上篇　理　论　篇

第一章　安全系统工程概论

安全这一概念，与人类的生存密切相关，如原始人懂得在其居住的部落周围挖掘出沟壕以防止野兽的袭击。毫无疑问，史前人就具有了制定安全计划的能力，这对他们得以幸存起了重要的作用。另外，人们从狩猎和农业实践中认识到生产工具和自然现象对人类的危害，发明了一些简单的防护办法。其后由青铜器到铁器时代，防护器械也随着生产工具的进步而发生了质的飞跃。我们的祖先在防瓦斯、防毒气、防冒顶等安全防护方面积累了许多经验，历史上屡有记载。如明代宋应星编著的《天工开物》一书中，就记载了有关处理矿内瓦斯和顶板的防护措施：“初见煤端时，毒气灼人，有将巨竹凿去中节，尖锐其末，插入炭中，其毒烟从竹中透上”。采煤时，“其上支板，以防压崩耳。凡煤炭取空，而后以土填实其中”等等，已比较明确地提出了采煤劳动保护措施。随着生产的发展，技术的进步，人们对安全技术的要求也越来越高。特别是 18 世纪工业革命以来，由于使用了蒸汽机，每年锅炉爆炸致使成千上万人的死亡。19 世纪末期和 20 世纪初期，西方世界进入资本主义的发展时期，工业生产规模不断扩大，煤矿、化工、水运、堤坝、土建等工程往往一次发生数百人甚至上千人的重大伤亡事故。生产条件的恶化、工伤事故和职业病日益严重，引起了人们的不安和广泛的关注。为加强管理，各国政府纷纷制定了有关安全的法令，用法律来促使企业对安全的重视，并加强了对安全技术的研究，从而使安全技术逐步形成了一个综合性学科。

二次世界大战以后，工业技术水平不断提高，规模不断扩大，核能、航天等尖端工业，石油、化工、冶金等重工业迅速发展，事故也越来越频繁，灾害越来越严重。这种工业技术的进步所带来的对人类的威胁和损害引起了人们对安全更为广泛的重视。为消除和避免危害，人们在长期的实践中，创造和总结了预防危害的办法。归结而言，可以把这些办法分成“问题出发型”和“问题发现型”两大类。

“问题出发型”实质上是在事故发生后从中吸取经验教训，进行预防的办法。例如从事故后果查找原因，采取措施以防止事故重复发生。通常我们所采取的各种组织和技术措施，如设立专职机构、制定立法标准、进行监督检查和宣传教育等，以及防尘排毒、防火防爆、安全防护设备、个人防护用具等都属此类。这也就是我们通常所说的传统安全工作方法。

传统安全工作法虽然为防止事故做出了并正在做出贡献，但又存在不少缺点。它的纵向分科、单项业务保安、事后处理等特点使得人们对事故难以做到防患于未然，从而导致安全工作总是跟在生产后面跑，事故预防跟不上技术进步的局面。究其原因，主要在于：

(1) 安全属性问题。由于安全是依附于生产而存在的，并且是为生产服务的。生产中如果不发生事故，则往往引不起人们的重视，看不到安全工作的作用和重要性，“安全第一、预防为主”挂在口头上，难于贯彻落实到实际工作中。不仅企业领导人忽视安全工作，甚至连直接在恶劣生产条件下作业的人员也掉以轻心。

(2) 由于工业技术在不断进步和发展，人们对技术中许多潜在的危险因素还认识不清，没有意识到发生事故后的严重后果。

(3) 由于安全工作所产生的经济效益是间接的，当发生事故造成损失后人们才感觉到安全工作的重要性，这就使得人们平时对安全工作不予重视，缺乏对安全工作进行深入细致的研究。

另外，传统安全工作法本身也存在着许多弱点，如：

(1) 凭经验和直感处理生产系统中的安全问题多，由表及里的深入分析、发现潜在的事故隐患少，难于彻底改善安全面貌。

(2) 定性的，即“安全”或“不安全”的概念多，而定量的概念少。如生产的安全性有多大，事故发生的可能性的大小，有多大的严重后果，都无法回答，不能给人以实质性的概念。

(3) 由于缺乏系统性，所以解决安全问题时总是片断地和零碎地进行，以致形成头痛医头，脚痛医脚，到处堵塞漏洞的被动局面。

(4) 管理上存在着严重的片面性，侧重于追究人员的操作责任，只抓“违章”而忽视了创造本质安全。

(5) 由于没有开展预测工作，没有进行事前的系统安全评价，工作重点只是处理已发生的事故，而忽略了从规划、设计阶段就开始抓安全工作。

(6) 没有肯定明确的目标值。究竟做到什么程度才算是安全，才能控制事故，心中无数，盲目性大。

总之，传统安全工作方法是一种凭经验、孤立、被动的工作方法。最近 50 多年来，科学技术的进步和生产的发展，引起了从生产工具到劳动对象、生产组织和管理的一系列变革，同时也给安全带来了许多新的问题，使人们深深地感觉到传统安全工作方法已不能适应工农业生产的迅速发展。因此，人们，特别是安全工作者总想找出一个方法，以能够事先预测事故发生的可能性，掌握事故发生的规律，作出定性和定量的评价，以便能在设计、施工、运行和管理中向有关人员预先发出事故危险性警告，并根据对危险性的评价结果采取相应的预防措施，以达到控制事故的目的。安全系统工程就是为了达到这一目的而产生和发展起来的。

采用安全系统工程控制事故发生的方法，即为上述所说的“问题发现型”方法。其实质是从系统内部出发，研究各构成要素之间存在的安全上的联系，查出可能导致事故发生的各种危险因素及其发生途径，通过重建或改造原有系统来消除系统的危险性，把系统发生事故的可能性降低到最小限度。

第一节　安全系统工程的概念

一、系统工程的概念

1．系　统

系统是由具有特定功能的、相互间具有有机联系的许多要素所构成的一个整体。任何一个系统都应该符合以下几个条件：必须由两个以上的要素所组成；要素间互有联系和作用；要素有着共同的目的和特定的功能；要素受外界环境和条件的影响。

