

普通高等院校安全工程专业
“十二五”规划教材

安全系统工程

主 编 王洪德

副主编 董四辉 王 峰



國防工業出版社

National Defense Industry Press

普通高等院校安全工程专业“十二五



安全系统工程

主 编 王洪德

副主编 董四辉 王峰

国防工业出版社

·北京·

内 容 简 介

本书是安全工程专业必修的专业基础课程教材。本书系统地介绍了安全系统工程的基本概念以及研究对象、目的、内容和方法。主要包括安全系统工程概论、系统安全分析、事故树分析、系统安全评价、系统安全预测、系统安全决策技术等方面的内容。为了加强和实际工作的联系,本书还列举了安全系统工程典型应用实例与分析。

本书可作为高等院校安全工程专业及其相关专业的教材,还可作为安全监察人员及安全科学与工程研究的技术人员、企业安全生产管理部门相关人员的参考用书。

图书在版编目(CIP)数据

安全系统工程/王洪德主编. --北京:国防工业出版社,
2013.2

普通高等院校安全工程专业“十二五”规划教材
ISBN 978-7-118-08594-5

I. ①安… II. ①王… III. ①安全系统工程—高等学校—教材 IV. ①X913.4

中国版本图书馆 CIP 数据核字(2013)第 009363 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 印张 15 1/4 字数 371 千字

2013 年 2 月第 1 版第 1 次印刷 印数 1—4000 册 定价 34.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777

发行邮购:(010)88540776

发行传真:(010)88540755

发行业务:(010)88540717

前 言

安全生产是我国的一项基本国策,是保护劳动者安全健康、保证经济建设可持续发展的基本条件。如何保证安全生产,一直为从事工业生产和安全管理工作者所关注,也是世界各国迫切需要研究和解决的课题。尤其是近年来,由于科技进步和工业生产的迅猛发展,生产规模日趋扩大,生产过程日益自动化,传统的安全工作方法由于不能掌握事故发生的内在规律和对事故进行预测,已很难适应现代安全生产及安全管理工作的要求,其结果是工业生产中不断发生灾难性的事故,造成严重的人身伤亡和巨大的经济损失。这种安全工作与现代化生产不相适应的情况,迫使需要从事安全工作的专家、学者和管理人员去寻求一种对系统的安全性可以进行定性定量评价,能够对事故发生的可能性进行预测的新方法,以便事先给有关人员提出警示,及时采取有效的预防措施,减少或防止事故的发生。安全系统工程正是在这种新形势的要求下应运而生的一门新兴交叉学科。

经过几十年的不断探索和实践,目前,安全系统工程已从应用技术发展到理论研究,并逐步形成自己的理论体系,而且,是安全工程专业学生和从事安全工程的人员需要了解和掌握的一门重要课程。据此,编者结合多年研究和实践,编写了这本《安全系统工程》教材。该教材系统地介绍了系统安全分析、系统安全评价、系统安全预测和系统安全决策等方面的内容。为了加强和实际工作的联系,本教材增加了安全系统工程典型应用实例一章。

本教材是安全工程专业必修的专业基础课程之一,也是相近专业学生学习和了解安全工程知识的主要课程。其先修课程为概率论及数理统计、线性代数、安全学原理和计算机应用技术,学生通过本课程的学习,能够了解和掌握采用系统工程的原理和方法,识别、分析、评价系统中的危险性,并根据其结果调整工艺、设备、操作、管理、生产周期和投资等因素,使系统可能发生的故事得到控制,并使系统安全性达到最佳状态。

全书共分七章:第1章安全系统工程概论,由大连交通大学王洪德编写;第2章系统安全分析,由西安建筑科技大学刘冬华和长安大学李亚兰共同编写;第3章事故树分析,由广西大学李晓泉编写;第4章系统安全评价,由大连交通大学王峰编写;第5章系统安全预测,由大连交通大学董四辉编写;第6章系统安全决策,由长安大学李亚兰编写;第7章典型应用实例,由广

