新编安全工程专业系列教材

安全系统工程

Anquan Xitong Gongcheng

主　编 / 吕　品　王洪德
主　审 / 沈斐敏　孙建华

中国矿业大学出版社
China University of Mining and Technology Press

新编安全工程专业系列教材

安全系统工程

主　编　吕　品　王洪德
副主编　魏春荣　彭　伟
主　审　沈斐敏　孙建华

中国矿业大学出版社

内 容 提 要

本书是《新编安全工程专业系列教材》之一，是安全工程专业必修的专业基础课程教材。全书系统地介绍了安全系统工程的基本概念以及安全系统工程研究对象、目的、内容和方法，内容包括：绪论；系统安全分析；事故树分析；危险、有害因素及危险源辨识；系统安全评价；系统安全预测；系统危险的控制。

本书主要供全国高等院校安全工程专业教学使用，也可供安全工程技术人员和企业安全生产管理部门相关人员参考。

图书在版编目(CIP)数据

安全系统工程/吕品，王洪德主编. —徐州：中国矿业大学出版社，2012.5

新编安全工程专业系列教材

ISBN 978-7-5646-1111-8

Ⅰ.①安… Ⅱ.①吕…②王… Ⅲ.①安全系统工程—教材 Ⅳ.①X913.4

中国版本图书馆 CIP 数据核字(2011)第 130347 号

书　　名　安全系统工程
主　　编　吕　品　王洪德
责任编辑　陈红梅
出版发行　中国矿业大学出版社有限责任公司
（江苏省徐州市解放南路　邮编 221008）
营销热线　(0516)83885307　83884995
出版服务　(0516)83885767　83884920
网　　址　http://www.cumtp.com　**E-mail**：cumtpvip@cumtp.com
印　　刷　徐州中矿大印发科技有限公司
开　　本　787×1092　1/16　**印张** 19.25　**字数** 477 千字
版次印次　2012 年 5 月第 1 版　2012 年 5 月第 1 次印刷
定　　价　36.00 元

《新编安全工程专业系列教材》
编审委员会

前　言

本书是全国高等院校安全工程专业“安全系统工程”必修课程的统编教材。

本书编写工作是在全国安全工程专业教学指导委员会直接领导下进行的，从教材大纲的编制、审定及相关内容划定，均由《新编安全工程专业系列教材》编审委员会反复讨论完成。我们严格遵照大纲的规定与要求，结合近年来的教学、实践与研究工作，编写了这本《安全系统工程》教材。

本书在编写过程中，力争做到选材内容新颖，充分反映近年来国内外安全科学领域最新技术发展；力求做到教材内容体系的完整性和条理性，教材内容少而精，深入浅出；注重以传授基础理论和基本知识为主，并适当阐述典型的应用技术，以求理论与实践相结合，以便学生理解和自学，有利于培养学生分析问题和解决问题的能力。

福州大学沈斐敏教授和黑龙江科技学院孙建华教授分别对书稿进行了审定，提出了许多宝贵的意见和建议，并对其结构体系和文字内容进行了细致的修改，这对提高书稿质量起到重要保证作用，在此表示衷心谢意。

本书具体编写分工如下：第 1 章绪论，由安徽理工大学吕品、彭伟共同编写；第 2 章系统安全分析，由大连交通大学王洪德编写；第 3 章事故树分析，由黑龙江科技学院魏春荣编写；第 4 章危险、有害因素及危险源辨识，由安徽理工大学吕品、彭伟共同编写；第 5 章系统安全评价，由山西大同大学姚有利编写；第 6 章系统安全预测，由河南理工大学邓奇根编写；第 7 章系统危险的控制，由安徽理工大学吕品、彭伟及中国劳动关系学院颜峻共同编写。参加本书编写的学校有：安徽理工大学、大连交通大学、黑龙江科技学院、山西大同大学、河南理工大学、中国劳动关系学院。

本书在编写过程中得到了各编写单位所在的学校、院系及教研室各方面的大力支持和帮助，在此特表示感谢。同时，本书编写过程中吸收了以前诸教材的优点，参考和引用了国内外近年来发表的相关科技文献，在此特向文献作者们表示诚挚的感谢。

由于编者水平有限，加之时间紧迫，书中难免存在错误和不妥之处，恳请广大读者不吝指正。

编　者

2012 年 5 月

目　录

1 绪　论

安全是人类生存和发展过程中永恒的主题。系统工程是系统科学中改造世界，并为改造过程中有效解决各种错综复杂的系统性问题而形成的一门综合性技术，它以运筹学、控制论、信息论、系统论中一些具有普遍意义的基本理论为指导，在自然科学、社会科学、工程建设及管理中发挥作用。从最初的系统论到基础科学系统学，再到技术科学，最后发展为系统工程。最近几十年来，许多学者和专家一直在探索将系统工程的理论和原理，运用到安全管理中，并逐步发展为安全系统工程，成为安全学科的重要组成部分。所以，安全系统工程是现代科学发展的一个必然产物，它同时涉及了自然科学和社会科学，既运用了系统论的观点和方法，又结合了工程学原理及有关专业知识来研究生产安全管理和工程，是20世纪60年代迅速发展起来的新兴学科。