所谓要素，指的是内部相互作用的基本组成部分，是完成某种功能无需再细分的最小单元。

由此可见，系统具有整体性、集合性、相关性、目的性、环境适应性和动态性等特征。为方便理解，对系统的四个主要属性解释如下：

（1）整体性：“系统是由具有特定功能的、相互间具有有机联系的许多要素所构成的一个整体”这一定义充分表达了系统具有整体性的含义。一个系统的完善与否主要取决于系统中各要素能否良好的组合，即是否能构成一个良好的实现某种功能的整体。换言之，即使每个要素并不都很完善，但它们可以综合、统一成为一个具有良好功能的系统，这就是一个较为完善的系统；反之，即使每个要素是良好的，但构成整体后却不具备某种良好的功能，这不能称之为完善的系统。

（2）相关性：系统内各要素之间是有机联系和相互作用的，要素之间具有相互依赖的特定关系，是互为相关的。如电子计算机系统是由运算、贮存、控制、输入、输出等硬件装置和操作系统软件（要素或子系统）通过特定的关系，有机地结合在一起而构成的。计算机系统的各要素都有相关关系，否则就无法实现某一特定功能。

（3）目的性：所有系统都为了实现某一特定的目标，没有目标就不能称之为系统。不仅如此，设计、制造和使用系统，最后总是希望完成特定的功能，而且要效果最好，这就是所谓最优计划、最优设计、最优控制和最优管理和使用等。

（4）环境适应性：任何一个系统都处于一定的物质环境之中，系统必须适应外部环境条件的变化，而且在研究和使用系统时，必须重视环境对系统的作用。

2．工　程

传统的“工程”概念指的是生产技术的实践。它往往以“硬件”作为其目标和对象，如采矿工程、桥梁工程、电气工程等等。它所研究的对象主要是人力、材料、价格等。系统工程的“工程”，其目标和对象既包括“硬件”，也包括“软件”，如人类工程、生态工程等，它泛指一切由人参加的，以改变系统某一特征为目标的工作过程，其含义较之传统概念中的“工程”更为广泛。

3．系统工程

系统工程是以系统为研究对象的。它是组织管理“系统”的研究，规划、设计、制造、试验和使用的科学方法，是对所有系统都具有普遍意义的科学方法。实质上，系统工程较明确地表述了：它属于工程技术，主要是组织管理的技术；它是解决工程活动全过程

的技术；它具有普遍的适用性。

系统工程不仅涉及到诸如采矿工程、机械制造工程、电气工程等科学技术领域，而且还涉及到信息论、控制论、运筹学、概率论、数理统计、最优化方法、系统模拟以及社会学、经济学等多种学科。系统工程是从横向方面把纵向科学组织起来的一项科学技术。其目的是应用系统的理论和方法去分析、规划、设计新的系统或改造已有的系统，使之达到最优化的目标，并按此目标进行控制和运行。它的基本思想就是用搞工程的办法搞组织管理，以系统为对象，把要组织和管理的事物，应用数学和电子计算机等工具，进行分析处理，求得系统最佳化的结果。随着科学的进步，社会实践活动的规模日益扩大，事物间的联系日趋复杂，这就形成了形式多样的各种系统。为使人们所研究的系统在技术上最先进，经济上最合算，运行中最可靠，时间上最节省，则需协调系统中各要素或系统间的关系，使之达到最佳的配合。运用系统工程能起到这样的作用。

在国际学术界，往往把系统分析（广义）作为系统工程的同义词来理解，可见系统分析在系统工程中占有极其重要的位置。系统分析的方法和过程又是系统分析的核心内容。系统分析，是利用系统科学原理对系统进行研究、探索，从中找出规律的具体方法。它是从系统的观点出发，以系统整体效益为目标，通过定性或定量的分析，找出系统中各要素之间的相互关系和各种可供决策者选择的方案，并对众多的方案进行综合评价，以求得最优方案的过程。

系统工程的开发和应用，并不是企图排斥或替代传统工程，而是以系统的观点和方法为基础，运用先进的科学技术和手段，从全面、整体、长远出发去考察问题，拟订目标和功能，并在规划、开发、组织、协调各关键时刻，进行分析、综合、评价，求得优化方案，然后用传统工程行之有效的方法去进行工程设计、生产、安装、建造新的系统或改造旧的系统。

总之，系统工程是一门特殊工程，它不仅是一门应用科学管理技术，而且还是一门跨越各学科领域的边缘科学。

二、安全系统工程

安全系统工程领域研究、解决的主要问题是：如何控制和消除导致人员死伤、职业病、设备或财产损失，最终实现在功能、时间、成本等规定的条件下，系统中人员和设备所受的伤害和损失为最小。

一般采用“安全性”来描述安全。与安全对立的概念是危险，同样也可用“危险性”来描述危险。在实际研究与使用中，通常是通过对系统危险性的研究，并以危险性的大小来表达其安全性。假定系统的安全性为 S，危险性为 D，则有 $S=1-D$。显然 D 越小，S 就越大，反之亦然。若消除了危险因素，就等于创造了安全。

实现系统的安全识别，分析、预测和评价系统中的危险性，消除或控制系统中所存在的危险是至关重要的。

近三十多年来，人们把系统工程应用于安全领域，形成了安全系统工程技术。所以，所谓安全系统工程，即是运用系统工程的原理和方法，对系统或生产过程中的危险性进行识别、分析、评价及预测，并根据其结果，采取综合安全措施予以控制或消除系统中存在的危险因素，使事故发生的可能性减少到最低限度，从而达到最佳的安全状态。

三、安全系统工程能有效防患于未然的原因

大量的实践结果表明，安全系统工程的应用能有效防患于未然。究其原因，最根本的是采用了系统工程的原理与方法来解决安全问题。为什么说采用系统工程的方法解决安全问题，才能有效地防患于未然呢？其理由如下：

