北京经济学院出版社

安全分析与事故预测

王 泽 申 编著

安全与卫生工程系列教材

劳动保护管理学
安全分析与事故预测
工业防毒技术
工业通风与防尘工程学
噪声控制工程
作业环境空气检测技术
电气安全工程
起重与机械安全工程学
锅炉压力容器安全工程学
防火与防爆

·安全与卫生工程系列教材·

安全分析与事故预测

王泽申 编著

北京经济学院出版社

1992年 北京

（京）新登字211号

安全分析与事故预测

王泽申　编著

北京经济学院出版社出版

（北京市朝阳区红庙）

北京市通县永乐印刷厂印刷

新华书店北京发行所发行

787×1092毫米　16开本　8.25印张　211千字

1990年9月第1版　1992年9月第1版第2次印刷

印数：8001—11000

ISBN7-5638-0145-6/F·82

定价：3.90元

《安全与卫生工程系列教材》出版说明

安全与卫生工程是受到国内外普遍重视的一门新兴学科。它着重研究工业生产过程中危害劳动者安全和健康的各种因素，并以相应的工程技术措施及现代管理措施保障劳动者的安全和健康。在我国，安全与卫生工程学科的发展与技术措施的广泛应用，对贯彻“安全第一，预防为主”的劳动保护方针，消除事故根源，保障广大职工的安全和健康，促进社会主义建设事业的顺利进行起着重要作用。

我社出版的《安全与卫生工程系列教材》，是北京经济学院安全工程系以富有教学经验的教师组成编写组，在多年教学科研实践的基础上，吸收国内外先进技术和方法编写而成的。本套教材系统地、详尽地介绍了安全与卫生工程技术的原理和方法。力求概念准确，条理清楚，论述深入浅出，做到科学性、先进性和实用性相结合。本套教材注意理论联系实际，附有必要的工程数据和工程图表、资料以利实用。本套教材可作为高等院校、大专院校相应专业的教材或教学参考书，也可作为各产业部门、厂矿企业劳动保护干部、管理干部的培训教材。

《安全与卫生工程系列教材》共计10本：

《劳动保护管理学》

《锅炉压力容器安全工程学》

《防火与防爆》

《电气安全工程》

《起重与机械安全工程学》

《安全分析与事故预测》

《工业通风与防尘工程学》

《噪声控制工程》

《工业防毒技术》

《作业环境空气检测技术》

此外，还有一本《作业环境空气监测方法》可与《作业环境空气检测技术》配合使用。

1990年7月

序　言

安全分析与事故预测，是一门把可靠性预测基本原理和方法用到对生产系统进行安全性分析与评价的一门学科。用这种方法，可以科学地分析生产系统中所存在的不安全因素，查明这些不安全因素之间的关系，以及它们对系统的影响，从而可以找出系统中的薄弱环节，并进一步对系统的安全性作出科学的评价。最终能够提出包括更改整个系统设计，以及从技术、教育和管理等几方面采取预防事故的综合性合理对策，以达到最大限度的保障系统安全的目的。

多年来，在国家劳动保护方针政策指引下，我国的安全工程和安全管理工作取得了很大成绩，也积累了丰富的经验。这些无疑是今后做好劳动保护工作的重要基础。

但是，随着国家经济建设的发展，原有的管理方法已经远远不能满足实际的需要。尤其是许多建立在经验基础上的方法已经难以解决现代生产过程中所出现的具有综合性原因的大量意外事件。所以，必须在原有的基础上引进一些现代管理的新方法，把这些先进方法与我国实际经验相结合，填补我国安全工程领域的空白。

事故预测，既是我们研究和分析复杂系统的必备的理论和方法，又是我们解决实际问题的综合性分析技术。它所涉及的知识领域相当广泛，相关科学较多，主要有安全原理、系统工程、人机工程、可靠性工程、管理工程、布尔代数、概率论与数理统计，以及各工程技术领域里的安全工程学等。

