

高等学校教材·航空、航天、航海系列
TEXTBOOKS FOR HIGHER EDUCATION

安全系统工程

邓琼 编著



西北工业大学出版社

高等学校规划教材

安全系统工程

邓 琼 编著

西北工业大学出版社

【内容简介】 本书全面地介绍了安全系统的概念以及安全系统分析、评价、预测和决策等基本原理和方法在安全系统工程中的应用。全书共分8章, 主要内容包括安全系统的基本概念、事故与危险源的基本概念、系统安全分析、系统安全评价、系统安全预测、系统安全决策以及系统可靠性分析基础和航空系统可靠性等。

本书主要作为高等院校安全工程专业学生的教材, 也可作为从事安全工程的技术人员和管理人员的参考用书。

图书在版编目 (CIP) 数据

安全系统工程/邓琼编著. —西安: 西北工业大学出版社, 2009. 8

ISBN 978-7-5612-2624-7

I. 安… II. 邓… III. 安全工程: 系统工程 IV. X913.4

中国版本图书馆 CIP 数据核字 (2009) 第 146942 号

出版发行: 西北工业大学出版社

通信地址: 西安市友谊西路 127 号 邮编: 710072

电 话: (029) 88493844 88491757

网 址: www.nwpup.com

印刷者: 陕西天元印务有限公司

开 本: 787 mm×1 092 mm 1/16

印 张: 13

字 数: 312 千字

版 次: 2009 年 8 月第 1 版 2009 年 8 月第 1 次印刷

定 价: 28.00 元

前 言

“安全系统工程”是安全工程专业的的主要专业课程之一，是系统工程的重要分支。安全系统工程的理论和方法不但可以应用于现代安全管理中，而且可以应用于先进的安全设计技术中。同时，系统安全的观点和方法对安全工程学科体系的形成和完善起着重要作用。因此，安全系统工程是以安全工程、系统工程、可靠性工程等技术为手段的一门新兴、交叉学科。

目前，针对各领域、各行业安全工程的专业书为从事安全工程的工作人员和安全工程专业的学生提供了参考，为充实和发展安全工程学科奠定了理论基础。本书与这些专业书相比，借鉴了其中的主要安全理论，更加突出了航空安全工程的特点。作者结合多年从事安全工程专业教学的实践，并在整理授课的教案及讲义的基础上进一步充实、提高，编著了这本书。本书不仅适合于航空安全工程专业学生学习，同时也适合于其他行业安全工程专业学生学习。本书的特色体现在：第一，系统地介绍安全性、可靠性分析以及评价的理论和方法；第二，突出航空安全工程专业的特色；第三，教材编写紧密结合安全工程专业发展的最新方向和先进技术。

