

- 国家自然科学基金面上项目 (71171199) 资助出版
- 国家自然科学基金青年科学基金项目 (71401179) 资助出版

复杂系统

风险传递与控制

王瑛 汪送 管明露 著



国防工业出版社
National Defense Industry Press

国家自然科学基金面上项目(71171199)资助出版

国家自然科学基金青年科学基金项目(71401179)资助出版

复杂系统风险传递与控制

王瑛 汪送 管明露 著

国防工业出版社

·北京·

内 容 简 介

本书从“点—线—面—体”的视角来综述事故致因理论,分析复杂系统的风险演化动力学过程。通过构建针对现代复杂系统事故致因与演化分析的“认知—约束”模型,从事故系统模型构建、事故系统风险动力学行为认知、关键致因节点辨识与控制角度深入阐述和分析复杂系统的风险传递与控制问题,并结合装备研制项目复杂系统进行了风险传递与控制的实证研究。试图从事故系统的角度来分析复杂系统的风险传递与控制问题是本书的特色。

本书涉及控制科学与工程、管理科学与工程、安全科学与工程、系统工程、复杂性科学等多个学科领域,主要读者对象为高等院校管理、安全、军事类本科生和研究生,亦可作为科学工作者、工程技术人员及高校教师的参考书。

图书在版编目(CIP)数据

复杂系统风险传递与控制/王瑛,汪送,管明露著. —北京:国防工业出版社,2015.1
ISBN 978-7-118-09772-6

I. ①复... II. ①王... ②汪... ③管... III. ①安全系统学 IV. ①X913

中国版本图书馆 CIP 数据核字(2014)第 247207 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)

三河市腾飞印务有限公司印刷

新华书店经售



*

开本 787×1092 1/16 印张 11 字数 270 千字

2015 年 1 月第 1 版第 1 次印刷 印数 1—2000 册 定价 35.00 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

安全事故一直伴随着人类的发展,随着现代复杂系统安全性、可靠性和自动化程度的提高,其复杂性和耦合性也日益增长,导致事故本质发生根本转变,即便是系统设计者也不能完全理解系统的各种潜在交互行为。现有的针对机械系统或简单机电系统的事故致因理论和模型难以有效应对复杂系统中各种动态的非线性效应,因此发展和完善新一代系统论模型显得迫在眉睫。

风险评估作为风险管理的重要环节,必须充分考虑风险的动态特性,才能有效提高评估的可信度。初始点风险通过有形介质或无形效应传输至系统的一系列点或面的过程称为风险传递,风险传递需要依托一定的传递载体和特定的传递路径。风险传递是风险动态特性的一种描述方式,因风险传递及其进一步的耦合效应,使得风险评估变为极为复杂,同时给风险控制带来较大困难。

《复杂系统风险传递与控制》是国家自然科学基金面上项目“基于结构本质安全的复杂系统组元作用机理研究(71171199)”和国家自然科学基金青年科学基金项目“复杂事故系统风险演化动力学机制研究(71401179)”共同研究成果之一。全书基于系统科学和复杂性科学思维,综合运用了控制科学与工程、系统工程、熵学、复杂网络等多学科的理论和方法,围绕所提出的“认知—约束”模型来展开研究,本着事故系统模型构建——事故系统行为(风险涌现与传递)认知——关键致因节点辨识与控制的研究主线,提出了一种面向复杂系统安全事故的事前预防、事中控制和事后分析的新一代系统论模型,并结合装备研制项目复杂系统进行了风险传递与控制的实证研究,相关结果对完善事故致因理论和预防系统性安全事故有积极意义。

在本书的编撰出版过程中,得到各级领导和同志们的支持与帮助,借此机会表示感谢,并特别感谢郭建圣、战仁军、李超、刘刚、袁博等同志对本书顺利出版做出的贡献。本书的出版意在抛砖引玉,希望能激起广大读者对风险传递与控制的研究兴趣。由于作者水平有限,书中难免存有疏漏之处,恳请读者批评和斧正。

作者

目 录

第1章 绪论	1
1.1 研究背景及意义	1
1.2 复杂系统安全事故与测度研究现状	2
1.2.1 事故致因理论研究现状	2
1.2.2 事故分析方法研究现状	4
1.2.3 事故测度—熵理论研究现状	6
1.3 复杂系统风险行为与控制研究现状	8
1.3.1 涌现问题研究现状	8
1.3.2 风险传递研究现状	10
1.3.3 安全控制研究现状	11
1.4 本书研究内容与章节安排	13
1.4.1 本书研究内容的确定	13
1.4.2 本书的章节安排	14
第2章 事故分析“认知—约束”模型框架	16
2.1 复杂系统安全性本质探析	16
2.1.1 事故成因复杂性根源	16
2.1.2 复杂系统安全性与可靠性关系探讨	18
2.1.3 安全—复杂系统的整体涌现	20
2.2 新系统论模型发展趋势分析	22
2.2.1 非系统论模型的缺陷	23
2.2.2 系统论模型的优势	24
2.2.3 发展新一代系统论模型的基本要求	25
2.3 “认知—约束”模型的构建	26
2.3.1 “认知—约束”模型的广义内涵	26
2.3.2 “认知—约束”模型的内在机制	27
2.3.3 “认知—约束”模型的数学描述	28
2.3.4 “认知—约束”模型的实施步骤	29