1.1 安全系统工程的基本概念

系统工程研究的对象是系统，系统科学的产生与应用促使人们用一个全新的观念来解决生产中的安全问题，即从系统的概念出发，用系统的思想方法来考察和解决生产中的安全问题。

1.1.1 系统

“系统”思想来源于人类长期的社会实践，存在于自然界、人类社会及人类思维描述的各个领域，早已为人们所熟悉。但从科学的角度来看，具有现代涵义的系统概念最早源于美国学者泰勒(F. W. Taylor)出版的《科学管理原理》一书。我国著名科学家钱学森教授曾对系统描述如下：系统是由相互作用和相互依赖的若干组成部分结合的具有特定功能的有机整体。

在美国的《韦氏大辞典》中，“系统”一词被解释为“有组织的或被组织化的整体；结合着的整体所形成的各种概念和原理的结合；由有规则的相互作用、相互依存的形式组成的诸要素集合”。在日本的工业标准(JIS)中，“系统”被定义为“许多组成要素保持有机的秩序向同一目的行动的集合体”。前苏联的大百科全书中定义“系统”为“一些在相互关联与联系之下的要素组成的集合，形成了一定的整体性、统一性”。

今天，人们从各种角度上研究系统，对系统下的定义有几十种。例如：“系统是诸元素及其正常行为的给定集合”，“系统是有组织的和被组织化的全体”，“系统是有联系的物质和过程的集合”，“系统是许多要素保持有机的秩序，向同一目的行动的东西”等，但其基本内涵大致相同。简单地说，所谓“系统”，是指由若干相互联系、相互作用的要素组成的具有特定结构与功能的有机整体。该概念主要包含以下内涵：

第一，系统是由若干要素组成的，要素是构成系统的组分或单元，单一要素不能成为系统，即系统内部具有可分的结构。

第二，系统在于“系”，即系统内要素与要素之间以及要素与系统整体之间存在着相互联系和相互作用，并形成其特定的结构。

第三，系统还在于“统”，即要素彼此之间联系成为一个统一的有机整体。

第四，系统作为一个有机整体对外界环境表现出特定的功能，功能之所以为整体所有，是功能以结构为载体，并在系统诸要素的功能耦合中突现出来。

系统无处不在，辩证唯物主义认为物质世界都是系统，如一个国家、一个企业、一台机器等，大到一望无垠的大海，小到分子、原子核，都可以看做系统。构成系统的要素（也称为元素、因素）本身也可能是系统，其相对于原来的系统来说是子系统。子系统本身又可以由更基本的要素组成，形成一种多级递阶结构。它们之间相互关联，分工合作，以实现整体的特定功能。

1）系统的分类

在自然界和人类社会中，普遍存在着各种不同性质的系统。为了对系统的性质加以研究，需要对系统存在的各种形态进行探讨。按照不同的划分条件，系统主要分成以下几种类型。

（1）按系统的起源分为自然系统和人造系统　自然系统是指自然过程产生的系统。这类系统是自然物（如矿物、植物、动物等）组成的系统，它由自然现象发展而来的，像海洋系统、生态系统等。人造系统是人类按照一定的目的设计和改造而成的，并由人的智能或机械的动力来完成特定目标的系统，如人类对自然物质进行加工，制造出各种机器所构成的各种工程系统。在实际中，大多数系统是自然系统与人造系统的复合系统。

（2）按组成系统的要素存在形态分为实体系统和概念系统　凡是以矿物、生物、机械和人群等实体为构成要素的系统，称为实体系统；凡是由概念、原理、原则、方法、制度、程序等概念性的非物质实体所构成的系统，称为概念系统。在实际中，实体系统和概念系统在多数情况下是结合的，实体系统是概念系统的物质基础，而概念系统往往是实体系统的中枢神经，指导实体系统的行为。

（3）按系统与环境的关系分为开放性系统和封闭性系统　开放系统是指与其环境之间有物质、能量或信息交换的系统。封闭系统则相反，即系统与环境互相隔绝，它们之间没有任何物质、能量和信息交换。值得强调的是，现实世界中没有完全意义上的封闭系统。系统的开放性和封闭性概念不能绝对化，只有作为相对的程度来衡量才比较符合实际。

（4）按系统与时间的依赖关系分为静态系统和动态系统　动态系统就是系统的状态变量随时间变化的系统，即系统的状态变量是时间的函数。静态系统则是表征系统运行规律的数学模型中不含有时间因素，即模型中的变量不随时间变化，它是动态系统的一种极限状态，即处于稳定的系统。大多数系统都是动态系统，但是动态系统中各种参数之间的相互关系是非常复杂的，要找出其中的规律性非常困难。为了简化起见，有时假设系统是静态的或使系统中的参数随时间变化的幅度很小而视同静态的。

