

安全系统工程

ANQUAN XITONG GONGCHENG

主编 谭钦文 徐中慧 刘建平 何友芳



重庆大学出版社

<http://www.cqup.com.cn>

A 安全系统工程

ANQUAN XITONG GONGCHENG

主编 谭钦文 徐中慧 刘建平 何友芳

重庆大学出版社

内 容 提 要

本书系统地阐述了安全系统工程的基本思想、方法和技术,并以典型应用为实例进行了分析。全书在介绍安全系统工程的基本概念、事故发生的原理、危险源辨识方法、系统安全分析技术、危险性评价及控制的基础上,增选了系统工程方法论、系统调查分析方法论和系统可靠性分析等系统思维和方法论基础。全书强调系统思维逻辑和实现方法的具体操作,基本概念和原理叙述深入浅出,重点突出;示例联系工程实际,并对求解逻辑和步骤进行了必要的讨论。

本书可作为安全工程及相关专业本科生的专业基础课教材,也可供安全工程专业研究生和工程技术人员参考。

图书在版编目(CIP)数据

安全系统工程/谭钦文等主编. —重庆:重庆大学出版社, 2014.11(2016.7 重印)

ISBN 978-7-5624-8605-3

I. ①安… II. ①谭…②徐…③刘…④何… III. ①安全系统工程 IV. ①X913.4

中国版本图书馆 CIP 数据核字(2014)第 223205 号

安全系统工程

主 编 谭钦文 徐中慧 刘建平 何友芳

责任编辑:陈 力 版式设计:陈 力

责任校对:关德强 责任印制:邱 瑶

*

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

POD:重庆书源排校有限公司

*

开本:787×1092 1/16 印张:18 字数:449千

2014 年 11 月第 1 版 2016 年 7 月第 6 次印刷

ISBN 978-7-5624-8605-3 定价:36.00 元

本书如有印刷、装订等质量问题,本社负责调换

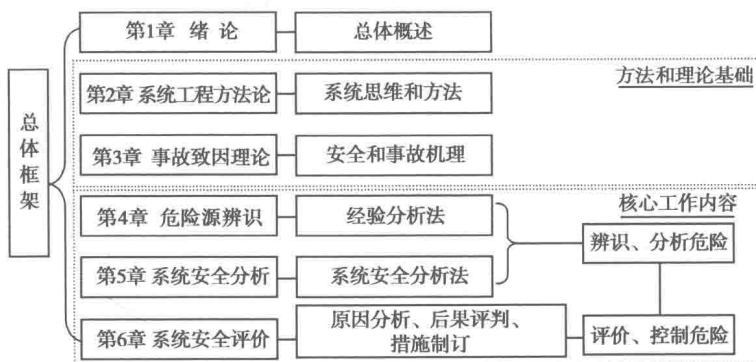
版权所有,请勿擅自翻印和用本书

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。其研究内容主要有辨识危险;预测后果;消除、控制导致事故的危险;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。其目的是运用“系统工程原理和方法”,依托“安全基本理论”,实现系统中的“危险性辨识、分析、评价和控制”。

要完成上述工作,首先必须掌握基本的系统工程思想和方法(第2章)和基本事故致因理论(第3章);其次,利用适当的系统调查分析方法,熟悉研究对象(第2章),并在此基础上根据事故致因机理,运用系统安全分析方法,完成对象系统的危险源辨识与分析(第4章、第5章);最后,利用系统安全分析和评价技术对事故后果作出预测和评价,并利用系统危险控制技术制订相应措施,实现系统的优化控制(第6章)。本教材共分为6章,其章节逻辑结构如下图所示。



安全系统工程总体框架图

本教材力求语言简洁、层次清晰、通俗易懂,从解决问题“思维模式”“理论需求”到“实践技能”逐层展开,注重理论联系实际,强调实用性和可操作。其中第一部分进行系统思想和系统方法介绍,注重系统思维方法和系统观念的建立;第二部分以安全工作核心内容为主线,展开系统安全分析、预测、评价和控制技术方面的基础理论方法及其典型工程应用实例实现过程与使用技巧介绍。强调实践技能培养,改变传统的“概念、原理、方法到简单案例套入应用”的编写思路和组织体系,变被动式“学知识”以备使用为“遇问题,变思路、求方案”,以期解决“理论与实践脱节”的问题。本书可作为大专院校安全工程及相关专业学生的选用教材,也可作为企业安全管理与技术人员,以及生产作业人员的培训教材,还可作为从事安全工程专业的科研人员,职业安全监督、监察与管理人员的参考书。

