普通高等教育“十五”国家级规划教材

陈宝智 编著

XITONG ANQUAN PINGJIA YU YUCE

系统安全评价与预测

冶金工业出版社

“十五”国家级规划教材

系统安全评价与预测

东北大学　陈宝智　编著

北　京
冶 金 工 业 出 版 社
2005

内 容 提 要

本书在介绍系统安全的基本理论、原则和观点的基础上，重点地介绍了系统安全评价与预测的理论、原则和方法，并介绍了一些反映该领域新进展的内容，如两类危险源的概念、重大事故危险源的辨识和评价等。

本书注重知识的系统性和可操作性，理论联系实际，文字简练，各章都附有思考题，除可作为高等学校教材外，还可供相关专业的科研人员、工程技术人员及管理人员参考或职业技术培训之用。

图书在版编目(CIP)数据

系统安全评价与预测/陈宝智编著. —北京：冶金工业出版社，2005.10

普通高等教育“十五”国家级规划教材

ISBN 7-5024-3769-X

Ⅰ.系… Ⅱ.陈… Ⅲ.安全系统分析—高等学校—教材 Ⅳ.X913

中国版本图书馆 CIP 数据核字(2005)第 102614 号

出版人 曹胜利（北京沙滩嵩祝院北巷 39 号，邮编 100009）

责任编辑 宋 良 王文涛 美术编辑 李 心

责任校对 杨 力 李文彦 责任印制 牛晓波

北京兴华印刷厂印刷；冶金工业出版社发行；各地新华书店经销

2005 年 10 月第 1 版， 2005 年 10 月第 1 次印刷

850mm×1168mm 1/32；7.875 印张；208 千字；238 页；1—3000 册

20.00 元

冶金工业出版社发行部 电话：(010)64044283 传真：(010)64027893

冶金书店 地址：北京东四西大街 46 号(100711) 电话：(010)65289081

冶金工业出版社部分图书推荐

书　　名	作　　者	定价(元)
安全原理(第2版)	陈宝智　编著	20.00
矿山事故分析及系统安全管理	招金集团公司	28.00
中国职业安全健康管理体系内审员培训教程		50.00
重大危险源辨识与控制	吴宗之　等编	35.00
危险评价方法及其应用	吴宗之　等编	47.00
中国冶金百科全书·安全环保卷	编委会	120.00
采矿手册(第6卷)矿山通风与安全	编委会	109.00
安全检测技术与仪表	罗怀永　等编	7.30
起重机司机安全操作技术	张应立　主编	70.00
环境保护及其法规(第2版)	任效乾　等编	45.00
环保知识400问(第3版)	张殿印　主编	26.00
矿山环境工程	韦冠俊　主编	22.00
环境噪声控制	李家华　主编	19.80
矿床无废开采的规划与评价	彭怀生　等著	14.50
矿山生态复垦与露天地下联合开采	杨福海　等著	20.00
工程爆破实用手册	刘殿中　等编	60.00
中国冶金矿山可持续发展战略研究	焦玉书　等编	45.00

前　言

“系统安全评价与预测”是安全工程专业的主要专业课程之一。本书在介绍系统安全的基本理论、原则和观点的基础上，重点介绍了系统安全评价与预测的理论、原则和方法。

系统安全是为了解决大规模复杂系统安全性问题而产生的理论、原则和方法体系，与以往的安全工程理论相比，在安全观念和方法论方面有许多创新，丰富和发展了安全工程的理论和方法。例如，它认为系统中存在着的危险源是事故发生的原因，人类的任何活动都存在着潜在的危险，安全只是一个相对的、主观的概念，所谓的安全是一种可以被人们接受的危险；它的一个基本原则，是从一个新系统构思、可行性研究阶段开始，直到系统报废为止的整个系统寿命期间内，都要辨识危险源、预测系统事故并采取相应措施控制危险源，评价其危险性是否在可接受的范围内。于是，事故预测与系统安全评价就成为系统安全工程的重要内容。事故预测与系统安全评价紧密地联系在一起，相辅相成。根据系统内存在危险源的情况预测可能发生的事故；通过对系统内危险源的危险性评价以及对危险源控制措施的评价，定量地预测事故发生的可能性，以及一旦发生事故时其后果的严重程度。