西大学李晓泉和大连交通大学董四辉编写;全书由王洪德主编。全书力图尽量包含安全系统工程所涉及的主要内容,以便使学生学完后,能对安全系统工程有一个整体性的认识。本书在叙述上力求做到通俗易懂,以便于学生学习和掌握。

本书在编写过程中参阅了大量的相关资料,在此,谨对原作者表示最诚挚的谢意。

由于编者水平有限,书中不妥之处在所难免,敬请读者不吝赐教。

编者
2012年10月

目 录

第 1 章 安全系统工程概论	1
1.1 系统论概述	1
1.1.1 系统的内涵	1
1.1.2 系统的分类	1
1.1.3 系统的特性	1
1.2 系统工程概述	3
1.2.1 系统工程的内涵	3
1.2.2 系统工程的特点	3
1.2.3 系统工程方法论	3
1.3 安全系统工程	7
1.3.1 基本概念	7
1.3.2 安全系统	10
1.3.3 安全系统工程及其研究对象	11
1.3.4 安全系统工程的研究内容	12
1.4 安全系统工程方法论基础	13
1.4.1 以霍耳方法论为代表的硬系统工程方法论	13
1.4.2 以切克兰德为代表的软系统方法论	14
1.4.3 物理—事理—人理系统方法论	14
1.4.4 从定性到定量的综合集成法	14
1.4.5 安全系统工程的学科基础	15
1.4.6 安全系统工程方法论结构体系	16
1.5 安全系统工程具体研究方法体系	18
1.5.1 常用的安全系统分析方法	18
1.5.2 常用的安全系统建模及模拟方法	19
1.5.3 常用的安全系统优化方法	19
1.5.4 常用的安全系统事故预测方法	20
1.5.5 常用的系统安全评价方法	21
1.5.6 常用的系统安全决策方法	22
1.6 安全系统工程的产生与发展	23
1.6.1 安全系统工程的产生	23
1.6.2 安全系统工程的发展	24

思考题	24
第 2 章 系统安全分析	25
2.1 系统安全分析概述	25
2.1.1 系统安全分析内容	25
2.1.2 系统安全分析方法	25
2.1.3 系统安全分析方法选择	26
2.2 安全检查表	27
2.2.1 基本原理	27
2.2.2 安全检查表分析方法	27
2.2.3 应用实例	30
2.3 预先危险性分析	30
2.3.1 基本原理	30
2.3.2 预先危险性分析方法	31
2.3.3 应用实例	33
2.4 危险和可操作性研究	35
2.4.1 危险和可操作性研究概述	35
2.4.2 危险和可操作性研究分析方法	35
2.4.3 应用实例	38
2.5 故障类型、影响和危险度分析	40
2.5.1 基本原理	40
2.5.2 故障类型和影响分析	40
2.5.3 故障类型、影响和危险度分析	45
2.5.4 应用实例	47
2.6 作业条件危险性分析	49
2.6.1 基本原理	49
2.6.2 作业条件危险性分析方法	49
2.6.3 应用实例	51
2.7 鱼刺图法	51
2.7.1 基本原理	51
2.7.2 分析方法	51
2.8 事件树分析	54
2.8.1 基本原理	54
2.8.2 分析步骤及应用范围	54
2.9 系统可靠性分析	56
2.9.1 基本概念	56
2.9.2 可靠度、维修度和有效度的常用度量指标	58
2.9.3 可靠度函数与故障率	58