本书共分 8 章。

第 1 章绪论，系统地介绍了与安全系统工程相关的概念和安全系统工程的研究对象、研究内容以及安全系统工程的产生和发展。

第 2 章事故与危险源，介绍了事故的基本概念和分类以及危险源的基本概念、危险源辨识的方法、分类和分级。

第 3 章系统安全分析，介绍了系统安全分析的理论和方法以及常用的几种定量和定性的安全分析方法。

第 4 章事故树分析，介绍了事故树的基本概念，事故树的编制、数学表达及其定性、定量分析方法等。

第 5 章系统安全评价（风险评价），介绍了先进的系统安全评价（风险评价）的理论和方法，其中详细分析并比较了几种常用的定性、定量的系统安全评价方法。

第 6 章系统安全预测，介绍了系统安全预测的基本概念、分类、分析程序、基本原则和方法以及常用的预测方法在安全生产中的应用。

第 7 章系统安全决策，介绍了系统安全决策的基本概念、类型、任务、要素、基本程序和几种常用的系统安全决策方法。

第 8 章系统可靠性分析基础和航空系统可靠性，介绍了系统可靠性分析的基本概念和航空系统可靠性技术。

全书力图包含安全系统工程所涉及的主要内容和理论方法。学生通过学习，能够对安全

系统工程有一个整体的认识。另外，作为教材，本书力求做到通俗易懂，便于学生学习和掌握。在本书的编写过程中，感谢叶婷硕士在文字输入方面给予的帮助。

由于编者水平有限，不足之处在所难免，敬请读者批评指正。

编著者

2009年5月

目 录

第 1 章 绪论	1
1.1 与安全系统工程相关的基本概念	1
1.2 安全系统工程的研究对象和研究内容.....	13
1.3 安全系统工程的产生和发展.....	16
本章小结	18
思考题	18
第 2 章 事故与危险源	19
2.1 事故.....	20
2.2 重大危险源的辨识.....	25
本章小结	40
思考题	41
第 3 章 系统安全分析	42
3.1 概述.....	43
3.2 安全检查表.....	46
3.3 预先危险性分析.....	50
3.4 故障类型与影响分析.....	52
3.5 危险性与可操作性分析.....	56
3.6 事故树分析.....	60
3.7 事件树分析.....	61
3.8 事故的因果分析.....	64
本章小结	68
思考题	68
第 4 章 事故树分析	69
4.1 事故树分析概述.....	69

4.2 事故树的编制.....	73
4.3 事故树的数学表达.....	76
4.4 事故树的定性分析.....	80
4.5 事故树的定量分析.....	86
本章小结	97
思考题	97
第5章 系统安全评价 (风险评价)	99
5.1 系统安全评价概述	100
5.2 安全检查评价法	107
5.3 生产作业条件安全评价	109
5.4 危险物质加工处理安全评价	114
5.5 概率危险性安全评价	120
5.6 人工神经网络安全评价法	122
5.7 模糊安全评价	125
5.8 几种安全评价方法的比较	133
本章小结.....	135
思考题.....	135
第6章 系统安全预测.....	136
6.1 系统安全预测概述	136
6.2 系统安全预测的方法	139
本章小结.....	151
思考题.....	152
第7章 系统安全决策.....	153
7.1 系统安全决策概述	154
7.2 安全决策的方法	159
7.3 各种安全决策方法中的共性问题	174
本章小结.....	174
思考题.....	174
第8章 系统可靠性分析基础和航空系统可靠性.....	176
8.1 系统可靠性分析基础	177

8.2 航空系统可靠性技术	187
本章小结.....	198
思考题.....	198
参考文献	200

第 1 章 绪 论

本章学习目标

- (1) 掌握与安全系统工程相关概念的定义和内涵。
- (2) 掌握安全系统工程的基本概念,了解安全系统工程的研究对象、研究内容和研究方法。
- (3) 了解安全系统工程的产生和发展历程。

安全系统工程,是以安全学和系统学为理论和基础,以安全工程、系统工程、可靠性工程等技术为手段,对系统风险和危险进行分析、预测、评价、控制,以实现系统及其全寿命周期过程中的安全为目标的科学技术。安全系统工程的基本理论和技术涉及自然科学和社会科学,是安全科学学科的重要分支,是现代科技发展的必然产物。

安全系统工程不但是安全科学的理论基础之一,而且是指导安全工作实践的基本理论之一。为了使读者对课程的内容有一个深入的了解,本章将从三个方面进行讲解,学习思路如图 1.1 所示。读者首先学习与安全系统工程相关的基本概念,其次掌握安全系统工程的研究对象和研究内容,最后了解安全系统工程的产生和发展历程,为整个课程的学习打好基础。