为了便于读者学习，本书在编写过程中已把有关的必要知识简明扼要的编入书中，期望能够对读者学习本书有所助益。

由于作者水平有限，书中论及问题难免有不妥之处，恳请读者批评指正。

在编写本书过程中，作者参阅了国内外学者的著作，并引用了其中有关材料，在此谨表谢意。

王泽申

1990年2月于北京经济学院

目　录

第一章　防止意外事件的基本原理

意外事件的防止是指控制人的行为、机器的动作以及物质环境的科学。“控制”一词含有防止及改正不安全情况和作业环境的意思。

所谓意外事件的防止，就是在事故未发生之前，所做的一切工作以减少机械的或物质的危害及人的不安全动作为原则。即防止伤害于未然为上策。

一、意外事件的发生顺序

意外事件的发生顺序的理论根据，是按照美国H·W海因里奇（H·W Heinrich）提出的“骨牌顺序”理论（domino sequence）。在事故发生后，对人身受到伤害的整个过程进行分析时，海氏认为是按以下五个因素的顺序发生的（见图1—1）：（1） M—世系及社会环境；（2） P—人为的过失；（3） H—不安全动作以及机械或物质的危害；（4）D—意外事件；（5） A—伤害。意外事件因素及其说明如表1—1所示。

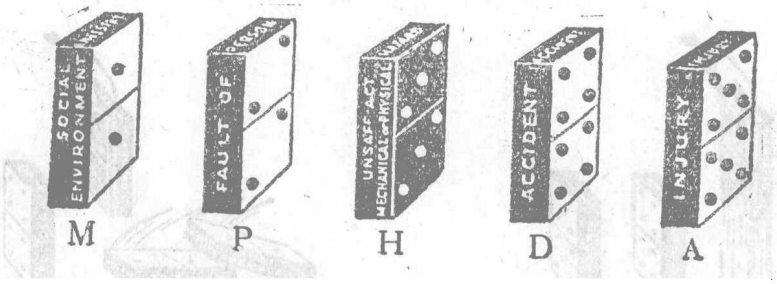

图1—1　意外事件五因素

在意外事件发生顺序中，五个因素有如连锁反应，在时间的推移过程中，它们以一定的关系依次发生。其发生顺序从M开始，它如果对P有影响，接着就会影响到H和D，只要D发生，最终就会出现A的结果。

一种伤害的发生，是一连串事件按照一定顺序发生的结果。一个依赖另一个，一个跟随着另一个以构成一定的顺序。这种情形如同一列竖立的骨牌排列成直线，如第一块倒落，则全列均倒，所以意外事件顺序也称骨牌顺序。一个意外事件不过为顺序中的一个因素而已。

在五因素顺序中，假若消除危险因素H，使此系列中断，则伤害不能发生，如图1—2及图1—3所示。所以，防止意外事件的着眼点应放在顺序的中心，也就是要防止人为的不安全动作及机械或物质的危害，即消除潜在的危害。

表1—1　　意外事件因素及其说明表

意外事件因素	因素说明
1.世系及社会环境	遗传或环境造成的结果 如鲁莽、脾气粗暴、神经病及其它来自遗传中的不良特性 环境可使人发展成具有不良的品行
2.人为的过失	由于先天遗传或后天习染的缺点而造成了不安全动作直接的原因，或发生机械的或物质的危害
3.不安全动作以及机械或物质的危害	人为的不安全动作，如站在悬吊的负荷下；开动机器时无警告；移去安全防护装置等等 机械或物质的危害，如无防护装置，无防护操作场所；缺乏栏杆的保护及光线不足等等造成直接的意外事件
4.意外事件	如人跌倒；飞物对人打击造成的事故
5.伤害	如骨折，裂伤等伤害