（1）使用系统工程方法，可以识别出存在于各个要素本身、要素之间的危险性。

我们知道,危险性存在于生产过程的各个环节,如原材料、设备、工艺、操作、管理之中。这些危险性是产生事故的根源。安全工作的目的就是要识别、预测、分析、控制和消除这些危险性，使之不致发展成为事故。利用系统可分割的属性，人们就可充分地、不遗漏地揭示存在于系统各要素（元件和子系统）中所存在的危险性，然后就可以采取措施对危险性加以消除，对不协调的部分加以调整，这就有可能消除事故的根源并使安全状态达到优化。

（2）使用系统工程的原理和方法，可以了解各要素间的相互关系，消除各要素由于互相依存、互相结合而产生的危险性。

要素本身可能并不具有危险性，但当进行有机的结合构成系统时，便产生了危险性。这种情况往往发生在子系统的交接面或相互作用时。

人机交接面是多发事故的场所，最突出的例子如人和压力机、传送设备等的交接面。对交接面的控制，在很大程度上可以减少伤亡事故。

危险物的质量、能量贮积都是构成重大恶性事故的物质根源。适当地调整加工量和处理速度，可以大量降低事故的严重性。

（3）系统工程所采用的一些手段都能用于解决安全问题。

系统工程几乎使用了各种学科的知识，但其中最重要的有运筹学、数学、控制论等，其所采用的手段几乎都适用于解决安全问题。如使用决策论，在安全方面可以预测发生事故可能性的大小；利用排队论，可以减少能量的贮积危险；使用线性规划和动态规划，可以采取合理的防止事故的手段。至于数理统计、概率论、可靠性工程和模糊数学，则可应用于预测和评价等。

第二节　安全系统工程的发展过程

1947 年 9 月，美国航空科学院报导了一篇题为“安全工程”的论文，其中写道：“正如飞机性能、稳定性和结构完整性一样，必须进行安全设计，并使之成为飞机不可分割的一部分。安全组也象应力组、空气动力系组和荷载组一样，必须成为制造厂的重要组织机构之一。”这是最早提出系统安全概念的一篇论文。

60 年代初，这一概念开始为合同文件所正式采用。由合同文件正式指派安全职责取代了通常的由设计人员，管理人员和工程师大致分工负责安全工作的作法。规程的公布促进了防止事故的系统安全方法的产生和发展。

1962 年 4 月，美国空军公布了弹道导弹部的 BSD 第 62－41 号文“发展空军弹道导弹的系统安全工程”，这一文件向与民兵式导弹计划有关的承包商提出了系统安全的要求。1963 年 9 月，这一文件修改后成为美国空军规程 MIL－S－3813O，“军用规程——对系统

及有关系统和设备的安全工程的一般要求”。1966年6月，此规程经过很小的修改，成为美国国防部的规程，MIL－S－3813OA 。最后在 1969年 7月，该规程又进一步地修改成为军用标准 MIL－STD－882,“对系统和有关子系统及设备的系统安全程序的要求”经国防部批准,MIL－STD－882 最终成为所有产品和系统采购的系统程序都必须遵守的标准。在上述这些标准中，首先建立了安全系统工程的概念，以及设计、分析、综合等原则。此后，由于这一先进技术的传播，使得人们对系统安全认识不断深化，工业中的许多企业采用安全系统计划的也逐渐多起来。

另外，英国以原子能公司为中心，从60年代中期开始收集有关核电站故障的数据，采用概率的方法对系统的安全性、可靠性进行评价，后来进一步推动了定量评价的工作，并设立了系统可靠性服务所和可靠性数据库。它们的任务是收集核电站的设备和装置的故障数据，提供给有关单位。

1974年，美国原子能委员会发表了原子能电站事故评价报告。该项研究是在原子能委员会的支持下，由麻省理工学院的拉斯姆逊教授组织十几个人，用 2年时间，花了 300万美元完成的,叫做‘拉氏报告”,即 WASH－1400。报告中收集了原子能电站各个部位历年发生的事故，分析了发生的概率，采用事故树和事件树分析方法，作出了核电站的安全性评价。这个报告发表后，引起了世界各国同行的关注。

日本引进安全系统工程的方法虽为时稍晚，但发展很快。自从1971 年科技联盟召开了“可靠性安全学术讨论会”以来，二十几年来在电子、宇航、航空、铁路、公路、原子能、化工、冶金、煤炭等领域的研究工作十分活跃。日本劳动省于1976年公布的化工联合企业6段安全评价方法，就贯穿了安全系统工程的内容。他们还推广事故树定性分析法，甚至要求每个工人都能熟练应用。

我国引进安全系统工程的方法（FTA）始于1976 年。1982 年，首次组织了全国性的安全系统工程研讨会。而后，安全系统工程的研究与应用热潮在全国兴起，目前已在全国范围内得到广泛的使用，在安全系统工程理论的研究上也取得了很多的成果，在发展安全系统工程理论上作出了贡献。

当前，安全系统工程已普遍引起了各国的重视，国际安全系统工程学会每两年举办一次年会。安全系统工程的应用几乎渗透到各个领域。

从安全系统工程的发展史可以看出，它最初是从研究军事产品的可靠性和安全性开始的，后来发展到对生产系统各个环节的安全分析，这就使安全系统工程的方法在安全技术工作领域中得到实际的应用。

第三节　安全系统工程的内容及其优越性

一、安全系统工程的内容

安全系统工程是一种综合性的技术方法。这是因为，在安全系统工程使用中，不仅要应用系统工程的原理和方法，而且还要熟悉所要研究的系统或生产过程及应采取的安全技术等，即安全系统工程所包括的内容是广泛的。由目前国内外的资料可见，安全系统工程

的内容主要包括事故成因理论、系统安全分析、安全评价和安全措施四个方面。

1．事故致因理论

为防止事故的发生，人们在生产实践中不断总结经验和教训，研究探索事故的发生规律，以了解事故为什么会发生，事故是怎样发生的，以及如何采取措施予以防范，并依此以模式和理论的形式加以阐述。由于这些模式和理论着重解释事故发生的原因以及针对事故成因因素如何采取措施防止事故，故人们就把这些模式和理论称为事故成因理论或事故致因理论。事故致因理论就是从事故的角度研究事故的定义、性质、分类和事故的构成要素与原因体系，分析事故成因模型及其静态过程和动态发展规律，阐明事故的预防原则及其措施。事故成因理论是指导事故预防工作的基本理论。

