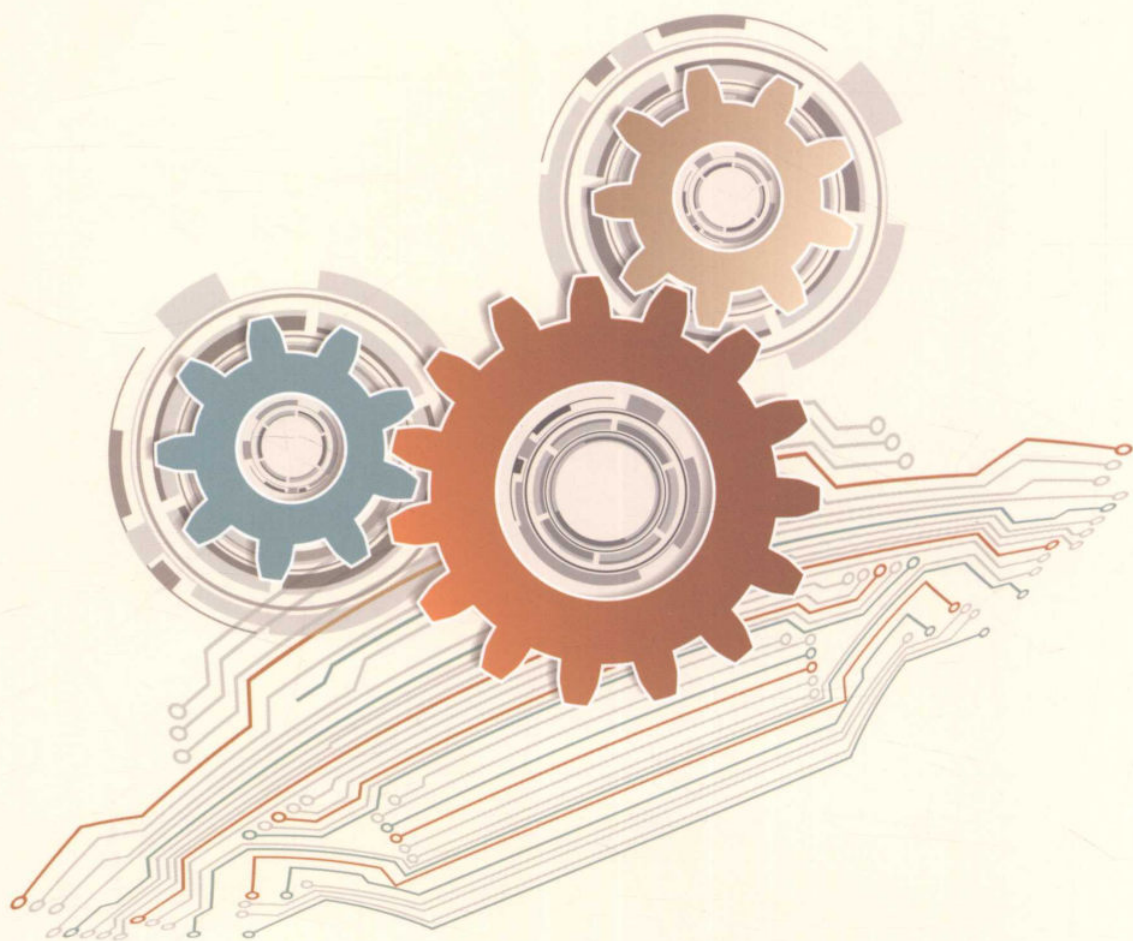


工业自动化技术与应用丛书



工业过程控制及安全技术

王华忠 编 著



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

工业自动化技术与应用丛书

工业过程控制及安全技术

王华忠 编著

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书在阐述安全系统工程基本原理的基础上,以系统化的观点,从功能安全国际标准的安全保护模型出发,全面地阐述和分析了用于工业过程的工业控制系统、工业控制中典型的安全保护策略和功能安全技术在生产安全中的应用,包括本质安全技术、工业报警、故障检测与诊断、常规控制系统的工艺连锁及安全仪表系统的安全连锁,并对相关的技术原理、基本概念、安全完整性等级评估与验证等做了详细介绍。针对工业化与信息化深度融合对工业控制系统安全带来的挑战,本书对工业控制系统信息安全的现状、典型特征、工业控制系统的脆弱性、安全监控与防护、有关标准及安全评估等内容进行了深入介绍,并结合工业控制系统测试床开发实例,分析了测试床在工业控制系统信息安全中的作用。

