普通高等教育“十一五”国家级规划教材

系统安全工程

邵　辉　主编

石油工业出版社
Petroleum Industry Press

普通高等教育“十一五”国家级规划教材

系统安全工程

邵　辉　主编

石油工业出版社

内 容 提 要

本书是教育部普通高等教育“十一五”国家级规划教材。教材以系统安全的思想统领全书，将系统论、风险管理理论、可靠性理论与安全技术相结合，突出了危险源辨识、危险性评价和危险源控制。全书共十三章，包括绪论、系统安全分析基础、安全检查表、预先危险性分析、故障类型及影响分析、事故树分析、事件树分析、危险与可操作性分析、危险度分析评价法、道化学公司火灾爆炸危险指数评价法、蒙德火灾爆炸毒性指数评价法、重大事故后果分析、安全决策方法简介。

本书可供高等院校安全工程及相关专业本科生、研究生使用，也可供从事安全工程的科研、设计、评价及工程技术与管理人员参考。

图书在版编目（CIP）数据

系统安全工程/邵辉主编．
北京：石油工业出版社，2008.5
普通高等教育“十一五”国家级规划教材
ISBN 978-7-5021-6502-4

Ⅰ．系…
Ⅱ．邵…
Ⅲ．安全工程—高等学校—教材
Ⅳ．X93

中国版本图书馆 CIP 数据核字（2008）第 029139 号

出版发行：石油工业出版社
（北京安定门外安华里 2 区 1 号　100011）
网　址：www.petropub.com.cn
编辑部：（010）64523612　发行部：（010）64523620
经　销：全国新华书店
印　刷：石油工业出版社印刷厂

2008 年 5 月第 1 版　2008 年 5 月第 1 次印刷
787×1092 毫米　开本：1/16　印张：17.5
字数：443 千字

定价：25.00 元
（如出现印装质量问题，我社发行部负责调换）

前　言

系统安全工程是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—机器（设备）—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、判断建立某种安全模型，运用系统论、风险管理理论、可靠性理论和工程技术手段辨识系统的危险源，评价系统的危险性，并采取控制措施使其危险性最小，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。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，随着我国走向世界的步伐加快，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技术与管理水平的提高。

“系统安全工程”课程在安全工程专业培养方案中处于重要位置，是安全工程专业的专业基础课，对安全工程专业人才培养起着承前启后的作用。

多年来，编者在“系统安全工程”课程的教学过程中进行了大量的探索性研究工作，取得了一定成果，并提出了“系统安全工程”课程教学的指导思想：

（1）培养学生系统安全的思想；

（2）培养学生掌握辨识危险的程序；

（3）培养学生掌握风险分析、评价的方法；

（4）培养学生控制危险的综合能力。

在编写过程中，编者力求将基本理论、基本分析方法与安全生产中的具体安全问题相结合，既注重提高安全技术与管理理论水平，又注重解决实际问题。在对理论和分析方法的阐述中强调了实用性和可操作性；在风格上力求简明性和趣味性；在表述上力求深入浅出，语言简练明了，案例生动有趣。

本书由邵辉教授总体策划，提出总体编写思路、制定总体框架，确定编写原则和各章内容。最后由邵辉教授担任主编、王凯全教授和蒋军成教授担任副主编，对全书进行了统调和统审。

全书编写分工如下：江苏工业学院邵辉编写第1、第2、第6、第10章，王凯全编写第5章，邢志祥编写第12章，赵庆贤编写第3、第8章，葛秀坤编写第4章；南京工业大学蒋军成编写第11章；江苏大学吕保和编写第7、第9章；大庆石油学院李伟编写第13章。

在本书编写过程中，编者参阅和利用了大量文献资料，在此对原著作者表示感谢。另外，要特别感谢江苏工业学院对《系统安全工程》教材编写给予的大力支持和关注。由于编者水平有限，书中存在一些不当之处，敬请专家、读者批评指正。

编　者

2008年2月

目　　录

1 绪　论

1.1 系统安全

1.1.1 系统安全的概念

系统安全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。系统安全理论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）。“系统安全”是相对“系统危险”而言的。系统安全与系统危险的关系参见图 1-1。

