



高职高专煤矿开采技术专业及专业群教材

# 安全系统工程

ANQUAN XITONG GONGCHENG

主 编 黄文祥 陈 晨  
副主编 曾 来 张艳艳



重庆大学出版社

## 内容提要

本书共6个教学情境,主要包括安全系统工程概述、事故致因理论、系统安全定性分析法、安全系统分析可定量分析法、系统安全评价及危险控制与安全决策等。本书可作为安全相关专业教材,也可作为相关专业科研和技术人员参考用书。

### 图书在版编目(CIP)数据

安全系统工程 / 黄文祥主编. -- 重庆:重庆大学出版社, 2019.5  
高职高专煤矿开采技术专业及专业群教材  
ISBN 978-7-5689-1170-2

I. ①安… II. ①黄… III. ①安全系统工程—高等职业教育—教材 IV. ①X913.4

中国版本图书馆 CIP 数据核字(2018)第 140828 号

## 安全系统工程

主 编 黄文祥 陈 晨

副主编 曾 来 张艳艳

策划编辑:周 立

责任编辑:李定群 版式设计:周 立

责任校对:谢 芳 责任印制:张 策

\*

重庆大学出版社出版发行

出版人:易树平

社址:重庆市沙坪坝区大学城西路 21 号

邮编:401331

电话:(023) 88617190 88617185(中小学)

传真:(023) 88617186 88617166

网址:<http://www.cqup.com.cn>

邮箱:fxk@cqup.com.cn(营销中心)

全国新华书店经销

重庆华林天美印务有限公司印刷

\*

开本:787mm×1092mm 1/16 印张:9 字数:209千

2019年5月第1版 2019年5月第1次印刷

ISBN 978-7-5689-1170-2 定价:38.00元

本书如有印刷、装订等质量问题,本社负责调换

版权所有,请勿擅自翻印和用本书  
制作各类出版物及配套用书,违者必究

# 前言

安全系统工程是高职院校安全相关专业必须掌握的一门核心课程。本书由重庆工程职业技术学院和重庆安全职业技术学院教师参与编写。参与人员包括具有安全生产现场经验的人员,也有长期从事安全系统工程教学的教师。本书共6个教学情境,主要介绍系统安全分析、系统安全评价和系统风险控制等内容。

本书在大量总结现有教材资料的基础上,结合相关企业单位对本知识的应用情况进行编写,编排结构与以往教材有显著区别。在进行理论讲解的同时,强调知识技能的应用,属于理论与实践相结合的教材类型。其中,主要围绕“任务目标—任务描述—知识准备—任务实施”的主线编排内容,特别是任务实施,强调知识的应用,每个任务都有知识的应用,更加符合高职高专的教育规律以及强调实践性和技术性的特征要求。本书可作为高职高专院校安全类专业课教材,也可作为安全各类培训教材。

本书由黄文祥、陈晨任主编,曾来、张艳艳任副主编。具体分工如下:重庆工程职业技术学院黄文祥负责教学情境2、教学情境4的任务4.1、教学情境3的任务3.5和任务3.6以及教学情境5的编写,重庆安全职业技术学院张艳艳负责教学情境1的编写,重庆工程职业技术学院曾来负责教学情境3的任务3.1至任务3.4、教学情境4的任务4.2的编写,重庆安全职业技术学院陈晨负责教学情境6的编写。

