

系统安全工程

XITONG ANQUAN
GONGCHENG

牟瑞芳 编著



西南交通大学出版社
[Http://press.swjtu.edu.cn](http://press.swjtu.edu.cn)

系统安全工程

牟瑞芳 编著

西南交通大学出版社

· 成 都 ·

图书在版编目 (C I P) 数据

系统安全工程 / 牟瑞芳编著. —成都: 西南交通大学出版社, 2014.3
ISBN 978-7-5643-2788-0

I. ①系… II. ①牟… III. ①交通运输安全—安全工程—高等学校—教材 IV. ①U491

中国版本图书馆 CIP 数据核字 (2013) 第 307651 号

系统安全工程

牟瑞芳 编著

责任编辑	周 杨
封面设计	墨创文化
出版发行	西南交通大学出版社 (四川省成都市金牛区交大路 146 号)
发行部电话	028-87600564 028-87600533
邮政编码	610031
网 址	http://press.swjtu.edu.cn
印 刷	四川森林印务有限责任公司
成品尺寸	185 mm × 260 mm
印 张	19
字 数	475 千字
版 次	2014 年 3 月第 1 版
印 次	2014 年 3 月第 1 次
书 号	ISBN 978-7-5643-2788-0
定 价	36.00 元

图书如有印装质量问题 本社负责退换
版权所有 盗版必究 举报电话: 028-87600562

前 言

随着经济的发展以及社会的不断进步,人们对于安全的需求日益增大,安全意识逐步提高。把安全生产、职业安全健康的管理、教育、科研和技术提高到更科学、理性、高效和精确的层次及水平,已成为安全工程教育和科研工作者的任务之一,也是社会的迫切需要。我国越来越多的高校增设了安全工程专业,培养了大批安全工程专业高素质人才。由于不同行业安全问题的差异,目前系统安全工程的教材百家齐放、各有特色,尚没有一本比较通用的适合不同行业安全工程专业的教材和参考书。作者在阅读国内外安全工程教材参考书和相关文献的基础上,结合多年教学和科研的工作经验,力争形成适合安全工程专业的通用的教材和参考书。

系统安全工程是安全工程专业重要的专业基础课。根据教育部安全科学与工程教学指导委员会对安全工程专业的要求,本书在编写过程中不仅侧重基本概念、系统安全理论以及系统安全分析与评价的理解和运用,而且注重系统安全理论的系统性、逻辑性和前瞻性。全书分为五章。第一章主要讲述安全科学发展历程以及系统安全相关概念。以人-机-环系统为主线,体现系统安全思想,为后续系统安全分析和评价奠定基础。第二章主要讲述事故致因理论。按照理论发展历程,将事故致因理论分为朴素的、近代的和现代的不同阶段,对每一种事故致因理论的特点、适用条件分析事故发生的规律,指出危险因素是事故发生的根本原因。第三章根据事故致因理论,讲述危险有害因素的概念、分类以及辨识方法。第四章和第五章分别从定性和定量角度进行系统安全分析。对每一种安全分析方法从原理、理论到方法的应用几个角度进行讲述。对复杂问题、抽象理论、复杂方法和技术尽量做到结合实际案例进行分析,有助于读者理解、吸收和应用。对每一系统安全分析方法给出了相应的分析模型。同时,每一章都配有一定数量的练习题。

在本书的编写过程中,研究生王列妮、徐梦秋、余强、游鹏飞、韩伟和杨锐等在资料收集和整理过程中付出了辛勤劳动。本书参考了国内外安全工程领域的研究成果,谨向原作者和出版社致以崇高的敬意和诚挚的感谢。

由于安全工程学涉及的领域非常广泛,安全工程学理论和方法体系还在不断研究和探索,虽然编者在本书的系统性、整体性、前瞻性和实用性等方面付出了极大的努力,也做了一些有益的尝试,但是由于编者学术水平有限,加之时间仓促,书中难免存在疏漏之处,恳请专家学者和广大读者批评指正。

