系统安全工程

SYSTEM SAFETY ENGINEERING

陈全　编著

天津科学技术出版社

系统安全工程

陈全　编著

天津科学技术出版社

图书在版编目（CIP）数据

系统安全工程 / 陈全编著. —天津：天津科学技术出版社，2010.11

ISBN 978-7-5308-6147-9

Ⅰ.①系…Ⅱ.①陈…Ⅲ.①安全工程—人-机系统

Ⅳ①X912.9

中国版本图书馆CIP数据核字（2001）第228891号

策划编辑：郑东红

责任编辑：王连弟

责任印制：王　莹

天津科学技术出版社出版

出版人：蔡　颢

天津市西康路35号　邮编 300051

电话：（022）23322399（编辑室）23332393（发行部）

网址：www.tjkjcbs.com.cn

新华书店经销

天津市同利印刷有限公司印刷

开本889×1 194 1/16　印张13.75　字数377 000

2010年12月第1版第1次印刷

定价：30元

作 者 名 单

陈　全　　冯　炘　　周　艳
赵代英　　李　玲　　怀　霞
支晓伟　　关文玲　　孙志民

前　言

随着经济的发展、科学技术的进步，出现了很多工业复杂系统，即指技术密集系统，包括技术设备、人、组织三类元素的复杂的社会——技术系统，如化工与石油化工、电力、铁路、矿山、核电等工业组织。系统科学认为，复杂系统的问题必须通过系统化的方法才能解决，传统的方法是无能为力的。对于现代的工业复杂系统，传统安全工作方法不足以解决其安全问题，必须采用系统化的安全工作方法。

系统安全的思想是安全科学发展到今天的最新成果。所谓系统安全，是人们为控制复杂系统事故而开发、研究出来的安全理论、方法体系，是在系统寿命期间内应用系统安全工程方法，辨识系统中的危险源，并采取控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。系统安全工程方法涉及危险源辨识、评价和控制的原理和方法。

系统安全的思想和系统安全工程方法产生于20世纪60年代。经过几十年的不断探索和实践，目前系统安全工程已从应用技术发展到理论研究，并逐步形成自身的理论和方法体系。但系统安全工程还是一个处于发展中的学科，自身的体系还处于不断的完善中。 在系统安全工程的研究和实践中，其理论和方法在不断地完善和出新。

我国20世纪80年代开始引入系统安全工程的理论和方法。随着近几年我国企业安全评价和职业健康安全管理体系实施工作的深入，系统安全工程理论和方法更多地应用到企业的安全管理过程中。从而促使从事安全工程研究的工作者进一步深入研究系统安全工程的理论和方法，同时也为总结系统安全工程理论和方法的企业实践应用经验创造了条件。

我国安全工程专业的高等教育近几年发展迅速，更多的安全工程专业的学生学习系统安全工程的专业课程。总结过去国内高等学校系统安全工程的教学经验，有必要进一步基于近几年国内系统安全工程理论研究的成果和应用实践的经验，在原有著作和相关文献的基础上，编写概念和逻辑思路清晰、系统全面、结合实际应用、通俗易懂的系统安全工程著作作为教学的指导。本书就是应这方面的需求而编写的。

本书融入了陈全教授和他的同事在安全工程领域多年的理论研究和应用实践成果。书中对系统安全的原理及相关基础概念做了详尽的分析和阐述，对相关著作涉及的局部理论和方法做以系统的整理和分类，力求使读者对系统安全工程建立一个全面、清晰的思路。为切实地解决系统安全工程方法的应用性问题，书中列举了较多的实际应用的案例。由于本人水平有限，书中谬误之处在所难免，敬请批评指正。

编者

目　录

第一章　系统安全工程方法的产生和发展

第一节　事故致因理论与系统安全

为了防止事故，必须弄清事故为什么会发生，造成事故发生的原因因素即事故致因因素有哪些。在此基础上，研究如何通过控制事故致因因素来防止事故发生。

事故是一种可能给人类带来不幸后果的意外事件。千百年来，人类主要是“从事故学习事故”，即根据事故发生后残留的关于事故的信息来分析、推论事故发生的原因及其过程。由于事故发生的随机性质以及人们知识、经验的局限性，使得对事故发生机理的认识变得十分困难。

