“十二五”江苏省高等学校重点教材

系统安全工程

（第二版）

邵　辉 ◎ 主编

石油工业出版社
Petroleum Industry Press

“十二五”江苏省高等学校重点教材

系统安全工程

（第二版）

邵　辉　主编

石油工业出版社

内 容 提 要

本书以培养学生解决复杂工程安全问题能力为目标，用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12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、危险与可操作性分析、危险度分析评价法、蒙德火灾爆炸毒性指数评价法、系统安全预测、系统安全综合评价、安全决策方法简介。

本书可供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．—2版．
北京：石油工业出版社，2016.4.
“十二五”江苏省高等学校重点教材
ISBN 978-7-5183-1171-2

Ⅰ．系…
Ⅱ．邵…
Ⅲ．系统工程—安全工程—高等学校—教材
Ⅳ．X913.4

中国版本图书馆CIP数据核字（2016）第048925号

出版发行：石油工业出版社
（北京朝阳区安华里2区1号　100011）
网　址：www.petropub.com
编辑部：（010）64256990　图书营销中心：（010）64523633
经　销：全国新华书店
排　版：北京苏冀博达科技有限公司
印　刷：北京中石油彩色印刷有限责任公司

2016年4月第2版　2016年4月第3次印刷
787毫米×1092毫米　开本：1/16　印张：16.75
字数：416千字

定价：34.00元
（如出现印装质量问题，我社图书营销中心负责调换）

第二版前言

普通高等教育“十一五”国家级规划教材《系统安全工程》自2008年出版以来，得到相关院校的大力支持与认可，2014年被评为“十二五”江苏省高等学校重点教材（编号：2014-1-061）。为了更好地发挥本教材在安全工程专业人才培养、安全生产教育培训中的积极作用，结合多年的教学实践对教材进行全面修订，形成《系统安全工程（第二版）》。

本次修订以中国工程教育认证通用标准（2015版）中的毕业要求为指导，在内容上形成相关知识要点，同时遵循“安全知识的学习与积累→系统安全思想、工程方法的训练→解决安全问题的综合能力形成”的“系统安全工程”课程教学指导思想，重点突出了解决复杂安全工程问题能力的培养。

本次修订在保持第一版的基本结构和篇幅的基础上，对相似的、陈旧的、过于理论化的内容进行了适当的合并与删除，对新标准、新技术、新方法等内容结合工程安全问题进行了补充，删除了第一版的第7章“事件树分析”，第10章“道化学公司火灾爆炸危险指数评价法”，第12章“重大事故后果分析”。增加了第10章“系统安全预测”，第11章“系统安全综合评价”。同时对第1章“绪论”，第2章“系统安全分析基础”，第6章“事故树分析”进行了较大幅度的修改。教材由原来的13章调整为现在的12章。

本书由邵辉担任主编，具体修订分工如下：第1、2、3、5、9章由邵辉负责，第4、6章由赵庆贤负责，第7、12章由黄勇负责，第8、10、11章由葛秀坤负责。王凯全、毕海普、袁雄军、时静洁等老师，束尧宸、李展、蔡志明等研究生也做了大量工作。本次教材修订得到江苏省教育厅、常州大学的大力支持和帮助，得到江苏高校品牌建设工程一期项目（苏高教〔2015〕11号，PPZY2015B154）的资助，在此一并表示感谢！

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

2015年12月

第一版前言

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

本章主要包括系统安全、系统安全的思想、系统安全工程基础、化工生产系统安全分析概述四个方面的内容，重点阐述了安全、危险源、系统安全与事故、人的失误与系统安全等概念，分析了危险源、事故隐患、意外事件、事故的逻辑关系，简介了“人—机器(设备)—环境”系统安全分析。

1.1 系 统 安 全

1.1.1 系统安全与事故

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、稳定性等同为系统的特定性能指标，同时要注意它和“安全系统”一词的不同。系统安全与系统危险的关系参见图 1.1。

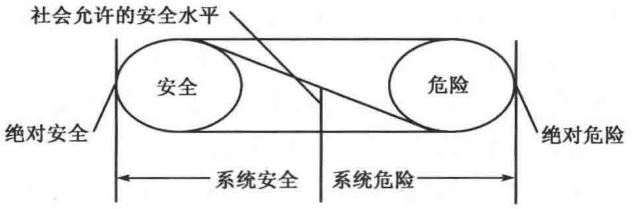

图 1.1　系统安全与系统危险的关系

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。

随着时代的发展、科学技术的进步，系统呈现出一个显著特征是设备、工艺及产品越来越复杂。如战略武器研制、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，元素之间存在着非常复杂的直接关系或间接关系。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的安全性问题受到人们广泛关注。