（5）按系统被控制类型分为控制系统和行为系统　控制是为了达到某个目的而给对象系统所施加的必要动作。因此，人们把为了实行控制而构成的系统叫做控制系统。当控制系统由控制装置自动进行时，称为自动控制系统。行为系统是以完成目的的行为作为构成要素而形成的系统。所谓行为，是指为了达到某一确定的目的而执行某种特定功能的一种

作用，这种作用能对外部环境产生某些效用。这种系统一般是根据某种运行机制而实现某种特定行为的系统，而不是受某种控制作用而运行的系统。

(6) 按系统包含的范围和复杂程度分为简单系统和复杂系统(大系统) 所谓简单系统，是指有性质相近的若干要素组成的系统，如物资系统等。复杂系统则是由人造系统和自然系统相结合的系统，如企业系统、社会经济系统等。

需要指出的是，系统的形态并不是一成不变的，它是随着人们认识客观世界的深度以及改造客观世界的需要，按照人们提出的分类标准进行划分的。在实际中，这些系统并非是孤立存在的，是相互依存、相互渗透或相互对立的。

2) 系统的特点

(1) 整体性 系统整体性说明，具有独立功能的系统要素以及要素间的相互关系是根据逻辑统一性的要求，协调存在于系统整体之中。也就是说，任何一个要素不能离开整体去研究，要素之间的联系和作用也不能脱离整体去考虑。系统不是各个要素的简单集合，否则它就不会具有作为整体的特定功能。脱离了整体性，要素的机能和要素之间的作用便失去了原有的意义，研究任何事物的单独部分不能得出有关整体性的结论。系统的构成要素和要素的机能、要素间的相互联系要服从系统整体的功能和目的，在整体功能的基础上展开各要素及其相互之间的活动，这种活动的总和形成了系统整体的有机行为。在一个系统整体中，即使每个要素并不都很完善，但它们也可以协调、综合成具有良好功能的系统。相反，即使每个要素都是良好的，但作为整体却不具备某种良好的功能，也就不能称之为完善的系统。系统作为一个整体可以实现远高于各元素各自所具有的功能，并且具有一定的稳定性、动态性和适应性。

(2) 递阶性 系统的划分是相对的，系统是由较小的系统构成的，反过来又是更大系统的一部分，并存在一定的递阶结构(或层次结构)，应根据研究问题的目的进行合理的系统划分。系统递阶结构是系统结构的一种形式，在不同层次结构中，子系统之间的从属关系或相互作用的关系不同，运动形式也不同，从而构成了系统的整体运动特性。

(3) 关联性 组成系统的各子系统之间以及系统中各元素之间有紧密的联系。这些元素及其联系的总和就是系统的结构，元素之间的联系又称为耦合。各元素之间是相互联系、相互影响、相互制约、相互作用的，关联性说明这些联系之间的特定关系和演变规律。

(4) 目的性 任何系统必须具有明确的功能以达到一定的目的，即系统都是为完成某种任务或实现某种目的而发挥其特定功能的。要达到系统的既定目的，就必须赋予系统特定的功能，这就需要在系统的整个生命周期，即系统的规划、设计、试验、制造和使用等阶段，对系统采取最优规划、最优设计、最优控制、最优管理等优化措施。系统的目的决定着系统的基本功能和作用，系统的功能一般是通过同时或顺次完成一系列任务来实现，这些任务完成的结果就达到系统最终的目的。

(5) 有序性 系统有序性主要表现在系统空间结构的层次性和系统发展的时间顺序性。系统可分成若干子系统，而子系统又由若干元素组成，这种系统的分割形式表现为系统空间结构的层次性。另外，系统的生命过程也是有序的，它总是要经历孕育、诞生、发展、成熟、衰老、消亡的过程，这一过程表现为系统发展的有序性。因此，系统的分析、评价、管理都应考虑系统的有序性。

(6) 动态性 系统的动态性表现为两方面：在空间上，系统与环境之间的交互性；在时间上，系统本身从产生、发展、衰退直至消亡有一个动态的变化过程。

(7) 环境适应性　任何一个系统都是在一定的外部物质环境下存在和发展的，它必然要与外界产生物质、能量和信息交换，系统要对这些信息、能量和物质进行转换和加工。外界环境的变化必然会引起系统内部各要素的变化，系统运转的结果又会反过来影响和作用于外部环境，系统是通过与环境的相互作用而实现其功能。不能适应环境变化的系统是没有生命力的，只有能够经常与外界环境保持最优适应状态的系统才是理想系统。