在科学技术落后的古代，人们往往把事故的发生看做是人类无法违抗的“天意”或“命中注定”，而祈求神灵保佑。随着社会的发展，科学技术的进步，特别是工业革命以后工业事故频繁发生，人们在与各种工业事故斗争的实践中不继总结经验，探索事故发生规律，相继提出了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。由于这些理论着重解释事故发生的原因以及针对事故致因因素如何采取措施防止事故，所以被称做事故致因理论。事故致因理论是指导事故预防工作的基本理论。

事故致因理论是一定生产力发展水平的产物。在生产力发展的不同阶段，生产过程中出现的安全问题不同，特别是随着生产方式的变化，人在生产过程中所处地位的变化，引起人们安全观念的变化，产生了反映安全观念变化的不同的事故致因理论。

一、早期事故致因理论

20世纪初，资本主义世界工业生产已经初具规模，蒸汽动力和电力驱动的机械取代了手工作坊中的手工工具。这些机械在设计时很少甚至根本不考虑操作的安全和方便，几乎没有什么安全防护装置。工人没有受过培训，操作很不熟练，加上长达11～13小时以上的工作日，伤亡事故频繁发生。根据美国一份被称为“匹兹伯格调查”的报告，1909年美国全国的工业死亡事故高达3万起，一些工厂的百万工时死亡率达到150～200人。根据美国宾夕法尼亚钢铁公司的资料，在20世纪初的4年间，该公司的2 200名职工中竟有1 600人在事故中受到了伤害。

面对广大工人群众的生命健康受到工业事故严重威胁的严峻情况，企业主的态度是消极的。他们说，“为了安全这类装门面的事，我没有钱”，“我手里的余钱也是做生意用的”。他们认为，“有些人就是容易出事，不管做什么，他们总是自己害自己”。

当时，世界各地的诉讼程序大同小异，只要能证明事故原因中有受伤害工人的过失，法庭总是袒护企业主。法庭判决的原则是，工人理应承受所从事的工作中通常可能方式的一切危险。

1919年，英国的格林伍德（M.Greenwood）和伍兹（H.H.Woods），对许多工厂里的伤亡事故数据中的事故发生次数按不同的统计分布进行了统计检验。结果发现，工人中的某些人较其他人更容易出现事故。从这种现象出发，后来法默（Farmer）等人提出了事故频发倾向概念，所谓事故频发倾向（accident proneness），是指个别人容易发生事故的、稳定的、个人的内在倾向。根据这种理论，工

厂中少数工人具有事故频发倾向，是事故频发倾向者，他们的存在是工业事故发生的主要原因。如果企业里减少了事故频发倾向者，就可以减少工业事故。因此，防止企业中有事故频发倾向者是预防事故的基本措施：一方面通过严格的生理、心理检验等，从众多的求职人员中选择身体、智力、性格特征及动作特征等方面优秀的人才就业；另一方面一旦发现事故频发倾向者则将其解雇。显然，由优秀的人员组成的工厂是比较安全的。

其实，工业生产中的许多操作对操作者的素质都有一定的要求，或者说，人员有一定的职业适合性。当人员的素质不符合生产操作要求时，人在生产操作中就会发生失误或不安全行为，从而导致事故发生。危险性较高的、重要的操作，要求人的素质较高。事故频发倾向论把工业事故的原因归因于少数事故频发倾向者的观点是错误的，但从职业适合性的角度，关于事故频发倾向的认识也有一定可取之处。

海因里希（W.H.Heinrich）的工业安全理论是该时期的代表性理论。美国的安全工程师海因里希在《工业事故预防（industrial accident prevention）》一书中，阐述了根据当时的工业安全实践总结出来的所谓工业安全公理。该工业安全公理又被称做“海因里希十条”，其主要内容如下。