本书由西南科技大学谭钦文、徐中慧、刘建平和何友芳任主编,李仕雄,王永强,谭汝媚,魏勇,刘年平,吴爱军,林龙沅,江丽,许秦坤,周煜琴,罗尧东,李雪,李春林和王海龙等参加编写。在成书和出版过程中得到了西南科技大学教材建设及精品课程建设项目和重庆大学出版社等的大力支持;西南科技大学研究生谢羽佳、耿龙、徐午言、苗东涛、陈玄超、辛保泉、许晴、贾梁等参与了大量的内容整理和编排工作;本书部分章节还参阅了许多著作和文献,在此一并表示感谢。

安全系统工程是一门尚在不断发展的交叉学科,涉及的知识面非常广泛。由于作者水平所限,书中难免存在疏漏之处,敬请广大读者和专家批评指正。

编 者

2014年8月

目 录

第1章 绪 论	1
1.1 安全系统工程	1
1.2 安全系统工程的研究对象、内容与方法	11
1.3 安全系统工程的产生与发展	19
思考题	23
第2章 系统工程方法论	24
2.1 系统学原理	24
2.2 系统工程原理及基本观点	27
2.3 系统工程方法论	30
2.4 系统调查分析方法论	58
思考题	69
第3章 事故致因理论	70
3.1 能量逸散失控理论	70
3.2 轨迹交叉理论	75
思考题	77
第4章 危险源辨识	78
4.1 基本概念和危险源分类	78
4.2 危险源辨识工作程序和内容	85
4.3 危险源辨识方法	87
4.4 危险源分级	91
4.5 重大危险源辨识	93
思考题	96
第5章 系统安全分析	98
5.1 系统安全分析概述	98
5.2 安全检查表	102
5.3 预先危险性分析	110

5.4 事件树分析·····	130
5.5 事故树分析·····	137
5.6 故障类型及影响分析·····	158
5.7 危险与可操作性分析·····	177
5.8 原因—后果分析·····	186
5.9 系统可靠性分析·····	192
思考题·····	203
第6章 系统安全评价 ·····	208
6.1 安全评价概述·····	208
6.2 作业条件危险性评价法·····	221
6.3 概率评价法·····	223
6.4 指数评价法·····	228
6.5 单元危险性快速排序法·····	244
6.6 机械工厂安全性评价·····	249
6.7 综合评价法·····	250
6.8 安全评价方法应用实例·····	266
思考题·····	276
参考文献 ·····	277

第 1 章

绪 论

在系统科学中,系统工程是改造客观世界,并使改造过程合理化的一门技术。它以运筹学、控制论、信息论、系统论中的一些具有普遍意义的基本理论为指导,在自然科学、社会科学以及工程建设和管理中发挥作用。近 30 年来,许多学者和科学家一直在探索将系统工程的理论和原理,运用到安全管理方面,并逐步发展为安全系统工程,成为安全科学中的主要分支。

安全系统工程是以信息论、控制论等为理论基础,以安全工程、系统工程、可靠性工程的原理和方法为手段,以安全管理、安全技术和职业健康为载体,对研究对象中的风险进行辨识、评价、控制和消除,以期实现系统及其全过程安全的新兴科学。

1.1 安全系统工程

1.1.1 系 统

(1) 系统的概念

“系统”的概念,来源于人类社会的实践经验,并在长期的社会实践中不断发展而逐渐形成。一般系统的创始人奥地利的贝塔朗菲指出:“系统的定义可以确定为一定的相互关系中,并与环境发生关系的各组成部分的总体。”我国科学家钱学森对系统的定义为:“把极其复杂的研究对象称为系统,即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,而且这个系统本身又是它所从属的一个更大系统的组成部分。”虽然对于系统概念有很多种理解,但其基本意义大致相同,即系统是由相互作用、相互依赖的若干组成部分结合而成的具有特定功能的有机整体。

系统是一种由若干元素组成的集合体,用它来完成某种特殊功能。系统中的元素间相互联系、相互渗透、相互促进,彼此间保持着特有的关系,保证系统所要达到的最终目的。一旦相互间的特定关系遭到破坏,就会造成工作被动和不必要的损失。