2.9.4	人操作可靠度预测	62
2.9.5	系统可靠度计算	68
	思考题	71
第3章	事故树分析	72
3.1	基本原理	72
3.2	事故树分析方法	72
3.2.1	事故树基本结构	72
3.2.2	事故树常用符号及其意义	73
3.2.3	事故树分析程序	78
3.2.4	事故树编制	78
3.2.5	事故树数学表达	83
3.2.6	事故树简化	88
3.3	事故树定性分析	90
3.3.1	最小割集定义与求法	90
3.3.2	最小径集定义与求法	95
3.3.3	结构重要度分析	98
3.3.4	最小割集和最小径集在事故树分析中的作用	98
3.4	事故树定量分析	99
3.4.1	结构函数	99
3.4.2	基本事件的发生概率	103
3.4.3	顶上事件发生概率的计算	105
3.4.4	概率重要度分析	114
3.4.5	临界重要度分析	115
3.5	事故树分析特点	116
	思考题	116
第4章	系统安全评价	118
4.1	系统安全评价概述	118
4.1.1	系统安全评价的定义	118
4.1.2	系统安全评价的内容	118
4.1.3	系统安全评价的分类	119
4.2	系统安全评价的原理和原则	120
4.2.1	系统安全评价的原理	120
4.2.2	系统安全评价的原则	124
4.3	系统安全评价的程序和依据	126
4.3.1	系统安全评价的程序	126
4.3.2	评价单元划分的原则和方法	128

4.3.3	系统安全评价的依据	129
4.4	系统安全评价方法	132
4.4.1	系统安全评价方法分类	132
4.4.2	系统安全评价方法选择	135
4.5	生产设备安全评价	136
4.5.1	生产设备安全评价概述	136
4.5.2	生产设备安全评价原则要点	137
4.5.3	生产设备安全评价一般要点	137
4.5.4	生产设备可操纵性安全评价要点	138
4.5.5	生产设备运转可靠性安全评价要点	139
4.5.6	生产设备检查和维修安全评价要点	140
4.5.7	生产设备事故和职业危害预防评价要点	141
4.5.8	生产设备安全评价其他要点	142
4.6	安全生产管理评价	143
4.6.1	安全生产管理评价概述	143
4.6.2	安全生产责任制评价要点	143
4.6.3	安全生产管理组织保障评价要点	144
4.6.4	建设项目“三同时”评价要点	145
4.6.5	安全生产教育培训评价要点	147
	思考题	151
第5章	系统安全预测	152
5.1	系统安全预测概述	152
5.1.1	安全预测分类	152
5.1.2	安全预测的基本原理	152
5.1.3	安全预测方法	153
5.2	经验推断预测法	153
5.2.1	头脑风暴法	153
5.2.2	特尔斐预测法	155
5.2.3	应用实例	159
5.3	时间序列预测法	160
5.3.1	滑动平均法	161
5.3.2	指数滑动平均法	161
5.3.3	应用实例	162
5.4	计算模型预测法	163
5.4.1	回归分析法	163
5.4.2	马尔可夫链预测法	165
5.4.3	灰色预测法	165

5.4.4	应用实例	167
	思考题	170
第6章	系统安全决策	171
6.1	系统安全决策概述	171
6.1.1	决策过程	173
6.1.2	决策要素	174
6.1.3	安全决策	175
6.1.4	决策的科学性	176
6.2	定性属性量化	179
6.2.1	量化等级与范围	179
6.2.2	量化方法	179
6.2.3	属性函数 $F(X)$ 规范化	180
6.2.4	权重及其量化方法	180
6.3	系统安全决策分析	182
6.3.1	确定性多属性决策方法	182
6.3.2	评分法	184
6.3.3	决策树法	186
6.3.4	模糊决策法	187
6.4	决策的稳定性和决策风险	190
6.4.1	决策的稳定性	190
6.4.2	决策风险	192
第7章	安全系统工程典型应用实例	194
7.1	铁路行车事故预测	194
7.1.1	铁路行车事故概述	194
7.1.2	铁路行车事故预测	194
7.2	铁路专用线危险源辨识及评价	195
7.2.1	铁路专用线主要危险有害因素识别与分析	195
7.2.2	评价单元的划分和评价方法的选择	202
7.2.3	铁路专用线安全评价	203
7.2.4	安全对策措施及建议	212
7.2.5	安全评价结论	215
7.3	皮带运输机绞伤事故树分析	216
7.3.1	概述	216
7.3.2	事故树	216
7.3.3	事故树定性分析	216
7.3.4	事故树定量分析	218