3) 系统的描述

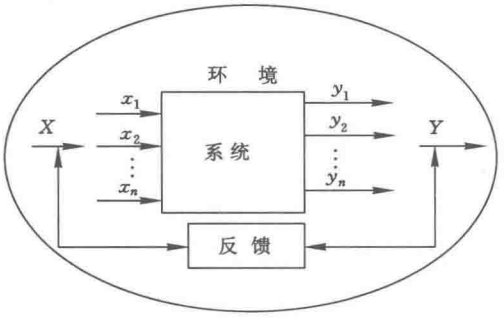

图 1.1　系统的描述

根据系统的定义及特性，可以用框图形式描述系统及其系统功能实现过程，如图 1.1 所示。由图可以看出，描述一个系统应包括 4 部分内容：系统元素，元素间的关系，边界条件，输入及输出的能量、物质、信息。其功能实现过程是外界对系统输入能量、物质和信息，在系统内进行处理，输出新的能量、物质和信息，并利用反馈对系统状态进行有效控制，这个过程是处在一定的环境中，并与环境进行能量、物质和信息交换。例如，安全系统输入安全管理、安全技术等信息，经过系统内部协调处理，输出结果为系统安全状态。这一过程受环境条件的制约，其输出结果有一反馈通道，以控制系统的输入，从而得到较理想的输出。

根据系统输入和输出的作用关系，系统数学模型可表示为：

$$Y = F(X_1, X_2, \cdots, X_i, M) \quad i = 1, \cdots, n$$

式中，$X_1, X_2, \cdots, X_i$ 为输入；M 为环境因素。

由此可得方程组：

$$\begin{aligned} y_1 &= f_1(x_1, x_2, \cdots, x_n, m_1) \\ y_2 &= f_2(x_1, x_2, \cdots, x_n, m_2) \\ &\vdots \\ y_n &= f_n(x_1, x_2, \cdots, x_n, m_n) \end{aligned}$$

可以看出，协调输入 x_i 之间的关系，考虑环境因素 m_i 的影响，并加以控制和改善，这样才能得到理想的输出结果。

1.1.2　系统工程

1) 什么是工程

随着人类文明的发展，人们可以建造出比单一产品更大、更复杂的产品，这些产品不再是结构或功能单一的东西，而是各种各样的所谓“人造系统”(如建筑物、轮船、飞机等)。于是，工程的概念就产生了，并且逐渐发展为一门独立的学科和技艺。

在现代社会中，“工程”一词有广义和狭义之分。就狭义而言，工程被定义为“以某种设想的目标为依据，应用有关的科学知识和技术手段，通过一群人的有组织活动将某个(或某些)现有实体(自然的或人造的)转化为具有预期使用价值的人造产品过程”。就广义而言，工程则被定义为是将自然科学的理论应用到各系统中而形成的各学科的总称，如机械工程、水利工程、化学工程、土木工程、环境工程等。

2) 什么是系统工程

系统工程是系统思想在工程上的实现，是20世纪50年代发展起来的一门新兴科学。它是以系统为研究对象，以现代科学技术为研究手段，以系统最佳化为研究目标的科学技术。如今，系统工程是一门正处于发展阶段的新兴学科，其应用领域十分广阔。由于它是一门与其他学科学相互渗透、相互影响非常密切的边缘学科，不同专业领域的人对它的理解不尽相同，因此要给出一个统一的定义比较困难。下面列举国内外学术和工程界对系统工程的一些定义，为全面认识系统工程这门学科的性质提供参考。

我国著名科学家钱学森教授指出："系统工程学是组织管理系统的规划、研究、设计、制造、试验和使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。"该定义明确指出：系统工程属于工程技术，主要是组织管理的技术，是解决工程活动全过程的工程技术，这种技术具有普遍的实用性。它科学地规划和组织人力、物力和财力，通过最佳方案的选择，使系统在各种约束条件下，达到合理、最经济、最有效的预期目标。

美国著名学者H. 切斯纳特(H. Chestnut)指出："系统工程认为虽然每个系统都由许多不同的特殊功能部分所组成，而这些功能部分之间又存在着相互关系，但是每一个系统都是完整的整体，每一个系统都要求有一个或若干个目标。系统工程则是按照各个目标进行权衡，全面求得最优解(或满意解)的方法，并使各组成部分能够最大限度地互相适应。"

日本学者三浦武雄指出："系统工程与其他工程学不同之处在于它是跨越许多学科的科学，而且是填补这些学科边界空白的边缘科学。因为系统工程的目的是研究系统，而系统不仅涉及工程学的领域，还涉及社会、经济和政治等领域，为了圆满解决这些交叉领域的问题，除了需要某些纵向的专门技术以外，还要有一种技术从横向把它们组织起来，这种横向技术就是系统工程。也就是研究系统所需的思想、技术和理论等体系化的总称。"