例如，现代石油石化工业的快速发展，石油石化生产安全问题越来越呈现出复杂性高、隐蔽性强、多米诺效应明显、风险控制参数多变等特征。同时，由于石油石化生产过程的能量密度大等特殊性，使得安全事故后果严重，发生的火灾、爆炸、中毒事故不仅造成重大的经济损失，甚至导致了大量的人员伤亡。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，甚至对人类的生存构成巨大威胁。和其他事物一样，事故也有积极的一方面。

首先，事故具有鲜明的反面教育作用，它向人们展示了事故的危害程度，警示人们必须按照科学规律办事，遵循自然规律。

其次，事故是一种特殊的科学实验。一个系统发生事故，说明该系统存在有不安全、不可靠的因素，从而以事故的形式展示了系统中实验无法获取的各种隐性的缺陷(包括各种时空状态下的不安全、不可靠的因素)。通过对事故的调查、分析，找出事故原因，研究并采取有效的事故控制措施，改变系统的工艺、设备，从而提高系统的性能，发展专业技术。

最后，事故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，一个崭新的学科诞生了，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无数惨烈事故的反作用下应运而生。

1947 年 9 月，美国航空科学院刊登了一篇题为《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。

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 420kg/cm^2、温度低达－196℃的低温液体。这种推进剂毒性远远超过第一次世界大战中使用的毒气，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着手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。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，改变了人们只注重事故单方面因素，如注重人员的不安全行为

而忽略系统硬件的故障在事故中的作用;或注重系统硬件而忽略了人员的不安全行为;或注重系统硬件、人员的不安全行为,而忽略环境条件的不良影响等。开始考虑如何通过全面改善系统"人—机器(设备)—环境"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,来自某种危险源的造成人员伤害或物质损失的可能性叫作危险。危险源是一些可能出问题的事物、人或环境因素等,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。既然没有绝对的安全,系统安全所追求的目标也就不是"事故为零"的极端理想情况,而是达到"最佳的安全程度",一种实际可能的、相对的安全目标。

(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 人失误与系统安全

人失误对于系统安全具有重要意义。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(活动)操作过程中,使系统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,甚至造成事故。

例如,国外的美国三里岛核电站事故,印度博帕尔农药厂的毒气泄漏事故和苏联切尔诺贝利核电站事故。国内的重庆开县川东北气矿"12·23"井喷事故。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. 人失误的客观存在性

人失误的产生原因非常复杂,既有人自身的因素(生理、心理因素),也有工作环境的因素,还有管理等方面的因素。在人类的活动过程中,总会产生各种各样形式的失误,这些失误由于没有造成事故,而被人们忽视。由于人失误是不可避免的,因此,在生产活动中仅凭直觉、靠侥幸是不能长期维持安全生产的。

要正确地认识人失误的客观存在性,应用系统安全的方法进行人的管理,充分考虑人的能力与水平,使人与系统能够协调一致,减少人失误的可能性,促进系统的本质安全化。

2. 人失误的类型

在不同条件下,不同的起因所引发的人失误的属性不同,一般从引起人失误的属性可分为两类:

一类是随机失误。由人的行为、动作的随机性引起的人失误,属于随机失误,与人的心理、

生理原因有关。随机失误往往是不可预测的，也是不会重复出现的。

二是系统失误。由系统设计不足或人的不正常状态引发的人失误属于系统失误。系统失误与工作条件有关，类似的条件可能引发失误再出现或重复发生。在人形成习惯后，不能适应操作程序变化或偶然情况时，系统失误会明显出现。

另外，从人失误的主观意愿上，又分为：

一是无意失误，也就是由于人自身的生理与心理因素、工作环境等方面的变化，而在无意愿的状态下发生的失误，这种失误对系统安全的影响具有隐蔽性。

二是有意失误，也就是为了个人利益，或出于兴趣、侥幸等心理，而有意为之的行为。如“三违”就是典型的有意失误。

3. 人失误的表现

人失误的表现是复杂多变的，比如遗漏或遗忘、把事弄颠倒、没按要求或规定的时间操作、无意识动作、调整错误、进行规定外的动作等。这些表现是人失误本质的外在显现，同一失误表现，对于不同的人，其本质内因是不同的。对同一本质内因，其失误的表现也会有不同。通过对这些失误表现的研究分析，找出失误与本质内因的关系，进行有针对性的教育、训练或合理安排工作，预防人失误，提高系统的安全度。

