋 ② 用钢制工具敲打设备、管道产生撞击火花 ③ 电器火花 ④ 电气线路陈旧老化或受到损坏产生短路火花 ⑤ 静电放电 ⑥ 雷击（直接雷击、雷电二次作用，沿着电气线路、金属管道侵入） ⑦ 车辆未配灭火器等	可能引起火灾、爆炸	财产损失、人员伤亡、造成严重经济损失	Ⅳ	（1）控制与消除火源 ① 严禁吸烟、携带火种、穿带钉皮鞋等进入易燃易爆区 ② 动火必须严格按动火手续办理动火证，并采取有效防范措施 ③ 使用防爆型电器，如防爆手电；使用安全电压（12V）防爆灯 ④ 使用青铜或镀铜工具，严禁钢质工具敲打、撞击、抛掷 ⑤ 按规定要求采取防静电措施，安装避雷装置 ⑥ 加强门卫，严禁机动车辆进入火灾、爆炸危险区 ⑦ 运送物料的机动车辆必须配备完好的阻火器 ⑧ 转动设备部位要保持清洁，防止因摩擦引起杂物等燃烧 ⑨ 周围居民区在一定范围内不能燃放烟花爆竹 （2）严格控制设备质量及其安装质量 ① 泵、阀、管线等设备及其配套仪表要选用合格产品，并把好安装质量关 ② 管道等有关设施在投产前要按要求进行试压 ③ 对设备、管线、泵、阀、仪表等要定期检查、保养、维修，保持完好状态

通过预先危险分析，可以得知，该工程存在着火灾、爆炸、中毒、窒息、淹溺、触电、噪声等危险因素，引发火灾、爆炸的主要因素是故障泄漏和存在点火源。

【例 2-6】 电气危险的 PHA 分析。

（1）电气火灾事故的 PHA 分析（见表 2-12）。电气设备火灾、爆炸事故在火灾和爆炸事故中占很大比例，仅就电气火灾而言，无论是发生频率还是所造成的经济损失，在火灾事故中所占的比例都有上升趋势。配电线路、高低压开关电器、熔断器、插座、照明器具、电动机、电热器具等电气设备均可能引起火灾。电容器、变压器等电气装置除可能引

试读版本仅供防疫期间线上浏览使用

起电气火灾外，本身还可能发生爆炸。电气火灾火势凶猛，如不及时扑灭，势必迅速蔓延。电气火灾除可能造成人身伤亡和设备损坏外，还可能造成大规模或长时间停电，给企业、国家财产造成重大损失。

表 2-12　电气火灾事故 PHA 分析

危险、有害因素	事故所处位置	现　象	结　果	危险等级
安装、接线疏忽引起相间短路	断路器	接触电阻增大、爆出火花	导线烧毁、引起电气火灾	—
安装环境潮湿		电源端相间布满水气引起击穿	配电箱被烧、建筑物起火	
额定电流选择偏大	断路器 熔断器	发生过载时在规定时间不动作	损害绝缘、接线端子和周围物体，严重时会引起短路	2
电流偏大	线缆	引起过载	保护不当会短路	2
线路超载		断路器频繁跳闸、无法用电	如强行使用，过载会引起短路	
漏电		三相对地短路	时间略长将引起电火花，酿成火灾	3
三相负载不平衡	单相用电设备	某相电压升高	严重时将烧毁单相用电设备，导致起火	2
中性线断裂		绝缘受损	保护不当将引起单相设备烧坏，产生电气火灾	2
单相接地	相线碰外壳和金属管道	小电流短路	引起打火或接弧，遇可燃物发生火灾	3

（2）电缆线路故障 PHA 分析（见表 2-13）。电缆线路是供、配电系统的重要组成部分，担负着输送电能的任务。电缆线路应满足生产设施对供电可靠性的要求，且在电能的供应、分配和使用中，不应发生人身事故和设备事故。

电缆线路主要由电力电缆、终端封头和中间接头三部分组成。电缆则主要由导电线芯、绝缘层、保护层组成。

电缆敷设在电缆沟和电缆隧道中，也有直接埋于地下的情况。直接埋在地下的方式，容易施工、散热良好，但检修、更换不便，不能可靠地防止外力损伤，而且易受土壤中酸碱物质的腐蚀。电缆终端头和中间接头是整个电缆线路的薄弱环节。约有 70% 的电缆线路故障发生在终端头和中间接头部位。安全运行对防止和减少事故发生有着十分重要的意义。

表 2-13　电缆线路故障 PHA 分析

危险、有害因素	事故原因	现　象	结　果	危险等级
外力破坏	机械损伤	线缆短路或断裂	意外断电	3

试读版本仅供防疫期间线上教学使用

（续）

危险、有害因素	事故原因	现象	结果	危险等级
终端头污染	绝缘表面脏污	绝缘击穿	断电	3
中间接头爆炸	接头浸水	爆炸	意外断电	3
腐蚀	化学腐蚀和电腐蚀	金属护套腐蚀	绝缘破坏	3
虫害	白蚁破坏	金属护套穿孔，绝缘受潮	绝缘击穿	3
长期负荷运行	设计和管理不当	在电场的作用下，会发生绝缘老化现象	电缆绝缘击穿或意外断电	3
电缆进水	储存、敷设、电缆头制作过程不良 外力破坏、中间接头击穿	金属护套胀裂，绝缘浸水	绝缘击穿或中间接头爆炸	3

（3）雷电事故的 PHA 分析（见表 2-14）。雷电是大气中的一种放电现象。雷电放电具有电流大、电压高的特点。其能量释放出来可能形成极大的破坏力。其破坏作用主要有以下几个方面：

1）直击雷放电、二次放电、雷电流的热量会引起火灾和爆炸。

2）雷电的直接击中、金属导体的二次放电、跨步电压的作用及火灾与爆炸的间接作用，均会造成人员的伤亡。

3）强大的雷电流、高电压可导致电气设备击穿或烧毁；发电机、变压器、电力线路等遭受雷击，可导致大规模停电事故；雷击可直接毁坏建（构）筑物。

表 2-14 雷电事故的 PHA 分析

危险、有害因素	事故原因	现象	结果	危险等级
雷击	防雷装置未动作	绝缘被击穿后剧烈放电使人身触电	火灾、爆炸设备伤害或人身伤亡	3
反击事故	接闪器、引下线、接地装置与邻近导体安全距离不够	绝缘击穿、剧烈放电	火灾、爆炸或人身伤亡	3
雷电侵入波	雷电侵入波沿低压线路进入室内 雷电侵入波的正变换电压与来自高压边的反变换电压击穿变压器的绝缘	人身触电 变压器绝缘击穿	人身伤亡 设备损坏	3

2.3 故障类型及影响分析

故障类型及影响分析（Failure Modes and Effects Aanlysis，简称 FMEA），是安全系统工

试读版本仅供防疫期间线上教学使用

程中重要分析方法之一。它采取系统分割的概念，根据实际需要把系统分割成子系统，或进一步分割成元件。然后对系统的各个组成部分进行逐个分析，寻求各组成部分中可能发生的故障、故障因素以及可能出现的事故，可能造成的人员伤亡的事故后果，查明各种故障类型对整个系统的影响，并提出防止或消除事故的措施。

FMEA 分析方法源于可靠性技术，最初只能做定性分析，后来在分析中增加了故障发生难易程度或发生概率的评价，将它与危险度分析（Criticality Analysis，CA）结合起来，发展成故障类型和影响危险性分析（FMECA），这样，如果确定了每个元件（或子系统）的故障发生概率，就可以确定系统的故障发生概率，从而实现对故障影响的定量评价。

2.3.1　基本概念及格式

1. 基本概念

（1）故障。故障是指系统或元素在运行过程中，不能达到设计规定的要求，因而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。

（2）故障类型。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，一般可从五个方面来考虑，即：运行过程中的故障；过早地起动；规定时间内不能起动；规定时间内不能停车；运行能力降级、超量或受阻。

（3）危险度。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。

（4）故障等级。故障等级是衡量故障对系统任务、人员和财务安全造成影响的尺度。人们根据故障造成影响的大小而采取相应的处理措施，因此评定故障等级很有必要，评定时可以从以下几个方面来考虑：

1）故障影响大小。

2）对系统造成影响的范围。

3）故障发生的频率。

4）防止故障的难易。

5）是否重新设计。

2. 格式

表 2-15 为故障类型与影响分析一般格式。

表 2-15　故障类型与影响分析表

子系统或设备部件	故 障 类 型	故 障 原 因	故 障 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，在编制分析图表时，只需在故障类型及影响分析的图表之中加上通过分析计算得出的危险程度数值和故障发生概率数值两列栏目即可。

3. 故障类型及影响分析的适用范围

FMEA 是一种归纳分析方法，主要是对系统的各组成部分，即元件、组件、子系统等进行分析，找出它们所能产生的故障及其类型，查明每种故障对系统安全的影响，判明故障的重要

试读版本仅供防伪和预览，上学使用

度，以便采取措施予以防止和消除。其优点是：从部件分析到故障，侧重上、下逻辑关系，容易掌握，有针对性，对硬件分析有较大优势；对于高风险的系统或子系统采用这种分析方法可以得到比 PHA 更为精确的结果。其缺点是：必须对系统的每个部件都进行分析，从经济上考虑较为不合理，尤其是大型、复杂系统，需耗费大量时间和精力；重在对单点故障及其对系统的影响分析，忽略了部件之间的相互作用，无法识别它们导致的组合故障类型对系统的影响。

在产品或系统的设计和研发阶段应合理使用 FMEA 方法，尤其在详细设计阶段，因为系统设计已细致到元器件层次，采用 FMEA 分析方法进行分析对保证设计的正确合理有积极作用，此时发现问题及时修改无需太昂贵的费用。理论上，FMEA 法适用于从系统到元器件任一层次的分析，实际中，常用于较低层次的分析，也常与其他方法结合使用。

2.3.2　FMEA 的步骤

（1）调查所分析系统的情况，收集整理资料。将所分析的系统或设备部件的工艺、生产组织、管理和人员素质、设备等情况，以及投产或运行以来的设备故障和伤亡事故情况进行全面调查分析，收集整理伤亡事故、设备故障等方面的有关数据和资料。

（2）危险源初步辨识。组织与该系统或设备部件有关的工人、技术人员和安全管理人员开展危险预知活动，摆明问题，从操作行为、设备、工艺、环境因素、管理状态等方面进行危险源辨识和分析。

（3）故障类型、影响及组成因素分析。危险源列出后，即根据收集整理的设备故障、伤亡事故情况等资料进行故障类型、影响及组成因素分析。

（4）故障等级分析。通过危险源辨识、故障类型及组成因素的分析，对系统中危险因素的基本情况有了初步了解，此时需进行故障等级分析，以衡量故障对系统造成的影响程度。

1）简单划分法。一般将故障对子系统或系统影响的严重程度分为 4 个等级，见表 2-16。简单划分法即以表 2-16 为依据，采用这种定性方法，直接判定故障模式的故障等级。

表 2-16　故障类型等级

故障等级	影响程度	危害后果
Ⅰ级	破坏性的	会造成严重人员伤害或系统损坏，必须设法消除
Ⅱ级	危险的	会造成较重人员伤害或系统损坏，需立即采取控制措施
Ⅲ级	临界的	会造成较轻人员伤害或系统损坏，但可排除和控制
Ⅳ级	可忽略	不会造成人员伤害和系统损坏

2）评点法。由于简单划分法是一种直接定性判别方法，基本上只考虑故障的危险性，不考虑其发生概率，因而具有一定的片面性。评点法可考虑故障影响大小、对系统造成影响的范围、故障发生概率等多个因素，实现对故障等级的半定量评估，因而得到了较为广泛的应用。评点法的计算形式多样，主要分为“乘积评点”和“求和评点”两种形式。

“乘积评点”形式：故障等级值 c_s 计算式为：

$$c_s = \sqrt[n]{c_1 c_2 \cdots c_i} = \sqrt[5]{c_1 c_2 c_3 c_4 c_5} \tag{2-1}$$

式中　c_s——总点数，$0 < c_s < 10$；

c_i——各因素的取值，$0 < c_i < 10$；

试读版本仅供试用期间线上教学使用

i——考虑的因素种类，$i=1$，2，3，…，n，一般取 $n=5$，即：

c_1——故障影响大小，即损失严重程度；

c_2——故障影响范围，即影响到系统的哪个层次；

c_3——故障频率；

c_4——防止故障的难易程度；

c_5——是否为新设计的工艺。

最后，根据 c_s 值划分故障等级，划分标准见表2-17。

表2-17　评点法故障等级划分表

故障等级	c_s 值	内　容	应采取的措施
Ⅰ（破坏性的）	7～10	完不成任务，人员伤亡	变更设计
Ⅱ（危险的）	4～7	大部分任务完不成	重新讨论设计，也可变更设计
Ⅲ（临界的）	2～4	一部分任务完不成	不必变更设计
Ⅳ（可忽略）	＜2	无影响	无

“求和评点”形式：故障等级值 c_s 计算式为：

$$c_s = \sum_{i=1}^{n} c_i \tag{2-2}$$

同理，一般取 $n=5$，此时 c_i 取值按表2-18划分。

表2-18　“求和评点”c_i 取值划分表

评价因素	内　容	c_i 值
故障影响大小 c_1	造成生命损失	5.0
	造成相当程度的损失	3.0
	组件功能损失	1.0
	无功能损失	0.5
故障影响范围 c_2	对系统造成两处以上的重大影响	2.0
	对系统造成一处重大影响	1.0
	对系统无过大影响	0.5
故障频率 c_3	容易发生	1.5
	能够发生	1.0
	不大发生	0.7
防止故障的难易程度 c_4	不能防止	1.3
	能够防止	1.0
	易于防止	0.7
是否为新设计的工艺 c_5	内容相当新的工艺	1.2
	内容和过去类似的设计	1.0
	内容和过去一样的设计	0.8

注：故障发生概率，非常容易发生，1×10^{-1}；容易发生，1×10^{-2}；较容易发生，1×10^{-3}；不容易发生，1×10^{-4}；难以发生，1×10^{-5}；极难发生，1×10^{-6}。

（5）检测方法与预防措施。检测主要采用常规或专门的方法测定故障和危险因素。预防措施是对故障因素和危险源的控制措施。

试读版本仅供防疫期间线上教学使用

（6）按故障危险程度与概率大小，分先后次序，轻重缓急地逐项采取预防措施。

2.3.3 FMEA（故障类型及影响分析）举例

【例 2-7】 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 2-19 中。

表 2-19 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	加强维修保护
	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、受冲压等	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
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	加强维修保护
	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	停机修理
	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

【例 2-8】 表 2-20 为起重机防止过卷装置和钢丝绳两组系统的 FMECA 应用实例。

表 2-20 起重机部分组成元素 FMECA 分析表

名称	组成元素	故障类型	故障原因	故障影响	发生概率	检查方法	校正措施	故障级别
防止过卷装置	电器零件	动作不可靠	零件失修	误动作	1×10^{-2}	通电检查	立即维修	$c_s=1+1+1.5+0.7+0.8=5$ Ⅱ（危险的）
	机械部分	变形、生锈	使用过久	损坏	1×10^{-4}	观察	警惕	$c_s=1+0.5+0.7+0.7+0.8=3.7$ Ⅲ（临界的）
	制动瓦块	间隙过大	螺钉松动	制动失灵	1×10^{-3}	观察	及时紧固	$c_s=3+1+1+0.7+0.8=6.5$ Ⅱ（危险的）
钢丝绳	绳股	变形、扭结	使用过久	绳断裂	1×10^{-4}	观察	及时更换	$c_s=1+0.5+0.7+0.7+0.8=3.7$ Ⅲ（临界的）
	钢丝	断丝15%	使用过久	绳断裂	1×10^{-1}	观察	立即更换	$c_s=1+1+1.5+1+0.8=5.3$ Ⅱ（危险的）

注：此处故障级别判断按照“求和评点”法进行，对每一类故障类型依据表 2-18 进行 c_i 取值，取值结果累加求得 c_s 值，最后按照表 2-17 划分故障等级。

试读版本仅供预览期间线上教学使用

2.4 危险性与可操作性研究

2.4.1 基本概念及特点

1. 基本概念

危险性与可操作性研究（Hazard and Operability Study，简记为 HAZOP），是英国帝国化学工业公司（ICI）于 1974 年针对化工装置而开发的一种危险性评价方法。

HAZOP 的基本过程是以关键词为引导，找出系统中工艺过程的状态参数（如温度、压力、流量等）的变化（即偏差），然后再继续分析造成偏差的原因、后果及可以采取的对策。通过危险性与可操作性研究的分析，能够探明装置及过程存在的危险，根据危险带来的后果，明确系统中的主要危险；如果需要，可利用事故树对主要危险继续分析，因此它又是确定事故树“顶上事件”的一种方法。在进行 HAZOP 分析过程中，分析人员对单元中的工艺过程及设备状况要深入了解，对于单元中的危险及应采取的措施要有透彻的认识，因此，HAZOP 分析还被认为是对工人培训的有效方法。

可操作性研究既适用于设计阶段，又适用于现有的生产装置。对现有生产装置分析时，如能吸收有操作经验和管理经验的人员共同参加，会收到很好的效果。

英国帝国化学工业公司开发的 HAZOP 分析方法，主要是应用于连续的化工过程。在进行若干改进以后，也能很好地应用于间歇过程的危险性分析。我国安全生产监督管理总局已于 2013 年 6 月 8 日发布了《危险与可操作性分析（HAZOP 分析）应用导则》（AQ/T 3049—2013），用于石油、化工、电子等工业的 HAZOP 分析。HAZOP 分析是一个对工艺单元或操作步骤运用引导词和工艺参数进行组合系统分析的过程，如图 2-6 所示。HAZOP 分析必须由不同的专业人员分组完成。

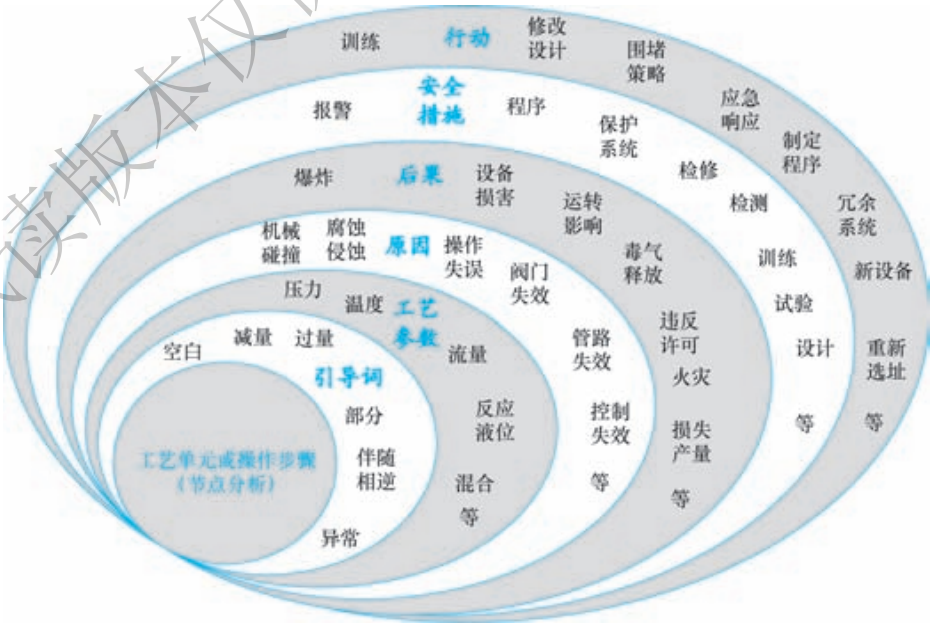

图 2-6　HAZOP 分析示意图

试读版本仅供防疫期间线上学习使用

2. HAZOP 分析的特点

HAZOP 分析具备以下特点：

（1）它从生产系统中的工艺状态参数出发来研究系统中的偏差，运用启发性引导词来研究因温度、压力、流量等状态参数的变动可能引起的各种故障的原因、存在的危险以及采取的对策。

（2）它是故障类型及影响分析的发展。它研究和运行状态参数有关的因素。它从中间过程出发，向前分析其原因，向后分析其结果。向前分析是事故树分析，向后分析是故障类型及影响分析，它有两种分析的特长，因为两种方法都有中间过程。中间过程可理解为故障类型及影响分析中的故障模式对子系统的影响，或者是事故树分析的中间事件。它承上启下，既表达了元件故障包括人的失误相互作用的状态，又表达了接近顶上事件更直接的原因。因此，不仅直观有效，而且更易查找事故的基本原因和发展结果。

（3）HAZOP 分析方法，不需要有可靠性工程的专业知识，因而很易掌握。使用引导词进行分析，既可启发思维，扩大思路，又可避免漫无边际地提出问题。

（4）研究的状态参数正是操作人员控制的指标，针对性强，利于提高安全操作能力。

（5）研究结果既可用于设计的评价，又可用于操作评价；既可用来编制、完善安全规程，又可作为可操作的安全教育材料。

2.4.2 分析步骤

HAZOP 全面考察分析对象，对每一个细节提出问题，如在工艺过程的生产运行中，要了解工艺参数（温度、压力、流量、浓度等）与设计要求不一致的地方（即发生偏差），继而进一步分析偏差出现的原因及其产生的后果，并提出相应的对等措施，如图 2-7 所示。

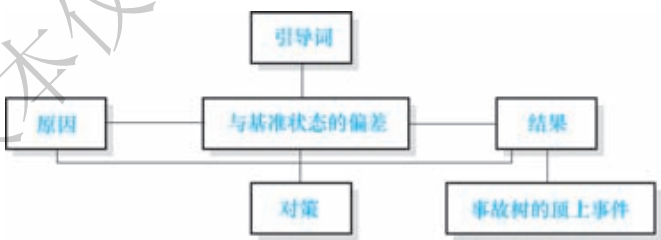

图 2-7 可操作性研究的分析步骤

（1）提出问题。为了对分析的问题能开门见山，单刀直入，所以在提问题时，只用 No（无）、More（多）、Less（少）、As Well As（伴随）、Part of（部分）、Reverse（相反）、Other Than（异常）来涵盖所有出现的偏差。

（2）划分单元，明确功能。将分析对象划分为若干单元，在连续过程中单元以管道为主，在间歇过程中单元以设备为主。明确各单元的功能，说明其运行状态和过程。

在 HAZOP 分析中，通常依据工艺划分为若干工艺单元（亦称为节点），然后对工艺单元内的工艺参数偏差进行分析。常见的工艺单元见表 2-21。

试读版本仅供阅读期间学习教学使用

表 2-21　常见工艺单元一览表

序　号	工艺单元（节点）	序　号	工艺单元（节点）
1	管线	8	熔炉/炉/窑
2	分批反应器	9	热交换器
3	连续反应器	10	软管
4	罐/槽/容器	11	公用工程和辅助设施
5	塔	12	其他
6	压缩机	13	以上节点的合理组合
7	鼓风机		

（3）定义引导词表。按引导词逐一分析每个单元可能产生的偏差，一般从工艺过程的起点、管线、设备等一步步分析可能产生的偏差，直至工艺过程结束。

（4）分析原因及后果。以化工装置为例，应分析工艺条件（温度、压力、流量、浓度、杂质、催化剂、泄漏、爆炸、静电等），开停车条件（试验、开车、检修；设备和管线，如标志、反应情况、混合情况、定位情况、工序情况等），紧急处理（气、汽、水、电、物料、照明、报警、联系等非计划停车情况），甚至自然条件（风、雷、雨、霜、雪、雾、地质以及建筑安装等）。分析发生偏差的原因及后果。

（5）制定对策。

（6）填写汇总表。为了按危险性与可操作性研究分析表（表 2-22）进行汇总填写，保证分析详尽而不发生遗漏，分析时应按照引导词表逐一进行。引导词表可以根据研究的对象和环境确定。表 2-23 和表 2-24 为两个引导词定义表。

表 2-22　危险性与可操作性研究分析表

引　导　词	偏　差	可 能 原 因	结　果	修 正 措 施

表 2-23　引导词定义表（一）

引导词	意　义	说　明
空白	设计与操作所要求的事件完全没有发生	没有物料输入，流量为零
过量	与标准值比较，数量增加	流量或压力过大
减量	与标准值比较，数量减少	流量或压力减小
部分	只完成功能的一部分	物料输送过程中某种成分消失或仅输送一部分
伴随	在完成预定功能的同时，伴随多余事件发生	物料输送过程中发生组分及相的变化
相逆	出现与设计和操作相反的事件	发生反向的输送
异常	出现与设计和操作要求不相干的事件	异常事件发生

试读版本仅供阅读期间学习教学使用

表 2-24 引导词定义表（二）

引导词	意 义	说 明
否	对标准值的完全否定	完全没有完成规定功能，什么都没有发生
多	数量增加	包括：数量的多与少，性质的好与坏，完成功能程序的高与低
少	数量减少	
而且	质的增加	完成规定功能，但有其他事件发生，如增加过程、组分变多
部分	质的减少	仅实现部分功能，有的功能没有实现
相反	逻辑上与规定功能相反	对于过程：反向流动、逆反应、程序颠倒 对于物料：用催化剂还是抑制剂
其他	其他运行状况	包括：其他物料和其他状态、其他过程、不适宜的运行过程、不希望的物理过程等

由表 2-23 和表 2-24 可以看出，在研究不同的系统时，可以定义不同的引导词，且即使引导词相同，其代表的意义也可以是不同的。因此，在进行可操作性研究时，必须根据引导词表分析各个单元产生的偏差。

2.4.3 实用实例

【例 2-9】 以 35t/h 燃油锅炉为例进行危险性与可操作性研究（见表 2-25）。

表 2-25 35t/h 燃油锅炉危险性与可操作性研究

引导词	偏 差	可能原因	结 果	修正措施
否	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 排污阀泄漏 ④ 判断失误（假水位） ⑤ 工作失误，误操作	造成爆管甚至锅炉爆炸	① 确保自动给水，高低位水位报警，低水位连锁等自动保护装置安全可靠，水位计灵敏可靠 ② 加强设备维修，确保给水系统、排污系统、设备、阀门、管道完好、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”（违章作业，违章指挥，违反劳动纪律）
	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 ③ 燃油雾化不良 ④ 燃油与空气混合差 ⑤ 操作不当或不遵守操作规程 ⑥ 喷燃器设计、制造不合理	锅炉灭火引发锅炉炉膛爆炸	① 燃油应符合设计要求 ② 锅炉炉膛和燃烧器的设计，应与设计使用燃油的特性相适应 ③ 燃油变化范围应符合有关技术标准 ④ 根据油品选择合理的雾化方法，确保燃油雾化质量 ⑤ 严格按操作规程操作，杜绝“三违” ⑥ 装设性质良好、安全可靠的灭火保护装置和炉膛火焰监控装置 ⑦ 在炉膛装设防爆门，炉墙应严密不漏

试读版本仅供防疫期间线上教学使用

（续）

引导词	偏　差	可能原因	结　果	修正措施
多	锅炉超压	① 安全阀失灵 ② 压力表故障 ③ 超压报警及联锁保护失灵 ④ 操作不当或不遵守操作规程或脱岗	造成爆管甚至锅炉爆炸	① 安全阀必须做到安全可靠，动作灵敏，定期校验，定期做排汽试验 ② 压力表必须做到灵敏可靠，装置齐全，定期校验 ③ 确保超压报警及联锁保护装置安全、可靠 ④ 应装设燃烧自动调节装置，并确保可靠 ⑤ 严格按操作规程操作，杜绝“三违”
	锅炉漏水	① 水位超限报警保护失灵，水位计失灵 ② 自动给水故障 ③ 判断失误 ④ 工作失误，误操作，违反劳动纪律（脱岗）	① 造成蒸汽管道水冲击 ② 带汽轮发电机组：造成汽轮机水冲击	① 确保自动给水装置，高水位报警装置可靠 ② 水位计应灵敏可靠，定期冲洗，定期校验 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”
	锅炉过热蒸汽超温(对无过热蒸汽的锅炉，此项无)	① 蒸汽温度自动调节装置失灵 ② 超温报警装置失灵 ③ 温度计故障 ④ 工作失误、误操作、脱岗	过热器管过热、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 确保温度计灵敏可靠，定期校验 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”
	锅炉严重结垢	① 炉外水处理不合格，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	造成锅炉受热面结垢，导致受热面过热而引发爆管	① 给水必须经炉外处理合格后才能进入锅炉，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查 ② 因空气潮湿及烟气冲刷造成外部腐蚀 ③ 停炉未做保养或保养方法不当造成停炉腐蚀 ④ 给水未除氧，pH值偏小等造成运行腐蚀	使受热面壁厚减薄造成爆管，甚至锅炉爆炸	① 坚持每年对锅炉定期检查，测定其壁厚，并制定相应措施 ② 切实加强停炉保养工作 ③ 按规定控制运行锅炉炉水碱度，锅炉给水的含氧量必须控制在规定范围内 ④ 停运锅炉应保持锅炉四周空气干燥，运行时尽可能少用含硫量较大的油，并防止尾部低温腐蚀
	供油量不足	油泵不够、油管道故障、油箱油不够	影响负荷、压力	① 加强维修检查 ② 提供充足的油源

试读版本仅供防疫期间线上教学使用

（续）

引导词	偏　差	可能原因	结　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、材质存在缺陷 ② 误操作或违章操作 ③ 无定期维护、保养	泄漏的燃油遇明火或高温引发火灾甚至爆炸	① 油系统的设备、管线的设计、安装、检验、造型、材质应符合相应的规程、规范、标准，做到严密不漏 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，其表面温度低于50℃ ④ 严格执行操作规程，加强劳动纪律，杜绝“三违” ⑤ 油系统附近应严禁烟火
	噪声	① 风机、水泵等设备运行产生噪声 ② 蒸汽排放	听力损伤	① 选用噪声小的设备 ② 应加装消声设施和放在单独的隔声机房内 ③ 蒸汽排放应设置消声器 ④ 对控制室采用隔离门、双层玻璃窗等隔声措施
	机械伤害	无罩及无防护栏杆	伤害职工身体	按规定对机械转动设备加罩或防护栏杆
	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，确保严密不漏，发现泄漏应及时处理 ② 锅炉及汽、水应加强保温，使其表面温度低于50℃
其他	地震、雷电	自然灾害	危及设备和人身安全	① 锅炉房厂房应根据标准按相应的地震烈度设计 ② 高层建筑物的层顶、烟囱顶部应设置避雷带，使需要保护的建筑物均在保护之内 ③ 控制室要防止感应电和雷电侵入