系统工程作为一门科学技术，是要改造自然界系统和创造出社会生活各方面人类所需要的系统，正如工程技术一样，系统工程是一类总名称，因体系性质不同还可以再分为门类。

系统工程的出现，为解决系统中的安全问题提供了先进的思想和方法，并在实践中产生了保证系统安全的一门新的科学技术——安全系统工程。

由此可见，系统工程研究对象是大型复杂的人工系统和复合系统；系统工程的研究内容是如何组织协调系统内部各要素的活动，使各要素为实现整体目标发挥适当作用；系统工程的研究目的是如何实现系统整体目标最优化。因此，系统工程是一项技术过程，是特殊的工程技术，是一项管理过程，是一门现代化的组织管理技术，是跨越许多学科的边缘科学。

广义的系统工程是探索、设计、分析、评价系统的统一方法论；狭义的系统工程是在控制论和信息论指导下以实现最优化为核心的各种技巧与方法的总称。

3) 系统工程的特点

(1) 整体性　整体性是系统工程最基本的特点，系统工程把所研究的对象看做一个整体系统，这个整体系统又是由若干部分(要素与子系统)有机结合而成的。因此，系统工程在研制系统时总是从整体性出发，从整体与部分之间相互依赖、相互制约的关系中去揭示系统的特征和规律，从整体最优化出发去实现系统各组成部分的有效运转。

(2) 协调性　用系统工程方法去分析和处理问题时，不仅要考虑部分与部分之间、部分与整体之间的相互关系，而且还要认真地协调它们的关系。因为系统各部分之间、各部分与整体之间的相互关系和作用直接影响到整体系统的性能，协调它们的关系便可提高整体系统的性能。

(3) 综合性　系统工程以大型复杂的人工系统和复合系统为研究对象，这些系统涉及

的因素很多，涉及的学科领域也较为广泛。因此，系统工程必须综合研究各种因素，综合运用，各门学科和技术领域的成就，从整体目标出发使各门学科、各种技术有机地配合，综合运用，以达到整体最优化的目的。如“阿波罗登月计划”，就是综合运用各学科、各领域成就的产物，这样一项复杂而庞大的工程没有采用一种新技术，而完全是综合运用现有科学技术的结果。

(4) 满意性　系统工程是实现系统最优化的组织管理技术，而系统整体性能的最优化则是系统工程所追求并要达到的目的。由于整体性是系统工程最基本的特点，所以系统工程并不追求构成系统的个别部分最优，而是通过协调系统各部分的关系，使系统整体目标达到最优。

1.1.3 安全系统工程的基本定义

1) 什么是安全

安全是人们频繁使用的词汇。“安”字是指不受威胁、没有危险，即所谓无危则安；“全”字是指完满、完整、齐备或指没有伤害、无残缺、无损坏、无损失等，可谓无损则全。安全通常是指免受人员伤害、疾病或死亡，或引起设备、财产破坏或损失的状态。可见，它既涉及人，又涉及物，而且还涉及各种情况下的局部或整体损失。当人们给出约束条件时，该定义也可限定为“人的伤害或死亡”，或者“设备、财产损失”。

目前，对安全还没有形成统一的准确的定义。例如，《职业健康安全管理体系规范》(GB/T 28001—2011)对“安全”定义为：“免除了不可接受的损害风险的状态。”从职业安全与安全工程学的角度来看，安全可以定义为：消除能导致人员伤害、疾病、死亡或引起设备财产的破坏和损失，以及危害环境的条件。

安全所涉及的范畴既有历史问题，又有现代课题。自人类社会诞生起，就存在安全问题。在当前的条件下，关于安全概念的理解可以分为两大类，即绝对的安全观和相对的安全观。绝对安全观认为：安全就是无事故、无危险，指客观存在的系统无导致人员伤亡、疾病，无造成人类财产、生命及环境损失的条件。这一观点在相当长的历史时期内很盛行，目前仍在相当一部分生产管理人员、科研人员和工程技术人员的思想上有着深深的烙印。在早期出版的一些典籍和教科书中，同样表明安全就是“无危险、无风险”的观点。相对安全观认为：安全是指客体或系统对人类造成的可能的危害低于人类所能允许的承受限度的存在状态。美国哈佛大学的劳伦斯教授认为，安全就是被判断为不超过允许限度的危险性，也就是指没有受到伤害或危险，或损害概率低的通常术语。也有人认为：安全是相对于危险而言的，世界上没有绝对的安全。还有学者认为：安全是指在生产、生活过程中，能将人员和财产损失(害)控制在可以接受的水平的状态。也就是说，安全即意味着人员和财产遭受损失(害)的可能性是可以接受的，如果这种可能性超过了可以接受的水平，即被认为是不安全的。目前，这些观点在学术界具有一定的代表性。

