系 统 安 全 工 程 学

陈喜山　编　著
撒占友　张永亮　梁晓春　岳丽宏　刘　芳　参　编

中国建材工业出版社

图书在版编目（悦陨孕）数据

系统安全工程学/陈喜山主编.—北京：中国建材工业出版社，圆园园员
陨杂月晕 苑-愿园员圆苑-园园园-远

Ⅰ.系… Ⅱ.陈… Ⅲ.安全工程-高等学校-教材 Ⅳ.载怨猿

中国版本图书馆 悦陨孕 数据核字（圆园园员）第 园猿愿园远号

系统安全工程学
陈喜山等编著

出版发行：中国建材工业出版社
地　　址：北京市西城区车公庄大街 远号
邮　　编：员园园园猿缘
经　　销：全国各地新华书店
印　　刷：北京鑫正大印刷有限公司
开　　本：苑愿苑皂皂×员园怨圆皂皂　员/员远
印　　张：员缘.缘
字　　数：猿苑缘千字
版　　次：圆园园员年 员月第 员版
印　　次：圆园园员年 员月第 员次
定　　价：圆苑.园园元

网上书店：http://www.jccbs.com.cn
本书如出现印装质量问题，由我社发行部负责调换。联系电话：（园员园）愿愿猿远怨苑远远

前　言

随着我国现代化建设的不断深入，生产生活中各个方面的安全问题日益显现出来，爆炸事故、火灾事故、交通事故等各行业领域中的事故已经成为我国社会主义现代化建设事业中经常遇到的问题。为了适应我国现代化建设的高速发展，保证社会主义现代化建设持续健康地向前推进，安全科学技术和安全管理理论也随之迅速发展起来。安全工程科学正是在这个大背景下迅速发展的一门新兴学科。系统安全工程学则是安全工程学科重要的基础理论课程之一。

本书是在以往的安全工程专业的授课教案基础上，经整理、调整、充实、提高、编撰而成。全书力求简明翔实，通俗易懂，一方面，要突出土建、交通等方向；另一方面，立足于夯实基础具有较宽厚的安全科学知识面。

本书定名为《系统安全工程学》主要考虑到安全工作都是针对某一特定系统而言的，从逻辑关系上分析应首先有某一特定的系统过程，然后才涉及该系统的安全问题。

本书的系统可靠性分析部分由撒占友同志编写；安全决策部分由张永亮同志编写；梁晓春同志编写了概论部分，同时对书稿进行了整理等工作；其他部分均由陈喜山同志编写；岳丽宏、刘芳同志对本书做了校对等工作。

在本书的编写中，喜获东北大学陈宝智教授的指导和鼓励，在这里表示衷心的感谢！

由于水平有限，书中若出现问题，敬请广大读者和专家给予批评指正。

编者

二〇〇一年 元月

目　　录

圆

员 概　　论

员援员 系统安全工程学的产生与发展

二次世界大战以后，全世界范围内的工业技术有了突飞猛进的发展，生产规模不断扩大，核能、航天、石油、化工、冶金等尖端工业和重工业发展迅速。与此同时，工业生产中发生事故的次数也越来越多，公害也越来越严重，造成了很大的社会问题，亟待解决。

圆园世纪缘园年代末，前苏联发射了第一颗人造地球卫星后，美国为了迎头赶上，随后进行了多次导弹技术的研究与开发。但是，由于仓促上阵准备不足，在短短不到两年的时间里竟连续四次出现重大事故，每次都造成了数以百万计美元的损失，最后只得推倒重来。

圆园世纪远园年代，美国空军总结了前面失败的教训，应用系统工程学的理论和方法研究导弹系统的安全可靠性。员怨远圆年第一次提出了“弹道导弹系统安全工程”的概念，根据其方法和原理制订了严格的“武器系统安全标准”。员怨远苑年，美国国防部采用这一安全标准，制订了代号为酝蕴原杂原猿愿员猿园标准，后来又多次修订，逐步完善并形成了“系统安全程序技术要求”，即酝蕴原杂栽阅原愿愿圆标准，成为了产业界系统安全工程的重要依据。随后系统安全工程的基本方法在化工和其他工业上开始应用，美国道化学公司针对化工厂的火灾爆炸事故的特点开发并不断完善了“火灾爆炸指数安全评价方法”即称道法。