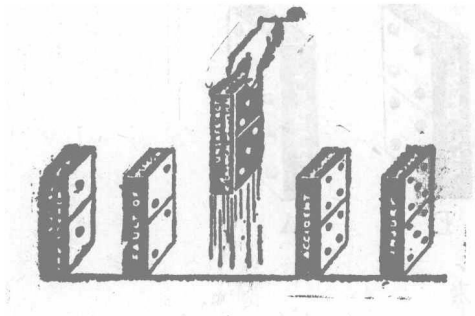

图1—2　移去不安全动作及机械危害构成的中央因素

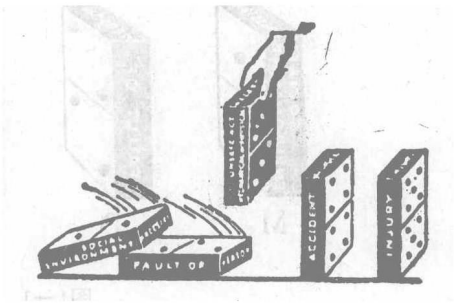

图1—3　移去中央因素使前面因素的动作无效

二、人与机器

近年来，在人与机械系统中，对人与机器的关系，人体差错等问题的认识正在逐年的提高。当把系统划分为人体和机器时，就人体而言，机器过于复杂，或者过于陈旧化，都必然导致系统障碍。对这个问题，一方面起因于人体与机器的协调，同时也起因于人体与机器本身的可靠性。在机器方面，通过材料和设计的改善，可以使可靠性变得很高；与此相反，要在人体方面做到这样的改善则是不可能的。因此，仅仅象过去使用机械部件那样来对待人体，要在本质上得到可靠性的改善是有限度的。加强训练固然会使差错有一些减少，但不能

根除差错。因此，在发生频率问题上，人体差错就变成了难以克服的关键。美国军队的有关统计中，有过这方面的实际报告，系统故障的40%是以人体差错为直接原因的。

人与机器关系中，人受到各种因素的影响远远超过机器，因此完成动作的可靠性也低于机器。由于存在着人为的差错，因而也降低了机械的可靠性。所以，对机器应考虑的是，即便是由于人的错误行动，使机器受到损坏，也要能够保护人不受到伤害。

人为的差错固然会造成许多意外事件，然而对机械进行有效的安全措施，是防止意外事件的重要因素。因此，为了保证安全，机械设备的维护，以及减少机械及物质的危害是基本的首要的法则。

三、引发重伤的基础

美国海因里奇根据调查统计结果，得出了致死伤害（包括重伤），轻伤和无伤害发生的概率之比为1：29：300，如图1—4所示。这比例表示发生于同一人的330件相似的意外事件中，其中300件不产生伤害，29件产生轻伤，只有一件产生重伤。根据国际劳工组织(ILO)的调查结果，这一比率为1：20：200。总之，伤害与无伤害之比为1：10，实际这个比例因事故的种类不同而异，坠落、触电的重伤比例较高。

这些比例仅用于累积平均的情况。重伤可由最先一事件产生，或由一群事件中任何一事件产生。从300：29：1比例中可看出，全部意外事件的0.003%产生重伤；8.8%产生轻伤；90.8%不产生伤害。