【例 2-10】 某工厂生产工艺简图如图 2-8 所示。物料 A 和物料 B 通过泵连续从各自的供料罐输送至反应器，在反应器中生成产品 C。假定为了避免爆炸危险，在反应器中物料 A 总是多于物料 B。为简化示例，将完整设计的诸多细节如压力影响、反应和反应物的温度、搅拌、反应时间、泵 A 和泵 B 的匹配性等简化和忽略。

按照 HAZOP 分析法，首先根据工厂生产工艺划分工艺单元如下：①物料 A 存储输送单元，即从盛有物料 A 的供料罐到反应器之间的管道，包括泵 A；②物料 B 存储输送单元，即从盛有物料 B 的供料罐到反应器之间的管道，包括泵 B；③反应器及产品输出单元，即反应器及相应物料或产品输出管道。此处对上述①工艺单元进行 HAZOP 分析，见表 2-26。对关键工艺单元，由引导词进行引导，形成偏差，分析偏差可能产生的原因、可能导致的后果，进而提出安全措施建议。对于其他工艺单元，亦可采用类似方法进行分析，直至对该生产系统的所有部分都分析完毕，并对结果进行整理和记录。

试读版本仅供防疫期间线上教学使用

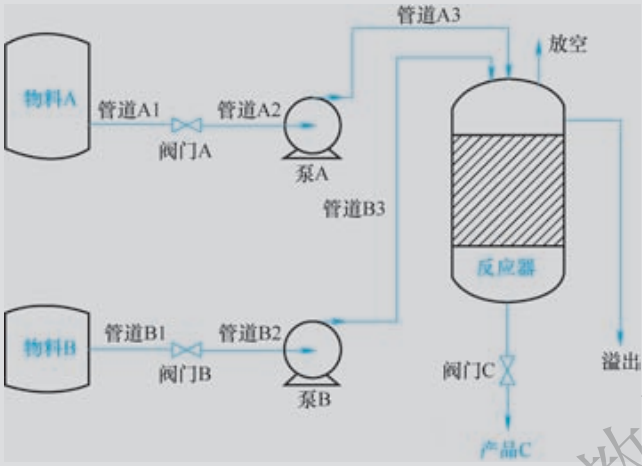

图 2-8　某工厂生产工艺简图

表 2-26　物料 A 存储输送单元的 HAZOP 分析表

引导词	要　素	偏　差	可能原因	后　果	修正措施
无 No	供料罐 A	无物料 A	A 供料罐是空的	没有 A 流入反应器；爆炸	考虑在 A 供料罐安装低液位报警器，外加一个液位低/低连锁停止泵
	阀门 A	没有输送物料 A	阀门 A 故障	没有 A 流入反应器；爆炸	① 物料 A 流量测量，外加一个低流量报警器以及当 A 低流量时联锁停泵 B ② 阀门、泵、管道日常检查和检修
	泵 A	没有输送物料 A	泵 A 停止	没有 A 流入反应器；爆炸	
	管道 A	没有输送物料 A	管路堵塞	没有 A 流入反应器；爆炸	
多 More	供料罐 A	物料 A 过量	向罐中加料超过罐容量	物料从罐 A 溢出	① 通过对罐的检测加以识别 ② 若没有预先识别，则可考虑高液位报警
	阀门 A	物料 A 流速增大	阀门 A 开度过大	输送到泵 A 的物料增加	通过对阀门的检测加以识别
	泵 A	物料 A 流速增大	叶轮尺寸选错；泵选型不对	产量可能减少；产品 C 中 A 过量	试车时检查泵的流量和特性
	管道 A	物料 A 流速增大	供料罐、阀门或泵故障导致	产量可能减少；产品 C 中 A 过量	管道 A3 加流量测速器
少 Less	供料罐 A	物料 A 更少	向罐中加料过少	产量可能减少；反应无法完成；爆炸	在供料罐 A 安装一个低液位报警器
	阀门 A	物料 A 流速降低	阀门 A 开度过小	输送到泵 A 的物料减少	通过对阀门的检测加以识别
	泵 A	物料 A 流速降低	叶轮尺寸选错；泵选型不对	产量可能减少；反应无法完成；爆炸	试车时检查泵的流量和特性

试读版本仅供防疫期间线上教学使用

（续）

引导词	要　素	偏　差	可能原因	后　果	修正措施
少 Less	管道 A	物料 A 流速降低	供料罐、阀门或泵故障；管道堵塞、泄漏	产量可能减少；反应无法完成；爆炸	管道 A3 加流量测速器
伴随 As Well As	供料罐 A	供料罐除 A 外还有其他物料	供料罐被污染	未知	① 进料前对卸入罐中的物料进行检查和分析 ② 检查操作程序
	阀门 A 泵 A 管道 A	物料 A 输送过程中在阀门、泵或管道处混入其他物质	阀门、泵、管道可能发生侵蚀、腐蚀、结晶或分解	未知	① 根据具体物料 A 物理化学特性，选用合适材质的输送器件 ② 检查操作程序
相反 Reverse	阀门 A 泵 A 管道 A	反向输送物料 A	泵故障；反应器压力高于泵出口压力	供料罐被返回的反应料污染	考虑管道 A3 安装一个止逆阀
异常 Other Than	供料罐 A	物料 A 异常	供料罐内原料错误	未知	进料前对卸入罐中的物料进行检查和分析
	阀门 A 泵 A 管道 A	物料 A 输送过程流速异常	阀门、泵故障；管道破裂	环境污染；可能爆炸	建议流量连锁跳车应有足够快的响应时间以阻止发生爆炸

【例 2-11】 考虑某个安全关键塑料元件的小批量生产过程。该元件必须严格满足材料特性和颜色的规范要求。加工顺序如下：①取 12kg 粉末 A；②放在搅拌器中；③取 3kg 着色剂粉末 B；④放在搅拌器中；⑤起动搅拌器；⑥混合 15min，停止搅拌器；⑦取出搅拌的混合物，分成 3 包（每包 5kg）；⑧清洗搅拌器；⑨向混合容器中加入 50L 树脂；⑩向混合容器中加入 0.5kg 硬化剂；⑪加入 5kg 混合粉末（A 和 B）；⑫搅拌 1min；⑬在 5min 内把混合物倒入模具。

HAZOP 分析的目的是检查哪些步骤有可能造成产品不符合规范要求。作为程序化的顺序，HAZOP 分析的部分是相关的连续指令。对这一顺序的 HAZOP 分析的部分内容示例见表 2-27，本示例采用了“问题记录”报告形式。

表 2-27　程序的 HAZOP 工作表示例

分析题目：程序								表页：	
程序题目：某元件的小规模生产			修订号：					日期：	
小组成员：								会议日期：	
分析部分：					指令：取 12kg 粉末 A				
序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
1	取粉末 A	无 No	没有取 A	操作失误	最终产品不合格	操作人员会注意到搅拌机中颗粒太小，颜色可能太亮	完全无物料 A 被认为是不可信的	无	

试读版本仅供预览期间线上教学使用

（续）

序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
2	取粉末A	伴随As Well As	有其他原料和A一起添加	原料A被杂质污染	颜色不合格，最终混合物不合格	使用前对所有交付的样品A进行检验		检查生产商的质量保证程序	
3	取粉末A	异常Other Than	取用了除A之外的物料	操作人员取用了错误的物料	混合物不可用；导致财产损失	仅把装有A和B的袋子放在操作区		每周检查物料保存是否规范；考虑对每种原料与混合产品使用不同颜色的包装袋	
4	取12kg粉末A	多More	取了过量的A	称重错误/操作人员失误	产品颜色不合格	每周检查一次称重；每6个月保养一次称重设备		对操作人员强调精确称重的重要性	
5	取12kg粉末A	少Less	取了过少的A	称重错误/操作人员失误	产品颜色不合格	每周检查一次称重；每6个月保养一次称重设备		对操作人员强调精确称重的重要性	
6	搅拌器	异常Other Than	原料A没有正确地放入搅拌器内，而是放在了其他地方	操作人员失误		操作现场只有一台搅拌器		如果需要安装其他搅拌器，那么要对安装位置进行审查	
7	加硬化剂	无No	未加入硬化剂	操作人员失误	最终混合物不合格；财产损失	操作人员必须签署一系列表格以确保硬化剂已经加入；最后还要对浇筑强度进行检测		审查操作人员失误概率，看是否还需要其他安全措施	
8	加硬化剂	伴随As Well As	其他物料同硬化剂一起加入	硬化剂被污染	最终混合物不可用	厂商提供的质量保证书；对所有样品进行检测		无	
9	加硬化剂	异常Other Than	加入的不是硬化剂而是其他物质		最终混合物不可用	不同硬化剂的物理隔离；操作人员检查	硬化剂提前称好并装袋；错误的概率会大大降低	等待硬化结果；采购询问和审查	

试读版本仅供防疫期间线上教学使用

（续）

序号	要素	引导词	偏差	可能原因	后果	安全措施	注释	建议安全措施	执行人
10	取0.5kg硬化剂	多 More	加入了过多的硬化剂	称重错误/操作人员失误	产品组件过脆；可能导致灾难性后果	每周检查一次称重；每6个月保养一次称重设备	安全措施不够	调查获得0.5kg预先称好的袋装催化剂的可能性；对每一交付样品进行检查	
11	取0.5kg硬化剂	少 Less	加入了过少的硬化剂	称重错误/操作人员失误	产品组件过脆；可能导致灾难性后果	每周检查一次称重；每6个月保养一次称重设备	安全措施不够	调查获得0.5kg预先称好的袋装催化剂的可能性；对每一交付样品进行检查	

2.4.4 适用范围

HAZOP法是一个能发现新的危险性的定性评价方法，特别适用于尚无经验的新技术开发，能辨识静态和动态生产过程中的危险性。所以危险与可操作性研究既适用于设计阶段，又适用于现有的生产装置。对现有生产装置进行分析时，如能吸收有操作经验和管理经验的人员共同参加，会收到很好的效果。

化工生产既有连续过程，又有间歇过程，原化工部劳动保护研究所在进行“光气及光气化产品企业安全评价”课题研究中对间歇过程中应用可操作性研究方法进行了研究，结果表明，在进行若干改进以后，可操作性研究也能很好地应用于间歇过程的危险性分析。在间歇过程中，分析的对象将不再是管道，而应该是主体设备，如反应器等。根据间歇生产的特点，分成3个阶段（即进料、反应、出料）对反应器加以分析。同时，在这3个阶段内不仅要按照关键词来确定工艺状态及参数可能产生的偏差，还要考虑操作顺序等项因素可能出现的偏差。这样就可对间歇过程进行全面、系统的考察。

尽管HAZOP分析方法在多个领域被证明是十分有效的，在实际应用中也不能忽略HAZOP本身的局限性：首先，HAZOP独立地考虑系统中的部分及每个部分中工艺偏差的影响，无法有效解决工艺系统之间的问题，这时应考虑采用事件树或事故树等更为详细的分析方法。其次，对于复杂系统，HAZOP不能完全识别出系统所有的危险和操作性问题，同时由于HAZOP分析是一种定性的分析方法，不能衡量系统失效后果的严重程度和可能性大小，因此，不能完全依赖于HAZOP分析，应联合其他方法对系统进行综合评价。此外，HAZOP分析的效果依赖于HAZOP组长能力及参会人员的经验，这对HAZOP分析会议的开展提出了较高的要求。

2.5 鱼刺图法

2.5.1 基本概念

鱼刺图又称因果分析图、因果图、特性图或树枝图等。该法在1953年首次应用于日本，后来介绍到其他国家，把它移植到安全分析方面，成为一种重要的事故分析方法。

试读版不允许供读期间线上教学使用

用这种方法分析事故，可以使复杂的原因系统化、条理化，把主要原因搞清楚，也就明确了预防对策。因其所绘制的分析图形像一条完整的鱼，有骨有刺，故名鱼刺图。

2.5.2　绘制方法

鱼刺图由原因和结果两部分构成。一般情况下，可从人的不安全行为（安全管理者、设计者、操作者等）和物质条件构成的不安全状态（设备缺陷、环境不良等）两大因素中，从大到小，从粗到细，由表及里，一层一层深入分析，则可得到如图2-9所示的鱼刺图。

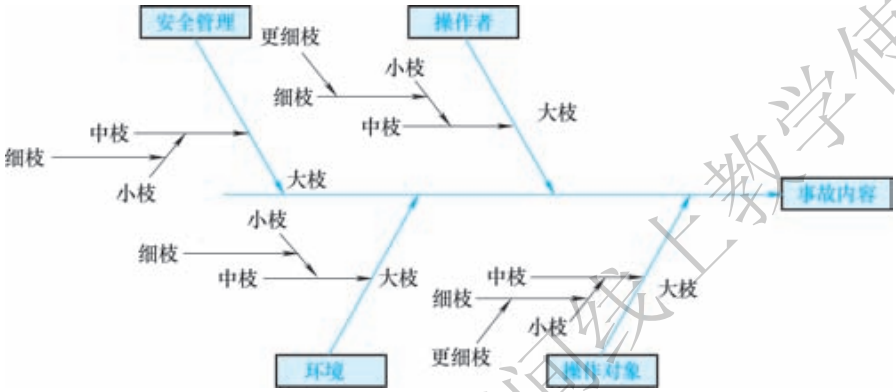

图2-9　鱼刺图结构

在绘制图形时，一般可按下列步骤进行：

（1）确定要分析的某个特定问题或事故，写在图的右边，画出主干，箭头指向右端。

（2）确定造成事故的因素分类项目，如安全管理、操作者、材料、方法、环境等并画大枝。

（3）将上述项目深入发展，中枝表示对应的项目造成事故的原因，一个原因画出一枝，文字记在中枝线的上下。

（4）将上述原因层层展开，一直到不能再分为止。

（5）确定鱼刺图中的主要原因，并标上符号，作为重点控制对象。

（6）注明鱼刺图的名称。

上述步骤可归纳为：针对结果，分析原因；先主后次，层层深入。

2.5.3　实用实例

【例2-12】 矿山事故的危险源存在于生产过程的各个环节，人与机的交界面是事故多发的场所，危险物的质量和能量的积聚是构成重大恶性事故的物质根源。这就需要应用系统工程的理论和方法，去分析、识别和评价生产系统中的危险性，根据其结果调整生产工艺、生产设备、操作规程、生产周期和投资等因素，使系统可能发生的事故得到控制，并使系统的安全性达到最佳状态。人的不安全行为和矿山机械是人—机关系中能量逆流的两大系列，其轨迹交叉点就构成事故。在人为因素系列中，不安全行为是基于生理、心理、动作几个方面而产生的；在机械因素系列中，从设计开始，经过制造的各种加工程序直至使用的整个过程，各个阶段都可能产生不安全状态。

对井下开采生产工艺事故、潜在的危险事故及生产爆炸事故分析如图2-10、图2-11、图2-12所示。

试读版本仅供预览期间线上教学使用

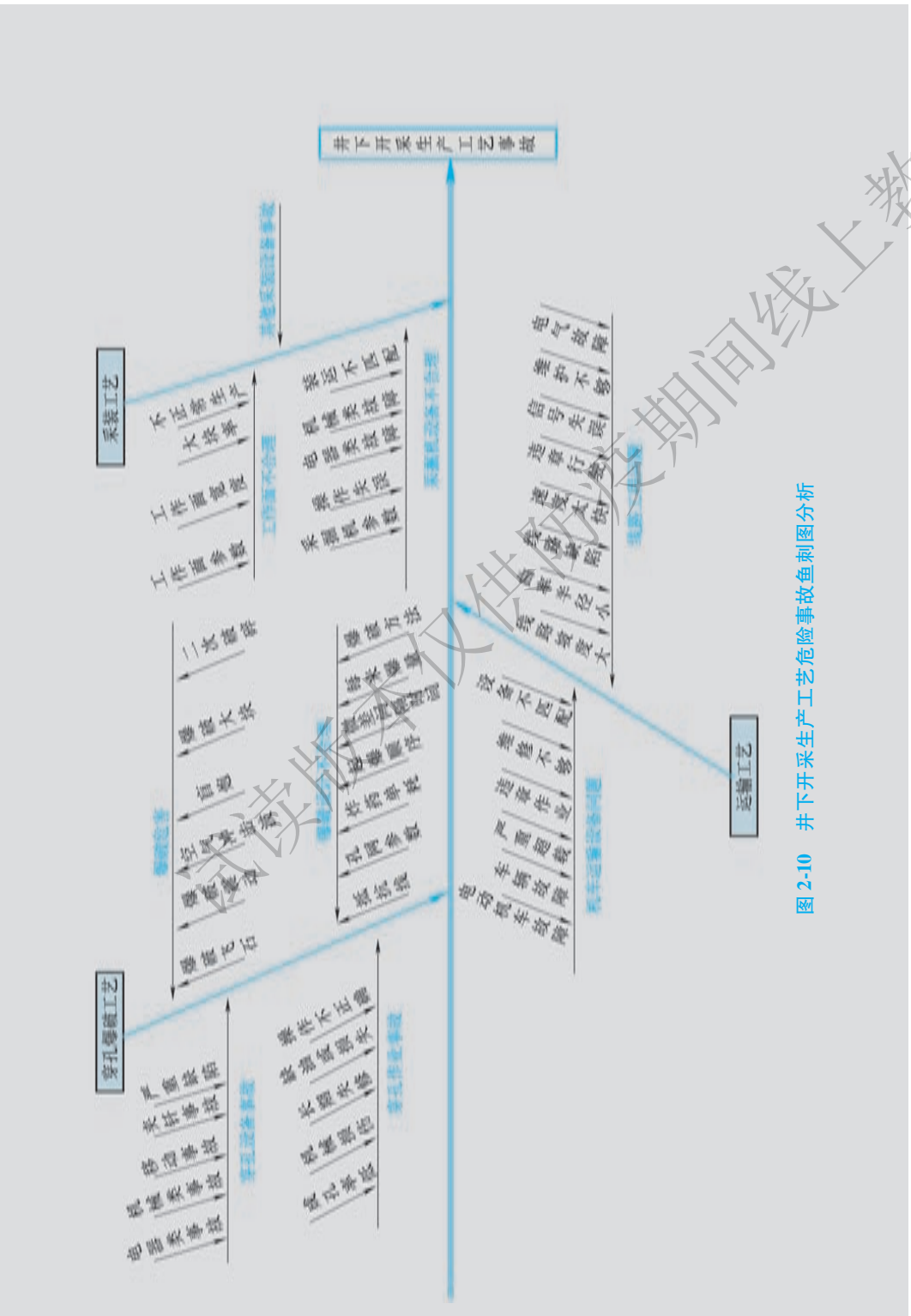

图 2-10 井下开采生产工艺危险事故鱼刺图分析

试读版本仅供试读期间线上教学使用

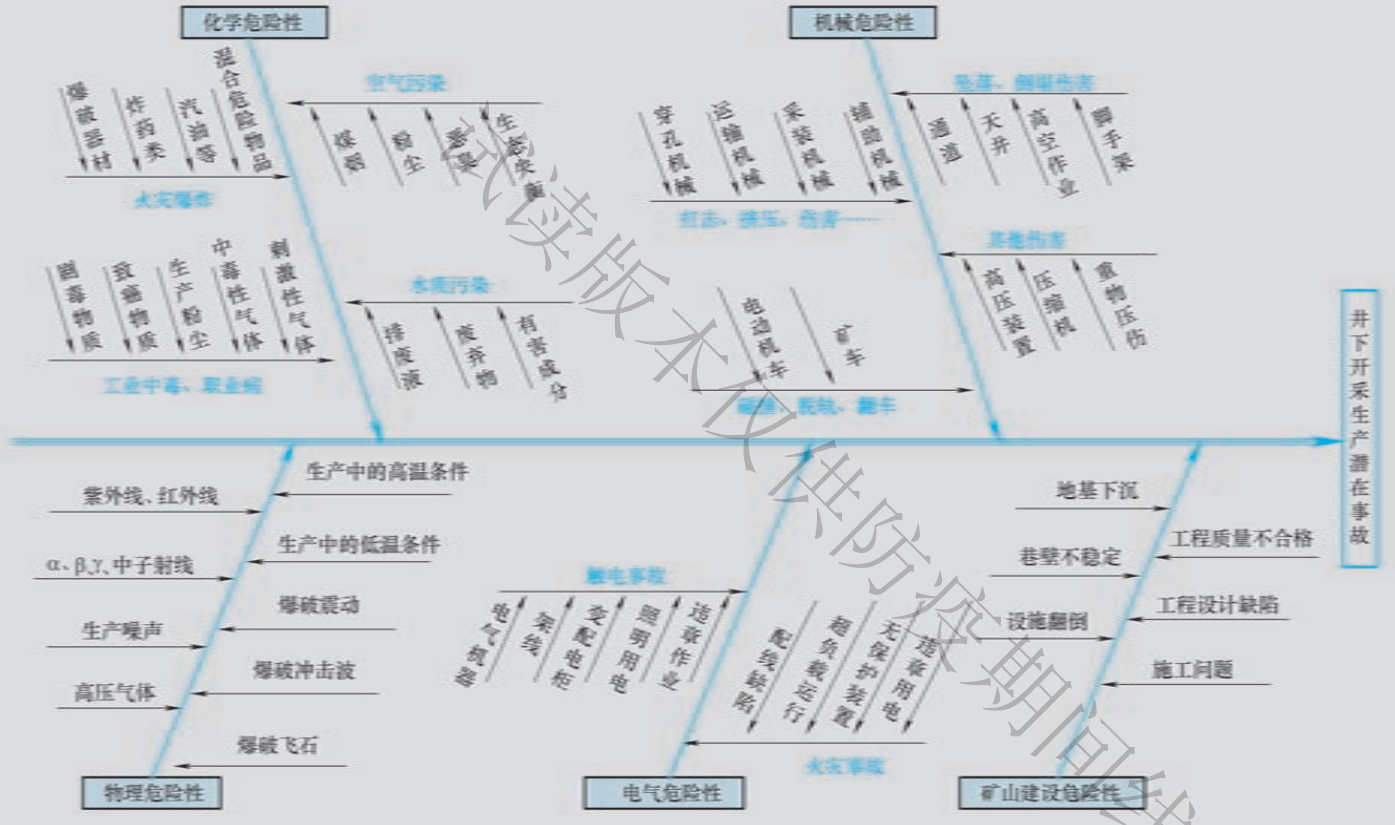

图 2-11　井下开采生产潜在危险事故鱼刺图分析

试读版本仅供防疫期间线上教学使用

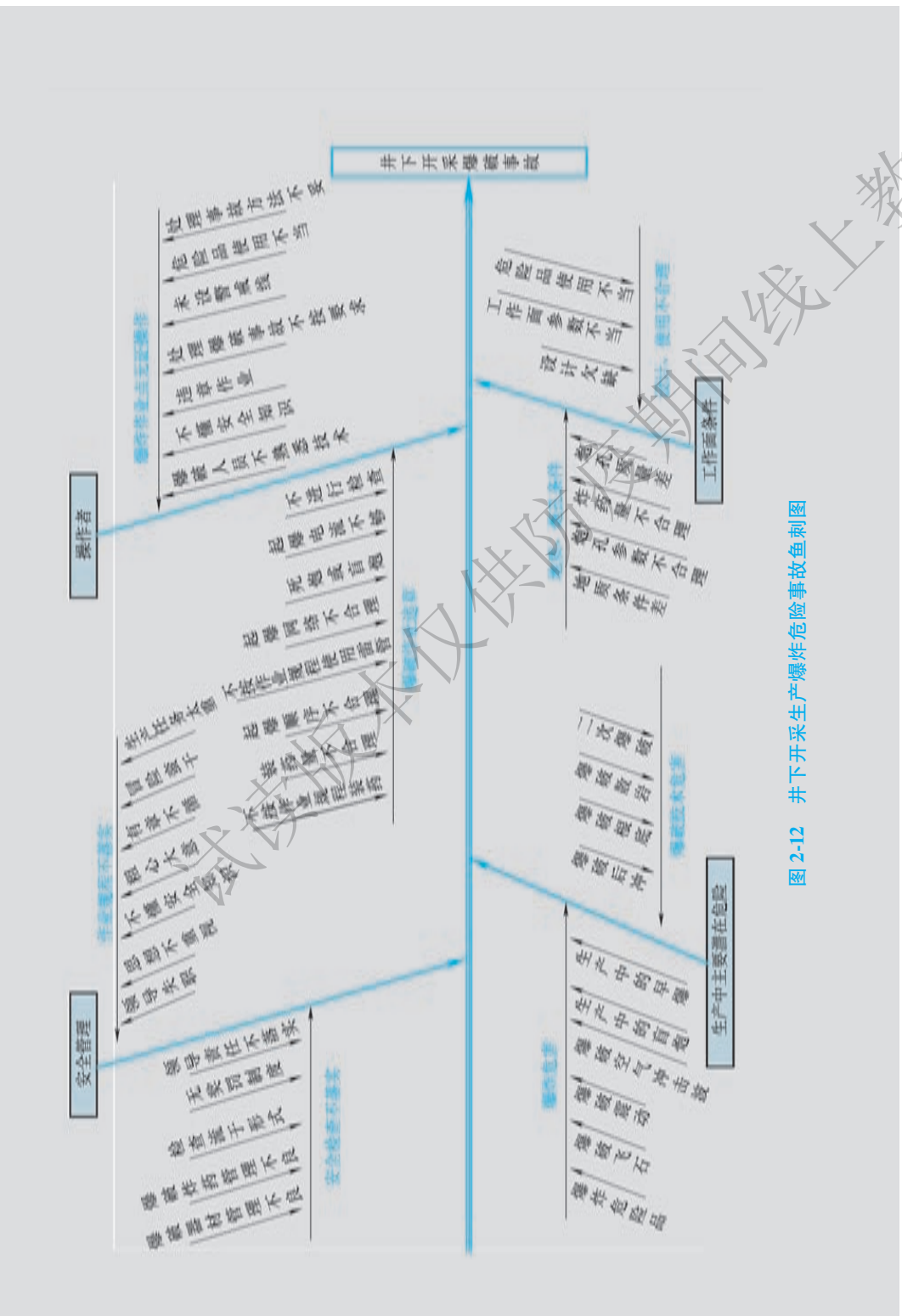

图 2-12 井下开采生产爆炸危险事故鱼刺图

试读版本仅供防疫期间线上教学使用

2.6 作业危害分析

作业危害分析又称作业安全分析（Job Hazard Analysis，简记为JHA）、作业危害分解（Job Hazard Breakdown，JHB），是一种定性风险分析方法。实施作业危害分析，能够识别作业中潜在的危害，确定相应的工程措施，提供适当的个体防护装置，以防止事故发生，防止人员受到伤害。适用于涉及手工操作的各种作业。一项调查表明，在实际工作中它是一种广为采用的方法。许多石油和天然气企业采用了这一方法。

美国职业健康安全管理局（OSHA）于1998年、2002年先后出版了专门介绍作业危害分析的手册，并两次进行了修订。OSHA的一些规范都重视这种分析方法。加拿大职业安全健康中心曾对这种方法做了较为详细的阐述。

2.6.1 含义及作用

作业危害分析将作业活动划分为若干步骤，对每一步骤进行分析，从而辨识潜在的危害并制定安全措施。作业危害分析是有助于将认可的职业安全健康原则在特定作业中贯彻实施的一种方法。这种方法的基点是职业安全健康是任何作业活动的一个有机组成部分，而不能单独剥离出来。

所谓的“作业”（有时也称“任务”）是指特定的工作安排，如“操作研磨机”“使用高压水灭火器”等。“作业”的概念不宜过于笼统，如“大修机器”，也不宜过细。

这种方法的优点是由许多有经验的人员参加危害分析，其结果可以确定更为理想的操作程序。开展作业危害分析能够辨识原来未知的危害，增加职业安全健康方面的知识，促进操作人员与管理者之间的信息交流，有助于制定出更为合理的安全操作规程。它还能用来对新的作业人员进行培训，为不经常进行的作业提供指导。作业危害分析的结果可以作为职业安全健康检查的标准，并协助进行事故调查。

2.6.2 分析过程

（1）“作业”的选择。理想情况下，所有的作业都要进行作业危害分析，但首先要确保对关键性的作业实施分析。

确定分析作业时，优先考虑如下作业活动：

1）频度和后果。频繁发生或不经常发生但可致灾难性后果的。

2）严重的职业伤害或职业病。事故后果严重、危险的作业条件或经常暴露在有害物质中。

3）新增加的作业。由于经验缺乏，明显存在危害或危害难以预料。

4）变更的作业。可能会由于作业程序的变化而带来新的危险。

5）不经常进行的作业。由于对从事的作业不熟悉而有较高的风险。

（2）将作业划分为若干步骤。选择作业活动之后，要将作业活动划分为若干步骤。每一个步骤都应是作业活动的一部分操作。

步骤划分得不能太笼统，否则分析时将会遗漏一些步骤以及与之相关的危害。另外，步骤划分也不宜太细，以避免出现太多的步骤。根据经验，一项作业活动的步骤一般不超过

试读版本仅供预览，非教学使用

10 项。如果作业活动划分的步骤实在太多，可先将该作业活动分为两个部分，分别进行危害分析。重要的是要保持各个步骤正确的顺序，顺序改变后的步骤在危害分析时有些潜在的危害可能不会发现，也可能增加一些实际并不存在的危害。按照顺序在表中记录每一步骤，说明它是什么而不是怎样做。