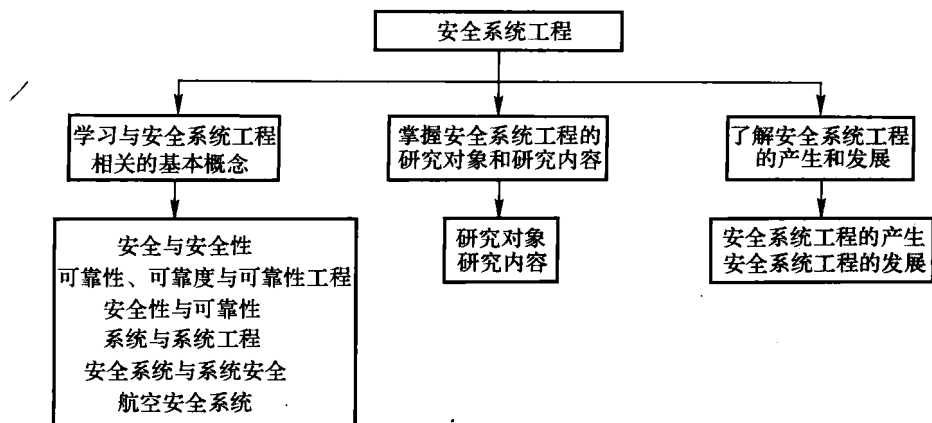


图 1.1 本章的学习思路

1.1 与安全系统工程相关的基本概念

1.1.1 安全与安全性

一、安全

安全同我们每一个人的生活息息相关,它是和我们的生命联系在一起的。安全又是人类

社会发展永恒的话题,从人类诞生伊始,人类就为了自己的生存与自然进行着斗争,为了安全而展开了形形色色的活动。随着科学技术的飞速发展,安全问题会变得越来越复杂,越来越多样化,对安全问题的研究也需要更深入、更具有科学性。在我们研究安全之前,首先需要弄清楚安全的基本概念。

“安全”一词是人们利用抽象思维而确定的一个概念或理念,对安全的描述可以是静态的,也可以是动态的;可以是定量的,也可以是定性的;可以是确定的,也可以是模糊的或不确定的。同时,从技术的角度出发,描述安全的状态或过程又是错综复杂的,其中的特征量无法统一。因此,如何界定安全的内涵是非常困难的事情。

从“安全”这个词本身的含义来理解,“安”是指不受威胁、没有危险,即无危则安,“全”是指完满、完全、齐备、没有伤害,无损坏,无损失,即无损(缺)则全。从这个层面上来理解,“安全”即为无危险、无伤害、无损缺,尽善尽美。这种字面的含义只能代表理想化的一种企盼,是一个抽象的概念。而要从安全科学的角度去规范安全的定义,一方面需要从安全的状态、过程、理念以及技术安全等方面出发,全面地了解安全的内涵;另一方面也需要从安全科学的发展历程去了解安全的实质内容和与其相关的理论体系。

1. 对安全的早期认识

首先,我们来看戴头盔这个现象。骑摩托车和骑自行车赛车时,规定必须戴头盔,否则认为是危险的;在马路上骑自行车,不必戴头盔,认为是安全的。同样是骑车,要求却不一样,体现了安全与危险的相对性,安全和危险的评判标准是车的速度。进入建筑工地,必须带头盔,否则认为是危险的;行走在大街上,就不用带头盔,认为是安全的。在这里安全和危险的评判标准是人的头部所能承受的打击能量和发生打击事件的概率。

人们对安全和危险的这种主观评判标准就是最早对安全定义的理解,即安全是指客观事物的危险程度能够为人们普遍接受的状态。这种状态就是指安全的相对性以及安全与危险之间的辩证关系,说明安全和危险不是互不相容的。当人们认为所处的状态是可以接受的,就认为是安全的;不能接受,就认为是不安全的。这种早期对安全的认识没有科学的依据和定量的判据,只是人们根据大量事故的统计和分析结果以及凭借经验对安全的初步理解。

2. 从工业化的角度认识安全

随着工农业生产的不断发展以及大机器的出现和广泛应用,生产过程中自动化程度和复杂程度不断提高。为了控制危险,安全生产,人们对安全的过程进行表征,对安全的状态进行定性和定量的描述。从工业化的角度认识安全,安全的定义可以表述为:安全是指没有引起死亡、伤害、职业病或财产、设备的损坏或损失或环境危害的条件。

这个定义来自美国军用标准 MIL-STD-882C《系统安全大纲要求》。1957年,苏联发射了第一颗人造地球卫星后,美国急于保护其空间技术优势,匆忙发展导弹武器。由于忽略了系统安全,在短短的一年半时间内发生了4次大的事故,造成了数百万美元的损失。1962—1969年,美国军方用了7年的时间,建立了较为完整的系统安全的概念,也给安全赋予了较为合理和完整的定义。从这个定义可以看出,安全的定义从开始仅仅关注人身伤害,进而到关注职业病、财产及设备的损耗直至关注环境危害,体现了人们对安全问题认识进化的全过程。

