

全国煤炭高职高专（成人）“十一五”规划教材

煤矿安全系统工程

景国勋 杨玉中 编著



Meikuang Anquan Xitong Gongcheng

中国矿业大学出版社

China University of Mining and Technology Press

TD7
J-366.3

山西煤炭高专(成人)“十一五”规划教材

煤矿安全系统工程

景国勋 杨玉中 编著

中国矿业大学出版社

煤炭高职高专(成人)“十一五”规划教材 建设委员会成员名单

主 任:李增全

副 主 任:刘咸卫 胡卫民 刘发威 仵自连

委 员:(按姓氏笔画为序)

王廷弼 王自学 王春阁 王宪军

牛耀宏 石 兴 刘卫国 刘景山

杜俊林 李玉文 李式范 李兴业

李学忠 李维安 张 军 张 浩

张贵金 陈润叶 周智仁 郝巨才

荆双喜 贺丰年 高丽玲 唐又驰

彭志刚

秘 书 长:王廷弼 李式范

副秘书长:耿东锋 孙建波

煤炭高职高专(成人)“十一五”规划教材 矿井通风与安全专业编审委员会成员名单

主 任: 仵自连

副主任: 王国际 张天驹 景国勋

委 员: (按姓氏笔画为序)

王永才 王永祥 王德银 仝洪昌

刘一新 刘玉洲 余明高 郑小欢

袁东升

前 言

安全系统工程是20世纪60年代迅速发展起来的一门新学科,是系统工程的一个重要分支,是工厂和企业安全生产最有成效的、科学的分析技术和管理理论。它的目的在于研究系统的危险及其原因和过程,以及对事故如何预防等问题。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、可靠性工程等的手段,对系统风险进行分析、评价、控制,以期实现系统及其全过程安全目标的科学技术,是现代科技发展的必然产物,是安全科学学科的重要分支。

我国从20世纪70年代开始研究和运用这一新的学科,80年代在有关部门和企业中广泛地推广应用安全系统工程。实践证明,在企业安全管理工作中,应用和推广安全系统工程技术,为矿山安全管理工作的开辟了一条新的途径,对提高安全管理水平、降低事故率有明显的效果,并且为企业实行安全管理科学化和现代化奠定了基础。

本书共分十章,由浅入深地介绍了安全系统工程的主要内容,主要包括事故致因理论、安全检查表分析法等系统安全分析方法、定性和定量的系统安全评价方法,以及系统危险的基本控制技术。总结了近几年国内外的研究成果和应用经验,尽力突出了矿山安全生产的特点,做到理论联系实际。

本书由河南理工大学的景国勋教授和杨玉中博士主笔并统稿,在编写过程中,得到了多方面的支持和帮助,在此一并表示衷心的感谢!

由于作者的水平所限,加之时间仓促,书中难免有不当之处,敬请批评指正!

作 者
2007年9月

目 录

第一章 概论	1
第一节 基本概念.....	1
第二节 安全系统工程的研究对象和研究内容.....	7
第三节 安全系统工程的产生与发展.....	9
第四节 安全系统工程的应用特点	11
习题与思考题	12
第二章 事故的致因理论	13
第一节 概述	13
第二节 事故致因理论的发展过程	19
第三节 事故致因理论	20
第四节 事故致因理论的应用	27
习题与思考题	28
第三章 煤矿安全检查表及其应用	29
第一节 概述	29
第二节 安全检查表的内容及分类	30
第三节 安全检查表的编制	31
第四节 安全检查表的应用与实施	33
习题与思考题	37
第四章 事件树分析法	38
第一节 事件树分析概述	38
第二节 事件树分析法	39
第三节 事件树分析的程序和事故发生的概率	41
第四节 施行事件树分析时应注意的问题	42
习题与思考题	44
第五章 事故树分析法	45
第一节 概 述	45
第二节 事故树分析程序	45