2.3.5 基于“认知—约束”模型的安全控制	30
第3章 集成 DEMATEL - ISM 方法的事故系统构模分析	32
3.1 复杂系统崩溃过程分析	32
3.1.1 脆性概念	32
3.1.2 复杂系统的脆性	33
3.1.3 从复杂系统到事故系统	34
3.2 复杂系统安全事故致因因素的提取	36
3.2.1 事故因素提取原则	36
3.2.2 一般性事故因素的提取	37
3.3 集成 DEMATEL - ISM 方法步骤	38
3.3.1 集成 DEMATEL - ISM 结构化方法的理论基础	38
3.3.2 决策实验室分析法 (DEMATEL)	40
3.3.3 解释结构模型 (ISM)	41
3.4 空军某飞行团事故系统的案例分析	43
3.4.1 案例背景及数据来源	43
3.4.2 计算过程与分析	46
3.4.3 结果与讨论	55
第4章 事故系统风险涌现的度量研究	56
4.1 风险涌现的界定与描述	56
4.1.1 复杂系统事故路径分析	56
4.1.2 风险涌现与风险熵的界定	58
4.1.3 风险涌现的动力学机制	59
4.2 事故致因节点独立风险熵度量	60
4.2.1 可拓学方法与改进	61
4.2.2 基于改进可拓学方法的独立风险熵度量	64
4.3 事故致因节点耦合风险熵度量	65
4.3.1 Copula 连接函数	65
4.3.2 基于 Copula 函数的耦合风险熵度量	66
4.4 跨层致因节点风险涌现度量	66
4.4.1 跨层致因节点风险熵	66
4.4.2 跨层致因节点极大风险熵	67
4.5 跨层风险涌现的 Arena 仿真	68
4.5.1 Arena 软件概述	68

4.5.2	跨层风险涌现的 Arena 仿真模型	69
4.5.3	跨层风险涌现仿真结果及分析	69
第 5 章	事故系统风险传递的 Arena 仿真	73
5.1	风险传递的描述及仿真流程	73
5.1.1	风险传递的形式化描述	73
5.1.2	风险传递的动力学机制	74
5.1.3	风险传递仿真要素及流程	75
5.2	风险传递 Arena 仿真模型构建	77
5.2.1	事故系统模型重构与描述	77
5.2.2	Arena 仿真模型	78
5.2.3	仿真目的与实验设计	80
5.3	初始风险涌现规律的影响分析	81
5.3.1	涌现均值对风险熵增长速率的影响	81
5.3.2	涌现均值对系统风险处置能力的影响	82
5.3.3	涌现均值对节点风险处置能力的影响	83
5.3.4	结果与讨论	87
5.4	节点参数对系统风险处置能力的影响分析	88
5.4.1	节点风险免疫力的影响	88
5.4.2	节点风险处置速率的影响	94
5.4.3	结果与讨论	98
5.5	网络结构对系统风险处置能力的影响分析	99
5.5.1	改变风险处置资源数的影响分析	99
5.5.2	改变初始风险涌现节点的影响分析	100
5.5.3	改变节点风险传递概率的影响分析	101
5.5.4	结果与讨论	102
第 6 章	事故系统关键致因节点的约束控制	103
6.1	熵权集结多维数据的节点重要度评估	103
6.1.1	静态评估参数提取	104
6.1.2	专家经验数据处理	106
6.1.3	动态风险传递的数据分析	106
6.1.4	熵权集结多维数据的致因节点重要度评估算法	107
6.1.5	计算结果及分析	108
6.2	基于约束熵的事故系统致因节点崩溃控制策略	110