3. 从安全科学的角度认识安全

随着人们对安全问题研究的不断扩展和各行各业对安全的重视,安全的基本概念也纳入了安全科学的范畴。安全不再是常识,而是科学,它有规律可循,有理论可依。其中还包含多

学科的理论,如自然科学、社会科学、系统工程、管理工程等多学科的理论 and 知识。安全作为一门科学,其定义为:安全是指不因人、机、媒介的相互作用而导致系统损失、人员伤亡、任务受影响或造成时间的损失。

这个定义将安全的概念扩展到了任务受影响或时间损失,这意味着即使没有遭受直接损失,也可能是安全科学关注的范畴,这样就使得安全学具有了动态的特征。同时,使得安全科学涵盖了安全管理方法与理论、安全经济学原理、安全行为理论、安全风险学、安全人机学原理等领域的学科理论和知识。

4. 从系统工程的角度认识安全

面对日益复杂的系统,安全已经不是单纯的安全问题,而是和系统工程紧密结合在一起并存在于系统的各个寿命周期阶段。由于系统中的各组成部分和各个研究发展阶段都存在安全的问题,从更加严格和规范化的意义上来讲,安全实际上是系统的安全。因此,从系统工程的角度来认识安全,安全的定义为:安全是指系统在其全寿命周期范围内,不因人、机、媒介的相互作用而导致系统损失、人员伤亡、任务受影响或造成时间的损失。

由此可见,安全的概念已不是传统的职业伤害和疾病,也不是仅存在于企业的生产过程中。安全科学关注的领域涉及人类生存、生活、生产活动的各个方面,贯穿于人类发展的各个阶段。从某种意义上说,人类社会的发展史可以看成是人类解决安全问题的奋斗史。

二、安全性

从安全的定义中我们了解到,安全是系统的一种状态或条件或概念,而在安全科学的研究过程中,常常需要对系统抵抗危险的能力进行评价,即系统的安全性。安全性是系统在可接受的最小事故损失条件下发挥其功能的一种品质,也可将安全性定义为“不发生事故的能力”。由此可见,安全是系统的状态或条件,安全性是系统的一种性能和能力。对于安全工作者来说,其任务就是结合管理、技术和教育等各种手段和措施,努力提高系统的安全性,减少事故造成的损失。

1.1.2 可靠性、可靠度与可靠性工程

1. 可靠性

可靠性是指系统在规定的条件下和规定的时间区间内完成规定功能的能力。理解这个定义应注意以下4个要点。

(1)“系统”通指作为单独研究和分别试验的对象任何元件、零件、部件、设备、机组等,在安全系统工程中,可靠性的研究对象除了上述的系统外,还包括人和环境的因素。

(2)“规定的条件”一般指的是使用条件、维护条件、环境条件、操作条件等,如载荷、温度、压力、湿度、振动、噪声、磨损、腐蚀等。这些条件必须在使用说明书中加以规定,这是判断发生故障时有关责任方的关键。

(3)“规定的时间区间”表明,由于可靠度是随时间而降低的,所以只能在一定的时间区间内考核达到的目标可靠度。对于规定的时间区间,不仅仅指日历时间,根据系统的不同,也可能是与时间成比例的次数、距离等,如应力循环次数、汽车的行驶里程等。

(4)“规定的功能”,首先要明确具体的功能是什么,怎样才能符合完成规定的功能。这种判

定有时很容易,有时却很难。例如,齿轮的折断就是失效,这很容易判定;但当齿面发生了某种程度的磨损时,对于某些机械不影响其正常运作,就不属于失效,而对于精密的机械来说,就是失效。

2. 可靠度

可靠度是指衡量系统可靠性的标准,是指系统在规定的时间内完成规定功能的概率,通常用 R 表示。考虑到 R 是时间的函数,可以表示为

$$R = R(t) \quad (1.1)$$

$R(t)$ 称为可靠度函数。如果就概率分布而言,它又称为可靠度分布函数,且是累积分布函数。它表示在规定的使用条件下和规定的时间内,无故障地发挥规定功能而工作的产品占全部工作产品的百分率。