（1）工业生产过程中人员伤亡的发生，往往是处于一系列因果连锁之末端的事故的结果；而事故常常起因于人的不安全行为或（和）机械、物质（统称物）的不安全状态。

（2）人的不安全行为是大多数工业事故的原因。

（3）由于不安全行为而受到了伤害的人，几乎重复了300次以上没有造成伤害的同样事故。换言之，人员在受到伤害之前，已经数百次面临来自物的方面的危险。

（4）在工业事故中，人员受到伤害的严重程度具有随机性质。大多数情况下，人员在事故发生时可以免遭伤害。

（5）人员产生不安全行为的主要原因有：①不正确的态度；②缺乏知识或操作不熟练；③身体状况不佳；④物的不安全状态及物理的不良环境。这些原因因素是采取预防不安全行为产生措施的依据。

（6）防止工业事故的4种有效的方法是：①工程技术方面的改进；②对人员进行说服教育；③人员调整；④惩戒。

（7）防止事故的方法与企业生产管理、成本管理及质量管理的方法类似。

（8）企业领导者有进行安全工作的能力，并且能把握进行安全工作的时机，因而应该承担预防事故工作的责任。

（9）专业安全人员及车间干部、班组长是预防事故的关键，他们工作的好坏对能否做好预防事故工作有重要影响。

（10）除了人道主义动机之外，下面两种强有力的经济因素也是促进企业安全工作的动力：①安全的企业生产效率也高，不安全的企业生产效率也低；②事故后用于赔偿及医疗费用的直接经济损失，只不过占事故总经济损失的1/5。

海因里希在他的“工业安全公理”中阐述了事故发生的因果连锁论，作为事故发生原因的人的因素与物的因素之间的关系问题，事故发生频率与伤害严重度之间的关系问题，不安全行为的产生原因及预防措施，事故预防工作与企业其他管理机能之间的关系，进行事故预防工作的基本责任以及安全与生产之间的关系等工业安全中最重要、最基本的问题。数十年来，该理论得到世界上许多国家事故预防工作者的赞同，作为他们从事事故预防工作的理论基础。尽管随着时代的前进，人们认识的深化，该“公理”中的一些观点已经不再是“自明之理”了，许多新观点、新理论相继问世，但是该理论中的许多内

容仍然具有强大的生命力，在现今的事故预防工作中仍然产生重大影响。

根据海因里希的观点，大多数工业伤害事故都是由于工人的不安全行为引起的。即使一些工业伤害事故是由于物的不安全状态引起的，而物的不安全状态的产生也是由于工人的缺点、错误造成的。因而，海因里希理论也和事故频发倾向论一样，把工业事故的责任归因于工人，表现出时代的局限性。

二、二次世界大战后的事故致因理论

到第二次世界大战时期，已经出现了高速飞机、雷达和各种自动化机械等。为防止和减少飞机飞行事故而兴起的事故判定技术及人机工程等，对后来的工业事故预防产生了深刻的影响。

事故判定技术（critical incident technique）最初被用于确定军用飞机飞行事故原因的研究。研究人员用这种技术调查了飞行员在飞行操作中的心理学和人机工程方面的问题，然后针对这些问题采取改进措施防止发生操作失误。战后这项技术被广泛应用于国外的工业事故预防工作中，作为一种调查研究不安全行为和不安全状态的方法，使得不安全行为和不安全状态在引起事故之前被识别和被改正。

第二次世界大战期间使用的军用飞机速度快，战斗力强，但是它们的操纵装置和仪表非常复杂。飞机操纵装置和仪表的设计往往超出人的能力范围，或者容易引起驾驶员误操作而导致严重事故。为了防止飞行事故，飞行员要求改变那些看不清楚的仪表的位置，改变与人的能力不适合的操纵装置和操纵方法。这些要求推动了人机工程学的研究。

人机工程学（ergonomics）是研究如何使机械设备、工作环境适应人的生理、心理特征，使人员操作简便、准确、失误少、工作效率高的学问。人机工程学的兴起标志着工业生产中人与机械关系的重大变化：以前是按机械的特性训练工人，让工人满足机械的要求，工人是机械的奴隶和附庸；现在是在设计机械时要考虑人的特性，使机械适合人的操作。从事故致因的角度，机械设备、工作环境不符合人机工程学要求可能是引起人的不安全行为、导致事故的原因。