2) 什么是安全系统

有了安全和系统的概念，我们对安全系统的概念可表述为：安全系统是以人为中心，由与生产安全问题有关的相互联系、相互作用、相互制约的若干个因素而构成的具有特定功能的有机整体，是生产系统的一个重要组成部分。

从定义可以看出，安全系统具有以下特点：

(1) 安全系统是由与安全有关的影响因素构成的有机体，如操作者、生产设备、安全管理、生产环境等。

(2) 安全系统的目的是实现安全生产。

(3) 安全系统是生产系统的组成部分,是附于生产之中的。

(4) 安全系统与生产系统中其他子系统相互联系,并贯穿于其他子系统中。

(5) 安全系统总是把环境因素看做是其系统的部分,并受其影响。

在工业企业里,人—机系统、安全技术、职业卫生和安全管理构成了一个安全系统。它除了具有一般系统的特点外,还有自己的结构特点。第一,它是以人为中心的人机匹配、有反馈过程的系统,在系统安全模式中要充分考虑人与机器的互相协调。第二,安全系统是工程系统与社会系统的结合。在系统中处于中心地位的人要受到社会、政治、文化、经济技术和家庭的影响,要考虑以上各方面的因素,系统的安全控制才能更为有效。第三,安全事故(系统的不安全状态)的发生具有随机性,首先是事故的发生与否呈现出不确定性,其次是事故发生后将造成什么样的后果在事先不可能确切得知。第四,事故识别的模糊性。安全系统中存在一些无法进行定量的描述的因素,对系统安全状态的描述无法达到明确的量化。安全系统工程活动要根据以上这些特点来开展研究工作,寻求处理安全问题的最佳解决方案。

3) 什么是安全系统工程

安全系统工程是系统工程学的一个重要分支,是一门涉及自然科学和社会科学的横断科学,是现代科技发展的必然产物。安全系统工程是应用系统工程学的原理和方法预先对研究对象中的危险进行辨识、分析、评价与控制,协调安全系统中各部分之间的关系,使系统安全性达到预期目标的工程技术。它是研究系统安全和系统的设计、工程技术手段以及管理方法的技术科学,又称为安全系统方法、安全系统科学等。

根据以上定义,安全系统工程的内涵如下:

(1) 安全系统工程是系统工程在安全中的应用,其理论基础是安全科学与系统科学,如预测技术、可靠性工程、人机工程、职业卫生学、行为科学、系统论、控制论、信息论、运筹学、优化理论等。

(2) 对系统危险因素进行辨识、分析、评价、预测和控制是安全系统工程的核心内容。

(3) 安全工程是一门综合性的边缘学科,追求的是整个系统或系统运行过程的安全。

(4) 安全系统工程的目的是使系统达到最佳安全状态,也就是在现有技术经济条件下,有效地控制事故,使系统风险在安全指标以下。

安全系统工程为安全工作者提供了一个既能对系统发生事故的可能性进行预测,又能对系统安全性进行定性、定量分析评价的方法,从而为安全决策者提供决策依据,并据此采取相应的安全措施。

1.2 安全系统工程产生与应用

1.2.1 安全系统工程的产生

1) 系统理论的发展

早在古代中国、希腊和罗马的哲学著作中就反映了系统观念。古希腊辩证法奠基人赫拉克利特(前 540—前 480)在《论自然界》一书中说:"世界是包括一切的整体"。古希腊唯物主义者德谟克利特(前 460—前 370)曾著有《宇宙大系统》一书,这是最早采用"系统"一词的著作。古希腊思想家亚里士多德(前 384—前 322),他提出的"整体大于它的各部分的总和"

的论点，是系统基本问题的一种表述，至今仍然正确。亚里士多德给自己的哲学所规定的任务是研究“原因”，要明白每一事物的“为什么”。在他看来，所有事物都有4个方面的原因：一是质料因，即事物由什么东西构成；二是形式因，即事物有什么样的形式结构；三是动力因，即说明什么力量使一定的质料取得一定的形式结构；四是目的因，即事物形成的目的是什么。

公元前6—前5世纪，我国春秋末期思想家老子强调自然界的统一性，在《老子》书中指出“天下万物生于有，有生于无”。南宋陈亮(1143—1194)的理一分殊思想，称理一为天地万物的理的整体，分殊是这个整体中每一事物的功能，试图从整体角度说明部分与整体的关系。

古代朴素唯物主义哲学思想虽然强调对自然界整体性、统一性的认识，却缺乏对这一整体各个细节的认识能力，因而对整体性和统一性的认识也是不完全的。恩格斯在《自然辩证法》中指出：“在希腊人那里——正因为他们还没有进步到对自然界的解剖、分析——自然界还被当做整体、从总的方面来观察。自然现象的总的联系还没有在细节上得到证明，这种联系在希腊人那里是直接观察的结果。这是希腊哲学的缺陷所在，由于这种缺陷，它后来不得不向其他的观点让步”。[①] 对自然界这个统一体各个细节的认识，这是近代自然科学的任务。