4. 引发人失误的常见因素

(1)精神不集中。无论从事何种生产或工作，精神或注意力集中是安全生产的首要前提，尤其是诸如驾驶员、塔吊司机、机床操作工、运行值班工等要害作业的工种，更需要精神的高度集中才可能在生产中做到万无一失。因此很多相关的行业都会对上述工种作出严格的要求和规定。如驾驶员在行车时不得与他人聊天、不得打手机；运行值班工不得在工作时看报纸、从事与运行无关的事等。

(2)麻痹大意。长期在一个岗位上工作，或是在比较容易掌握的熟练工种工作，会使员工熟能生巧，运作自如，这样当然对提高生产效率是有好处的，但同时也会产生负面效应，即麻痹大意。如建筑业的脚手架工，对于有些年纪较轻、身体灵活、动作敏捷的员工，在做过几个工程的脚手架装拆之后，便以为自己完全可以放心大胆的作业了，有时图一时省事，应该绑扎安全带而不进行绑扎，也可能多次不绑扎安全带不会出事故，便以为凭自己的技术完全可以放心大胆的工作，便把安全规定置之一旁，这样有可能在某次工作中由于主观或客观的原因，造成高处坠落的事故。

(3)好奇乱动，违反劳动纪律。员工由于性格、心理状态的影响，会在生产过程中产生各种好奇，在没有操作技能的状态下，或不遵守劳动纪律就乱动、乱操作而造成失误事故。

(4)不佩戴或不正确佩戴劳动防护用品。有的员工在作业时嫌佩戴劳动防护用品不方便，例如夏天戴安全帽、穿防砸皮鞋会感觉很热而摘掉安全帽、穿起不到防砸作用的鞋；车工在操作时嫌戴眼镜麻烦而摘掉眼镜；在噪声很大的房间戴耳塞会使耳朵感觉不舒适而摘掉耳塞等，以上行为都会造成失误伤害。

(5)使用不安全的工具。工具的安全性对操作者的健康安全有着直接的影响，有的操作者或图省事，或不了解工具的使用规范，由于工具的不安全造成人身事故。如在潮湿的环境下进行电钻作业，应使用国家规定的三类电动工具，如果使用一类或二类电动工具，就有可能造成触电事故。又如有的操作者为了省事，将木制锤把换成钢管的，由于钢管壁很滑，在操作时容易造成锤子脱手而出现事故。

(6)不按规定的速度进行作业。为了生产的安全,企业对厂内机动车的行车速度、机械设备的运行速度、流水线上的传动速度等作出了明确要求。但在生产中,往往会出现超速作业、超速行车、超速传递的现象,由于违反了正常的作业规律,发生事故的机率大大提高。

(7)拆除安全装置。为了保证作业人员的安全,在机械设备的轴、轮、齿上会有安全防护装置,但有的操作者为了维护或取物方便等原因,将安全防护装置部分拆除或整体拆除,由此造成的操作者或其他相关方的绞伤、挤伤、拉伤甚至死亡事故已屡见不鲜。

(8)在不安全处逗留。有的作业场所是严禁无关人员进入和停留的,如电力高压区、起重机下、强辐射区等,一旦进入,危及生命。

(9)不合理的配置、装载、混装等。如将不同化学性质、可能造成燃烧或爆炸的物品放置在一起;在运输机械上装货超出载重量;将不同型号、不是同一配置的零件强行结合等。

(10)在狭窄或狭小的场所进行作业。有的作业需要一定的空间和距离,如修理汽车底盘,应在地沟内作业;建筑业绑扎钢筋应在较宽阔的地面上进行。有的作业人员不顾作业条件的安全性,给事故的发生提供了机会。

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:

1.2.1 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。

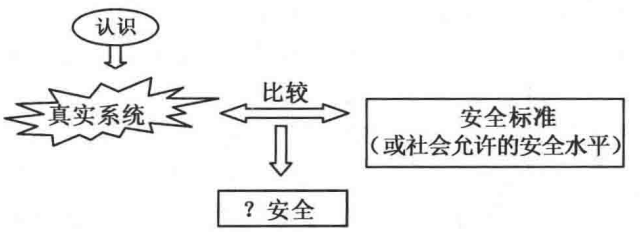

图 1.2 安全的认识过程

由图 1.2 可知,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。所以安全伴随着人们的活动过程,它是一种与时间、空间相关联的系统状态。如人们过马路斑马线的过程,就是一个对安全认识、判断、选择与实施的活动过程,对