第二次世界大战后，科学技术飞跃进步。新技术、新工艺、新能源、新材料和新产品不断出现，与日俱增。这些新工艺、新能源、新材料和新产品给工业生产和人们的生活面貌带来巨大变化的同时，也给人类带来了更多的危险。据说，世界上每20分钟就有一种新的化学物质问世，其中每一种都可能具有危险性。科技的发展也把作为现代物质文明的各种工业产品送到各类人们的面前。这些产品中有些会威胁人员安全。美国1972年涉及产品安全的投诉案件超过50万起。工业部门要保证消费者利用其产品的安全。在公众的强烈要求下，美国于1972年通过了消费品安全法，日本等国也相继通过了相似的法律。这些法律的共同特征是，制造厂家必须对其产品引起的事故完全负责。

随着战后工业迅速发展带来的广泛就业，使得企业不能像战前那样进行“拔尖”的人员选择。除了极少数身心有问题的人之外，广大群众都有机会进入工业部门；工人运动的蓬勃发展，企业主不能随意地开除工人。这就使职工队伍素质发生了重大变化。

战后，人们对所谓的事故频发倾向的概念提出了新的见解。一些研究表明，认为大多数工业事故是由事故频发倾向者引起的观念是错误的，有些人较另一些人容易发生事故，是与他们从事的作业有较高的危险性有关。越来越多的人认为，不能把事故的责任简单地说成是工人的不注意，应该同时注重机械的、物质的危险性质在事故致因中的重要地位。于是，出现了所谓的“轨迹交叉论”，认为人的因素和物的因素运动轨迹的交叉导致事故发生。在事故预防工作中比较强调实现生产条件、机械设备的安全，先进的科学技术和经济条件为此提供了物质基础和技术手段。

能量意外释放论的出现是人们对伤亡事故发生的物理实质认识方面的一大飞跃。1961年和1966年，

吉布森（Gibson）和哈登（Hadden）提出了一种新概念：事故是一种不正常的，或不希望的能量释放，各种形式的能量是构成伤害的直接原因。于是，应该通过控制能量，或控制作为能量达及人体媒介的能量载体来预防伤害事故。根据能量意外释放论，可以利用各种屏蔽来防止意外的能量释放。

与早期的事故频发倾向理论、海因里希因果连锁论等强调人的性格特征、遗传特征等不同，战后人们逐渐地认识了管理因素作为背后原因在事故致因中的重要作用。人的不安全行为或物的不安全状态是工业事故的直接原因，必须加以追究。但是，它们只不过是其背后的深层原因的征兆，管理上缺陷的反映，只有找出深层的、背后的原因，改进企业管理，才能有效地防止事故。

三、系统安全

20世纪50年代以后，科学技术进步的一个显著特征是设备、工艺和产品的越来越复杂。战略武器的研制、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复杂巨系统相继问世。这些复杂巨系统往往由数以千、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；在它们被研制和被利用的过程中常常涉及到高能量。系统中微小的差错就可能引起大量的能量意外释放，导致灾难性的事故。“蝼蚁之穴”可毁千里长堤。这些复杂巨系统的安全性问题受到了人们的关注。

人们在开发研制、使用和维护这些复杂巨系统的过程中，逐渐萌发了系统安全的基本思想。作为现代事故预防理论和方法体系核心的系统安全（system safety）概念产生于美国研制民兵式洲际导弹的过程中。

当时，负责该研究项目的美国空军官员们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。在此以前，美国空军曾发生过许多飞行事故。一般的，空军官员们都把事故的原因归因于飞行员的操作失误。由于导弹上没有飞行员，爆炸安全是由导弹自身的问题造成的，不能再把导弹爆炸的责任推到飞行员身上。很明显，分析导弹爆炸原因应该追究导弹投入试验之前的构思、设计、建造和维护等方面的问题。空军官员的安全观念发生了巨大的变化。

系统安全是人们为预防复杂巨系统事故而开发、研究出来的安全理论、方法体系。所谓系统安全，是在系统寿命期间内应用系统安全工程和管理方法，辨识系统中的危险源，并采取控制措施使其危险性最小，从而使系统在规定的性能、时间和成本范围内达到最佳的安全程度。