随着系统安全评价与预测的理论在实践中不断发展，新理论、新方法不断涌现，课程知识体系有了较大的变化，原有的教材内容已经不能适应教学的要求。为了适应新的教学要求，及时反映本学科的最新科研成果，满足工程领域的需求，笔者根据新的“系统安全评价与预测”课程教学大纲和工程实际应用的需要，在系统总结多年来的教学经验和科研成果的基础上，编写了本书。

编写过程中，在将系统安全评价和预测基本知识加以系统化的同时，增加了一些反映该领域新进展的内容，如两类危险源的概念，重大事故危险源的辨识和评价等。系统安全预测与评价具有很强的实践性，它产生于安全工程实践，并在实践中不断发展。本书在介绍理论、原则和方法的同时，注意了可操作性的问题。书中除了引用一些典型例子之外，每章还附有一些练习题和思考题，以帮助学生学习运用这些理论、原则和方法。

本书汲取了东北大学安全工程专业教师们二十多年来在讲授该课程中积累的宝贵经验，参考、引用了大量的国内外文献。张培红、李刚、钟茂华、肖国清等博士参与了本书的编写，并根据教学过程中发现的问题提出了修改意见，使得内容更臻完善。在此谨向诸位同事、文献作者表示诚挚的谢意。

由于本人学识所限，书中有不当之处，敬请读者批评指正。

作　者

2005年6月

目　录

1 总　论

1.1 系统安全评价与预测概述

安全工程领域涉及的危险，主要是指人们在生产活动和生活活动中意外发生的各种事故造成的人员伤亡、财产损失或环境污染的危险。面对这些危险，人们做出种种努力以回避危险，追求安全。安全工作的根本目的，就是防止事故的发生，并且在事故发生后，尽量减少事故所造成的人员伤亡、财产损失或环境污染。

为了防止发生事故，需要预测事故；只有预测了事故，才能有针对性地采取措施，防止事故的发生。

人们希望充分利用已有的科学技术知识去认识事故发生的规律，在事故发生前预测事故的发生和事故可能造成的后果，从而先行采取措施防止事故发生，或者在一旦发生事故时，最大限度地避免、减少人员伤亡和财产损失。

很久以来，人们在事故预防方面，基本上是“从事故学习事故”，即分析、研究以往事故发生的原因和总结防止事故的经验，获得预测这类事故再发生的知识，从而指导事故预防工作。例如，根据人员操作机器时曾经发生机械伤害事故的经验，人们可以预测机械厂发生机械伤害事故的可能性。

这种“从事故学习事故”的方式，是科学的、必要的，在今后的事故预防工作中，仍然要继续采用这种方法。然而，事故是一种随机发生的小概率事件，仅凭事故后留下的有限信息来分析、研究其发生原因，是一件非常困难的事情。这种“从事故学习事故”的方式进行的预测只能是定性的，即仅是对未来事故发生可能性的预测。

随着科学技术的进步，新材料、新能源、新技术、新工艺、新产品不断涌现，新种类的事故发生的可能性及其事故后果的严重程

度也在增加。事故的教训往往是用人们的鲜血和生命换来的，其代价是非常高昂的。人们不能等发生了事故并造成严重伤亡之后才来总结经验，研究预防事故的办法。

事故会造成损失，预防事故也需要成本，因此安全也有投入和产出的问题。为了科学、经济合理地预防事故，人们已经不满足于对事故发生可能性的定性预测，还希望能够定量地预测事故的发生及其后果，评价系统的安全状况是否符合人们期望的标准。这就需要研究新的事故预测及安全评价的理论和方法。

20 世纪 60 年代末出现的系统安全工程为我们提供了系统的、定量的事故预测和安全评价的理论和方法。在系统安全工程中，事故预测与系统安全评价紧密地联系在一起，相辅相成。根据系统内存在危险源的情况，预测可能发生的事故；通过对系统内危险源的危险性评价和对危险源控制措施的评价，定量地预测事故发生的可能性以及一旦发生事故时其后果的严重程度。

1.1.1 系统安全评价与预测的产生

系统安全评价与预测是系统安全工程的基本内容之一，与系统安全工程同时产生和发展。

20 世纪 50 年代以后，科学技术进步的一个显著特征是设备、工艺和产品越来越复杂。战略武器研制、宇宙开发和核电站建设等使得作为现代先进科学技术标志的大规模复杂系统相继问世。这些复杂的系统往往由数以千万计的元件、部件组成，元件、部件之间以非常复杂的关系相连接；在研制及使用它们的过程中常常涉及到高能量。系统中的微小差错就会引起大量能量的意外释放，导致灾难性的事故，“蝼蚁之穴”可毁千里长堤。这些大规模复杂系统的安全性问题受到了人们的关注。