本书编写过程中参阅了大量资料,在此对原作者表示诚挚的谢意。

由于编者水平有限,书中难免有疏漏,敬请批评指正。

编者  
2019年1月

# 目 录

|               |                           |     |
|---------------|---------------------------|-----|
| <b>教学情境 1</b> | <b>安全系统工程概述</b> .....     | 1   |
| 任务 1.1        | 基本概念 .....                | 1   |
| 任务 1.2        | 安全系统工程的研究对象和研究内容 .....    | 7   |
| 任务 1.3        | 安全系统工程的产生与发展 .....        | 9   |
| 任务 1.4        | 安全系统工程的应用特点 .....         | 12  |
| <b>教学情境 2</b> | <b>事故致因理论</b> .....       | 14  |
| 任务 2.1        | 事故致因理论的发展 .....           | 14  |
| 任务 2.2        | 几种代表性的事故致因理论 .....        | 17  |
| <b>教学情境 3</b> | <b>系统安全定性分析法</b> .....    | 30  |
| 任务 3.1        | 安全检查表分析 .....             | 30  |
| 任务 3.2        | 预先危险性分析 .....             | 37  |
| 任务 3.3        | 故障类型及影响分析 .....           | 43  |
| 任务 3.4        | 危险和可操作性研究分析 .....         | 48  |
| 任务 3.5        | 作业条件危险性评价法 .....          | 51  |
| 任务 3.6        | 因果分析法(鱼刺图) .....          | 53  |
| <b>教学情境 4</b> | <b>安全系统分析可定量分析法</b> ..... | 57  |
| 任务 4.1        | 事件树分析法 .....              | 57  |
| 任务 4.2        | 事故树分析 .....               | 62  |
| <b>教学情境 5</b> | <b>系统安全评价</b> .....       | 88  |
| 任务 5.1        | 安全评价概述 .....              | 88  |
| 任务 5.2        | 危险、有害因素识别及评价单元划分 .....    | 95  |
| 任务 5.3        | 安全评价方法 .....              | 106 |
| 任务 5.4        | 安全对策措施及评价结论 .....         | 110 |

|        |                 |     |
|--------|-----------------|-----|
| 教学情境 6 | 危险控制与安全决策 ..... | 116 |
| 任务 6.1 | 危险控制的基本原则 ..... | 116 |
| 任务 6.2 | 固有危险控制 .....    | 119 |
| 任务 6.3 | 人为失误控制 .....    | 122 |
| 任务 6.4 | 安全决策 .....      | 126 |
| 参考文献   | .....           | 135 |

# 教学情境 **I**

## 安全系统工程概述

---

### 【情境描述】

安全系统工程概论是学习安全系统工程的基础。本情境主要介绍安全系统工程基本概念,安全系统工程的研究对象和研究内容,安全系统工程产生和发展过程以及安全系统工程应用特点。其目的是对学生起到引导作用,使学生初步具备安全系统工程基础知识。

### 任务 1.1 基本概念

#### 【任务目标】

1. 了解系统、系统工程概念的内涵。
2. 掌握安全系统、安全系统工程概念的内涵。

#### 【任务描述】

安全系统工程概念的产生是在系统、系统工程、安全系统等概念陆续出现后逐渐形成的。要了解安全系统工程内涵,必须先了解系统、系统工程及安全系统等基本概念。这些概念是学好安全系统工程的基础知识。

#### 【知识准备】

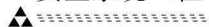
#### 1.1.1 系统、系统工程

安全系统工程是以安全学和系统科学为理论基础,以安全工程、系统工程、可靠性工程等  
为手段,对系统风险进行分析、评价和控制,以期实现系统及其全过程安全目标的科学技术。

安全系统工程是现代科技发展的必然产物,是安全科学学科的重要分支。

安全系统工程是一门涉及自然科学和社会科学的横断科学。在定义安全系统工程之前,需要弄清相关学科的有关概念。

系统工程的研究对象是系统。系统就是由相互作用和相互依赖的若干组成部分结合成的具有特定功能的有机整体。系统有自然系统与人造系统、封闭系统与开放系统、静态系统



与动态系统、实体系统与概念系统、宏观系统与微观系统、软件系统与硬件系统之分。不管系统如何划分,凡是能称其为系统的,都具有以下特性:

### (1) 整体性

系统是由两个或两个以上相互区别的要素(元件或子系统)组成的整体。构成系统的各要素虽然具有不同的性能,但它们通过综合、统一(而不是简单拼凑)形成的整体就具备了新的特定功能。就是说,系统作为一个整体才能发挥其应有功能。因此,系统的观点是一种整体的观点,一种综合的思想方法。

### (2) 相关性

构成系统的各要素之间、要素与子系统之间、系统与环境之间都存在着相互联系、相互依赖和相互作用的特殊关系。通过这些关系,使系统有机地联系在一起,发挥其特定功能。

### (3) 目的性

任何系统都是为完成某种任务或实现某种目的而发挥其特定功能的。要达到系统的既定目的,就必须赋予系统规定的功能,这就需要在系统的整个生命周期,即系统的规划、设计、试验、制造和使用等阶段,对系统采取最优规划、最优设计、最优控制、最优管理等优化措施。

### (4) 有序性

系统有序性主要表现在系统空间结构的层次性和系统发展的时间顺序性。系统可分成若干子系统和更小的子系统,而该系统又是其所属系统的子系统。这种系统的分割形式表现为系统空间结构的层次性。另外,系统的生命过程也是有序的。它总是要经历孕育、诞生、发展、成熟、衰老及消亡的过程。这一过程表现为系统发展的有序性。系统的分析、评价和管理都应考虑系统的有序性。

