中国劳动关系学院精品课系列教材

安全系统工程

许素睿 编著

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

中国劳动关系学院精品课系列教材

安全系统工程

许素睿 编著

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书内容包括绪论、安全检查表、预先危险性分析、故障类型和影响分析、危险和可操作分析、事件树、事故树、安全评价、安全预测、安全决策等共十二章。

本书的特色及创新主要体现在以下几个方面：一是学科知识体系完整，内容涵盖系统安全分析、系统安全评价、系统危险控制、安全预测和安全决策，每种系统安全分析方法自成一章；二是强化理论联系实际，例题均结合工业实际，且每章末尾也有一定数量的练习题；三是应用型习题提供答案解析，便于学生自学。

本书可作为安全工程及相关专业本科教材，也可供安全、防灾等方面研究人员学习参考，同时可作为生产经营单位安全管理及技术人员的教育培训教材。

图书在版编目(CIP)数据

安全系统工程 / 许素睿编著. —上海：上海交通大学出版社，2015

ISBN 978-7-313-13805-7

Ⅰ.①安… Ⅱ.①许… 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(2015)第 229584 号

安全系统工程

编　　著：许素睿

出版发行：上海交通大学出版社　　地　　址：上海市番禺路 951 号

邮政编码：200030　　电　　话：021-64071208

出 版 人：韩建民

印　　刷：昆山市亭林印刷有限责任公司　　经　　销：全国新华书店

开　　本：787mm×960mm　1/16　　印　　张：15.25

字　　数：284 千字

版　　次：2015 年 10 月第 1 版　　印　　次：2015 年 10 月第 1 次印刷

书　　号：ISBN 978-7-313-13805-7/X

定　　价：42.00 元

前　言

根据安全工程本科专业的要求和规定，安全系统工程是安全工程专业的专业基础课程，是本专业的主干学科，在安全工程本科学科建设中起着重要作用。在继续深造方面，该课程被很多高校和科研院所列为安全工程专业攻读硕士和博士学位入学考试的专业课考试课程。在资格考试方面，安全系统工程是目前我国注册安全评价师考试的主要课程，还是我国注册安全工程师考试的基础课程。在职业生涯中，安全系统工程是安全工程专业学生从事安全管理和安全技术工作所必备的基本功，在中国劳动关系学院组织的第三方课程反馈中本课程被已毕业的学生公认为100%需要。在生产实践中，安全系统工程为改善我国安全工作的面貌作出了重要贡献。据此，作者结合近十年的一线课堂教学经验，编写了这本《安全系统工程》教材，并获得中国劳动关系学院“十二五”规划教材立项。

本书作为高校安全工程专业的本科教材，在参考同类教材的基础上，又有其特色及其创新性，主要表现在：一是学科知识体系完整、重点突出。该教材系统地介绍了系统安全分析、系统安全评价、系统危险控制、安全预测和安全决策的主要内容。章节安排上每种系统安全分析方法自成一章，原理方法阐述详细，注重学生对各种系统安全分析方法的理解，与硕士研究生入学考试的理论要求深度相匹配，应用部分用较多实例加以说明。二是强化理论联系实际、学以致用。课程本身对实践性要求非常强且应用范围广泛，应用例题的选择有工业工程也有学生身边的问题；还会选择相同例题用不同的方法进行分析，相同系统不同方法分析能更好地理解各种方法的应用特点；并在教材最后增加了安全系统工程应用实例一章。在理解方法的基础上，更注重对学生应用能力的培养，使学生真正能学以致用。同时结合注册安全评价师考试，与其方法能力的要求相匹配。三是应用型习题提供答案解析，便于学生自学。为了更好地让学生理解相关知识点，每章后面提供一定数量的练习题，同时对应用型的习题附上参考答案，以便学生加深理解和灵活应用。

全书共分十二章：第一章绪论、第二章安全检查表、第三章预先危险性分析、第四章故障类型及影响分析、第五章危险和可操作性研究、第六章事件树分析、第八章系统安全分析的其他方法及小结，由许素睿编写；第七章事故树分析，由谢振华编写；第九章安全评价、第十章安全预测、第十一章安全决策、第十二章安全系统工程应用实例，由谢振华、许素睿编写。

本书在编写过程中，参考了大量相关的文献资料，在此向这些作者表示最诚挚

的谢意。同时也要感谢项原驰为本书所付出的辛苦，尤其是书中大量图表的编写工作。更要感谢中国劳动关系学院科研处为我们提供这样一个能够展示我们多年的教学研究并与大家交流的机会。由于编者水平有限，加之时间仓促，书中疏漏和错误在所难免，敬请读者不吝赐教。

