普通高等教育“十一五”国家级规划教材

系统安全工程

樊运晓　罗　云　编著

化学工业出版社

普通高等教育“十一五”国家级规划教材

系统安全工程

樊运晓　罗　云　编著

化学工业出版社

·北京·

本书以生命周期为时间序列，以危险辨识—危险分析—风险评价—危险控制为空间序列介绍系统安全分析方法，方法强调其产生发展过程、适用条件、应用优势及局限性。全书共十一章，其中第一章是绪论，介绍这门学科的发展、基本概念及研究内容；第二章是针对危险的类型、辨识方法以及重大危险源作以介绍，它是后面章节危险分析的基础。第三至八章是基本的危险分析方法，第九章和第十章分别介绍常用的危险分析和风险评价方法，第十一章是基于生命周期的概念对前面各种分析方法应用的模拟实践。本教材适用于安全工程专业及其他相关专业的本科教学，也可作为广大安全工程教学与研究工作者和从事生产安全实践工作者的参考读本。

图书在版编目（CIP）数据

系统安全工程/樊运晓，罗云编著．—北京：化学工业出版社，2009.1
普通高等教育“十一五”国家级规划教材
ISBN 978-7-122-04035-0

Ⅰ．系… Ⅱ．①樊…②罗… Ⅲ．安全工程-高等学校-教材 Ⅳ．X93

中国版本图书馆 CIP 数据核字（2008）第 180544 号

责任编辑：满悦芝　　装帧设计：关　飞
责任校对：宋　玮

出版发行：化学工业出版社（北京市东城区青年湖南街 13 号　邮政编码 100011）
印　　装：三河市延风印装厂
720mm×1000mm　1/16　印张 16¼　字数 329 千字　　2009 年 3 月北京第 1 版第 1 次印刷

购书咨询：010-64518888（传真：010-64519686）　售后服务：010-64518899
网　　址：http://www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　　价：29.80 元

版权所有　违者必究

前　言

安全工程专业在我国是一门新兴专业，短短 20 年的时间已有上百所高校设有此专业，特别是近几年发展势头更是如雨后春笋一般。安全系统工程是该专业重要的专业基础课；《安全工程专业本科教学方案设计研究》对我国 50 余所开设安全工程本科专业院校的专业课程设置情况进行统计分析，安全系统工程课程是开设学校数目最多的一门课程，所占比例高达 72.22%，该课程同时是安全工程专业攻读硕士学位和博士学位入学考试的专业课考试课程，是目前我国注册安全评价师考试的主要课程，同时还是我国注册安全工程师考试的基础课程。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，安全系统工程的应用在生产实践中也为改善我国安全工作的面貌建立了不可磨灭的功勋。但追本溯源，当我们寻找“安全系统工程”的起源时，我们不得不遗憾地发现“安全系统工程”是源于 System Safety Engineering 一词，这一词语的翻译应当是“系统安全工程”，它之所以被译成“安全系统工程”除翻译之外还有一些特定的历史原因，然而其知识体系的确应称为“系统安全工程”。本教材的编写是作者在阅读大量的国外《系统安全工程》教材和国内《安全系统工程》教材及麻省理工学院等著名学府的《系统安全工程》开放课程和有关系统安全培训课件的基础上完成的，教材编写时既注意尊重“系统安全”这门学科本身的发展历程及其知识结构以及对生产安全的指导作用，同时兼顾它在我国的生产实践及应用。

系统安全工程课程本身对实践性要求非常强，其所面对的研究对象是工业工程，在石油、化工、冶金、煤矿、交通、建筑等各行各业都有着普遍的应用。这门学科是理论与实践相结合十分密切的课程；对于各行各业的安全生产都有着技术上的指导意义，现已成为企业用于阻止事故发生、减小事故损失的重要手段。因此，学习这门课程应具备相当的行业基础知识，而该课程面对的学生主要是刚刚修完基础课的大三学生，除了认识实习时能稍稍接触实践以外，学生对行业生产实际状况了解很少，这就为教材编写工作带来很大难度。目前安全工程专业培养的是“通才型”人才，学生在校期间学校培养没有明确的行业倾向，这就要求教师在教学过程中要注重学生对各种危险分析方法的理解，更要注重对学生应用方法能力的培养，教会他们学以致用。因而本教材在编写过程中，例题的选择强调学生熟悉的系统、从学生身边的问题或运用基础课知识就能解决的问题出发，培养学生掌握、运用系统安全工程方法的能力。避免因过多说明某项工程背景而冲淡本课程的主题。