圆园世纪苑园年代，系统安全工程学的基本原理和方法逐步在除军事工业之外的其他工业领域得以广泛应用和进一步完善。围绕原子能工业的安全问题，美国原子能委员会发表的“商用核电站风险评价报告（宰粤杂匀原员源园园）”中成功应用了系统安全分析和评价技术；日本劳工省针对化工生产系统的全过程提出了“六步骤安全评价法”，不仅规定了评价方法和评价技术，同时也规定了生产系统不同阶段的安全评价方法；这期间，在冶金、航空、交通、电子等行业中相继开发出了许多系统安全分析方法和评价方法。系统安全工程学的基本原理和分析方法在各行各业开始全面应用。

圆园世纪愿园年代以来，系统安全工程学在世界各国得到广泛重视，国际性学术组织得以发展壮大，出版了许多专著。研究工作逐渐从被动应用其他领域的成果转移到系统安全基本理论和方法研究方面。员怨愿缘年在美国（休斯敦）

召开的第六届国际学术大会上就有 30多个地区和国家的代表参加，议题涉及国民经济的各行各业。

我国系统安全工程的应用于 20世纪 80年代初开始起步，相继成立了相关的学术组织，以系统安全工程为中心，开展开发研究和推广应用等工作。目前，各行各业积极推广应用系统安全工程学的原理和方法，取得了可喜成果。全国有 50所高校增设了安全工程本科专业、硕士点和博士点。这些都为普及和推广系统安全工程学知识、推进现代安全管理创造了有利条件，同时也为创新出适合我国各行业实际的系统安全工程学的理论和方法打下良好基础。

2.2 系统安全工程学的基本概念

系统安全工程学是 20世纪中期随着世界经济的发展而发展起来的一门新兴学科，是以系统工程的方法研究和解决工业生产过程中安全问题，运用现代科学和技术手段辨识、控制和消除系统中的危险源，实现系统安全的新学科。在弄清什么是系统安全工程学之前应首先弄清有关的基本概念。

2.2.1 系统、系统工程

系统是由相互作用、相互依赖的若干部分组合而成的具有特定功能的有机整体。

系统无处不在，如由若干个零部件组成的可以完成特定作业的机器设备，由传动、行走等部分组成的车辆，由处室、车间、班组及作业单元组成的工厂，甚至于由星系组成的整个宇宙都是一个系统。

系统应具有如下的基本特征，否则便不称其为系统：

(1) 具有整体性

系统是能够相互区别的各个部分组成的整体，各个部分都要服从于实现整体最优目标的需要。

(2) 具有层次性

一个系统可分成许许多多小的部分，这些小的部分本身也是一个有机的整体，具有一定的功能，是原系统的子系统。而子系统又可分成更小的子系统，一直分到不能再分为止。例如一个工厂 （系统） 可以分成若干个车间 （子系统），车间又可以分成若干个班组 （子系统） 等。

由于系统的层次性，在系统安全分析时可以把系统分为若干子系统进行分析。

(3) 具有目的性

对于整个系统来说,是以完成某种特定的功能,达到某种特定的目标为目的的。

⑶源 具有相关性

系统的相关性是系统内部各部分之间相互联系、相互作用、相互依赖的关系。

⑷缘 具有适应性

系统的适应性是指系统通过自我调节适应环境变化的性质，这种适应是通过与环境间进行的能量、物质和信息的交换来实现的。

⑸述 具有动态性

整个系统和系统中的组成部分都是随着时间的改变而不断改变的，不是一成不变的。

系统工程就是运用系统分析的理论，对系统的规划、研究、设计、制造、试验和使用等各阶段进行有效的组织管理的科学技术方法。系统工程是属于组织管理方面的工程技术，是解决工程活动全过程的工程技术，是具有普遍适应性的工程技术。

员题题题 安全、危险及系统安全

安全是指不发生导致人身伤害、设备或财产损失事故的状态。当某些导致发生上述事故状态的概率是可以接受时，也可视为安全。从工业生产角度上看，安全不仅是人和物不会受到伤害和损失的理想状态，也是满足安全技术指标要求的技术状态。安全工作中还涉及到安全性的概念。安全性是指不发生导致人身伤害、设备或财产损失的可能性，是判断和评价系统安全性能的重要指标。