客观世界都是由大大小小的系统组成的。组成系统的子系统和要素又由一定数量的元

素组成,各有其特定的功能和目标,他们之间相互关联,分工合作,以达到整体的共同目标。例如任何的生产系统都是由人、机器、原材料、方法和环境 5 个子系统组成。它们集合在一起的共同目标是多出好产品,使企业的经济效益最大化,从而推动企业向前发展。而生产系统又是人类社会经济大系统的一个组成部分,或者说是一个子系统。

任何一个团体、工厂、企业都可称为一个系统,在这个系统中,包含管理机关、运行体系;继续往下分,又出现一个系统,我们称其为子系统,它们包括班组及其成员等。

(2) 系统的分类

分类是系统研究的基本方法,其目的是为了更好地了解和理解系统的性质和特征,按照不同的分类标准可以把系统分为以下类型。

1) 按照系统的起源分类

①自然系统。由自然物组成的系统。它是由自然现象发展而来的,如银河系、太阳系、地球、山脉系统、河流系统、森林系统、矿产系统等。

②人造系统。由人类按一定的目的设计和改造而成的,并由人的智能或机械动力来完成特定目标的系统,如政府机构、民间团体、交通运输系统、电力传输系统、企业系统等。

2) 按照系统与环境的关系分类

①开放性系统。与外界环境发生联系的系统。

②封闭性系统。与外界环境隔绝或不受外界环境影响的系统。

3) 按照组成系统的要素存在的形态分类

①实体系统。组成系统的元素是实体的,物理方面的存在物的系统。

②概念系统。以概念、原理、原则、方法、制度、程序等非物理方面的存在物组成的系统。

4) 按照系统与时间的依赖关系分类

①静态系统。决定系统特性的因素不会随时间的变化而变化的系统。

②动态系统。决定系统特性的因素是随时间的变化而变化的系统。

5) 按照物质运动的发展阶段分类

①无机系统。如力学系统、物理系统、化学系统等。

②有机系统。如生物系统等。

③人类社会系统。如管理系统、经营系统、作业系统等。

6) 按照系统包含的范围分类

①大型系统。如生态平衡系统等。

②中型系统。如工程系统等。

③小型系统。如班组管理系统等。

7) 按照系统的构成分类

①简单系统。由性质相近的若干要素组成的系统,如物资系统等。

②复杂系统。由人造系统和自然系统相结合的系统,如农业系统、企业系统和武器系统以及社会经济大系统等。

8) 按照系统的功能分类

①环境系统。自然系统和人类社会共同组成大系统,以及与所要研究的系统周围具有一定关系的系统。

②军事系统。由军人组成的、旨在对国家和本国人民,负有保卫国家安全以及对世界和

平作出贡献的整个系统。

③安全系统。由人、机、料、法、环等组成的维持社会团体、机关、企业等安全运行的系统。

某些系统的形态并不是一成不变的,它是随着人们认识客观世界的深度,以及改造客观世界的需要,按照人们提出的分类标准进行划分的。在实际工作中这些系统也并非是孤立存在的,有时是相互交叉、相互依存、相互独立和相辅相成的。

(3) 系统的特征

从系统的观点来看,系统的特征主要有以下几个方面。

1) 集合性

集合性表明系统是由许多(至少两个)可以相互区别的要组成。例如,一个工业企业是一个系统,它的要素集合如图 1.1 所示。



图 1.1 工业企业的组成要素

2) 相关性

相关性是指系统内部的要素与要素之间、要素与系统之间、系统与其环境之间存在着这样那样的联系。联系又称关系,常常是错综复杂的。如果不存在相关性,众多的要素就如同一盘散沙,只是一个集合(set)而不是一个系统(system)。

3) 层次性

系统可分成若干个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结构的层次性。例如,我国的行政系统包含国家—省(自治区、直辖市)—市—县—乡镇;军队系统包含军—师—(旅)—团—营—连—排。