### (5) 环境适应性

系统是由许多特定部分组成的有机集合体,而这个集合体以外的部分就是系统的环境。系统从环境中获取必要的物质、能量和信息,经过系统的加工、处理和转化,产生新的物质、能量和信息,然后再提供给环境。另一方面,环境也会对系统产生干扰或限制,即约束条件。环境特性的变化往往能够引起系统特性的变化,系统要实现预定的目标或功能,必须能够适应外部环境的变化。研究系统时,必须重视环境对系统的影响。

系统工程是组织管理系统的规划、设计、制造、试验及使用的科学方法,是一种对所有系统都具有普遍意义的科学方法。这个定义表示:

- ① 系统工程属工程技术范畴,主要是组织管理各类工程的方法论,即组织管理工程。
- ② 系统工程是解决系统整体及其全过程优化问题的工程技术。
- ③ 系统工程对所有系统都具有普遍适用性。

系统工程是 20 世纪 50 年代发展起来的一门新兴学科。它是以系统为研究对象,以现代科学技术为研究手段,以系统最佳化为研究目标的科学技术。它是发展很快、应用很广的一门管理学科。它的广泛应用为管理学的发展,为各行各业、各个领域管理现代化提供了基本理论和方法。

关于系统工程所属各子学科的命名问题,钱学森指出,正如工程技术各有专业一样,系统工程也还是一个总类名称,因体系性质不同,还可以再分为门类,如工程体系的系统工程叫工程系统工程,生产企业或企业体系的系统工程叫经济系统工程。这种命名原则为系统工程在各专业领域的发展提供了条件,从而免去一些关于名词术语叫法的不必要之争。

### 1.1.2 安全系统与安全系统工程

安全一词是人们经过抽象思维确定的一个概念或理念。目前所见到的文献对安全这个概念的诠释普遍存在两个问题:一是缺乏科学的严密性;二是安全一词太大众化了,以致不管人们如何下定义,都很难包容一般意义上安全理念的内涵。

安全描述的是一种客观存在的状态吗?回答并非是肯定的。因为对安全状态描述的主要特征量是什么,在安全科学界尚难统一。有人说无事故、无隐患的状态就是安全状态;从动力学原理出发,也有人提出用系统从无序到有序,渐变与突变的统一,非畸变来描述安全动态。这样的表述虽是有一定的科学性,但因安全因素的高度复杂性和极强的时间依赖性,故上述方法所表述的安全状态必然有很大的局限性,可能与实际相差甚远,也可能带有很大的理想化色彩。但又与人们想象中的“平安无事”可能根本不是一回事。因为人们有时说的安全、平安不过是代表一种期盼,故是一种理想化的抽象的概念。如果承认安全一词描述的是一种状态,但这种状态也绝非是一种事故为零的所谓“绝对安全”的概念。从科学的角度讲,“绝对安全”的状态在客观上是不存在的。平安也好,安全也好,其本身就带有很大的模糊性、不确定性和相对性,故“安全状态”具有动态特征,就是说安全所描述的状态具有动态特征,它是随时间而变化的。

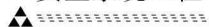
安全的动态特征还体现在它不只是一个相对稳定的状态特征,还可作为对事故—安全过程的一种表征。过程表征和状态表征最本质的区别就在于前者描述的是事物的发展趋势,后者描述的是一种目标。从这个角度讲,安全一词表述的又可认为是动态过程。正如有的文章所表述的:渐变对应于灾害过程的孕育、维持,突变对应于灾害过程的启动和剧烈地扩展。但灾变不仅是灾害发生,也是系统由不稳定向新的稳定(安全)跃迁的触发器。

当然从技术的角度讲,已经提出并应用的安全失效率、安全度、安全系数等量化的计算方法、标准及其表征的安全技术状态和安全与否的结论是科学和严密的。但这与通常讲的安全的概念相比显然要狭隘得多。

状态、过程、理念、技术安全都是定义安全这个概念应该考虑的内涵。可见,人们试图通过一个简单的定义就想把安全如此丰富复杂的内涵表述清楚是一件非常困难的事情。

从科学原理出发,定义事物多采用两种办法:一种是从事物的组成考虑;另一种是从事物的功能考虑,或两者兼顾。

安全表述的是一个复杂物质系统的动态过程或状态,过程或状态的目标是人物将不会受到伤害或损失。安全也可表述的是人们的一种理念,即人物将不会受到伤害和损失的理想状态。安全也可表述的是一种特定的技术状态,即满足一定安全技术指标要求的物态。