危险是指导致人身伤害、设备或财产损失的状态。同样，安全工作中还涉及到危险性的概念。所谓的危险性就是表示危险状态发生的可能性。

危险源是指可能导致系统危险状态的不安全因素。任何系统中都不可避免地存在着某些类型的危险源。辨识这些危险源，采取控制或消除措施是系统安全的基本内容。根据危险源的不同性质又分为第一类危险源和第二类危险源。

第一类危险源是指系统中存在的、可能发生意外释放的能量或危险物质的危险源。如爆炸物、有毒有害物质、电力设备、运动车辆等。

第二类危险源是指导致系统中约束、限制能量或有害物质的屏蔽措施失效或破坏的各种不安全因素的危险源。它包括人、物、环境三方面的因素。如人的误操作、防护设施失效、环境温度过高等。

可靠性是指系统在特定的条件下，在规定的时间内完成规定功能的性能，是判断和评价系统性能的重要指标。系统由于可靠性差而不能完成规定功能的现象称为故障。

系统安全是指人们为解决复杂系统的安全性问题而开发、研究的安全理

论、原则和方法体系，是在所研究的系统寿命期间内辨识系统中的危险源并采取控制措施使其危险性最小，从而使该系统在规定的性能、时间和成本范围内达到最佳的安全程度。

员圆圆猿 系统安全的观念

(员) 没有绝对的安全

安全是相对的,危险是绝对的。任何事物中都包含有不安全的因素,具有一定的危险性,安全只是一个相对的概念。从此种意义上讲,安全又可以理解为没有超出允许限度的危险。这一允许限度是人们用来判断安全与危险的分界线。

(圆) 安全工作贯穿于系统存在的始终

安全工作贯穿于系统寿命的全过程，是系统安全的基本原则和重要特征。它充分体现了“安全第一，预防为主”的安全工作总方针。在新系统的构思、论证、设计、建造、运行、维护以及直到废弃的各个阶段都要辨识、评价和预防控制系统中的危险源。

(猿) 危险源及危险性的认识

根据道格拉斯的系统安全的三命题，关于危险源及危险性的认识主要有以下三方面：

员 在某一系统中不可能彻底地消除一切危险源和危险性；

圆 在某一系统中可以采取措施控制危险源，减少现有危险源的危险性；

猿 系统安全是降低系统整体的危险性，而不是只彻底地消除几种选定的危险源及危险性。

(源) 不可靠是不安全的原因

一般来说，系统的不可靠会导致系统的不安全。当系统发生故障时，不仅影响系统功能的实现，而且还会导致发生事故，造成人员伤亡或财产损失。例如，汽车操纵系统失灵会导致汽车失控，造成伤亡事故。

可靠性着眼于保证实现系统的功能，研究故障发生前直到故障发生为止的系统状态；安全性着眼于防止事故的发生，侧重于研究故障发生后对系统的影响。可见二者的连接点是故障，在防止故障的发生方面二者是一致的，密切关联的。通常，在提高系统可靠性的同时，既可以保证实现系统的功能，又可以提高系统的安全性。

员圆猿 系统安全工程学及其主要内容

系统安全工程学是运用科学和工程技术手段辨识、消除或控制系统中的危险源，实现系统安全的科学。系统安全工程的基本任务就是辨识、评价和控制

源

系统的危险源，降低系统的危险性。因此系统安全工程学的主要内容包括了如何辨识危险源，如何评价系统的危险源和危险性，如何控制系统的危险源，降低系统的危险性等方面的任务。

员题提示 危险源辨识

危险源辨识就是发现和识别系统中的危险源，是安全评价、危险源控制、降低系统危险性的基础。只有准确地找出危险源才能准确地对其进行安全评价，才能有效地采取措施控制危险源，降低系统的危险性。危险源的辨识一般有两种方法：

(员 经验对比分析法

它是基于与有关的标准、规范、规程或经验相对比来辨识危险源的方法。由于通常的标准、规范、规程或安全检查表等都是从大量的经验中总结出来的，所以经验对比分析法是一种基于经验的方法，只适用于有以往或类似的经验可供参考的情况。