编 者

2013 年 9 月

目 录

第1章 绪 论	1
1.1 国内外安全科学的发展历程	1
1.2 系统安全工程	3
1.3 人-机-环系统	16
1.4 基本概念及相互关系	20
复习思考题	24
第2章 事故致因理论	25
2.1 概 述	25
2.2 事故致因理论	27
2.3 危险因素辨识	42
复习思考题	51
第3章 危险因素辨识定性分析方法	52
3.1 安全检查表	52
3.2 因果图表	60
3.3 预先危险分析	61
3.4 危险和可操作性分析	68
3.5 如果……怎么办	84
3.6 操作与支持危害分析	88
3.7 安全要求/标准分析	100
3.8 故障风险分析	106
3.9 功能风险分析	110
3.10 屏障分析	120
复习思考题	132
第4章 危险因素定量分析方法	133
4.1 统计图表法	133

4.2 故障类型及影响分析	140
4.3 事件树分析	154
4.4 事故树分析	165
4.5 马尔科夫分析	215
4.6 共因失效分析	227
复习思考题	245
第 5 章 系统安全评价	246
5.1 概 述	246
5.2 安全评价方法	260
复习思考题	296
参考文献	297

第1章 绪论

安全工程是20世纪60年代迅速发展和完善的一门崭新的学科。它是以生产过程中的人、机、环境系统为研究对象,以消除和控制系统中的危险因素为目的,把要研究的安全问题,经分析、推理、判断建立某种安全系统模型,进而用系统工程的方法和理论进行分析、预测、评价,并采取防范措施消除或控制系统中的不安全因素,杜绝系统事故的发生或使事故发生减少到最低限度,使系统达到最佳的安全状态。它在保证安全生产方面显示了巨大的效果。

在国外,系统安全工程已得到广泛的应用,成为工业生产中必须采用的安全技术。在国内,随着我国走向世界,系统安全工程正在受到极大的重视。从系统安全工程的教育、研究到工程实践都得到长足的发展。

实践证明,系统安全工程是搞好安全工作、降低伤亡事故和财产损失的有效手段。系统安全工程的普及和推广,将有助于我国安全面貌的改善和安全管理水平的提高。

本章主要阐述安全、交通安全等基本概念,强调系统的安全以及安全科学的发展及其理论体系。

1.1 国内外安全科学的发展历程

1.1.1 国外安全科学发展历程

16世纪,西方国家开始进入资本主义社会,至18世纪中叶,蒸汽机的发明使劳动生产率空前提高,但劳动者在自己创造的机器面前致病、致伤、致残、致死事故与手工时期相比也显著地增加了。起初,资本所有者为了获得最高利润率,把保障工人安全、舒适和健康的一切措施视为不必要的浪费,甚至还把损害工人的生命和健康,压低工人的生存条件本身看作不变资本使用上的节约,以此作为提高利润的手段。

后来由于劳动者的斗争和大生产的实际需要,迫使西方各国先后颁布劳动安全方面的法律和改善劳动条件的有关规定。这样,资本所有者不得不拿出一定资金改善工人的劳动条件。同时需要一些工程技术人员、专家和学者研究生产过程中不安全、不卫生的问题。从而许多国家先后出现了防止生产事故和职业病的保险基金会等组织,并赞助建立了无利润的科研机构,如德国于1863年建立的威斯特伐利亚采矿联合保险基金会,1887年建立的公用工程事故共同保险基金会和事故共同保险基金会等;1871年德国建立了研究噪声与振动、防火与防爆、职业危害防护理论与组织等内容的科研机构;1890年荷兰国防部支持建立了以研究爆炸预防技术与测量仪器,以及进行爆炸性鉴定的实验室。到20世纪初许多西方国家建立了与安