如图 1.2 所示为企业管理的层次,它分为战略规划层(高层)、经营管理层(中层)和作业层(基层)。大企业的中层又可分为若干层次,构成一座金字塔。

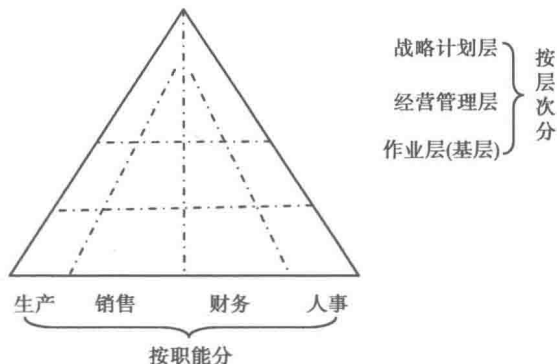


图 1.2 企业管理的层次

4) 整体性

系统是作为一个整体出现的,是作为一个整体存在于环境之中、与环境发生相互作用的,系统的任何组成要素或者局部都不能离开整体去研究。

系统的整体性又称为系统的总体性、全局性。系统的局部问题必须放在系统的全局之中才能有效地解决,系统的全局问题也必须放在系统的环境之中才能有效地解决。局部的目标和诉求,要素的质量、属性和功能指标,要素与要素之间、局部与局部之间的关系,都必须服从整体或总体的目的,它们共同实现系统整体或总体的功能。系统的功能和特性,必须从系统的整体或总体来加以理解,加以要求,使之实现并且优化。系统的整体观念或总体观念是系统概念的精髓。

5) 涌现性

系统的涌现性包括系统整体的涌现性和系统层次间的涌现性。

系统的各个部分组成一个整体之后,就会产生出整体具有而各个部分原来没有的某些东西(性质、功能、要素),系统的这种属性称为系统整体的涌现性。

系统的层次之间也具有涌现性,即当低层次上的几个部分组成上一层级时,一些新的性质、功能、要素就会涌现出来。

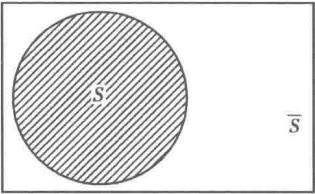
6) 目的性

系统工程所研究的对象系统都具有特定的目的。研究一个系统,首先必须明确它作为一个整体或总体所体现的目的与功能。人们正是为了实现一定的目的,才组建或改造某一个系统的。例如,学校的目的主要是培养合格的人才;企业的目的主要是生产合格的产品,提供相应的服务,并获取显著的经济效益等。

明确系统的目的性,是开展系统工程项目的首要工作。与目一词意义相近的术语有目标、指标。系统的目的常常通过更具体的目标或指标来描述。系统总是多目标或多指标的,它们也分为若干层次,构成一个指标体系。

7) 系统对于环境的适应性

任何一个系统都存在于一定的环境之中,在系统与环境之间具有物质的、能量的和信息的交换。环境的变化必定对系统及其要素产生影响,从而引起系统及其要素的变化。系统要获得生存与发展,必须适应外界环境的变化,这就是系统对于环境的适应性。



系统必须适应环境,就像要素必须适应系统一样,由图 1.3 可知:

$$\text{系统}(S) + \text{环境}(\bar{S}) = \text{更大的系统}(\Omega) \quad (1.1)$$

这就要求研究系统时必须放宽眼界,不但要看到整个系统本身,还要看到系统的环境或背景。只有在一定的背景下考察系统,才能看清系统的全貌;只有在一定的环境中研究系统,才能有效地解决系统中的问题。

总之,系统这个概念,其含义十分丰富。它与要素相对应,意味着总体与全局;它与孤立相对应,意味着各种关系与联系;它与混乱相对应,意味着秩序与规律。研究系统,意味着从事物的总体与全局上、从要素的联系与结合上去研究事物的运动与发展,找出其固有的规律,建立正常的秩序,实现整个系统的优化。

1.1.2 系统工程

系统工程是20世纪50年代发展起来的一门新兴科学,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工程学。

系统工程从系统的观点出发,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,达到合理、经济、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。这是因为系统工程采用了新的方法论,这种方法论的基础就是系统分析的观点,即一种“由上而下”“由总而细”的方法。它不着眼于个别单元的性能是否优良,而是要求巧妙地利用单元间或子系统之间的相互配合与联系,来优化整个系统的性能,以求得整体的最佳方案。