7.3.5	结论	222
7.4	事故树案例分析	223
7.4.1	用事故树评估引起高校学生宿舍火灾原因风险	223
7.4.2	对偶成功树	225
7.4.3	结构重要度分析	226
7.4.4	求顶上事件发生的概率	226
7.4.5	求概率重要度系数	227
7.4.6	求关键重要度	228
	参考文献	231

第 1 章 安全系统工程概论

1.1 系统论概述

1.1.1 系统的内涵

从实际应用角度,钱学森把系统(System)定义为“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”。从工程和技术层次看,系统的本质特征是整体性和功能性,而整体性和功能性来源于诸多部分的相互作用、相互依赖。

美籍奥地利生物学家贝塔朗非(Ludwig Von Bertalanffy, 1910—1972)给出的系统定义是“处于相互作用中的要素的复合体”。把系统的组分追究到元素,在多元性和关联性之外不再施加进一步的限定,使这个定义可以普遍适用于不同领域和层次,因而属于基础科学层次的系统定义,称为一般系统理论。以贝氏理论为基础,系统的基本定义:

两个以上事物或对象相互关联而形成的统一体,叫做系统;因相互关联而被包含在系统中的那些事物或对象,叫做系统的组成部分,简称组分。

周围世界存在各种各样的系统,一列火车、一所学校、一座城市,都是系统。对生产系统而言,系统构成包括人员、物资、设备、资金、任务指标、信息六个要素。

1.1.2 系统的分类

按系统形式划分有自然系统与人造系统;按系统结构复杂程度划分有简单系统和复杂系统;此外还可划分为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等。

1.1.3 系统的特性

由系统的定义可以直接推知系统有如下基本特性:

(1) 多元性(Multiformity)或多组分性。一个系统至少要有两个组分,系统的常态是包含多个组分,有些系统具有成千上万甚至更多数目的组分,理论上存在包含无穷多个组分的系统,如整数系和实数系。相反,只有一个组分的事物,或者说不能划分为不同组分的事物,是非系统。必须强调,多组分性是系统的存在前提。

(2) 相关性(Correlation)或相干性。同一系统的不同组分之间必定相互关联。系统不存在孤立元(跟别的组分没有联系的组分)。如果一个集合或群体中至少有一个孤立元,那么它不是系统,而是非系统。没有多元性就没有相关性,多元性是造就系统的必要条件;相关性是造就系统的充分条件,相关性本身隐含着多元性(单一组分不存在),相关性在系统形成中具有决定性作用,通过相关性使系统组分有机联系在一起,发挥其特定功能。

(3) 统一性(Unitarity)或一体性。多元性加上相关性,造就了系统的一体性。诸多对象一旦相互关联而成为系统,它能够作为统一体而与他物彼此关联,与他物相互作用,因而被人们

当成一个事物去认识和对待；而诸多对象则转化为系统的组分，处于系统的内部。一体性要求意味着系统具有完全性、完备性，残缺不全者不是系统。

(4) 整体性(Integrity)。多元性是基础，相关性是主导，一体性是目标。三者综合集成，造就了系统的整体性。作为系统的事物，必定整体地存在，整体地运行，整体地延续，整体地跟其他事物发生关联，整体地演化，整体地消亡，等等，呈现出一系列整体特性。整体性包含了多元性、相关性和一体性，整体性是系统最重要的属性。贝塔朗非把系统科学界定为关于整体性的科学。

(5) 有序性(Orderliness)。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。

(6) 环境适应性(Environmental Adaptability)。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。