这个比例数字本身并无意义，但却表明了事件与伤害程度之间适合偶然性概率法则，对协助防止意外事件有很大意义，因为它强调防止事故发生机会的重要性。

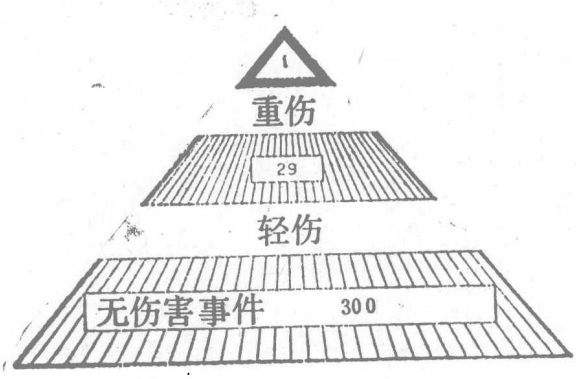

图1—4　300：29：1比例图

事实上，如把“意外事件”与“伤害”作为必然的因果关系，就会出现没有严重的伤害产生，就不会有严重的意外事件的误解。然而实际上，数以千计严重伤害的产生，是由于存在着产生伤害事件的潜在危险。例1，某工人在湿楼板上滑倒，致跌伤膝盖骨。此工人经常弄湿很大一片地板而不擦干已成了达6年之久的习惯，滑倒机会几乎每天发生。估计比例为1800：1：0。例2，某圆锯工人在锯木板工作时，由于违返规定，没有使用推杆，结果锯掉大拇指。完成此类工作，平均每天20次，达三个月之久，用此法已经超过1500次，曾有许多轻微的割伤和数百次的擦伤。估计比例为350：40：1。例3，某机械师企图用手把5英寸宽的皮带放在直径24英寸正在回转的带轮上时，结果被皮带轮卷进而碾死。此人经常穿一套宽大长袖工作服，站在摇动的梯子上，用手滑上皮带，当快速回转的皮带轮挂上静止的皮带时，他能及时的把手抽出来。此人使用此法挂皮带轮已有数年之久。曾有33次臂部及手部擦伤。估计比例为600：33：1。

潜在的伤害不仅危及很多人的生命，而且常常导致物资财富的损失。如有一客车加油站的工作人员，嗜好吸雪茄，当客车加油时，此人常疏于雪茄从他的口边掉下来，落到靠近加

油管附近多次，结果有一次致使一客车加油时发生火灾，造成17人死伤。

从上述几个例子可以得出这样的结论，即一大群伤害中，轻伤对产生意外事件的原因有很大的价值。同样，凡能造成意外事件及造成重伤或轻伤的不安全情况，应在伤害未产生之前予以改正。

Frank E. Bird, Jr. 也作了类似的研究。他于1969年，在美国297个公司作了调查，对1,753,498个事件进行分析。这些公司有21种不同类型的工业，工作超过3×10^9工作小时以上的有1,750,000职工。Frank E. Bird, Jr. 调查结果如图1—5所示。

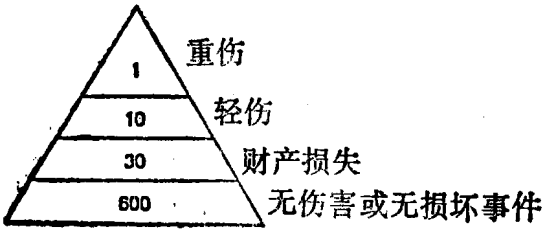

图1—5 Bird意外事件比率研究

图1—4中的1：29：300比例是在对同一人出现相似的意外事件的基础上进行分析研究得出的比例；而图1—5中所示的比例，是在很多不同类型意外事件中，对多数人进行分析的结果。

从Heinrich和Bird的分析研究，可以明显地看出，无伤害事件是重伤发生的基础。所以，研究重点应放在无伤害的意外事件，分析基础应放在重伤原因的意外事件上。

第二章　系统安全概述

一、系统安全的由来和发展

1947年9月，在美国航空科学学院（IAS）发表了题为“安全工程”（Engineering for Safety）的论文，在此论文中首次提出了系统安全的概念。直到本世纪60年代初，系统安全概念才被作为合同项目正式采用。

本世纪50年代末发展了导弹系统。到了60年代初，为了对军事武器系统危险性进行检验，因此需要尽快对系统安全问题进行研究。民兵式洲际弹道导弹（ICBM）发射控制系统安全性分析就是作为正式的系统安全研究科目之一。

1962年4月，美国空军发表了第一个有关系统安全开发的“空军弹道导弹系统安全工程学”（System Safety Engineering for the Development of Air Force Ballistic Missiles）的说明书。此后，随着对系统安全研究的深化，又扩大了说明书的应用范围。1963年9月，美国空军又拟定了军用标准MIL—S—38130。1966年6月，将这个标准修订为MIL—S—381308A。1969年7月将此标准再一次做了修订，最后修改成MIL—STD—882。这个标准不仅被定为美军装备合同上的必要条件，而且也是一般产业系统安全计划的有效方针。后来，美国国家航空和航天管理局（NASA）也制定了系统安全计划，对系统的危险性辨别、评价与控制方面取得了很大的成功。

在美国军事装备安全系统发展的同时，核武器和原子能产业的出现，也对安全性提出了极为重要的课题。为此，美国原子能委员会和国防部分别对有关核物质和核武器的处理实行了严格控制。这些规定的制订，可以说从另一个方面促进了系统安全的发展。

