

高等教育“十二五”规划教材
新编安全工程专业系列教材

安全系统工程 (双语)

Safety System Engineering

主 编 / 邓奇根 高建良 刘明举

主 审 / 景国勋



中国矿业大学出版社

China University of Mining and Technology Press

高等教育“十二五”规划教材
新编安全工程专业系列教材

安全系统工程

(双语)

主 编 邓奇根 高建良 刘明举
副主编 牛国庆 王 燕 冉玉体
主 审 景国勋

中国矿业大学出版社

内 容 提 要

本书 2011 年列入中国煤炭教育协会高等教育“十二五”教材规划,是《新编安全工程专业系列教材》之一。全书以安全学、系统工程学为基础,贯穿系统工程的思想,系统地介绍了安全系统的概念、系统安全分析方法、事故树分析方法、系统安全预测、系统安全评价、系统危险控制等方面的内容。

本书可作为高等院校安全工程专业及其相关专业的教材,同时可供从事安全工程的技术人员或管理人员参考使用,还可作为注册安全工程师考试参考用书。

图书在版编目(CIP)数据

安全系统工程;双语:中文、英文/邓奇根,高建良,刘明举主编. —徐州:中国矿业大学出版社, 2011.8

新编安全工程专业系列教材

ISBN 978 - 7 - 5646 - 1049 - 4

I. ①安… II. ①邓… ②高… ③刘… III. ①安全工程: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(2011)第 081545 号

书 名 安全系统工程(双语)

主 编 邓奇根 高建良 刘明举

责任编辑 陈红梅

出版发行 中国矿业大学出版社有限责任公司

(江苏省徐州市解放南路 邮编 221008)

营销热线 (0516)83885307 83884995

出版服务 (0516)83885767 83884920

网 址 <http://www.cumtp.com> E-mail: cumtpvip@cumtp.com

印 刷 徐州中矿大印发科技有限公司

开 本 787×1092 1/16 印张 15 字数 387 千字

版次印次 2011 年 8 月第 1 版 2011 年 8 月第 1 次印刷

定 价 28.00 元

(图书出现印装质量问题,本社负责调换)

《新编安全工程专业系列教材》 编审委员会

顾问 周世宁

主任 袁 亮

副主任 景国勋 蒋军成 刘泽功

李树刚 程卫民 林柏泉

执行副主任 王新泉 杨胜强

委员 (按姓氏拼音为序)

柴建设 陈开岩 陈网桦 贾进章 蒋承林

蒋曙光 廖可兵 刘 剑 刘章现 吕 品

罗 云 马尚权 门玉明 孟燕华 倪文耀

宁掌玄 撒占友 沈斐敏 孙建华 孙金华

谭世语 唐敏康 田水承 王佰顺 王宏图

王洪德 王 凯 王秋衡 吴 强 解立峰

辛 嵩 徐凯宏 徐龙君 许满贵 叶建农

叶经方 易 俊 易赛莉 余明高 张德琦

张国华 张敬东 张巨伟 周 延 朱 锴

秘书长 马跃龙 陈红梅

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、保证经济建设持续发展的基本条件。随着我国社会经济的发展,生产生活各个领域的安全问题日益显现出来,安全问题已经成为我国构建和谐社会的主要障碍之一。

安全科学则为生产生活的持续健康发展提供了必要的保障。安全系统工程也可以看做系统工程的一个重要分支,“安全系统工程”是安全工程专业的核心课程之一,也是相近专业学生学习和了解安全工程知识的主要课程,最能体现安全学科的综合属性。

双语教学是我国高等教育与国际接轨、教育改革的必然趋势,也是我国当前教学改革的重点及热点。为了适应社会发展的需求,双语教学近年来逐渐进入了课堂,是培养国际化人才最有效的途径。目前国内诸多高校正在陆续开设“安全系统工程”的双语课程,如何在着重于人才的全面素质培养上下功夫,既能在知识传授方面深入浅出地介绍本学科领域的知识,又能在语言环境上营造出一个氛围,使学生能够较为轻松地学习,本教材希望在此方面做一些探索。