在讨论对安全一词的理解和认识之后,再来讨论一下安全的属性问题。安全一词所涉及的纷繁复杂因素与它的自然属性和社会属性有着密切的关系。

所谓安全的自然属性,可从两个方面来讨论:一是安全是人的生理与心理需要,或者说由生命及生的欲望决定了的自我保护意识,这是天生的,是安全存在的主动因素。二是人类对天灾的无奈以及新陈代谢生老病死的规律不可抗拒,使人们不得不把生命安全经常提到议事日程,这虽然是被动因素,但它与前一个主动因素相结合,就决定安全是自古以来人类生活、生存、进步的永恒的主题。

安全的社会属性也可从以下两个方面来阐述:

①自从人类有组织活动以来,社会安定、有序、进步始终是各社会阶段追求的目标,而这一目标实现的重要标志之一就是安全。这是社会促动安全的主动因素。但是,人类的社会活动,如政治、军事、文化、社交,有的对安全直接起破坏作用,有的间接影响着安全;人类的经济活动,如生产(职业)、高技术灾害(化学品致灾、核事故隐患、电磁环境公害、航天事故、航空事故)、交通灾害,则是自人类开展经济活动以来就存在的突出的安全问题,如今更加突出的一个安全问题是环境问题。环境恶化(包括自然环境和人为环境)是人类生活、生存安全的重要威胁。因此,在第15届世界职业安全卫生大会上与会专家指出,向21世纪人们提出的挑战性问题是“环境、安全、健康问题”,即 Q. E. & OSH 是一个严重影响国民经济可持续发展的大问题。人类的社会活动、经济活动、交通和环境一方面本身在不断制造事故,另一方面也通过技术和管理措施不断消除隐患,减少事故。但受政治利益和经济利益的驱使,安全技术管理措施多数是被动的。

②关于安全的社会属性,也有人提出人伦智的观点。人伦是在一个人群(社会性的结合)中发生的。夫妇、父子、兄弟、朋友、同事构成人际关系,人们以诚相待,共谋生命的延续、生活的充实,并以此抵制唯利是图就称为人伦智。在资本主义社会,各个人际关系上的人伦智相当低微、暗弱。然而,人伦智却是“职业灾害困局”中唯一的脱困希望之所寄,它的潜在能量是可以信赖的。人伦智也应属安全社会属性中的主动因素。

如果把安全的自然属性和社会属性合起来考虑,安全代表的是什么?它可能既是理念的,又是物质的;既是抽象的概念,又是客观的、有形的;既是当前的实实在在的事物,又可能是将来的一个可望而不可即的目标。

还可看出,安全的自然属性与社会属性中都存在着很强的促动安全的主动因素,这是安全科学发展的基础。

安全问题纷繁复杂的关系正是因安全问题的自然属性与社会属性的交融,正像人是一样,而社会的复杂性正是安全问题复杂的根本原因之一。

### 1.1.3 安全系统及其特点

安全问题是一个复杂的系统工程问题。或者说,解决安全问题要用系统工程的理论和方法。这种认识目前已经具有广泛的共识。但是,说到“安全系统”则存在着歧义。其实“安全系统”这个定义能否成立,关键还在于它的特殊性和客观性。所谓特殊性,是指它与一般系统的区别。如前所述,其客观性的问题是不容置疑的,而其特殊性或个性可归纳为以下方面:

### (1) 系统性

与安全有关的影响因素构成了安全系统。因为与安全有关的因素纷繁交错,所以安全系统是一个复杂的巨系统。很难找到一个因素及其相关性如此复杂的能与之相比的系统。由于安全系统中各因素之间,以及因素与目标之间的关系多数有一定灰度,因此,安全系统是灰色系统。