促进系统安全发展的另一个因素是产品安全。20世纪60年代以来，美国技术的飞速发展和环境的骤变，要求缩短新产品开发时间已势在必行。再象过去通过计划、设计、试制、改进等花费较长时间来研制新产品，煞费苦心地采用新技术，很可能还没有实现商品化就已陈旧不堪了。因此，很多新产品在没有充分确定安全性的情况下，就投放市场销售了。这也是20世纪60年代美国灾害大量发生的原因之一。后来，为了在较短的时间内研制出无损于安全性的新产品，也提出了系统安全研究的必要性。

随着工业的高度发展，设备的复杂程度增加，由于故障而带来的损失也在增大，人与机器之间关系的处理也愈来愈复杂。现在，系统安全方法不仅应用于军事工业、原子能工业方面，而且应用于许多需要用工程上的方法来解决问题的地方。如防止公害、预防事故与灾害、机械设备的研制、城市建设、交通、运输、通讯等部门。

二、系统安全术语

1.安全

“安全”一词，在拉丁文中为salvus，可译成卫生或安全之意。根据希腊的记载，“安

全”一词的来源是“完整”的意思。在梵语词中为“没有受伤”或“完整”之意。

根据韦伯斯特大词典（Webster's New International Dictionary），安全可做如下定义：

安全是免除了引起个人伤害、疾病、或死亡的状态；或者是免除了设备损坏或财产损失的状态；或者是免除了环境危害的状态。

根据上述定义，可以看出，安全是一种状态，解脱了暴露于危险状态，免除了伤害、灾害，或损失的状态。即处在安全状态（条件）下，则不会受到伤害、灾害、或者危险的影响，不再有危险或灾害的威胁；不致受到危险，或者损失威胁的危害。

2.系统安全

系统是相互间具有有机联系的组成部分结合起来，成为一个能完成特定功能的总体，这种各组成部分的有机的结合体就称为系统。

图2—1所示为一系统图。系统包含有输入E_i，系统模型F（S），输出E_0等三个要素。

图2—1 系统图表示

例如，有一客机和机内的所有成员为一系统，假定确定的目的是将机内成员及货物运往某一目的地。此系统包括的要素E_i，F（S），E_0应做如下考虑：

（1）系统输入E_i：如天气状况、维修及大检修状况，机组人员的培训情况，个人条件，以及对付突然事态变化的应变能力等等。

（2）系统模型F（S）：如满足一定高度的速度需要的燃料消耗情况；由于强风引起的偏航、倾斜状况；由于飞机着陆速度及着陆状态作用引起的制动机构变化情况等等。

（3）系统输出E_0：系统输出E_0决定于输入E_i，即根据不同的输入情况产生不同的输出情况。

根据E_i的情况，有两种E_0情况，一种是没有危险出现，即任何危险出现时都能控制，这种情况，输出E_0表示了安全状态。另一种是出现一次，或更多次危险，至少有一次危险不能控制，这种情况，输出E_0表示了不安全状态。

一个系统的安全，与多方面因素有关，如提供的程序、系统的设备、使用人员、合理的操作条件等等都会影响系统的安全。

系统的安全与控制和合理性两个基本方面有关。前者是为了使设备不受损坏及保障人身安全，对危险性要进行辨别与控制。控制与系统安全的“安全”有关。后者合理性是与系统安全的“系统”有关的。因此，系统安全包括了两方面内容，控制与合理性。

系统安全可做如下定义：

系统安全是一种最佳安全状态，包括运行效能、时间、成本，以及其它适用于与安全有关方面处于最佳状态。也就是，能实现整个系统的安全状态。

3.危险性及其分类

安全性的对立面为危险性。

产生灾难或存在潜在状态的灾难称为危险性。

这里灾难是指没有计划的事件的出现，如人身伤害；疾病或死亡；设备损坏或财产损失；以及环境的危害等。

在人们的生活中，说不定会遇到一些意外的灾害危险。要完全根除全部灾害，往往是难以做到的。例如，预测到大的危险性，即使对之采取了全面对策，但只要稍有漏洞，就会残留发生危险的可能性。另外，用于防止灾害的资金和人力，也往往是有限度的。所以，要使那些危险性比较高的灾害发生的可能性尽量降低，或者万一发生灾害时，尽量把它的受害程度控制在较轻的程度上。