6.2.1	约束熵概念的引入	110
6.2.2	约束熵度量模型的构建	110
6.3	基于 Arena 仿真的节点重要度排序结果验证	111
6.3.1	基于备用风险处置资源的验证	111
6.3.2	基于节点风险处置速率的验证	114
6.3.3	结果与讨论	114
6.4	应急约束熵配置的仿真分析	115
6.4.1	应急约束熵被所有节点共享时的配置分析	115
6.4.2	应急约束熵被重要节点独享时的配置分析	116
6.4.3	应急约束熵被重要节点按级共享时的配置分析	117
6.4.4	应急约束熵数量对系统性能的影响分析	118
6.4.5	结果与讨论	119
6.5	实证研究	119
6.5.1	约束熵的工程意义	119
6.5.2	空军某飞行团安全控制策略分析	120
第 7 章	研制项目复杂系统 GERT 网络上的风险传递	124
7.1	装备项目型供应链概述	124
7.1.1	装备供应链研究现状	124
7.1.2	航空装备项目型供应链	125
7.2	GERT 随机网络概述	126
7.2.1	GAN 网络的构成与特点	126
7.2.2	矩母函数	129
7.2.3	信号流图	130
7.2.4	GERT 随机网络解析法原理	131
7.3	研制项目 GERT 网络上的风险传递	133
7.3.1	研制项目的 GERT 网络建模	133
7.3.2	GERT 网络上单风险传递的解析法求解	134
7.3.3	GERT 网络上多风险传递的解析法求解	135
7.4	GERT 网络上多风险传递解析法求解案例	136
7.4.1	案例背景	136
7.4.2	计算过程及分析	137
7.5	GERT 网络上多风险传递的蒙特卡洛模拟	139
7.5.1	蒙特卡洛方法	139
7.5.2	Crystal Ball 仿真软件	140

7.5.3	GERT 网络中环路的等价化简	140
7.5.4	仿真过程及结果分析	144
第 8 章	基于贡献度和风险分担的风险传递控制策略	148
8.1	供应链利益分配方法	148
8.1.1	按劳分酬法	148
8.1.2	契约式利益分配法	148
8.1.3	基于 Shapley 值的利益分配法	149
8.2	基于节点重要度的行为主体贡献度建模	150
8.2.1	行为主体贡献度的含义	150
8.2.2	节点位置重要度	150
8.2.3	节点属性重要度	151
8.2.4	节点贡献度模型	152
8.3	行为主体抗风险努力程度评价	153
8.3.1	主动识别风险因素的评价	153
8.3.2	积极控制本环节风险的评价	154
8.3.3	藏匿和转嫁风险的惩罚	154
8.4	基于贡献度和抗风险努力程度的利益分配	155
8.4.1	基于贡献度的固定利益分配	155
8.4.2	基于抗风险努力程度的超额利益分配	155
参考文献		157

第 1 章 绪 论

1.1 研究背景及意义

安全是人类永恒的话题，安全事故一直伴随着人类的发展。随着现代复杂系统安全性、可靠性和自动化程度的提高，安全事故发生概率显著减小，但世界安全事故统计资料表明，安全问题仍然十分严峻，类似惨痛事故依旧重复发生，即使“相当”安全的复杂系统，也可能会发生事故，而且一些事故往往是灾难性的，如：1986 年 1 月 28 日美国“挑战者号”航天飞机的爆炸、1986 年 4 月苏联切尔诺贝利的核电站悲剧、2008 年年初我国南方地区的冰雪灾害、2009 年 5 月 31 日法航飞机的空中解体等。这些事故的发生或者来源于系统内部结构的突变(如“挑战者号”航天飞机密封装置故障)；或者来源于系统外界环境的突变(如南方冰灾中暴雪、严寒等骤变天气导致的电力系统的崩溃)。环境突变通过改变系统边界的稳定性，进而影响系统组元的排列秩序，促使系统内部结构突变，从而引发安全事故，因此可以认为安全事故的根本致因在于系统内部结构的突变。安全事故的预防对策就是实现系统结构的本质安全。

根据结构决定功能原理，系统结构安全决定系统功能安全，系统结构稳定和系统边界稳定共同维系着系统功能的本质安全，系统结构稳定是系统结构安全的充分条件。系统结构功能逻辑关系分析法是一种识别系统、掌握系统，从而更好地控制和利用系统的方法。系统结构是系统组元排列秩序的表征，信息和能量是组元之间交互的媒介。研究组元之间的交互作用，可以从信息和能量的转移中找到某些规律，这种组元之间的微观作用在宏观上表征为结构演变，这种演变一旦发展为一种失控的突变，就会造成系统崩溃，进而引发安全事故。因此复杂系统内部组元间错综复杂的信息和能量交互过程影响着系统结构的本质安全。如何控制组元间信息和能量的交互模式对于维持系统结构稳定性，进而促进系统结构安全和系统功能安全意义重大。

由于复杂系统是由层次众多、复杂关联的若干子系统所组成，子系统则又包含了若干层次错综复杂的组成元素，此外，复杂系统的自组织性、自适应性、涌现性、不确定性、预决性、演化和开放性等特点进一步导致了其事故致因的复杂性。于是针对传统机械系统或简单机电系统的事故致因方法在分析软件日益密集的现代复杂系统时就显得难以胜任。目前煤矿、交通、电力、航空等系统事故频繁，就进一步表明了现有事故致因理论模型的局限性，同时发展和完善新一代面向现代复杂系统事故致因分析的系统论模型就显得迫在眉睫。