“求木之长，必源其根本；欲流之远，必浚其泉源”。系统安全工程知识体系以生命周期为时间序列，以危险辨识—危险分析—风险评价—危险控制为空间序列介绍系统安全分析方法，方法强调其产生发展过程、适用条件及应用优势及局限性，

为了使学生能够较好地理解某个项目或系统基于生命周期各阶段的危险分析，本教材第十一章虚拟某工厂 VCM 项目从研发至项目终止各阶段的危险分析，通过背景资料的描述、分析方法的选择以及分析准备和分析过程的记录等系列环节，一方面使学生理解危险分析如何在生产中贯穿整个项目的生命周期，另一方面也使学生身临其境，通过模拟实践弥补现实教学中学生工程背景欠缺的现象。这部分内容参考自廖学品教授编著的《化学过程危险性分析》，由化学工业出版社出版。

另外，在事故树、因果分析法等内容上，逻辑门符号采用国际上较为统一的表达符号，本教材符号与国外教材及众多分析软件的符号相一致。

本教材在申报普通高等教育“十一五”国家级规划教材时书稿已基本完成，但某些知识体系和知识点包括一些术语的准确定义一直不能令人满意，几年来，在不断学习和教学实践中在这些方面加以调整和完善，最终得到较为满意的结果。作为编著者，我们非常感谢中国地质大学（北京），这门课程从中文讲授到双语教学再到优质课程建设以及精品课程建设，使我们有机会在各方面得以深入研究；感谢中国地质大学（北京）工程技术学院和安全教研室在这门课程的教学中给予我们足够的空间和许多的激励，使我们有机会进行新的尝试。另外我要特别感谢四川大学轻纺与食品学院廖学品教授，我查遍所有可能获得的资源，没有哪个实例能比 VCM 模拟实践更好地说明系统安全工程的内涵，感谢廖教授的辛苦工作以及对本书引用的同意。

我们还要深深感谢教材参考文献的作者，更要感谢那些提供精彩教案、教学培训大纲等而又无法查到姓名的编写者以及 the system safety society 论坛上给予我们众多帮助和热烈讨论的同仁。

作为本书的编著者，我们衷心感谢化学工业出版社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。

我们知道书中一定还有不足之处，真诚地恳请读者朋友给予批评指正。

编著者

2008. 12

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第一章　绪论

第二章　危险辨识

第三章　预先危险分析

第四章　故障模式及影响分析

第五章　危险与可操作性研究

第六章　事故树分析

第七章 事件树分析

第八章 因果分析法

第九章　其他危险分析方法

第十章　其他事故风险评价方法

第十一章　系统安全工程模拟实践

参考文献

第一章 绪 论

当我们打开报纸、电视或网络的时候，时常可以看到各种各样的事故。人类社会随着科技的进步而发展，但科学技术的发展是一面双刃剑，在它给我们带来舒适、便利的同时，也给人类带来了许许多多的事故和灾难。面对事故和灾难，过去人们通常是基于单个事件进行“亡羊补牢”。这种事后型阻止事故发生的安全哲学、安全方法具有滞后性，而系统安全工程就是研究如何针对系统的生命周期采取有计划的、有规律且系统的方法进行危险识别、危险分析和危险控制，从而达到阻止或减少事故目的的一门学科。生产安全的实践推动着系统安全工程的形成与发展。

第一节 系统安全工程发展简史

1947 年 9 月，美国航空业一篇题为《为了安全的工程》的科技论文最先提出了系统安全的概念。作者认为，如同绩效、稳定性和整体结构一样，安全必须融入飞机的设计、建造之中。在制造企业的组织结构中，安全小组也应该像应力组、动力学组和重量组一样重要。系统安全工程得以真正的发展是在 20 世纪 50 年代末 60 年代初。1957 年前苏联发射了第一颗地球人造卫星之后，美国为了赶上空间优势，匆忙地进行导弹技术开发，实行所谓研究、设计、施工齐头并进的方法，由于对系统的可靠性和安全性研究不足，在一年半的时间内连续发生了四次重大事故，每一次都造成了数百万美元的损失，最后不得不全部报废，从头做起。弹道系统的发展需要一种新的方法来测验与武器系统有关的危险，正式、严谨的系统安全方案应运而生，美国空军以系统安全工程的方法研究导弹系统的可靠性和安全性，于 1962 年第一次提出了 BSD-Exhibit-62-41《弹道火箭系统安全工程学》，1963 年，这份文件被修改形成空军规范 MIL-S-38130，即《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》，这对以后发展多弹头火箭的成功创造了条件；1966 年 6 月美国国防部将其做了微小改动，采用了空军的安全标准，制订了 MIL-S-38130A。1969 年，这个规范被进一步修改，形成美国军标 MIL-STD-882《系统及相关子系统和设备的系统安全方案》，在这项标准中首次奠定了系统安全工程的概念以及设计、分析等基本原则。该标准起初是针对美国国防部的要求，后来适用于所有系统和产品。该标准于 1977 年、1984 年、1993 年及 2000 年分别进行了四次修订，标准号分别为 MIL-STD-882A、MIL-STD-882B、MIL-STD-882C 和