划分作业步骤之前，应观察操作人员的操作过程。观察人通常是操作人员的直接管理者，但较为透彻的分析常需要另外的人，职业安全健康委员会的成员是合适的人选，关键是要熟悉这种方法。被观察的操作人员应具有工作经验并熟悉整个作业，非常需要操作人员的充分合作和参与，因为他们的经验是至关重要的。

还应当在正常的工作时间和工作状态下观察作业活动，如一项作业活动是在夜间进行的，那么就应在夜间进行观察。

（3）辨识危害。根据对作业活动的观察、掌握的事故（伤害）的资料以及经验，依照危害辨识清单依次对每一步骤进行危害的辨识，辨识的危害列入表中。

为了辨识危害，还需要对作业活动作进一步的观察和分析。另外，在辨识危害阶段不必试图去解决发现的问题。

辨识危害应该思考的问题是：可能发生的故障或错误是什么？其后果如何？事故是怎样发生的？其他的影响因素有哪些？发生的可能性？以下是危害辨识清单的部分内容：

1）是否穿戴个体防护服或配备个体防护器具？

2）操作环境、设备、地槽、坑以及危险的操作是否得到有效的防护？

3）维修设备时，是否对惰性化处理的设备采取了隔离？

4）是否有能引起伤害的固定物体，如锋利的设备边缘？

5）操作者能否触及机器部件或夹在机器部件之间？

6）操作者能否受到运动的机器部件或移动物品的伤害？

7）操作者是否会处于失去平衡的状态？

8）操作者是否管理着带有潜在危险的装置？

9）操作者是否需要从事可能使头、脚受伤或被扭伤的活动（往复运动的危害）？

10）操作者是否会被物体冲撞或撞击到机器或物体？

11）操作者是否会跌倒？

12）操作者是否会由于提升、拖拉物体或运送笨重物品而受到伤害？

13）作业环境是否存在危害因素——粉尘、化学物质、放射线、电焊弧光、热、高噪声？

（4）确定相应的对策。危害辨识以后，需要制定消除或控制危害的对策。确定对策时，从工程控制、管理措施和个体防护三个方面加以考虑：

1）消除危害。消除危害是最有效的措施，有关这方面的技术包括：改变工艺路线、修改现行工艺、以危害较小的物质替代、改善环境（通风）、完善或改换设备及工具。

2）控制危害。当危害不能消除时，采取隔离、机器防护、工作鞋等措施控制危害。

3）修改作业程序。完善危险操作步骤的操作规程、改变操作步骤的顺序以及增加一些操作程序（如锁定能源的措施）。

4）减少暴露。这是在没有其他解决办法时的一种选择。减少暴露的一种办法是减少在危害环境中暴露的时间，如完善设备以减少维修时间、配备合适的个体防护器材等。为了降低事故的影响程度，设置一些应急设备（如洗眼器等）。确定的对策要填入表中。对策的描述应具

试读版本仅供阅读期间线上教学使用

体，说明应采取何种做法以及怎样做，避免过于原则的描述，如“小心”“仔细操作”等。

（5）信息传递。作业危害分析是消除和控制危害的一种行之有效的方法，因此，应当将作业危害分析的结果传递给所有从事该作业的人员。

2.6.3　应用举例

【例 2-13】　作业活动为：从储罐顶部人孔进入，清理化学物质储罐的内表面。运用作业危害分析方法，将该作业活动划分为9个步骤并逐一进行分析，分析结果列于表2-28。

表 2-28　作业危害分析表

步　骤	危害辨识	对　策
① 确定罐内的物质种类，确定在罐内的作业及存在的危险	▲爆炸性气体 ▲氧含量不足 ▲化学物质暴露的气体、粉尘、蒸气（刺激性、毒性）、液体（刺激性、毒性、腐蚀、过热） ▲运动的部件/设备	▲根据标准制定有限空间进入规程 ▲取得有安全、维修和维护人员签字的作业许可证 ▲具备资格的人员对气体检测 ▲通风至氧含量为19.5%～21.5%，并且任一可燃气体的含量低于其爆炸下限的10% ▲提供合适的呼吸器材 ▲提供保护头、眼、身体和脚的防护服 ▲参照有关规范提供安全带和救生索，如果有可能，清理罐体外部
② 选择和培养操作者	▲操作人员呼吸系统或心脏有疾患，或有其他身体缺陷 ▲操作人员的操作失误	▲卫生医师检查，能适应于该工作，培训操作人员 ▲按照有关规范，对作业进行预演
③ 设置检修用设备	▲软管、绳索、器具脱落的危险 ▲电气设施中电压过高、导线裸露 ▲电动机未锁定并未做出标记	▲按照位置，顺序地设置软管、绳索、管线及器材以确保安全 ▲设置接地故障断路器 ▲如果有搅拌电动机，加以锁定做出标记
④ 在罐内安放梯子	▲梯子滑倒	▲将梯子牢固地固定在孔顶部或其他固定部件上
⑤ 准备入罐	▲罐内有气体或液体	▲通过现有的管道清空储罐 ▲审查应急预案 ▲打开罐 ▲工业卫生专家或安全专家检查现场 ▲罐体接管法兰处设置盲板（隔离） ▲具备资格的人员检测罐内气体（经常检测）
⑥ 罐入口处安放设备	▲脱落或倒下	▲使用机械操作设备 ▲罐顶作业处设置防护栏
⑦ 入罐	▲从梯子上滑脱 ▲暴露于危险的作业环境中	▲按有关标准，配备个体防护器具 ▲外部监护人员观察、指导入罐作业人员，在紧急情况下能将作业人员自罐内营救出来

试读版本仅供防疫期间线上教学使用

（续）

步　骤	危害辨识	对　策
⑧ 清洗储罐	▲发生化学反应，生成烟雾或散发空气污染物	▲为所有操作人员和监护人员提供防护服及器具 ▲提供罐内照明 ▲提供排气设备 ▲向罐内补充空气 ▲随时检测罐内空气 ▲轮换操作人员或保证一定时间的休息 ▲如果需要，提供通信工具以便于得到帮助 ▲提供2人作为后备救援，以应付紧急情况
⑨ 清理	▲使用工具而引起伤害	▲预先演习 ▲使用运料设备

复　习　题

1. 安全检查表的优点有哪些？其适用范围如何？

2. 使用预先危险分析法应注意哪些问题？预先危险分析一般以表格形式列出，请编制PHA的典型格式表。

3. 什么是故障类型与影响分析？试采用“乘积评点法”对起重机防止过卷装置和钢丝绳两组系统进行FMECA分析。

4. HAZOP分析的适用条件如何？试用HAZOP法对图2-8的反应器及产品输出单元进行分析。

5. 在JHA分析中，通常把正常的工作分解为若干步骤，对每一步骤的危害进行辨识，本章列出了辨识清单的部分内容，在此基础上，你是否有新的分类方法对辨识内容进行归类？

6. 某废气洗涤系统如图2-13所示，废气中主要危险有害气体包括：HCl气体、CO气体。洗涤流程如下：为了稀释废气中CO气体和HCl气体的浓度，在洗涤废气之前先向废气中通入一定量的N_2气体，然后再进行洗涤。首先NaOH溶液反应器，会吸收混合气中的HCl气体，HCl气体处理完，会进入第二个CO处理的氧化反应器，在这里会供应氧气进来，跟CO起反应燃烧，然后产生CO_2排放到大气。

（1）简要说明以下安全评价方法：安全检查表法、预先危险性分析、故障类型及影响分析、危险和可操作性研究及故障树分析方法各自主要适用的评价对象。

（2）从以上评价方法中选出一种最适用本例的方法对该系统中氮气流量危险有害因素进行分析。

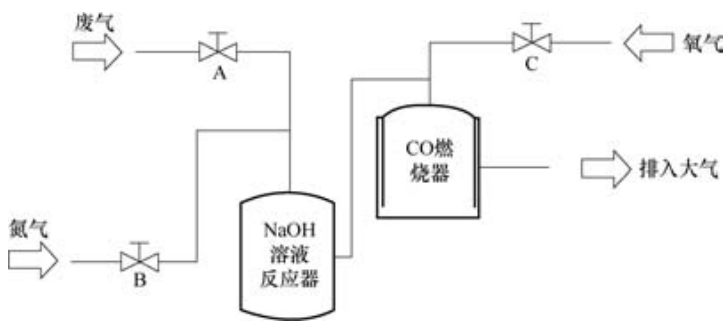

图2-13　某废气洗涤系统

试读版本仅供防疫期间线上教学使用

第3章 系统安全定量分析

本章学习目标：

了解事件树分析和事故树分析的基本原理，掌握事件树编制并学会运用其进行系统定性和定量分析，重点掌握事故树的编制及其运用，包括：最小径集、最小割集、结构重要度的计算和分析，顶上事件发生概率的计算和分析。

本章学习方法：

可参考有关布尔代数、概率论的书籍，首先掌握事故树符号及其运算相关的基本概念；在分析、理解事件树和事故树分析原理的基础上，明确事件树和事故树的编制原理和计算原理，并注重理论联系实际，具有运用以上方法开展系统安全分析的实践能力。

试读版本仅供防疫期间线上教学使用

3.1 事件树分析

事件树分析（Event Tree Analysis，简称 ETA）是安全系统工程中重要的分析方法之一。它建立在概率论和运筹学的基础之上。在运筹学中，它用于对不确定的问题做决策，故又称为决策分析法（Decision Tree Analysis，简称 DTA）。虽然在不同的地方应用时名称不同，但方法是一样的。

3.1.1 事件树分析的含义、目的及特点

事件树分析法是事故分析的技术方法之一。它的实质是利用逻辑思维的规律和形式，从宏观的角度去分析事故形成的过程。

事件树分析法从事件的起始状态出发，用逻辑推理的方法，设想事故发展过程；进而根据这一过程了解事故发生的原因和条件。

事件树是判断树在灾害分析上的应用。判断树（Decision Tree）是以元素的可靠性系数表示系统可靠程度的系统分析方法之一，是一种既能定性，又能定量分析的方法。

事件树分析的目的：

（1）判断事故发生与否，以便采取直观的安全措施。

（2）指出消除事故的根本措施，改进系统的安全状况。

（3）从宏观角度分析系统可能发生的事故，掌握事故发生的规律。

（4）找出最严重的事故后果，为确定顶上事件提供依据。

事件树分析的主要特点如下：

（1）用于对已发生事故的分析，也可用于对未发生事故的预测。

（2）在对事故分析和预测时，事件树分析法比较明确，寻求事故对策时比较直观。

（3）事件树分析可用于管理上对重大问题的决策。

（4）搞清楚初期事件到事故的过程，系统地图示出种种故障与系统成功、失败的关系。

（5）对复杂的问题，可以用此方法进行简捷推理和归纳。

（6）提供定义故障树顶上事件的手段。

事件树分析技术基于如下定义：

（1）事故场景（Accident Scenario）：最终导致事故的一系列事件。这些事件的后果是从一个初始事件开始，随后按照时空序列开展的中枢事件，最终导致不期望的状态出现。

（2）初始事件（Initiating Event）：触发事故序列开始的故障或不期望事件。初始事件是否导致事故，依赖于系统中安全控制措施是否成功运行。

（3）环节事件（Pivotal Event）：介于初始事件和最终事故之间的中间事件。环节事件是系统中安全措施的成功或者失败事件。

（4）事件树（Event Tree）：将某一初始事件可能导致的事故场景和产生的多个后果加以图形化的模型。

（5）事件树分析（Event Tree Analysis）：通过建立事件树，利用逻辑思维的规律和形式，分析事故的起因、发展和结果的过程。

3.1.2 事件树分析的基本原理

事件树是一种从原因到结果的过程分析。其基本原理是：任何事物从初始原因到最终结果所经历的每一个中间环节都有成功（或正常）或失败（或失效）两种可能或分支。如果将成功记为1，并作为上分支，将失败记为0，作为下分支；然后再分别从这两个状态开始，仍按成功（记为1）或失败（记为0）两种可能分析；这样一直分析下去，直到最后结果为止，最后即形成一个水平放置的树状图。

从事故的发生过程看，任何事故的瞬间发生都是由于在事物的一系列发展变化环节中接二连三“失败”所致。因此，利用事件树原理对事故的发展过程进行分析，不但可以掌握事故过程规律，还可以辨识导致事故的危险源。

事件树分析是利用逻辑思维的规律和形式，分析事故的起因、发展和结果的整个过程。利用事件树，分析事故的发生过程，是以“人、机、物、环境”综合系统为对象，分析各环节事件成功与失败两种情况，从而预测系统可能出现的各种结果。

3.1.3 事件树分析的步骤

事件树分析通常包括四步：确定初始事件、找出与初始事件有关的环节事件、画事件树、说明分析结果。

（1）确定初始事件。初始事件是事件树中在一定条件下造成事故后果的最初原因事件。它可以是系统故障、设备失效、人员误操作或工艺过程异常等。一般情况下分析人员选择最

试读结束，需要全本PDF请访问 防发期网络上学使用

感兴趣的异常事件作为初始事件。

（2）找出与初始事件有关的环节事件。环节事件可看作对初始事件依次做出响应的安全功能事件，即可成为防止初始事件造成不期望后果的预防措施。

（3）画事件树。把初始事件写在最左边，各种环节事件按顺序写在右面；从初始事件画一条水平线到第一个环节事件，在水平线末端画一垂直线段，垂直线段上端表示成功，下端表示失败；再从垂直线两端分别向右画水平线到下个环节事件，同样用垂直线段表示成功和失败两种状态；依次类推，直到最后一个环节事件为止。如果某一个环节事件不需要往下分析，则水平线延伸下去，不发生分支，如此便得到事件树。

（4）说明分析结果。在事件树最后面写明由初始事件引起的各种事故结果或后果。为清楚起见，对事件树的初始时间和各环节事件用不同字母加以标记。

事件树的树形结构如图 3-1 所示。

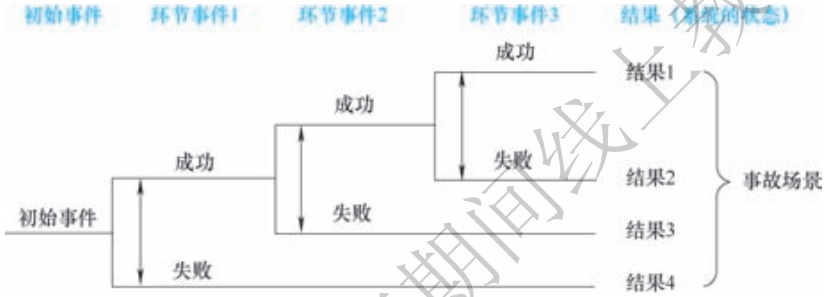

图 3-1　事件树的树形结构

在事件树分析中，大多环节事件都具有“成功”和“失败”这两个二元特征，但这并不是必须的，环节事件可以有多个分支，但各个分支必须是互斥的。如果能够获得初始事件和各环节事件的可靠度/发生概率，就可以计算系统失败的概率，从而实现定量化评估。事件树定量分析的概念如图 3-2 所示。

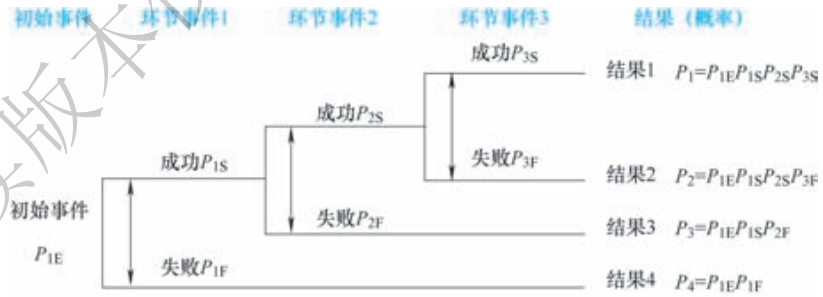

图 3-2　事件树定量分析概念图

3.1.4　事件树分析实例

【例 3-1】　对于图 3-3 的反应装置流程，取出输送原料 A 的泵与阀门系统进行事件树分析，如图 3-4、图 3-5 所示。

试读版本仅供防疫期间线上教学使用

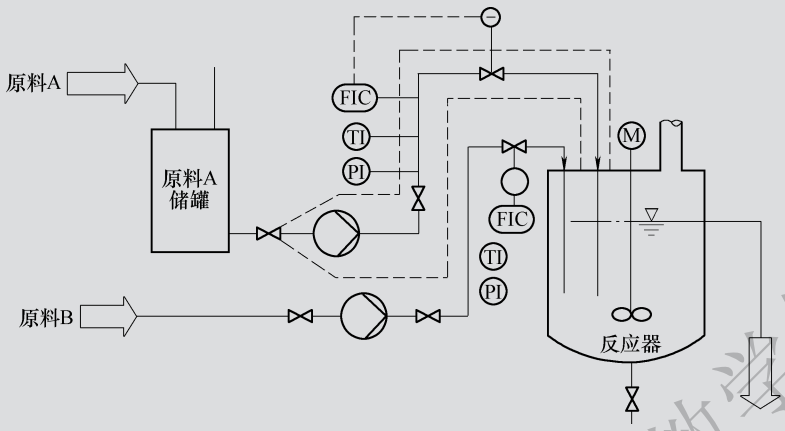

图 3-3 反应装置流程示意图

FIC—流量调节 TI—温温测量 PI—压力测量

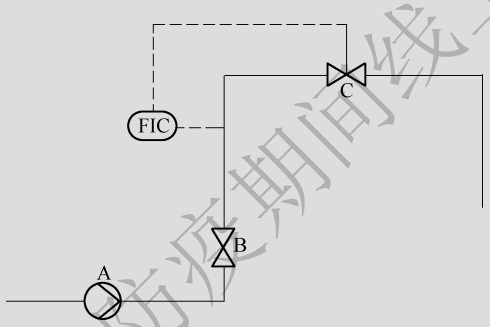

图 3-4 原料 A 输送系统示意图

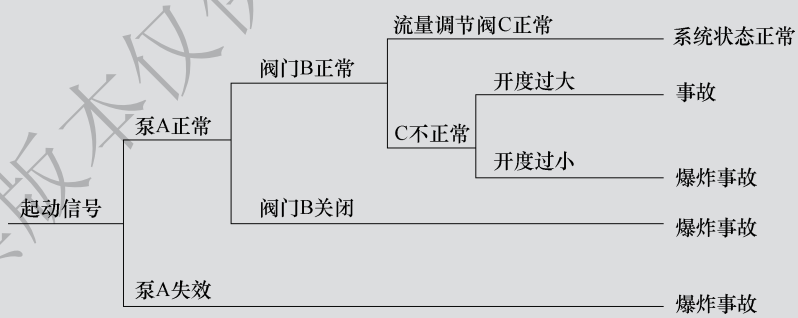

图 3-5 原料 A 输送系统事件树

由图 3-5 可以看出，导致事故的危险源有泵 A 失效、阀门 B 关闭、流量调节阀 C 不正常。

【例 3-2】 有一泵和两个串联阀门组成的物料输送系统如图 3-6 所示。物料沿箭头方向顺序经过泵 A、阀门 B 和阀门 C，泵起动后的物料输送系统的事件树如图 3-7 所示。设泵 A、阀门 B 和阀门 C 的可靠度分别为 0.95、0.9、0.9，则系统成功的概率为 0.7695，系统失败的概率为 0.2305。

试读版本仅供防疫期间线上教学使用

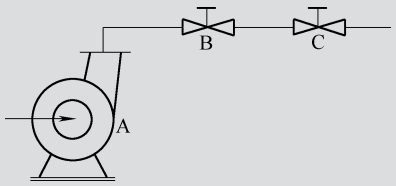

图 3-6　阀门串联的物料输送系统

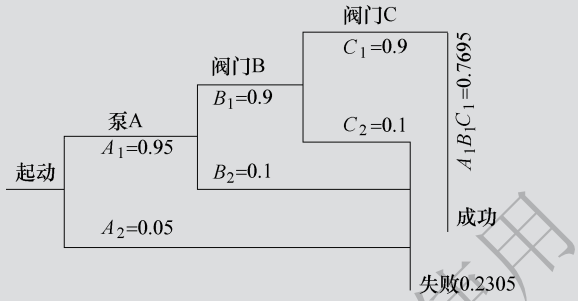

图 3-7　阀门串联输送系统事件树图

【例 3-3】　有一个泵和两个并联阀门组成的物料输送系统，如图 3-8 所示。

图 3-8 中 A 代表泵，阀门 C 是阀门 B 的备用阀，只有当阀门 B 失效时，阀门 C 才开始工作。同【例 3-2】一样，假设泵 A、阀门 B 和阀门 C 的可靠度分别为 0.95、0.9、0.9，则按照它的事件树（图 3-9），可得知这个系统成功的概率为 0.9405，系统失效的概率为 0.0595。从以上两例可以看出，阀门并联物料系统的可靠度比阀门串联时要大得多。

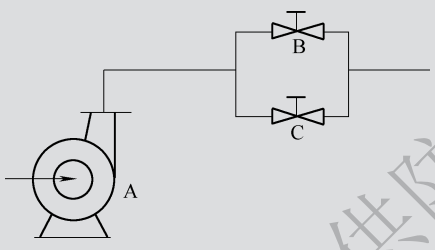

图 3-8　阀门并联的物料输送系统

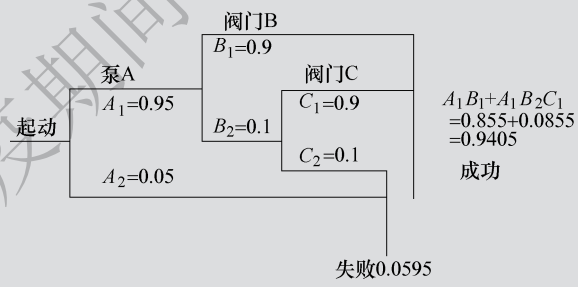

图 3-9　阀门并联输送系统事件树图

【例 3-4】　某工厂有 4 台氯磺酸储罐，在检修失灵的紧急切断阀的过程中氯磺酸罐发生爆炸，致使 3 人死亡，用事件树分析的结果如图 3-10 所示。检修失灵的紧急切断阀的一般程序如下：

（1）反应罐内的氯磺酸移至其他罐。

（2）将水徐徐注入，使残留的浆状氯磺酸分解。

（3）氯磺酸全部分解且烟雾消失以后，往罐内注水至满罐为止。

（4）静置一段时间后，将水排出。

（5）打开人孔盖，进入罐内检修。

可是在这次检修时，负责人为了争取时间，在上述第（3）项任务未完成的情况下，连水也没排净就命令维修工人去开人孔盖。由于人孔盖螺栓锈死，两名检修工用气割切断螺栓时，突然发生爆炸，负责人（安全科长）和两名检修工当场死亡。

从分析这次事故的事件树图可以看出，紧急阀失灵会引起事故，对其进行修理时，会发生如图 3-10 所示的 16 种不同的情况，这次爆炸事故属于图 3-10 中的第 12 种情况。

试读版本仅供防疫期间线上教学使用

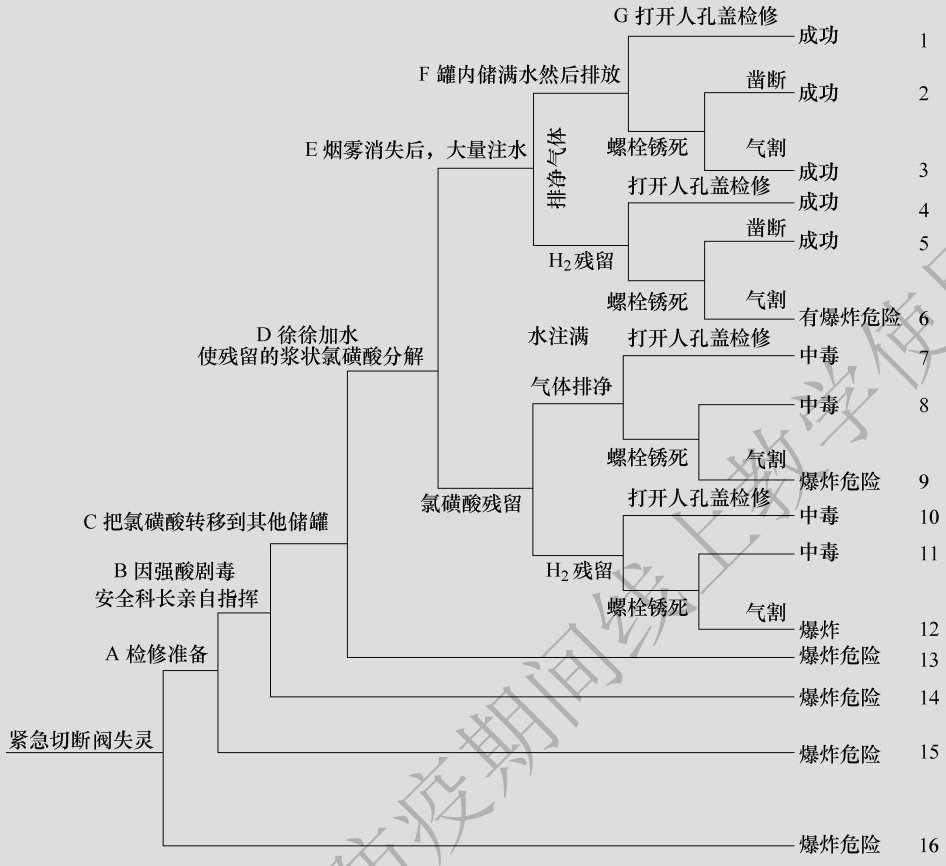

图 3-10　氯磺酸储罐爆炸事故事件树图

【例 3-5】　一斜井提升系统，为防止跑车事故，在矿车下端安装了阻车叉，在斜井里安装了人工起动的捞车器。当提升钢丝绳或连接装置断裂时，阻车叉插入轨道枕木下阻止矿车下滑。当阻车叉失效时，人员起动捞车器拦住矿车。设钢丝绳断裂概率为 10^{-4}，连接装置断裂概率为 10^{-6}，阻车叉失效概率为 10^{-3}，捞车器失效概率为 10^{-3}，人员操作捞车器失误概率为 10^{-2}。画出因钢丝绳（或连接装置）断裂引起跑车事故的事件树，计算跑车事故发生概率。

（1）编制跑车事故事件树如图 3-11 所示。

（2）由编制的斜井矿车提升事件树可知，系统状态为“跑车事故”的有④、⑤、⑧、⑨，它们的概率分别为：

$$P_4 = P(\mathrm{A}) \times P(\overline{\mathrm{B}}) \times P(\overline{\mathrm{C}}) \times P(\mathrm{D}) \times P(\overline{\mathrm{E}}) = (1-10^{-4}) \times 10^{-6} \times 10^{-3} \times (1-10^{-2}) \times 10^{-3}$$
$$= 9.899 \times 10^{-13}$$

$$P_5 = P(\mathrm{A}) \times P(\overline{\mathrm{B}}) \times P(\overline{\mathrm{C}}) \times P(\overline{\mathrm{D}}) = (1-10^{-4}) \times 10^{-6} \times 10^{-3} \times 10^{-2} = 9.999 \times 10^{-12}$$

$$P_8 = P(\overline{\mathrm{A}}) \times P(\overline{\mathrm{C}}) \times P(\mathrm{D}) \times P(\overline{\mathrm{E}}) = 10^{-4} \times 10^{-3} \times (1-10^{-2}) \times 10^{-3} = 9.9 \times 10^{-11}$$

$$P_9 = P(\overline{\mathrm{A}}) \times P(\overline{\mathrm{C}}) \times P(\overline{\mathrm{D}}) = 10^{-4} \times 10^{-3} \times 10^{-2} = 10^{-9}$$

试读版本仅供防疫期间线上教学使用

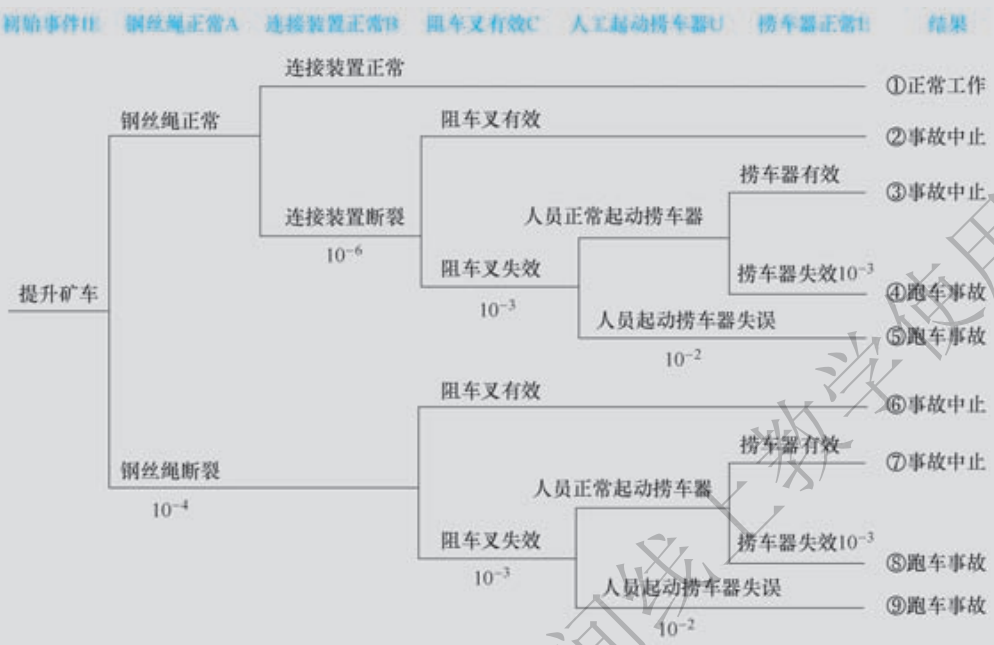

图 3-11　斜井提升矿车跑车事件树

由此可得，矿车斜井提升系统发生“跑车事故”的概率为：

$$P_{跑车} = P_4 + P_5 + P_8 + P_9 \approx 1.10998801 \times 10^{-9}$$

3.2　事故树分析

事故树就是从结果到原因描述事件发生的有向逻辑树，对这种树进行演绎分析，寻求防止结果发生的对策，这种方法就称为事故树分析法（Fault Tree Analysis，简称 FTA）。“树”的分析技术属于系统工程的图论范畴，是一个无圈（或无回路）的连通图。