不同的复杂系统具有截然不同的系统结构，因此从个别复杂系统物理结构本身去研究结构与功能之间的关联是极为困难的，而且所研究的特殊复杂系统的结构功能逻辑关系，对于其余的复杂系统并非适用。此外对于事故而言，很多系统致因并非仅存在于物

理系统内部,如人为失误、环境扰动等就属于客观复杂系统外部的事故因素。此时就需要将复杂系统事故分析抽象为一般性问题来展开研究,如可在扩大系统边界的前提下,根据一定的映射规则来提取复杂系统一般性的事故因素,并通过结构化处理方法获得递进的因素层次结构模型,也即构建与客观复杂系统相对应,而系统边界更大且系统元素具有较强聚类特性的事故系统。进一步可通过认知事故系统的各种行为,特别是其风险动力学行为,来获得复杂系统的安全控制对策。由于事故系统是包含普适性事故因素的一般性系统,因此基于事故系统动力学行为分析所揭示的事故规律,在应用于实际复杂系统时,只需添加所研究复杂系统的专有特性即可。这样就可以获得复杂系统较为通用的基于事故系统结构稳定性视角的安全性研究方法,此时所提取的事故因素的范围更为广泛,易于捕捉到事故的本质致因和指导未来类似事故的预防。

因此,将非结构化或半结构化的事故因素进行结构化处理,构建与复杂系统相对应的具有递阶层次结构的事故系统模型,就可以通过认知事故系统中致因节点的行为特性及致因节点间的关联特性来阐明安全事故的成因机制,进而提供基于关键致因节点牵连控制的复杂系统安全控制新对策。同时用熵来测度危险源所引发的致因节点风险状态,就可以实现对事故系统中风险动力学行为的量化分析,从而使得基于关键致因节点的约束控制具有更强的针对性和经济性。通过对上述问题的研究,可望完善事故致因理论,同时可为安全事故的事前分析及复杂系统的优化设计提供理论指导和技术支持。

1.2 复杂系统安全事故与测度研究现状

近年来,关于复杂系统安全性问题的研究取得了一系列的成果,各种事故致因理论不断被提出和完善,众多学者尝试着从不同视角来分析和测度事故成因与演化,从而使对复杂系统安全事故的研究出现了蓬勃发展的趋势。

1.2.1 事故致因理论研究现状

安全科学是一门阐明事故发生和预防规律的科学。事故致因理论是阐明事故为什么会发生,事故是怎样发生的,以及如何防止事故发生的理论,其在安全科学理论中占有十分重要的位置。掌握事故规律对于提高系统安全性和预防未来类似事故具有重大意义。伴随着生产力的发展、生产方式的改变,以及人们安全观念的转变,事故致因理论不断发展和完善。根据事故因素的分布情况及关联特性,本节将从“点源”、“线源”、“面源”和“体源”四个角度对现有的事故致因理论进行综述。

20世纪初,资本主义世界工业生产已经初具规模,机械化工生产在提高生产力的同时也带来了大量的工业生产事故。于是,1919年,Greenwood和Woods提出了“事故倾向性格”论。1926年Newbold,1936年Farmer相继对其进行了进一步补充和完善。这些理论认为事故集中于部分“事故频发倾向者”或“事故遭遇倾向者”,其根源在于人的性格缺陷或心理原因。这里所指的个性性格缺陷和心理原因被认为是事故发生的唯一原因,因此可以将该理论归类为“点源”事故致因理论。

“点源”与文献中的单因素理论有类似指向,这种单一的事故致因主要指人或者环境,前者将事故归咎于人的性格或心理缺陷,后者则认为环境是事故的直接原因,而忽

视人的主观能动性，也有学者将技术因素视为单因素。

“点源”或者单因素理论只是从某一个方面、某一个角度研究事故发生的规律，是最简单原始的理论，它忽略了事物之间的联系性，也因此这种理论被迅速取代，随着系统复杂化、规模化程度的提高，单因素理论开始向多因素理论方向发展。

“线源”事故致因理论将单个的“点源”因素视为有前后关联的事件，以事故链的形式进行呈现。1936年，Heinrich提出了事故因果连锁理论，他认为伤害事故的发生是一连串依次发生的事件，并以五块多米诺骨牌(社会环境、人的失误、人的不安全行为或物的不安全状态、事故和伤害)来形象地描述这种因果关系，因此该理论也被称为“多米诺骨牌”理论。在此基础上，1974年，Frank Bird提出了管理失误连锁理论，同年，John Adams提出了和Frank相似的因果连锁模型，日本学者也提出了北川彻三事故因果连锁理论。