编　者

2015 年 8 月

目　录

第一章　绪　论

人类社会在发展过程中经历了各种各样的事故，事故带来的意外情况会造成死亡、疾病、伤害、损伤或其他损失，严重制约了经济发展和社会进步。

从事故预防的角度来看，安全工作方法可分为“问题出发型”和“问题发现型”两大类。

“问题出发型”方法是在事故发生后吸取经验教训，制订出预防事故的方法。一个系统发生事故，说明该系统存在某些不安全、不可靠的问题。人们通过对事故的调查、分析，找出事故原因，采取措施防止事故重复发生。通常采取各种管理和技术措施，如制定法律法规和标准、设置安全机构、进行监督检查和宣传教育，以及防火防爆措施、安全防护设备、个人防护用品等，都属此类。这就是通常所说的传统安全工作方法。

“问题发现型”方法是从系统内部出发，研究系统各构成要素之间存在的安全上的联系，分析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降低或消除系统的危险性，把发生事故的可能性降低到最小。这就是采用安全系统工程控制事故的方法，即安全系统工程工作方法。

传统安全工作方法是凭经验，事后被动的工作方法。而人们特别是安全工作者希望找到一种方法，能够在事故发生前就预测到事故发生的可能性，掌握事故发生规律，做出定性和定量评价的安全工作方法，以便在系统的设计、施工、运行、管理中对发生事故的危险性加以辨识，并且能够根据对危险性的评价结果，提出相应的安全措施，达到控制事故的目的。安全系统工程就是为了达到这个目标而发展起来的。

第一节　安全系统工程的基本概念

一、安全

安全(Safety)是一种状态，人们免遭不可接受风险的状态。安全是一个相对的概念，对于一个组织，经过风险评估，确定了不可接受风险，那么就要采取措施将不可接受风险降至可允许的程度，使得人们免遭不可接受风险的伤害，进而实现安全。这是从系统安全思想的“安全是相对的思想”对安全的界定。

二、系统

1. 定义

钱学森描述系统(System)的概念时说,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,而且该"系统"本身又是它所从属的一个更大系统的组成部分。

2. 特性

一般来说,系统具有四个特性:

(1)整体性。系统是由两个或两个以上的要素(元件或子系统)组成的整体。构成系统的各个要素虽然具有不同的性能,但它们通过综合(而不是各要素性能的简单相加)形成了一个统一的整体,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。例如,一台计算机就是由主板、电源、CPU、硬盘、键盘、显示器等硬件通过特定的关系,有机地结合在一起所形成的一个系统。

(3)目的性。任何一个系统,不论其大小,都具有特定的功能,没有目标的系统是不存在的。特别是人类创造的系统,总是为了实现某一目的而设计、制造出来的。

(4)环境适应性。任何一个系统都存在于一定的环境之中,因此它必然要与周围环境发生物质、能量和信息的交换,以适应外部环境的变化。在研究系统的时候,环境往往起着重要的作用,必须予以重视。适者生存就是这个道理。

3. 功能结构

系统的功能是接收信息、能量和物质,并根据时间序列产生信息、能量和物质。这就要求合理地管理和控制能量、物质和信息的流动,来保证系统的安全和在最优状态下工作。

系统虽然种类繁多,可大可小,但若对其结构进行仔细分析,就可以看出系统主要由三部分组成,即输入、处理和输出,如图 1—1 所示。任何系统都具有输出某产物的目的,而且一定是先有输入,再经处理,才能得到输出。处理是使输入变为输出的一种活动,通常由人和设备分别完成或联合承担。比如汽车制造厂生产汽车是由入口输入了原材料,经过加工和作业,进行整体装配,这就相当于处理部分,装配好的汽车再由出口输出。这种以物质流动为主的系统称为生产系统。一项计划也可视为输入,经过执行,即处理阶段,最后得到了结果,就是输出。这种以信息流为主的系统称为管理系统。系统处理后的结果,不一定是理想的,这就需要验证

和修正，通过改善执行环节来达到预期的目的，这个过程就是反馈。

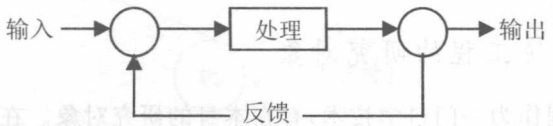

图 1—1 系统的功能结构示意图

三、工程

工程(Engineering)是指服务于特定目的的各项工作(软硬件)的总体。例如安全工程、环境工程、水利工程、希望工程等。这里所说的工程具有广泛的意义，不仅指与物质、能量等有关的工作，而且包括信息处理、人的行为、心理研究等各个方面。

四、系统工程

系统工程(System Engineering)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、技术等多方面的最新科学成就和知识的一门综合性的科学技术。钱学森称“系统工程是组织管理的科学”。

五、安全系统工程

安全系统工程(System Safety Engineering)是指采用系统工程方法，识别、分析、评价系统中的危险性，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，使系统可能发生的事故得到控制，并使系统安全性达到最好的状态。