事故致因理论中的事故模式（是人们对事故机理所作的逻辑抽象或数学抽象，用于描述事故成因、经过和后果，是研究人、物、环境和管理及事故处理这些因素如何作用而形成事故和造成损失的。）对于事故的分析、预防、处理均具有重要的作用。事故模式有很多种，目前世界上较为流行的有 13 种，它们是系统理论、事故因果连锁论、流行病学论、能量交换模式、不安全行为论、寿命单元改变论、屡次失误模式、人的因素论、人机理论、动机论、同时发生论、决策模式、生物节律论等。

2．系统安全分析

系统安全分析是安全系统工程的核心内容，它是安全评价的基础。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、查明系统存在的危险性，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，关系到整个工作的成败。

系统安全分析法，目前国内外提出的已有数十种之多。综合这些方法，可将其归为文字表格法、逻辑分析法、统计图表分析法、调查实验法和数学解析法等五大类共 16 种基本方法。各种方法除了它们各有自己的特点（特定的运用范围）外，其中有不少方法是雷同或重复的。因而，在使用时应设法了解系统，并选用合适的，具有特色的分析法。我国目前较常采用的有事件树、事故树、故障类型影响等分析法和安全检查法及因果分析图法（鱼刺图法），事故比重图，事故趋势图，事故控制图，主次图等。

在进行系统安全分析时，可根据需要把分析进行到不同的深度，可以是初步的或详细的，定性的或定量的。每种深度都可以得出相应的答案，以满足不同项目和不同情况的要求。

3．安全评价

安全评价是对系统存在的危险性进行定性或定量的分析，得出系统存在的危险点与发生危险的可能性及其程度，以预测出被评价系统的安全状况。

安全评价是预测预防事故的高级阶段，它往往是建立在系统安全分析的基础上，结合其他理论进行的。不同的评价方法有不同的安全评价结果。定性评价的结果只能用大概的度量信息表现，只能让人们知道系统中危险性的大致情况；定量评价的结果则能用较为精确的量值表现，可以以较为直观的数量形式反映安全的状况。

安全评价是一种预测安全状况的手段，并非防止、控制事故发生的实际措施。安全评价是安全系统工程的重要组成部分与实用性较强的内容。正确的安全评价必须有科学的安

全理论做指导，使之能真正揭示安全状况变化的规律并予以准确描述，并以一种可辩识度量的信息显示出来。

安全评价方法可依据评价的目的或采用的基本理论进行分类。目前较常见的方法有定性和定量评价、预先评价、日常评价、事后评价、全面评价、局部评价等。现代安全评价是以系统科学原理、耗散结构理论、现代数学和控制理论等作为理论基础的。

4. 安全措施

对一个系统进行评价后，根据评价结果，针对系统中的薄弱环节或潜在危险，提出调整修正的措施，以消除事故的发生或使发生的事故得到最大限度的控制。

安全措施主要包括宏观控制措施、微观控制措施和安全目标管理。

宏观控制措施是以整个系统作为控制对象，人们是根据系统的安全状况进行决策，选定控制措施。通常采用的控制措施主要有法制手段（政策、法令法规、规章制度）、经济手段（奖、惩）和教育手段。

微观控制措施是以具体的危险源作为控制对象，人们对系统中固有的危险源和人的不安全行为进行控制。对于固有危险源，具体的控制措施可采用控制、保护、隔离、消除、保留和转移等方法。对人的不安全行为，主要依据行为科学原理，采用人的安全化与操作安全化的方法进行控制。

安全目标管理就是把一定时期内所要完成的安全指标，分解到各具体部门或个人。各接受安全指标的部门或个人，根据自身系统的安全状况，在管理人员的指导下，采取具体控制措施，对系统中的不安全因素进行控制，以达到预期的安全效果。安全目标的实施分目标制定阶段、目标执行阶段和目标成果评价阶段。安全目标管理主要采用法律、行政、经济、教育及技术工程的手段。

二、安全系统工程的优越性

如上几节所述，安全系统工程是在传统安全的基础上发展起来，由多门现代学科综合形成的一门新技术，使用起来有许多优越性，其优点可简述如下：

(1) 可以打破传统安全中单一的、凭经验的那种相互独立，自我封闭的界限。

(2) 该方法逻辑性强、明白、直观，能定性、定量地进行安全分析和评价，能全面系统，合理地解决安全问题。

(3) 可以避免传统安全中对事故的“浅层”分析，从人机关系、人和环境、人和物的关系等诸种关系中寻找真正的事故原因和查出未想到的原因。

(4) 通过分析，可以了解到系统存在的薄弱环节及可能发生危险性的尺度，有利于有的放矢采取相应措施预防事故的发生。

(5) 通过评价和优化技术，可以找出最适当的方法使各分系统之间达到最佳配合，用最少的投资达到最佳的安全效果和大幅度地减少伤亡事故。

(6) 安全系统工程的方法，不仅适用于工程，而且适用于管理，并且能用来指导产品的设计、制造、使用维修和检验。

(7) 可以促进各项标准的制订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，如安全设计标准、人机工程标准等。同时为了定量计算，还可促进积累有关可靠性（包括人和物）的数据。

（8）可以迅速提高安全工作人员的水平。安全系统工程是一门实践性很强的科学，真正搞好安全系统工程必须熟悉生产，学会各种分析和评价方法，这对提高安全工作人员的素质是大有好处的。

当然，安全系统方法的最大优点是预防和减少事故发生，这在实践中得到了证明。

第四节　安全系统工程的方法论

一、研究方法上的整体化

安全系统工程的研究方法，是从整体观念出发的，它不仅把研究对象视为一个整体，还可以把系统分解为若干个子系统，对每个子系统的安全性要求，要与实现整个系统的安全性指标相符合。对于评价过程中子系统之间或者系统与系统之间的矛盾，都要根据总体协调的需求来选择解决方案。因此，系统安全要贯穿到规划、设计、制造、使用、维护等各个阶段。