“线源”事故致因理论，考虑到了事故因素的多元化，认为事故与原因之间存在着必然的因果联系，“因”与“果”有继承性，事故链中下游事件是上游事件的结果，上游事件是下游事件的原因，因果通过多个层次相继发生。“线源”理论考虑到了从纵深方向挖掘事故的本质原因，但将事故过程描述为线性的链式结构，又显得过于绝对和简单。此外，“线源”事故致因理论将“线”的末端视为事故的初始事件，又似乎回到了“点源”理论，事实上，仅仅依靠消除初始事件是不足以预防安全事故的，初始事件是广泛而随机的。Zahid H也指出基于线性失效链的安全分析与风险评估方法，在对现代复杂系统进行建模与分析时具有较大局限性，“线源”事故模型只适合于分析只含有物理部件失效和人为失误的简单系统。

“点源”和“线源”事故致因理论适合于分析简单系统的事故成因，随着系统复杂程度的提高，新技术的引入、经济趋势以及管理环境改变等因素通常会产生新类型危险源，这时就需要相应地更新事故模型。此时，事故致因的范围也不再是局限于单一“点源”或者单一的事故链(“线源”)，而是多条事故链所组成的事故网络，因此可以将该类事故致因理论界定为“面源”事故致因模型。“面源”是一种形象化的表示，只为说明因素间未出现层次结构的划分。

1949年，Gorden基于流行病传染机理而提出的“病理学”理论；1961年，由Gibson提出，并在1966年经Hadden完善的“能量转移理论”；1969年，J. Surry提出，并在20世纪70年代初得到发展的瑟利模型；1995年，Reason提出的组织失效模型等都属于典型的“面源”事故致因理论。

“面源”事故致因理论已初步体现了系统论的观点，综合运用了信息论、系统论和控制论的观点、方法，该类理论认为事故背后存在复杂的致因网络是较为形象的，同时指出事故的致因是多而广泛的，这是较“点源”和“线源”理论的重大突破。系统论模型认为事故的发生是一种涌现现象，根源在于复杂的部件交互导致系统结构的突变，最终酿成事故。如果事故的发生是一种涌现，则其致因必然出现了层次结构的跃迁，因此“面源”事故理论应该向“体源”事故理论方向发展。

“体源”事故致因理论认为事故成因不是简单的事故链，也不是处于同一层面的事故致因网络，而是具有等级层次结构的立体事故致因网络。动态和变化的观点是该类事故致因理论的基础。两类危险源理论、综合原因论等理论属于此类。综合原因论认为事故

是社会因素(基础原因)、管理因素(间接原因)和事故隐患(直接原因)被偶然事件触发所造成的结果。

“体源”事故致因理论从系统论的角度指出事故因素呈立体的网状结构分布,也即事故因素间存在递进的层次结构,这种层次结构的跃迁对应着事故的涌现过程。然而现有事故致因理论和模型大多针对的是事故发生后的事后分析,较少关注事故的预防问题,部分学者意识到危险源控制的重要性,但同时缺乏系统论的视角,忽略了多数事故共同的潜在性系统致因。因此为有效提高现代复杂系统的安全管理水平,需要基于系统论的视角,在提高认知能力的同时,不断强化对潜在事故致因的约束控制。

层次结构是系统的主要特征,同时层次结构关系到系统的稳定,进而决定着系统的安全。研究复杂系统的层次结构就是为实现其结构的本质安全化,而通过研究事故因素的层次结构,确保事故系统的相对稳定也可以在一定程度上实现复杂系统的安全稳定。因此,可以从结构—功能的角度来研究复杂系统安全事故。

1.2.2 事故分析方法研究现状

自 Bertalanffy 唤醒现代科学对复杂性的兴趣开始,对复杂系统的研究一直是学术界的热点和前沿。在现代复杂系统中,组元种类及层次结构的错综复杂性以及信息、能量交互模式的错综复杂性,导致了复杂系统事故成因的复杂性。系统的功能本质安全实现途径如图 1.1 所示,系统结构本质安全是实现系统功能本质安全的前提,系统结构稳定对于系统结构的本质安全有促进作用,通过深入到系统微观层面的组元交互中,强化组元间的正效交互作用,减小组元间的负效交互作用,方可维系系统结构的稳定。关于从结构的角度的研究事故问题方面,Rasmussen 和 Svendsen 提出了一种 AcciMap 方法来对事故系统进行结构化分析,以确定事故因素间的复杂交互关系。