(7) 系统的整体涌现性(Entire Emergence Nature of System)。简单地强调系统科学是关于整体性的科学，可能引起误解。贝塔朗非指出存在两类整体和整体性。一类是加和性整体，整体是各个孤立元素的总和。元素的加和性特征意味着，不论它处于整体之内还是之外，这些特征都是一样的，只要知道了元素在孤立状态中的特征，并汇集起来，即可获得整体的特征。另一类是组合性整体，或非加和性整体。所谓组合性特征，就元素而言，指同一元素处于整体内部和处于整体外部时，是不一样的；就整体而言，组合性整体特征指依赖于组分之间特定关系的那些特征。欲理解整体的组合性特征，不仅要知道各组分，而且要知道组分之间的关系。如化合物的特征不是其组成元素的特征的加和，而是不同物质元素经过化学反应(一种特殊的相互作用)而产生的特征。只有这种组合性整体，才能称为系统。

应当指出，任何系统都具有加和式整体性。例如，一架飞机的总质量是各部件质量的加和，等等。总之，凡只涉及质量或能量之类的特性，由于物质不灭和能量守恒，整体必定等于组分之和。对于这类加和性整体，自然科学已经做出了透彻研究。

组合性或非加和性的说法不够深刻，更科学的称谓是涌现性。系统整体具有而它的元素或组分及其总和却不具有的特征，称为系统的整体涌现性。或者说，诸多组分一旦按照某种方式整合为系统就会呈现出来，一经分解为独立的组分便不复存在的特征，就是整体涌现性。贝塔朗非曾借用亚里士多德的命题“整体大于部分之和”来直观地表述这种整体涌现性，并获得广泛认可。从字面看，这是一个被量化的命题，容易引导人们把整体涌现性局限于系统的定量属性。整体涌现性固然有定量的内涵，但它首先是指系统的定性特征，整体具有组分之和没有的新质，即新的定性特征。几种化学原料成分经过化学反应而产生的化合物，具有与原料完全不同的化学性质。一堆自行车零件无法派上用场，一经组装为自行车，就是一个交通工具。这些都是系统产生的整体涌现性，有时也称为系统新质或系统质。又如，相同可靠性的 N 个元件合成整体，其整体的可靠性可以千变万化，这是由于受系统的效应所影响。

系统科学第一次指明系统的整体涌现性归根结底源于四种效应:组分效应、规模效应、结构效应、环境效应。综合而言,整体涌现性是一种系统效应。安全系统发生事故也可以表述为系统的一种涌现性。因此,有关系统涌现性的发生机理、调节和控制方法等也可以运用于安全系统。

1.2 系统工程概述

20世纪以来,一方面是科学技术获得极大发展,另一方面是生产流程和经营管理的巨型化、复杂化,导致工程活动也呈巨型化和复杂化趋势。因此,如何应用科学技术于工程活动的组织管理,成为时代的迫切需要。

1.2.1 系统工程的内涵

工程的灵魂是它所使用的技术,技术的高低优劣决定工程的优劣。技术=工具+设备+程序+方法,工具和设备属于硬技术,不同类型的工程拥有不同的硬技术,不属于系统科学的研究范畴;工程组织管理的程序和方法属于软技术,既然工程都是作为过程系统而存在和展开的,适用于工程的方法和程序就应当符合系统的思想和原理,必须讲究整体性、相关性、有序性、环境适应性等。作为工程实践活动,还讲究可靠性、平稳性、时效性、安全性等,这就是为什么在“工程”一词前面加上“系统”修饰词的缘故。

系统工程是以系统为研究对象,以达到系统整体最佳效果为目标,对系统的规划、设计、制造、试验和使用等各个阶段进行有效的组织、管理。它是一门融合最新科学成就和知识的综合性科学技术。

切忌把系统工程跟土木工程、冶金工程、建筑工程、航天工程等并列起来,以为系统工程不过是在这些已有工程之外的另一类新的工程。系统工程其实不是工程实践,而是做好工程实践必须应用的方法、程序和技术,是一种知识体系。简言之,系统工程是组织管理的技术。

1.2.2 系统工程的特点

根据系统的概念,其特点可以概括为以下几点:

- (1) 系统工程是一种知识体系,不是工程实践。
- (2) 系统工程是工程技术,不是科学理论,讲究的是实际功效。
- (3) 系统工程是普遍适用的方法,一切工程都适用。