在系统概念上，系统除了材料、能量、信息三大要素以外，在系统的各要素中，应格外重视人。我国和日本的有关事故统计资料表明，包含人的不安全行为造成灾害的次数，一般在 90%以上。因此在研究、分析、评价系统安全时，不能忽视人在系统中所起的作用，而是必须从整体出发，全面考虑系统中的各种因素。

二、技术应用上的综合化

安全系统工程综合应用多种学科技术，使之相互配合，使系统实现安全化，即系统工程的最优化。

人们在“安全问题”上所研究、遇到的“系统”往往是复杂的。对系统各要素间的关系越揭示得清晰、深刻、精确，就越能获得最佳应用多种技术的成就。因而，在研究综合运用各学科和各项技术过程中，人们从全面的系统观点出发，采用逻辑、概率论、数理统计、模型和模拟技术、最优化技术等数学方法，并用计算机进行处理和分析计算，把系统内部要素间的关系和不安全状态，用简明的语言、数据、曲线、图表清楚地描述出来或把所研究的问题在定性的基础上数量化表示，显示出那些不易直观觉察的各种要素间的相互关系，使人们能深刻、全面地了解和掌握所研究的对象，作出最优决策，保证整个系统能按预定计划达到安全目标。

三、安全管理科学化

安全工作中的规划、组织、控制和决策等统称为安全管理。安全管理工作对实现系统安全、经济效益等具有重要意义，所以，科学化的管理对实现系统安全至关重要。安全系统工程的 6 个主要任务（即寻找、发现系统事故隐患；预测由故障引起的危险；选择、制定和调整安全措施方案和安全决策；组织安全措施和对策的实施；对措施的效果进行全面的评价；不断采取改善措施，以求得最佳效果）体现出了安全管理科学化的主要特征。

第二章　事故致因理论

第一节　事　故　概　论

一、事故的基本概念

1. 事　故

人们在实现其目的的行动过程中，突然发生了与人的意志相违背的，迫使其有目的的行动暂时或永久停止的事件。

从上述定义可见，事故包含着三种意思：

(1) 有目的的行动过程。如开采煤炭、乘车前往某处，均为有目的的行动过程。

(2) 所发生的事件是突然的、与人的意志相违背的。如在生产过程中，谁都不希望从巷道顶板上掉下大块的岩块，但有时它却偏偏冒顶，这种情况就是与人的意志（或叫本意）相反。它是一种随机事件。

(3) 突发事件发生后出现其有目的的行动暂时或永久停止的后果。

如果任一突发事情发生且迫使人们有目的的行动暂时中止或永久性地停止这一结果出现，则认为事故发生。譬如，某人骑自行车去某地，中途掉入沟里，那么则可认为这是一起事故，因它具备了三个条件。掉入沟里，且不讨论其是否摔坏，仅此也足以中止他原有的行动过程，则产生了不希望的后果。

由事故的定义可见，它的范畴是广泛的。它包含着生产事故与非生产事故之分。我们在此仅讨论生产事故。

2. 生产事故

企业在生产过程中突然发生的伤害人体，损坏财物，影响生产正常进行的意外事件。

生产事故包括设备事故、伤亡事故（工伤事故）、未遂事故。

从某种程度上讲，在生产事故包含的三种事故中，工伤事故危害最大。

(1) 工伤事故(伤亡事故)：

定义：在生产区域中发生的，与生产有关的人身伤害、急性中毒等事故叫工伤事故。

人身伤害指的是个人或集体在行动过程中，接触了与周围条件有关的外来能量，致使人身生理机能部分或全部丧失的现象（即造成的结果是使人暂时地或长期地丧失劳动能力）。比如，某人在采煤时，顶板掉落，击中身体的某一部位致人受伤，叫伤害，也叫做工伤。因顶板的冒落是属能量（势能）的转移，而对人体来说，被击中，则说明它吸收了外来的能量，由于这一非正常的能量的吸入，使得人体生理机能受到伤害，所以，就称为工伤事故。又比如，一个非生产人员人骑自行车，撞到栏杆身亡，这也叫伤亡事故，但它不属于工伤事故。

所以，伤亡事故一般分为工伤和非工伤二大类。

(2) 设备事故：在生产过程中突然发生导致设备、财物损坏的意外事件。

(3) 未遂事故：通常指的是，虽然在行动中，突然发生了与人的意志相反的情况，但无造成人身的伤害，叫未遂事故。

在这里应强调指出的是，事故发生的结果到底是造成伤亡还是未遂，这完全是受偶然性支配，只有毫厘之差的问题，两者的界线不是很明显，其本质仅是一个偶然性的问题，所以，在进行安全管理时，切不能忽视未遂事故，对伤亡、未遂事故，都应做为防范对象，这在安全管理上是一个极为重要的观点。

二、伤亡事故的特征

1. 事故的因果性

所谓因果性，指的是某一现象作为另一现象发生的根据的两种现象之关连性。

实际上，事故是相互联系的许多原因的结果，则事故这一现象，与其它现象是互相依存与制约的关系。这种相互依存与制约的关系就是因果关系。

必然引起别的现象的事件叫作原因，而由原因所引起的别的现象就是结果。

因果关系具有继承性（或称非单一性），即第一阶段的结果往往是第二阶段的原因。

从图 6－1 中见，许多事故构成要素①是“因”，导致了某一事件②的结果；而②又是下一阶段结果③的“因”，往后可以同理类推。随着时间的推移，可以由近因找到远因。此图则直观地表明了事故的因果性。

比如支架不牢是原因①，造成了顶板掉落②结果，而②结果又是造成压到人这一现象（结果）的原因。

我们可以从压到人这一结果找出是顶板掉落这一原因，而从顶板掉落可以查出支架不牢的原因。

事故的因果性，启示我们在制定预防措施时，应尽最大努力掌握造成事故的直接和间接原因，深入剖析其根源，以防事故发生。

2. 事故的偶然性

从本质上讲，伤害事故是一个随机事件，即在某一条件下，既可能发生，也可能不发生。

其偶然性是客观存在的，事故是随时间过程产生某些意外情况而显现出来的一种现象，所以很难决定出它所有的规律。但在一定的范畴内，用一定的科学仪器或手段，却可找出其近似的规律。例如，收集分析大量的案例，或采用概率的方法，就可找出事故的规律性。实际上由于事故的因果性，决定它具有规律性。