本书按照安全保护层的结构层次来统领各种安全策略,侧重于对工业控制系统及与工业过程相关的安全技术进行全面、系统和完整的介绍。在内容安排上,既有传统的功能安全知识,又结合了最新的安全仪表系统、工业控制系统信息安全等内容。同时结合实际工程案例剖析相关知识点,有利于培养读者在进行工业过程控制系统设计时必备的安全意识,以及针对工业过程的安全分析、评估和综合实施各类安全策略的能力。

本书可以作为自动化类、安全系统工程、网络空间安全等相关专业大学本科生、研究生的教材,也可以作为工业企业安全技术人员、工业信息安全公司和相关工程设计人员的参考书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

工业过程控制及安全技术 / 王华忠编著. —北京:电子工业出版社, 2020.2
(工业自动化技术与应用丛书)
ISBN 978-7-121-38140-9

I. ①工… II. ①王… III. ①过程控制 IV. ①TP273

中国版本图书馆 CIP 数据核字(2019)第 271252 号

责任编辑:陈韦凯 特约编辑:田学清
印 刷:北京七彩京通数码快印有限公司
装 订:北京七彩京通数码快印有限公司
出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:787×1092 1/16 印张:20.5 字数:525 千字
版 次:2020 年 2 月第 1 版
印 次:2020 年 2 月第 1 次印刷
定 价:69.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888, 88258888。

质量投诉请发邮件至 zltts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式: chenwk@phei.com.cn, (010) 88254441。



前言

工业控制系统在石油、化工、电力、交通、冶金、市政等关键基础设施领域得到了广泛应用，其与企业管理信息系统构成了现代企业的综合自动化系统（IT 与 OT 融合的系统），其中，工业控制系统处于底层核心地位。随着现代工业生产规模不断扩大，工业控制系统的作用越来越重要。提高工业控制系统的可靠性和抗风险能力，确保工业控制系统及其受控过程安全稳定运行一直是安全生产的生命线。

工业控制系统在发展过程中，不断受到各类信息技术的影响，并且与被控的物理过程不断融合，已成为复杂的信息物理融合系统，如“工业 4.0”、工业互联网等新兴工业的生产和制造模式。伴随着互联网+在不同行业的推进，以及物联网应用的爆发式增长，工业控制系统的安全运行面临着巨大的挑战。近年发生的伊朗布什尔核电站和乌克兰电力系统被网络攻击的重大事件使得全球范围内工业生产的安全态势呈现出新的特点。传统的安全问题与新兴的信息安全问题交汇在工业生产及控制中，这导致传统的安全技术和管理手段已经不能满足信息时代的安全需求。在复杂多变的安全形势下，我国已把关键基础设施信息安全上升到国家安全层面，凸显了其重要性和紧迫性。然而，由于工业生产控制与安全技术属于交叉的新兴领域，无论是现有的自动化技术人员、功能安全技术人员，还是信息安全技术人员，都无法独立面对工业化与信息化深度融合给工业生产控制及其安全带来的挑战。当前社会对系统地掌握工业生产控制、工业生产安全、工业信息安全理论与技术的复合型工程技术人才的需求很大，但供给严重不足。各校的控制工程专业为了满足国家对制造业相关控制领域高级工程技术人才的需求，对专业学位研究生的教学培养计划进行了调整，设置了控制、计算机、信息安全等多学科交叉的课程，强化理论与应用相结合。在这个背景下，作者结合自己多年的工业控制系统研究与工程实践经验，以及近年来在功能安全、工业控制系统信息安全领域的科研工作，尝试把相关的知识进行交叉融合，编写了本教材，以满足广大工程技术人员继续教育和相关专业学生的学习需求。

本书分为 6 章。

第 1 章介绍了安全系统工程的基本知识，使得读者能从安全系统工程角度理解工业生产与工业控制中的安全问题。

第 2 章介绍了工业控制系统的相关核心知识，对典型工业控制系统及其应用做了概述性介绍，并从安全保护层的角度出发，概括地介绍了工业生产过程及控制中的一些基本安全策略，包括工业报警、生产控制中的硬保护措施与软保护措施等。