从以上事故树分析的定义来看，事故树分析从结果开始，寻求结果事件（通称顶上事件）发生的原因事件，是一种逆时序的分析方法，这与事件树方法相反。另外事故树分析是一种演绎的逻辑分析法，将结果演绎成构成这一结果的多种原因，再按逻辑关系构建，寻求防止结果发生的措施。

事故树分析能对各种系统的危险性进行辨识和评价，不仅能分析出事故的直接原因，而且能深入地揭示出事故的潜在原因。用它描述事故的因果关系直观、明了，思路清晰，逻辑性强，既可定性分析，又可定量分析。现在 Matlab 等计算工具都有用于 FTA 定量分析的子程序（模块），其功能非常强大，而且使用方便。事故树分析已成为系统分析中应用最广泛的方法之一。

3.2.1　事故树分析的发展概况

事故树分析描述了事故发生和发展的动态过程，便于找出事故的直接原因和间接原因及

试读版本仅供防疫期间线上教学使用

原因的组合。可以用其对事故进行定性分析，辨明事故原因的主次及未曾考虑到的隐患；也可以进行定量分析，预测事故发生的概率。但事故树分析是数学和专业知识的密切结合，事故树的编制和分析需要坚实的数学基础和相当的专业技能。

事故树分析是一种演绎推理法，这种方法把系统可能发生的某种事故与导致事故发生的各种原因之间的逻辑关系用一种称为事故树的树形图表示，通过对事故树的定性与定量分析，找出事故发生的主要原因，为确定安全对策提供可靠依据，以达到预测与预防事故发生的目的。FTA 具有以下特点：

（1）事故树分析是一种图形演绎方法，是事故事件在一定条件下的逻辑推理方法。它可以围绕某特定的事故作层层深入的分析，因而在清晰的事故树图形下，表达系统内各事件间的内在联系，并指出单元故障与系统事故之间的逻辑关系，便于找出系统的薄弱环节。

（2）FTA 具有很大的灵活性，不仅可以分析某些单元故障对系统的影响，还可以对导致系统事故的特殊原因如人为因素、环境影响进行分析。

（3）采用 FTA 进行分析的过程，是一个对系统更深入认识的过程，它要求分析人员把握系统内各要素间的内在联系，弄清各种潜在因素对事故发生影响的途径和程度，因而许多问题在分析的过程中就被发现和解决了，从而提高了系统的安全性。

（4）利用事故树模型可以定量计算复杂系统发生事故的概率，为改善和评价系统安全性提供了定量依据。

事故树分析还存在许多不足之处，主要是：FTA 需要花费大量的人力、物力和时间；FTA 的难度较大，建树过程复杂，需要经验丰富的技术人员参加，即使这样，也难免发生遗漏和错误；FTA 只考虑（0，1）状态的事件，而大部子系统存在局部正常、局部故障的状态，因而建立数学模型作结构重要度分析时，会产生较大误差；FTA 虽然可以考虑人的因素，但人的失误很难量化。

事故树分析仍处在发展和完善中。目前，事故树分析在自动编制、多状态系统 FTA 、相依事件的 FTA、数据库的建立及 FTA 技术的实际应用等方面尚待进一步分析研究，以求新的发展和突破。

3.2.2 事故树的基本结构

事故树的基本结构如图 3-12 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 3-12 中表示的事件。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 3-12 中 X_i 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，它们既是造成顶上事件的原因，又是由基本事件产生的结果，如图 3-12 中 A_1、A_2、A_3、A_4、A_5 所表示的事件。

3.2.3 事故树的符号及其意义

事故树是由各种符号和其连接的逻辑门组成的。下面仅将常见的符号予以介绍和说明。

试读版本仅供防疫期间线上教学使用

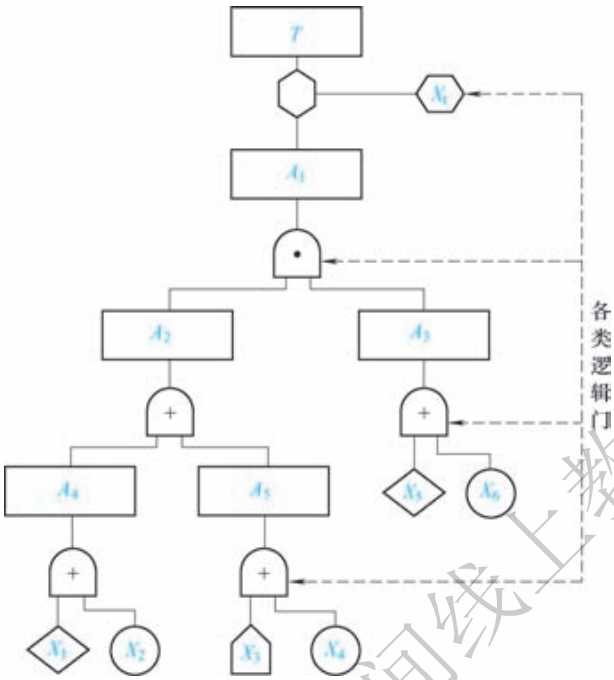

图 3-12　事故树的基本结构

1. 事件符号

（1）矩形符号。如图 3-13a 所示，用矩形符号表示顶上事件或中间事件。将事件扼要记入矩形框内。必须注意，顶上事件一定要清楚明了，不要太笼统。例如“交通事故”“爆炸着火事故”，对此人们无法下手分析，而应当选择具体事故。如“机动车追尾”“机动车与自行车相撞”“建筑工人从脚手架上坠落死亡”“道口火车与汽车相撞”等具体事故。

（2）圆形符号。如图 3-13b 所示，圆形符号表示基本事件，可以是人的差错，也可以是设备、机械故障、环境因素等。它表示最基本的事件，不能再继续往下分析了。例如，影响驾驶员视野条件的“曲线地段”“照明不好”，驾驶员本身问题影响行车安全的“酒后开车”“疲劳驾驶”等原因，将事故原因扼要记入圆形符号内。

（3）屋形符号。如图 3-13c 所示，屋形符号表示正常事件，是系统在正常状态下发生的正常事件。如：“机车或车辆经过道岔”“因走动取下安全带”等，将事件扼要记入屋形符号内。

（4）菱形符号。如图 3-13d 所示，菱形符号表示省略事件，即表示事前不能分析，或者没有再分析下去的必要的事件。例如，“驾驶员间断瞭望”“天气不好”“臆测行车”“操作不当”等，将事件扼要记入菱形符号内。

图 3-13　事件符号

试读版本仅供防疫期间线上教学使用

2. 逻辑门符号

即连接各个事件，并表示逻辑关系的符号。其中主要有：与门、或门、条件与门、条件或门以及限制门。

（1）与门符号。与门连接表示输入事件 B_1、B_2 同时发生的情况下，输出事件 A 才会发生的连接关系。两者缺一不可，表现为逻辑积的关系，即 $A = B_1 \cap B_2$。在有若干输入事件时也是如此，如图 3-14a 所示。

“与门”用与门电路图来说明更容易理解，如图 3-14b 所示。

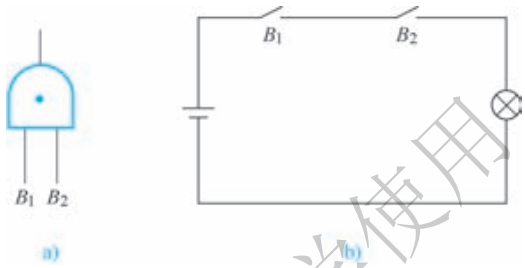

图 3-14 与门符号及与门电路图

当 B_1、B_2 都接通（$B_1 = 1$，$B_2 = 1$）时，电灯才亮（出现信号），用布尔代数表示为 $X = B_1 B_2 = 1$。

当 B_1、B_2 中有一个断开或都断开（$B_1 = 1$，$B_2 = 0$ 或 $B_1 = 0$，$B_2 = 1$ 或 $B_1 = 0$，$B_2 = 0$）时，电灯不亮（没有信号），用布尔代数表示为 $X = B_1 B_2 = 0$。

（2）或门符号。表示输入事件 B_1 或 B_2 中，任何一个事件发生都可以使事件 A 发生，表现为逻辑和的关系即 $A = B_1 \cup B_2$。在有若干输入事件时，情况也是如此，如图 3-15a 所示。

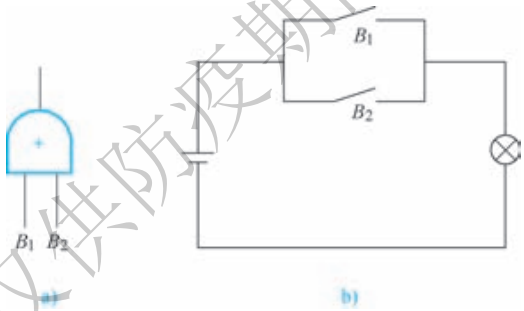

图 3-15 或门符号及或门电路图

或门用相对的逻辑电路来说明更好理解，如图 3-15b 所示。

当 B_1、B_2 断开（$B_1 = 0$，$B_2 = 0$）时，电灯才不会亮（没有信号），用布尔代数表示为 $X = B_1 + B_2 = 0$。

当 B_1、B_2 中有一个接通或两个都接通（即 $B_1 = 1$，$B_2 = 0$ 或 $B_1 = 0$，$B_2 = 1$ 或 $B_1 = 1$，$B_2 = 1$）时，电灯亮（出现信号），用布尔代数表示为 $X = B_1 + B_2 = 1$。

（3）条件与门符号。表示只有当 B_1、B_2 同时发生，且满足条件 α 的情况下，A 才会发生，相当于三个输入事件的与门。即 $A = B_1 \cap B_2 \cap \alpha$。将条件 α 记入六边形内，如图 3-16 所示。

图 3-16 条件与门符号图

（4）条件或门符号。表示 B_1 或 B_2 任何一个事件发生，且满足条件 β，输出事件 A 才会发生，将条件 β 记入六边形内，如图 3-17 所示。

试读版本仅供防疫期间线上教学使用

图 3-17　条件或门符号图

（5）限制门符号。它是逻辑上的一种修正符号，即输入事件发生且满足条件 γ 时，才产生输出事件。相反，如果不满足，则不发生输出事件，条件 γ 写在椭圆形符号内，如图 3-18 所示。

3. 转移符号

当事故树规模很大时，需要将某些部分画在别的纸上，这就要用转出和转入符号，以标出向何处转出和从何处转入。

转出符号，它表示向其他部分转出，△内记入向何处转出的标记，如图 3-19a 所示。

转入符号，它表示从其他部分转入，△内记入从何处转入的标记，如图 3-19b 所示。

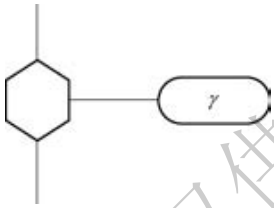

图 3-18　限制门符号图

图 3-19　转移符号

3.2.4　事故树分析程序

事故树分析虽然根据对象系统的性质、分析目的的不同，分析的程序也不同，但是一般都按照下面介绍的基本程序进行。有时，使用者还可根据实际需要和要求，来确定分析程序。图 3-20 为事故树分析的一般程序。

（1）熟悉系统。要求全面了解系统的整个情况，包括工作程序、各种重要参数、作业情况。必要时画出工艺流程图和布置图。

（2）调查事故。要求在过去事故实例、有关事故统计的基础上，尽量广泛地调查所能预想到的事故。包括分析系统已发生的事故，也包括未来可能发生的事故，同时也要调查外单位和同类系统发生的事故。

（3）确定顶上事件。所谓顶上事件就是我们要分析的对象事件——系统失效事件。对调查的事故，要分析其严重程度和发生的概率，从中找出后果严重且发生概率大的事件作为顶上事件。

试读版本仅供防疫期间线上教学使用

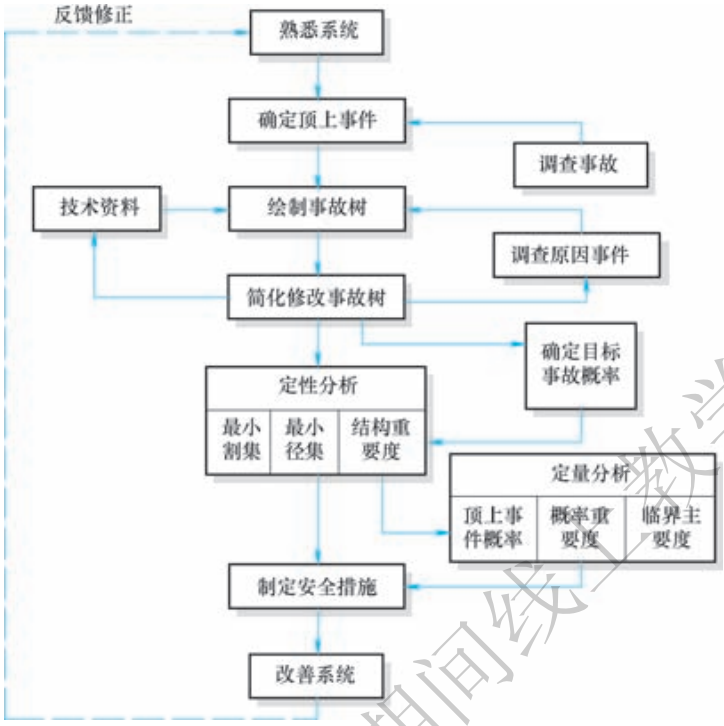

图 3-20　事故树分析的一般程序

（4）确定目标事故概率。根据以往的事故记录和同类系统的事故资料进行统计分析，求出事故发生的概率（或频率），然后根据这一事故的严重程度确定要控制的事故发生概率的目标值。

（5）调查原因事件。调查与事故有关的所有原因事件和各种因素，包括设备故障、机械故障、操作者的失误、管理和指挥错误、环境因素等，尽量详细查清原因和影响。

（6）绘制事故树。这是事故树分析的核心部分之一。根据上述资料，从顶上事件开始，按照演绎法，运用逻辑推理，一级一级地找出所有直接原因事件，直到最基本的原因事件为止。按照逻辑关系，用逻辑门连接输入输出关系（即上下层事件），画出事故树。

（7）定性分析。根据事故树结构进行化简，求出事故树的最小割集和最小径集，确定基本事件的结构重要度大小。根据定性分析的结论，按轻重缓急分别采取相应对策。

（8）计算顶上事件发生概率。首先根据所调查的情况和资料，确定所有原因事件的发生概率，并标在事故树上。根据这些基本数据，求出顶上事件（事故）发生概率。

（9）分析比较。要根据可维修系统和不可维修系统分别考虑。对可维修系统，把求出的概率与通过统计分析得出的概率进行比较，如果两者不符，则必须重新研究，看原因事件是否齐全，事故树逻辑关系是否清楚，基本原因事件的数值是否设定得过高或过低等。对不可维修系统，求出顶上事件发生概率即可。

（10）定量分析。定量分析包括下列三个方面的内容：

1）当事故发生概率超过预定的目标值时，要研究降低事故发生概率的所有可能途径，可从最小割集着手，从中选出最佳方案。

试读版本仅供防疫期间线上教学使用

2）利用最小径集，找出根除事故的可能性，从中选出最佳方案。

3）求各基本原因事件的临界重要度系数，从而对需要治理的原因事件按临界重要度系数大小进行排队，或编出安全检查表，以求加强人为控制。

（11）制定安全措施。绘制事故树的目的是查找隐患，找出薄弱环节，查出系统的缺陷，然后加以改进。在对事故树全面分析之后，必须制定安全措施，防止灾害发生。安全措施应在充分考虑资金、技术、可靠性等条件之后，选择最经济、最合理、最切合实际的对策。

在具体分析时，可以根据分析的目的、投入人力物力的多少、人的分析能力的高低以及对基础数据的掌握程度等，进行到不同程度。如果事故树规模很大，也可以借助电子计算机进行分析。

3.2.5　事故树的编制

1. 编制程序

（1）确定顶上事件。顶上事件就是所要分析的事故。选择顶上事件，一定要在详细了解系统情况、有关事故的发生情况和发生可能、事故的严重程度和事故发生概率等资料的情况下进行，而且事先要仔细寻找造成事故的直接原因和间接原因。然后，根据事故的严重程度和发生概率确定要分析的顶上事件，将其扼要地填写在矩形框内。

顶上事件也可以是已经发生过的事故。如车辆追尾、道口火车与汽车相撞等事故。通过编制事故树，找出事故原因，制定具体措施，防止事故再次发生。

（2）调查或分析造成顶上事件的各种原因。顶上事件确定之后，为了编制好事故树，必须将造成顶上事件的所有直接原因事件找出来，尽可能不要漏掉。直接原因事件可以是机械故障、人的因素或环境因素等。

要找出直接原因，可以采取对造成顶上事件的原因进行调查，召开有关人员座谈会的方法，也可根据以往的一些经验进行分析，确定造成顶上事件的原因。

（3）绘事故树。在确定顶上事件并找出造成顶上事件的各种原因之后，就可以用相应事件符号和适当的逻辑门把它们从上到下分层连接起来，层层向下，直到最基本的原因事件，这样就构成一个事故树。

在用逻辑门连接上下层之间的事件原因时，若下层事件必须全部同时发生，上层事件才会发生时，就用“与门”连接。逻辑门的连接问题在事故树中是非常重要的，含糊不得，它涉及各种事件之间的逻辑关系，直接影响着以后的定性分析和定量分析。

（4）认真审定事故树。画成的事故树图是逻辑模型事件的表达。既然是逻辑模型，那么各个事件之间的逻辑关系就应该相当严密、合理。否则在计算过程中将会出现许多意想不到的问题。因此，对事故树的绘制要十分慎重。在制作过程中，一般要进行反复推敲、修改，除局部更改外，有的甚至要推倒重来，有时还要反复进行多次，直到符合实际情况、比较严密为止。

2. 事故树编制的注意事项

事故树应能反映出系统故障的内在联系和逻辑关系，同时能使人一目了然，形象地掌握这种联系与关系，并据此进行正确的分析，为此，建造事故树应注意以下几点：

（1）熟悉分析系统。绘制事故树由全面熟悉开始，必须从功能的联系入手，充分了解

与人员有关的功能，掌握使用阶段的划分等与人员有关的功能，包括现有的冗余功能以及安全、保护功能等。此外，使用、维修状况也要考虑周全。这就要求广泛地收集与系统相关的设计、运行、流程图、设备技术规范等技术文件及资料，并进行深入细致的分析研究。

（2）循序渐进。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。

（3）选好顶上事件。建造事故树首先要选定一个顶上事件，顶上事件是指系统不希望发生的故障事件。选好顶上事件有利于使整个系统故障分析相互联系起来，因此，对系统的任务、边界以及功能范围必须给予明确的定义。顶上事件在大型系统中可能不止一个，一个特定的顶上事件可能只是许多系统失效事件之一。顶上事件在很多情况下是用FMEA——故障类型及影响分析、危险预先性分析或事件树分析得出的。一般考虑的事件有：对安全构成威胁的事件——造成人身伤亡或导致设备财产的重大损失（火灾爆炸、中毒、严重污染等），妨碍完成任务的事件——系统停工或丧失大部分功能，严重影响经济效益的事件——通信线路中断、交通停顿等妨碍提高经济收益的因素。

（4）准确判明各事件间的因果关系和逻辑关系。对系统中各事件间的因果关系和逻辑关系必须分析清楚，不能有逻辑上的紊乱及因果矛盾。每一个故障事件包含的原因事件都是事故事件的输入，即原因——输入，结果——输出。逻辑关系应根据输入事件的具体情况来定，若输入事件必须全部发生时顶上事件才发生，则用“与门”；若输入事件中任何一个发生时顶上事件即发生，则用“或门”。

（5）避免门与门相连。为了保证逻辑关系的准确性，事故树中任何逻辑门的输出都必须也只能有一个结果，不能将逻辑门与其他逻辑门直接相连。

3. 常用的事故树编制软件

事故树被广泛应用于系统安全评价中，而在实际应用中，系统往往由众多复杂要素构成，手工绘制事故树工作量较大，且对复杂事故树最小割集、最小径集、顶上事件概率的计算是一个庞大的工程，基于此，很多学者或机构开发了事故树绘制与分析软件，给安全工程技术和管理人员提供操作简单、功能丰富、快速实现事故树绘制及分析的工具。

常用的事故树分析软件有：FreeFta、EasyDraw、CARA-FaultTree、CAFTA 等。通过应用软件，可以很方便地选择各种事件符号和逻辑门符号，快速绘制事故树，并通过相应的最小割集、最小径集、顶上事件概率计算等软件功能，实现快速求解。图 3-21 展示了常用分析软件的界面。

各种事故树软件为事故树的编制及相应计算提供了简单快捷的工具，但事故树编制是建立在对系统进行全面分析基础上的。也就是说，事故树软件仅提供了一个绘制和分析的工具，事故树分析的核心内容依然是分析人员运用事故树分析的原理和方法对研究对象进行系统的分析。

试读版本仅供防疫期间线上教学使用

3.2.6　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，还要利用布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。

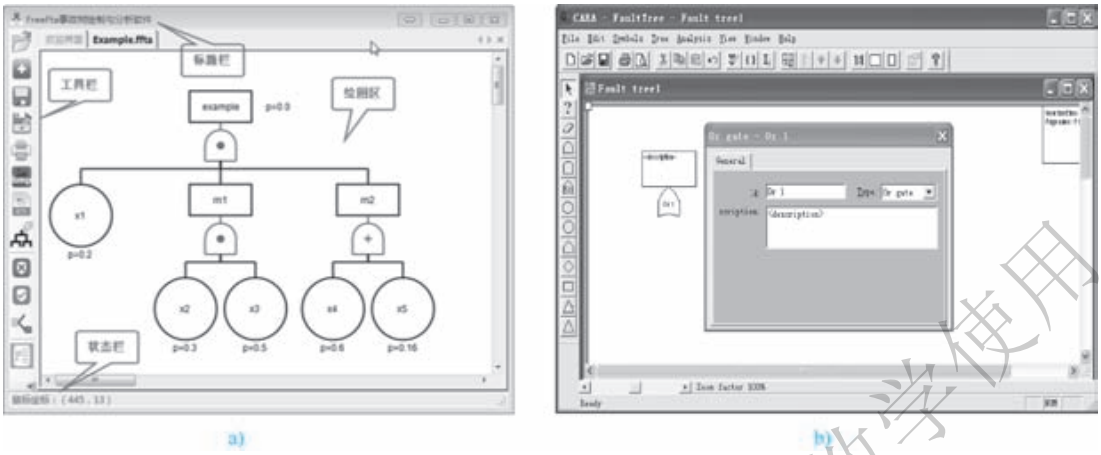

图 3-21　常用的事故树分析软件的界面

a）FreeFta 主界面　b）CARA-FaultTree 主界面

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。

1. 布尔代数的基本知识

（1）集合的概念。具有某种共同属性的事物的全体叫作集合，集合中的事物叫作元素。包含一切元素的集合称为全集，用符号 Ω 表示；不包含任何元素的集合称为空集，用符号 Φ 表示。

集合之间关系的表示方法如下：

1）集合以大写字母表示，集合的定义写在括号中。

2）集合之间的包含关系（即从属关系）用符号表示，子集 B_1 包含于全集 Ω 中，记为 $B_1 \in \Omega$。

3）两个子集相交之后，相交的部分为两个子集的共有元素的集合，称之为交集。两个集合相交的关系用符号 $\cap$ 表示，如 $C_1 = B_1 \cap B_2$。

4）两个子集相交之后，合并成一个较大的子集，这两个子集中元素的全体构成的集合称之为并集，并集的关系用符号 $\cup$ 表示，如 $C_2 = B_1 \cup B_2$。

事故树分析就是研究某一个事故树中各基本事件构成的各种集合，以及它们之间的逻辑关系，最后达到最优化处理的一门技术。

（2）逻辑运算。逻辑运算的对象是命题。命题是具有判断性的语言。成立的命题叫作真命题，其真值等于 1；不成立的命题叫作假命题，其真值等于 0。这里的真值“1”和“0”并不是数字，而是表示两个对立事物的符号。例如命题“8 − 3 = 5”成立，这是真命题，其真值为 1；命题“2 + 3 > 5”不成立，这是假命题，其真值为 0。

逻辑代数也可进行运算，其基本运算有三种，即逻辑加、逻辑乘、逻辑非。其中逻辑加、逻辑乘用得较普遍。

1）逻辑加。给定两个命题 A、B，对它们进行逻辑运算后构成的新命题为 S，若 A、B 两者有一个成立或同时成立，S 就成立；否则 S 不成立。则这种 A、B 间的逻辑运算叫作逻辑加，也叫“或”运算。构成的新命题 S，叫作 A、B 的逻辑和。记作 $A \cup B = S$ 或记作 $A +$

试读版仅供防疫期间线上教学使用

$B=S$。均读作“$A+B$”。逻辑加相当于集合运算中的“并集”。

根据逻辑加的定义可知：

$$1+1=1;\ 1+0=1;\ 0+1=1;\ 0+0=0$$

2）逻辑乘。给定两个命题A、B，对它们进行逻辑运算后构成新的命题P。若A、B同时成立，P就成立，否则P不成立。则这种A、B间的逻辑运算，叫作逻辑乘，也叫“与”运算。构成的新命题P叫作A、B的逻辑积。记作$A\cap B=P$，或记作$A\times B=P$，也可记作$AB=P$，均读作A乘B。逻辑乘相当于集合运算中的“交集”。

根据逻辑乘的定义可知：

$$1\times1=1;\ 1\times0=0;\ 0\times1=0;\ 0\times0=0$$

3）逻辑非。给定一个命题A，对它进行逻辑运算后，构成新的命题为F，若A成立，F就不成立；若A不成立，F就成立。这种对A所进行的逻辑运算，叫作命题A的逻辑非，构成的新命题F叫作命题A的逻辑非。A的逻辑非记作“$\overline{A}$”，读作“A非”。逻辑非相当于集合运算的求“补集”。

根据逻辑非的定义，可以知道：

$$\overline{1}=0;\ \overline{0}=1;\ \overline{\overline{1}}=1;\ \overline{\overline{0}}=0$$

（3）逻辑运算的法则。逻辑代数运算的法则很多，有的与代数运算法则一致，有的不一致。这里只介绍几种常用的运算法则，以便记忆和运用。

对合律：$\overline{\overline{A}}=A$

交换律：$A+B=B+A$，$AB=BA$

结合律：$A+(B+C)=(A+B)+C$，$A(BC)=(AB)C$

分配律：$A+BC=(A+B)(A+C)$，$A(B+C)=AB+AC$

等幂律：$A+A=A$，$A\cdot A=A$

吸收律：$A+AB=A$，$A(A+B)=A$

在事故树分析中“$A+AB=A$”“$A+A=A$”和“$A\cdot A=A$”几个法则用得较多。

2. 概率论的一些基本知识

进行事故树分析需要用到概率论的一些基本知识。例如，概率和与概率积的计算。为了给出概率和与概率积的计算公式，必须首先给出下列定义：

（1）相互独立事件。一个事件发生与否不受其他事件的发生与否的影响。假定有A、B、C、…、N事件，其中每一个事件发生与否都不受其他事件发生与否的影响，则称A、B、C、…、N为独立事件。

（2）相互排斥事件。不能同时发生的事件。一个事件发生，其他事件必然不发生。它们之间互相排斥，互不相容。假定有A、B、C、…、N事件，A发生时，B、C、…、N必然不发生；B发生时，A、C、…、N事件必须不发生，则A、B、C、…、N事件称为互斥事件。

（3）相容事件。一个事件发生与否受其他事件的约束，即在其他事件发生的条件下才发生的事件。设A、B两事件，B事件只有在A事件发生的情况下才发生，反之亦然，则A、B事件称为相容事件。

在事故树分析中，遇到的基本事件大多数是独立事件。所以下面简单介绍n个独立事件的概率和与概率积的计算公式。

n个独立事件的概率和，其计算公式为：

试读版仅供防疫期间线上教学使用

$$P(A+B+C+\cdots+N)=1-[1-P(A)][1-P(B)][1-P(C)]\cdots[1-P(N)] \quad (3\text{-}1)$$

式中　P——独立事件的概率。

n 个独立事件的概率积，其计算公式为：

$$P(ABC\cdots N)=P(A)P(B)P(C)\cdots P(N) \quad (3\text{-}2)$$

3. 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，便得到了布尔代数表达式。以图3-22（事故树结构）为例，其布尔代数表达式及展开过程如下：

$$\begin{aligned}T&=A_1X_t=A_2A_3X_t\\&=(A_4+A_5)(X_5+X_6)X_t\\&=(X_1+X_2+X_3+X_4)(X_5+X_6)X_t\end{aligned}$$

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表述。对于给出的事故树可以写出相应的布尔代数表达式；相反，给出布尔代数表达式就可以绘出相应的事故树。

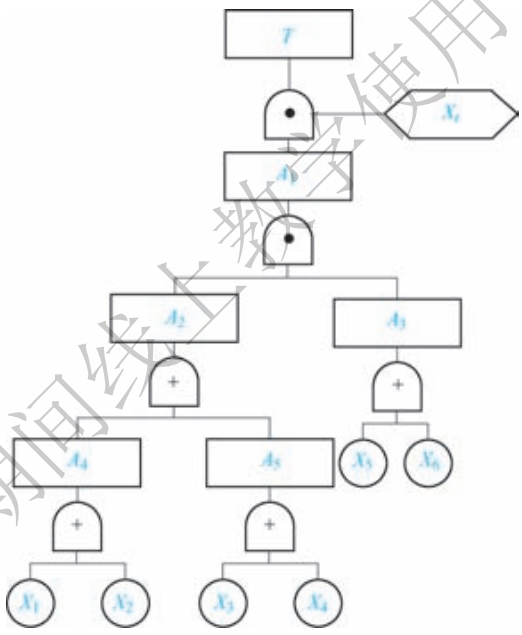

图 3-22　某事故树图

4. 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。

如果事故树中各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：

$$g(x_1x_2\cdots x_n)=q_1q_2\cdots q_n=\prod_{i=1}^{n}q_i \quad (3\text{-}3)$$

各基本事件逻辑“加”的概率应为：

$$g(x_1+x_2+\cdots+x_n)=1-(1-q_1)(1-q_2)\cdots(1-q_n)=1-\prod_{i=1}^{n}(1-q_i) \quad (3\text{-}4)$$