(1) 系统工程的定义

系统工程(System Engineering)是为了使系统性能的公认尺度达到最大而进行的关于许多系统元素相互间复杂关系的设计,在设计时对以任何方式和系统相关联的所有因素加以考虑,包括人力的利用以及该系统各个组成部分特性的利用。它是一种管理方法,是一种用于管理系统的规划、研究、设计、制造、试验和使用的科学方法。

系统工程是以系统为研究对象的一门边缘学科。它是根据总体协调的需要,把自然科学和社会科学中的某些思想、理论、方法、策略和手段等有效地结合起来,应用于人类实践,运用系统理论、现代数学、控制论、信息论和电子计算机等工具,对系统的构成要素、组织机构、信息交换和自动控制等功能进行分析研究,从而达到最优设计、最优控制和最佳管理的目的,是为更加合理地研制和运用系统而采取的各种组织管理技术的总称。也可以简单地定义为: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。这个定义,比较明确地表述了3层意思:系统工程属于工程技术,主要是组织管理的各类工程方法论;是解决工程活动整体及其全过程优化问题的工程技术;这种技术具有普遍的适用性。

(2) 系统工程的理论基础

系统工程是一门边缘学科,涉及很多学科,但究其理论基础,大致可分为两类:共同理论基础和分支理论基础。

1) 共同理论基础

共同理论基础是奠定和发展系统工程理论和方法的专业知识,如运筹学、控制论、信息论、计算科学等,其发展为系统工程提供了理论和方法,对系统分析、综合、优化和控制提供了可靠的理论依据和手段。

2) 分支理论基础

工程学的分支理论基础是系统工程实践中所需的专业知识。它是系统工程应用到某一特定领域时所需的特殊理论基础。如安全系统工程是系统工程在安全领域中的应用,应用时必须以安全工程为其理论基础,才能解决生产过程中的安全问题,并使之达到最优状态。

(3) 系统工程的特征

系统工程的基本原理就是用管理工程的办法组织管理整个系统。它以系统为对象,把要组织和管理的物,用概率、统计、运筹和模拟等方法,经过分析、推理、判断和综合,建成某种系统模型,以最优化的方法,求得最佳结果。使系统达到技术上先进、经济上合算、时间上节约、能协调运转的最优效果。因此,它具有以下特征:

- ①优化的方法使系统达到最佳。
- ②与具体的环境和条件、事物本来的性质和特征的密切相关性。
- ③它着眼于整个系统的状态和过程,不拘泥于局部的、个别的部分,它表现出系统最佳途径并不需要所有子系统都具有最佳的特征。
- ④它包含着深刻的社会性,涉及组织、政策、管理、教育等上层建筑因素。
- ⑤它的精华在于,它是软技术,即在科学技术领域,由重视有形产品转向更加重视无形产品带来的效益。

1.1.3 安全系统工程

安全系统工程是运用系统论的观点和方法,结合系统工程学原理及有关专业知识,对所研究对象中的危险进行辨识、分析、评价与控制,使系统或生产过程达到一种最佳安全状态的综合性技术科学,是系统工程学的一个重要分支。

(1) 基本概念

1) 安全与危险

安全和危险是一对互为存在前提的术语,在安全评价中,主要是指人和物的安全和危险。

安全是指免遭不可接受危险的伤害。它是一种使伤害或损害的风险限制处于可以接受的水平的状态。安全程度用安全性指标来衡量。其实质就是防止事故,消除导致死亡、伤害、急性职业危害及各种财产损失发生的条件。

危险也是一种状态,指存在引起人身伤亡、设备破坏或降低完成预定功能能力的状态。当存在危险时,就存在产生这些不良影响的可能性。危险也就是人们所不愿意见到的可以造成人身伤害、财产损失、环境破坏的威胁。人们在现实生活中始终面临着大量的危险(如自然灾害的伤害、生产过程事故等)。通常人们采用危险性大小来衡量危险程度。危险性是对危险系统的客观描述,说明危险的相对程度。它用危险概率和危险严重度来表示危险可能导致的后果。危险概率是发生危险的可能性。它可用定量的方法表示,一般用单位时间内危险可能出现的次数来描述。危险严重度是对危险造成结果的评价。