在MIL-STD-882A标准中提供了确定危险严重程度的分类等级（见表2—1）。

表2—1

分类等级	危险性	设备破坏	伤害
Ⅳ	安全的（Safe）	无	无
Ⅲ	临界的（Marginal）	较小	无，或较轻伤害
Ⅱ	危险的（Critical）	主要系统损坏	较轻，或严重伤害
Ⅰ	破坏性的（Catastrophic）	系统损失	严重伤害或死亡

第Ⅳ类：安全的。由于人的失误、设计缺陷，或设备出现故障，没有造成个人伤害，或者设备的损坏。

第Ⅲ类：临界的。由于人的失误、设计缺陷、或设备出现故障使系统性能降低，或设备出现故障，但能控制住严重危险的产生，或者说还没有产生有效的破坏。

第Ⅱ类：危险的。由于人的失误、设计缺陷，或设备故障，造成个人伤害，或严重的设备破坏，需要立即采取措施来控制。

第Ⅰ类：破坏性的。由于人的失误、设计缺陷，或设备故障，严重地降低系统的可靠性，造成随之而来的系统损失，或者造成人员的严重伤害或死亡。

危险性等级可根据危险系数C。加以确定，如表2—2所示。

表2—2

危险等级	危险系数 Cs
Ⅰ	>7～10
Ⅱ	>4～7
Ⅲ	>2～4
Ⅳ	<2

危险系数C。与表2—3中所示的每个评分要素的危险系数C_i有关。危险系数C_i根据评分5项要素来确定。C_i确定之后，可按照下式计算出危险系数C。：

$$C_。=(C_1 \cdot C_2 \cdots\cdots C_i)^{1/i} \qquad (2—1)$$

式中

C。—危险系数；

C_i—第i个评分要素危险系数，$1 \leqslant C_i \leqslant 10$；

i—评分要素，$1 \leqslant i \leqslant 5$。

表2—3

评分要素 i	危险系数 Ci
1.功能性故障影响的重要程度	Ci = 1～10
2.影响系统范围	
3.故障发生频率	$1 \leqslant i \leqslant 5$
4.故障防止的可能性	
5.新规范设计程度	

例：假定有一设备，根据现场调查获得的统计数据，估计各要素危险系数分别为：$C_1=2$，$C_2=4$，$C_3=5$，$C_4=8$，$C_5=10$。求此设备的危险系数C。。

$$C_。=(C_1 \cdot C_2 \cdot C_3 \cdot C_4 \cdot C_5)^{1/i}$$
$$=(2\times4\times5\times8\times10)^{1/5}$$
$$=5.0237729\approx5$$

根据计算结果可知，危险性等级为第Ⅱ类，属于危险性的等级分类。

4.危险矢量

危险矢量（Hazard Vector）是衡量系统危险程度的指标，可用危险程度来表示。

危险程度与两个因素有关，一个是与危险作用的严重程度有关（如危险等级分类中属于那种分类，用C表示），另一个是与此种危险出现的概率（P）有关。

即

$$HL=f(C_i, P_i) \qquad (2—2)$$

式中

HL—危险程度；

C_i—与第i种危险有关的加权因数（建立在四种危险等级分类基础上）；

P_i—第i种危险出现的概率。

由上式可以看出，与第i种危险有关的一对值（C_i，P_i）确定了危险矢量。一般来说，C相当于方向、范筹，P等于大小。

5.最佳系统安全

最佳系统安全就是确定系统安全的最佳特性，或选择系统安全的最佳条件。要获得“最佳安全”的系统，就必须应用科学的知识和科学的研究方法作出各种可能达到目标的比较方案。比较方案涉及到对各种结构形式的选择，如系统模型F（S）和系统输入E_i的选择。实际上，在工程技术、可靠性、维修性设计中，在人员的教育培训以及其他与安全有关学科设计中可以采用这种比较选择方法获得最佳安全系统。即在方案比较过程中，在产生最佳安全情况的过程中来选择。