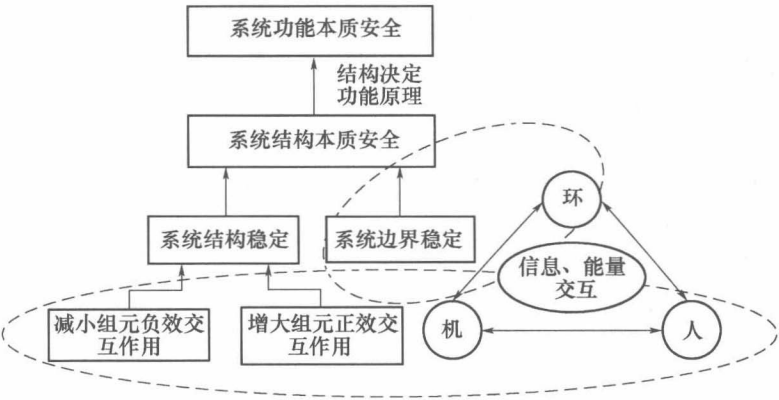


图 1.1 系统功能本质安全实现途径

复杂系统安全性得不到有效保证,一方面在于事故机理过于复杂,安全控制的实施难度大;另一方面则在于复杂系统运行中安全需求和功能需求通常是相互背离的。Zhe Chen 等将安全需求视为控制结构来约束系统行为,提供了一种基于安全约束的系统建模方法。实际上安全需求应成为系统行为的约束条件,从某种程度上来说,约束系统行为

就是为了维护系统的稳定性。而这种行为约束,主要体现在结构的相互牵制中。

复杂系统的结构包括空间结构、功能结构和时间结构。物理系统脆弱性由系统空间结构决定,其脆弱性又受到系统环境和人为因素的影响。在内外界的干扰和冲击下,系统表现出固有的脆性属性。脆性结构的脆性度不仅取决于设计制造所赋予的抗干扰、冲击能力,同时与使用阶段的干扰、冲击强度有关。因此在进行系统设计时,必须赋予结构一定的安全裕度。

本质安全设计理念最早由 Kletz 于 1978 年提出,考虑到系统脆性作为一种本质属性,为实现系统的本质安全化就应提高系统组元的抗干扰能力,在经济可承受的前提下,提高系统的安全裕度。本质安全需要合理配置系统在运行过程中的基本交互作用、规范交互作用及文化交互作用的耦合关系,从而实现系统的内外在和谐性。因此,系统结构的本质安全化就是在一定的干扰和冲击下结构能保持固有的稳定特性。魏震波等提出了一种基于电网状态与结构的综合脆弱性评估模型,在评估复杂系统脆弱性时,除了应监控节点的状态特征外(可靠性问题),对节点在网络中的重要程度也应进行考虑(安全性问题),实际上对复杂系统性能的评价应是可靠性与安全性的统一,脆弱性评估是实现复杂系统使用阶段本质安全化的有效保障。薛飞等也指出,电网的安全问题必须从运行状态与网络结构两个角度来展开分析。

复杂系统结构的本质安全是指一种具有较强自适应、自协调能力,抗风险能力强的耗散结构,而本质安全的减小、替代、适度(缓和)和简化等基本原则为实现复杂系统结构本质安全提供了手段。本质安全评价指标是实现本质安全定量评估的有效途径,对于复杂系统结构的本质安全而言,结构稳定性无疑是一个重要的衡量指标,而结构稳定性又恰恰受制于系统组元的交互作用。目前对本质安全的评估多注重对单一指标的估计和衡量,较少考虑各个指标间的交互和耦合作用,而事实上,事故的发生并非只是单因素所致。因此 James J.H. Liou 提出了一种针对航线安全预测的综合模型,考虑了各个评价指标间的耦合交互作用对系统安全度的影响。考虑评价指标间的耦合问题,也是对系统组元交互作用的一种侧面表征。

然而结构本质安全化方面的研究较少深入到系统内部微观层面的危险源的运动规律中去,事实上只有通过阐明从危险源到脆性结构间的演变关系,进而分析子系统脆性联系导致的系统结构突变,才可以进一步探明系统安全事故的本质致因。有学者从状态和结构两个方面来对电网系统安全性进行评估,体现了系统思维,也因此为本书研究提供了思路,即从因素个体特性和因素关联特性两个方面去分析复杂系统的事故成因。

事故系统是由事故因素所组成的系统,现代复杂系统的事故因素呈立体网状结构分布。

在事故因素结构化处理中,在解释结构模型(Interpretative Structural Modeling, ISM)应用方面,李树砖等应用 ISM 方法构建了煤矿瓦斯爆炸致因解释结构模型,找出了表层直接因素、中层间接因素、深层根本因素。许晶等基于 MATLAB 软件构建了群体性事件 45 种诱发因素的多层递阶解释结构模型,阐述了诱发因素间的逻辑关系。田彦清等通过构建作业场所风险影响因素体系,给出作业场所风险影响因素的 5 级多层递阶解释结构模型,并采用层次分析法确定了表层直接影响因素的权重。钟诗颖等基于 ISM 方法构建了火灾事故因素间的递阶层次结构模型。这些研究表明,ISM 方法可以实现因素的层级划分。