系统安全在许多方面发展了事故致因理论。按照系统安全的观点，系统中存在的危险源（hazard）是导致事故发生的根源。系统中不可避免地会存在或出现某些种类的危险源，不可能彻底消除系统中所有的危险源。不同的危险源可能有不同的风险（risk）。由于不能彻底地消除所有的危险源，也就不存在绝对的安全。所谓的安全，只不过是没有超过可接受限度的风险。因此，系统安全的目标不是事故为零，而是最佳的安全程度。

系统安全理论认为，可能意外释放的能量是事故发生的根本原因，而对能量控制的失效是事故发生的直接原因。这涉及能量控制措施的可靠性问题。在系统安全研究中，不可靠被认为是不安全的原因；可靠性工程是系统安全工程的基础之一。研究可靠性时，涉及物的因素时，使用故障或失效（fault、failure）这一术语；涉及人的因素时，使用人的不安全行为（ruman error）这一术语。这些术语的含义较以往的人的不安全行为、物的不安全状态深刻得多。一般的，一起事故的发生是许多人的不安全行为和物的故障相互复杂关联、共同作用的结果，即许多事故致因因素复杂作用的结果。因此，在预防事故时必须在弄清事故致因因素相互关系的基础上采取恰当的措施，而不是相互孤立地控制各个因素。

系统安全注重整个系统寿命期间的事故预防，尤其强调在新系统的开发、设计阶段采取措施控制危险源。对于正在运行的系统，如工业生产系统，管理方面的疏忽和失误是事故的主要原因。约翰逊（W.G.Johnson）等人很早就注意了这个问题，创立了系统安全管理的管理疏忽与风险树（management oversight and risk tree，MORT）。近年来世界各国努力推行的现代职业健康安全管理体系（occupational health and safety management system，OHSMS）则集中地体现了系统安全的管理思想和方法。

第二节　系统安全工程的内容

为了解决复杂系统的安全问题，人们做了许多工作，开发防止系统发生事故的方法。新方法被一个个地开发出来，新的概念逐渐产生，安全工程原有的概念和方法，正确的部分被保留和改进，并从其他领域吸收了许多有用的技术和方法，形成了系统安全的理论和方法体系。其中，系统安全工程方法是实现系统安全的手段。

系统安全工程（system safety engineering）方法运用科学和工程技术手段辨识、控制系统中的危险源，实现系统安全。系统安全工程方法包括系统危险源辨识、评价和控制。

一、危险源辨识

危险源辨识（hazard identification）是识别、确定系统中危险源对象及其特性的工作。这是一项非常重要的工作，它是危险源控制的基础，只有辨识了危险源之后才能有的放矢地考虑如何采取措施控制危险源。

以前，人们主要根据以往的事故经验进行危险源辨识工作。例如，美国的海因里希（W. H. Heinrich）建议通过与操作者交谈或到现场检查，查阅以往的事故记录等方式识别危险源。在系统比较复杂的场合，危险源辨识工作会较困难，需要利用专门的方法，还需要许多知识和经验。

二、危险源控制

危险源控制（hazard control）是利用工程技术（engineering）、教育培训（education）和管理手段（enforcement）来控制危险源，即所谓事故控制的3E原则。

通过技术手段控制危险源的基本理论依据是能量意外释放论。从防止危险源能量意外释放导致事故而言，危险源控制技术包括防止事故发生的安全技术和避免或减少事故损失的安全技术。前者在于约束、限制系统中的能量，防止发生意外的能量释放；后者在于避免或减轻意外释放的能量对人或物的作用。显然，在采取危险源控制措施时，我们应该着眼于前者，做到防患于未然。另一方面也应做好充分准备，一旦发生事故时防止事故扩大或引起其他事故，把事故造成的损失限制在尽可能小的范围内。

教育培训是通过提高人的意识、能力来控制人的不安全行为或失误。教育培训的重要性，首先在于它能够提高人员控制事故的责任感和自觉性。其次，安全技术知识的普及和安全技能的提高，能使人员掌握事故发生的客观规律，提高安全操作技术水平，进而有效控制事故。