人们在承认事故偶然性的同时，更重要的是在其偶然性的背后，却存在着必然的规律性。在安全管理中要善于从偶然性中找出其必然性，认识事故发生的规律，及时地把事故消灭在萌芽之中，所以说，在安全事故管理中，认识事故的规律是很重要的。

3. 事故的潜伏性、预测性

事故的发生是不能脱离时间而存在的，在人的全部活动和机械体系作业时的运动，其所经过的时间内，不安全隐患是客观存在的，如果条件成熟就会显现而导致事故，否则就暂时不予显现，所以，任何活动都存在着发生事故的危险。这就是事故的潜伏性，事故

的潜伏性启示人们必须注意事故潜在的危险。

对事故可能的潜伏性的预测是非常重要的。所谓预测，就是人们根据以往积累的经验和知识，通过研究构思出一个模型，即所谓的“预测模型”。经对“预测模型”的计算，就可得知事故的潜在危险。显然，如果“预测模型”的准确性高，预测的结果就准确，否则，可能偏差较大。所以，对于潜在性的预测，很关键的是取决于模型的准确性。

如果事故的潜伏危险因素能被准确地预测出来的话，人们则可有的放矢地采取措施，使潜在的因素不至于转换，这样就可避免事故的发生。

另外，人们也可通过五感（视、听、嗅、味、触）对外界条件取得信息，再经大脑综合判断而预测其结果。但这种判断也离不开过去的经验，所以说，经验对“建模”、“直接预测”都是非常重要的。

但值得提出的是，在自然环境中，有时经验不起作用的情况也是存在的。例如井下的瓦斯，无色、无味、无臭，单凭人的五感是无法预测的。只有用科学仪器来扩大人的五感的灵敏度才能收到效果，所以使用科学仪器和科学方法是提高直接预测可靠性的重要途径。

当然，事故的潜在性与预测性是一般而言的。在实际生产中，也常有一些“突然”发生的事故，这是事故的特殊性——具有突然性。对于此类事故，往往难于预测，比如天灾，就属此类。

总而言之，突然性的事故毕竟是少数，人们讨论、注意的应是一般性。所以，安全工作一个很重要的重点就是应放在及时发现事故的潜在危险上，以根除隐患而不使之再现为事故，故此，提高事故预测的可靠性是非常重要的。

要搞好预测，应认真总结人们以往积累的经验，对已发生的事故进行追综，分析其所以发生的根本原因，观察了解其倾向，以便发现未来同类事件的危险潜在性，并加以控制或排除，使之不导致显现的事故。

三、事故法则

所谓事故法则，常称为 300:29:1 法则，是由美国一位安全工程师享瑞齐氏于 1973 年对 55 万起事故统计分析后发现的一个统计规律。

统计表明，涉及同一工人的 330 件相似的意外事件中，有 300 起未产生伤害，29 件产生轻、微伤，1 次产生死亡，故称 300:29:1 法则。

这个法则受到了美国其它国家安全界的普遍承认。300:29:1 这一法则，用如图 2－1 所示的三角形表示，称为事故三角形。

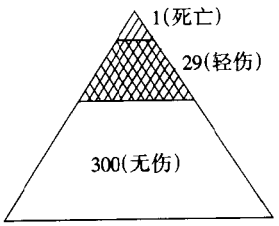


图 2－1　事故三角形示意图

300:29:1 法则表明，1 次的死亡和 29 次的轻微伤是包含于 330 次之中，这是个统计数据。事实上，也许死亡就是一连串事件的第一次，或许是最后一次，或许是发生在 330 次当中的任何一次。现在用下面一例来说明这个比例关系。

如某矿一工人，图省事，每次上下班都违章走轨道上山，从走轨道上山之日起，到他死亡之日止，约一年时间（约 275 天 = 25 天 × 11 月）。在这 275 天中，共走 550 次，在这 550 次中，为了躲车，曾摔倒受轻微伤 18 次（病历卡记

录上），最后，因下放煤时，司机急刹车，钢丝绳上跳，把他打死，故其伤亡比例是 531∶18∶1。

由事故法则及简单的例子揭示出这样的一个问题，尽管严重伤害是个偶然事件，但人在伤害以前却曾有多次暴露于不安全因素之中，是有多次的隐患或无伤害做为前面事件的。

比如上面所举的例子，他走了 550 次，实际上其受伤害的隐患早已存在，并已发生了 18起的轻伤，最后直至被打死亡。如果说，这个工人按规定不走轨道上山，那么，他就可以避免死亡。

故此事故法则在防止事故发生上具有重要的意义。人们要想清除 1∶29 的伤亡事故，就得使事故（包括 300 次的无伤事故）都不发生。可这样比喻：生产过程如航行于大海中的轮船，1 和 29 是明显的礁石，而 300 是暗礁，是潜在危险。船只有绕过这些暗礁，才能避免碰船，所以说人们在进行事故预防时，对于未遂事故切勿掉以轻心，而应引起足够的重视。