(圆 系统安全分析法

系统安全分析法是从安全的角度出发，运用系统工程等分析手段，揭示系统中可导致故障或事故的各种因素及相互关系，从而辨识系统危险源。它既可以用于有经验可寻的危险源辨识，也可以用于无经验可寻的危险源辨识。

员题提圆 安全评价

安全评价 (危险性评价) 是对系统中的危险源危险性进行的综合评价。它包括对系统危险源自身危险性评价和对危险源控制效果的评价。前者是采取危险源控制措施的基础；后者是采取危险源控制措施后的效果评价。

员题提猿 危险源控制

危险源控制就是利用工程技术和管理手段控制或消除危险源，防止事故发生、人员伤害和财产损失。

危险源控制技术主要包括防止事故发生的安全技术 (预防技术) 和事故发生后减少或避免损失的安全技术 (应急技术)。

管理手段主要是发挥计划、组织、指挥、协调、控制等功能来控制系统中的人、物和环境因素，有效地控制危险源，减小或降低危险性。

实际安全工作中，危险辨识、安全评价和危险源控制并不是严格分阶段独立进行的，而是相互交叉、相互重叠的。一方面，在辨识危险源时，需要进行安全评价，看其对系统安全性的影响程度；另一方面，进行危险源控制时，要对控制措施的效果进行评价；同时，在采取危险控制措施时又可能带来新的危

险源和危险性，因此又需要进一步进行危险源辨识和安全评价。

思　考　题

1. 系统安全工程学的发展状况如何？
2. 何谓安全？何谓危险？二者关系如何？
3. 何谓系统、系统工程和系统安全工程？
4. 系统安全工程学的主要内容有哪些？
5. 系统安全的基本观念有哪些？
6. 何谓第一类危险源？何谓第二类危险源？

圆 事故的基本概念及统计预测

圆员 事故的基本概念

要学习掌握系统安全工程学的基本原理和方法，首先应了解和掌握伤亡事故的概念和统计方法，它们是系统安全工程学的基础。

圆员员 事故概念

事故是指人们在实现某种意图而进行的生产和生活活动中，突然发生的，违反人们意志的，迫使生产和生活活动暂时或永久停止的意外事件。

根据事故统计规则，伤亡事故是指损失工作日达到或超过 员天的人身伤害或急性中毒的事故。

工伤事故是指在生产过程中发生的伤亡事故。未遂事故是指既没有造成人员伤害，也没有造成财物损失和环境破坏的事故，也称为险兆事故。

失能伤害是指除死亡之外使人体永久或在一定时间内失去某种能力的伤害。分为暂时性失能伤害 (受伤害者或中毒者暂时不能从事原岗位工作的伤害)、永久性部分失能伤害 (受伤害者或中毒者的肢体或某些器官功能不可逆丧失的伤害)、永久性全失能伤害 (受伤害者或中毒者完全残废的伤害)。

圆员圆 事故分类

按事故的性质分为责任事故和非责任事故。责任事故是指本来可以预见、抵御和避免的事故，但由于人为的原因没有采取预防措施从而造成的事故；非责任事故是由于自然灾害造成的事故和由于科技水平所限而无法避免的事故。据统计，责任事故占所发生事故的 怨园豫以上，因此对其应引起足够的认识。

按事故的伤害程度分为轻伤、重伤和死亡。轻伤是指损失工作日低于 员园园豫日的失能伤害；重伤是指损失工作日大于等于 员园园豫日的失能伤害；死亡是指造成死亡的事故。永久性全失能伤害和死亡损失的工作日均为 远园园个。

按事故的严重程度分为轻伤事故、重伤事故和死亡事故。轻伤事故是指只有轻伤，无重伤和死亡的事故；重伤事故是指只有重伤，无死亡的事故；死亡事故是指有死亡的事故。其中，一次事故中死亡 员~圆人的事故称为重大伤亡事故；一次事故中死亡 猿人及超过 猿人的事故称为特大伤亡事故。按事故致伤