全科学有关的组织和科研机构。据 1977 年统计,德国建立 36 个,英国 44 个,美国 31 个,法国 46 个,荷兰 13 个。从内容上看,有安全工程、卫生工程、人机工程、灾害预防处理、预防事故的经济学、职业病理论分析和科学防范等。美国的安全教育发展较快,到 70 年代末,一部分大学设立了卫生工程、安全工程、安全管理、毒物学和安全教育方面的硕士和博士学位。日本在研究安全方面虽起步较晚,但发展却较快,它注重吸收世界各国的经验和教训,在安全工程学这一科学技术层次上进行了研究和发展。到 1970 年为止,日本大学增设了反应安全工程学、燃烧安全工程学、材料安全工程学和环境安全工程学等四个讲座课程,继而又在研究生院设置了硕士课程。至 1977 年,在日本大学中开设有关安全工程学讲座课程或学科的总计为 48 个,现在日本国内与安全工程有关的大学教育系和研究机构达 76 个,杂志 36 种,学会和协会 33 个。由于坚持安全工程学的研究和实践,日本近 20 年来产业事故频率、死亡人数逐年下降,持居世界最低水平,安全工程学在日本日益受到人们的重视。

由此可见,为了解决生产过程中劳动者的安全 and 健康,国外对安全科学的研究已有足够的深度和广度。这说明安全科学作为一门真正的交叉科学正日益受到越来越多的人重视。

1.1.2 国内安全科学发展历程

在 20 世纪 80 年代初期,我国安全研究和管理人员深感必须采用系统工程方法,才能真正改变企业被动的安全局面。换言之,必须先发现问题,采用系统工程方法找出系统中存在的所有危险源,加以辨识、分析和评价,从而找出解决问题的措施,防患于未然,我国安全研究和应用也大致经历了四个发展阶段:

1. 安全技术工作和系统安全分工合作时期

初期安全工作者和产品系统安全工作者的分工是明确的,前者负责工人的安全,后者负责产品的安全,两者分工协作、密切配合,共同完成生产任务。

2. 安全技术工作引进系统安全分析方法阶段

由于系统安全分析是针对系统各个环节本身的特点和环境条件进行定性和定量的安全性分析,做出科学的评价,并据此采取针对性的安全措施,所以这种方法对安全工作十分有用。

3. 安全管理引用安全系统工程方法阶段

由于安全系统工程不仅可以评价各个环节的可靠性和安全性问题,而且对系统开发的各个阶段也可以进行评价。因此,企业的安全管理各阶段(检查、操作、维修、培训)都可以使用这种方法提高系统性和准确性。

4. 以安全系统工程方法改革传统安全工作阶段

在安全工作中广泛使用安全系统工程方法,使传统安全工作进行改革的趋势需要不断地在实践中总结经验。目前,贯穿系统科学思想的安全管理方法不断涌现,并延伸出很多新学科。

2011 年 3 月 8 日,国务院学位委员会和教育部联合发布了“关于印发《学位授予和人才培养学科目录(2011 年)》的通知”(学位〔2011〕11 号)。在《学位授予和人才培养学科目

录(2011)》中,将安全学科列为一级学科(原仅是矿业工程下的二级学科),成为工学门类中三十八个一级学科之一,具体名称为安全科学与工程,代码为0837。

安全学科自20世纪50年代建立本科始发展至今,设立“安全工程”本科的高校有127所,硕士有46所,博士有20所,年招收本科生、硕士生、博士生分别为7000名、1000名和280名左右。近年来的实践显示,安全学科能否独立为一级学科已成为安全学科建设与发展,以及安全人才培养壮大的瓶颈。

1.1.3 理论发展阶段

安全科学的发展从理论上讲大体分为三个阶段:

1. 经验型阶段(事后反馈决策型)

长期以来,人们认为安全仅仅是以技术形式依附于生产,从属于生产,仅仅在事故发生后进行调查研究、统计分析和整改措施,以经验作为科学,安全处于被动局面,人们对安全的理解与追求是自发的、模糊的。

2. 事后预测型(预期控制型)

人们对安全有了新的认识,运用事件链分析、系统过程化、动态分析与控制等方法,达到防止事故的目的。总之,传统的安全技术建立在事故统计基础上,这基本属于一种纯反应式的。安全科学缺乏理性,人们仅仅在各种产业的局部领域发展和应用不同的安全技术,以至对安全规律的认识停留在相互隔离、重复、分散和彼此缺乏内在联系的状态。