3. 可靠性工程

可靠性工程是指研究系统可靠性的工程技术。可靠性工程要解决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。

1.1.3 安全性与可靠性

在了解安全性与可靠性之前,我们首先来做一个测试。

每个人从宿舍到教室上课,中间经过食堂,会发生什么意外呢?也许会吃坏了东西,拉肚子;也许会滑倒,扭伤脚;也许会被热饭烫伤了手……可能会有许多意外事件的发生。从这些可能意外发生的事件中,我们可以简单地计算一下发生各种事故的概率,也可以估算我们从宿舍到教室要保证能正常上课的可能性有多大,这就是最简单的可靠性。

从这个小测试中我们可以看到,安全性关心的是从宿舍—食堂—教室这个过程中,人身是否受到伤害,是否影响到正常上课,正常上课的条件和状态;可靠性关心的是从宿舍—食堂—教室这个过程中,上课这种活动能正常进行的概率是多少。也就是说,安全性关注的是宿舍—食堂—教室各个环节是否安全,不考虑上课能否正常进行;可靠性关注的是能否正常上课。

对于航空系统,安全性关心的是在飞行过程中能否不发生事故,不会造成机毁人亡的事件。可靠性关心的是能否完成运送乘客、物资以及特殊的行动计划和预定的功能。

从这些事例中可以看到,安全性和可靠性从表面上看,似乎是分离的、没有联系的,其关注的方向各不相同。而实际上,安全性和可靠性作为判断和评价系统功能的两项重要指标,在系统的全寿命周期范围内,两者是相互联系、相互作用的,是辩证对立统一的一个整体。

(1) 有些可靠性和安全性的指标是一致的,系统不可靠是系统不安全的原因,即不可靠现象导致不安全事故的发生。当系统发生故障(不可靠)时,不仅影响系统功能的实现(不可靠工作),还会导致发生事故,造成人员伤亡或财产损失(不安全)。例如,汽车操纵系统失误,会导致汽车失控;建筑物材料强度不够,会导致倒塌;飞机的发动机发生故障时,不仅影响飞机正常飞行,还可能使飞机失去动力而坠机,造成机毁人亡的后果。此时,提高可靠性就能够保证安全性,好的安全性指标是从保证高的可靠性水平入手的。

(2) 可靠性着眼于维持系统功能的发挥,实现系统目标;安全性着眼于防止事故发生,避免人员伤亡和财产损失。因此,两者的着眼点不同,造成有些时候可靠性和安全性的指标是矛

盾的,提高安全性可能会导致不能正常工作。例如,炸药的钝化会使炸药在制备、储存、运输、使用等环节上更加安全,但是钝感炸药的起爆条件会更加苛刻,当起爆能量达不到要求时,就不能可靠地作用。而采用敏感的炸药,可以保证在使用中可靠起爆,但其安全性又得不到保障。

值得注意的是,从表面上看,安全性工程贯穿了系统设计、研制、生产、使用等寿命周期的全过程,可靠性仅关注是否能够可靠作用和可靠使用的能力。其实并不是如此,可靠性工程也是贯穿于系统研究的各个阶段的,如可靠性工程在设计阶段考虑设计可靠性、可靠性目标、可靠性预计、可靠度分配,在研制阶段考虑可靠性试验,在生产阶段考虑质量管理和质量控制,在使用过程中,考虑可靠性统计等。因此,无论是安全性还是可靠性,都贯穿于系统的全寿命周期的各个阶段。就系统的功能而言,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。系统的可靠性和安全性是两个既有区别又有联系的功能性指标,在系统安全研究中,需要广泛利用、借鉴可靠性研究中的一些理论和方法,如系统安全分析中常用的故障类型与影响分析、事件树分析、事故树分析等,都是系统可靠性分析的方法。

1.1.4 系统与系统工程

一、系统

系统工程的研究对象是系统。我国科学家钱学森把极其复杂的研究对象称为系统,认为正如工程技术各个专业一样,系统工程也是一个总类总称,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称为工程系统工程,生产企业或企业体系的系统工程称为经济系统工程等。