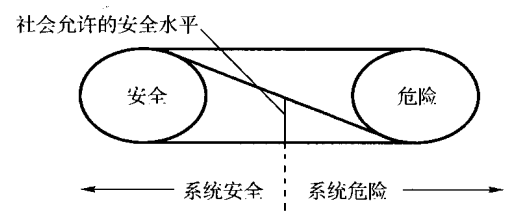

图 1-1　系统安全与系统危险的关系

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整个系统生命周期，直到系统报废为止。

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的元素组成，元素之间以非常复杂的关系相连接。由于系统在研究制造或使用过程中往往涉及高能量，系统中微小差错就会导致灾难性的事故，因此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。安全组也要像应力组、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 年代至 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将气体加压到 420kg/cm^2、温度低达－196℃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，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具有腐蚀性。当时负责该项目的美国空军的官员们并没有认识到他们建造的导弹系统潜伏着巨大的危险性。在洲际导弹试验开始的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。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。

1.1.2 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，任何事物中都潜伏着危险因素，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，某种危险源造成人员伤害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等，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。在生产过程中要注意减少系统总的危险性，而不是只去消除几种特定的危险。

④由于人的认识能力有限和事物不断发展的客观性，有时不能完全认识系统中的危险源和危险，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、环境、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，只能通过相关的方法、措施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。

1.1.3 系统安全中人的失误

作为系统安全应用对象的导弹系统、武器系统主要是一些由机械、电子零部件组成的硬件系统。当把系统安全推广到核电站、化工生产等包括人在内的系统时，又会遇到了人的因素问题。人在这些系统中可以作为一种系统元素考虑，在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。

20世纪70年代末的美国三里岛核电站事故曾引起一阵恐慌，约20万人撤离；1984年印度的博帕尔农药厂的毒气泄漏事故和1986年苏联的切尔诺贝利核电站事故，数十万人失

去生命。国内的如2003年重庆开县川东北气矿“12·23”井喷事故，243人因硫化氢中毒死亡，65000人被紧急疏散。2005年3月29日晚，京沪高速公路淮安段上行线103km+300m处，一辆载有约35t液氯的山东槽罐车鲁H00099与山东货车鲁QA0398相撞，导致槽罐车液氯大面积泄漏；由于肇事的槽罐车驾驶员逃逸，货车驾驶员死亡，延误了最佳抢险救援时机，造成了公路旁3个乡镇村民重大伤亡等。这些巨大的复杂系统的意外事故都曾给人类带来过惨重的灾难。对这些事故的调查表明，人失误，特别是管理失误是造成事故的罪魁祸首。因而，当今世界范围内系统安全理论研究的一个重大课题，就是关于人失误的研究。

1.2 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，是安全工程专业同学必须具备的最基本素质。系统安全的思想反映在三个方面。

1.2.1 安全是相对的思想

首先要理解什么是安全。

美国安全工程师学会（ASSE）编写的《安全专业术语辞典》以及《英汉安全专业术语辞典》中，将安全定义为：安全意味着可以容忍的风险程度。

长期以来，人们一直把安全和危险看作截然不同的、相对立的。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。

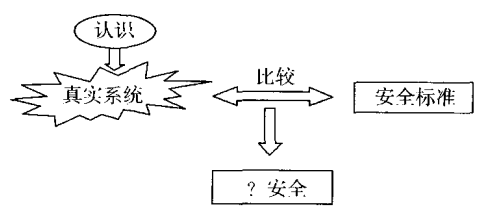

图1-2 安全的认识过程

安全是通过对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映，这一过程可用图1-2加以说明。

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：认识的客观、真实性；安全标准的科学、合理性。安全伴随着人们的活动过程，它是一种状态，与时间、空间相联系。

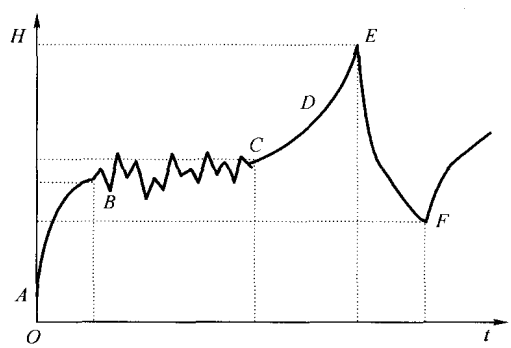

图1-3 系统生命周期中的“*R-M*”（Rheology-Mutation）曲线

1.2.2 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。系统生命周期中的安全问题可用图1-3表示。