15世纪下半叶，近代科学开始兴起，力学、天文学、物理学、化学、生物学等科目从混为一体的哲学中分离出来，获得日益迅速的发展。研究自然界的方法主要是分析方法，包括实验、解剖和观察，把事物分成各个独立的部分，分门别类孤立地进行研究。这种方法对当时的自然科学的发展起过积极的作用。19世纪下半叶，自然科学已取得了伟大成就。特别是能量转化、细胞和进化论的发现，揭示了客观世界的普遍联系。这个世纪自然科学为马克思主义哲学提供了丰富的材料，系统观成了辩证唯物主义世界观的组成部分。

1945年3月，贝塔朗菲在德国《“哲学”周刊》第十八期发表了《关于普遍系统论》，他在文章中首次阐述系统论概念。他指出：“存在着适用于综合系统或子系统的模式、原则和规律，而不论其具体种类、组成部分的性质和它们之间的‘力’的情况如何，我们提出了一门称为一般系统论的新学科。一般系统论乃是逻辑和数学的领域，它的任务是确立适用于‘系统’的一般原则。”这时系统论才作为一门新兴学科得到当时科学界人士的确认。1968年3月，贝塔朗菲发表了《普通系统论的基础、发展和应用》一书，进一步阐述了系统论的基本概念、原理、范畴、体系及其微分方程的描述方式，是一部比较全面地论述系统论的完整著作。

系统科学是在自然科学、数学科学和社会科学3大部门之外正在形成的一个新的科学技术部门。按照我国科学家钱学森的观点，系统科学包含：工程技术——系统工程；技术科学——运筹学、控制论和信息论；基础科学——系统学；又从系统学通过一座桥梁——系统观，达到人类知识的最高概括——马克思主义哲学。所以，系统科学体系可以表达为：工程技术、技术科学、基础科学和哲学4个台阶，系统科学的建立必将极大加强人类直接改造客观世界的能力，促进科学技术与经济的发展。

2）安全系统工程的发展

科学技术的进步、生产的发展，提高了生产力，促进了社会的发展。然而，在技术进步和生产发展的同时，也会产生许多威胁人类安全与健康的问题，如生产过程中所造成的事故给

① 《马克思恩格斯全集》第九卷，第438页，北京：人民出版社，2009年版。

人类带来不幸和灾难，制约了经济发展和社会进步。另一方面，事故的发生也有积极的一面。首先，事故具有反面教育意义，事故向人们展示了事故造成的后果和损失，给予人们许多教训，使人们必须按照科学规律办事，保证人们活动的安全性。其次，事故是一种特殊的科学实验。一个系统发生事故，说明该系统存在各种不安全因素，从事故原因分析中我们可以得到无法从实验室中得到的实验数据。人们通过对事故的调查、分析，找出事故原因，研究并采取有效控制事故的措施，改变系统工艺流程、设备、环境等，从而提高系统的安全性。再者，事故也是诞生新的科学技术的催化剂。事故的负面效应对人类产生了巨大冲击作用，从而激发人类更大的决心和毅力去投入更多的力量研究事故。通过对事故资料的收集、整理、分析、研究，一个崭新的自然学科就在人们的努力下诞生了，这就是作用与反作用机制。在科学技术发展的历史上，几乎每一个学科的诞生都离不开事故这种反作用机制的作用。

安全系统工程产生于20世纪60年代初期美、英等发达国家，是现代科学技术发展的必然产物。它的产生和发展与军事工程、尖端技术的紧迫需要密切相连。第二次世界大战期间，德国试验V-1型导弹时，发射11次就失败了10次，事故率高达90.9%。于是，他们请来了数学家和物理学家，进行可靠性研究，这就是安全系统工程的雏形。1957年，前苏联宣布制成了洲际导弹，并把第一颗人造卫星送上了天，这使美国政府大为震惊，为了占领空间优势，美国匆忙地进行导弹技术的开发，采用了规划、设计、研制、试验同时并进的方法，由于对系统的可靠性和安全性研究不足，在导弹系统研发过程中仅仅一年半的时间就连续发生4起重大事故，造成惨重损失，每次都造成了数百万美元的损失，使得研制系统因为安全缺陷而报废，研制计划落空。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、可靠性，并于1962年提出了“弹道导弹系统安全工程”，制定了《武器系统安全标准》，1963年提出了“系统安全程序”。到1967年7月，由美国国防部确认，将该标准提格为美军标准，之后又经2次修订，成为现在的《系统安全程序要求》(MIL-STD-882B)。它以标准的形式规范了美国军事系统的工程项目在招标以及研发过程中对安全性的要求和管理程序、管理方法、管理目标。这就是由事故引发的军事系统的安全系统工程。