生活在现实世界里的每一个人都要面临大量的危险。面对众多的危险,人们不断努力去追求所谓的安全。按一般的理解,安全是没有伤害、损害或危险,不遭受危害或损害的威胁,或免除了伤害的威胁。然而世界上没有绝对的安全,安全即为没有超过允许限度的危险。按此理解,安全也存在危险,只不过其危险性很小,人们可以接受它。这种没有超过允许限度的危险被称为可接受的危险。

所谓可接受的危险,是来自某种危险源的实际危险,但是它不能威胁有知识而又谨慎的人。例如,在交通拥挤的道路上骑自行车,虽然能发生交通事故,但是人们仍然愿意骑车代步。

被社会公众所接受的危险称为“社会允许危险”。在安全评价中,社会允许的危险是判别安全与危险的标准。

同时,安全也是一个相对主观的概念,安全是一种心理状态。对于同一事物是安全还是危险的认识,不同的人是不一样的;即使同一个人当其具有不同的心理状态、不同的立场、不同的目的时,对危险的认识也是不同的。

研究表明,有许多因素影响着人们对危险的认识程度。一般来说,当人们进行某项活动时,可能获得的利益越多,所能承受的危险程度就越高。如图 1.4 所示,处于 A 处且相对获得的利益较少的人认为是安全的,而处于 B 处且获利较多的人也认为是安全的。美国原子能委员会曾引用利益与危险关系图来说明人们从事非自愿的活动所获得的利益与承受的危险之间的关系,如图 1.5 所示。

影响可接受危险程度的因素还包括人们是否自愿从事某项活动,危险的后果是否立即出现,对危险的认识程度等。

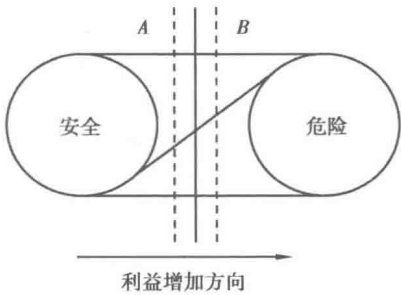


图 1.4 社会允许方向

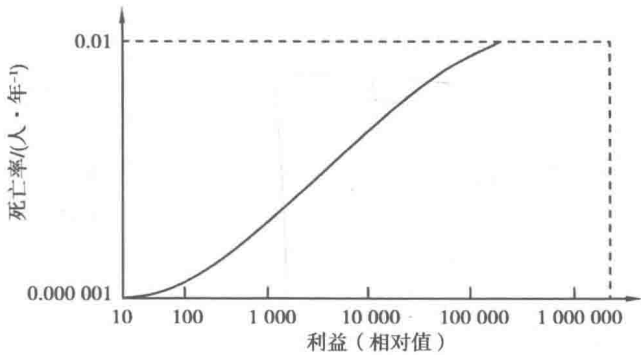


图 1.5 利益与危险关系

- 经过人们对危险的认识和实际危险之间关系的研究,容易得到如下结果:
- ①人们往往认为疾病死亡人数低于交通事故死亡人数,实际上前者是后者的若干倍。
 - ②低估了一次死亡人数少、但大量发生的事故的危险性。
 - ③高估了一次死亡许多人、但很少发生的事故的危险性。

在人们的心目中一般认为平均每年只导致一次死亡 300 人的社会活动比导致平均每天死亡 1 人的社会活动更加危险。出现这种情况的原因是一些精神的、道义的和和社会心理因素起的作用。

2) 安全标准

安全是一个相对的、主观的概念。评定状态是否安全需要有一个界限、目标或标准,通过与量化的风险率或危害程度进行比较,判定其是否达到人们所期盼的安全程度。我们把这个标准称为安全标准。受技术、资金等因素的制约,危险是不可能完全杜绝的。安全标准实际上是一个社会各方面可以接受的危险度。例如 20 世纪 60 年代,美国根据交通事故统计资

料得出,每年每 103 个美国人中有 25 人因乘坐小汽车死亡,但是当时美国人没有因为这种风险而放弃使用小汽车,说明这个分析能够被美国社会所接受,所以这个风险率可作为美国人使用小汽车作为交通工具的安全标准。

确定安全标准的方法有统计法和风险与收益比较法。对系统进行安全评价时,也可以对评价得到的危险指数进行统计分析,确定适用一定范围的安全标准。

对于有统计数据的行业,常用事故可能造成人员的伤亡或事故可能造成的经济损失作为制订安全标准的依据。根据海因里希事故调查报告统计规律:

死亡(重伤):轻伤:无伤害 = 1:29:300

因而可以通过死亡率来推断伤亡情况,把平均死亡率作为安全标准制订的依据。例如英国化学工业的 FAFR(工作一亿个小时的死亡率)为 3.5,英国帝国化学公司(ICI)提案取 0.35 作为安全标准。而美国各公司的安全标准大都取各行业安全标准的十分之一。

(2) 安全系统及其特点

1) 安全系统的概念

安全系统是以人为中心,由安全工程、卫生工程技术、安全管理、人机工程等几部分组成,以消除伤害、疾病、损失,实现安全生产为目的的有机整体,它是生产系统的一个重要组成部分。

2) 安全系统的特点

安全系统的特点可以归纳为如下几个方面。

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。由于安全系统中的各因素之间,以及因素与目标之间的关系多数有一定灰度,所以安全系统又称为灰色系统。

依据安全问题所涉及的范围大小不同,安全系统大小之差可能很悬殊。一般来讲,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,则不仅为机和物,肯定要把人一机一环境都考虑进来。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,即便是一台设备,如果把它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、时间延滞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源、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确定性,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确定,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(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了随机的特征(外在随机性)。由于安全系统把环境看成是它的组成部分,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”确定安全系统各因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由于安全系统本身不清楚;它可能只是人们的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。安全系统发展过程的突变或畸变,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规律。

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故事的启动,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。

3) 安全的动力学特征

从系统的结构和功能形成看,可将系统分为两类;一类是自组织系统,另一类是被组织系统。协同学的创始人哈肯教授曾给自组织下了一个非常经典的定义,他认为,如果系统在获得空间的、时间的或功能的结构过程中,没有外界的特定制约,便说系统是自组织的。这里的“特定”一词是指,那种结构或功能并非外界强加给系统的,而且外界以非特定的方式作用于系统的。可见,自组织与被组织的区别就在于,系统行为是否受外界某种特定干预的影响。显然,自组织的动力在系统内部,是自己运动的结果;而被组织的动力在系统外部,是在外部特定的干预下运动的结果。一般而言,自组织系统因其动力来自系统内部,因而它具有持久

永恒的生机和活力;相反,被组织系统因其动力来自系统外部,因而其生机和活力随外部干预状态的变化而变化。

安全系统是物质系统。安全系统既可能是自组织的,也可能是被组织的,也可能两者兼而有之。对安全来说,所谓外界的特定干预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,其本质组织程度从相对较低向相对较高演化;另一种则是维持相同组织层次,但复杂程度必定相对增加。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、地震、战争、纵火、瞎指挥、违规操作等,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,所谓的开放性将不起作用,无序—有序的过程也就不会发生。

(3) 安全系统工程简介

人类社会在发展过程中经历了各种各样的事故,人类为了自身的生存和发展,不仅要采取各种安全措施来解决生产中的各种事故,还要研究生产过程中各种事故之间的内在联系和变化规律。通过实践,人们总结出对付事故的两种办法。

第一种是事故发生后吸取教训,进行预防的方法,有人也称这种方法为“问题出发型”。例如,从事故后果查找原因,采取措施防止事故重复发生。通常采取的各种组织和技术措施,如设立专职机构,制定法规标准,进行监督检查和宣传教育,以及防尘防毒,防火防爆,使用安全防护设备、个人防护用具等,都属此类,这就是通常的传统安全工作方法。

第二种是用系统工程控制事故的方法,有人也称这种方法为“问题发现型”。这种方法是从系统内部出发,研究各构成部分存在的安全联系,检查可能发生事故的危险性及其发生途径,通过重新设计或变更操作来减少或消除危险性,把发生事故的可能性降低到最低限度。这就是系统科学的思想,运用系统的思路解决生产中遇到的安全问题。

1) 安全系统工程的定义

安全系统工程是指应用系统工程的基本原理和方法,辨识、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的一门综合性技术科学。

对这个定义,可以从以下几个方面理解:

①安全系统工程是系统工程在安全工程学中的应用,安全系统工程的理论基础是安全科学和系统科学。

②安全系统工程追求的是整个系统或系统运行全过程的安全。

③安全系统工程的核心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是将系统风险控制在人们能够容忍的限度以内,