以化工企业为例，对图1-3加以说明。*AB*阶段表示某工艺单元刚刚建立运行时，设备刚刚投入使用，处于浴盆曲线中的早期失效期，可靠性较低，极易发生故障；人员由于刚刚开始生

产，对工艺流程和设备的操作较为生疏，极易操作失误，且对设备故障的处理不够熟练；安全措施和管理不够完善，对于设备的维护和人员操作培训的管理不够。此时，系统风险呈现减速增长的趋势。由于系统的风险一直存在，因此在初始点，即 $t\rightarrow 0+$ 时，系统风险的值（H）并不为零。

BC 阶段表示工程单元进入稳定的运行阶段。设备度过早期失效期，运行较为稳定，故障的发生率降低；人员对于设备的操作开始熟练，出错较少，即使设备有意外情况发生，操作人员也可以根据经验采取及时有效的处理；安全措施逐渐到位，管理条款也愈加严密，防范措施成熟，此时系统风险以极低的速度增长。BC 阶段中的波动，描述的是危险的发生与抑制的过程，该阶段会出现一些故障或误操作，可以通过正确的方法加以消除。虽然灾场风险存在波动，但是灾害没有发生，从本质上来讲，还是比较安全的。当然，如果 BC 阶段中任意一次波动处理不当，都会导致 BC 阶段结束，提前进入 CD 阶段。因此，加强设备维护，提高员工安全操作水平，建立危机防范制度，有助于 BC 阶段的延长。

随着工作时间的推移，工艺单元中的设备出现磨损，发生事故的概率增加；人员由于长期从事相同的工作，由于对工艺过于熟悉，容易产生麻痹大意的心理，导致操作失误增加，危机处理也不能完全按照规定达到准确有效地控制灾害的发生。此时，系统风险进入 CD 阶段，呈现加速增长的趋势。

当系统在这样的危险状态下维持一段时间，潜在的能量不断集聚，最终突破系统的约束向外释放引发事故，人员和财产就会有伤亡和损失，即 DE 阶段。

此后，工艺瘫痪，设备无法运行，需经过 EF 阶段对整体的工艺加以恢复和调整。在 F 点时，新的工艺单元建立，新的系统形成 新的风险，即存在新的初始风险值，成为另一次“流变-突变”过程的起点。

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。本质化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。本质化安全是系统的理想状态，是安全工作追求的目标。

②工程化安全。工程化安全思想是对本质化安全的补充，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。

本质化安全和工程化安全构成了系统生命周期安全的思想。

1.2.3 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，这里介绍其中的一种。

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，

称为第二类危险源。它主要包括物的故障、人的失误和环境因素。

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——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——目的是得到各种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——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”对策对危险源进行综合控制。

1.3 系统与系统工程

1.3.1 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 2 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点。这里对系统的四个主要特点加以说明。

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、最优控制以及最优管理和使用等。

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，而且在研究和使用系统时，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，系统由三个部分组成，即输入、处理和输出，如图 1-4 所示。任何系统都具有输出某种产物的功能。如化工企业，它输入原材料、能源、信息，经过加工或作业（化学操作或物理操作），最后输出所需的物质流的系统，称为生产系统。再如，若以信息流为主体的系统，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。

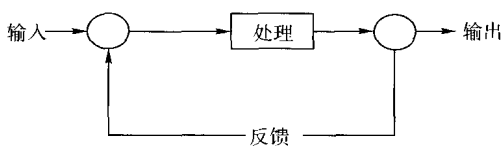

图 1-4　系统的功能结构示意图

当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。

1.3.2　系统工程

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、电气工程等，它所研究的对象主要是人力、材料、价格等。系统工程中的“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。

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，经济上最合理，运行中最可靠，时间上最节省，则须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、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。

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、长远的观点出发去考察问题，拟定目标和功能，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。

1.4 系统安全工程概述

1.4.1 系统安全工程与安全系统工程

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），它们之间是有区别的。

（1）系统安全工程

系统安全工程是运用系统论、风险管理理论、可靠性理论和工程技术手段辨识系统中的危险源，评价系统的危险性，并采取控制措施使其危险性最小，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。系统安全工程的基本内容包括：

①危险源辨识——运用系统安全分析方法发现、识别系统中危险源的工作。

②危险性评价——评价危险源导致事故、造成人员伤害或财产损失的危险程度的工作。危险源的危险性评价包括对危险源自身危险性的评价和对危险源控制措施效果的评价两个方面的问题。