(4) 系统工程的精华是系统的观点,强调从总体着眼构思,从局部着手实现,从全局出发用好局部,从全过程出发关照好各个阶段。

1.2.3 系统工程方法论

1. 霍耳三维结构

如何把系统的思想贯穿于工程项目的组织管理之中,使工程活动具有足够的科学性、可行性、经济性、实效性,美国系统工程专家霍耳(A·D·Hall)于1969年提出的一种系统工程方法论——霍耳三维结构(Hall Three Dimensions Structure, HTDS)模式,提供了最具说服力的框架和思路。

霍耳三维结构,又称霍耳系统工程(Hall System Engineering),与软系统方法论对比,称为硬系统方法论(Hard System Methodology, HSM)。霍耳三维结构模式的出现,为解决大型复杂系统的规划、组织、管理问题提供了一种统一的思想方法,因而在世界各国得到了广泛应用。霍耳三维结构是将系统工程整个活动过程分为前后紧密衔接的七个阶段和七个步骤,同时还考虑了为完成这些阶段和步骤所需要的各种专业知识和技能。这样,就形成了由时间维、逻辑维和知识维所组成的三维空间结构,如图 1-1 所示。

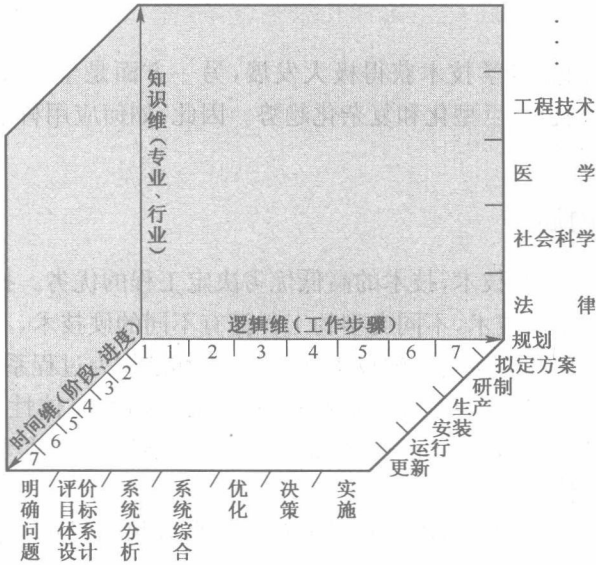


图 1-1 霍耳三维结构图

图 1-1 中,时间维表示系统工程活动从开始到结束按时间顺序排列的全过程,分为规划、拟定方案、研制、生产、安装、运行、更新七个时间阶段;逻辑维是指时间维的每一个阶段内所要进行的工作内容和应该遵循的思维程序,包括明确问题、评价目标体系设计、系统分析、系统综合、优化、决策、实施七个逻辑步骤;知识维列举需要运用包括工程技术、医学、建筑、商业、法律、管理、社会科学、艺术等各种知识和技能。三维结构体系形象地描述了系统工程研究框架,对其中任一阶段和每一个步骤,又可进一步展开,形成多层次树状体系。

2. 霍耳三维结构分析

1) 逻辑维(解决问题的逻辑过程)

运用系统工程方法解决某一大型工程项目时,一般可分为七个步骤:

(1) 明确问题。由于系统工程研究的对象复杂,包含自然界和社会经济各个方面,而且研究对象本身的问题有时尚不清楚,如果是半结构性或非结构性问题,也难以用结构模型定量表示。因此,系统开发的最初阶段首先要明确问题的性质,特别是在问题的形成和规划阶段,搞清楚要研究的是什么性质的问题,以便正确地设定问题,否则,以后的许多工作将会劳而无功,造成很大浪费。国内外学者在问题的设定方面提出了许多行之有效的办法,主要有:

① 直观的经验方法。这类方法中,比较知名的有头脑风暴法(Brain Storming),又称 5W1H 法,日本人将这类方法叫做创造工程法。这一方法的特点是总结人们的经验,集思广益,通过分散讨论和集中归纳,整理出系统所要解决的问题。