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。

如果图3-22中各基本事件是相互独立的，利用上述式（3-1）和式（3-2），求图3-22事故树的概率函数，代入下式：

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

式中　q_t——控制门事件的发生概率。

3.2.7　事故树的化简及意义

在事故树编制完成之后，为了准确计算顶上事件发生的概率，需要化简事故树，消除多

试读版本仅供预览期间线上教学使用

余事件，特别是在事故树的不同位置存在同一基本事件时，必须利用布尔代数进行整理，然后才能计算顶上事件的发生概率，否则就会造成定性分析或定量分析的错误。

化简的方法就是反复运用布尔代数法则，化简的程序是：①代数式若有括号应先去括号将函数展开；②利用幂等法则归纳相同的项；③充分利用吸收法则直接化简。

【例 3-6】 如图 3-23 所示，在该事故树中 3 个基本事件概率为 $q_1=q_2=q_3=0.1$，求顶上事件的发生概率。

解：

$$T=A_1A_2=X_1X_2\ (X_1+X_3)$$

按独立事件概率和与积的计算公式，顶上事件发生概率为：

$$\begin{aligned} q_T &= q_1q_2\ [1-(1-q_1)(1-q_3)] \\ &= 0.1\times 0.1\times [1-(1-0.1)\times(1-0.1)] \\ &= 0.0019 \end{aligned}$$

布尔代数化简：

$$\begin{aligned} T &= X_1X_2\ (X_1+X_3)\ (\text{未经化简形式}) \\ &= X_1X_2X_1+X_1X_2X_3\ (\text{应用分配律展开}) \\ &= X_1X_2+X_1X_2X_3\ (\text{应用等幂律去掉多余的 } X_1) \\ &= X_1X_2\ (\text{应用吸收律去掉多余的 } X_3\text{，达到最简形式}) \end{aligned}$$

所以：

$$q_T=q_1q_2=0.01$$

其等效树图如图 3-24 所示。没简化时，有无关事件 X_3，化简后，只要有 X_1、X_2 发生，不论 X_3 发生与否，顶上事件都发生。因此，必须化简，才能正确进行事故树的定性、定量分析。

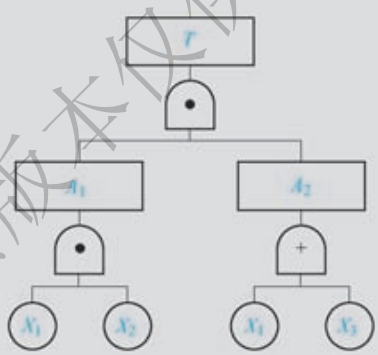

图 3-23 事故树图

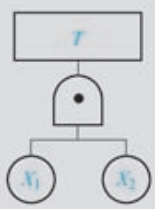

图 3-24 等效树图

【例 3-7】 化简如图 3-25 所示的事故树。

解： 事故树的结构函数为：

$$\begin{aligned} T &= A_1+A_2 \\ &= X_1X_2+\ (X_3+B) \end{aligned}$$

试读版本仅供防疫期间线上教学使用

$$= X_1X_2 + [X_3 + (X_1X_3)]$$
$$= X_1X_2 + X_3$$

所以，其等效图如图 3-26 所示。

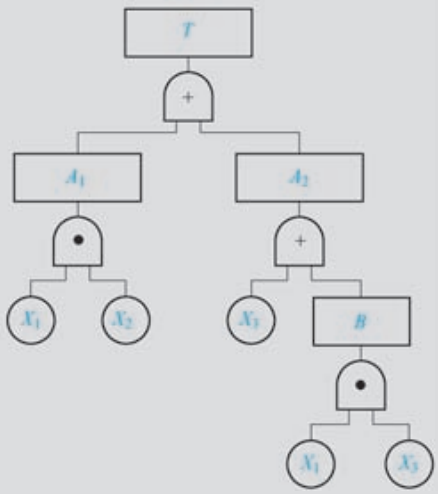

图 3-25　事故树示意图及等效图

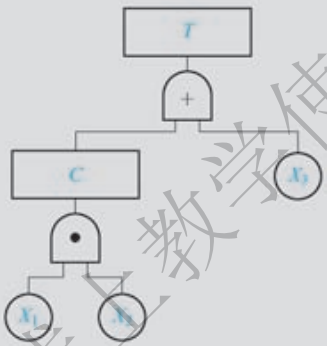

图 3-26　事故树的等效图

3.2.8　事故树的定性分析

事故树的定性分析，是依据事故树对所有事件只有发生“1”或不发生“0”两种状态进行分析的方法。定性分析的目的是根据事故树的结构查明顶上事件发生的途径，确定顶上事件的发生模式、起因及影响程度，为改善系统安全提供可选择的措施。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。

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基本事件都发生，则顶上事件必然发生。但是，大多数情况下并不是一定要求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集合称为割集。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集合。最小割集指明了哪些基本事件同时发生就可以引起顶上事件发生的事故模式。

（2）求解方法。求解方法有三种。

1）行列法。行列法是 1972 年福塞尔提出的方法，所以也称其为福塞尔法。其理论依据是：“与门”使割集容量增加，而不增加割集的数量；“或门”使割集的数量增加，而不增加割集的容量。这种方法是从顶上事件开始，用下一层事件代替上一层事件，把“与门”连接的事件按行横向排列，把“或门”连接的事件按列纵向摆开。这样，逐层向下，直至各基本事件，列出若干行，最后利用布尔代数化简，便得到所求的最小割集。

试读版本仅供防疫期间线上教学使用

为了说明这种计算方法，下面以图 3-27 所示的事故树为例，求其最小割集。

可以看到，顶上事件 T 与中间事件 A_1、A_2 是用“或门”连接的，所以，应当成列摆开，即：

$$T \xrightarrow{\text{或门}} \begin{cases} A_1 \\ A_2 \end{cases}$$

A_1、A_2 与下一层事件 B_1、B_2、X_1、X_2、X_4 的连接均为“与门”，所以成行排列：

$$\begin{cases} A_1 \xrightarrow{\text{与门}} X_1 B_1 X_2 \\ A_2 \xrightarrow{\text{与门}} X_4 B_2 \end{cases}$$

下面依此类推：

$$\begin{cases} X_1 B_1 X_2 \xrightarrow{\text{或门}} \begin{cases} X_1 X_1 X_2 \\ X_1 X_3 X_2 \end{cases} \\ X_4 B_2 \xrightarrow{\text{或门}} \begin{cases} X_4 C \xrightarrow{\text{与门}} X_4 X_4 X_5 \\ X_4 X_6 \end{cases} \end{cases}$$

整理上式得：

$$\begin{cases} X_1 X_1 X_2 \\ X_1 X_3 X_2 \\ X_4 X_4 X_5 \\ X_4 X_6 \end{cases}$$

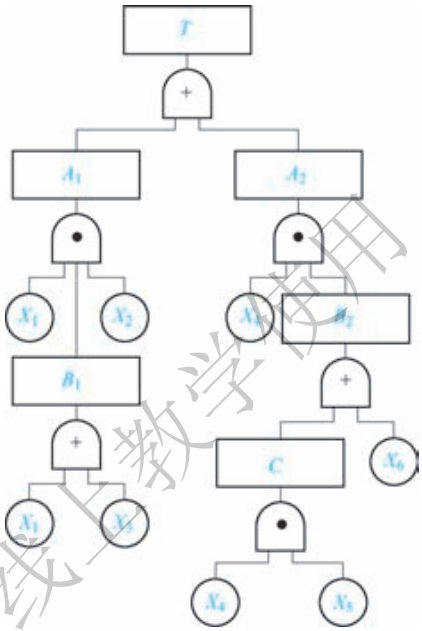

图 3-27　事故树示意图

下面对这四组集合用布尔代数化简，根据 $A \cdot A = A$，则 $X_1 \cdot X_1 = X_1$，$X_4 \cdot X_4 = X_4$，即：

$$\begin{cases} X_1 X_1 X_2 \\ X_1 X_3 X_2 \\ X_4 X_4 X_5 \\ X_4 X_6 \end{cases} \rightarrow \begin{cases} X_1 X_2 \\ X_1 X_2 X_3 \\ X_4 X_5 \\ X_4 X_6 \end{cases}$$

又根据 $A + A \cdot B = A$，则 $X_1 \cdot X_2 + X_1 \cdot X_2 \cdot X_3 = X_1 \cdot X_2$，即：

$$\begin{cases} X_1 X_2 \\ X_1 X_2 X_3 \\ X_4 X_5 \\ X_4 X_6 \end{cases} \rightarrow \begin{cases} X_1 X_2 \\ X_4 X_5 \\ X_4 X_6 \end{cases}$$

于是，就得到三个最小割集 $\{X_1, X_2\}$、$\{X_4, X_5\}$、$\{X_4, X_6\}$。按最小割集化简后的事故树，如图 3-28 所示。

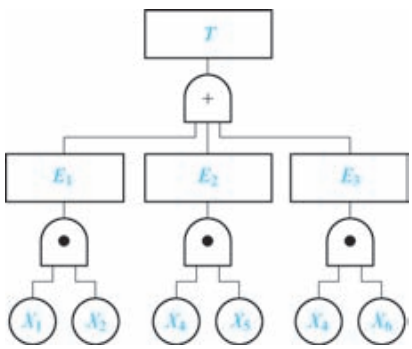

图 3-28　图 3-27 事故树的等效图

2）结构法。这种方法的理论根据是事故树的结构完全可以用最小割集来表示。下面再来分析图 3-27 所示事故树示意图：

$$T = A_1 \cup A_2 = (X_1 B_1 X_2) \cup (X_4 B_2)$$

试读版本仅供防疫期间线上教学使用

$$
\begin{aligned}
&= X_1(X_1 \cup X_3)X_2 \cup X_4(C \cup X_6) \\
&= (X_1X_2) \cup (X_1X_3X_2) \cup X_4(X_4X_5 \cup X_6) \\
&= (X_1X_2) \cup (X_1X_2X_3) \cup (X_4X_4X_5) \cup (X_4X_6) \\
&= (X_1X_2) \cup (X_4X_5) \cup (X_4X_6)
\end{aligned}
$$

这样，得到的三个最小割集$\{X_1, X_2\}$、$\{X_4, X_5\}$、$\{X_4, X_6\}$完全与上例用行列法得到的结果一致。说明这种方法是正确的。

3）布尔代数化简法。这种方法的理论依据是：上述结构法完全和布尔代数化简事故树法相似，所不同的只是“∪”与“+”的问题。实质上，布尔代数化简法中的“+”和结构式中的“∪”是一致的。这样，用布尔代数化简法最后求出的若干事件逻辑积的逻辑和，其中，每个逻辑积就是最小割集。现在还以图3-27所示为例，进行化简：

$$
\begin{aligned}
T &= A_1 + A_2 = X_1B_1X_2 + X_4B_2 \\
&= X_1(X_1 + X_3)X_2 + X_4(C + X_6) \\
&= X_1X_2 + X_1X_3X_2 + X_4(X_4X_5 + X_6) \\
&= X_1X_2 + X_1X_2X_3 + X_4X_4X_5 + X_4X_6 \\
&= X_1X_2 + X_4X_5 + X_4X_6
\end{aligned}
$$

所得的三个最小割集$\{X_1, X_2\}$、$\{X_4, X_5\}$、$\{X_4, X_6\}$与第一种、第二种算法的结果相同。总的来说，三种求法都可应用，而以第三种算法最为简单，较为普遍采用。

2. 最小径集的概念及求法

（1）最小径集的概念。如果事故树中的全部基本事件都不发生，则顶上事件一定不会发生。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集合称为径集。径集中的基本事件之间是逻辑“加”（或称为“或”）的关系。

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集合。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。

（2）最小径集的求法。求最小径集是利用它与最小割集的对偶性，首先作出与事故树对偶的成功树，就是把原来事故树的“与门”换成“或门”，“或门”换成“与门”，各类事件发生换成不发生。然后，利用上节所述方法，求出成功树的最小割集经对偶变换后就是事故树的最小径集。图3-29给出了两种常用的转换方法。

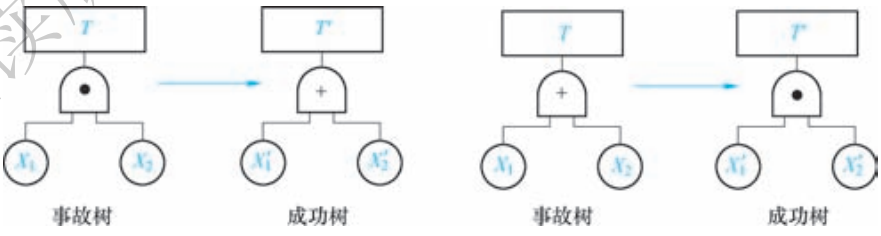

图3-29　与事故树对偶的成功树的转换关系图

为什么要这样转换呢？因为，对于“与门”连接输入事件和输出事件的情况，只要有一个事件不发生，输出事件就可以不发生，所以，在成功树中换用“或门”连接输入事件和输出事件；而对于“或门”连接的输入事件和输出事件的情况，则必须所有输入事件均

试读版本仅供预览期间线上教学使用

不发生，输出事件才不发生，所以，在成功树中换用“与门”连接输入事件和输出事件。例如图 3-29 所示，其中：T'、X_1'、X_2' 表示事件 T、X_1、X_2 不发生。

例如，图 3-30 所示为与图 3-27 事故树对偶的成功树。

用 T'、A_1'、A_2'、B_1'、B_2'、C'、X_1'、X_2'、X_3'、X_4'、X_5'、X_6' 分别表示各事件 T、A_1、A_2、B_1、B_2、C、X_1、X_2、X_3、X_4、X_5、X_6 不发生。

用布尔代数化简法求最小径集：

$$
\begin{aligned}
T' &= A_1'A_2' \\
&= (X_1' + B_1' + X_2')(X_4' + B_2') \\
&= (X_1' + X_1'X_3' + X_2')(X_4' + C'X_6') \\
&= (X_1' + X_2')[X_4' + (X_4' + X_5')X_6'] \\
&= (X_1' + X_2')(X_4' + X_4'X_6' + X_5'X_6') \\
&= (X_1' + X_2')(X_4' + X_5'X_6') \\
&= X_1'X_4' + X_1'X_5'X_6' + X_2'X_4' + X_2'X_5'X_6'
\end{aligned}
$$

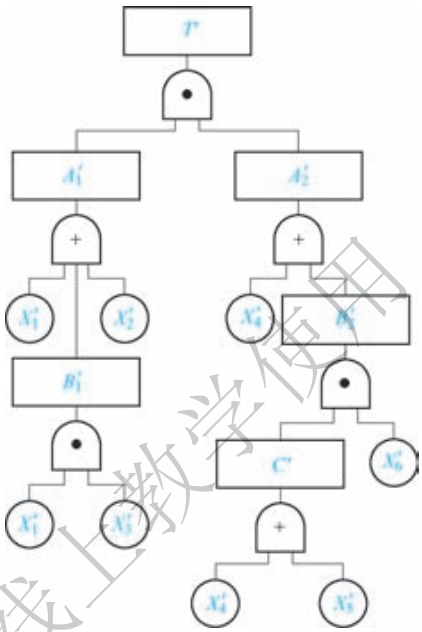

图 3-30　与图 3-27 所示事故树对偶的成功树图

这样，就得到成功树的 4 个最小割集，经对偶变换就是事故树的 4 个最小径集，即：

$$T = (X_1 + X_4)(X_1 + X_5 + X_6)(X_2 + X_4)(X_2 + X_5 + X_6)$$

每一个逻辑和就是一个最小径集，则得到事故树的 4 个最小径集为：$\{X_1, X_4\}$、$\{X_2, X_4\}$、$\{X_1, X_5, X_6\}$、$\{X_2, X_5, X_6\}$。

同样，也可以用最小径集表示事故树，如图 3-31 所示。其中 P_1、P_2、P_3、P_4 分别表示 4 个最小径集。

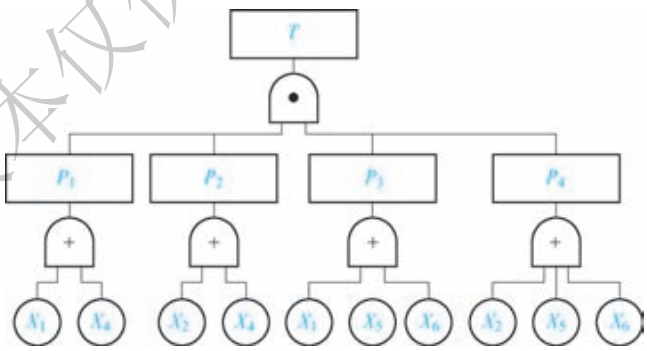

图 3-31　用最小径集等效表示的图 3-27 中的事故树

3. 判别割（径）集数目的方法

就一个具体的系统而言，如果事故树中的“与门”多、“或门”少时，则最小割集的数目较少，分析时从最小割集入手较为简便。反之，如果事故树中的“或门”多、“与门”少时，则最小径集的数目较少，分析时从最小径集入手较为简便。

但是，一个系统往往是很复杂的，有时很难根据“与门”“或门”的数目判定割、径集

试读版本仅供防疫期间线上教学使用

的数目。下面介绍一种求割、径集的数目的公式。

求割集数目公式：

$$x_i=\begin{cases}x_{i,1}x_{i,2}\cdots x_{i,\lambda_i}, & i\text{ 为与门时}\\ x_{i,1}+x_{i,2}+\cdots+x_{i,\lambda_i}, & i\text{ 为或门时}\end{cases}$$

求径集数目公式：

$$x_i=\begin{cases}x_{i,1}x_{i,2}\cdots x_{i,\lambda_i}, & i\text{ 为或门时}\\ x_{i,1}+x_{i,2}+\cdots+x_{i,\lambda_i}, & i\text{ 为与门时}\end{cases}$$

式中　i——门的编号或代码；

$x_{i,j}$——第 i 个门的第 j 个输入变量（$j=1,2,\cdots,\lambda_i$）；当输入变量是基本事件时，$x_{i,j}=1$；当输入变量是门 K 时，$x_{i,j}=x_k$；

λ_i——第 i 个门输入事件的数量；

x_i——表示门 i 的变量，若门 i 是紧接着顶上事件的门，则 $x_i=X_{TOP}$ 即为割（径）集的数目。

求径集的数目时，也可先求出原事故树的成功树，然后用求割集数目公式求取。

如图 3-32 所示：首先根据事故树画出成功树，再给各基本事件赋予“1”，然后根据输入与输出事件之间的逻辑门确定“加”或“乘”。

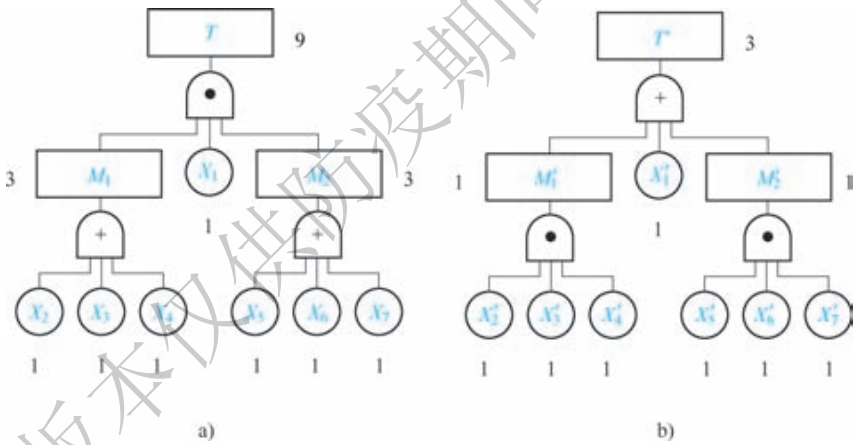

图 3-32　割（径）集的求法

a）事故树　b）成功树

割集数目：$M_1=1+1+1=3$

$M_2=1+1+1=3$

$T=3\times3\times1=9$

径集数目：$M_1=1\times1\times1=1$

$M_2=1\times1\times1=1$

$T=1+1+1=3$

从上例可看出，割集数目比径集数目多，此时用径集分析要比用割集分析简单。如果估算出某事故树的割、径集数目相差不多，一般从分析割集入手较好。这是因为最小割集的意义是导致事故发生的各种途径，得出的结果简明、直观。另外，在做定量分析时，用最小割

试读版本仅供防疫期间线上教学使用

集分析，还可采用较多的近似公式，而最小径集则不能。

必须注意，用上述方法得到的割、径集数目，不是最小割、径集的数目，而是最小割、径集的上限。只有当事故树中没有重复事件时，得到的割、径集数目才是最小割、径集的数目。

4. 最小割集和最小径集在事故树分析中的作用

最小割集和最小径集在事故树分析中起着极其重要的作用，其中，尤以最小割集最突出，透彻掌握和灵活运用最小割集和最小径集能使事故树分析收到事半功倍的效果，并为有效地控制事故的发生提供重要依据。

最小割集和最小径集的主要作用是：

（1）最小割集表示系统的危险性。一般认为，事故树的最小割集越多，系统越危险。求出最小割集可以掌握事故发生的各种可能，为事故调查和事故预防提供方便。

一起事故的发生，并不都遵循一种固定的模式，如果求出了最小割集，就可以马上知道发生事故的所有可能途径。例如：求得图 3-27 所示事故树的最小割集为$\{X_1,X_2\}$、$\{X_4,X_5\}$、$\{X_4,X_6\}$，并绘出了它的等效图。这样，它就直观明了地告诉我们，造成顶上事件（事故）发生的途径共三种；或者 X_1，X_2 同时发生；或者 X_4，X_5 同时发生；或者 X_4，X_6 同时发生。这对全面掌握事故发生规律，找出隐藏的事故模式是非常有效的，而且对事故的预防工作提供了非常全面的信息。这样就可以防止头痛医头、脚痛医脚、挂一漏万的问题。

（2）最小径集表示系统的安全性。一般认为，事故树的最小径集越多，系统越安全。求出最小径集可以知道，要使事故不发生，有几种可能方案。例如：图 3-31（最小径集等效表示的图 3-27 中的事故树）共有 4 个最小径集：$\{X_1,X_4\}$，$\{X_2,X_4\}$，$\{X_1,X_5,X_6\}$，$\{X_2,X_5,X_6\}$。从这个等效图的结构看出，只要卡断“与门”下的任何一个最小径集 P_i，就可以使顶上事件不发生，也就是说，上述四组事件中，任何一组不发生，顶上事件就可以不发生。

（3）最小割集能直观地、概略地告诉人们，哪种事故模式最危险，哪种稍次，哪种可以忽略。例如，某事故树有三个最小割集：$\{X_1\}$、$\{X_1,X_3\}$、$\{X_4,X_5,X_6\}$（如果各基本事件的发生概率都相等）。一般来说，一个事件的割集比两个事件的割集容易发生；两个事件的割集比三个事件的割集容易发生……因为一个事件的割集只要一个事件发生，如 X_1 发生，顶上事件就会发生；而两个事件的割集则必须满足两个条件（即 X_1 和 X_3 同时发生）才能引起顶上事件发生，这是显而易见的。

（4）利用最小径集可以经济地、有效地选择预防事故的方案。从图 3-31 中看出，要消除顶上事件 T 发生的可能性，可以有四种途径，究竟选择哪种途径最省事、最经济呢？从直观角度看，一般以消除含事件少的最小径集中的基本事件最省事、最经济。消除一个基本事件应比消除两个或多个基本事件要省力。

（5）利用最小割集和最小径集可以直接排出结构重要度顺序（详见结构重要度求解）。

（6）利用最小割集和最小径集计算顶上事件的发生概率和定量分析（详见顶上事件的发生概率求解）。

5. 结构重要度分析

结构重要度分析是从事故树结构入手分析各基本事件的重要程度。结构重要度分析一般可以采用两种方法，一种是精确求出结构重要度系数，一种是用最小割集或最小径集排出结

试读版本仅供预览，非完整版本使用

构重要度顺序。

（1）求各基本事件的结构重要度系数。在事故树分析中，各个事件都是两种状态，一种状态是发生，即 $X_i=1$；一种状态是不发生，即 $X_i=0$。各个基本事件状态的不同组合又构成顶上事件的不同状态，即 $\Phi(X)=1$ 或 $\Phi(X)=0$。

在某个基本事件 X_i 的状态由0变成1（即 $0_i \rightarrow 1_i$），其他基本事件的状态保持不变，顶上事件的状态变化可能有三种情况：

$\Phi(0_i,X)=0 \rightarrow \Phi(1_i,X)=0$，则 $\Phi(1_i,X)-\Phi(0_i,X)=0$

$\Phi(0_i,X)=0 \rightarrow \Phi(1_i,X)=1$，则 $\Phi(1_i,X)-\Phi(0_i,X)=1$

$\Phi(0_i,X)=1 \rightarrow \Phi(1_i,X)=1$，则 $\Phi(1_i,X)-\Phi(0_i,X)=0$

第一种情况和第三种情况都不能说明 X_i 的状态变化对顶上事件的发生起什么作用，唯有第二种情况说明 X_i 的作用，即当基本事件 X_i 的状态从0变到1，其他基本事件的状态保持不变，顶上事件的状态 $\Phi(0_i,X)=0$ 变到 $\Phi(1_i,X)=1$，也就说明，这个基本事件 X_i 的状态变化对顶上事件的发生与否起了作用。把所有这样的情况累加起来乘以一个系数 $1/2^{n-1}$，定义为结构重要度系数（n 是该事故树的基本事件的个数）。

现在，以图3-33所示的事故树为例，求出各基本事件的结构重要度系数。

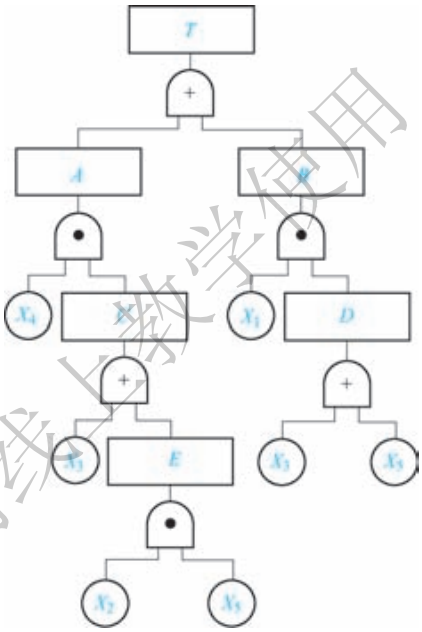

图3-33　事故树示意图

图3-33所示的事故树共有五个基本事件，其状态组合和顶上事件的状态见表3-1。

表3-1　基本事件的状态值与顶上事件的状态值表

编　号	X_1	X_2	X_3	X_4	X_5	$\Phi(X)$	编　号	X_1	X_2	X_3	X_4	X_5	$\Phi(X)$
1	0	0	0	0	0	0	17	1	0	0	0	0	0
2	0	0	0	0	1	0	18	1	0	0	0	1	1
3	0	0	0	1	0	0	19	1	0	0	1	0	0
4	0	0	0	1	1	0	20	1	0	0	1	1	1
5	0	0	1	0	0	0	21	1	0	1	0	0	1
6	0	0	1	0	1	0	22	1	0	1	0	1	1
7	0	0	1	1	0	1	23	1	0	1	1	0	1
8	0	0	1	1	1	1	24	1	0	1	1	1	1
9	0	1	0	0	0	0	25	1	1	0	0	0	0
10	0	1	0	0	1	0	26	1	1	0	0	1	1
11	0	1	0	1	0	0	27	1	1	0	1	0	0
12	0	1	0	1	1	1	28	1	1	0	1	1	1
13	0	1	1	0	0	0	29	1	1	1	0	0	1
14	0	1	1	0	1	0	30	1	1	1	0	1	1
15	0	1	1	1	0	1	31	1	1	1	1	0	1
16	0	1	1	1	1	1	32	1	1	1	1	1	1

试读版本仅供防疫期间线上教学使用

以基本事件 X_1 为例，可从表3-1查出，基本事件 X_1 发生（即 $X_1=1$），不管其他基本事件发生与否，顶上事件也发生（即 $\Phi(X)=1$）的组合，共12个，即编号18，20，21，22，23，24，26，28，29，30，31，32。这12个组合中的基本事件 X_1 的状态由发生变为不发生时，即 $X_1=0$，其顶上事件也不发生（即 $\Phi(X)=0$）的组合，共7个，即编号18（1 0 0 0 1），20（1 0 0 1 1），21（1 0 1 0 0），22（1 0 1 0 1），26（1 1 0 0 1），29（1 1 1 0 0），30（1 1 1 0 1）。也就是说，在12个组合当中，有5个组合不随基本事件 X_1 的状态变化而改变顶上事件的状态，即 $X_1=0$ 时，顶上事件也发生，编号为23，24，28，31，32的5个组合就是这类情况。上面谈到的7个组合就是前面讲的第二种情况的个数。用7再乘一个系数 $1/2^{n-1}=1/16$，就得出基本事件 X_1 的结构重要度系数7/16，用公式表示为：

$$I_{\Phi(1)}=\frac{1}{2^{n-1}}\sum\left[\Phi(1_i,X)-\Phi(0_i,X)\right]=\frac{1}{16}\times(12-5)=\frac{7}{16}$$

同样，可以逐个求出事件2～事件5的结构重要度系数为：

$$I_{\Phi(2)}=\frac{1}{16};\ I_{\Phi(3)}=\frac{7}{16};\ I_{\Phi(4)}=\frac{5}{16};\ I_{\Phi(5)}=\frac{5}{16}$$