③危险源控制——利用工程技术和管理手段消除、控制危险源，防止危险源导致事故、造成人员伤害和财物损失的工作。危险源控制技术包括防止事故发生的安全技术和避免或减少事故损失的安全技术。

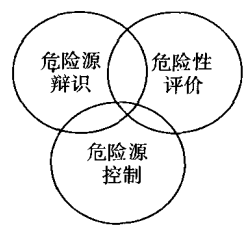

图 1-5 系统安全工程的基本内容

系统安全工程强调危险源辨识、危险性评价、危险源控制活动。它既是一个有机的整体，也是一个循序渐进发展的过程，强调通过持续的努力，实现系统安全水平的不断提升。系统安全工程的基本内容参见图 1-5。

（2）安全系统工程

所谓安全系统工程，即采用系统工程的原理和方法，识别、分析和评价系统中的危险性，为调整工艺、设备、操作、管理、生产周期和费用等因素提供依据，以使系统所存在的危险因素能得到消除或控制，使事故的发生减少到最低程度，从而达到最佳安全状态。简言之，安全系统工程就是应用系统工程的原理和方法，分析、评价及消除系统中的各种危险，实现系统安全的一整套管理程序和方法体系。安全系统工程的主要内容包括以下四个方面：

①系统安全分析——在安全系统工程中占有十分重要的地位。为了充分认识系统的危险性，就要对系统进行细致的分析。根据需要可以把分析进行到不同程度，可以是初步的或详

细的，也可以是定性的或定量的。

②系统安全预测——在系统安全分析的基础上，运用有关理论和手段对安全生产的发展或者事故的发生等作出的一种预测。

③系统安全评价——系统安全分析的目的就是为了进行安全评价。通过评价了解到系统中的潜在危险和薄弱环节，并最终确定系统的安全状况。

④安全管理措施——根据评价的结果，对照已经确定的安全目标，对系统进行调整，对薄弱环节和危险因素增加有效的安全措施，最后使系统的安全性达到安全目标所要求的水平。

长期以来，人们对于系统安全工程和安全系统工程概念以及内涵的认识和理解尚不明确、不统一。归纳起来，两者的异同见表 1-1。

表 1-1　系统安全工程和安全系统工程的异同

项　目		系统安全工程	安全系统工程
同	目标相同	实现系统整体安全性	
	主要技术方法相同	系统安全分析、系统安全评价	
异	理论基础不同	系统论、风险管理理论、可靠性理论	系统工程理论
	内涵不同	强调安全工程的逻辑性、持续性、递进性	强调安全工程的全过程、全方位、全人员性质
	侧重点不同	技术层面	管理层面

1.4.2　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：

①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，教会人们必须按照科学规律办事。

②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，改变了系统的工艺、设备，从而提高了系统的性能，发展了专业技术。

③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。通过对事故的信息，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。

系统安全工程也正是在这种事故的反作用力下应运而生的。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 WASH 1400 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20世纪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。

化工生产的危险性和化工事故的危害性是众所周知的。随着工业规模的扩大和事故破坏后果的日益严重化，迫使化工企业加倍努力，严格控制事故，特别是化工厂的火灾爆炸事故。为此，美国道化学公司于1964年发表了化工厂“火灾爆炸指数评价法”，俗称道氏法。该法经过多年的应用、修改，已不断完善。之后，英国帝国化学公司在此基础上开发了蒙德评价法，日本提出了岗三法、正田法。20世纪70年代，日本劳动省发表的评价方法，另辟蹊径，它是以分析与评价、定性评价与定量评价相结合为特点的“化工企业安全评价指南”，亦称“化工企业六阶段安全评价法”。这些就是化工系统的系统安全工程。

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。到了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。

目前，系统安全工程在全国各个行业得到广泛的应用。特别是在高危行业，国家安全生产监督管理总局颁布了一系列的法规文件，进一步规范系统安全工程的应用，取得了良好的效果，如《安全评价通则》（AQ 8001—2007）、《安全预评价导则》（AQ 8002—2007）、《安全验收评价导则》（AQ 8003—2007）、《安全现状评价导则》、《危险化学品包装物、容器定点生产企业生产条件评价导则（试行）》、《危险化学品生产企业安全评价导则（试行）》、《危险化学品经营单位安全评价导则（试行）》、《煤矿安全评价导则》、《非煤矿山安全评价导则》、《民用爆破器材安全评价导则》、《烟花爆竹生产企业安全评价导则（试行）》等。