全书共分6章,各章节编写分工如下:第1章由河南理工大学高建良、牛国庆编写;第2章由河南理工大学高建良、王燕共同编写;第3章由河南理工大学邓奇根编写;第4章由河南理工大学王燕、刘彦伟编写;第5章由河南理工大学牛国庆、冉玉体共同编写;第6章由河南理工大学刘明举、赵发军共同编写;附件Ⅰ、附件Ⅲ由河南理工大学冉玉体编写;附件Ⅱ由河南理工大学刘彦伟编写。全书由河南理工大学邓奇根、高建良和刘明举任主编,并由邓奇根负责全书的统稿工作,河南理工大学景国勋教授担任本书主审。全书力图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。

全书力求内容丰富、语言简洁、层次清晰、通俗易懂,突出内容的基础性,注重理论联系实际,强调实用性和可操作性。

本书在编写和出版的过程中,山东科技大学曹庆贵教授提供了大量的第一手资料,给予了全过程的指导和帮助;南京师范大学研究生徐宁对本书的编写给予了无私的帮助,在此一并表示衷心的感谢和崇高的敬意!本书在编写过程中参阅了大量的文献,在此对文献的作者表示最诚挚的谢意!

双语教材编写对编者还是一个挑战,书中还有诸多地方值得探讨和研究。由于编者水平有限,书中疏漏和错误在所难免,恳请广大读者批评指正并提出宝贵意见。

编 者

2011年6月

目 录

1 绪论/1 INTRODUCTION	1
1.1 安全系统工程基础/Basics of Safety System Engineering	2/3
1.2 安全系统工程的研究对象、内容及方法/Research Objects, Contents and Methods of SSE	4/5
1.3 安全系统工程的产生与发展/Origin and Development of SSE	8/11
1.4 安全系统工程的应用特点/Application Characteristics of SSE	10/14
复习思考题	12
2 系统安全分析/2 SYSTEM SAFETY ANALYSIS	17
2.1 概述/Overview	18/19
2.2 安全检查表/Safety Checklist	20/23
2.3 预先危险性分析/Preliminary Hazard Analysis	28/31
2.4 危险性和可操作性研究/Hazard and Operability Analysis	32/37
2.5 故障类型和影响分析/Failure Mode and Effects Analysis	38/45
2.6 事件树分析/Event Tree Analysis	46/55
2.7 统计图表分析法/Statistics Chart Analysis	50/59
复习思考题	64
3 事故树分析/3 FAULT TREE ANALYSIS	71
3.1 事故树分析概述/Introduction to FTA	72/73
3.2 事故树的定性分析/Qualitative Analysis of FT	78/81
3.3 事故树的定量分析/Quantitative Analysis of FTA	90/95
3.4 基本事件的重要度分析/Importance Analysis of Basic Event	98/105
3.5 事故树分析的应用/Application of FTA	102/109
复习思考题	108
4 系统安全预测/4 SYSTEM SAFETY PREDICTION	113

4.1 预测的种类、原则及程序/Types, Principles and Procedures of Prediction	114/115
4.2 预测方法/Prediction Methods	118/121
复习思考题.....	130
5 系统安全评价/5 SYSTEM SAFETY ASSESSMENT	133
5.1 安全评价概述/Introduction to Safety Assessment	134/135
5.2 道化学火灾、爆炸指数评价法/Dow's Fire & Explosion Index Method	136/139
5.3 系统安全综合评价/Comprehensive Assessment of System Safety	148/151
5.4 系统安全评价的技术文件/Technical Documents of Safety Assessment	160/165
5.5 安全评价结论/Compilations of SSA	172/178
复习思考题.....	176
6 系统危险控制/6 SYSTEM RISK CONTROL	183
6.1 危险控制的基本原则/Basic Principles of Risk Control	184/185
6.2 安全决策/Safety Decision	186/187
6.3 人为失误控制措施/Control Measures of Human Error	198/203
6.4 固有危险控制技术/Control Techniques of Inherent Hazards	202/209
复习思考题.....	206
附录.....	211
附录 I	211
附录 II	216
附录 III	226
参考文献.....	229

1 绪 论

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,以期望实现系统及其全过程安全目标的科学技术。

安全系统工程是随着生产的发展而发展起来的。它是现代科技发展的必然产物,也是安全科学学科的重要分支。

1 INTRODUCTION

Safety System Engineering(SSE) is defined as the combination of tasks and activities of system safety management and SSE enhances operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of system life cycle.