系统论的创始人奥地利学者贝塔郎非指出,系统的定义可以确定为处于一起的相互关系中,并与环境发生关系的各组成部分的总体。

从系统工程学科的角度去考虑,系统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。例如,铁路系统由车辆、轨道、变电站、车站以及通信设备等构成,各个组成部分相互依赖,共同作用;功能是将旅客、货物从一个地方安全地运抵另一个地方。

对于大系统来讲,它的各个子系统本身又可以单独成为一个系统,这个系统又可以分成若干个子系统。由此分下去,直至系统中的各个元件、单元。例如,火控系统是由雷达、指挥仪、火炮、炮弹等组成的复杂系统,它的每一个单元本身又可以自成系统。对于火控系统来讲,炮弹是子系统,如果把炮弹作为系统来定义,那么它的子系统又是引信、弹丸、发射药、药筒、底火等。其中,底火又由底火体、外壳、垫片、压盖、火帽、加强帽、点火药等组成。火帽作为点火或起爆序列中的首发元件,由火帽壳、加强帽、击发药、加强药、虫胶漆等组成。

系统的特征表现在以下5个方面。

1. 整体性

系统由相互区别的各要素(元件或子系统)组成,各要素具有不同的性质和功能,但组成系统后,形成新的特定功能,具有整体的特点。例如飞机是由许多部件组成的,在飞机的制造过程中,对于制造者来说,只是制造飞机的零部件,保证零部件的质量和性能;而设计者将这些

部件组合在一起,就构成了飞机整体,并体现飞机整体的性能。

2. 相关性

系统的各个组成部分相互联系,相互依赖,相互作用,有机联系在一起。例如,引信由保险与解除保险机构、目标探测装置、发火机构、战斗部等组成,保险与解除保险机构用来保障引信使用前和使用中的安全性和可靠性,目标探测装置用以实现引信发火时机、发火方式的选择,发火机构接受目标探测的信号,对引信中的首级火工元件输出发火信号,引信发火后,通过爆炸序列的作用,将发火能量放大,引爆战斗部,使得整个引信作用。因此,系统中的各个子系统虽然发挥的作用不同,却是相互联系、相互依赖的。

3. 目的性

任何系统都是为了完成某种任务或实现某种目的而发挥其特定功能。要达到系统的预定目的,就必须赋予系统规定的功能,在系统的整个寿命周期内,达到最优规划、最优设计和最优控制。例如,飞机系统是为了完成空中飞行功能,火车的功能是为了完成运输的功能。

4. 有序性

有序性表现在空间结构的层次性和系统发展的时间顺序性。其具体表现为:在进行安全分析时,首先在空间结构上将系统分割为各个子系统,各个子系统又可以再细化为分系统,分系统又可分解为各个作用单元。其次在时间顺序上,每个作用单元、分系统、子系统和整个系统都有其发生、发展、成熟、衰弱、消亡过程,在各自的寿命阶段,都赋予了不同的功能。由此构成了系统在空间和时间上的有序性。

5. 环境适应性

环境的变化可能引起系统特性和功能的变化,同一个系统在不同的环境中发挥不同的作用。系统的适应性是指系统通过自我调节适应环境变化的性质,这种适应是通过与环境进行能量、物质和信息的交换来实现的。也就是说,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。因此,环境对系统功能的实现起着十分重要的作用。

二、系统工程

系统工程是以系统为研究对象,以达到总体最佳效果为目标,为达到这一目标而采取组织、管理、技术等手段,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的一门综合性的科学技术。系统工程是一种对所有系统都具有普遍意义的科学方法,属于工程技术的范畴,主要包括组织管理各类工程的方法论,是组织管理工程、解决系统整体及其全过程优化问题的工程技术。

系统工程是一门新兴的科学,研究安全科学,必须与系统工程的理论和技术紧密结合。

(一) 系统工程方法

系统工程方法主要有工程逻辑、工程分析、统计理论和概率论、运筹学等。

1. 工程逻辑

工程逻辑是从工程的观点出发,用逻辑学与哲学的一般思维方法进行系统的探讨和应用,同时把符号逻辑作为重要内容。

2. 工程分析

工程分析是运用基本理论,系统地、有步骤地解决各类工程问题。在分析过程中需要正确

地运用数学方法。

3. 统计理论和概率论

统计理论和概率论是由系统工程的数学特点所决定的,即系统的输入量与输出量带有很大的随机性。并且,在复杂的系统工程中常常会遇到随机函数的问题,因此,需要采用统计理论和概率论来处理系统工程中所遇到的数学问题。