第 3 章介绍了隶属于安全保护层的工业过程故障检测与设备状态监测技术，使读者了解相关的知识及其应用技术。

第 4 章和第 5 章重点介绍了安全保护层中重要的功能安全知识与安全仪表系统，阐述了功能安全的基本概念、安全仪表系统安全完整性等级评估与验证，并通过工程案例介绍了安全仪表系统在过程工业中的应用。

第6章介绍了工业互联时代新的安全问题——工业控制系统信息安全问题，阐述了工业控制系统信息安全的基础知识、工业控制系统漏洞、工业控制系统信息安全标准和工业控制网络安全监控技术等，从而使读者深刻地了解工业控制系统安全问题的本质，掌握提高工业控制系统信息安全的理论和技术，为工业控制系统安全运行保驾护航。

本书注重理论与实践相结合，所用案例都来自实际工业现场。全书内容具有很强的可读性、实用性、学科交叉性和新颖性。

本书可以作为高校自动化类、安全系统工程、网络空间安全等相关专业学生的教学用书，也可以作为工业控制系统安全相关人员的培训教材，还可以作为对工业过程控制及工业过程安全技术感兴趣的读者或技术人员的参考书。通过学习本书，希望读者能够全面了解工业生产过程控制中的基本安全技术及工业安全中的安全评估、安全监测、安全防护技术、安全生命周期等知识，为确保工业生产安全打下系统和扎实的基础。

本书由华东理工大学王华忠主编，南京工业大学吕波参与编写了部分内容。本书的编写得到了德国希马（上海）有限公司蒋卉和张薇薇、中国石化齐鲁分公司功能安全专家张国会等行业专家的支持。本书的出版获得了华东理工大学研究生教育基金的资助，在此一并表示感谢。

本书在编写过程中，除了引用作者多年的工程实践与研究内容，还参考了不少国内外论文、期刊、书籍及互联网上的资料，受篇幅限制，无法将所有参考文献一一列出，在此对这些资料的作者表示由衷的感谢，同时也声明，所参考文献的版权属于原作者。

由于所著内容交叉性强，且受时间和作者水平限制，疏漏在所难免，恳请读者提出批评建议，以便进一步修订完善，作者的E-mail是 hzwang@ecust.edu.cn。

编著者



目 录

第1章 绪论	(1)
1.1 安全系统工程相关概念	(1)
1.1.1 安全与安全标准	(1)
1.1.2 安全系统	(1)
1.1.3 系统工程	(2)
1.1.4 安全系统工程	(2)
1.2 安全系统工程的研究对象、内容与特点	(3)
1.2.1 安全系统工程的研究对象	(3)
1.2.2 安全系统工程的内容	(4)
1.2.3 安全系统工程的特点	(6)
1.3 工业生产安全	(7)
1.3.1 工业生产安全问题	(7)
1.3.2 工业生产安全的主要保障措施	(7)
1.4 本书内容介绍与安排	(8)
复习思考题	(10)
第2章 工业控制系统及其基本安全策略	(11)
2.1 工业控制系统概述	(11)
2.1.1 工业自动化的一般概念	(11)
2.1.2 工业控制系统的体系结构	(13)
2.1.3 工业控制系统的组成	(18)
2.2 工业控制系统的发展及其关键技术	(24)
2.2.1 工业控制系统的发展	(24)
2.2.2 控制装置(控制器)的类型	(29)
2.2.3 工业控制系统人机界面技术	(37)
2.2.4 工业控制系统控制器编程技术及语言规范	(39)
2.2.5 工业控制系统的数据通信及其功能安全	(42)
2.2.6 工业控制系统实时数据交换规范——OPC 与 OPC UA	(44)
2.3 集散控制系统	(48)
2.3.1 集散控制系统概述	(48)
2.3.2 集散控制系统的特点	(49)
2.3.3 集散控制系统的组成	(50)