与一般系统不同,安全系统总是把环境因素看成其系统的组分。其典型的因素及其关系如图 1.1 所示。

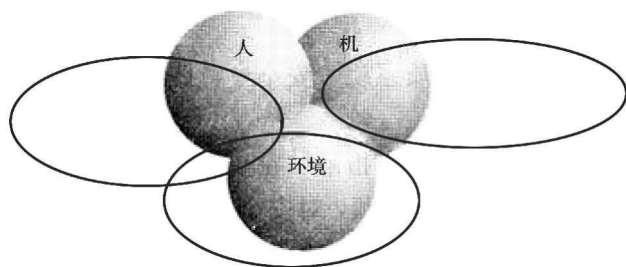


图 1.1 安全系统典型的组成因素及其关系图

依据安全问题所涉及范围大小不同,安全系统大小之差可能很悬殊。一般来说,纯属技术领域的安全系统如一台设备、器具,可能只涉及机和物;对一个车间甚至一个工厂,考虑安全问题的系统范围,则不只是机和物,肯定要把“人—机—环境”都扯进来。实际上,“人—机—环境”的提法是考虑了安全问题的空间跨度和时间跨度两个方面。如此说来,即便是一台设备,如果把它的制造安全与使用安全考虑进来,也仍然是“人—机—环境”的复杂系统。

安全系统的目标不是寻求最优解。这是因为安全系统目标的多元化,以及安全目标的极强相对性、时间依赖性与其理想化理念很难协调,所以安全系统的目标解是具有一定灰度的满意解或可接受解。

### (2) 开放性

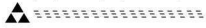
安全系统是客观存在的。这是因为安全系统是建立在安全功能构件的物质基础之上。但同时安全系统总是寄生在客体(另一个系统)中。在处理方法上,如果把客体看成一个黑匣子,安全系统是通过客体的能量流、物流和信息流的流入-流出的非线性变化趋势,确认安全和事故发生的可能性,因此,安全系统具有开放性特点。

开放性不仅是安全系统在动态中保持稳定存在的前提,也是安全系统复杂性及安全一事转换发生的重要机制。

### (3) 确定性与非确定性

“确定性”是指制约系统演化的规则是确定性的,不含任何随机性因素。确定性的特征是演化方向及演化结果是确定的,可精确预测。“非确定性”或者具有演化方向和演化结果不确定,或者具有刻画事物运动特征的特征量不能客观精确地确定的特征。非确定性包括随机性和模糊性。

“随机性”可能有两个方面的来源:一是在不含任何外在的随机影响因素作用下,完全由



“确定性”系统演化而产生的随机性(如产生混沌),这种随机性称为本质随机性;二是系统还可能因其外在影响因素的随机作用而产生随机性行为,从而使系统在一定条件下表现出随机性的特征(外在随机性)。由于安全系统把环境看成它的组分,因此,对安全系统而言,本质随机性和外在随机性的区别不是绝对的。

“模糊性”是指事物的本身不清楚或衡量事物的尺度不清楚。对于安全系统而言,就是指系统的构成及其相互关系,以及组成与目标的关系不清楚。造成这些不清楚的可能来源在于主观和客观两个方面,即具有主观模糊性和客观模糊性。首先,刻画安全运行轨迹的以模糊数学方法建立的数学模型具有主观模糊性。因为数学模型常常不可能“严格地”确定安全系统各要素之间及其与目标之间完整的客观关系。当然,对于自然的技术因素之间的关系尚好一些。而对于社会的因素及其与技术因素的耦合关系将难于量化,因而也将难于建立准确的数学关系。应该强调的是,出现上述问题不完全是因安全系统本身不清楚,它可能只是人们对安全系统主观模糊性的表现。

另外,对安全系统安全度的评价尺度以及构成安全度等级的评价指标体系也具有客观模糊性,即从事物的本质上无法给出其客观衡量尺度。

#### (4) 安全系统是有序与无序的统一体

序主要反映事物的组成的规律和时域。依据序的性质,可分为有序、混沌序和无序。有序通常同稳定性、规则性相关联,主要表现为空间有序、时间有序和结构有序。无序通常与不稳定、无规则相关联。而混沌序则是不具备严格周期和对称性的有序态。现代复杂系统演化理论认为,复杂系统的演化中,不同性质的序之间可以相互转化。安全系统序的转化结果是否引发灾害或使灾害扩大,取决于序结构的类型及系统对特定序结构下的运动的(灾害意义上的)承受能力。

有序和无序,确定性和非确定性都会在系统演化过程中通过其空间结构、时间结构、功能结构和信息结构的改变体现出来。

#### (5) 突变性或畸变性

安全系统过程的突变或畸变,或过程由连续到非连续变化在本质上还是服从于量变引起质变的哲理。量变到质变的转化形式可用畸变、突变或飞跃来描述,但也可通过渐变实现。因此,安全系统的渐变也可能孕育着事故,而突变、畸变则肯定对应于灾害事故的启动,是致灾物质,或能量的突然释放。