3. 综合系统论(综合对策型)

认为事故是人、技术与环境的综合功能残缺所致,安全问题的研究应放在开放系统中,建立安全的科学性、系统性、动态性。从事故的本质中去防止事故,揭示各种安全机理并将其系统化、理论化,变成指导解决各种具体安全问题的科学依据。在这一阶段中安全科学不仅涉及人体科学和思维科学,而且涉及行为科学、自然科学、社会科学等所有大的科学门类。

1.2 系统安全工程

1.2.1 概念

1. 系统

(1) 系统的定义。

系统是由相互作用、相互依赖的若干元素结合而成的具有特定功能的有机整体。任何一个系统都应该符合以下条件:

- ① 元素。系统必须由两个以上的元素所组成。
- ② 元素间的联系。系统的各元素间互有联系和作用。

③ 边界条件。系统元素受外界环境和条件的影响。

④ 输入、输出的动态平衡。系统元素有着共同的目的和特定的功能，为完成这些功能，系统必须保持输入、输出的动态平衡。

(2) 系统的特点。

系统具有目的性、整体性、集合性、相关性、环境适应性和动态性等特征。这里对系统的四个主要特点说明如下：

① 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。

② 整体性。系统的定义就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地组合，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。

③ 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、储存、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。

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，而且在研究和使用时，必须重视环境对系统的作用。

(3) 系统的功能结构。

为了实现系统自身的正常运行和功能，系统需要以一定的方式构成，应具有保持和传递能量、物质和信息的特征。系统种类繁多，根据控制论观点，系统由三部分组成，即输入、处理和输出，如图 1.1 所示。任何系统都具有输出某种产物的功能。例如运输企业，它输入原材料、能源、信息，经过组织或作业，最后输出，产生了人或物的空间位移，称为运输生产系统。再如，若以信息流为主体的系统，如一项计划可视为输入，计划经过执行，即处理阶段，最后得到的结果视为输出。这种系统称为管理系统。

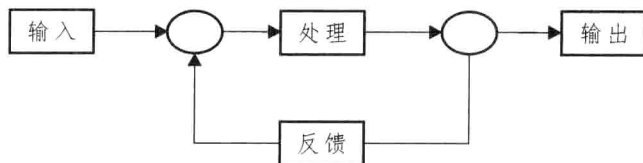


图 1.1 系统功能结构示意图

处理后得到的结果与原定目标不一致时，需要修正，改善执行环节。以达到预期的目标。这个过程就是反馈。

2. 系统工程

(1) 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

化学工程、建筑工程、采矿工程、电气工程、交通运输工程等，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”，如人机工程、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。

（2）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。

系统工程不仅涉及具体的工程，如化学工程、机械制造工程、电气工程等科学技术领域，而且还涉及信息论、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，经济上最可靠，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。

系统工程就是从系统的观点出发，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、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。

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。

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。

系统工程具有以下三个特点：

① 研究方法的整体性。即把研究对象看作一个整体，同时，把研究过程也看作一个整体，按系统工程的三维结构，即时间维（工作阶段）、逻辑维（思维步骤）和知识维整体配合研究解决问题。

② 应用学科的综合性。综合运用多学科理论和管理工程技术，揭示并协调系统各要素之间以及系统与外部环境之间的关系，为实现系统整体功能最优化提供决策、计划、方案和方法。

③ 组织管理的科学化。运用数学方法、计算机技术定量（或定量与定性相结合）分析、评价系统构成和状态，以达到最优设计、最优控制和最优管理的目标。

1.2.2 系统安全理论

1. 系统安全的概念

系统安全 (System Safety) 是指在系统生命周期内应用系统安全工程和系统安全管理方法, 辨识系统中的危险源, 并采取有效的控制措施, 使其危险性达到最小, 从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。系统安全是人们为解决复杂系统的安全性问题而开发、研究出来的安全理论、方法体系。系统安全与系统危险的关系参见图 1.2。