于同一个人来说，每次过马路斑马线的过程都是不同的。另外，同一马路斑马线、同一时间，对于不同的人，其过马路斑马线的过程也是不同的。

1.2.2 安全伴随着系统生命周期的思想

系统从诞生到报废要经历一个时间序列，在这一时间序列的发展过程，系统由构思开始，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），如图 1.3 所示。

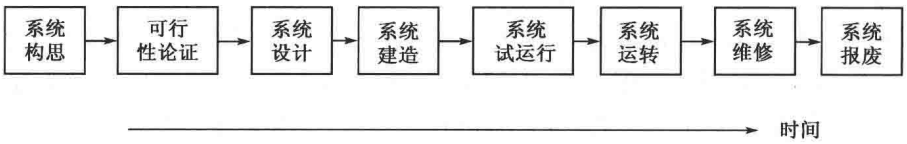

图 1.3　系统的生命周期

系统在生命周期的各个环节都存在不同的安全问题，其系统的安全问题随时间呈现“浴盆”式的变化规律，如图 1.4 所示。

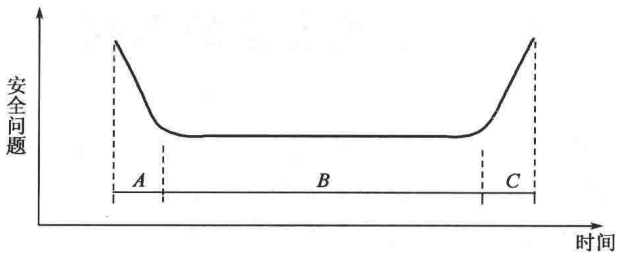

图 1.4　系统生命周期中安全问题随时间发展的浴盆曲线

由图 1.4 可见，在系统发展的时间序列中，系统安全问题呈现三个显著的阶段 A、B、C。A 为系统的青少年期，包括系统的构思、可行性论证、设计、建造、试运转等时期，在该时期，系统的安全问题较多，随着系统的成长安全问题逐步下降，系统趋于成熟。B 为系统的青壮年期，系统的各个方面均处在良好的状态，因此系统运行稳定、可靠，故障率较低。C 为系统的衰老期，系统的运行机能衰退，安全问题显著增加。

由此可见，在安全管理工作中，必须正确认识系统的生命周期，把握系统所处的生命周期阶段，根据安全问题在系统生命周期中的变化规律，采取有针对性的安全对策与措施。

系统生命周期中的安全问题可用图 1.5 进行表述。下面以化工生产为例对图 1.5 加以说明。AB 阶段表示某工艺单元刚刚建立运行时，设备开始投入使用，处于浴盆曲线中的青少年期，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 $t \to 0+$ 时，系统风险的值并不为零。

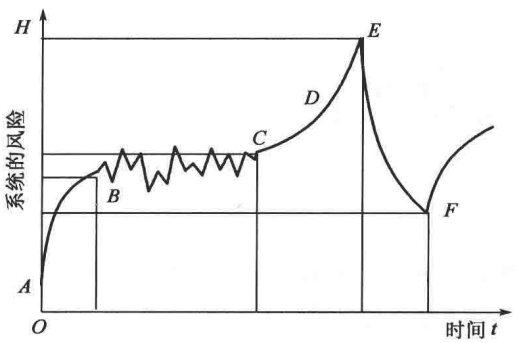

图 1.5　系统生命周期中的系统风险随时间变化曲线

BC 阶段表示工程单元进入稳定的运行阶段。

设备度过青少年期，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。虽然系统风险存在波动，但是事故没有发生，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，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的控制水平。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，也就是系统在停电或失去公用工程时，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

1. 危险源的定义

危险源是可能导致死亡、伤害、职业病、财产损失、工作环境破坏或这些情况组合的根源或状态。

在 GB/T 28001—2011《职业健康安全管理体系　要求》中，将危险源定义为：可能导致人身伤害和(或)健康损害的根源、状态或行为，或其组合。危险源由三个要素构成：潜在危险性、存在条件和触发因素。

具体来说，危险源是指系统中具有潜在能量和物质释放危险的、可造成人员伤害、在一定的触发因素作用下可转化为事故的部位、区域、场所、空间、岗位、设备及其位置。它的实质是具有潜在危险的源点或部位，是爆发事故的源头，是能量、危险物质集中的核心，是能量从那里传出来或爆发的地方。危险源存在于确定的系统中，不同的系统范围，危险源的区域也不同。例如，从全国范围来说，对于危险行业(如石油、化工等)具体的一个企业(如炼油厂)就是一个