因而，基本事件结构重要度排序如下：

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

如果不考虑基本事件的发生概率，仅从基本事件在事故树结构中所在位置来看，事件 X_1、X_3 最重要，其次是 X_4、X_5，最不重要的是基本事件 X_2。

下面用简易办法确定各基本事件的结构重要度系数：

X_1 的结构重要度系数：从表3-1中可知，$X_1=1$，$\Phi(X)=1$ 的个数是12个，而 $X_1=0$ 时，$\Phi(X)=1$ 的个数为5（即编号为7，8，12，15，16），那么：

$$I_{\Phi(1)}=\frac{1}{2^{n-1}}\times(12-5)=\frac{1}{16}\times7=\frac{7}{16}$$

X_2 的结构重要度系数：从表3-1可知，$X_2=1$，$\Phi(X)=1$ 的个数是9，而 $X_2=0$ 时，$\Phi(X)=1$ 的个数为8（即编号7，8，18，20，21，22，23，24），那么：

$$I_{\Phi(2)}=\frac{1}{2^{n-1}}\times(9-8)=\frac{1}{16}\times1=\frac{1}{16}$$

X_3 的结构重要度系数：从表3-1中可知 $X_3=1$，$\Phi(X)=1$ 的个数是12，而 $X_3=0$ 时，$\Phi(X)=1$ 的个数为5（即编号12，18，20，26，28），那么：

$$I_{\Phi(3)}=\frac{1}{2^{n-1}}\times(12-5)=\frac{1}{16}\times7=\frac{7}{16}$$

X_4 的结构重要度系数：从表3-1中可知 $X_4=1$，$\Phi(X)=1$ 的个数是11，而 $X_4=0$ 时，$\Phi(X)=1$ 的个数为6（即编号18，21，22，26，29，30），那么：

$$I_{\Phi(4)}=\frac{1}{2^{n-1}}\times(11-6)=\frac{1}{16}\times5=\frac{5}{16}$$

X_5 的结构重要度系数：从表3-1中可知，$X_5=1$，$\Phi(X)=1$ 的个数是11，而 $X_5=0$ 时，$\Phi(X)=1$ 的个数为6（即编号7，15，21，23，29，31），那么：

$$I_{\Phi(5)}=\frac{1}{2^{n-1}}\times(11-6)=\frac{1}{16}\times5=\frac{5}{16}$$

这样，用简易方法计算出的各基本事件结构重要度系数与上述方法计算出的结果完全一

试读版本仅供防发热网线上教学使用

致，但这种方法简便得多。

结构重要度分析属于定性分析，要排出各基本事件的结构重要度顺序，不一定非求出结构重要度系数不可，因而大可不必花很大的精力编排基本事件状态值和顶上事件状态值表，而一个个去数去算。如果事故树结构很复杂，基本事件很多，列出的表就很庞大，基本事件状态值的组合很多（共2^n个），这就给求结构重要度系数带来很大困难。因此，一般用最小割集或最小径集来排列各种基本事件的结构重要度顺序。这样较简单，而效果相同。

（2）用最小割集或最小径集进行结构重要度分析。

1）最小割集或最小径集排列法。这种直接排序方法的基本原则如下：

① 频率。当最小割集中的基本事件个数不等时，基本事件少的割集中的基本事件比基本事件多的割集中的基本事件结构重要度大。

例如，某事故树的最小割集为$\{X_1,X_2,X_3,X_4\}$，$\{X_5,X_6\}$，$\{X_7\}$，$\{X_8\}$。从其结构情况看，第三、四两个最小割集都只有一个基本事件，所以X_7和X_8的结构重要度最大；其次是X_5，X_6，因为它们位于两个事件的最小割集中；最不重要的是X_1，X_2，X_3，X_4，因为它们所在的最小割集中基本事件最多。这样就可以很快排出各基本事件的结构重要度顺序：

$$I_\Phi(7)=I_\Phi(8)>I_\Phi(5)=I_\Phi(6)>I_\Phi(1)=I_\Phi(2)=I_\Phi(3)=I_\Phi(4)$$

② 频数。当最小割集中基本事件的个数相等时，重复在各最小割集中出现的基本事件，比只在一个最小割集中出现的基本事件结构重要度大；重复次数多的比重复次数少的结构重要度大。

例如，某事故树有8个最小割集：$\{X_1,X_5,X_7,X_8\}$，$\{X_1,X_6,X_7,X_8\}$，$\{X_2,X_5,X_7,X_8\}$，$\{X_2,X_6,X_7,X_8\}$，$\{X_3,X_5,X_7,X_8\}$，$\{X_3,X_6,X_7,X_8\}$，$\{X_4,X_5,X_7,X_8\}$，$\{X_4,X_6,X_7,X_8\}$。在这8个最小割集中，X_7和X_8均各出现过8次；X_5和X_6均各出现过4次；X_1，X_2，X_3，X_4均各出现过2次。这样，尽管8个最小割集基本事件个数都相等（4个），但由于各基本事件在其中出现的次数不同，仍可以排出其结构重要度顺序：

$$I_\Phi(7)=I_\Phi(8)>I_\Phi(5)=I_\Phi(6)>I_\Phi(1)=I_\Phi(2)=I_\Phi(3)=I_\Phi(4)$$

③ 看频率又看频数。在基本事件少的最小割集中出现次数少的事件与基本事件多的最小割集中出现次数多的事件相比较，一般前者大于后者。

例如，某事故树的最小割集为$\{X_1\}$，$\{X_2,X_3\}$，$\{X_2,X_4\}$，$\{X_2,X_5\}$，其结构重要度顺序为：

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

上述原则，对最小径集同样适用。当然，也可以用两种方法互相检验结果的正确性。

2）简易算法。给每一最小割集都赋予1，而最小割集中每个基本事件都得到相同的一份，然后每个基本事件积累得分，按其得分多少，排出结构重要度的顺序。

【例3-8】 某事故树最小割集$K_1=\{x_5,x_6,x_7,x_8\}$，$K_2=\{x_3,x_4\}$，$K_3=\{x_1\}$，$K_4=\{x_2\}$。试确定各基本事件的结构重要度。

解：

$$x_5=x_6=x_7=x_8=\frac{1}{4}$$

$$x_3=x_4=\frac{1}{2}$$

试读版本仅供防疫期间线上教学使用

$$x_1 = x_2 = 1$$

$$\text{所以 } I_{\Phi(1)} = I_{\Phi(2)} > I_{\Phi(3)} = I_{\Phi(4)} > I_{\Phi(5)} = I_{\Phi(6)} = I_{\Phi(7)} = I_{\Phi(8)}$$

（3）用最小割集或最小径集进行结构重要度分析的 3 个公式。

公式一：

$$I_{\Phi(i)} = \frac{1}{k}\sum_{j=1}^{k}\frac{1}{n_j}\quad (j \in k_j) \tag{3-5}$$

式中　k——最小割集总数；

k_j——第 j 个最小割集；

n_j——第 k_j 个最小割集的基本事件数。

公式二：

$$I_{\Phi(i)} = \sum_{x_i \in k_j}\frac{1}{2^{n_j-1}} \tag{3-6}$$

式中　$n_j - 1$——为第 i 个基本事件所在 K_j 中各基本事件总数减 1；

$I_{\Phi(i)}$——第 i 个基本事件的结构重要度系数。

公式三：

$$I_{\Phi(i)} = 1 - \prod_{x_i \in k_j}\left(1 - \frac{1}{2^{n_j-1}}\right) \tag{3-7}$$

式中　$I_{\Phi(i)}$——第 i 个基本事件的结构重要度系数；

n_j——第 i 个基本事件所在 K_j 的基本事件总数；

$n_j - 1$——2 的指数。

【例 3-9】 已知某事故树的最小割集 $K_1 = \{x_1, x_2, x_3\}$，$K_2 = \{x_1, x_2, x_4\}$。利用上述 3 个近似式求 $I_{\Phi(i)}$。

解：（1）利用近似计算式（3-5）求解。

因为　$I_{\Phi(1)} = \frac{1}{k}\sum_{j=1}^{k}\frac{1}{n_j}\quad (j \in K_j)$

所以　$I_{\Phi(1)} = \frac{1}{2}\times\left(\frac{1}{3}+\frac{1}{3}\right) = \frac{1}{3}$

所以　$I_{\Phi(2)} = \frac{1}{2}\times\left(\frac{1}{3}+\frac{1}{3}\right) = \frac{1}{3}$

所以　$I_{\Phi(3)} = \frac{1}{2}\times\left(\frac{1}{3}+0\right) = \frac{1}{6}$

所以　$I_{\Phi(4)} = \frac{1}{2}\times\left(0+\frac{1}{3}\right) = \frac{1}{6}$

则各基本事件结构重要度序数排列如下：

所以　$I_{\Phi(1)} = I_{\Phi(2)} > I_{\Phi(3)} = I_{\Phi(4)}$

（2）利用式（3-6）求解。

因为　$I_{\Phi(i)} = \sum_{x_i \in k_j}\frac{1}{2^{n_j-1}}$

试读版本仅供防疫期间线上教学使用

所以　$I_{\Phi(1)}=\frac{1}{2^2}+\frac{1}{2^2}=\frac{1}{2}$

所以　$I_{\Phi(2)}=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$

所以　$I_{\Phi(3)}=\frac{1}{2^2}=\frac{1}{4}$

所以　$I_{\Phi(4)}=\frac{1}{4}$

故　$I_{\Phi(1)}=I_{\Phi(2)}>I_{\Phi(3)}=I_{\Phi(4)}$

（3）利用式（3-7）求解。

因为　$I_{\Phi(i)}=1-\prod_{x_i\in k_j}\left(1-\frac{1}{2^{n_j-1}}\right)$

所以　$I_{\Phi(1)}=I_{\Phi(2)}=1-\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{2^2}\right)=\frac{7}{16}$

所以　$I_{\Phi(3)}=I_{\Phi(4)}=1-\left(1-\frac{1}{2^2}\right)=\frac{1}{4}$

故　$I_{\Phi(1)}=I_{\Phi(2)}>I_{\Phi(3)}=I_{\Phi(4)}$

则此例用3个不同公式求出的排序结果一致。

【例3-10】 已知某事故树的最小割集 $K_1=\{x_1,x_2\}$，$K_2=\{x_3,x_4,x_5\}$，$K_3=\{x_3,x_4,x_6\}$。利用上述3个近似式求 $I_{\Phi(i)}$。

解：（1）利用近似计算式（3-5）求解。

因为　$I_{\Phi(1)}=\frac{1}{k}\sum_{j=1}^{k}\frac{1}{n_j}\quad(j\in K_j)$

所以　$I_{\Phi(1)}=I_{\Phi(2)}=\frac{1}{3}\times\frac{1}{2}=\frac{1}{6}$

所以　$I_{\Phi(3)}=I_{\Phi(4)}=\frac{1}{3}\times\left(\frac{1}{3}+\frac{1}{3}\right)=\frac{2}{9}$

所以　$I_{\Phi(5)}=I_{\Phi(6)}=\frac{1}{3}\times\frac{1}{3}=\frac{1}{9}$

则各基本事件结构重要度系数排列如下：

所以　$I_{\Phi(3)}=I_{\Phi(4)}>I_{\Phi(1)}=I_{\Phi(2)}>I_{\Phi(5)}=I_{\Phi(6)}$

（2）利用式（3-6）求解。

因为　$I_{\Phi(i)}=\sum_{x_i\in k_j}\frac{1}{2^{n_j-1}}$

试读版本仅供防疫期间线上教学使用

所以　$I_{\Phi(1)}=I_{\Phi(2)}=\frac{1}{2}$

所以　$I_{\Phi(3)}=I_{\Phi(4)}=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$

所以　$I_{\Phi(5)}=I_{\Phi(6)}=\frac{1}{2^2}=\frac{1}{4}$

故　$I_{\Phi(1)}=I_{\Phi(2)}=I_{\Phi(3)}=I_{\Phi(4)}>I_{\Phi(5)}=I_{\Phi(6)}$

（3）利用式（3-7）求解。

因为　$I_{\Phi(i)}=1-\prod_{x_i\in k_j}\left(1-\frac{1}{2^{n_j-1}}\right)$

所以　$I_{\Phi(1)}=I_{\Phi(2)}=1-\left(1-\frac{1}{2}\right)=\frac{1}{2}$

所以　$I_{\Phi(3)}=I_{\Phi(4)}=1-\left(1-\frac{1}{2^{3-1}}\right)\left(1-\frac{1}{2^{3-1}}\right)=\frac{7}{16}$

所以　$I_{\Phi(5)}=I_{\Phi(6)}=1-\left(1-\frac{1}{2^{3-1}}\right)=\frac{1}{4}$

故　$I_{\Phi(1)}=I_{\Phi(2)}>I_{\Phi(3)}=I_{\Phi(4)}>I_{\Phi(5)}=I_{\Phi(6)}$

则此例用3个不同公式求出的排序结果不一样，就其正确性（精度大小）而言，用式（3-7）求出的是正确的。

由上述两例计算可见，利用近似公式求解结构重要度排序时，可能出现误差。因此，在选公式时，应酌情选用。一般来说，对于最小割集中的基本事件个数（n_j）相同时，利用3个公式均可得到正确的排序；若最小割集（最小径集）间的阶数差别较大时，式（3-6）、式（3-7）就可以保证排列顺序的正确；若最小割集（最小径集）间的阶数差别仅为1或2阶时，使用式（3-5）、式（3-6）就可能产生较大的误差。在上述3个近似计算公式中，式（3-7）的所求结果的精度最高（说明：上述3个公式同样适用于最小径集，把 K_j 改成 P_j 即可）。

分析结构重要度，排出各种基本事件的结构重要度顺序，可以从结构上了解各基本事件对顶上事件的发生影响程度如何，以便按重要度顺序安排防护措施，加强控制，也可以依此顺序编写安全检查表。

（3）系统薄弱环节预测。对于最小割集来说，它与顶上事件用或门相连，显然最小割集的个数越少越安全，越多越危险。而每个最小割集中的基本事件与第二层事件用与门连接，因此割集中的基本事件越多越有利，基本事件少的割集就是系统的薄弱环节。对于最小径集来说，恰好与最小割集相反，径集数越多越安全，基本事件多的径集是系统的薄弱环节。

根据以上分析，可以从以下四种途径来改善系统的安全性：

1）减少最小割集数，首先应消除那些含基本事件最少的割集。

2）增加割集中的基本事件数，首先应给含基本事件少、又不能清除的割集增加基本

武汉轻工大学疫期网线上教学使用

事件。

3）增加新的最小径集，也可以设法将原有含基本事件较多的径集分成两个或多个径集。

4）减少径集中的基本事件数，首先应着眼于减少含基本事件多的径集。

总之，最小割集与最小径集在事故预测中的作用是不同的：最小割集可以预示出系统发生事故的途径，而最小径集却可以提供消灭顶上事件最经济、最省事的方案。

在对某一事故树做薄弱环节预测时，要区别不同情况，采取不同做法。

事故树中或门越多，得到的最小割集就越多，这个系统也就越不安全。对于这样的事故树最好从求最小径集着手，找出包含基本事件较多的最小径集，然后设法减少其基本事件树，或者增加最小径集数，以提高系统的安全程度。

事故树中与门越多，得到的最小割集的个数就较少，这个系统的安全性就越高。对于这样的事故树最好从求最小割集着手，找出少事件的最小割集，消除它或者设法增加它的基本事件数，以提高系统的安全性。

【例 3-11】 某触电伤亡事故树如图 3-34 所示，用事故树定性分析方法写出此事故树的所有最小割集和最小径集，并给出分析结论。

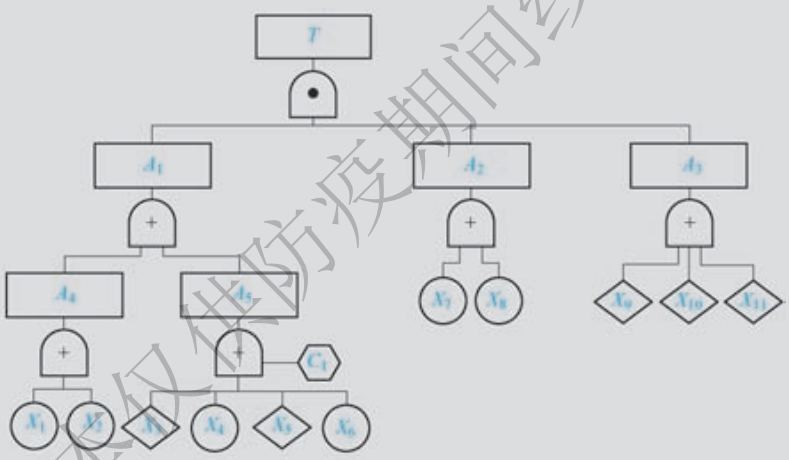

图 3-34　触电伤亡事故树

触电伤亡事故树的事件含义为：

T：触电伤亡；

A_1：设备及设施带电；　A_2：安全用具不起作用；　A_3：保护接地失效；

A_4：电源设施带电；　A_5：设备外壳带电；　X_1：开关漏电；

X_2：线路漏电；　X_3：热元件变形带电；　X_4：电动机漏电；

X_5：意外造成电源与设备相接；　X_6：控制电器漏电；

C_1：漏电保护失效；　X_7：没有使用；　X_8：因脏湿绝缘失效；

X_9：保护接地不合格；　X_{10}：接地不良；　X_{11}：未接地。

解： 事故树定性分析结果：

（1）全部最小割集见表 3-2。

试读版本仅供防疫期间线上教学使用

表 3-2 全部最小割集表

序 号	最 小 割 集	序 号	最 小 割 集
1	$\{X_1, X_7, X_9\}$	19	$\{C_1, X_7, X_9, X_3\}$
2	$\{X_2, X_7, X_9\}$	20	$\{X_1, X_8, X_9\}$
3	$\{X_1, X_7, X_{10}\}$	21	$\{X_1, X_7, X_{11}\}$
4	$\{C_1, X_8, X_9, X_3\}$	22	$\{C_1, X_7, X_{10}, X_3\}$
5	$\{C_1, X_7, X_{11}, X_3\}$	23	$\{C_1, X_7, X_9, X_4\}$
6	$\{C_1, X_7, X_9, X_5\}$	24	$\{C_1, X_7, X_9, X_6\}$
7	$\{X_2, X_8, X_9\}$	25	$\{X_2, X_7, X_{10}\}$
8	$\{X_2, X_7, X_{11}\}$	26	$\{X_1, X_8, X_{10}\}$
9	$\{X_1, X_8, X_{11}\}$	27	$\{C_1, X_8, X_{10}, X_3\}$
10	$\{C_1, X_8, X_{11}, X_3\}$	28	$\{C_1, X_8, X_9, X_4\}$
11	$\{C_1, X_8, X_9, X_5\}$	29	$\{C_1, X_8, X_9, X_6\}$
12	$\{C_1, X_7, X_{10}, X_4\}$	30	$\{C_1, X_7, X_{10}, X_5\}$
13	$\{C_1, X_7, X_{10}, X_6\}$	31	$\{C_1, X_7, X_{11}, X_4\}$
14	$\{C_1, X_7, X_{11}, X_5\}$	32	$\{C_1, X_7, X_{11}, X_6\}$
15	$\{X_2, X_8, X_{10}\}$	33	$\{X_2, X_8, X_{11}\}$
16	$\{C_1, X_8, X_{10}, X_4\}$	34	$\{C_1, X_8, X_{10}, X_5\}$
17	$\{C_1, X_8, X_{10}, X_6\}$	35	$\{C_1, X_8, X_{11}, X_4\}$
18	$\{C_1, X_8, X_{11}, X_5\}$	36	$\{C_1, X_8, X_{11}, X_6\}$

（2）全部最小径集见表 3-3。

表 3-3 全部最小径集表

序 号	最 小 径 集	序 号	最 小 径 集
1	$\{X_1, C_1, X_2\}$	3	$\{X_7, X_8\}$
2	$\{X_9, X_{10}, X_{11}\}$	4	$\{X_1, X_2, X_3, X_4, X_5, X_6\}$

（3）基本事件结构重要度近似值见表 3-4。

表 3-4 基本事件结构重要度近似值

事 件	结构重要度近似值	事 件	结构重要度近似值
C_1	0.959431	X_6	0.551205
X_1	0.822021	X_7	0.964152
X_2	0.822021	X_8	0.964152
X_3	0.551205	X_9	0.891280
X_4	0.551205	X_{10}	0.891280
X_5	0.551205	X_{11}	0.891280

试读版本仅供防疫期间线上教学使用

（4）分析结论。

1）从事故树的结构上看，“或门”比较多，说明在人员操作不当或者设备连接不好或者设备质量不良的情况下，触电事故很容易发生。

2）从事故树的最小割集和最小径集看，割集数目很大，最小径集数目小，也说明触电事故容易发生，同时预防的途径较少。

3）从结构重要度上看，C_1、X_7、X_8 的系数最大，其次是 X_9、X_{10}、X_{11}，说明要预防触电事故，应重点预防 C_1、X_7、X_8 和 X_9、X_{10}、X_{11}。即电气设备一定要良好接地，保持干净，而且漏电保护装置要良好。

3.2.9　事故树定量分析

事故树定量分析是在定性分析的基础上进行的。定量分析有两个目的，首先是在求出各基本事件概率的情况下，计算顶上事件的发生概率，并根据所获得的结果与预定的目标进行比较。如果事故的发生概率及其造成的损失为社会所认可，则不必投入更多的人力、物力进一步治理。如果超出了目标值，就应采取必要的系统改进措施，使其降至目标值以下。

另一个目的是，计算出概率重要系数和临界重要系数。以便了解改善系统应从何处入手，以及根据重要程度的不同，按轻重缓急安排人力、物力，分别采取对策，或按主次顺序编制安全检查表，以加强人的控制，使系统处于最佳安全状态。

1. 基本事件的发生概率

研究基本事件的发生概率，是为了对事故树进行定量分析。通过定量分析，使人们得出能够比较的概念，为系统安全评价提供必要的数据，为选择最优安全措施提供依据。

进行定量分析，首先要知道系统各元件发生故障的频率或概率。基本事件发生概率主要包括物的故障系数和人的失误概率两个方面。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。所以，从应用角度来看，频率比概率更有用，它可以从所积累的比较多的统计资料中得到。需要指出的是，用频率代替概率，并不否认概率能更精确、更全面地反映事件出现可能性的大小，只是由于在目前的条件下，取得概率比取得频率更为困难。所以，我们才用频率代替概率，以计算概率的方法来计算频率。

（1）物的故障概率。要计算物的故障概率，首先必须取得物的故障率。所谓物的故障率，是指设备或系统的单元（部件或元件）工作时间的单位时间（或周期）的失效或故障的概率，它是单元平均故障间隔期 $\overline{T}$ 的倒数，若物的故障率为 λ，则有：

$$\lambda = \frac{1}{\overline{T}}$$

$\overline{T}$ 一般由厂家给出，或通过实验室得出。它是元件从运行到故障发生时所经历时间 t_i 的算术平均值，即：

$$\overline{T} = \frac{\sum_{i=1}^{n} t_i}{n}$$

式中　n——所测元件的个数。

试读版本仅供防疫期间线上教学使用

若元件在实验室条件下测出的故障率为 λ_0，亦即故障率数据库储存的数据。实际应用时，还必须考虑比实验室条件恶劣的现场因素，适当选择使用条件系数 K 值。那么，实际使用的故障率为：

$$\lambda = K\lambda_0$$

有了故障率，就可以计算元件的故障发生概率 q。对一般可修复系统，即系统故障修复后仍投入正常运行的系统，单元的故障发生概率为：

$$q = \frac{\lambda}{\lambda + \mu} \tag{3-8}$$

式中 μ——可维修度。

可维修度是反映单元维修难易程度的量度，是所需平均修复时间 τ（从故障发生到投入运行的平均时间）的倒数，即 $\mu = \frac{1}{\tau}$，因为 $\overline{T} \propto \tau$，故 $\lambda \propto \mu$，所以：

$$q = \frac{\lambda}{\lambda + \mu} \approx \frac{\lambda}{\mu} = \lambda\tau \tag{3-9}$$

因此，单元的故障发生率近似为，单元故障率与单元平均修复时间的积。

对一般不可修复系统，即使用一次就报废的系统，如水雷、导弹等系统，单元的故障发生概率为：

$$q = 1 - e^{-\lambda t} \tag{3-10}$$

式中 t——元件的运行时间。

如果把 $e^{-\lambda t}$ 按无穷级数展开，略去后面的高阶无穷小，则：

$$q \approx \lambda t \tag{3-11}$$

现在，许多工业发达的国家都建立了故障率数据库，而且若干国家，如北美和西欧某些国家已联合建库，用计算机存储和检索，为系统安全和可靠性分析提供了良好的条件。从我国开展安全系统工程和可靠性工程的发展趋势看，也应该建立数据库，储存事故资料。

但是，安全系统工程的应用，事故树分析的应用，并不是从建立故障率数据库才开始的，我们现在所面临的是在没有数据库的情况下来评价故障率，这就存在如何求取故障率的问题。

在目前情况下，可以通过长期的运行经验，或若干系统平行的运行过程，粗略地估计元件平均故障间隔期，其倒数就是所观测对象的故障率。例如，某元件现场使用条件下的平均故障率间隔期为 4000h，则其故障率为 2.5×10^{-4}/h。若系统运行是周期性的，亦可将周期化为小时。

在事故树分析中，对于维修比较简单的单元，可近似地用故障率代替故障发生概率。

（2）人的失误概率。人的失误是另一种基本事件。人的失误大概有以下五种情况：

1）忘记做某项工作。

2）做错了某项工作。

3）采取了不应采取的某项步骤。

4）没有按规定完成某项工作。

5）没有在预定时间内完成某项工作。

人的失误原因特别复杂，因此，估算人的失误概率非常困难，许多专家进行了大量的研

试读版本仅供防疫期间线上教学使用

究，但目前还没有较好地确定人的失误率的方法。1961 年，斯温（Swain）和罗克（Rock）曾提出了“人的失误率预测法”（THERP），这是一种比较常见的方法，这种方法的分析步骤如下：

1）调查被分析者的操作程序。

2）把整个程序分成各个操作步骤。

3）把操作步骤再分成单个动作。

4）根据经验或实验得出每个动作的可靠度。

5）求出各个动作的可靠度之积。得到每个操作步骤的可靠度。如果各个动作有相容事件，则按条件概率计算。

6）求出各操作步骤的可靠度之积，得到整个程序的可靠度。

7）求出整个程序的不可靠度（1 减可靠度），便得到进行事故树分析（FTA）所需要的人的失误概率。

人的失误概率受多种因素影响，如作业的紧迫程度、单调性、不安全感，人的生理状况，教育、训练情况，以及社会影响和环境因素等。因此，仍然需要用修正系数 K 修正人的失误概率。

R. L. 布朗宁经过大量的观测研究后认为，人员进行重复操作时，失误率为 $1\times10^{-3}\sim1\times10^{-2}$，并推荐取 1×10^{-2}。

2. 顶上事件发生概率的计算

已知各基本事件的发生概率，若各基本事件又是独立事件时，就可以计算顶上事件的发生概率。目前，计算顶上事件发生概率的方法有若干种，下面介绍较简单的几种。

（1）求事故树的基本事件概率积之和。顶上事件状态 $\Phi(X)=1$ 的所有基本事件的状态组合，求各个基本事件状态（$X_i=1$ 或 0）的概率积之和，用公式表达为：

$$Q=\sum\Phi(X)\prod_{i=1}^{n}q_i^{X_i}(1-q_i)^{1-X_i} \tag{3-12}$$

式中　Q——顶上事件发生概率函数；

$\Phi(X)$——顶上事件状态值，$\Phi(X)=0$ 或 $\Phi(X)=1$；

$\sum$——求 n 个事件的概率积；

X_i——第 i 个基本事件的状态值，$X_i=0$ 或 $X_i=1$；

q_i——第 i 个基本事件的发生概率。

以图 3-35 的简单事故树为例，利用式（3-12）求顶上事件 T 的发生概率。

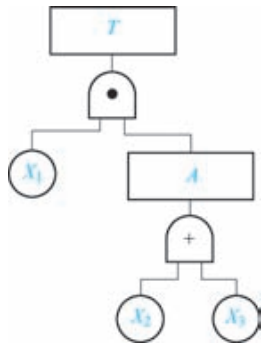

图 3-35　事故树示意图

设 X_1、X_2、X_3 均为独立事件，其概率均为 0.1，顶上事件的发生概率为：

$$\begin{aligned}Q&=\sum\Phi(X)\prod_{i=1}^{n}q_i^{X_i}(1-q_i)^{1-X_i}\\&=1\times q_1^1(1-q_1)^0q_2^0(1-q_2)^1q_3^1(1-q_3)^0+\\&\quad 1\times q_1^1(1-q_1)^0q_2^1(1-q_2)^0q_3^0(1-q_3)^1+\\&\quad 1\times q_1^1(1-q_1)^0q_2^1(1-q_2)^0q_3^1(1-q_3)^0\\&=q_1(1-q_2)q_3+q_1q_2(1-q_3)+q_1q_2q_3\\&=0.1\times0.9\times0.1+0.1\times0.1\times0.9+0.1\times0.1\times0.1\end{aligned}$$