化工企业的危险性和化工事故的危害性是众所周知的。随着工业规模的扩大和事故破坏后果的日益严重化，迫使化工企业加倍努力，严格控制事故，特别是化工厂的火灾爆炸事故。为此，美国道化学公司于1964年发表了化工厂“火灾爆炸指数评价法”，俗称道氏法。该方法经过多年的应用，前后修改了6次，出了第七版，并出版了教科书。该方法是以根据化学物质的理化特性确定的物质系数为基础，综合考虑一般工艺过程和特殊工艺过程的危险特性，计算系统火灾爆炸指数，评价系统损失大小，并据此考虑安全措施，修正系统风险指数。之后，英国帝国化学公司在此基础上开发了蒙德评价法，日本提出了岗三法。20世纪70年代日本劳动省发表的评价方法，另辟蹊径，它是以分析与评价、定性评价与定量评价相结合为特点的“化工企业安全评价指南”，亦称为“化工企业六步骤安全评价法”。该评价方法是一种对化工系统的全过程如何进行评价的管理规范。它不仅规定了评价方法、评价技术，也规定了系统生命周期每个阶段用哪种评价方法，如何进行评价等。这就是化工系统的安全系统工程。

20世纪60年代初，美国的一些学者开始将系统工程的原理、方法、步骤等引用到安全工作中，形成了一门安全系统专门学科。用该理论对生产中的安全问题进行了定性和分量的分析，效果非常显著。随着研究的深入，安全系统工程理论还能对系统安全状况进行预测预报，使安全工作有了一个质的飞跃。1961年5月，美国总统宣布实行“阿波罗”登月计划，

其中就采用了系统工程的方法。

20世纪70年代初，日本引进了这一技术，并于1973年创建了综合安全工程研究所，专门进行这方面的研究推广。1971年，自日本科协主持召开可靠性安全性研讨会以来，在电子、宇航、航空、铁路、汽车、原子能、化工、冶金等领域，研究工作十分活跃。为了全面推行安全系统工程的方法，日本政府还颁布了一些法规，规定在一些重要的工业部门从厂址选择、规划、设计、运行、更新、报废各个阶段，都必须运用安全系统工程的方法。

几十年来，世界性安全系统工程的开发已达到相当广泛和深入的地步。美国、英国、法国、德国、加拿大、日本等国家都有相当庞大的科研队伍从事这一学科的研究，发表了大量的文献资料，特别是事故树分析方法的理论发展极快。随着电子计算机技术的发展，安全系统工程已开发许多定性、定量分析的程序，缩短了分析时间。

在我国，安全系统工程研究是从20世纪70年代开始的。天津东方化工厂应用安全系统工程成功地解决了高度危险企业的安全生产问题。1976年我国引进安全系统工程的研究方法，1980年中国科学院组建了系统工程研究所，随后又成立了中国系统工程学会，不少大学设置了该专业课程。1982年7月，劳动人事部在北京主持召开了安全系统工程座谈会，首次组织了全国性的安全系统工程研讨会，后来安全系统工程的研究在全国兴起。安全系统工程在冶金、化工、机械和国防工业等行业得到了迅速发展。20世纪80年代中后期，人们研究的注意力逐渐转移到系统安全评价的理论和方法，开发了多种系统安全评价方法，特别是企业安全评价方法，重点解决了对企业危险程度的评价和企业安全管理水平的评价。目前，在全国范围内安全系统工程的原理和方法已被越来越多的企业所接受、应用，取得了很好的效果；同时，在安全系统工程理论的研究上也取得丰硕的成果。

当前，安全系统工程引起了各国的重视，安全系统工程的应用几乎应用到各个领域。今后一段时间要把推广应用安全系统工程作为安全工作的一项重大改革，使安全工作实现3个转变：从传统安全转到系统安全，即从以经验为主转变到依靠科学；从处理事故转变为预测事故，即从被动转变为主动；从一般事故转变到目标管理，即控制事故。从而可以解决以下几个问题：

(1) 安全机构的工作效率和安全干部的素质进一步提高。

(2) 对潜在的危险源及其危害的分析认识更加符合实际。

(3) 安全生产的物质技术条件进一步改善，设备安全化、安全装置完善化、可靠化，环境无害化。

(4) 避免重复事故的措施更加有效。

(5) 安全标准、制度、法规更加健全。

1.2.2 安全系统工程的特点

为了进一步促进安全系统工程理论和应用的发展，有必要进一步明确其特点。

1) 系统性

无论是系统安全分析、系统安全评价的理论，还是系统安全管理模式和方法的应用都表现了系统性的特点，它从系统的整体出发，综合考虑系统的相关性、环境适应性等特性，始终追求系统总体目标的满意解或可接受解。

2) 预测性

安全系统工程的分析技术和评价技术的应用，无论是定性的还是定量的，都是为了预测系统存在的危险因素和风险水平，是通过这些预测来掌握系统安全状况如何，风险能否接