在进行方案比较时，系统应具备如下几个特点：

a.具有最简单的系统结构。

b.操作和维修作业要简单化。

c.确保当系统任一组成部分失效时，也不能导致整个系统失效，或出现死亡事故。

d.应当提供表明系统某部分失去工作能力而由此可能导致整个系统失效的指示仪器。

没有系统的输出目标E_0，则不可能作出方案选择的评价。但是，若给输出目标E_0的定量值则是困难的。因此，E_0和F（S）通常是建立在要求人体不受伤害基础上来考虑。

6.系统安全范围

系统安全是属于多学科领域范畴的。要完成系统安全的功能和职责，需要具有广泛的科学知识以及各种学科的相互配合。例如，伤害或财产损失可能由以下几点因素造成：

a.设计、材料或加工质量上的缺陷。

b.由于制造、试验，以及运转负荷而造成功能降低。

c.在操作或维修中，由于人的疏忽或失误造成的差错。

d.环境对系统的影响，如其他系统或自然环境对本系统的影响。

e.意外事件的出现。

从上述几点因素可看出，预防伤害或财产的损失不是一门学科所能解决的，需要各种学科综合运用，相互配合。

系统安全不仅要解决单一危害问题，而且要解决综合性危害问题。

（1）单一危害

一般来说，从所分析系统内的所有事件能产生危害来考虑，因此，系统安全具备多学科特性。这些危害包括机械危害和操作危害，其定义如下：

机械危害，是一种约束或阻止一定的设备运行的危害。以一个或更多单元的失效或降低功能来出现这种危害。

操作危害，是一种不产生设备或系统失效的危害。尽管如此，还是约束或阻止了系统的功能。

例如，太阳光辐射干扰无线电通讯就是一种操作危害，辐射产生的天线电干扰可能阻碍了通讯，但不破坏设备本身。

另一种比较明确表述的危害分类，是按照内因危害和外因危害来分。

内因危害是一种由于设计、材料、加工质量，或操作程序等一系列缺陷而造成的危害。

外因危害是由于系统外界现象对该系统作用而产生的危害。例如，闪电或宇宙辐射等。

以上二者之间的主要区别是：内因危害是由于系统内部自身引起的；而外因危害则是由于系统外界因素作用而使系统失效。

（2） 综合危害

除了单一危害之外，还应考虑在安全分析中各种危险因素组合起来作用是非常有必要的。特别是一些危害组合一起，或一定类型危害组合一起而出现系统危险时，就不能仅仅考虑单一危害作用，应当综合考虑。

例如，辐射危害就是综合危害作用的情况。大约30年以前，平均每人受到周围环境的辐射量小于1毫雷姆每小时。第一次原子弹爆炸以后，以及核武器的试验已经增加了周围环境的地面辐射。

据国外一些人的主张，由于原油和天然气是有一定使用限度的，人们期望广泛利用各种辐射源，特别是在世界上很多国家想利用核反应发电。根据一些学者的看法，这样做的结果可能将会出现三个问题，一是核反应容器如果发生故障，则将会出现射线逸出或核辐射物质进入大气；二是核发电所排出的放射性废物有可能会污染环境；三是逸出的放射性物质在70,000英尺高空超速扩散。

综上所述，平均每人受到周围外界的辐射量有所增加。

7.系统寿命周期

对于一个系统，从系统初步设计阶段（或称阐明概念）开始到系统操作运行整个过程称做系统寿命周期。一般系统寿命周期的图解形式如图2—2所示。它包括系统初步设计（阐明概念）、系统技术设计（合同制定）、系统研制（开发）、系统生产以及系统操作运行等阶段。有的系统寿命周期将清理阶段包括进去，做为寿命周期的最后阶段。图2—2中的各个阶段都有一定的重叠，而且任一阶段所得到的信息可以反馈给先开始的阶段。寿命周期不同阶段之间的重叠部分，不同系统当然各不相同。