试读版本仅供预览期间线上教学使用

$$=0.009+0.009+0.001$$

$$=0.019$$

这种计算方法具有较强的规律性，可用计算机编制程序进行计算。但当事故树的基本事件很多时，这种算法，即使是用计算机也难以胜任了。

（2）求各基本事件概率和。在定性分析中，给出了最小割集的求法，以及用最小割集表示的事故树等效图，利用等效图再来推出最小割集求顶上事件发生概率的公式。

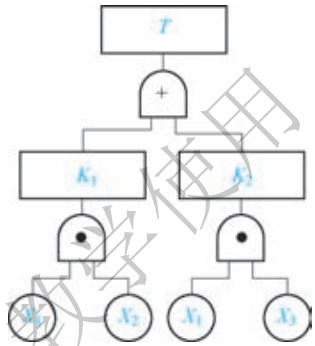

图 3-36　用最小割集表示的图 3-35 事故树等效图

仍以图 3-35 简单事故树示意图为例，其最小割集为 $\{X_1, X_2\}$、$\{X_1, X_3\}$，用最小割集表示的等效图如图 3-36 所示。这样可以把其看作由事件 K_1、K_2 组成的事故树。按照求概率和的计算公式，K_1+K_2 的概率为：

$$Q=1-(1-q_{K_1})(1-q_{K_2}) \tag{3-13}$$

因为两个最小割集中都有 X_1，利用此式直接代入进行概率计算，必然造成重复计算 X_1 的发生概率。因此，要将上式展开，消去其中重复的概率因子，否则将得出错误的结果。由于

$$\begin{aligned} Q &= 1-(1-q_{K_1})(1-q_{K_2}) \\ &= 1-1+q_{K_1}+q_{K_2}-q_{K_1}q_{K_2} \\ &= q_{K_1}+q_{K_2}-q_{K_1}q_{K_2} \end{aligned}$$

而

$$q_{K_1}=q_1q_2=0.1\times0.1=0.01$$

$$q_{K_2}=q_1q_3=0.1\times0.1=0.01$$

$$q_{K_1}q_{K_2}=q_1q_2q_3=0.1\times0.1\times0.1=0.001$$

故：

$$Q=0.01+0.01-0.001=0.019$$

以上两种方法计算结果是一致的。

（3）直接分步算法。对给定的事故树，若已知其结构函数和基本事件的发生概率，从原则上来讲，应用容斥原理中的逻辑加与逻辑乘的概率计算公式就可以求得顶上事件发生的概率。

设基本事件 X_1，X_2，…，X_n 的发生概率分别为 q_1，q_2，…，q_n，则这些事件的逻辑加与逻辑乘的故障计算公式如下。

逻辑加（或门连接的事件）的概率计算公式：

$$\begin{aligned} &g(X_1\cup X_2\cup\cdots\cup X_n) \\ &=1-(1-q_1)(1-q_2)\cdots(1-q_n) \\ &=1-\prod_{i=1}^{n}(1-q_i)=P_0 \end{aligned} \tag{3-14}$$

式中　g——顶上事件（或门事件）发生的概率函数；

P_0——或门事件的概率；

q_i——第 i 个基本事件的概率；

n——基本事件数。

试读版本仅供防疫期间线上教学使用

逻辑乘（与门连接的事件）的概率计算公式：

$$g(X_1 \cap X_2 \cap \cdots \cap X_n) = q_1 q_2 \cdots q_n = \prod_{i=1}^{n} q_i = P_A \tag{3-15}$$

式中　P_A——与门事件的概率；

其他符号同上。

直接分步算法适于事故树规模不大，而且事故树中无重复事件时使用。从底部的门事件算起，逐次向上推移，至算到顶上事件为止。

【例 3-12】 如图 3-37 所示的事故树，已知各基本事件的概率，求顶上事件发生的概率。$q_1 = 0.01$，$q_2 = 0.01$，$q_3 = 0.02$，$q_4 = 0.02$，$q_5 = 0.03$，$q_6 = 0.03$，$q_7 = 0.04$，$q_8 = 0.04$。

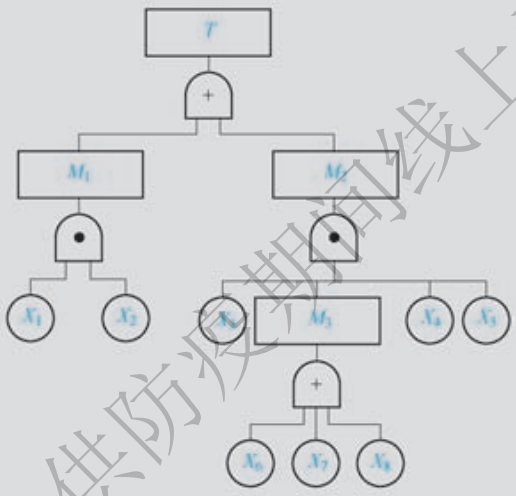

图 3-37　某事故树图

解：（1）先求 M_3 的概率，因为是或门连接，故按式（3-14）求得：

$$P_{M_3} = 1 - (1 - 0.03)(1 - 0.04)(1 - 0.04) = 1 - 0.839395 = 0.10605$$

（2）求 M_2 的概率，因为是与门连接，按式（3-15）求得：

$$P_{M_2} = 0.02 \times 0.10605 \times 0.02 \times 0.03 = 0.00000127$$

（3）求 M_1 的概率，因为是与门连接，按式（3-15）求得：

$$P_{M_1} = 0.01 \times 0.01 = 0.0001$$

（4）求 T 的概率，因为是或门连接，故按式（3-14）求得：

$$P_T = 1 - (1 - 0.001)(1 - 0.00000127) = 0.001$$

（4）利用最小割集计算顶上事件发生的概率。如果各最小割集中彼此没有重复的基本事件，则可以先求各个最小割集的概率，即最小割集所包含的基本事件的交（逻辑与）集，然后求所有最小割集的并（逻辑或）集概率，即得顶上事件的发生概率。

由于与门的结构函数为：

试读版本仅供防疫期间线上教学使用

$$\Phi(X)=\bigcap_{i=1}^{n}x_i=\prod_{i=1}^{n}x_i \tag{3-16}$$

或门的结构函数为：

$$\Phi(X)=1-\prod_{i=1}^{n}(1-x_i)=\bigcup_{i=1}^{n}x_i \tag{3-17}$$

式中 x_i——第 i 个基本事件；

n——基本事件数。

根据最小割集的定义，如果在割集中任意去掉一个基本事件，就不成为割集。换句话说，也就是要求最小割集中全部基本事件都发生，该最小割集才存在，即：

$$G_r=\bigcap_{i\in G_r}x_i \tag{3-18}$$

式中 G_r——第 r 个最小割集（$r=1,2,3,\cdots,n$）；

x_i——第 i 个最小割集中的基本事件。

在事故树中，一般有多个最小割集，只要存在一个最小割集，顶上事件就会发生，因此，事故树的结构函数为：

$$\Phi(X)=\bigcup_{r=1}^{N_G}G_r=\bigcup_{r=1}^{N_G}\bigcap_{i\in G_r}x_i \tag{3-19}$$

式中 N_G——系统中最小割集数；

其他符号意义同前。

因此，若各个最小割集中彼此没有重复的基本事件，可按下式计算顶上事件的发生概率：

$$g=\bigcup_{r=1}^{N_G}\prod_{x_i\in G_r}q_i \tag{3-20}$$

式中 N_G——系统中最小割集数；

r——最小割集数序数；

i——基本事件序数；

$x_i\in G_r$——第 i 个基本事件属于第 r 个最小割集；

q_i——第 i 个基本事件的概率。

【例 3-13】 设某事故有三个最小割集：$\{X_1,X_2\}$，$\{X_3,X_4,X_5\}$，$\{X_6,X_7\}$。各基本事件发生概率分别为：q_1，q_2，q_3，…，q_7，求顶上事件发生概率。

解： 根据事故树的三个最小割集，可做出用最小割集表示的等效图（见图 3-38）。

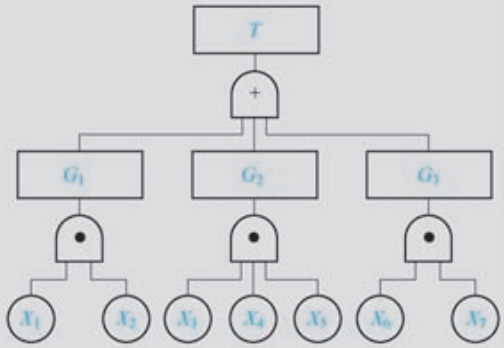

图 3-38 用最小割集表示的等效图

试读版本仅供防疫期间线上教学使用

3 个最小割集的概率，可由各个最小割集所包含的基本事件的逻辑与分别求出：

$$q_{G_1}=q_1q_2,\quad q_{G_2}=q_3q_4q_5,\quad q_{G_3}=q_6q_7$$

顶上事件的发生概率，即求所有最小割集的逻辑或，得：

$$\begin{aligned}g&=1-(1-q_{G_1})(1-q_{G_2})(1-q_{G_3})\\&=1-(1-q_1q_2)(1-q_3q_4q_5)(1-q_6q_7)\end{aligned}$$

从结果可看出，顶上事件发生概率等于各个最小割集的概率积的和。

用式（3-20）计算事故树顶上事件的概率，要求各最小割集中没有重复的基本事件，也就是最小割集之间是完全不相交的。若事故树各基本事件中有重复事件，则上式不成立。

例如：某事故树共有 3 个最小割集，分别为：

$$G_1=\{x_1,x_2\},G_2=\{x_2,x_3,x_4\},G_3=\{x_2,x_5\}$$

则该事故树的结构函数式为：

$$\begin{aligned}T&=G_1+G_2+G_3\\&=x_1x_2+x_2x_3x_4+x_2x_5\end{aligned}$$

顶上事件发生概率为：

$$\begin{aligned}g&=q(G_1+G_2+G_3)\\&=1-(1-q_{G1})(1-q_{G2})(1-q_{G3})\\&=(q_{G1}+q_{G2}+q_{G3})-(q_{G1}q_{G2}+q_{G1}q_{G3}+q_{G2}q_{G3})+q_{G1}q_{G2}q_{G3}\end{aligned}$$

式中，$q_{G1}q_{G2}$是 G_1G_2 交集的概率，即 $x_1x_2x_2x_3x_4$，根据布尔代数等幂律，有：

$$x_1x_2x_2x_3x_4=x_1x_2x_3x_4$$

故：

$$q_{G1}q_{G2}=q_1q_2q_3q_4$$

同理：

$$q_{G1}q_{G3}=q_1q_2q_5$$

$$q_{G2}q_{G3}=q_2q_3q_4q_5$$

$$q_{G1}q_{G2}q_{G3}=q_1q_2q_3q_4q_5$$

所以顶上事件的发生概率为：

$$g=(q_1q_2+q_2q_3q_4+q_2q_5)-(q_1q_2q_3q_4+q_1q_2q_5+q_2q_3q_4q_5)+q_1q_2q_3q_4q_5$$

由此，若最小割集中有重复事件时，必须将式（3-20）展开，用布尔代数消除每个概率积中的重复事件得：

$$g=\sum_{r=1}^{N_G}\prod_{x_i\in G_r}q_i-\sum_{1\leqslant r<s\leqslant N_G}\prod_{x_i\in G_r\cup G_s}q_i+\cdots+(-1)^{N_G-1}\prod_{r=1}^{N_G}q_i \tag{3-21}$$

式中　r，s——最小割集序数；

$\sum_{r=1}^{N_G}$——求 N_G 项代数和；

$x_i\in G_r$——属于第 r 个最小割集的第 i 个基本事件；

$\sum_{1\leqslant r<s\leqslant N_G}\prod_{x_i\in G_r\cup G_s}$——属于任意两个不同最小割集的基本事件概率和的代数和；

试读版本仅供防疫期间线上教学使用

$x_i \in G_r \cup G_s$——第 i 个基本事件或属于第 r 个最小割集，或属于第 s 个最小割集；

$1 \leqslant r < s \leqslant N_G$——任意两个最小割集的组合顺序。

（5）利用最小径集计算顶上事件发生的概率。如果各最小径集中彼此没有重复的基本事件，则可以先求各个最小径集的概率，即最小径集所包含的基本事件的并（逻辑或）集的概率，然后求所有最小径集的交（逻辑与）集概率，即得顶上事件的发生概率。因此可按下式计算：

$$g = \prod_{r=1}^{N_P} \bigcup_{x_i \in P_r} q_i = \prod_{r=1}^{N_P} \left[1 - \bigcap_{x_i \in P_r} (1 - q_i)\right] \tag{3-22}$$

式中　N_P——系统中最小径集数；

r——最小径集序数；

i——基本事件序数；

$x_i \in P_r$——第 i 个基本事件属于第 r 个最小径集；

q_i——第 i 个基本事件的概率。

【例 3-14】 设某事故树有三个最小径集：$P_1 = \{x_1, x_2\}$，$P_2 = \{x_3, x_4, x_5\}$，$P_3 = \{x_6, x_7\}$。各基本事件发生的概率分别为：q_1，q_2，…，q_7，求顶上事件发生的概率。

解： 根据事故树的三个最小径集，做出用最小径集表示的等效图，如图 3-39 所示。

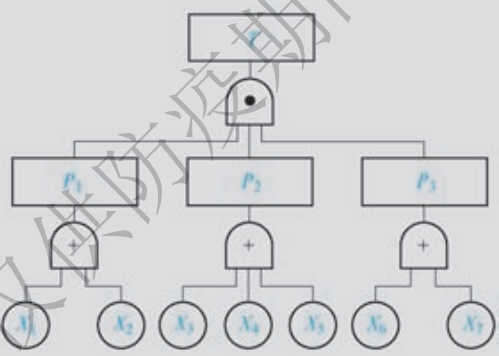

图 3-39　用最小径集表示的等效图

三个最小径集的概率，可由各个最小径集所包含的基本事件的逻辑或分别求出：

$$q_{p_1} = 1 - (1 - q_1)(1 - q_2)$$

$$q_{p_2} = 1 - (1 - q_3)(1 - q_4)(1 - q_5)$$

$$q_{p_3} = 1 - (1 - q_6)(1 - q_7)$$

顶上事件的发生概率，即求所有最小径集的逻辑与，得：

$$g = [1 - (1 - q_1)(1 - q_2)][1 - (1 - q_3)(1 - q_4)(1 - q_5)][1 - (1 - q_6)(1 - q_7)]$$

用式（3-22）计算任意一个事故树顶上事件的发生概率时，要求各最小径集中没有重复的基本事件，也就是最小径集之间是完全不相交的。

如果事故树中各最小径集中彼此有重复事件，则式（3-22）不成立，需要将式（3-22）展开，消去概率积中基本事件 x_i 不发生概率（$1 - q_i$）的重复事件，即：

试读版本仅供防疫期间线上教学使用

$$g=1-\sum_{r=1}^{N_P}\prod_{x_i\in P_r}(1-q_i)+\sum_{1\leqslant r<s\leqslant N_P}\prod_{x_i\in P_r\cup P_s}(1-q_i)-\cdots+(-1)^{N_P-1}\prod_{\substack{r=1\\x_i\in p_r}}^{N_P}(1-q_i)\quad(3\text{-}23)$$

式中符号同前。

【例 3-15】　某事故树共有三个最小径集：$P_1=\{x_1,x_2\}$，$P_2=\{x_2,x_3\}$，$P_3=\{x_2,x_4\}$。各基本事件发生的概率分别为：q_1，q_2，q_3，q_4，求顶上事件发生的概率。

解： 根据题意，可写出其结构函数式为：

$$T=P_1P_2P_3=(x_1+x_2)(x_2+x_3)(x_2+x_4)$$

顶上事件发生的概率为：

$$g=q(P_1P_2P_3)=[1-(1-q_1)(1-q_2)][1-(1-q_2)(1-q_3)][1-(1-q_2)(1-q_4)]$$

将上式进一步展开得：

$$\begin{aligned}g=&1-(1-q_1)(1-q_2)-(1-q_2)(1-q_3)+(1-q_1)(1-q_2)(1-q_2)(1-q_3)-\\&(1-q_2)(1-q_4)+(1-q_1)(1-q_2)(1-q_2)(1-q_4)+(1-q_2)(1-q_3)\\&(1-q_2)(1-q_4)-(1-q_1)(1-q_2)(1-q_2)(1-q_3)(1-q_2)(1-q_4)\end{aligned}$$

根据等幂律：

$$x_ix_i=x_i$$

所以：

$$(1-q_i)(1-q_i)=(1-q_i)$$

整理上式得：

$$\begin{aligned}g=&1-[(1-q_1)(1-q_2)+(1-q_2)(1-q_3)+(1-q_2)(1-q_4)]+\\&[(1-q_1)(1-q_2)(1-q_3)+(1-q_1)(1-q_2)(1-q_4)+\\&(1-q_2)(1-q_3)(1-q_4)]-(1-q_1)(1-q_2)(1-q_3)(1-q_4)\end{aligned}$$

（6）顶上事件发生概率的近似计算。

在事故树分析时，往往遇到很复杂很庞大的事故树，有时一棵事故树牵扯成百上千个基本事件，要精确求出顶上事件的发生概率，需要相当大的人力和物力。因此，需要找出一种简便方法，它既能保证必要的精确度，又能较为省力地算出结果。

实际上，即使精确算出的结果也未必十分精确，这是因为：①凭经验给出的各种机械部件的故障率本身就是一种估计值，肯定存在误差；②各种机械部件的运行条件（满负荷或非满负荷运行）、运行环境（温度、湿度、粉尘、腐蚀等）各不相同，它们必然影响着故障率的变化；③人的失误率受多种因素影响，如心理、生理、个人的智能、训练情况、环境因素等，这是一个经常变化、伸缩性很大的数据。

因此，对这些数据进行运算，必然得出不太精确的结果。所以，我们赞成用近似计算的办法求顶上事件的发生概率。实际上，至今所有报道事故树分析实用的文献，都是采用近似计算的方法。尤其是在许多技术参数难以确认取值的情况下，这是一种值得提倡的方法。

另外，在求近似值的过程中，略去的数值与有效数字的最后一位相比，相差很大，有时相差几个数量级，完全可以忽略不计。

课程资源仅供防疫期间线上教学使用

近似算法是利用最小割集计算顶上事件发生概率的公式得到的。一般情况下，可以假定所有基本事件都是统计独立的，因而每个割集也是统计独立的。下面介绍两种常用的近似算法的公式。

设有某事故树的最小割集等效树如图 3-40 所示。

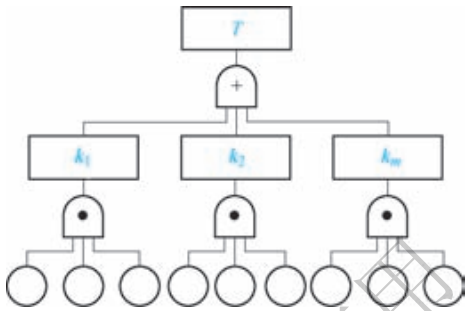

图 3-40　某事故树最小割集等效图

顶上事件与割集的逻辑关系为：$T=k_1+k_2+\cdots+k_m$。顶上事件 T 发生的概率为 q，割集 k_1，k_2，…，k_m 的发生概率分别为 q_{k_1}，q_{k_2}，…，q_{k_m}，由独立事件的概率和概率积的公式分别得：

$$\begin{aligned}q(k_1+k_2+\cdots+k_m)&=1-(1-q_{k_1})(1-q_{k_2})\cdots(1-q_{k_m})\\&=(q_{k_1}+q_{k_2}+\cdots+q_{k_m})-(q_{k_1}q_{k_2}+q_{k_2}q_{k_3}+\cdots+q_{k_{(m-1)}}q_{k_m})+\\&\quad(q_{k_1}q_{k_2}q_{k_3}+\cdots+q_{k_{(m-2)}}q_{k_{(m-1)}}q_{k_m})-\cdots+(-1)^{m-1}q_{k_1}q_{k_2}\cdots q_{k_m}\end{aligned}$$

事故树顶上事件发生的概率，按式（3-21）计算收敛得非常快，（2^{N_G-1}）项的代数和中主要起作用的是首项与第二项，后面一些项数值极小。只取第一个小括号中的项，将其余的二次项、三次项等全都舍弃，则得顶上事件发生概率近似公式即首项近似公式：

$$Q\approx q_{k_1}+q_{k_2}+\cdots+q_{k_m}$$

这样，顶上事件发生概率近似等于各最小割集发生概率之和。

1）首项近似法。根据利用最小割集计算顶上事件发生概率的式（3-21），设：

$$\sum_{r=1}^{N_G}\prod_{x_i\in G_r}q_i=F_1$$

$$\sum_{1\leqslant r<s\leqslant N_G}\prod_{x_i\in G_r\cup G_s}q_i=F_i$$

$$\vdots$$

$$\prod_{r=1}^{N_G}q_i=F_{N_G}$$

则式（3-21）可改写为：

$$g=F_1-F_2+\cdots+(-1)^{N_G-1}F_{N_G}$$

逐次求出 F_1，F_2，…，F_{N_G}的值，当认为满足计算精确度时就可以停止计算。通常 $F_1\geqslant F_2$，$F_2\geqslant F_3$，…，在近似计算时往往求出 F_1 就能满足要求，即：

$$g\approx F_1=\sum_{r=1}^{N_G}\prod_{x_i\in G_r}q_i \tag{3-24}$$

该式说明，顶上事件发生概率近似等于所有最小割集发生概率的代数和。

仍以图 3-35 简单事故树为例，其最小割集的等效图如图 3-36 所示。图中基本事件 X_1，X_2，X_3 的发生概率分别为 $q_1=q_2=q_3=0.1$，用近似公式计算顶上事件发生概率：

$$Q=q_{k_1}+q_{k_2}=q_1q_2+q_1q_3=0.1\times0.1+0.1\times0.1=0.02$$

直接用原事故树的结构函数求顶上事件发生概率：

因为

$$T=X_1(X_2+X_3)$$

试读版本仅供预览，请购买上教学使用

则

$$Q' = q_1[1-(1-q_2)(1-q_3)] = 0.1\times[1-(1-0.1)(1-0.1)] = 0.019$$

Q 与 Q' 相比，相差 0.001。因此，在计算顶上事件发生的概率时，按简化后的等效图计算才是正确的。

2）平均近似法。有时为了提高计算精度，取首项与第二项之半的差作为近似值：

$$g \approx F_1 - \frac{1}{2}F_2 \tag{3-25}$$

在利用式（3-21）计算顶上事件发生概率值过程中，可以得到一系列判别式：

$$g \leqslant F_1$$
$$g \geqslant F_1 - F_2$$
$$g \leqslant F_1 - F_2 + F_3$$
$$\cdots\cdots$$

因此，F_1，F_1-F_2，$F_1-F_2+F_3$，…，顺序给出了顶上事件发生概率的近似上限与下限。

$$F_1 > g > F_1 - F_2$$
$$F_1 - F_2 + F_3 > g > F_1 - F_2$$
$$\cdots\cdots$$

这样经过上下限的计算，便能得出精确的概率值。一般当基本事件发生概率值 $q_1 < 0.01$ 时，采用 $g = F_1 - \frac{1}{2}F_2$ 就可以得到较为精确的近似值。

【例 3-16】 某事故树如图 3-41 所示，已知 $q_1 = q_2 = 0.2$，$q_3 = q_4 = 0.3$，$q_5 = 0.25$。其顶上事件发生的概率为 0.1323。现试用式（3-24）和式（3-25）求该事故树顶上事件发生概率的近似值。

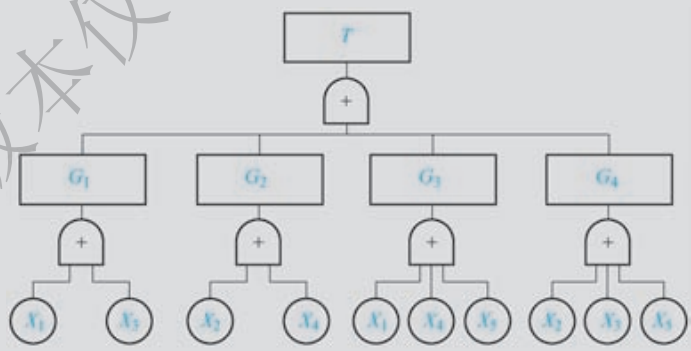

图 3-41　事故树示意图

解： 根据式（3-24）有：

$$g \approx \sum_{r=1}^{N_G}\prod_{x_i\in G_r} q_i = q_1q_3 + q_2q_4 + q_1q_4q_5 + q_2q_3q_5$$
$$= 0.2\times0.3 + 0.2\times0.3 + 0.2\times0.3\times0.25 + 0.2\times0.3\times0.25$$
$$= 0.15$$

试读版本仅供防疫期间线上教学使用

其相对误差：

$$\varepsilon_1 = \frac{0.1323 - 0.15}{0.1323} \times 100\% = -13.4\%$$

由于：

$$F_2 = q_{G_1}q_{G_2} + q_{G_1}q_{G_3} + q_{G_1}q_{G_4} + q_{G_2}q_{G_3} + q_{G_2}q_{G_4} + q_{G_3}q_{G_4} = 0.007425$$

根据式（3-25）有：

$$\begin{aligned} g &\approx F_1 - \frac{1}{2}F_2 \\ &= 0.15 - 0.0037125 \\ &= 0.1463 \end{aligned}$$

其相对误差：

$$\varepsilon_2 = \frac{0.1323 - 0.1463}{0.1323} \times 100\% = -10.6\%$$

该事故树的基本故障率是相当高的，计算结果误差尚且不大，若基本事件故障率降低后，相对误差会大大地减少，一般能满足工程应用的要求。

3. 概率重要度分析

结构重要度分析是从事故树的结构上分析各基本事件的重要程度。如果进一步考虑基本事件发生概率的变化会给顶上事件发生概率以多大影响，就要分析基本事件的概率重要度。利用顶上事件发生概率 Q 函数是一个多重线性函数这一性质，只要对自变量 q_i 求一次偏导数，就可得出该基本事件的概率重要度系数：

$$I_{q(i)} = \frac{\partial Q}{\partial q_i} \tag{3-26}$$

当利用上式求出各基本事件的概率重要度系数后，就可以了解诸多基本事件，减少哪个基本事件的发生概率可以有效地降低顶上事件的发生概率，这一点，可以通过下例看出。

【例 3-17】 设事故树最小割集为 $\{X_1, X_3\}$、$\{X_1, X_5\}$、$\{X_3, X_4\}$、$\{X_2, X_4, X_5\}$。各基本事件概率分别为：$q_1 = 0.01$，$q_2 = 0.02$，$q_3 = 0.03$，$q_4 = 0.04$，$q_5 = 0.05$，求各基本事件概率重要度系数。

解： 顶上事件发生概率 Q 用近似方法计算时：

$$\begin{aligned} Q &= q_{k_1} + q_{k_2} + q_{k_3} + q_{k_4} \\ &= q_1q_3 + q_1q_5 + q_3q_4 + q_2q_4q_5 \\ &= 0.01 \times 0.03 + 0.01 \times 0.05 + 0.03 \times 0.04 + 0.02 \times 0.04 \times 0.05 \\ &= 0.002 \end{aligned}$$

各个基本事件的概率重要度系数为：

$$I_{q(1)} = \frac{\partial Q}{\partial q_1} = q_3 + q_5 = 0.08$$

试读版本仅供防疫期间线上教学使用

$$I_{q(2)}=\frac{\partial Q}{\partial q_2}=q_4q_5=0.002$$

$$I_{q(3)}=\frac{\partial Q}{\partial q_3}=q_1+q_4=0.05$$

$$I_{q(4)}=\frac{\partial Q}{\partial q_4}=q_3+q_2q_5=0.031$$

$$I_{q(5)}=\frac{\partial Q}{\partial q_5}=q_1+q_2q_4=0.0108$$

这样，就可以按概率重要度系数的大小排出各基本事件的概率重要度顺序：

$$I_{q(1)}>I_{q(3)}>I_{q(4)}>I_{q(5)}>I_{q(2)}$$

这就是说，减小基本事件 X_1 的发生概率能使顶上事件的发生概率迅速降下来，它比按同样数值减小其他任何基本事件的发生概率都有效。其次是基本事件 X_3，X_4，X_5，最不敏感的是基本事件 X_2。

从概率重要度系数的算法可以看出这样的事实：一个基本事件的概率重要度如何，并不取决于它本身的概率值大小，而取决于它所在最小割集中其他基本事件的概率积的大小及它在各个最小割集中重复出现的次数。

4. 临界重要度分析

一般情况，减少概率大的基本事件的概率要比减少概率小的容易，而概率重要度系数并未反映这一事实，因此，它不是从本质上反映各基本事件在事故树中的重要程度。而临界重要度系数 I_{C_i} 则是从敏感度和概率双重角度衡量各基本事件的重要度标准，其定义式为：

$$I_{C_i}=\frac{\partial Q/\partial q_i}{Q/q_i} \tag{3-27}$$

它与概率重要度系数的关系是：

$$I_{C_i}=\frac{q_i}{Q}I_{q(i)} \tag{3-28}$$

上面例子已得到的某事故树顶上事件概率为 0.002，各基本事件的概率重要度系数分别为：

$I_{q(1)}=0.08$，$I_{q(2)}=0.002$，$I_{q(3)}=0.05$，$I_{q(4)}=0.031$，$I_{q(5)}=0.0108$

则各基本事件的临界重要度系数为：

$$I_{C_1}=\frac{q_1}{Q}I_{q(1)}=\frac{0.01}{0.002}\times 0.08=0.4$$

$$I_{C_2}=\frac{q_2}{Q}I_{q(2)}=\frac{0.02}{0.002}\times 0.002=0.02$$

$$I_{C_3}=\frac{q_3}{Q}I_{q(3)}=\frac{0.03}{0.002}\times 0.05=0.75$$

$$I_{C_4}=\frac{q_4}{Q}I_{q(4)}=\frac{0.04}{0.002}\times 0.031=0.62$$

试读版本仅供预览期间线上教学使用

$$I_{C_5}=\frac{q_5}{Q}I_{q(5)}=\frac{0.05}{0.002}\times 0.0108=0.27$$

因此就得到一个按临界重要度系数的大小排列的各基本事件重要程度的顺序：

$$I_{C_3}>I_{C_4}>I_{C_1}>I_{C_5}>I_{C_2}$$

与概率重要度相比，基本事件 X_1 的重要程度下降了，这是因为它的发生概率最低。基本事件 X_3 最重要，这不仅是因为它敏感度最大，而且它本身的概率值也较大。

5. 利用概率重要度求结构重要度

在求结构重要度时，基本事件的状态设为“0，1”两种状态，即发生概率为50%，因此，当假定所有基本事件发生概率均为1/2时，概率重要度系数就等于结构重要度系数，即：

$$I_{\Phi(i)}=I_{q(i)}\qquad (q_i=1/2) \tag{3-29}$$

利用这一性质，我们可以用定量化的手段准确求出结构重要度系数。

【例3-18】 用式（3-29）求图3-33所示事故树各基本事件的结构重要度系数。

解： 令各基本事件发生概率为 $q_1=q_2=q_3=q_4=q_5=1/2$，根据所给出事故树的结构列出算式，并化简，则：

$$\begin{aligned}T&=A+B=X_4C+X_1D\\&=X_4(X_3+E)+X_1(X_3+X_5)\\&=X_4(X_3+X_2X_5)+X_1(X_3+X_5)\\&=X_3X_4+X_2X_4X_5+X_1X_3+X_1X_5\end{aligned}$$