第三节 事故树的构成	46
第四节 布尔代数及化简	49
第五节 事故树的最小割集与最小径集	51
第六节 基本事件结构重要度分析	56
第七节 事故树的定量分析	57
第八节 事故树分析实例	63
习题与思考题	65
第六章 故障类型和影响分析	67
第一节 故障类型	67
第二节 分析程序	71
第三节 致命度分析	72
第四节 应用实例	73
习题与思考题	78
第七章 危险性和可操作性研究	79
第一节 基本概念和术语	79
第二节 研究步骤	80
第三节 应用实例	82
习题与思考题	84
第八章 危险预测和预先分析技术	85
第一节 危险预测技术	85
第二节 危险性预先分析	97
第三节 危险预知活动	101
第四节 生物节律理论与事故控制	105
习题与思考题	107
第九章 系统安全评价	108
第一节 概述	108
第二节 检查表式安全评价法	113
第三节 矿山工程安全评价法	114
第四节 作业条件危险性评价法	116
第五节 火灾爆炸指数评价法	118
第六节 系统安全综合评价法	127
第七节 可靠性安全评价法	128
第八节 程序框图安全评价法	133
习题与思考题	136

第十章 危险控制技术.....	137
第一节 系统危险控制的基本措施.....	137
第二节 人为失误及其控制.....	140
第三节 安全目标管理.....	146
习题与思考题.....	155
参考文献.....	156

第一章 概 论

安全系统工程是 20 世纪 60 年代迅速发展起来的一门新学科,是系统工程的一个重要分支,是工厂和企业安全生产最有成效的、科学的分析技术和管理理论。它的目的在于研究系统的危险及其原因和过程,以及对事故如何预防等问题。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、可靠性工程等的手段,对系统风险进行分析、评价、控制,以期实现系统及其全过程安全目标的科学技术,是现代科技发展的必然产物,是安全科学学科的重要分支。

第一节 基本概念

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。

一、系统

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,凡是能称为系统的,都具有如下特性:

(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。所以,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、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、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、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。一方面,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。

二、系统工程

系统工程是以系统为研究对象的。1978年我国科学家钱学森指出:系统工程是组织管理系统的规划、研究、设计、制造、试验和使用的科学方法,是一种对所有系统都具有普遍意义的科学方法。简单地说,系统工程是用现代科学方法组织管理各种系统的规划、设计、生产和使用的一门科学,是对系统所有组成部分的综合,以达到全系统的最优效率。

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。

系统工程学的主要研究内容是系统的模式化、最优化和综合评价,进而对系统进行定性和定量分析,为决策提供最优方案。

系统工程有以下三个基本特点:

(1) 研究方法的整体化。它是从整体出发,不仅把研究对象作为一个整体,而且把研究过程也视为一个整体。从整体与部分相互依赖、互相制约的密切关系中考虑问题,用具体过程和步骤把设想变为现实。

(2) 应用技术的综合化。系统工程是综合使用技术。必须注意各个阶段和每个步骤以及各个流程之间的联系,使各种技术有机地结合起来,以达到系统整体效益最优化。

(3) 寻求目标的最优化。系统工程的研究立足于现有条件,力求达到最佳效果或者达到预期的目标,而消耗资源最少,使用资金最省。

三、可靠性、可靠度、可靠性工程

可靠性是指系统在规定的条件下和规定的时间内完成规定功能的能力。这里,规定的条件都是设计规定的,规定的功能也是设计赋予的。

可靠度是衡量系统可靠性的标准,它是指系统在规定的时间内完成规定功能的概率。相反,系统在规定的条件下和规定的时间内不能完成规定功能的概率就是系统的不可靠度。

可靠性工程就是研究系统可靠性的工程技术。可靠性工程要解决的是如何提高系统可靠度,使系统在其寿命周期内正常运行,圆满完成其规定功能的问题。

就系统规定功能而言,系统整体功能除了应具备加工产品、提供服务等功能外,还必须有保障人员、设备、财产、环境不受损害的安全功能。系统可靠性与系统安全性是两个既有区别又有联系的功能,与它们相对立的是分支学科或分支系统。

四、安全系统与安全系统工程

(一) 对安全的理解和认识

“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的安全理念的内涵。

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。这样的表述虽具有一定的科学性,但由于安全因素的高度复杂性和极强的时间依赖性,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企盼,因此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,但这种状态也决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,所以“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安全描述的不只是一个相对稳定的状态特征,安全一词还可作为对事故—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、安全系数等定量化的计算方法、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。但这和通常讲的安全的概念相比显然要狭义得多。