4. 运筹学

运筹学是指有目标地、定量地做出决策,在一定的约束条件下使系统达到最优化。

(二) 系统工程的原理

系统工程的主要原理有系统原理、整分合原理、反馈原理、封闭原理和动态相关性原理等。

1. 系统原理

现代管理对象都可以看做是一个系统,它包含若干分系统(子系统),同时又和外界的其他系统发生着横向的联系。为了达到现代化管理的优化目标,就必须运用系统理论,对管理进行充分的系统分析,使之优化。

2. 整分合原理

整分合原理是在整体规划下明确分工,在分工基础上进行有效的综合。其中,整体规划是在对系统进行深入、全面分析的基础上,把握系统运动规律,确定整体目标,制订规划与计划。分工是指确定系统构成,明确各个局部的功能,对整体目标分解,确定各个局部的责、权、利。有效的综合是指对各个局部进行有力的组织管理,使各个局部协调配合、综合平衡地发展,保证最佳整体效应。该原理从本质上讲,就是整体把握,科学分解,组织综合。

3. 反馈原理

反馈是控制论和系统论的基本概念。反馈原理要求把反馈信息与输出信息进行比较,用比较所得的偏差对信息的再输入产生影响,起到控制的作用,以达到预定的目的。通过反馈可以及时掌握外部条件和内部条件的不断变化,及时调整系统状态,保证目标实现。

4. 封闭原理

任何一个系统的管理手段、管理过程都必须构成一个连续封闭的回路,这样才能形成有效的管理活动。封闭原理可以使管理手段、管理过程各部分、各环节相对独立,既充分发挥功能,又相互衔接,相互制约,首尾相连,形成一条封闭的管理链。图 1.2 所示给出了管理链的构成。

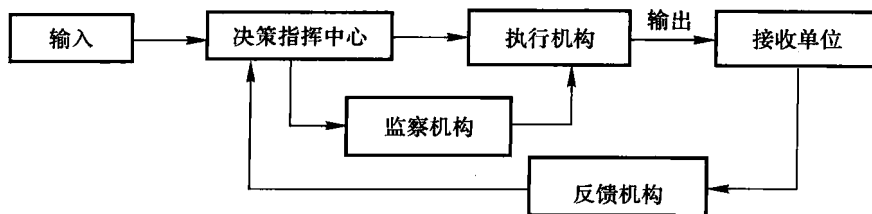


图 1.2 管理链的构成

值得注意的是,这种封闭是相对的。从空间上讲,封闭系统不是孤立系统,它要受到系统管理的作用,与上、下、左、右各个系统都有输入和输出的关系,应协调平衡地发展,而不是自行

其是地发展。从时间上讲,事物是不断发展的,永远不能做到完全预测未来的一切。因此,必须求得动态的发展,在变化中不断前进。

5. 动态相关性原理

动态相关性原理是指构成系统的各个要素是运动和发展的,又是相互关联和相互制约的,并随着时间、地点以及人们的努力程度而发生着变化。因此,要提高管理的效果,必须掌握各个要素之间的动态相关特征,充分利用相关因素的作用。

使用系统工程方法,可以识别出存在于各个要素本身、要素之间的危险性,可以了解各个要素间的相互关系,消除各个要素由于相互依存、相互结合而产生的危险性。

1.1.5 安全系统与系统安全

一、安全系统

与安全问题相关的系统称之为安全系统。安全问题是一个复杂的系统工程问题,解决安全问题要运用系统工程的理论和方法。安全系统与一般系统有共同点,也有其特殊性。安全系统的特性表现在以下6个方面。