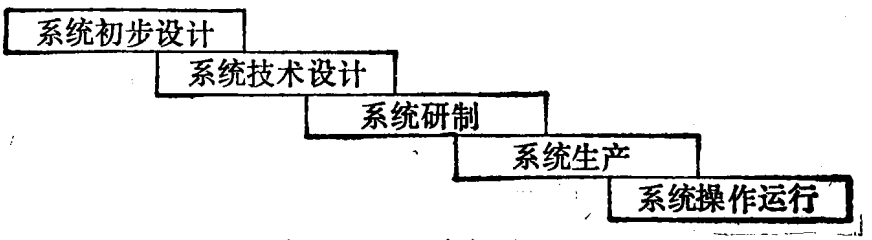

图2—2 系统寿命周期

在系统初步设计阶段，要完成以下几方面主要内容：

（1） 评价作为不同设计特性的系统安全条件而采取的技术途径。另外，开始进行从各种可能的方案中选择最佳方法。

（2） 对新型的或是有工艺水平发展的技术，在此阶段需要确定安全调查范畴。

（3） 确定系统安全运行所需的参数。例如，容许的最大事故率或容许的死亡人数。这项

工作对系统设计和试验有着深远的意义。

（4）在这阶段应确定需要进行特殊安全研究的范围。例如，需要建立系统新的安全比率要求，系统的使用限制，或系统试验中容许承担的风险数量和类型。

系统技术设计阶段一般分为三个阶段。在前两阶段进行的系统安全工作主要有以下几方面：

（1）提出系统安全程序计划的初步草案。

（2）进行危险性分析。其目的是判断在系统中将会出现什么危险，以及估价有关使用或操作系统的风险。

（3）制定系统说明中的有关安全要求和限制问题。

（4）解决签定合同的有关问题。

在第三阶段进行的主要工作则在于确定并开始系统寿命周期的研制、生产和运行阶段所需的工作。

在系统研制阶段的工作是：提供设计标准；评价系统安全状况；规定系统的操作者和用户的培训项目；审查试验计划，确保设计的安全性都能经过足够的试验；拟定故障和事故的报告系统；建立描述险情分析以及危险发生的方法。

系统生产阶段的安全工作主要是确保在前面阶段已达到的安全水平保持下来。

系统操作运行阶段通常进行的工作包括：

（1）对在这一阶段中所有运行的设备和生产过程的变化进行评价，以确保早先达到的安全水平不致下降。

（2）检查运行情况，以确保在此阶段中所进行的维修过程本身无危险性，不降低原有的安全水平，也不引起由于系统外部原因发生的危害。为此，需要扩大危险性分析，以便辨识由于维修活动而造成的一些问题。为确保在维修后不会给系统带来任何危险，需要确定适宜的质量特性。

（3）调查在运行阶段所发生的所有意外事件。这项工作包括检查失灵和发现危险征兆。

在清理阶段要作的基本工作包括检查、处理系统危险物使用的方法，以确保系统正常地进行。

8.危险分析与系统寿命周期关系

图2—3所示为系统寿命周期与危险分析的关系。图形的下面部分与图2—2相同，为系统寿命周期图。图形上面部分为系统进行危险性分析的不同类型。系统各个阶段和不同类型危险性分析是相对时间而言的。因此，这个图形表明了危险分析的特点是怎样随系统寿命周期的每个阶段而变化的。在系统寿命周期初期阶段，危险性分析重点放在通过分析修改设计来消除那些发现的危险。在寿命周期的随后各阶段，当系统设计更加详细具体，以及生产即将开始时，危险分析的重点转移到危险控制。

在系统寿命初步设计阶段的早期阶段，设计的变更可能受到系统图修改的影响，但这种变化的串级影响是小的。在寿命周期随后阶段，如果进行同样的修改，则可能要改变详图和相关图，以及系统图。因此，增加了串级影响和增大了结构管理的工作量。在寿命周期的后期，变更设计将会带来更大的问题，不仅成本高，而且每一改变需要花费更多的时间。因此，这些改变将导致进度错动，进度错动本身可能产生把不安全因素带入系统的问题。