此为试读，需要完整PDF请访问：www.ertongbook.com

MIL-STD-882D，前三者标准名称均为《系统安全规划要求》（System Safety Programe Request），2000 版名称为《系统安全实践标准》（Standard Practice for System Safety）。

如同空军逐渐形成了系统安全的要求一样，美国国家航空和宇宙航行局（NASA）也认识到有必要将系统安全作为其管理方案的一部分，空军的成功在于提供了部件或系统的危险以及危险的控制方法等有价值的数据，NASA 的成功则在于推进通过危险辨识、评价和控制的作法来实现系统安全的目的。1965 年，美国波音公司和华盛顿大学在西雅图召开了系统安全工程的专门学术讨论会议，以波音公司为中心对航空工业开展了安全性、可靠性分析和设计的研究，用在导弹和超音速飞机的安全性评价方面，取得了很好的成果。但是这个新生事物在初创时期，并不能为所有的人接受，由于不重视这个方法以致造成了 1967 年发生的阿波罗宇航员三人被烧死的事故，这次教训使系统安全理论得以提升，陆续推广到航空、航天、核工业、石油、化工等领域。

1964 年，美国道（DOW）化学公司根据化工生产的特点，开发出“火灾、爆炸危险指数评价法”，用于对化工生产装置进行安全评价，该方法历经 6 次修订，到 1993 年已发展到第七版。1974 年，英国帝国化学公司（ICI）蒙德（MOND）部在道化学公司评价方法的基础上，引进了毒性的概念，并发展了某些补偿系数，提出了“蒙德火灾、爆炸、毒性指标”评价方法。

另外，英国以原子能公司为中心，从 20 世纪 60 年代中期开始收集有关核电站故障的数据，对系统的安全性和可靠性问题，采用了概率评价方法，后来进一步推动了定量评价的工作，并设立了系统可靠性服务所和可靠性数据库。它们的任务是收集核电站的设备和装置的故障数据，提供给有关单位。1974 年，美国原子能委员会发表了有关核电站事故评价报告。这项报告是该委员会委托麻省理工学院的拉斯姆逊教授，组织了十几个人，用了两年时间，花了 300 万美元完成的，称作“拉氏报告”，即 WASH-1400。报告收集了核电站各个部位历年发生的故障及其概率，采用了事件树及事故树的分析方法，做出了核电站的安全性评价。这个报告发表后，引起了世界各国同行的关注。后来，美国原子能委员会又撤消了这份报告，但在 1979 年美国发生三里岛核电站放射性物质泄露事故后，总统组织的调查委员会重新认定 WASH-1400 的分析方法是正确的。

日本引进系统安全工程的方法虽为时稍晚，但发展很快。自 1971 年召开“可靠性、安全性学术讨论会”以来，几十年来在电子、宇航、航空、铁路、公路、原子能、化工、冶金等领域，该方法研究十分活跃。

当前，系统安全工程已普遍引起了各国的重视，国际系统安全工程学会每两年举办一次年会。1983 年在美国休斯敦召开第六次会议，参加国有四十多个，讨论议题涉及广泛，可以看出这门学科越来越引起人们的兴趣。