危险源。而从一个企业系统来说，可能某个车间、仓库就是危险源，一个车间系统可能某台设备是危险源。因此，分析危险源应按系统的不同层次来进行。

因此，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。

2. 危险源的分类

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。

在具体的安全管理工作中，应根据企业的实际情况，灵活地应用危险源分类，提高安全管理的效能。例如在 GB 6441—1986《企业职工伤亡事故分类》中将人的不安全行为归纳为 13 大类，参见表 1.1。将物的不安全状态和环境的不良归纳为 4 大类，参见表 1.2。

表 1.1　人的不安全行为分类

序号	不安全行为	序号	不安全行为
1	操作失误、忽视安全、忽视警告	4	用手代替手动操作
1.1	未经许可开动、关停、移动机器	4.1	用手代替手动工具
1.2	开动、关停机器未给信号	4.2	用手清除切屑
1.3	开关未锁紧、造成意外转动、通电	4.3	不用夹紧固件，手拿工件进行加工
1.4	忘记关闭设备	5	物件存放不规范
1.5	忽视警告标志、警告信号	6	进入危险场所
1.6	操作按钮、阀门、扳手等错误	6.1	进入吊装危险区
1.7	供料或送料速度过快	6.2	易燃易爆场所明火
1.8	机器超速运转	6.3	冒险信号
1.9	酒后作业	7	攀、坐不安全位置
1.10	冲压机作业，手伸进冲压模	8	在起吊物下作业或停留
1.11	工件固定不牢	9	机器运转加油、检修、焊接、清扫等
1.12	用压缩空气吹扫铁屑	10	有分散注意力行为
2	造成安全装置失效	11	忽视使用防护用品
2.1	拆除安全装置	12	防护用品不规范
2.2	调整错误造成安全装置失灵	12.1	旋转设备附近穿肥大衣服
3	使用不安全设备	12.2	操作旋转零部件戴手套
3.1	临时不固定设备	13	其他类型的不安全行为
3.2	无安全装置设备		

表 1.2　物的不安全状态和环境的不良分类

序号	不安全状态分类	序号	不安全状态分类
1	防护、保险、信号等装置缺陷	2.8	起吊绳索不符要求
1.1	无防护罩	2.9	设备带病运行
1.2	无安全保险装置	2.10	设备超负荷运转
1.3	无报警装置	2.11	设备失修
1.4	无安全标志	2.12	地面不平
1.5	无护栏或护栏损坏	2.13	设备保养不良、设备失灵
1.6	电气未接地	3	个人防护用品等缺少或缺陷
1.7	绝缘不良	3.1	无个人防护用品、用具
1.8	危房内作业	3.2	防护用品不符安全要求
1.9	防护罩未在适当位置	4	生产场地环境不良
1.10	防护装置调整不当	4.1	照明不足
1.11	电气装置带电部位裸露	4.2	烟尘弥漫视线不清
2	设备、设施、工具、附件有缺陷	4.3	光线过强、过弱
2.1	设计不当、结构不合安全要求	4.4	通风不良
2.2	制动装置缺陷	4.5	作业场地狭窄
2.3	安全距离不够	4.6	作业场地杂乱
2.4	拦网有缺陷	4.7	地面滑
2.5	工件有锋利倒棱	4.8	操作工序设计和配置不合理
2.6	绝缘强度不够	4.9	环境潮湿
2.7	机械强度不够	4.10	高温、低温

3. 危险源的控制原则

如何解决危险源问题？应从三个方面思考：

(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。

4. 危险源、事故隐患、意外事件、事故的逻辑关系

危险源、事故隐患、意外事件、事故是安全管理中非常重要的几个概念。前面已经对危险源的概念进行介绍，下面主要介绍事故隐患、意外事件、事故。

事故隐患。所谓隐患(Hidden Peril)是指隐藏的祸患，事故隐患即隐藏的、可能导致事故的祸患。这是一个在长期工作实践中大家形成的共识用语，一般是指那些有明显缺陷、毛病的事物，相当于人的不安全行为、物的不安全状态或不良的环境因素等。

意外事件。本书所表达的意外事件是指生产活动偏离了原来设计的路径(或状态)，但没有形成伤害(或损失)后果的状态。