人们在开发研制、使用和维护这些大规模复杂系统的过程中，逐渐萌发了系统安全的基本思想。作为一种现代安全工程理论和方法体系的系统安全，起源于 20 世纪 50 年代到 60 年代美国研制民兵式洲际导弹的过程中。

当时采用的导弹推进剂是由气体加压到41.2MPa，温度低达－196℃的低温液体。这种推进剂的化学性质非常活泼且有剧毒，其毒性远远超过战争中使用的毒气，其破坏性比烈性炸药更猛烈，其腐蚀性超过工业生产中使用的腐蚀性化学物质。负责该研制项目的美国空军官员们开始并没有认识到他们着手建造的导弹系统潜伏着巨大的危险性。在洲际导弹试验的头一年半里就发生了4次爆炸，造成了惨重的损失。在此之前，美国空军曾发生多次飞行事故。空军官员们一般都把事故的原因归因于飞行员的操作失误。但是由于导弹上没有飞行员，爆炸完全是由导弹自身的问题造成的，而不能再把导弹爆炸的责任推到驾驶员身上。很明显，分析爆炸原因应该查出导弹投入试验之前的构思、设计、制造和维护等方面的问题。以此为契机，美国开始了系统安全方面的研究。

此前，没有可以用来解决这些复杂系统的安全性的方法。为此，人们做了许多工作，开发防止系统发生事故的方法。新方法被一个一个地开发出来了，新概念逐渐产生了；安全工程原有的概念和方法中正确的部分被保留和改进了，并从其他领域吸收了许多有用的科学技术和工作方法，形成了系统安全的理论、原则和方法体系。其中，系统安全工程则是实现系统安全的手段。

系统安全工程首先在美国空军内应用之后，又推广到美国陆军和海军。1969年美国国防部颁发《系统安全大纲要求》，即MIL-STD-882标准，详细规定了武器系统开发研究、生产制造和使用、维护的系统安全标准。1984年颁发了修订版MIL-STD-882B，1993年又颁布了新版本MIL-STD-882C。该标准对系统安全的实施和要求做了全面的规定，建立了系统安全的完整概念，给出了系统安全分析、设计、评价的基本原则、内容及要求，提出了定性的系统安全评价方法，是系统安全产生和发展的一个重要标志。

在这一阶段，人们研究开发了许多以系统可靠性分析为基础的系统安全分析方法，可以定性或定量地预测系统故障或事故。

此后，系统安全工程进入航天、航空及核工业等领域，系统安全评价与预测进入了一个新的发展阶段。

1.1.2 概率危险性评价

在核电站系统安全工程的研究和应用方面，美国麻省理工学院的拉斯马森(N. C. Rasmussen)教授从1972年起，由美国原子能委员会出资300万美元，花费50人·年的工作量，完成了萨里(Sarrey)核电站和桃花谷(Peach bottom)核电站的概率危险性评价。在该研究中，在没有核电站事故先例的情况下预测了核电站事故，应用事件树分析和故障树分析等系统安全分析方法，建立了核反应堆事故模型，并输入各种故障率数据，进行了概率危险性评价。1975年美国原子能委员会发表了题为《美国商用核电站事故危险性评价》的安全研究报告，WASH 1400(NUREG 701014)。

拉斯马森的研究报告曾在美国国内引起核电站支持者和反对者之间的激烈争论。但是，不久后发生的三哩岛核电站事故证明，该研究采用的系统安全分析方法和概率危险性评价方法是正确的。1980年美国原子能委员会发表核电站安全目标，1981年出版了《概率危险性评价指南》。之后，系统安全工程以及概率危险性评价受到世界各国的重视。

20世纪70年代以后，系统安全工程逐渐推广到航天、航空、石油、化工、矿山工业等领域。

继核工业领域应用之后，概率危险性评价被成功地应用于化学工业和石油化学工业领域。1976～1978年间，英国原子能机构就坎维岛(Can Vey)化学和石油化学工业安全性问题进行了概率危险性评价。由于此次评价是概率危险性评价在非核领域的首次应用，引起了科技界人士的极大兴趣，也受到工业界一些人士的怀疑。1981年英国安全与健康委员会进行了复评，肯定了评价结果，认为概率危险性评价是一种有效的决策辅助工具。