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。

(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辨识、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。

第二节 安全系统工程的研究对象和内容

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。在生产安全领域，系统是指在特定的工作环境中，为完成某项操作任务或特定的功能而整合在一起的人员、规程、设备等。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，生产必须的机器设备、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，分别称为人子系统、机器子系统和环境子系统。

1. 人的子系统

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。研究人的子系统时，不仅把人当作“生物人”，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；不仅把人的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、有主观能动性的生物。

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，以及要从人体测量学、生理学、心理与生理过程有关参数出发对仪表、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、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，三者之间的关系如图 1－2 所示。例如理化因素影响机器的精度、寿命甚至损坏机器；机器产生的噪声、振动、温度、尘毒又影响人和环境；人的心理状态和生理状况往往是引起误操作的主观因素；社会环境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，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。

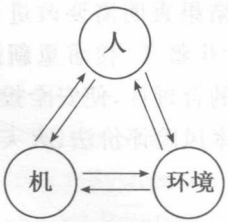

图 1—2 人—机—环境关系图

二、安全系统工程的内容

安全系统工程是一种综合性的技术方法，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的科学技术。其主要包括以下四个方面的内容：

1. 系统安全分析

系统安全分析是安全系统工程的核心内容，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、定量描述的一种技术方法。通过对系统进行深入、细致的分析，充分了解和查明系统存在的危险性，估计事故发生的概率和可能产生伤害及损失的严重程度，为确定出哪种危险能够通过修改系统设计或改变控制系统运行程序来进行预防提供依据。所以，分析结果的正确与否，关系到整个安全工作的成败。

系统安全分析的方法有几十种，它们从各个不同的角度对系统的安全性进行分析。每一种系统安全分析方法都有其产生的历史背景和适用条件，各有优缺点。要完成一个准确的分析往往需要综合使用多种分析方法，有时还要相互比较，看哪些方法和实际情况更为吻合。因此，在使用时应首先了解、熟悉系统，并选用合适的、具有特色的分析方法。常用的系统安全分析方法主要有安全检查表、预先危险性分析、故障类型及影响分析、危险和可操作性研究、事件树分析、事故树分析等。

2. 系统安全评价

系统安全评价是以系统安全分析为基础，对系统存在的危险性进行定性和定量分析，得出系统存在的危险点与发生危险的可能性及其严重程度，以得到被评价系统的安全状况。

安全评价可分为定性评价和定量评价。定性评价的结果用大概的度量信息表现，让人们能够知道系统中危险性的大致情况。但这比起用传统安全方法来，已经系统和准确多了。定量评价的结果则能用较为精确的量值表现，以较为直观的数量形式反映安全的状况。只有经过定量评价才能充分发挥安全系统工程的作用，决策者可以根据评价的结果选择技术路线，监管部门可以根据评价结果督促企业

改进安全状况。当安全评价的结果表明需要改进系统的安全状况时，就必须采取安全措施，减少危险因素及其发生概率，接着重新进行安全评价，直到达到安全要求。同时也应当评价投入资金的合理性，使安全投资取得最大的安全效益。

常用的安全评价方法有概率风险评价法、火灾爆炸危险指数评价法、模糊综合评价法等。

3. 系统危险控制

系统安全工程的最终目的是控制危险。对一个系统进行安全分析和评价后，针对系统中的薄弱环节或潜在危险，提出调整修正的措施，以消除事故的发生或使发生的事故得到最大限度的控制。

安全措施主要包括安全技术措施和安全管理措施两个方面。通常采用的安全措施有法制手段、安全教育、安全防护装置、改善作业环境、改进工艺过程或修改设计、加强安全管理等。

4. 安全预测和安全决策

安全预测是在分析、研究系统过去和现在安全资料的基础上，利用各种知识和科学方法，对系统未来的安全状况进行预测，预测系统存在的危险种类及危险程度，以便对事故进行预报和预防。常用的安全预测方法有德尔菲预测法、回归预测分析法、灰色系统预测法等。

安全决策是针对生产活动中需要解决的特定安全问题，根据安全法律法规、标准、规范等的要求，运用现代科学技术知识和安全科学的理论与方法，提出各种安全措施方案，经过分析、论证与评价，从中选择最优方案并予以实施的过程。

第三节 安全系统工程的产生及应用

一、安全系统工程的产生

安全系统工程产生于20世纪50年代末美、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内就连续发生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和可靠性，并于1962年第一次提出了BSD－Exhibit－62－41《导弹火箭系统安全工程学》；1963年这份文件被修改成空军规范MIL－S－38130《军事规范——针对系统、有关子系统和设备安全工程的通用要求》；1966年6月美国国防部将其做了微小的改动，制定了MIL－S－38130A；1969年这个规范被进一步修改，形成了美国军标MIL－STD－882《系统及相关子系统和设备的系统安全方