1.4.3 系统安全工程的研究内容

系统安全工程是一种综合性的技术方法，在研究过程中不仅要应用系统论、风险管理理论、可靠性理论，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。

从目前国内外的资料分析可见，系统安全工程的研究内容主要包括事故致因理论、系统安全分析、安全评价、安全措施和安全价值分析五个方面。

（1）事故致因理论

事故的发生有其自身的发展规律和特点。了解事故的发生、发展和形成过程，对于辨识、评价和控制危险源具有重要意义。

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，事故怎样发生，以及如何采取措施予以防范，并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。事故致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，目前较为流行的事故致因理论有：事故频发倾向理论、海因里希工业安全理论、能量意外释放理论、管理失误论、扰动起源理论、事故遭遇倾向理论、现代因果连锁理论、轨迹交叉理论、两类危险源理论等。

(2) 系统安全分析

系统安全分析是实现系统安全的重要手段，是系统安全工程的核心内容，也是安全评价的基础。其目的是通过对系统进行深入、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，关系到整个安全工作的成败。

系统安全分析的方法有数十种之多，这些方法有定性的、也有定量的，有逻辑推理的、也有综合比较的。要完成一个准确的分析，就要事先了解各种分析方法的特点、适用场合，经过比较，再决定采用哪种分析方法。但不管采用哪种分析方法，都要事先建立一个系统模型。这种模型大多数采用图解方式，表示出系统各单元之间的关系。这样易于为人们掌握系统各单元之间的关系和影响，便于查到事故的真正原因和危险性大小。

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，也可以是定性的或定量的。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

安全评价是以系统安全分析为依据，只有通过分析，掌握了系统中存在的潜在危险和薄弱环节、发生事故的概率和可能的严重程度等，才能正确地进行安全评价。

安全评价分为定性评价和定量评价。定性分析的结果用于定性评价，而定量分析的结果用于定量评价。任何定量方法总是在定性的基础上开始的，但是定性评价只能够知道系统中的危险性的大致情况，如危险性因素的多少和严重程度等。要想深入了解系统的安全状态，还有待于定量评价。只有经过定量评价，才能充分发挥系统安全工程的作用；通过定量评价的结果，决策者才可以选择最佳方案，领导和监察机关才可以根据评价结果督促企业改进安全状况，保险公司就可以按企业的安全性要求，规定不同的保险金额。

安全评价是预测预防事故的高级阶段。它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。

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。安全评价是系统安全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，以一种可辨识度量的信息

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

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，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。

此外，安全措施还可分为宏观控制措施、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，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，对系统中固有的危险源和人的不安全行为进行控制。对于固有的危险源，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，主要依据行为的科学原理，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。

(5) 安全价值（安全成本）分析

当系统中的危险性被认识后，为了控制和消除这些危险因素，以提高系统的安全性时，需要采取各种安全措施，这就要有一定的资金投入。为了评价资金的合理性，必须进行安全价值分析。

安全投资不同于一般的投资，它不产生直接的投资效益，而主要是能减少未来的企业损失。为了判断安全投资的合理性，需要知道投资前后损失期望值的变化。安全投资也叫安全成本。

降低安全成本，实现最大经济利益，是企业的追求。如何处理好安全成本与企业安全度（是指没有危险、不受威胁、不出事故的程度）的关系，对企业的生存与发展非常重要。就安全成本的组成来说，增加直接安全成本，企业的安全度将提高。反过来，企业安全度提高，间接安全成本将降低。它们的关系可用图 1-6 表示。

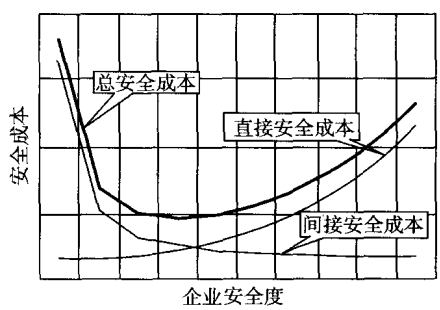

图 1-6 安全成本与企业安全度的关系

图中将安全成本这一经济问题与安全保障这一技术问题辩证地有机联系起来，为安全工作的优化提供了清晰的思路。由图可见：

①当直接安全成本投入较少时，间接安全成本将会很高。这说明在安全上少投入，表面