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,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,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、物不会受到伤害或损失。安全表述的也可以是人们的一种理念,即人物不会受到伤害和损失的理想状态。安全表述的还可以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。

在讨论了对安全一词的理解和认识之后,我们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,可以从两个方面来讨论: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以从两方面来阐述:

(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。所以在 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”,且这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。但由于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,人际以诚相待,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。有观点认为,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综合起来考虑,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又不可及的目标。

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由于安全问题的自然属性与社会属性的交融,正像人是社会的一样,而社会的复杂性正是安全问题复杂的根本原因之一。

(二) 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。所谓特殊性就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以归纳为如下若干方面。

(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,很难找到一个因素数及其相关性复杂得能与之相比的系统。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,所以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是其系统的组分,其典型的因素及其关系如图 1-1 所示。

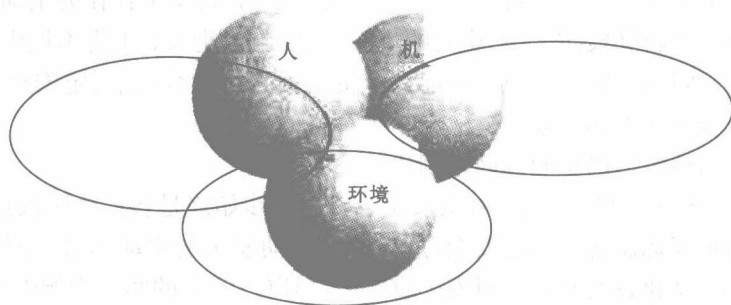


图 1-1 安全系统典型的组成因素及其关系图

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。一般地讲,纯属技术领域的安全系统,比如一台设备、器具,可能只涉及机和物;而对于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,肯定要把人一机一环境都扯进来。实际上,人一机一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,即使是一台设备,如果把它的制造安全与使用安全考虑进来,也仍然是人一机一环境的复杂系统。

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一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故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、可精确预测的。“非确定性”是指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(例如产生混沌),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是它的组分,所以对安全系统而言,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,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以量化,因而也将难以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由于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的尺度。

(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服从于量变引起质变的哲理。

量变到质变的转化形式可以用畸变、突变或飞跃来描述,但也可通过渐变实现。所以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。

(三) 安全系统的动力学特征

安全系统是物质系统。安全过程既可能是自组织的,也可能是被组织的,也可能是两者兼而有之。

所谓自组织的,是指系统在获得空间、时间或功能的结构过程中,没有外界的特定干预(所谓外界的特定干预,对安全来说主要是指社会属性中的被动因素)。它可能有两种发展形式:一种是非组织的向组织的有序发展过程,其本质是组织程度从相对较低到相对较高演化;另一种则是维持相同组织层次,但复杂性相对增长。前一种过程反映了安全系统组织层次跃升过程;后一种过程则标志着安全系统组织结构与功能从简单到复杂的组织水平的提高。

安全系统的自组织的演化过程主要是反映它的自然属性与社会属性共同作用的过程和结果。因为安全系统也是开放系统,它可以不断与外界交换物质、能量和信息,从而出现上述的两种发展形式,即从原有的混沌无序状态转变为一种在时间、空间或功能上的有序状态。

一旦安全过程出现被组织的情况,如不可预见的天灾、人为诱发地震、战争、人为纵火、瞎指挥、违规操作等等,则会发生灾难或事故。

当然安全系统也是非线性系统,因而也具有非线性系统的共同特征。非线性是系统产生自组织行为的内因,没有这个内因,所谓开放性将不起作用,无序—有序的过程也就不会发生。

不少学者为了研究安全动力学而引进熵的概念。例如:引进“负熵流”以考虑安全系统与外界的物质能量和信息交换;引进“剩余熵”作为判断体系失稳与否的依据。虽然都有一定的局限性,但熵仍然是今后研究安全过程发展趋势的重要概念与方法,因为熵的大小是状态自发实现的可能性的量度;同时从信息论的角度考虑,熵又是描写不肯定性大小的量,即熵愈大,不肯定性愈大,即:

$$H = - \sum_{i=1}^n P_i \lg P_i$$

式中 H ——熵;