② 预测法。系统要分析的问题常常与技术发展趋势和外部环境的变化有关,其中有许多

未知因素,这些因素可用打分的办法或主观概率法来处理。预测法主要有特尔斐法、情景分析法、交叉影响法、时间序列法等。

③ 结构模型法。复杂问题可用分解的方法,形成若干相关联的相对简单的子问题,然后用网络图方法将问题直观地表示出来。常用的方法有解释结构模型法(ISM法)、决策实验室法(DEMATEL法)、图论法等。其中,用图论中的关联树来分析目标体系和结构,可以很好地比较各种替代方案,在问题形成、方案选择和评价中是很有用的。

④ 多变量统计分析法。用统计理论方法所得到的多变量模型一般是非物理模型,对象也常是非结构的或半结构的。统计分析法中比较常用的有因子分析(Factor Analysis)法、主成分分析(Principal Components Analysis)法等。此外,还有利用行为科学、社会学、一般系统理论和模糊理论来分析,或几种方法结合起来分析,使问题明确化。

(2) 建立价值体系或评价体系。评价体系要回答以下一些问题:评价指标如何定量化,评价中的主观成分和客观成分如何分离,如何综合评价,如何确定价值观问题等。行之有效的价值体系方法有以下几种:

① 效用理论。该理论是从公理出发建立的价值理论体系,反映了人的偏好,建立了效用理论和效用函数,并发展为多属性和多隶属度效用函数(Utility Function)。

② 费用/效益分析法。多用于经济系统评价,如投资效果评价、项目可行性研究等。

③ 风险估计(Risk Evaluation)。在系统评价中,风险和安全性评价是一个重要内容,决策人对风险的态度也反映在效用函数上。在多个目标之间有冲突时,人们也常根据风险估计来进行折中评价。

④ 价值工程。价值是人们对事物优劣观念准则和评价准则的总和。例如,要解决的问题是否值得去做,解决问题的过程是否适当,结果是否令人满意等。以生产为例,产品价值主要体现在产品的功能和质量上,降低投入成本和增加产出是两项相关的准则。价值工程是个总体概念,具体体现在设计、制造和销售各个环节的合理性上。

(3) 系统分析。不论是工程技术问题还是社会环境问题,系统分析首先要对所研究的对象进行描述,建模的方法和仿真技术是常采用的方法,对难以用数学模型表达的社会系统和生物系统等,也常用定性和定量相结合的方法来描述。系统分析的主要内容涉及以下几方面:

① 系统变量的选择。用于描述系统主要状态及其演变过程的是一组状态变量和决策变量,因此,系统分析首先要选择出能反映问题本质的变量,并区分内生变量(Endogenous Variable)和外生变量(Exogenous Variable),用灵敏度分析法可区别各个变量对系统命题的影响程度,并对变量进行筛选。

② 建模和仿真。在状态变量选定后,要根据客观事物的具体特点确定变量间的相互依存和制约关系,即构造状态平衡方程式,得出描述系统特征的数学模型。在系统内部结构不清楚的情况下,可用输入输出的统计数据得出关系式,构造出系统模型。系统对象抽象成模型后,就可进行仿真,找出更普遍、更集中和更深刻反映系统本质的特征和演变趋势。现已有若干实用的大系统仿真软件,如用于随机服务系统的 GPSS 软件,用于复杂社会经济系统仿真的系统动力学(System Dynamics, SD)软件等。

③ 可靠性工程。系统可靠性工程是研究系统中元素的可靠性和由多个元素组成的系统整体可靠性之间的关系。一般讲,可靠的元件是组成可靠系统的基础,然而,局部的可靠性和整体可靠性间并非简单的对应关系,系统工程强调从整体上来看问题。在 20 世纪 40 年代,冯·诺依曼(Von Neumann)开始研究用重复的不那么可靠的元件组成高度可靠系统的问题,并进行