四、事故构成及其分类

工伤事故包括：伤害部位、伤害种类、伤害程度三个要素。

1. 伤害部位

伤害部位有头、脸、眼、鼻、耳、口、牙、上肢、手、手指、下肢、足、脚趾、肩、躯干、皮肤、粘膜、内脏、血液、神经末梢、中枢神经。

2 伤害程度

我国分死亡事故、重伤事故和轻伤事故。国外分死亡、丧失劳动能力（终生致残）、部分丧失劳动能力（部分致残）、暂时不能劳动，要医疗不休工、无伤害等。

3. 伤害种类

按照 GB6441－86 《企业职工伤亡事故分类标准》的规定，因工伤亡事故分成 20 种：

（1）物体打击（指落物、滚石、锤击、碎裂、崩块、砸伤等伤害，不包括因爆炸而引起的物体打击）；

（2）车辆伤害（包括挤、压、撞、倾覆等）；

（3）机械伤害（包括绞、辗、碰、插、戳等）；

（4）起重伤害（指起重设备或操作过程中所引起的伤害）；

（5）触电（包括雷击）；

（6）淹溺；

（7）灼烫；

（8）火灾；

（9）高空坠落（包括从架子上、屋顶上 、以及从平地上坠入坑内等）；

（10）坍塌（包括建筑物、堆置物倒塌和土石塌方等）；

（11）冒顶片帮；

（12）透水；

（13）放炮；

（14）火药爆炸（指生产、运输贮藏过程中发生的爆炸）；

(15)瓦斯爆炸(包括煤尘爆炸)；

(16) 锅炉爆炸；

(17) 容器爆炸；

(18) 其他爆炸（包括化学物爆炸，炉膛爆炸等）；

(19) 中毒和窒息（煤气、油气、沥青、化学、一氧化碳中毒等）；

(20) 其他伤害（热伤、跌伤、车伤、野兽咬伤等）。

这是具有法定意义的分类方法。它概括了全国工业生产的各方面的事故，覆盖面很广，分类也比较简单，似乎粗了一点。但太细了，统计起来不方便。

第二节　事故致因理论简介

事故的模式是指用于阐明事故的成因、始未过程和后果的模型。

事故模式对于人们认识事故的本质，指导事故调查、事故分析、事故预防及事故责任者的处理有着重要的作用，所以必须加以研究。

目前国内外提出的事故模型有很多种。各种模型都有着自己的特点，对于我国来说，在生产实践、教学与科研中影响较大的模型主要有 13 种，下面对目前几种常用的模型做简单的介绍。

一、人为失误论

人为失误论认为，一切事故都是由于人的失误造成的，诸如工人的违章、管理上的失误等等。

这一模型在东欧一些国家很为流行，尤其是在前苏联很流行。因为我国原来的工业模型很多是效仿苏联的，所以这一模型对我们的影响较大。其具体表现是在对事故的分析、处理和在采取对策上，很强调人的作用。

人为失误模型中，目前常用的有二个模型。

1. 人为失误为主因的模型

人为失误为主因的模型如图 2－2 所示。

人为失误为主因的模型表明：工人在生产过程中，各种刺激不断出现，如果工人响应的动作不出现失误，则事故不会发生，又重新接受新的刺激与干扰。

若当接受刺激所响应的动作失误，就要看这种失误的后果是否导致危险，如果无危险，则出现了未遂事故；如果危险，则要看运气－机遇。若机遇好，则成为未遂事故，否则，就会出现伤亡事故。

从整个模型的实质上看，只要出现人为失误，就可能导致事故发生；或者说，伤亡事故都是人为失误造成的。

从上面的分析可见，这一模型是有局限性的。因在生产过程中，客观上存在着许多非人为因素，如工作面的压力、地质条件、设备新旧问题等。在事故模型中，都未体现出来。另外，虽然该模型突出了人的失误所可能造成的危害性，但它却无法解释人为什么会出现失误。一般说来，这一事故模型对于机械制造行业针对性强些，对于矿山行业，针对

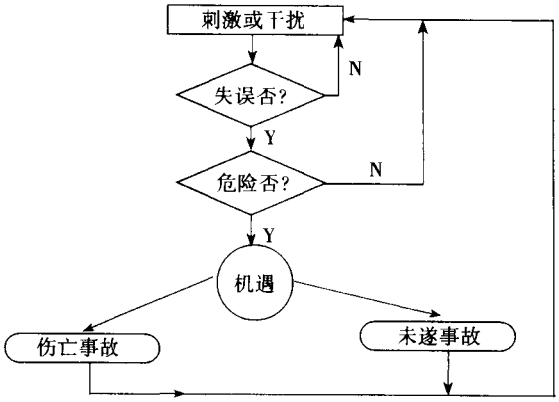


图2-2　人为失误为主因的模型

性似乎就差得多。

目前国际上对于煤矿生产的事故模型尚无人研究出来，但最近美国几位学者综合了许多模型，对金矿的事故模型进行了研究，并提出了“金矿中以人为失误为主因的事故模型”。

2．以管理失误为主因的模型

该模型认为，事故之所以发生，是因为客观上存在着不安全因素及众多的社会因素和不利的环境条件。这一理论认为，人的不安全行为和物的不安全状态是造成事故的主要原因。但是，造成“人的不安全行为——人的失误”和“物的不安全状态”的背后往往是由于“管理上的失误”所造成的。从这一基点出发，作者认为“管理失误”是发生事故的本质原因。

由图可见，人的不安全行为可以造成物的不安全状态，而物的不安全状态又会客观上造成人发生不安全行为的环境条件。

从图2-3可见，“隐患”往往是由物的不安全状态和管理上的缺陷共同偶合而成的。显然，如果“隐患”一经形成，这时，如果出现“人的不安全行为”，则会导致事故的发生。比方

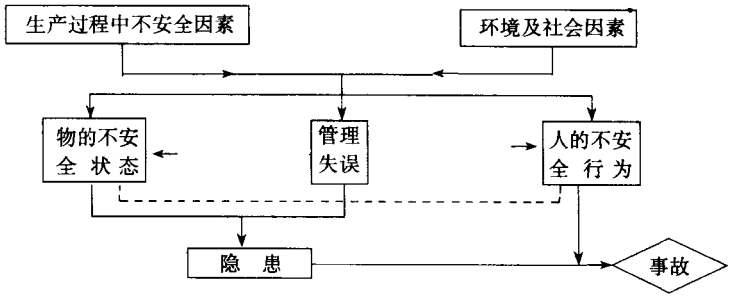


图2-3　以管理失误为主因的模型

说，绞车提升钢丝绳由于使用年限超限而已发生断股，但若在正常操作时尚不至于马上断裂，按要求，如果及时更换，则可避免事故的隐患的存在，但由于管理不善，不按章及时更换，则客观上埋下了“隐患”。这样的钢丝绳，如果在运行过程中进行急刹车，可以断