原因分为如表 圆员的 圆缘类：

表 圆员 事故的致伤原因分类

序 号	类 别	序 号	类 别	序 号	类 别
员	物体打击	愿	火 灾	员缘	瓦斯爆炸
圆	车辆伤害	怨	高处坠落	员远	锅炉爆炸
猿	机械伤害	员园	坍 塌	员苑	压力容器爆炸
源	起重伤害	员员	冒顶片帮	员愿	其他爆炸
缘	触 电	员圆	透 水	员怨	中毒和窒息
远	淹 溺	员猿	放 炮	圆园	其 他
苑	灼 烫	员源	火药爆炸		

圆园圆园 事故的统计分析

圆园圆园员 事故统计分析的作用及概念

（员）事故统计分析的作用

事故的统计分析就是运用数理统计的方法对事故的数据进行处理、分析，从而研究事故的发生发展规律，明确安全工作的方向。事故的统计分析在安全工作中具有以下的重要作用：

员 可以用以描述一个企业或部门的安全状况；

圆 可以用以作为观察事故发生趋势的依据；

猿 可以用以判断和确定事故发生的范围；

源 可以用以作为探查事故原因的依据；

缘 可以用以作为制定安全措施的依据；

远 可以用以预测未来事故的依据。

早在 圆园世纪 猿园年代美国的工程师海因里希运用事故统计分析方法，在对大量的调查数据进行统计分析后发现了，在同一个人发生的 猿园起同种事故中，猿园起没造成伤害，圆怨起造成了轻微伤害，只有 员起造成了严重伤害的重要结论，即著名的 员颐圆怨颐猿园的法则。这一法则的重要性不在于比例数如何精确，而是说明了事故发生的次数（频率）与伤害程度（严重度）之间的随机关系，即每发生一起严重伤害事故就要有大量的无伤害事故和轻微伤害事故的存在。因此全力以赴防止个人发生同种事故是防止严重伤害的关键。这一统计分析结果为我们提供了安全工作的方向和依据。

愿

(四) 事故统计分析的概念

为了便于理解举一具体例子对事故的统计概念加以说明。表 圆圆中列出了某大型建筑企业两年内各月份的事故次数。

表 圆圆 某大型建筑企业两年内各月份的事故次数

事故次数 / 月份 / 年份	员	圆	猿	源	缘	远	苑	愿	怨	员园	员员	员圆
第一年	远	员员	缘	圆	猿	缘	远	苑	猿	圆	员	源
第二年	苑	源	愿	猿	圆	员	园	源	怨	猿	源	缘

表 圆猿中列出了事故统计的各项参数。

表 圆猿 事故的统计参数

在一个月内发生的事故次数 (c)	事故频数 (f_c)	累计事故频数 ($\sum_{c=0}^{c} f_c$)	事故频率 ($p_c=\frac{f_c}{\sum f_c}$)	累计事故频率 ($\sum_{c=0}^{c} p_c$)
园	员	员	园.园园苑	园.园园苑
员	圆	猿	园.园愿猿	园.园缘圆
圆	猿	远	园.园缘圆	园.园缘圆
猿	源	员园	园.员远苑	园.员远苑
源	源	员源	园.员远苑	园.猿猿源
缘	猿	员苑	园.园缘圆	园.苑愿猿
远	圆	员怨	园.园愿猿	园.怨员苑
苑	圆	圆员	园.园愿猿	园.缘缘圆
愿	员	圆圆	园.园苑远	园.愿远远
怨	员	圆猿	园.园苑远	园.缘愿猿
≥员园	员	圆源	园.园苑远	员.园园园

事故频数 (f_c)，是指在规定的统计范围内某种事故出现的次数 (c)，在本例中是指全年发生 c 次事故的月数 (见表 圆猿中第 圆栏)。事故频数的分布见图 圆员 在某规定值以下某种事故频数之和称为累计事故频数 ($\sum f_c$)，本例中是指事故频数的累计 (见表 圆猿中第 猿栏)。事故频数的累计分布见图 圆圆

事故频率 (p_c)，是指事故频数与被测的所有事故次数之比 (见表 圆猿中第源栏)。在某规定值以下某种事故频率之和称为累计事故频率 ($\sum p_c$)，本例中是指事故频率的累计 (见表 圆猿中第 缘栏)。同样，事故频率和累计事故频率也可以绘制成类似图 圆员和图 圆圆的分布图。

怨