在结构方程模型(Structural Equation Modeling, SEM)应用方面,傅贵等采用结构方程模型对安全文化的关键要素、构成因子以及因子间的因果关系进行了研究。郭凯运用结构方程模型分析了煤矿安全影响因素及其因果变量间的相互关系,设计了模型的路径,构建了因素评估分析模型。汤志伟等基于问卷调查和结构方程模型分析了网络群体性事件诱发因素及其因素之间的相互关系,构建了网络群体性事件诱发因素模型。SEM方法可定量地研究因素间的复杂关联。

此外,施式亮等应用分形理论的 R/S 分析方法建立煤矿安全指标分形时间序列,以此来表征煤矿安全生产复杂非线性系统的动力学特征。Yan Fu Wang 等提出了一种用于评估人和组织因素对事故贡献的模型,首先通过定性方法求潜在的事故因素,进一步通过贝叶斯网络进行定量分析,以找出关键因素。

上述结构化分析方法中,ISM 方法应用最为广泛,且较容易掌握,而 SEM 方法需要建立在广泛的问卷调查基础上,贝叶斯网络应用也较为广泛,但计算复杂度较高。

事故的发生来自于系统结构的崩溃,也可以认为是事故系统的某种结构突变。从结构的角度来研究安全性问题,就必须对结构状态进行准确度量。系统结构因各种因素的影响而呈现复合不确定性,而熵作为不确定性的最佳测度就可以被有效运用。此外,熵还可以实现对系统状态的量和质的统一度量。

1.2.3 事故测度—熵理论研究现状

1854 年,德国物理学家 K·Clausius 引入态函数熵来描述热力学第二定律。1856 年,Clausius 把可逆过程中工质吸收的热量 Q 与绝对温度 T 之比值称为 Entropy。1923 年,普朗克来中国讲学时,我国字典里还没有与 Entropy 对应的汉字,胡刚复教授翻译时就在商字的基础上加了个“火”字(表示与热有关)来代表 Entropy,从此在我国汉字库里就有了“熵”字。随后,耗散结构理论的提出,推动了熵概念和熵理论在各个领域的蓬勃发展。

1. “熵”的宏观意义——热力学熵

熵概念来源于热力学,如果一定工质进行可逆卡诺循环,在绝对温度 T 下吸收了微元热量 dQ ,则把熵的变化 ΔS 记为:

$$\Delta S = \frac{dQ_r}{T} \quad (1.1)$$

$$\Delta S = S_A - S_B = \int_A^B \frac{dQ_r}{T} \quad (1.2)$$

式中, $\Delta S \geq 0$, 取“=”时表示用于孤立系统可逆过程;取“>”时表示用于孤立系统不可逆过程。上式表明,熵仅与工质的状态有关,而与其经过的路径无关,是一个状态量。

2. “熵”的微观意义——统计物理熵(Boltzmann 熵)

奥地利物理学家 Boltzmann 在研究气体分子运动过程中,基于把热理解为微观世界分子运动的观点,对熵做出了微观解释,认为熵就是表示粒子之间的混乱程度的物理量,当一个系统处于平衡时,系统的微观能量状态个数越多,熵也越大。

因此有下式所示的 Boltzmann 熵公式:

$$S = k \ln w \quad (1.3)$$

式中, k 为 Boltzmann 常数, w 为确定的宏观状态所包含的微观状态数。该式表明宏观系统的无序度可以用微观状态数来表示。

3. 信息熵

1948 年, 信息论创始人 Shannon 把 Boltzmann 熵的概念引入信息论中, 把熵作为一个随机事件的不确定性或信息量的量度, 从而奠定了现代信息论的科学理论基础, 大大地促进了信息论的发展。Shannon 信息熵是一个独立于热力学熵的概念, 但具有热力学熵的基本性质(单值性、可加性和极值性), 并且具有更为广泛和普遍的意义, 所以称为广义熵。它是熵概念和熵理论在非热力学领域泛化应用的一个基本概念。

信息是熵的对立面, 熵是系统无序度的度量, 获得信息就可以减小系统的熵。因此, 信息熵可定义为:

$$S = -k \sum_{i=1}^n P_i \ln P_i \text{ (离散状态信息熵)} \quad (1.4)$$

$$S = -k \int_{-\infty}^{+\infty} f(x) \ln f(x) dx \text{ (连续状态信息熵)} \quad (1.5)$$

式中, k 为常数, n 为系统状态的数目, P_i 为状态 i 出现的概率, $\sum_{i=1}^n P_i = 1$; $f(x)$ 为连续状态下的概率密度函数, 通常取 $k=1$, 并定义 $0 \ln 0 = 0$ 。