1981 年，原国家劳动总局科技人员了解到国外关于“系统安全”思想的介绍时，出于本身的专业敏感性，立即对其产生了极其浓厚的兴趣，于是着手翻译一册

较权威的著作《系统安全工程导论》，同时与设在美国的系统安全学会国际部（System Safety Society International）建立了联系，陆续得到了该学会提供的部分资料和信息。只是由于我国的经济基础较差，以及其他的一些原因，使得当时“系统安全”在我国的进展受到一定制约，但国内诸多科研单位与大专院校对“系统安全”十分关注，并在各个行业领域进行了大胆的尝试，这些研究也引起了许多大中型生产经营单位和行业管理部门的高度重视。但随着时间的推移，由于特殊的原因，系统安全工程在我国逐渐用“安全系统工程”代替，尽管名称有所改变，但其在实践中的应用仍在不断发展，特别是对安全评价工作起了很大的促进作用。1987年原机械电子部率先推出了第一个安全评价标准——《机械工厂安全性评价标准》，1991年国家“八五”科技攻关项目就“易燃、易爆、有毒重大危险源辨识、评价技术”方面进行了研究，使安全评价逐渐步入正轨。与此同时，我国安全预评价工作伴随着建设项目“三同时”工作的开展而纵深发展，《安全评价通则》以及各类安全评价导则的出台、安全评价师的资格考试都促进了系统安全工程的理论和实践的进一步发展。

第二节　系统安全工程基本概念

一、系统

系统（System）的定义很多，钱学森的定义为“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”，斋藤嘉博的定义为“由若干部件或子系统相互间有机地结合起来可完成某一功能的综合体”。MIL-STD-882中定义系统为：“系统是不同复杂程度的人员、规程、材料、工具、设备、设施及软件的组合；这些组分在拟定支持的操作环境中整合在一起完成某项给定的任务以实现某项特别的目的或使命。”在MIL-STD-882D中，系统的定义被进一步修改为“为满足既定需求或目标而形成的人员、生产和程序的有机组合”（An integrated composite of people，products，and processes that provide a capability to satisfy a stated need or objective）。

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功能而整合在一起的人员、规程、设备等。不同的行业、不同的岗位、不同的工作，甚至同一工作中不同的人员所面临的系统都各不相同，在生产安全系统中，其共性的要素主要包括人、机、环，如图1-1所示。

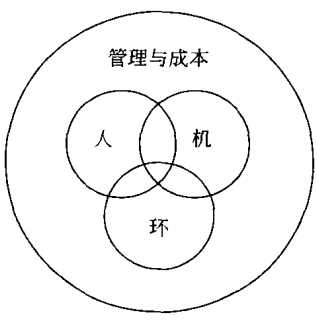

图1-1　生产安全系统要素

在生产安全系统中，“人”不仅指生产操作人员，还包括安全管理人员、安全技术人员、同样还包括厂长、经理等企业的决策层；“机”是指生产过程中使用

的机器、设备，还包括生产设施等；而“环”主要是针对工作环境，如厂房的温度、噪声、粉尘等因素。

生产安全系统三要素间不是孤立的，它们彼此交互，相互依存，通过管理、程序、成本等加以协调。随着科技的进步和发展，要素间的交互日益复杂，许多事故的发生往往在于现代科技不能很好地辨识它们之间的相互作用。在系统安全工程中，谈到系统，必须考虑系统的生命周期。

二、危险与事故

危险（Hazard）是导致人员伤亡或疾病，或导致系统、设备、社会财富损失、损坏或环境破坏的任何真实或潜在的条件（MIL-STD-882D）。事故（Mishap，Accident）是导致人员伤亡或职业病，设备、社会财富损失、损坏或环境破坏的不希望发生的单个或一系列事件（MIL-STD-882D）。危险并不等于事故，它是导致事故的潜在条件；而事故则是已经真实发生了的损失、损坏或伤亡等。危险是事故的前兆，只有在一些触发事件刺激下，危险才可能演变为事故，二者之间的关系见图 1-2。

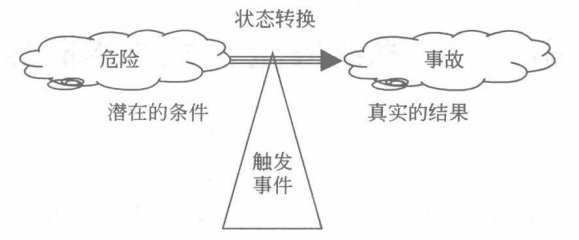

图 1-2　危险与事故关系

（来源：Clifton A. Ericson，Hazard Analysis Techniques for System Safety，John Wiley & Sons，Inc）