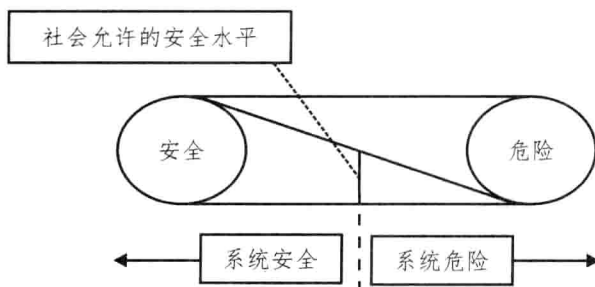


图 1.2 系统安全与系统危险的关系

系统安全的基本原则就是在一个新系统的构思阶段就必须考虑其安全性的问题, 制定并执行安全工作规划 (系统安全活动), 并且把系统安全活动贯穿于生命整个系统生命周期, 直到系统报废为止。

系统安全泛指系统中的安全性, 它与系统中的可靠性等同为系统的特定性能指标, 注意它和“安全系统”一词的不同。

20 世纪 50 年代以来, 科学技术进步的一个显著特征是设备、工艺及产品越来越复杂。战略武器的研制、宇宙开发及核电站建设等使得作为现代科学技术标志的大规模复杂系统相继问世。这些复杂系统往往由数以千万计的元素组成, 元素之间以非常复杂的关系相连接, 在被研究制造或使用过程中往往涉及高能量。系统中的微小差错就会导致灾难性的事故, 大规模复杂系统安全性问题受到人们的广泛关注。

1947 年 9 月, 美国航空科学院报道了一篇题为“安全工程”的论文, 文中写道: “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。安全组也像应力组、空气动力组和荷载组一样, 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。

系统安全的基本思想是人们在研制、开发、使用、维护这些大规模复杂系统的过程中, 逐渐萌发的。在 20 世纪 50 ~ 60 年代美国研制洲际导弹的过程中, 系统安全的理论逐渐形成。

导弹的推进剂是一种气体加压到 420 kg/cm^2 、温度低达 -196°C 的低温液体, 这种推进剂的化学性质非常活泼, 且有剧毒。其毒性远远超过第一次世界大战中使用的毒气的毒性, 其爆炸性比烈性炸药更强烈, 并且比工业中使用的腐蚀性化学物质更有腐蚀性。当时负责该项目的美国空军的官员们并没有认识到他们着手建造的导弹系统潜伏着巨大的危险。在洲际导弹试验开始的头一年半里就发生了四次爆炸, 损失惨重。事故调查结果表明, 主要原因是产品安全性存在重大问题。于是, 这个产品被报废, 重新进行设计。美国空军于 1962 年明确

提出了以系统工程的方法研究导弹系统安全性的文件。1963年美国空军制定了“系统和有关子系统以及设备的安全工程通用要求”，作为系统和设备的设计指导。1966年美国国防部对空军的标准作了修改，发布了自己的标准。1969年又再次修订了这个标准，发布了“系统、有关子系统与设备的系统安全大纲”，在这个标准中首先建立了较为完善的系统安全的概念，以及安全分析、设计和评价等的基本原则。

2. 系统安全理论的主要创新观点

系统安全理论包括很多区别于传统安全理论的创新概念，主要表现在：

(1) 在事故致因理论方面，改变了人们只注重操作人员的不安全行为，而忽略硬件的故障在事故致因中作用的传统观念，开始考虑如何通过改善物的系统的可靠性来提高复杂系统的安全性，从而避免事故。

(2) 没有任何一种事物是绝对安全的，任何事物中都潜藏着危险因素，通常所说的安全或危险只不过是一种主观的判断。能够造成事故的潜在危险因素称作危险源，来自某种危险源的造成人员伤亡或物质损失的可能性叫做危险。危险源是一些可能出问题的事物或环境因素，而危险表征潜在的危险源造成伤害或损失的机会，可以用概率来衡量。