管理也是危险源控制的重要手段。管理的基本功能是计划、组织、协调、控制。通过一系列有计划、有组织的系统安全管理活动，控制系统中物的因素和人的因素，以有效地控制危险源。

当危险源自身的特性表明，其可能导致的事故后果足够小时，可以不必考虑对危险源采取控制措施。

三、危险源评价

1. 危险源重要度的评价

基于事故致因因素的分析来阐述危险源的概念（第二章第二节），结果表明，危险源涉及可能意外释放能量的能量物质或载体、直接可能诱发能量物质或载体意外释放能量的物的不安全状态和人的不安全行为两方面因素、导致伤亡事故发生深层次的管理因素。在实际的安全管理过程中，可对危险源涉及的不同方面的因素进行重要度的评价。

对可能意外释放能量的能量物质或载体的危险源做重要度的评价，可针对评价结果，采取对危险源实施分级监控管理和针对性应急准备和响应（第三章第一节）。

对物的不安全状态和人的不安全行为两方面因素实施重要度评价，可针对评价结果，采取对危险源实施分级监控管理和针对性的控制措施，如确定系统故障的维修方式等（第四章第二节）。

2. 危险源的风险评价

系统安全工程方法引入了风险管理（risk manangement）的原理和方法。事故是人们不希望发生的危险事件，也是一种随机事件，本身存在着不确定性，它具有对企业目标实现有不利影响的风险。

企业可通过风险管理过程控制事故的风险。一个规范的风险管理过程包括：风险识别；风险分析；风险评价；风险应对。这在系统安全工程领域内体现为：危险源辨识；风险评价；控制措施确定。

危险源的风险评价（risk assessment）实际体现为对危险源控制措施效果的评价。对危险源采取了控制措施后，通过对其实施风险评价，可以表明危险源控制措施的效果是否达到了预定的要求。如果采取控制措施后风险仍然很高，则需要进一步研究对策，采取更有效的措施使风险降低到预定的标准。

按一般意义上的理解，应该在危险源辨识的基础上进行危险源的风险评价，依据风险评价的结果确定危险源的控制措施。但实际工作中，这三方面的工作并非按这样的程序分阶段独立进行，而是相互交叉、相互重叠进行的，如图1-1。

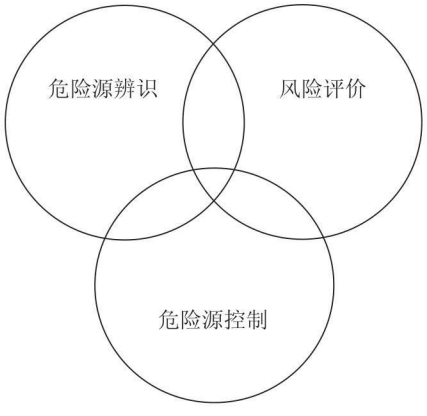

图1-1　危险源辨识、控制和评价

第二章　相关术语和定义

在系统安全工程方法中有一些具有特定含义的术语和定义，理解掌握这些具有特定含义的术语和定义，是进一步掌握系统安全工程方法的前提条件。GB/T28001-2009《职业健康安全管理体系要求》中涉及系统安全工程方法的术语有如下几个：事件（incident）；事故（accident）；危险源（hazard）；危险源辨识（hazard identification）；风险（risk）；可接受风险（acceptable risk）；风险评价（risk assessment）。在我国的安全生产管理领域，还有一些相应的与上述术语具有相关联含义的术语，诸如：未遂事故；危险因素、有害因素、不安全因素、事故隐患；危险因素或不安全因素识别、隐患排查；安全评价或危险评价。本章对上述术语一并做出分析阐述。