危险在一定的条件下转变成为事故，危险与事故就像同一事物的两个对立面，图 1-3 则是对此的一个说明。两个面看上去非常相似，但结果并不相同。

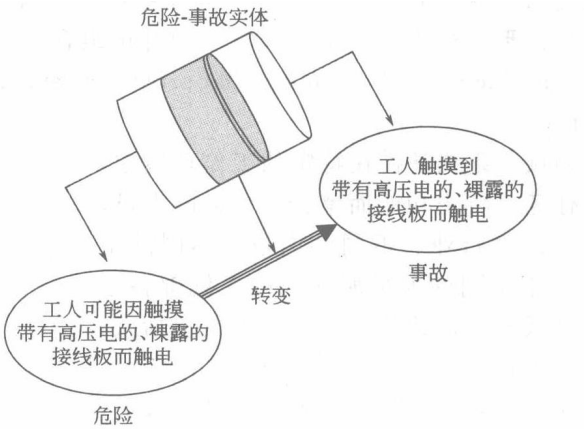

图 1-3　危险与事故，同一实体，不同状态

（来源：Clifton A. Ericson，Hazard Analysis Techniques for System Safety，John Wiley & Sons，Inc）

危险含有危险因素（Hazardous Element，HE）、触发机理（Initiaing Mechanicsm，IM）和威胁目标（Target and Threat，T/T）属性。危险因素属性是促进危险产生的根源，如导致爆炸的危险的能量；触发机理属性是指触发事件导致危险发生，从而将危险转变为事故；威胁目标属性是指人或设备面对伤害、损坏的脆弱性，它反映了事故的严重度。危险的三要素可通过危险三角形表示，见图 1-4，图 1-5 是图 1-3 危险属性的实例，表 1-1 给出几个危险属性的例子。可以看出，当危险的三个属性同时具备时，事故则会发生。

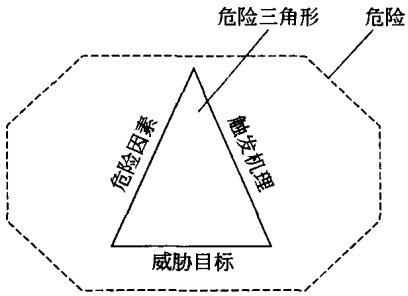

图 1-4　危险三要素图

（来源：Clifton A. Ericson，Hazard Analysis Techniques for System Safety，John Wiley & Sons，Inc）

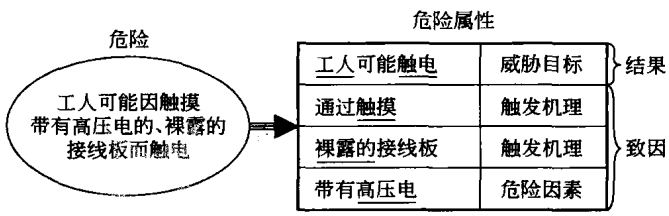

图 1-5　危险属性实例

表 1-1　危险属性实例

危险因素	触发机理	威胁目标
弹药	没有标识；射频能	爆炸，死伤
高压储罐	储罐破裂	爆炸，死伤
燃料	油料泄漏且遇火源	火灾、系统损坏或死伤
高电压	因暴露而触摸	触电，死伤

三、事故风险

谈及风险（Risk），人们可能更多地将这个概念与金融、财务联系在一起，生产安全领域风险的概念与它们是一致的，它所体现的是由于生产过程中的不安全而产生的事故对企业造成的损失，又称为事故风险（Mishap Risk），通过危险演变成事故的发生概率（或可能性）和危险演变事故的事故严重度（或后果）两个维度来表示。MIL-STD-882D 对事故风险的定义如下。

风险是用潜在事故的严重度（Severity）和发生概率（Probability）来表达事故的影响和可能性。

通常人们用 R＝S×P 或 R＝S·P 来表达风险，“×”和“·”是指逻辑相乘，并非真正数学意义上的“相乘”。事故风险的确定会在后面第四节事故风险评估中进一步论述。

事故风险的概念表明：风险是由两个因素确定，既要考虑后果，又要考虑其发生概率。例如乘坐交通工具有出现交通事故的可能，因而说乘坐交通工具有危险，但是乘飞机和乘汽车哪一个风险更小呢？需要从风险两个维度综合比较。由此也说明，风险虽有大小、高低之分，但任何时候风险都不可能为零。因而事故风险的存在具有绝对性。

四、安全

在安全工程领域，安全（Safety）的概念有着众多的描述。在系统安全工程学科中，安全与风险相对，它表明人们对一定事故风险的接受程度。如 MIL-STD-882D 对安全的定义如下：安全是对导致人员伤亡或职业病，或设备、社会财富损坏或环境破坏的条件的认可（Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.）。