SSE develops as industry develops. It is the product of modern science and technology and also becomes an important branch of safety science.

1.1 安全系统工程基础

1.1.1 系统

系统工程的研究对象是系统,它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。系统具有以下4个特性:

1) 整体性

系统是由2个或2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)形成一个统一的整体就具备了新的特定功能,系统作为一个整体才能发挥其应有功能。

2) 相关性

系统内各要素之间是相互联系、相互依赖、相互作用的特殊关系,通过这些关系把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。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) 环境适应性

任何一个系统都处于一定的物质环境之中,系统必须适应外部环境条件的变化。在研究系统时,必须重视环境对系统的影响。

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科学技术。

系统工程是组织管理系统的规划、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。

1.1.3 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。对于这个定义,可以从以下几个方面理解:

(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是将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。

1.1 Basics of Safety System Engineering

1.1.1 System

System is the study object of system engineering, which is a combination of people, procedures, facility, and/or equipment all functioning within a given or specified working environment to accomplish a specific task or set of tasks. A system embodies four characteristics:

1) Integrity

A system is a complete whole composed by two distinct elements (components or subsystems). Different elements form an unified whole which is equipped with certain new functions through synthesizing and unifying instead of random assembling although the elements have different functions. Only when new functions appear, may a system perform functions properly and effectively.

2) Relativity

Elements in a system are interactive and independent, through which the system is linked effectively and may perform its functions.

3) Purposefulness

Any system aims at certain tasks or goals. In order to fulfill certain aims of a system, prescribed functions must be embodied so as to offer the system optimal planning, designing, controlling, and managing and so on in system life cycle, i. e. the phases of planning, designing, experimenting, manufacturing and applying.

4) Environment adaptability

Any system is in a certain physical environment, so it must adapt to the changes of the environmental conditions. The effects of environments on the system must be taken into consideration in system research.

1.1.2 System Engineering

As a new science in 1950s, system engineering studies system, applying modern science and technology with the aim of system optimization.

System engineering is a scientific methodology of planning, designing, manufacturing, experimenting and applying in organization and management systems, it is applicable to any systems.

1.1.3 SSE

SSE, based on basic theories and methodologies of system engineering, pre-identifies and analyzes hazardous elements existing in system, assesses and controls them to ensure the expected system safety. To be more specific:

(1) The theoretical basis of SSE is the science of safety and system. It is a system engineering of industrial and mining enterprises with field of occupational safety and health.

1.2 安全系统工程的研究对象、内容及方法

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以下3个部分: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,每一个部分就是该系统的一个子系统,分别称为人子系统、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,不仅把人当做“生物人”、“经纪人”,更要看做“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;不仅把人子系统看做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、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。

3个子系统相互影响、相互作用的结果就是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,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、系统安全预测、系统安全评价和系统风险控制。

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

(2) The purpose of SSE is pursuing the safety of the whole process of the system as well as its whole process.

(3) The key point of SSE is the identification, analysis and assessment of system hazardous elements, system safety decision and accident control.

(4) The expected safety target of SSE is to control system risks to an acceptable level. That is to say, to control accidents economically and effectively and keep system risks under safety index.

1.2 Research Objects, Contents and Methods of SSE

1.2.1 *Research Objects of SSE*

As a scientific approach, SSE has its own research objects. Any manufacturing system is composed of three factors: first, operating and managing personnel who are engaged in manufacturing activities; second, physical conditions which are necessary to manufacturing such as machines and factory buildings; third, environment in which manufacturing takes place. The above three factors comprise “man-machine-environment system”; each factor is one subsystem of the whole system and they are called man subsystem, machine subsystem, and environment subsystem, respectively.