综上所述,安全系统虽然与一般系统、非线性系统等有若干共同点,但安全系统的个性还是非常明显的,这是决定它客观存在并区别于其他系统的根本原因。

### 1.1.4 安全系统工程

安全系统工程是采用系统工程的基本原理和方法,预先识别、分析系统存在的危险因素,评价并控制系统风险,使系统安全性达到预期目标的工程技术。

对这个定义,可从以下4个方面理解:

①安全系统工程的理论基础是安全科学和系统科学。它是工矿企业劳动安全卫生领域

的系统工程。

②安全系统工程追求的是整个系统的安全和系统全过程的安全。

③安全系统工程的重点是系统危险因素的识别、分析,系统风险评价和系统安全决策与事故控制。

④安全系统工程要达到的预期安全目标将是系统风险控制在人们能够容忍的限度以内,也就是在现有经济技术条件下,最经济、最有效地控制事故,使系统风险在安全指标以下。

### 【任务实施】

#### (1) 任务准备

课件,多媒体教学设备。

#### (2) 任务应用

**应用 1.1** 因本任务主要是要求学生掌握相关概念的内涵,故采取课堂讨论的方式,对学生分组。要求选定一组学生,对相关概念以自己理解的方式,口头表达出来,其他组的学生针对其表达的概念进行补充完善。

## 任务 1.2 安全系统工程的研究对象和研究内容

### 【任务目标】

1. 了解安全系统工程的研究对象。
2. 熟悉安全系统工程的研究内容。

### 【任务描述】

学好安全系统工程,必须首先熟悉安全系统工程研究对象和内容。本任务主要从这两个方面做详细介绍,介绍安全系统工程主要的研究内容人子系统、机器子系统、环境子系统,并把安全工程研究内容归纳为系统安全分析、系统安全评价、系统安全决策与事故控制。

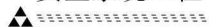
### 【知识准备】

#### 1.2.1 安全系统工程的研究对象

安全系统工程作为一门科学技术,有它本身的研究对象。任何一个生产系统都包括3个部分,即从事生产活动的操作人员和管理人员,生产必需的机器设备、厂房等物质条件,以及生产活动所处的环境。这3个部分构成一个“人—机—环境”系统,每一部分就是该系统的一个子系统,称为人子系统、机器子系统和环境子系统。

##### (1) 人子系统

该子系统的安全与否涉及人的生理和心理因素,以及规章制度、规程标准、管理手段、方法等是否适合人的特性,是否易于为人们所接受的问题。研究人子系统时,不仅把人当成“生物人”“经纪人”,更要看成“社会人”,必须从社会学、人类学、心理学、行为科学角度分析问题、解决问题;不仅把人子系统看成系统固定不变的组成部分,更要看到人是一种自尊自爱、



有感情、有思想、有主观能动性的人。

### (2) 机器子系统

对该子系统,不仅要考虑工件的形状、大小、材料、强度、工艺、设备的可靠性等方面考虑其安全性,而且要考虑仪表、操作部件对人提出的要求,以及从人体测量学、生理学、心理与生理过程有关参数对仪表和操作部件的设计提出要求。

### (3) 环境子系统

对该子系统,主要应考虑环境的理化因素和社会因素。理化因素主要有噪声、振动、粉尘、有毒气体、射线、光、温度、湿度、压力、热及化学有害物质等;社会因素有管理制度、工时定额、班组结构及人际关系等。

3个子系统相互影响、相互作用的结果就使系统总体安全性处于某种状态。例如,理化因素影响机器的寿命、精度甚至损坏机器;机器产生的噪声、振动、温度、尘毒又影响人和环境;人的心理状态、生理状况往往是引起误操作的主观因素;环境的社会因素又会影响人的心理状态,给安全带来潜在危险。这就是说,这3个相互联系、相互制约、相互影响的子系统构成了一个“人—机—环境”系统的有机整体。分析、评价、控制“人—机—环境”系统的安全性,只有从3个子系统内部及3个子系统之间的这些关系出发,才能真正解决系统的安全问题。安全系统工程的研究对象就是这种“人—机—环境”系统(以下简称“系统”)。