(3) 不可能根除一切危险源和危险，可以减少来自现有危险源的危险性，宁可减少总的危险性而不是只彻底去消除几种选定的危险。

(4) 由于人的认识能力有限，有时不能完全认识危险源和危险，即使认识了现有的危险源，随着生产技术的发展，新设备、新技术、新工艺、新材料和新能源的出现，又会产生新的危险源。由于受技术、资金、劳动力等因素的限制，对于认识了的危险源也不可能完全根除。由于不能全部根除危险源，只能把危险降低到可接受的程度，即可接受的危险。安全工作的目标就是控制危险源，努力把事故发生概率降到最低，即使发生事故时，也可把伤害和损失控制在较轻的程度上。

(5) 系统安全中的人失误。作为系统安全应用对象的导弹系统、武器系统是一些由机械、电子零部件组成的硬件系统，当把系统安全推广到核电站等包括人在内的系统时，就又遇到了人的因素问题。人作为一种系统元素，发挥功能时会发生失误（Error）。这与以往工业安全中的术语“人的不安全行为”不同，系统安全中采用术语“人失误”（Human Error）。

里格比（Rigby）认为，人失误是人的行为的结果超出了系统的某种可接受的限度。换言之，人失误是指人在生产操作过程中实际实现的功能与被要求的功能之间的偏差，其结果可能以某种形式给系统带来不良影响。

人失误产生的原因包括两方面：

一是由于工作条件设计不当，即可接受的限度不合理引起人失误；

二是由于人员的不恰当行为造成人失误。除了生产操作过程中的人失误，还要考虑设计失误、制造失误、维修失误以及运输保管失误等，因而较以往工业安全中的“不安全行为”，人失误对人的因素涉及的内容更广泛、更深入。

3. 系统安全的思想

系统安全理论是为解决复杂系统的安全问题而开发、研究出来的安全理论、方法体系。系统安全的思想，就是应用系统安全工程解决安全问题的思想。系统安全的思想是安全生产

的灵魂，是企业职工必须具备的最基本素质。系统安全的思想反映在三个方面：

（1）安全是相对的思想。

长期以来，人们一直把安全和危险看作截然不同、相互对立的。系统安全的思想认为，世界上没有绝对安全的事物，任何事物中都包含有不安全的因素，具有一定的危险性。安全是通过系统的危险性和允许接受的限度相比较而确定，安全是主观认识对客观存在的反应，这一过程可用图 1.3 加以说明。

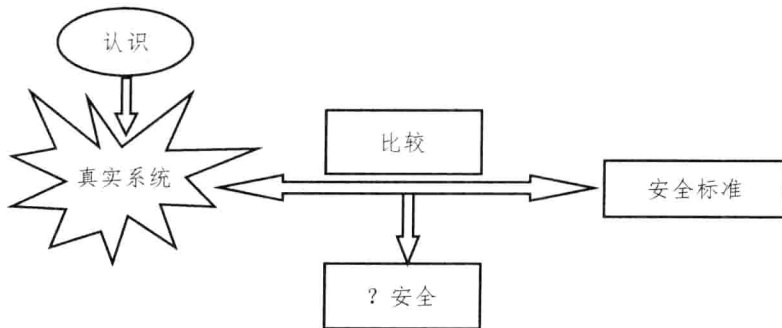


图 1.3 安全的认识过程

因此，安全工作的首要任务就是在主观认识能够真实地反映客观存在的前提下，在允许的安全限度内，判断系统危险性的程度。在这一过程中要注意：

- ① 认识的客观、真实性；
- ② 安全标准的科学、合理性。

所以安全是伴随人们的活动过程。它是一种状态，与时、空相联系。

（2）安全伴随着系统生命周期的思想。

系统的生命周期从系统的构思开始，经过可行性论证、设计、建造、试运转、运转、维修直至系统报废（完成一个生命周期），其各个环节都存在不同的安全的问题。要充分认识系统生命周期中安全的两个方面：