1) **Man subsystem**

Whether the man subsystem is safety or not involves the problems as the following, physiological and psychological factors of human, the properly whether the prescriptions, regulation criteria and managing methods etc. suit human or not and whether it's likely to be accepted by human. During the study, man should be regarded not merely as one in nature or in a company, but as one in a society. Problems must be analyzed and solved from the perspective of sociology, anthropology, psychology and behavior science. In man subsystem, man should not only be looked on as an eternal composing part, but also as a kind of creature of self-respect and self-love, with feelings, thoughts and subjective initiatives.

2) **Machine subsystem**

For this subsystem, the safety of the workpiece shape, size, material, intensity, technology and reliability of equipments should be taken into account. Meanwhile, requirements of meters and operating pieces on man, and requirements of meters and operating pieces from the perspective of anthropometry, physiology, relevant parameters of psychology and physiology process designing should not be ignored.

3) **Environment subsystem**

For this subsystem, physicochemical and social factors need to be considered. physicochemical factors include noise, vibration, dust, poisonous gases, cosmic ray, sunlight, temperature, humidity, pressure, heat, chemical hazardous substance and so on. Social factors are composed of management system, time quota, personnel organization and interpersonal relationship etc. .

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。这是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。

2) 系统安全预测

预测是研究未来的一门学科。随着科学技术的进步和生产水平的日益提高,人类的预测活动越来越频繁,涉及的领域越来越广阔,预测方法和手段越来越科学和先进,广泛应用于经济、技术和社会发展的各个领域。预测技术和控制手段的有效结合,是现代安全技术的基本发展方向。

3) 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,通过分析来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。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。

4) 系统风险控制

任何一项系统安全预测技术、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,也不能发挥其应有的作用。因此,在出现系统安全预测技术、系统安全分析和系统安全评价技术的同时,也出现了系统风险控制。其最大的特点是从系统的整体性、相关性和有序性出发,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。

1.2.3 安全系统工程的研究方法

安全系统工程的研究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以下5个方面:

1) 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。

2) 本质安全方法

这是安全技术追求的目标,也是研究安全系统工程方法的核心。由于安全系统把安全问题中的人—机(物)—环境统一为一个“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。

3) 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

The three subsystems interact and interplay, which make the safety of overall system in a certain state. For example, physicochemical factors affect the life cycle and precision of machines or even damage machines; noise, vibration, temperature, dust, and poisonous gases of machine subsystem affect man and environment subsystems; the states of human's psychology and physiology are usually subjective factors of mal-operation; social factors in environment subsystem will affect human's psychology and bring potential hazards to safety. That is to say, the above three subsystems, which interact, restrict and influence each other form an organic whole of "man-machine-environment". Only starting from the relations in and between these subsystems, can safety problems be really solved in analyzing, assessing and controlling the safety of "man-machine-environment system". The object of SSE is "man-machine-environment system".

1.2.2 Research Contents of SSE

SSE is a scientific approach (technique) which studies how to utilize theories and methodologies of system engineering to ensure system safety. The main technological methodologies are system safety analysis, system safety prediction, system safety assessment and system risk control.

1) System safety analysis

In order to increase system safety and reduce or exterminate accidents, the prerequisite is to identify the hazardous elements in advance, then to master their characteristics thoroughly and to understand clearly the degree of their effects on system safety. Only in this way, can the main potential hazards be found out and effective protection measures be taken to improve system safety. "preliminary" means that, no matter which stage the system is in its life cycle, safety analysis must be carried out, hazardous factors be identified and mastered before the operation of certain stage. This is what needs to be solved in system safety analysis.

System safety analysis is a kind of technical approach which employs theories and methodologies of system engineering to identifies, analyzes existed hazards in a system and makes qualitative and quantitative descriptions with reference to practical needs. According to relevant references, there are many forms and methods on system safety analysis and cautions in operation as well.