言，它马上会导致断裂而造成事故。

所以从这一模型可以清楚地看出，要想事故不发生，则应杜绝“不安全状态”、“管理失误”和“人的不安全行为”的发生。

应强调指出的是，物的不安全状态有时往往较难发现，而“人的不安全行为”是自由性的，随机的，行动较容易被发现。所以，在事故分析中，常把“人的失误”看成最主要的，往往是断定为事故的直接责任者，有时，这种判定是正确的，但有时却是不对的，因为大家应看到“物质”在事故中是呈第一性的，所以，在事故的分析与预防时，应注意重视“物的不安全状态”。另外，从模型上看，假定“物的安全状态”已经存在，但若管理不失误，则就可以避免危险性的扩大，这样，就可避免事故的发生。

譬如，在一个工作面的开口处，由于原有的巷道与新掘出的巷道交叉，造成暴露面积的加大，在这一区域，顶板压力显然要增大。此时，若作业规程没明确地规定加强支护，工人按这样的不完善的作业规程进行作业，没进行足够的支护，造成了物的不安全状态。这实际上就是埋下了事故的隐患，倘若没有进行及时的处理，就会酿成事故。

二、骨牌论

海因里希按事故发生顺序，把其编排成易懂的 5 个骨牌，即所谓的骨牌论，如图 2－4所示。图中（c）示意去掉“C”使系列中断，伤亡事故则可避免。

图 2－4 中各个骨牌的含义如下：

A：社会环境和管理欠缺。如遗传及生活环境差、家庭生活不幸福、人际关系不好、无事业心、经济困难、工作担子太重、领导不重视安全、教育培训不够、领导无方、作业方法未标准化、工作纪律差等。

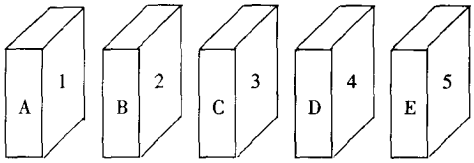
B：个人的欠缺（人为过失）。即个人的身体及精神状态欠佳，如个性粗暴无情、轻浮、幼稚、傲慢、自暴自弃、过分兴奋、误解、烦闷、担心、不满、喝酒成风、睡眠不足、过度疲劳、身体状况不好、无视安全规章、知识与技术缺乏等等。

C：人的不安全行为和物的不安全状态。不安全行为是指造成事故的人为错误，主要常表现在冒险作业，高速操作，未经许可就进行操作，错误地运行设备，人为地使安全装置失效，向同事发出错误的警告或进行错误的防护，不适当地使用个人防护设备，不正确地装载、放置设备或物体，作业姿势不良，作业位置不当，不正确地进行运输、提升，对运转中的设备进行检修，投掷工具，赤脚作业，开玩笑等等。

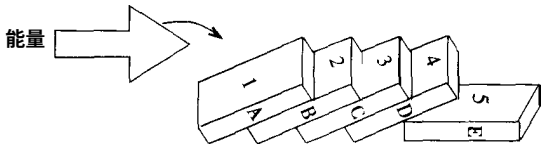
不安全状态是指能导致事故发生的物质条件，主要常表现在没有充分地支撑或防护，使用不良的工具、设备或物资，工作场所过分狭小或条件恶劣，没有良好的预警系统，存在火灾和爆炸危险，工作面顶板破碎，地质水文条件复杂，存在着危险的大气条件（气体、粉尘、烟雾、水蒸气），噪声过大，照明不好，通风不良，工艺过程不合理，作业方法不当，安全整顿差等方面。

D：事故。发生了与人的意志相违背的事情，是指前 3 种因素经连锁反应，使潜在的危险暴露出来，暂时或永久地迫使生产停止。

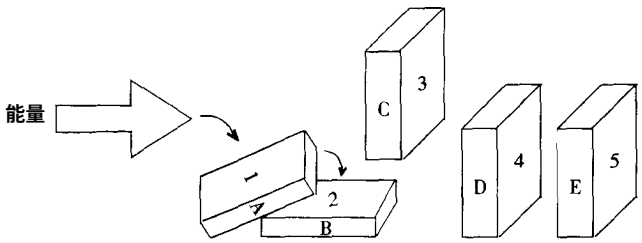
E：人身伤亡。由于事故发生而导致人体伤害。示意图中（a）表明：若按因果顺序，伤亡事故为 5 个因素：A 的发生促使 B 的发生，而 B 的发生又造成 C 的发生。C 的出现促成了 D 的发生，由于 D 的发生，产生了 E 的结果。



(a)伤亡事故五因素



(b)伤亡事故的发生过程



(c)

图2-4　骨牌论模型示意图

显然，如果紧紧相挨的5个骨牌的前3个中的任一个倒下，则后边的骨牌也就会接连倒下，见图（b）这就表明，事故和伤亡之所以产生是由于前3个因素的作用。图（a）、（b）表现了事故的组成要素及其连锁反应。事故是在时间的过程中显现出来的，它是组成要素的一种连锁反应的结果。诚然，若能采取措施，防止或避免第一、第二个骨牌倒下，则不会导致下一步的倾倒，就可避免事故和伤亡的发生。然而，由于第一、第二个骨牌所包含的是社会环境、管理和个人欠缺因素，所以在实际工作中要做到防止“倾倒”是件难事。从图（c）可见，若抽掉中心的“C”骨牌，那么，即使第一、二张牌倒下，也不致于发生事故。从预防事故和伤亡出发，在事故预防中，应集中精力，设法消除骨牌C，使系列中断，则可避免事故和伤亡的发生。由此可见，安全工作的中心应放在排除人的不安全行为和物的不安全状态，清除事故隐患。

三、能量意外释放论

(一)能量意外释放论事故模型

第二次世界大战以后，科学技术有了飞跃的进步，新技术、新工艺、新能源、新材料、新产品不断出现，与日俱增。这些新技术、新工艺、新能源、新材料、新产品在使工业生产和人们生活面貌发生巨大变化的同时，也给人类带来了更多的危险。面对生产、生活中出现的越来越多的新危险，人们必须研究、采取更有效的安全防护措施。先进的科学技术和发达的经济为此提供了技术手段和物质基础。

为了有效地采取安全技术措施控制危险源，人们对事故发生的物理本质进行了深入的探讨。1961年吉布森、1966年哈登等人提出了解释事故发生机理的能量意外释放论（见