① 本质化安全。本质安全是系统安全的根本保证，从系统的构思、设计开始就融入系统，对系统有两个基本的要求。一是系统正常运行条件下本身是安全的，也就是系统在其生命周期中不依赖保护与修正安全设备也能安全运行。二是系统的故障安全，也就是系统在失去电或公用工程时，系统能保持稳定状态。本质安全是系统的理想状态，是安全工作所追求的目标。

② 工程化安全。工程化安全思想是对本质安全的补充，其主导思想就是应用工程安全保护设备进一步加强系统在其生命周期中的安全性，但是必须确保工程安全设备在系统出现问题时不产生故障。

本质安全和工程化安全构成了系统生命周期安全的思想。

（3）系统中的危险源是事故根源的思想。

危险源是可能导致事故的潜在的不安全因素。任何系统都不可避免地存在某些危险源，而这些危险源只有在触发事件的触发下才会产生事故。

有关危险源的分类方法很多，这里只介绍一种：

第一类危险源：根据能量意外释放理论，能量或危险物质的意外释放是伤亡事故发生的本质。于是，把生产过程中存在的，可能发生意外释放的能量（能源或能量载体）或危险物质称为第一类危险源。

第二类危险源：导致能量或危险物质约束或限制措施破坏或失效、故障的各种因素，称作第二类危险源。它主要包括物的故障、人为失误和环境因素。

一起伤亡事故的发生往往是两类危险源共同作用的结果。第一类危险源是伤亡事故发生的能量主体，决定事故后果的严重程度；第二类危险源是第一类危险源造成事故的必要条件，决定事故发生的可能性。

综上所述，安全工作的一个重要指导思想就是辨识系统中的危险源和消除触发事件的思想。

如何解决危险源问题？应从以下三个方面思考：

① 识别危险源。就是具有专门安全知识与技术的人员，利用现代安全检测技术及设备，应用危险源识别方法与技术进行系统的危险辨识。

② 危险源的评价分析。目的是得到各危险源引发事故的可能性和后果严重程度，对危险源进行排序。

③ 危险源的控制。就是应用由工程技术（Engineering）对策、教育（Education）对策和法制（Enforcement）对策组成的“3E”对策进行危险源的综合控制。

1.2.3 系统安全工程

目前国内有两种提法，一是系统安全工程（System Safety Engineering），二是安全系统工程（Safety System Engineering）。有关这方面的争议是学术上的一种讨论。本书主张系统安全工程的提法，这也是国外较流行的提法。

1. 系统安全工程的定义及发展过程

（1）系统安全工程的定义。

有关系统安全工程的定义有不同的描述，这里给出较流行的一种。系统安全工程就是应用系统工程的原理与方法，识别、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。由于系统安全工程是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，从而为有关决策提供决策依据，并据此采取相应安全措施。

系统安全工程的逻辑结构如图 1.4 所示。

系统安全工程是系统工程学科的一个分支，它的学科基础除有系统论、控制论、信息论、运筹学、优化理论等外，还有其特有的学科基础，如预测技术、可靠性工程、人机工程、行为科学、安全心理学、职业安全卫

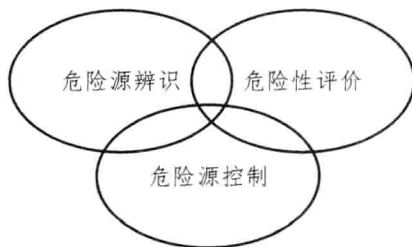


图 1.4 系统安全工程的逻辑结构

生学、安全生产法规、法律以及与其相关的各种工程学等多门学科和技术。

（2）系统安全工程的发展过程。

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，它向人们展示了破坏的恶果，教人们必须按照科学规律办事。

其次，事故是一种特殊的科学实验。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）的实验。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。

再次，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、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的这种不懈努力与坚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。

系统安全工程也正是在这种事故的反作用下应运而生的。系统安全工程产生于 20 世纪 60 年代初期美英等工业发达国家。首先使用于军事工业方面，随后在原子能工业上也相继提出了保证系统安全的问题，并于 1974 年由美国原子能委员会发表了 WASH1400 报告，即商用核电站风险评价报告。这个报告发表后，引起世界各国的普遍重视，推动了系统安全工程的进一步发展。