(1) Based on the system characteristics, the requirements and aims of analysis, employ different analysis methods in that no method is applicable to any cases because of its characters and limitations. Several methods need to be used simultaneously to make up for limitations of each other or make comparisons; hence, results of analysis can be verified.

(2) The methods should not be utilized mechanically, they need to be reformed or simplified when necessary.

(3) Never be restricted to the application of the methods, but explore new ways and methods based on system theories instead. Meanwhile, the former effective methods also need to be improved to form systematic safety analysis methods.

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,考虑人一机匹配以及采用人一机匹配的理论和方法是安全系统工程方法的重要支撑点。

4) 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,还要有指标(目标)的多元化的表示方法和测算方法。

5) 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。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。

1.3 安全系统工程的产生与发展

1.3.1 安全系统工程的产生

安全系统工程产生于20世纪60年代初期的美、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一年半的时间就连续发生4起重大事故,造成惨重损失,从而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”,制定了《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,将该标准提升为美军标准;之后又经2次修订,成为现在的《系统安全程序要求》(MIL-STD-882B)。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。

20世纪60年代中期英国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《核电站风险报告》(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。

美国道化学公司于1964年发表了化工厂《火灾、爆炸危险指数评价法》,俗称为道氏法。该法经过多年的实用,修改了6次,出版了第七版。该评价法是以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。20世纪70年代日本劳动省发表的评价方法,另辟蹊径,它就是以分析与评价、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》,亦称为《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

2) System safety prediction

Prediction is a science of studying future. With the development of science and technology, and the development of production, human's prediction activities are more and more frequent, prediction fields broader, prediction methods and techniques more advanced. It is widely applied to many fields, such as economy, technology and social development. The effective combination between prediction techniques and controlling methods is the main stream of modern safety technology.

3) System safety assessment

System safety assessment, based on system safety analysis, identify the hazardous elements in the system. However, that does not mean that measures must be taken to all the hazardous elements. Instead, it needs to have a good grasp of the accident risks through system safety assessment and then compare them with relevant system safety index. If the accidents risks are above the index, measures need to be taken to control the hazards with the aim of keeping them below the index.

4) System risk control

Any system safety techniques of prediction, analysis or assessment will not be able to take effect as expected if there are no effective management skills and methods. Therefore, system risk control develops with system safety techniques of prediction, analysis and assessment. Its key characteristics is to carry out safety management on system in full scale during its whole process based on the integration, relevance and orderliness of system, so as to control system safety.

1.2.3 Research Methods of SSE

Based on the theory of safety science, a research method of SSE develops and matures on the basis of former research methods. Generally speaking, there are five methods:

1) From the integrality of a system

Research methods of SSE must start from the integrality of the system, on which the methods process and target of solving safety problems are considered. For example, safety requirements on each subsystem must be consistent with that of the whole system and other functions. In the process of system research, contradictions between subsystems and the system or between subsystems themselves must make use of system optimization to find solutions which are acceptable to each part. Meanwhile, system optimization should be utilized through all the phases of system planning, designing, developing and applying.

2) Essential safety approach

Essential safety approach is the aim of safety technology, and it is also the kernel of SSE approaches. Due to the consideration of man-machine-environment in safety as one "system", the kernel aim is essential safety, which is the methods and techniques of system essential safety regardless of studying from system contents or objectives.

3) The match of man and machine

The match of man and machine is a crucial factor among that affecting system safety. The man-machine match which studies safety in industry is safety man and machine engineering; while

法、如何进行评价等。

民用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、冶金等行业开发了许多系统安全分析方法和评价方法。

1.3.2 安全系统工程的发展

当前,安全系统工程已普遍引起了各国的重视,安全系统工程得到了快速的发展。在我国,安全系统工程的研究、开发是从 20 世纪 90 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示范作用。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。到了 20 世纪 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,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工程范畴。

1.4 安全系统工程的应用特点

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体现了系统性的特点,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等级。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。所以,安全系统工程也可称为是系统的事事故预测技术。

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