了可靠性理论探讨。钱学森教授也提出,现在大规模集成电路的发展使元器件的成本大大降低,如何用可靠性较低的元器件组成可靠性高的系统,是个很有现实意义的问题。近年来,已采用的可靠性和安全性评价方法有事故树(FTA)或事件树(ETA)等树状图形方法。

(4) 系统综合。系统综合是在给定条件下,找出达到预期目标的手段或系统结构。一般来讲,按给定目标设计和规划的系统,在具体实施时,总与原来的设想有些差异,需要通过对问题本质的深入理解,做出具体解决问题的替代方案,或通过典型实例的研究,构想出系统结构和简单易行的能实现目标要求的实施方案。系统综合的过程常常需要有人参与,计算机辅助设计(CAD)和系统仿真可用于系统综合,通过人机的交互作用,以及人的经验知识,使系统具有推理和联想的功能。近年来,知识工程和模糊理论已成为系统综合的有力工具。

(5) 系统方案的优化选择。在系统的数学模型和目标函数已经建立的情况下,可用最优化方法(Optimization Method)选择使目标值最优的控制变量值或系统参数。所谓优化,就是在约束条件规定的可行域内,从多种可行方案或替代方案中得出最优解或满意解。实践中要根据问题的特点选用适当的最优化方法,目前应用最广的仍是线性规划(Linear Programming)和动态规划(Dynamic Programming),非线性规划(Nonlinear Programming)的研究很多,但实用性尚有待改进,大系统优化已开发了分解协调的算法。组合优化适用于离散变量(Discrete Variable),整数规划中的分枝定界法(Branch and Bound Method)、逐次逼近法等的应用也很广泛。多目标优化问题的最优解处于目标空间的非劣解集上,可采用人机交互的方法处理所得的解,最终得到满意解。当然,多目标问题也可用加权的方法转换成单目标来求解,或按目标的重要性排序,逐次求解,例如目标规划法(Goal Programming Method)。

(6) 决策。决策就是管理,决策就是决定,人类的决策管理活动面临着被决策系统的日益庞大和日益复杂。决策又有个人决策和团体决策(Group Decision)、定性决策和定量决策、单目标决策(Single-objective Decision)和多目标决策(Multi-objective Decision)之分。在系统分析和系统综合的基础上,人们可根据主观偏好、主观效用和主观概率做决策。决策的本质反映了人的主观认识能力,因此,就必然受到人的主观认识能力的限制。

近年来,决策支持系统(Decision Support System, DSS)受到人们的重视,系统分析者将各种数据、条件、模型和算法放在 DSS 中,该系统甚至包含了有推理演绎功能的知识库,使决策者在做出主观决策后,力图从决策支持系统中尽快得到效果反映,以求得到主观判断和客观效果的一致。DSS 在一定条件下起到决策的科学化和合理化作用。但是,在真实的决策中,被决策对象往往包含许多不确定因素和难以描述的现象,如社会环境和人的行为不可能都抽象成数学模型,即使是专家系统(Expert System, ES),也不可能将逻辑推演、综合和论证过程做到像人的大脑那样,有创造性思维,也无法判断许多随机因素。群决策有利于克服某些个人决策中主观判断的失误,但群决策的过程较长。为了实现高效率的群决策,在理论方法和应用软件开发方面,研究人员做了大量工作。如多人多目标决策理论、主从决策理论、协商谈判系统、冲突分析(Conflict Analysis, CA)等,有些应用软件已实用化。

(7) 制定计划。有了决策就要付诸实施,实施就要依靠严格的有效的计划。以工厂为例,为实现工厂的生产任务和发展战略目标,就要制定当年的生产计划和未来的发展规划。厂内还要按厂级、车间级和班组级分别制定实施计划。一项大的开发项目,涉及设计、开发、研究和施工等许多环节,每个环节又涉及组织大量的人、财、物。在系统工程中常用的计划评审技术(Program Evaluation and Review Technique, PERT)和关键路线法(Critical Path Method, CPM)在制定和实施计划方面起了重要的作用。