由于信息熵具有对不确定性和无序度进行描述的能力, 因此可以用于对系统风险状态的度量。杨丽娟等基于信息熵的不确定性度量的性质, 构建了一种用于度量金融和保险业中的数据尾部风险的累积剩余熵模型。Dionisio 等采用信息熵对金融市场的不确定性进行了度量。袁博等提出了一种用于评估股票风险的熵风险度量模型, 基于收益波动来度量投资风险, 使得对投资风险度量更为客观。张群等采用三维熵式度量模型对风险投资方案进行了评价和排序。这些研究表明熵可以用于对风险的度量。

4. 极大熵

部分学者将非热力学领域的熵增原理称为最大熵原理。这主要是取自熵增原理中封闭系统的熵自动增到最大且稳定在最大熵状态, 即任何物质系统总是在约束下争取(呈现)最大自由权状态, 最终导致系统达到约束所允许的最混乱、最复杂、最丰富的状态。该原理最为经典的应用是 E. T. Jaynes 的极大熵准则: 一个系统, 如果它的状态受到许多相互独立的、均匀小的随机因素影响(称为基本对称系统), 则其状态的概率分布, 应在表征这个系统状态的约束条件下, 使这个分布的熵最大。因此, 在选择分布函数时, 应选择使熵能最大化的分布。

在传统的风险度量方法中, 方差度量法占据着重要的位置, 这是因为风险中的损失和收益变化均是随机变量, 而方差是统计学中最常用的描述随机变量特性指标。采用方差度量风险需要获得一些先验信息来设定先验分布, 在缺乏大样本数据时, 先验分布的设定常依赖于决策者的主观判断和主观意愿, 而极大熵准则恰好能弥补这种缺陷的客观规则, 由它设定的先验分布是唯一能够做出的无偏假设。

极大熵准则用于构造先验概率分布的优点体现在: ①极大熵的解是最超然的, 在数

据不充分前提下求解,解必须和已知数据吻合,同时必须对未知部分作最少假定;②用极大熵法求得的解满足一致性要求,不确定性的测度(熵)与试验步骤无关。

设随机变量 X 的概率密度函数为 $f(x)$,则熵可定义为:

$$H(X) = - \int_R f(x) \ln f(x) dx \quad (1.6)$$

式中, R 为随机变量所在的集合。根据极大熵准则,随机变量 X 的概率分布应为:

$$\text{Max}[H(X)] = \text{Max} \left[- \int_R f(x) \ln f(x) dx \right] \quad (1.7)$$

同时将先验信息构成如下约束:

$$\int_R f(x) dx = 1 \quad (1.8)$$

$$\int_R f(x) g_j(x) dx = E[g_j(\cdot)] \quad (j = 1, 2, \dots, m) \quad (1.9)$$

式中, $g_j(\cdot)(j=1,2,\dots,m)$ 是根据先验信息所获得的矩信息函数表达式。极大熵就是在给定的约束下所求得的最大熵值。

由于熵可以用于测度不确定性,也可以作为系统状态的量和质的统一度量,因此本书将采用熵来测度风险状态,提出风险熵的概念。“体源”事故致因理论刻画出了一种立体的致因网络,结构化处理方法可用于分析因素间的层次结构和关联关系,基于熵理论可实现对系统风险状态的度量,然而事故通常起源于初始危险源的出现,初始危险源会触发系统一定的风险状态。

1.3 复杂系统风险行为与控制研究现状

基于静态的分析与评估来研究复杂系统的安全事故往往难以取得较好的效果,复杂系统的事故过程是一个复杂的非线性动力学过程,因此必须以动态的眼光来看待,事故发生实际上就是风险的涌现与传递过程,安全控制措施也必须紧扣事故动态性的本质。

1.3.1 涌现问题研究现状

随着复杂性科学和系统科学的日益兴起,作为二者研究核心的“涌现”便成为研究焦点,涌现理论也随之而生。系统科学把复杂系统整体才具有的,而孤立的系统元素及其总和不具备的特性,称为整体涌现性。涌现的重要研究目标之一就是要建立起涌现特征与微观机制的联系,认识并控制涌现特征。本节将从涌现概念、特征机制和复杂系统安全涌现三个方面进行综述。

有关“涌现”的思想,可以追溯到很远的历史,亚里士多德的“整体大于部分之和”,老子的“有生于无”,都是古代朴素“涌现”观念或思想的代表性语言。“涌现”作为学术术语的提出,可以追溯到19世纪上半叶英国J.S.Mill关于两种因果关系的学说。

涌现概念界定方面:Holland把复杂系统的从简单的局部产生复杂的整体的现象称为涌现,即“涌现是从小原因中产生的大结果”。龚小庆指出涌现就是构成系统的各个主体