第一节　事件、事故、未遂事故

事件（incident）是发生或可能发生与工作相关的健康损害（ill health）或人身伤害（无论严重程度）、或者死亡的情况。

事故（accident）是一种发生人身伤害、健康损害或死亡的事件。

事件是国际职业健康安全专业领域使用的一种术语表达。它本身包含着二种情况对象：一是人们在从事工作活动中不期待发生的造成伤害、健康损害或死亡的事情；二是有可能造成伤害、健康损害或死亡后果，但由于一些偶然因素，实际上没有造成伤害、健康损害或死亡的事情。例如，人员在地板上行走滑倒，会有二种情况出现：一是跌伤肢体；二是跌倒后无伤害。事故是指上述事件中的前一种情况。事件与事故之间的关系是事件包含事故，事故是事件中的一种情况。

我国的职业健康安全专业领域用事故和未遂事故来表述事件包含的两种情况。在国际上也有用“near-miss”、“near-hit”、“close call”或“dangerous occurrence”表述未发生伤害、健康损害或死亡的事件。

美国的海因里希（W. H. Heinrich）对事件进行过较为深入的研究，他在调查了5 000多起伤害事故后发现，在330起类似的事故中，300起事故没有造成伤害，29起引起轻微伤害，一起造成了严重伤害。即严重伤害、轻微伤害和没有伤害的事故件数之比为1∶29∶300，这就是著名的海因里希法则，如图2-1。而其中的300起无伤害事故，即为未遂事故。

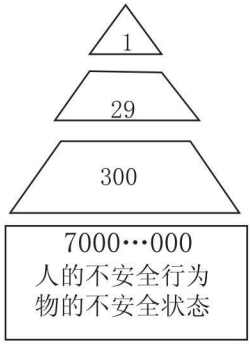

图2-1 海因里希法则示意图

海因里希法则反映了事故发生的频率与事故后果严重度之间的一般规律，且说明事故发生后其后果的严重程度具有随机性质或者说其后果的严重度取决于机会因素。因此，一旦发生事故，控制事故后果的严重程度是一件非常困难的工作。为了防止严重伤害的发生，应该全力以赴地防止未遂事故的发生。

某工人在地板上滑倒，跌坏膝盖骨，造成重伤。调查表明，该工人经常弄湿地板而不擦干，且达6年之久。他在湿滑的地板上行走时经常滑倒，无伤害、轻微伤害及严重伤害的比例为1 800∶0∶1。

某机械师企图用手把皮带挂到正在旋转的皮带轮上，由于他站在摇晃的梯子上，徒手不用工具，又穿了一件袖口宽大的衣服，结果被皮带轮卷入而死亡。事故调查表明，他用这种方法挂皮带已达数年之久，手下的工人均佩服他技艺高超。查阅4年来的就诊记录，发现他曾被擦伤手臂33次，估计无伤害、轻微伤害与严重伤害的比例为1 200∶33∶1。

海因里希法则是根据同类事故的统计资料得到的结果，实际上不同种类的事故这个比例是不相同的。日本学者青岛贤司的调查表明，日本重型机械和材料工业的重、轻伤之比为1∶8，而轻工业则为1∶32。美国也有按事故类型分类进行的统计，如表2-1。而同一企业中不同的生产作业，这个比例也会有所差异。表2-2为我国某钢铁公司1951～1981年间各类伤亡事故的比例。

表2-1　事故类型及伤害严重度

事故类型	暂时丧失劳动能力比例/%	部分丧失劳动能力比例/%	完全丧失劳动能力比例/%
运　　输	24.3	20.9	5.6
坠　　落	18.1	16.2	15.9
物体打击	10.4	8.4	18.1
机　　械	11.9	25.0	9.1
车　　辆	8.5	8.4	23.0
手工工具	8.1	7.8	1.1
电　　气	3.5	2.5	13.4
其　　他	15.2	10.8	13.8

表2-2　某钢铁公司伤亡事故情况

部　　门	死亡人数/人	重伤比例/%	轻伤人数/人
钢铁焦化	1	2.25	138
工矿企业	1	3.48	197
机械铸造	1	4.44	408
原 材 料	1	6.89	430
运　　输	1	1.76	73
采　　矿	1	1.89	91

海因里希法则阐明了事故发生频率与伤害严重程度之间的普遍规律，即一般情况下，事故发生后造成严重伤害的可能性是很小的，大量发生的是轻微伤害或者无伤害，这也是为什么人们容易忽视安全问题的主要原因之一。