1. 系统性

安全系统是由与安全有关的影响因素构成的,由于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大系统,具有系统的特性。同时,安全系统与一般系统不同,具有其特殊性。这种特殊性表现在安全系统始终把人和环境看成是系统的组成部分。例如,一台设备或仪器,仅从其功能考虑,可能只是机和物。而对于一个车间甚至一个工厂,如果考虑安全问题的系统范围,就不能只考虑机和物,而要将人和环境考虑进去。实际上,人-机-环境是考虑了安全问题的空间跨度和时间跨度两个方面,即使是一台设备,如果把它的制造安全与使用安全考虑进去,仍然是人-机-环境的复杂系统。

2. 开放性

安全系统是客观存在的,它总是寄生在客体(这里的客体可以认为是与安全系统相联系的另一个系统,如交通系统、煤矿系统、建筑系统、航空航天系统等)中。我们可以把客体看成是一个黑匣子,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。

开放性显示出安全系统的复杂性和安全-事故发生之间转换的重要机制。图1.3和图1.4所示分别给出了开放性的示意图与输入和输出函数关系的数学模型。

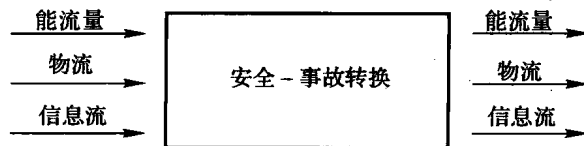


图 1.3 开放性的示意图

在图1.4中, x 可能是安全教育、安全管理、安全技术等; y 可能是安全管理水平、事故率、损失等。协调 x 和 y 之间的关系,应考虑环境因素的影响。

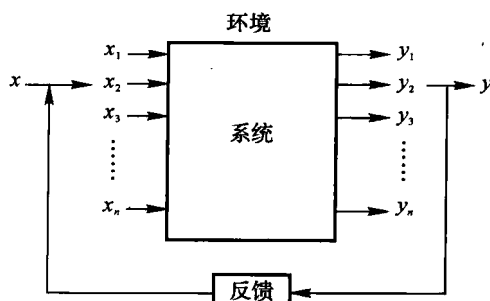


图 1.4 输入和输出函数关系的数学模型

3. 确定性和非确定性

确定性指制约系统演化的规则是确定的,不含任意随机性因素,演化方向和演化结果确定,可以精确预测。非确定性指演化方向和演化结果不确定,或者具有描述事物运动特征的特征量不能客观精确地确定特征。非确定性包含随机性和模糊性。

随机性表现在以下两个方面。

第一,在不合任何外在的随机影响因素作用下,完全由“确定性系统”演化而产生随机性。这种随机性称为本质随机性。

第二,系统可能因其外在影响因素的随机作用而产生随机性行为。这种随机性称为外在随机性。由于安全系统把环境因素看成其组成部分,所以这两种随机性对安全系统而言不明显。

模糊性指事物的本身不清楚或衡量事物的尺度不清楚。安全系统组成目标关系不清楚,原因有两个,一是主观模糊性,二是客观模糊性。例如,建立一个安全评价体系,各组成部分的影响有可能是独立的,有可能是相互影响的,不能准确确定。另外,对于社会的因素、人的因素以及技术因素的耦合关系也难于量化,很难建立准确的数学关系。

应该强调的是,安全系统的非确定性并不是由于安全系统本身不清楚造成的,而是人们对安全系统主观模糊性的表现。同时,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,无法给出客观的衡量尺度。

4. 安全系统是有序与无序的统一体

序是反映事物的组成规律和时域。依据序的性质,序可以分为有序、混沌序和无序三种形式。有序与稳定性、规则性相关联,表现为时间有序、空间有序和结构有序。无序与不稳定、无规则相关联。混沌序指不具备严格周期和对称性的有序态。对安全系统来讲,提出序的概念主要是指不同性质的序之间可以相互转让。如序的转化结果是否引发灾难或使灾害扩大,取决于序结构的类型及系统对特定结构下的运动的承受能力。

5. 突变性或畸变性

安全系统过程的突变或畸变,或过程由连续变化到非连续变化,本质上还是服从量变到质变的规律。量变到质变的转化形式可以用畸变、突变或飞跃来描述,但也可以通过渐变实现。例如,安全系统的渐变可能孕发事故,而突变和畸变则对应于灾害事故的启动,是致灾物质或致灾能量的突然释放。