例如骑自行车有致使头部受伤的危险，戴上头盔可以减少事故风险，但在我国人们很少见到骑自行车戴头盔的人，这表明我们认为骑自行车不戴头盔的风险是可以接受的，即是安全的。但澳大利亚法律明确规定，行人骑自行车必须戴上头盔。这表明：事故风险的存在是绝对的，而安全只是相对的，它随着国情的不同，企业发展程度的不同而不同。

五、系统安全

系统安全（System Safety）是针对产品、系统、项目或活动的生命周期，应用特殊的技术手段和管理手段，进行系统的、前瞻性的危险辨识与危险控制。美国军标 MIL-STD-882D 中对系统安全定义如下。

针对系统生命周期各个阶段，应用工程和管理的原理、准则以及技术，结合操作效果及适宜性、时间及资金投入等条件约束达到可接受的事故风险水平（The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of the system life cycle.）。

系统安全的概念强调从一个产品、一项工程最初的概念设计阶段开始，直至后续的设计阶段、生产阶段、测试使用，直至其报废、放弃各阶段，始终进行安全分析与危险控制的活动。

过去人们对于安全的认识没有系统的概念，对于安全的认知往往是基于单个事

件或某个部件，对于事故的预防也是基于“亡羊补牢”事后型的预防，图 1-6 就是航天业飞行-处理-再飞行安全方式的一个例子：建造飞机，让它飞行；如果飞机不能工作，则寻找问题所在，然后尝试让它再飞行。这种方式，只有当事故出现时，才进行事故调查，寻找事故的致因，从而确定采取什么样的措施以防止类似事故的发生。尽管对已经存在的系统进行了修改，增加了安全保护措施，甚至制定了相应的安全制度，但这些矫正会使整个系统不得不进行很大的再投入，对先前的投资也许造成巨大的浪费。这种安全方式对整个系统而言是滞后的，而系统安全则具有超前性。

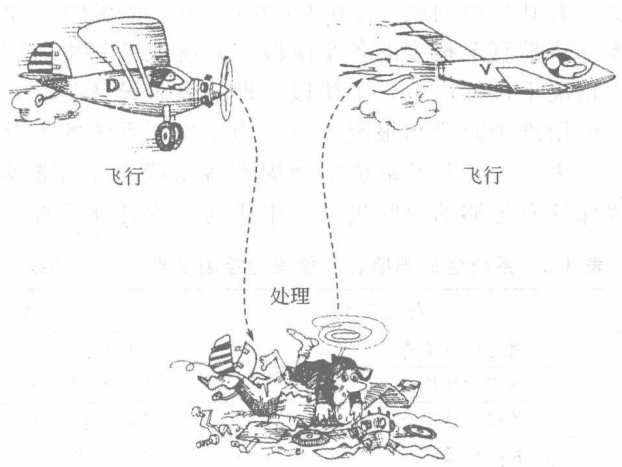

图 1-6　飞行-处理-再飞行安全方式

（来源：Harold E. Roland，Brian Moriarty. System Safety Engineering and Management，New York. Wiley，1983）

系统安全强调在产品或系统真正生产之前已经将可接受的安全要求通过严谨的计划和周密的组织融入在设计之中。在事故或损失还没有产生之前通过系统的危险辨识和评价而加以控制。只有这些危险被消除或控制在可接受的水平内才可能进一步进行研发、测试、使用或维修，因而所有的改正措施也都是在事故或损失发生前就进行的。当然这些措施不仅包括工程的手段，也还包括管理手段。

系统安全的目的就是通过危险辨识，减小危险的技术方法，以保护人员、系统、设备和环境免于危险的影响。其基本目标在于消除可能导致人员伤亡或职业病、系统损坏或环境破坏的危险。如果这些危险最终不能被消除，则采取控制措施尽可能减小其风险。当然另一基本目标则是尽可能在产品或系统的生命周期早期阶段完成危险辨识和控制，以保证最小的投入和最大的效益。

六、系统安全工程

MIL-STD-882D 定义系统安全工程（System Safety Engineering）为运用理学和工学原理、准则及技术，采用专门的专业知识和技术进行危险辨识和危险控制，以减少相关事故风险的一门工程学学科（An engineering discipline that employs

此为试读，需要完整PDF请访问：www.ertongbook.com