P_i ——概率。

(四) 安全系统工程

安全系统工程是系统工程的一个重要分支,是安全领域的科学管理技术。它是以工程

设计、安全原理和系统工程的分析方法为基础,对系统的安全性进行定性和定量分析、评价及预测,并采取综合措施控制系统的危险性,使系统达到最优化安全状态。

安全系统工程的任务是在目标、时间及费用等制约条件下,对系统的整个生命周期内的各阶段实施综合分析,根据对可能产生危险的分析和判断,为系统设计提供必要的信息,以便消除潜在的危险或把危险控制在一定的限度之内,从而获得最佳的安全指标。

由此可以看出,安全系统工程的特点是:

- (1) 安全系统工程是系统工程在安全领域的应用。
- (2) 系统安全性分析是安全系统工程的核心。
- (3) 危险的预防和控制是安全系统工程的主要内容。
- (4) 达到最优化安全状态是安全工程学的精髓,是安全工程学的最终体现。

第二节 安全系统工程的研究对象和研究内容

一、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三个部分,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。这三个部分构成一个“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到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,不仅把人当作“生物人”、“经纪人”,更要看作“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;不仅把人子系统看作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:对于该子系统,不仅要从工件的形状、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:对于该子系统,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、化学有害物质等;社会因素有管理制度、工时定额、班组结构、人际关系等。

三个子系统相互影响、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;环境中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,这三个相互联系、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,只有从三个子系统内部及三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”)。

二、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。

(一) 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生搬硬套,必要时要根据实用、好用的原则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。

(二) 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,在使用过程中也应和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。

(三) 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。最典型的例子是美军标准《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。

三、安全系统工程的方法论

安全系统工程的方法是依据安全学理论,在总结过去经验型安全方法的基础上日渐丰富和成熟的。概括起来可以归纳为如下五个方面:

(一) 从系统整体出发的研究方法

安全系统工程的研究方法必须从系统的整体性观点出发,从系统的整体考虑解决安全问题的方法、过程和要达到的目标。例如,对每个子系统安全性的要求,要与实现整个系统

的安全功能和其他功能的要求相符合。在系统研究过程中,子系统和系统之间的矛盾以及子系统与子系统之间的矛盾,都要采用系统优化方法寻求各方面均可接受的满意解;同时要把安全系统工程的优化思路贯穿到系统的规划、设计、研制和使用等各个阶段中。

(二) 本质安全方法

这是安全技术追求的目标,也是安全系统工程方法中的核心。由于安全系统把安全问题中的人—机(物)—环境作为一个“系统”来考虑,因此,不管是从研究内容来考虑,还是从系统目标来考虑,核心问题就是本质安全化,就是研究实现系统本质安全的方法和途径。

(三) 人—机匹配法

在影响系统安全的各种因素中,至关重要的是人—机匹配。在产业部门研究与安全有关的人机匹配称为安全人机工程,在人类生存领域研究与安全有关的人机匹配称为生态环境和人文环境问题。显然,从安全的目标出发,考虑人—机匹配,以及采用人—机匹配的理论和方法是安全系统工程方法的重要支撑点。

(四) 安全经济方法

由于安全的相对性原理,所以,安全的投入与安全(目标)在一定经济、技术水平条件下有对应关系。也就是说,安全系统的“优化”同样受制于经济。但是,由于安全经济的特殊性(安全性投入与生产性投入的渗透性、安全投入的超前性与安全效益的滞后性、安全效益评价指标的多目标性、安全经济投入与效用的有效性等)就要求安全系统工程方法,在考虑系统目标时,要有超前的意识和方法,要有指标(目标)的多元化的表示方法和测算方法。

(五) 系统安全管理方法

安全系统工程从学科的角度讲是技术与管理相交叉的横断学科;从系统科学原理的角度讲它是解决安全问题的一种科学方法。所以,安全系统工程是理论与实践紧密结合的专业技术基础,系统安全管理方法则贯穿到安全的规划、设计、检查与控制的全过程。所以,系统安全管理方法是安全系统工程方法的重要组成部分。

第三节 安全系统工程的产生与发展

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作用,它向人们展示了破坏的恶果,教育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。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。

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