目前，在海上石油平台的设计、建造、运行中也已经广泛地应用概率危险性评价。

1.1.3 重大事故危险源控制

随着化学工业、石油化学工业的发展，大量易燃易爆、有毒有

害的物质相继问世。它们作为工业生产的产品或原料在被生产、加工处理、储存和运输过程中一旦发生事故，其后果非常严重。特别是20世纪70年代以后，世界范围内发生了许多震惊世界的重大火灾、爆炸、有毒有害物质泄漏事故。这些事故的共同特点是，事故造成的人员伤亡、物质损失、环境污染程度非常严重，其影响范围往往超出工厂的围墙，威胁公众安全，甚至威胁邻国居民安全。因此，重大事故预防问题受到了世界各国的广泛关注。

一些欧洲国家较早地提出了重大事故危险源控制的问题。

1974年，英国的弗利克斯堡(Flixborough)工厂发生了环己烷蒸气云爆炸事故，有28人丧生，89人受伤，2450幢房屋损坏，直接经济损失达700万美元。以此次事故为契机，英国健康和安全委员会(HSE)建立了重大危险源咨询委员会，进行重大危险源控制和立法方面的咨询。

1976年，意大利的塞韦索(Seveso)工厂和曼福莱多尼亚(Manfredonia)工厂发生大量毒物泄漏事故。塞韦索工厂的环己烷泄漏事故，有30人受伤，22万人疏散。面对频繁发生的重大事故，欧共体于1982年颁布了《关于工业活动中重大事故危险源的指令》，即塞韦索指令，要求各加盟国、行政监督部门和企业等承担在重大事故控制方面的责任和义务。例如，要求企业必须提出安全报告，让企业自己了解自身的危险性。最初，该指令把重点放在掌握化工企业危险物质的储存量和识别设备、工艺异常上，后来扩展到核电站安全、环境污染控制等方面问题。

世界其他地区也相继发生了一些重大事故。例如，1984年墨西哥城发生石油液化气爆炸事故，有650人丧生，数千人受伤；1984年印度博帕尔农药厂发生甲基异氰酸盐泄漏，导致2000人死亡、2万人受伤。我国曾发生了黄岛油库火灾、南京炼油厂火灾等重大事故。

1988年国际劳工局(ILO)颁布了《重大事故控制指南》，指导各国的重大事故危险源控制工作。

到1991年，欧共体各加盟国都已经把塞韦索指令移植到国内

法律中。例如，英国首先颁布了工业重大事故防止法，要求企业提出包括定量分析在内的内部报告和外部报告；意大利规定，如果安全报告有不实之处，企业负责人将被处以包括监禁在内的重罚。

1993 年国际劳工局通过了《预防重大工业事故公约》。该公约要求各成员国必须采取措施控制重大危险源。

在重大事故危险源控制实践中，系统安全评价与预测又有了许多新发展。例如，适用于化工生产那样工艺过程危险源辨识的危险性与可操作性研究，适用于重大危险源评价的火灾爆炸指数法、事故后果分析等。

系统安全工程作为现代安全工程的标志，越来越广泛地应用于安全工程的各个领域，并在实践中不断发展、完善。

1.1.4 中国的系统安全评价与预测

我国自 20 世纪 70 年代末、80 年代初开始了系统安全评价与预测的研究和应用，并与工业安全的理论、方法紧密结合，使得原本为解决大规模复杂系统安全性问题的系统安全工程迅速在工业安全领域推广和普及。

改革开放以来，国家十分重视企业安全工作，在贯彻“安全第一，预防为主”安全生产方针、加强安全管理的同时，注重采用先进安全科学技术，“安全是科学”逐渐深入人心。改革开放政策也为学习国外先进安全科学技术打开了方便之门，国内一些院校、研究所开始介绍、研究系统安全工程，并把系统安全工程用于一般工业安全领域。

最初的研究主要集中在作为危险源辨识方法的各种系统安全分析方法方面，预测可能发生的事故，应用故障树分析、事件树分析等方法分析事故发生的原因，进行定性的安全评价，指导事故预防工作。一些行业、部门、地区有组织地推广，使得系统安全分析方法迅速普及。许多企业的安全专业人员都能应用故障树分析等方法进行事故原因分析。一些企业，如鞍山钢铁公司等，结合中国企业安全工作的实际情况，开展了群众性的危险源辨识、评价和控