## 1.2.2 安全系统工程的研究内容

安全系统工程是专门研究如何用系统工程的原理和方法确保实现系统安全功能的科学技术。其主要技术手段有系统安全分析、系统安全评价和安全决策与事故控制。

### (1) 系统安全分析

要提高系统的安全性,使其不发生或少发生事故,其前提条件就是预先发现系统可能存在的危险因素,全面掌握其基本特点,明确其对系统安全性影响的程度。只有这样,才有可能抓住系统可能存在的主要危险,采取有效安全防护措施,改善系统安全状况。这里所强调的“预先”是指:无论系统生命过程处于哪个阶段,都要在该阶段开始之前进行系统的安全分析,发现并掌握系统的危险因素。这就是系统安全分析要解决的问题。

系统安全分析是使用系统工程的原理和方法,辨别、分析系统存在的危险因素,并根据实际需要对其进行定性、定量描述的技术方法。根据有关文献介绍,系统安全分析有多种形式和方法,使用中应注意:

①根据系统的特点、分析的要求和目的,采取不同的分析方法。因为每种方法都有其自身的特点和局限性,并非处处通用。使用中,有时要综合应用多种方法,以取长补短或相互比较,验证分析结果的正确性。

②使用现有分析方法不能死搬硬套,必要时要根据实用、好用的需要对其进行改造或简化。

③不能局限于分析方法的应用,而应从系统原理出发,开发新方法,开辟新途径,还要在以往行之有效的一般分析方法基础上总结提高,形成系统性的安全分析方法。

## (2) 系统安全评价

系统安全评价往往要以系统安全分析为基础,通过分析,了解和掌握系统存在的危险因素,但不一定要对所有危险因素采取措施。而是通过评价掌握系统的事故风险大小,以此与预定的系统安全指标相比较,如果超出指标,则应对系统的主要危险因素采取控制措施,使其降至该标准以下。这就是系统安全评价的任务。

评价方法也有多种,评价方法的选择应考虑评价对象的特点、规模,评价的要求和目的,采用不同的方法。同时,在使用过程中,也应与系统安全分析的使用要求一样,坚持实用和创新的原则。过去 20 年,我国在许多领域都进行了系统安全评价的实际应用和理论研究,开发了许多实用性很强的评价方法,特别是企业安全评价技术和重大危险源的评估、控制技术。

## (3) 安全决策与事故控制

任何一项系统安全分析技术或系统安全评价技术,如果没有一种强有力的管理手段和方法,也不会发挥其应有的作用。因此,在出现系统安全分析和系统安全评价技术的同时,也出现了系统安全决策。其最大的特点是从系统的完整性、相关性、有序性出发,对系统实施全面、全过程的安全管理,实现对系统的安全目标控制。最典型的例子是美国军用标准《系统安全程序》,美国道化学公司的安全评价程序,国际劳工组织、国际标准化组织倡导的《职业安全卫生管理体系》。系统安全管理是应用系统安全分析和系统安全评价技术,以及安全工程技术为手段,控制系统安全性,使系统达到预定安全目标的一整套管理方法、管理手段和管理模式。

### 【任务实施】

#### (1) 任务准备

课件,多媒体教学设备。

#### (2) 任务应用

**应用 1.2** 因本任务主要是理论介绍,故采用课堂讨论的方式对本任务的知识进行应用。首先对学生进行分组,要求每组学生谈谈对安全系统工程研究方法和内容的看法。最后教师进行总结。

## 任务 1.3 安全系统工程的产生与发展

### 【任务目标】

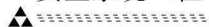
1. 了解安全系统工程产生和发展的过程。
2. 了解发展安全系统工程的重要性。

### 【任务描述】

要学好安全系统工程,必须熟悉安全系统工程的发展历史和发展必然。通过对其发展历史过程的学习,可使学生明确安全系统工程的重要性,提高学生学习的积极性。

### 【知识准备】

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,它与其他事物一样,也有积极的一方面。例如,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。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。最后,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。

安全系统工程也正是在这种事故的反作用下应运而生的。安全系统工程产生于20世纪60年代初期美英等工业发达国家。这一时期,由于美国在导弹系统研发过程中仅仅1年半的时间就连续发生4起重大事故,造成惨重损失,因此,迫使美国空军以系统工程的基本原理和管理方法来研究导弹系统的安全性、可靠性,并于1962年提出了“弹道导弹系统安全工程”,制订了“武器系统安全标准”;1963年提出了“系统安全程序”;到1967年7月由美国国防部确认,将该标准提格为美国军用标准;之后又经两次修订,成为现在的MIL-STD-882B“系统安全程序要求”。它以标准的形式规范了美国军事系统的工程项目在招标以及研发过程中对安全性的要求和管理程序、管理方法、管理目标。这就是由事故引发的军事系统的安全系统工程。