该事故树的最小割集为 $\{X_3,X_4\}$、$\{X_2,X_4,X_5\}$、$\{X_1,X_3\}$、$\{X_1,X_5\}$。

顶上事件发生概率为：

$$\begin{aligned}Q&=q_3q_4+q_2q_4q_5+q_1q_3+q_1q_5-(q_2q_3q_4q_5+q_1q_3q_4+q_1q_3q_4q_5+\\&\quad q_1q_2q_3q_4q_5+q_1q_2q_4q_5+q_1q_3q_5)+(q_1q_2q_3q_4q_5+q_1q_2q_3q_4q_5+\\&\quad q_1q_2q_3q_4q_5+q_1q_3q_4q_5)-q_1q_2q_3q_4q_5\\&=q_3q_4+q_2q_4q_5+q_1q_3+q_1q_5-q_1q_3q_5-q_2q_3q_4q_5-q_1q_3q_4-\\&\quad q_1q_2q_4q_5+q_1q_2q_3q_4q_5\end{aligned}$$

则概率重要度系数为：

$$I_{q(1)}=\frac{\partial q_r}{\partial q_1}=q_3+q_5-q_2q_4q_5-q_3q_5-q_3q_4+q_2q_3q_4q_5=\frac{7}{16}$$

$$I_{q(2)}=\frac{\partial q_r}{\partial q_2}=q_4q_5-q_3q_4q_5-q_1q_4q_5+q_1q_3q_4q_5=\frac{1}{16}$$

$$I_{q(3)}=\frac{\partial q_r}{\partial q_3}=q_4+q_1-q_1q_5-q_2q_4q_5-q_1q_4+q_1q_2q_4q_5=\frac{7}{16}$$

$$I_{q(4)}=\frac{\partial q_r}{\partial q_4}=q_3+q_2q_5-q_2q_3q_5-q_3q_1-q_1q_2q_5+q_1q_2q_3q_5=\frac{5}{16}$$

$$I_{q(5)}=\frac{\partial q_r}{\partial q_5}=q_2q_4+q_1-q_1q_3-q_2q_3q_4-q_1q_2q_4+q_1q_2q_3q_4=\frac{5}{16}$$

试读版本仅供防疫期间线上教学使用

于是得：

$$I_{q(1)}=I_{q(3)}=\frac{7}{16};\ I_{q(4)}=I_{q(5)}=\frac{5}{16};\ I_{q(2)}=\frac{1}{16}$$

三种重要度系数中，结构重要度系数从事故树结构上反映基本事件的重要程度；概率重要度系数反映基本事件概率的增减对顶上事件发生概率影响的敏感度；临界重要度系数从敏感度和自身发生概率大小双重角度反映基本事件的重要程度。其中，结构重要度系数反映了某一基本事件在事故树结构中所占的地位，而临界重要度系数从结构及概率上反映了改善某一基本事件的难易程度，概率重要度系数则起着一种过渡作用，是计算两种重要度系数的基础。一般可以按这三种重要度系数安排采取措施的先后顺序，也可按三种重要度顺序分别编制相应的安全检查表，以保证既有重点、又能全面检查的目的。在三种检查表中，只有通过临界重要度分析产生的检查表，才能真正反映事故树的本质，也更具有实际意义。

事故树定量分析目前主要用于以可靠性、安全性为基础的评价方法。但是，可以预见，随着全面质量管理、安全系统工程、计算机技术的应用以及数据库的建立，事故树的定量分析将会在铁路运输领域得到更为广泛的应用。

【例 3-19】 某事故树如图 3-42 所示，X_1，X_2，X_3，X_4，X_5 均为基本事件，其概率分别为 0.01，0.02，0.03，0.04，0.05。求各基本事件的概率重要度、临界重要度。

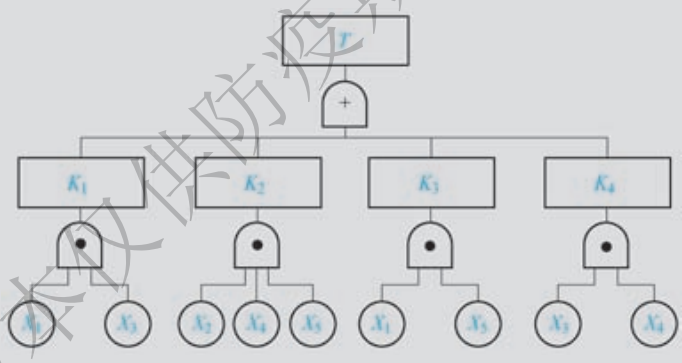

图 3-42　事故树图例

解： 应用顶上事件发生概率计算公式求得顶上事件的发生概率为 0.002。各基本事件的概率重要度、临界重要度见表 3-5。

表 3-5　各基本事件的概率重要度、临界重要度

基本事件	X_1	X_2	X_3	X_4	X_5
概率重要度系数	0.08	0.002	0.05	0.031	0.0108
临界重要度系数	0.4	0.02	0.75	0.62	0.27

试读版本仅供防疫期间线上教学使用

6. 事故树分析应用实例

【例 3-20】 环氧乙烷合成爆炸事故树分析。

（1）工艺流程简述。原料乙烯、纯氧和循环气经预热后进入列管式固定床反应器，乙烯在银触媒下选择氧化生成环氧乙烷；副反应是乙烯深度氧化生成二氧化碳。反应气经热交换器冷却后进入环氧乙烷吸收塔，用循环水喷淋洗涤，吸收环氧乙烷。未被吸收的气体经二氧化碳吸收塔除去副反应生成的二氧化碳后，再经循环压缩机返回氧化反应器。环氧乙烷生产工艺流程简图如图 3-43 所示。

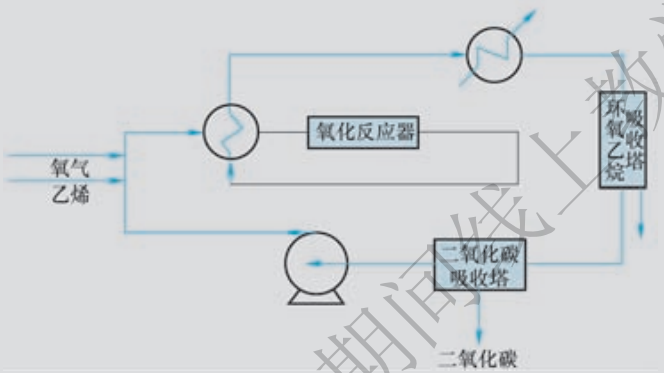

图 3-43 环氧乙烷生产工艺流程简图

（2）工艺条件及危险因素。

反应温度：环氧乙烷合成和副反应都是强放热反应，反应温度通常控制在 220～280℃。反应温度较高时，易使环氧乙烷选择性降低，副反应增加。

反应压力：环氧乙烷合成过程，主反应体积减小，而副反应体积不变。所以可加压操作，加快主反应速度，提高收率。但压力过高，易产生环氧乙烷聚合及催化剂表面积炭，影响催化剂寿命。操作压力通常为 1～3MPa。

原料配比：乙烯在氧气中的爆炸极限为 2.9%～79.9%，混合气中氧的最大安全含量（体积分数）为 10.6%。在原料气中，一般乙烯含量（体积分数）为 12%～30%，氧的含量（体积分数）不大于 10%，其余为二氧化碳和惰性气体。

由上述情况可以看出，环氧乙烷生产过程中发生爆炸的主要危险是发生异常化学反应，超过设备压力允许范围引起的。混合可燃气爆炸极限（上下限），与混合气的温度、压力和组成有关。如压力上升，爆炸上下限都将扩大；温度上升，则下限扩大。惰性气体或循环气的减少都会导致混合气中氧的含量增大。对于与爆炸范围关联的温度、压力和组成都必须严格按设定值控制，并避开爆炸范围。否则就会使生产过程处于危险状态。这种危险主要是气相反应中氧气含量达到爆炸极限，在起爆源存在下发生燃烧或爆炸。再分析工艺过程中固有的起爆源，如静电火花、明火及可能发生的局部火灾等因素，便可绘制出环氧乙烷合成爆炸事故树图，如图 3-44 所示。

试读版本仅供防发期间线上教学使用

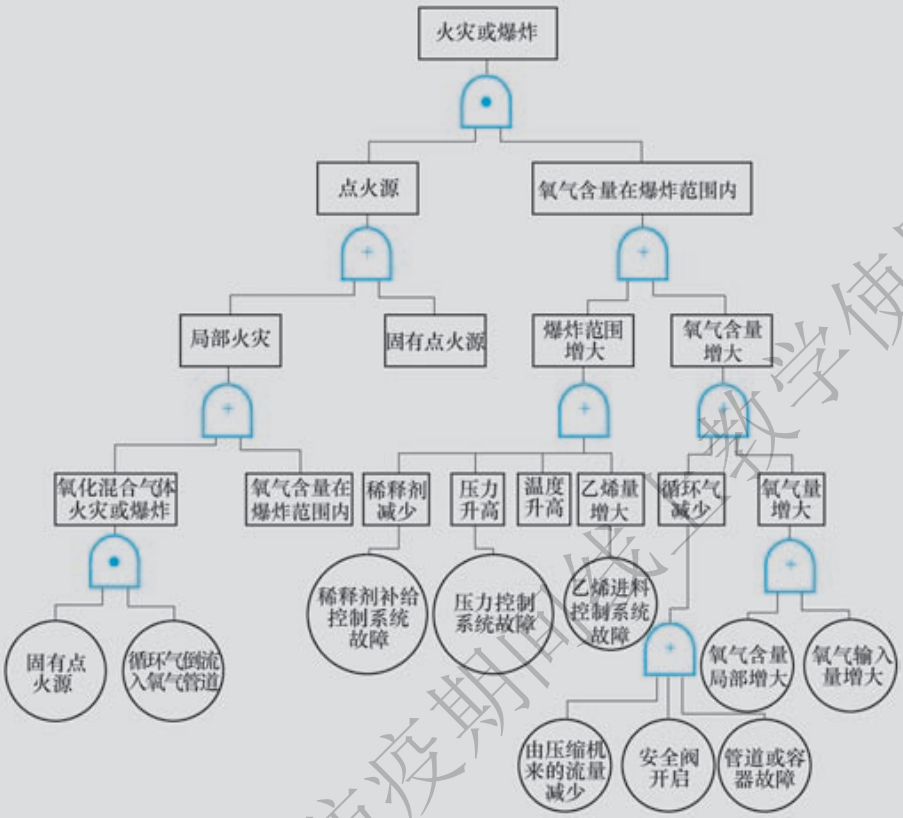

图 3-44　环氧乙烷生产中火灾爆炸事故树图

【例 3-21】　高氯酸火灾、爆炸事故树图。

高氯酸钠法制高氯酸的流程为，氯酸钠经电解生成的高氯酸钠与盐酸复分解反应，滤出结晶，再经蒸馏即可得到高氯酸。高氯酸生产原料极不稳定，受摩擦、冲击、遇热及火花，易发生燃烧和爆炸。氯酸钠与盐酸混合，能生成有毒和易爆的二氧化氯气体。高氯酸与浓硫酸或醋酸酐混合，能够脱水生成无水高氯酸。超过一定浓度的高氯酸（浓度在85%以上），在高于室温的条件下，能自行分解并猛烈爆炸。根据以上分析，可绘制出高氯酸火灾、爆炸事故树图，如图 3-45 所示。

【例 3-22】　蒸汽锅炉缺水爆炸事故树分析与计算。

蒸汽锅炉是工业生产中常用设备，又是比较容易发生灾害性事故的设备。由于蒸汽锅炉实际运行的工作条件十分恶劣，造成受压元件失效的原因往往是错综复杂的。引起锅炉爆炸的主要事件有：锅炉结垢、炉壁腐蚀、缺水和超压。下面仅就锅炉缺水引起爆炸作为顶上事件进行分析。

试读版本仅供防疫期间线上教学使用

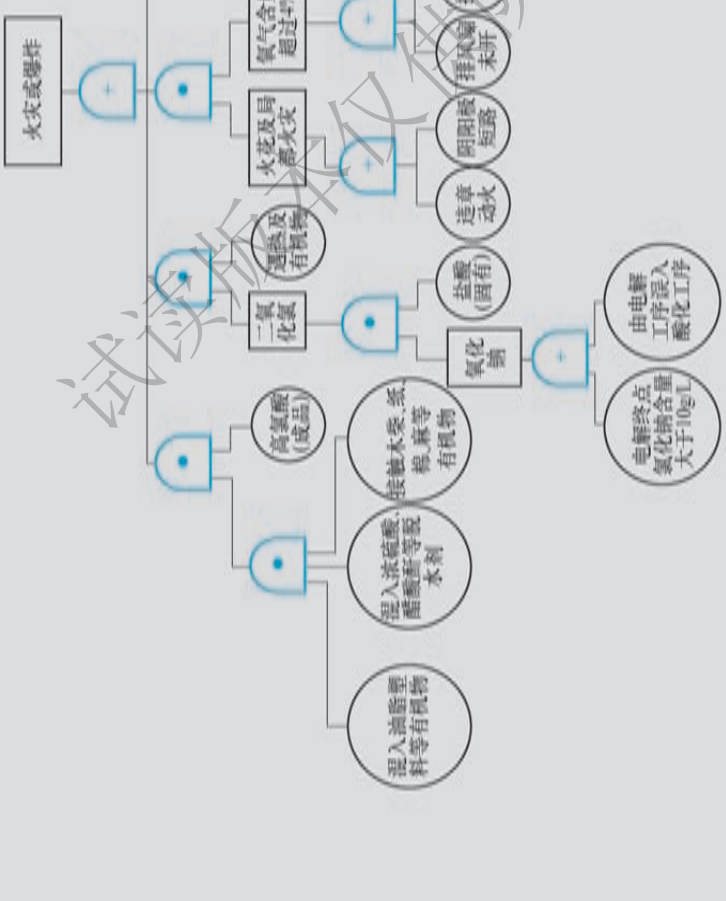

图 3-45 高氯酸火灾、爆炸事故树图

试读版本仅供防疫期间线上教学使用

（1）建造事故树。

1）确定顶上事件：锅炉缺水。缺水的直接原因事件：警报器失灵（基本事件）、水位下降（系统故障事件）、未察觉（系统故障事件）。各个事件用与门连接。

2）水位下降的直接原因事件：给水故障（系统故障事件）、排污阀故障（部件故障事件）。各个事件用或门连接。

给水故障的直接原因事件：管道阀门故障（基本事件）、自动给水调节失灵（基本事件）、停水（基本事件）、泵损坏（基本事件）、没蒸汽泵（基本事件）、爆管（基本事件）。各个事件用或门连接。

排污阀故障的直接原因事件：阀门关闭不严（基本事件）、未关阀（基本事件）。各个事件用或门连接。

3）未察觉的直接原因事件：判断失误（系统故障事件）、工作失误（系统故障事件）。各个事件用或门连接。

其中，判断失误的直接原因事件为：叫水失误（部件故障事件）、假水位（部件故障事件）。各个事件用或门连接。

而叫水失误的直接原因事件有：忘记叫水（基本事件）、叫水不足（基本事件）。各个事件用或门连接。

假水位的直接原因事件：水位计损坏（基本事件）、没定期冲洗（基本事件）、水位计安装不合理（基本事件）、汽水共腾（部件故障事件）。各个事件用或门连接。

假水位直接原因事件中的汽水共腾的直接原因事件：水的硬度高（基本事件）、蒸汽旋塞关闭（基本事件）。各个事件用或门连接。

（2）绘制事故树图，如图3-46所示。

（3）定性分析。

1）判别最小割（径）集数目。根据“加乘法”判断该事故树的最小割集共有72个。画出事故树的成功树图，如图3-47所示，求得该成功树的最小径集共有3个。

2）求结构函数：

$$\begin{aligned}\overline{T} &= \overline{x}_1 + \overline{M}_1 + \overline{M}_2 \\ &= \overline{x}_1 + \overline{M}_3\,\overline{M}_4 + \overline{M}_5\,\overline{M}_6 \\ &= \overline{x}_1 + \overline{x}_6\,\overline{x}_7\,\overline{x}_8\,\overline{x}_9\,\overline{x}_{10}\overline{x}_{11}\overline{x}_2\,\overline{x}_3 + \overline{M}_7\,\overline{M}_8\,\overline{x}_4\,\overline{x}_5 \\ &= \overline{x}_1 + \overline{x}_2\,\overline{x}_3\,\overline{x}_6\,\overline{x}_7\,\overline{x}_8\,\overline{x}_9\,\overline{x}_{10}\overline{x}_{11} + \overline{x}_{12}\overline{x}_{13}\overline{x}_{14}\overline{x}_{15}\overline{x}_{16}\overline{x}_{17}\overline{x}_{18}\overline{x}_4\,\overline{x}_5\end{aligned}$$

即得到三组最小径集为：

$$P_1 = \{x_1\}$$

$$P_2 = \{x_2, x_3, x_6, x_7, x_8, x_9, x_{10}, x_{11}\}$$

$$P_3 = \{x_4, x_5, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}\}$$

3）求结构重要度。由于该事故比较简单，而且没有重复事件，利用最小径集来判别结构重要度。x_1是单事件的最小径集，因此：

$$I_\Phi(1) > I_\Phi(i)\quad (i=2, 3, \cdots, 18)$$

试读版本仅供预览期间线上教学使用

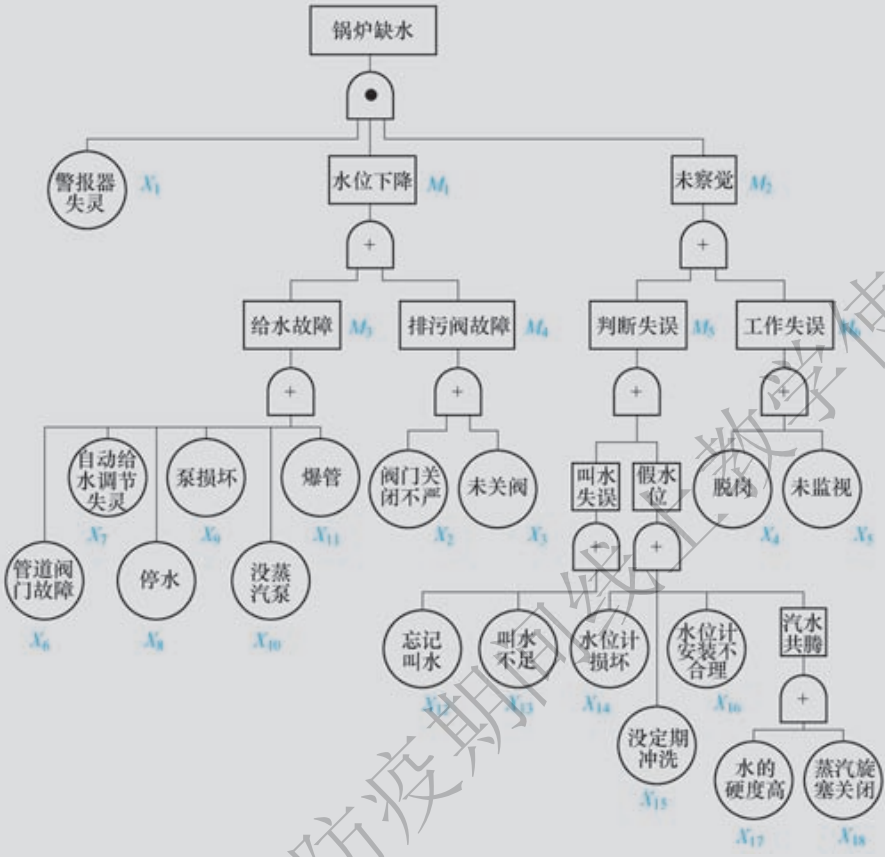

图 3-46　蒸汽锅炉缺水爆炸事故树图

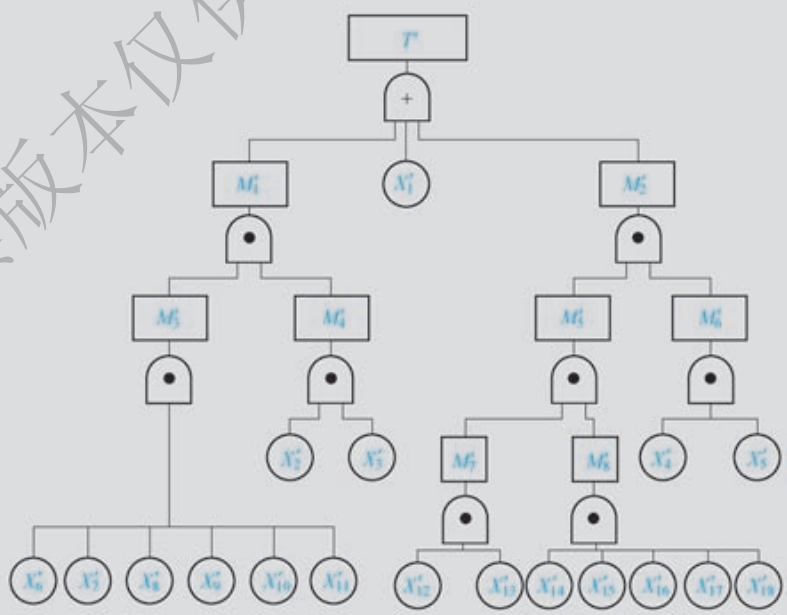

图 3-47　蒸汽锅炉缺水爆炸事故树的成功树图

试读版本仅供防疫期间线上教学使用

x_2，x_3，x_6，…，x_{11}共有8个事件同时出现在P_2中，因此：

$$I_\Phi(2)=I_\Phi(3)=I_\Phi(6)=\cdots=I_\Phi(11)$$

x_4，x_5，x_{12}，…，x_{18}共有9个事件同时出现在P_3中，因此：

$$I_\Phi(4)=I_\Phi(5)=I_\Phi(12)=\cdots=I_\Phi(18)$$

所以结构重要度的顺序为：

$$I_\Phi(1)>I_\Phi(2)=I_\Phi(3)=I_\Phi(6)=\cdots=I_\Phi(11)>I_\Phi(4)$$
$$=I_\Phi(5)=I_\Phi(12)=\cdots=I_\Phi(18)$$

（4）结论。锅炉缺水引起锅炉爆炸是一种恶性事故，因而防止缺水是个重要的问题。

通过定性分析，最小割集最多72个，最小径集3个。也就是说发生缺水事故有72种可能性。但从3个径集可得出，只要采取径集方案中的任何一个，锅炉缺水事故就可以避免。

第一方案（x_1）是最佳方案，只要保证警报器灵敏可靠，锅炉缺水就可以预防。其次是第二方案（x_2,x_3,x_6,…,x_{11}），为保证锅炉水位不发生异常情况，就要求给水设备处于良好状态，并且管道阀门畅通。第三方案是水位下降后操作人员未及时发现并进行判断的一些事件，操作人员的岗位工作占主要地位。

造成缺水的主要原因：在18个基本事件中，警报器失灵是最主要原因事件（x_1），其次是操作人员脱岗（x_4）及排污阀门故障（x_2）。若抓住3个关键，就抓住了预防锅炉缺水的主要环节。

复　习　题

1. 补充【例3-11】的详细计算过程。

2. 石棉瓦是一种大量应用在简易房屋、临时工棚的屋面结构上的轻型建筑材料。它的优点是页面大、重量轻、使用方便、价格便宜、施工速度快、经济效益好，缺点是强度差、质地脆，受压易破碎，故在搭建或检修施工中踏在石棉瓦上极易发生坠落伤亡事故。

当踏破石棉瓦坠落，且高空作业、地面状况不好时，则导致坠落伤亡事故。事故是由于安全带不起作用和脚踏石棉瓦所造成的。而未用安全带、安全带损坏、因移位安全带取下、支撑物损坏等是造成安全带不起作用的原因；而脚踏石棉瓦发生坠落由以下几个因素引起：脚下滑动踏空、身体不适或突然生病、身体失去平衡、椽条强度不够、桥板倾翻、未铺桥板、桥板铺得不合理。

（1）画出事故树，求最小割集，并画出事故树等效图。

（2）画出成功树，求最小径集，并画出成功树等效图。

（3）结构重要度分析。

（4）求顶上事件的概率。

基本事件的概率值见表3-6。

试读版本仅供防疫期间线上教学使用

表 3-6 基本事件的概率值

代 号	名 称	q_i	代 号	名 称	q_i
X_1	未用安全带	0.15	X_7	身体失去平衡	0.005
X_2	安全带损坏	0.0001	X_8	橡条强度不够	5×10^{-5}
X_3	因移动而取下	0.25	X_9	桥板倾翻	1×10^{-4}
X_4	支撑物损坏	0.001	X_{10}	未铺桥板	0.001
X_5	脚下滑动踏空	0.005	X_{11}	桥板铺得不合理	0.001
X_6	身体不适或突然发病	1×10^{-5}	X_{12}	高度、地面状况	0.3

3. 某反应器系统如图 3-48 所示。该反应是放热的，为此在反应器的夹套内通入冷冻盐水以移走反应热。如果冷冻盐水流量减少，会使反应器温度升高，反应速度加快，以致反应失控。在反应器上安装温度测量控制系统，并与冷冻盐水入口阀门联结，根据温度控制冷冻盐水流量。为安全起见，安装了温度报警器，当温度超过规定值时自动报警，以便操作者及时采取措施。该系统各安全功能故障率见表 3-7，试以冷冻盐水减少为初始事件编制事件树，并计算出现反应失控的概率。

表 3-7 某型号反应器安全功能故障率

安 全 功 能	温度报警器报警	操作者发现超温	操作者恢复冷却剂流量	操作者紧急关闭反应器
故障率	0.01	0.25	0.25	0.1

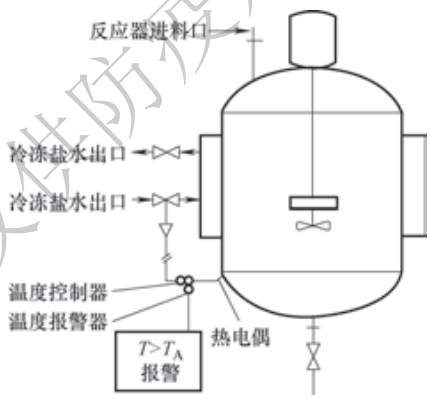

图 3-48 某型号反应器示意图

4. 火灾发展一般可以分为四个阶段，初期阶段、发展阶段、全盛阶段和衰减阶段。假设一个建筑防火分区失火，如果灭火器和自动水喷淋系统灭火失败，就会导致火灾进一步发展，这时灭火器或自动水喷淋系统已经不能有效地控制扑灭火灾，火灾就会超过阶段Ⅰ而发展到阶段Ⅱ。在阶段Ⅱ火灾处于发展阶段，人们可以使用室内消火栓将火灾扑灭。这个阶段影响火灾发展的主要因素是室内消火栓和排烟设备的工作状况。在阶段Ⅱ，室内温度逐渐升高，同时会产生大量高温、有毒的烟气，这些高温、有毒的火灾烟气对人员使用室内消火栓扑救火灾十分不利。所以，排烟设备的及时起动是保证人员使用室内消火栓成功扑灭火灾的关键。

（1）试以火灾发展超出阶段Ⅰ为初始事件，考虑排烟设备和室内消火栓的情况，用事件树方法分析阶段Ⅱ火灾发展的可能结果。

试读版本仅供防疫期间线上教学使用

（2）假设排烟设备成功开启的概率为 P_1，室内消火栓成功灭火的概率为 P_2，试计算阶段Ⅱ火灾发展的可能后果的概率。

5. 已知某事件 T 的事故树如图 3-49 所示。

（1）试计算此事故树的最小割集、最小径集，并进行分析。

（2）用 q_i 表示各基本事件 X_i 发生的概率，$q_1=0.01$；$q_2=0.02$；$q_3=0.03$；$q_4=0.04$，计算顶上事件发生的概率。

（3）分析各基本事件的结构重要度和概率重要度。

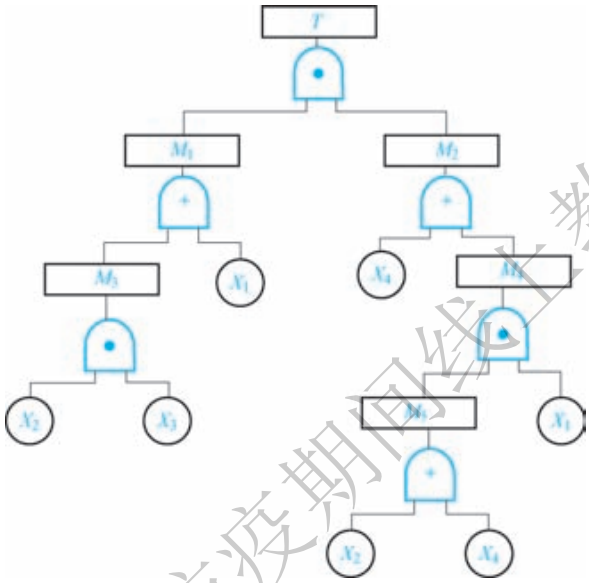

图 3-49　某事故树示意图

试读版本仅供防疫期间线上教学使用