继美国之后其他各国在安全系统工程方面也展开了研究，并取得很大的成果。如英国在 60 年代中期开始收集有关核电站故障的数据，对系统的安全性和可靠性问题，采用了概率评价方法，进一步推动了定量评价工作，并设立了系统可靠性服务所和可靠性数据库。日本引进系统安全工程的方法虽然较晚，但发展很快，已在电子、宇航、航空、铁路、公路、原子能、汽车、化工、冶金等工业领域大力开展了研究与应用。

民品工业也存在系统安全工程的诞生与发展问题。20 世纪 60 年代正是美国市场竞争日趋激烈的年代，许多新产品在没有得到安全保障的情况下就投放市场，造成许多使用事故，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。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，这也可以称之为民品工业的系统安全工程。

在我国系统安全工程的研究、开发是从 20 世纪 70 年代末开始的。天津东方化工厂应用系统安全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、应用系统安全工程起了带头作用。其后是各类企业借鉴引用国外的系统安全分析方法，对现有系统进行分析。到 80 年代中后期，人们研究的注意力逐渐转移到系统安全评价的理论和方法，开发了多种系统安全评价方法，特别是企业安全评价方法，重点解决了对企业危险程度的评价和企业安全管理水平的评价。

这期间，许多专家学者的相关专著也相继问世了，以系统的观点、方法，系统地总结了国内外安全系统的理论与方法，这些论著的共同观点是：

① 安全系统工程是在事故逼迫下产生的。安全系统工程也好，系统安全工程也好，都是

在人类从事社会经济活动中由于发生事故的规模如此巨大,事故损失如此惨重,以致人们再也承受不起这么严重的灾难,不得不在现有安全技术基础上,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。即,预先的系统安全分析、系统安全评价技术和对系统整个生命周期实施全过程安全控制的系统安全管理工程。

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,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年代的产生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 美国导弹技术的开发促使安全系统工程的诞生,但它不是安全系统工程产生的唯一发源地。美国导弹技术的开发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”。同时也必须看到,在同一时期,还有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FTA、ETA、FMEA等,这些行业的安全系统工程都是在20世纪60年代短短几年时间产生的,因此,我们把所有这些成功的理论通过科学的总结形成一个完整的学科——安全系统工程,应当说是顺理成章的。

④ 安全系统工程不仅包括分析与评价技术,也应包括管理程序、管理方法等管理科学的内容,它也是以系统工程为基础的安全工程。

各类有关安全系统工程的论著,其内容都是以系统工程为基本原理,包括系统安全分析、系统安全评价和系统安全管理三部分内容。通过分析和评价认识风险,通过工程技术管理控制风险,使系统安全性达到预定的目标。

基于这种思想,迄今国外发表的系统安全分析、系统安全评价、系统安全管理技术与方法属于安全系统工程范畴;国内已经实践证明对预先控制事故、提高系统安全性确有实效的,具有系统工程鲜明特点的安全分析、安全评价和安全管理技术与方法也应当属于安全系统工程范畴。

2. 安全系统工程与系统安全工程的区别

(1) 安全系统工程。

安全系统工程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。其研究内容主要有危险的识别、分析与事故预测;消除、控制导致事故的危險;分析构成安全系统各单元间的关系和相互影响,协调各单元之间的关系,取得系统安全的最佳设计等。目的是使生产条件安全化,使事故减少到可接受的水平。

安全系统工程的发展过程大致经历了四个阶段:

① 军事装备零部件的可靠性和安全性问题研究。始自20世纪50年代末期美国的军事工业,后来发展到其他工业生产部门,使可靠性管理与质量管理相对分工。

② 工业安全管理开始引起系统工程方法。如60年代初应用事故树分析法(FTA)和故障类型影响分析法(FMEA)等。

③ 从60年代中期开始,引用了系统工程计划的方法,对系统开发的各阶段,如计划编制、开发研究、制造标准、操作程序等进行安全评价。