在另一方面，海因里希法则也指出，未遂事故虽然没有造成人身伤害和经济损失，但由于其发生的原因和发展的过程极可能造成严重伤害，因而我们必须对其进行深入研究，探讨其发生原因和发展规律，从而采取相应的措施，消除事件原因或斩断事件发展过程，达到控制和预防事件的目的。也就是说，根据海因里希法则，在同类事件中未遂事故和轻伤事故发生的可能性要比严重伤害事故大得多，只要我们关注未遂事故，研究未遂事故，就有可能控制严重伤害事故的发生，这也是事故控制的重要手段之一。对于一些未知因素较多的系统，如采用新技术、新设备、新工艺、新材料、新产品等的系统更是如此。日本曾经掀起的“消灭300”运动，其目的正在于此。美国有关学者也曾进行过类似的研究，他们

在某企业对两组执行同样操作的员工做了一次对比试验，对其中的甲组进行正常管理，对乙组则要求及时上报未遂事故，经专家分析后采取相应措施。一年后的统计数据表明，乙组的事故率比甲组有明显的降低。

当然，研究未遂事故也有很多困难，其一，也是最主要的问题，就是人们对其不重视。只要事故的发生没有造成严重后果，许多人认为只是虚惊了一场，未遂事故之后我行我素，依然如故，员工如此，管理层如此，政府部门也是如此。其二，未遂事故数量庞大，对其进行调查、统计、分析研究需要投入大量的人力、物力，在有些情况下，这种投入是令人难以承受的。其三，未遂事故的界定困难。在大量的各类突发事件中，哪些属于未遂事故，在有些情况下是模糊的，对它的界定会因人们理解的程序，观察事物的角度的不同而有所不同。其四、因为我们只关心那些可能会造成严重事故的未遂事故，但在大量的未遂事故中筛选出这类事故，要依赖于人的经验和直觉。

第二节　危险源、危险因素、有害因素、不安全因素、事故隐患

危险源（hazard）是可能导致人身伤害和（或）健康损害的根源、状态或行为。

危险源的概念源自于现代安全科学的系统安全的发展。系统安全是事故致因理论发展至今的最新成果，也是安全科学所提出的用于指导事故控制的最新理论和方法。

事故致因理论是研究分析导致事故发生原因因素的科学理论。系统中可能导致事故发生的原因因素被称之为事故致因因素（accident-causing factor）。随着人类社会生产的发展，事故致因理论也经历了其发展的不同阶段。

系统安全认为，世界上不存在绝对安全的事物，任何人类活动中都存在可能导致事故的因素，系统中可能导致事故发生的因素在系统安全中被称作危险源（hazard）。

系统中所有的事故致因因素在系统安全中都被视作危险源，正如威廉汉姆（Willie Hammer）将危险源定义为可能导致人员伤亡或财产损失的条件（condition）。初期的系统安全只是将系统中可能导致事故发生的各种因素都作为危险源去考虑，并没有将危险源与其他相关的事故致因理论加以联系，深入分析危险源的基本概念，对危险源进行分类。随着安全科学技术的发展，基于事故致因理论，各种涉及危险源的基本概念及分类的理论被提出。

国外学者不倾向于对危险源进行分类，他们把生产作业场所中包含某种能量、可能导致某种事故的单元作为危险源，在对危险源实施评价和控制时进一步识别单元内和与单元相关联的更具体的事故致因因素（也可以称作危险源）。

国内学者基于事故致因因素在事故发生发展过程中的作用，提出了两类危险源和三类危险源的理论。

我国的安全生产法规，基于我国实际的安全生产管理实践，将相关的事故致因因素表述为“危险因素”、“有害因素”、“不安全因素”、“事故隐患”等。这些术语概念被日常地应用到我国具体的安全生产实践活动中。

尽管上述这些危险源理论和涉及的相关概念，都是基于不同的角度和目的提出的，但涉及同一专业方面出现过多的理论和概念，如果不加以诠释，就会使得系统安全理论的学习和应用变得复杂起来。