原子弹是可怕的,从而在人们的心里存在着对以放射性物质为动力的核电站的恐惧心理。因此,在社会压力下各国的政府对核电站的要求极其严格,同时在核安全方面的研究投入了巨大的人力、物力。英国在这方面的研究开始比较早,到20世纪60年代中期就已建成了系统可靠性服务所和可靠性数据库,成功开发了概率风险评价(PRA)技术,从而以概率来计算核电站系统风险大小以及是否可以接受。到1974年美国原子能委员会发表了拉斯姆逊教授的“商用核电站风险评价报告”(WASH-1400),从而成功地开发应用了系统安全分析和系统安全评价技术。该报告的科学性和对事故预测的准确性得到了“三哩岛事件”(核电站堆芯熔化造成放射性物质泄漏事故)的证实。这就是核工业的安全系统工程。

化工企业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。该法经过多年的实用,修改了6次,出了第七版,并出版了教科书。该法是以根据化学物质的理化特性确定的物质系数为基础,综合考虑一般工艺过程和特殊工艺过程的危险特性,计算系统火灾爆炸指数,评价系统损失大小,并据此考虑安全措施,修正系统风险指数。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。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”,也称“化工企业六步骤安全评价法”。该评价法是一种对化工系统的全过程如何进行评价的管理规范。它不仅规定了评价方法、评价技术,也规定了系统生命周

期每个阶段用哪种评价方法,如何进行评价等。这就是化工系统的安全系统工程。

民品工业也存在安全系统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、汽车及冶金等行业开发了许多系统安全分析方法和评价方法,这也可称为民品工业的安全系统工程。

在我国,安全系统工程的研究、开发是从20世纪70年代末开始的。天津东方化工厂应用安全系统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、应用安全系统工程起了带头作用。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如下:

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因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。

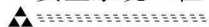
②现代科学技术的发展为安全系统工程的产生提供了必要条件。20世纪40年代产生了系统可靠性工程,50年代出现了系统工程,以及这一期间现代数学和计算机技术的迅速发展,使安全系统工程在20世纪60年代产生成为科学技术发展的必然产物,也是相关学科相互影响的必然结果。

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策源地。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,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3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。

### 【任务实施】

#### (1) 任务准备

课件,多媒体教学设备。

#### (2) 任务应用

**应用 1.3** 因本任务主要是理论介绍,故采用课堂讨论的方式对本任务的知识进行应用。首先对学生进行分组,要求每组学生对安全系统工程发展重要性进行阐述,并结合目前安全系统工程发展情况,对安全系统工程未来发展进行展望。

## 任务 1.4 安全系统工程的应用特点

### 【任务目标】

熟悉安全系统工程的应用特点。

### 【任务描述】

学习安全工程学的最终目标是应用。安全系统工程的应用与其他学科应用有不同之处。本任务主要介绍安全系统工程的应用特点,为以后安全系统工程理论联系实际奠定基础。

### 【知识准备】

安全系统工程是一门应用性很强的科学技术学科。几十年来,许多经典的应用范例始终激励人们进行不懈的探索,不断充实和发展其自身的理论体系,以期实现更好的应用效果,这是安全系统工程始终保持快速发展的重要原因。为了进一步促进学科发展,提高其实用性,有必要进一步明确安全系统工程的应用特点:

#### (1) 系统性

无论是系统安全分析、系统安全评价的理论,还是系统安全管理模式和方法的应用都表现了系统性的特点。它从系统的整体出发,综合考虑系统的相关性、环境适应性等特性,始终追求系统总体目标的满意解或可接受解。

#### (2) 预测性

安全工程学的分析技术与评价技术的应用,无论是定性的,还是定量的,都是为了预测系统存在的危险因素和风险水平。它是通过这些预测来掌握系统安全状况如何,风险能否接受,以便决定是否应当采取措施,控制系统风险。因此,安全系统工程也称系统的事故预测技术。

#### (3) 层序性

安全系统工程的应用是按照系统的时空两个跨度有序展开,管理规范的执行,一般是按照系统生命过程有序进行,而且贯彻到系统的方方面面。因此,安全系统工程具有明显的“动态过程”研究特点。