2.4 监督控制与数据采集 (SCADA) 系统	(57)
2.4.1 SCADA 系统的概述	(57)
2.4.2 SCADA 系统的组成	(58)
2.4.3 SCADA 系统的应用	(61)
2.4.4 SCADA 系统、DCS 与 PLC 的比较	(62)
2.5 工业控制系统的报警功能与报警管理系统	(65)
2.5.1 工业控制系统的报警功能	(65)
2.5.2 工业过程先进报警系统 (AAS) 的功能设计	(69)
2.6 工业生产的安全保护措施与联锁	(71)
2.6.1 工业生产的安全保护措施	(71)
2.6.2 常规控制系统的安全联锁功能	(74)
2.7 工业控制系统电源、接地、防雷与环境适应性	(76)
2.7.1 电源系统设计	(76)
2.7.2 接地系统设计和防雷设计	(77)
2.7.3 环境适应性设计技术	(79)
复习思考题	(81)
第3章 故障检测与诊断	(82)
3.1 故障检测与诊断技术概述	(82)
3.1.1 故障检测与诊断的基础知识	(82)
3.1.2 故障诊断系统的性能指标	(85)
3.1.3 故障诊断方法综述	(86)
3.2 多变量统计故障诊断方法	(95)
3.2.1 主元分析法和偏最小二乘法	(95)
3.2.2 基于主元分析的故障诊断方法	(98)
3.2.3 基于变量贡献图的故障诊断方法	(100)
3.2.4 基于核函数主元分析 (KPCA) 的故障诊断方法	(101)
3.2.5 仿真示例	(104)
3.3 BP 神经网络及其在工业过程故障诊断中的应用	(112)
3.3.1 BP 神经网络基本原理	(112)
3.3.2 BP 神经网络在冷冻机组故障诊断中的应用	(115)
3.4 支持向量机及其在工业过程故障诊断中的应用	(117)
3.4.1 支持向量机原理与分类算法	(117)
3.4.2 支持向量机故障诊断方法原理	(120)
3.4.3 仿真示例	(121)
3.5 多模态工业过程状态监测	(122)
3.5.1 多模态工业过程状态监测概述	(122)
3.5.2 MPCA 及其在间歇过程状态监测中的应用	(123)

3.6 机械设备状态监测与故障诊断	(127)
3.6.1 机械设备状态监测与故障诊断概述	(127)
3.6.2 机械设备状态监测中的信号处理	(131)
复习思考题	(133)
第4章 功能安全与安全仪表系统	(134)
4.1 功能安全基础	(134)
4.1.1 安全功能与功能安全	(134)
4.1.2 危险与风险	(135)
4.1.3 风险评估	(135)
4.1.4 风险降低与保护层模型	(136)
4.1.5 安全完整性等级	(139)
4.1.6 必要的风险降低与 SIL 的关系	(140)
4.1.7 安全生命周期	(141)
4.2 安全仪表系统	(143)
4.2.1 安全仪表系统的概念	(143)
4.2.2 安全仪表系统的分类	(144)
4.2.3 安全仪表系统与基本过程控制系统	(145)
4.2.4 安全仪表系统的安全性与可用性	(147)
4.2.5 安全仪表系统的种类及其特征	(148)
4.2.6 安全仪表系统相关的主要参数	(155)
4.3 风险评估与 SIL 定级	(158)
4.3.1 过程危险分析	(158)
4.3.2 主要的风险分析方法	(158)
4.3.3 安全保护层分析 (LOPA) 与示例	(162)
4.3.4 SIF 的 SIL 确定方法	(164)
4.4 安全仪表系统的结构及其可靠性分析与计算	(167)
4.4.1 安全仪表系统的冗余结构及其定性分析	(167)
4.4.2 安全仪表系统冗余结构的故障树分析	(170)
4.4.3 安全仪表系统冗余结构的可靠性框图分析	(174)
4.4.4 安全仪表系统冗余结构的马尔可夫模型分析	(178)
4.5 安全仪表系统的设计与应用	(183)
4.5.1 安全仪表系统的设计原则	(183)
4.5.2 安全仪表系统的设计步骤	(184)
4.5.3 SIF 的 PFD 计算	(185)
复习思考题	(186)
第5章 安全仪表系统工程案例	(188)
5.1 引言	(188)

5.2	工艺流程概述	(188)
5.2.1	工艺流程	(188)
5.2.2	主要工艺参数	(189)
5.3	废气处理站的安全完整性等级评估	(190)
5.3.1	安全仪表系统的设计流程与风险评估中的参照标准	(190)
5.3.2	废气处理站的安全完整性等级评估	(194)
5.3.3	废气处理站燃烧器节点的 HAZOP	(196)
5.3.4	废气处理站的 LOPA 与 SIL 等级确定	(199)
5.4	废气处理站安全仪表系统的设计与验证	(206)
5.4.1	SIS 安全需求规范	(206)
5.4.2	废气处理站安全仪表系统的 SIF 回路设计	(207)
5.4.3	安全仪表系统的 SIF 验证	(209)
5.5	基于 HIMA 安全仪表产品的废气站安全仪表系统实施	(213)
5.5.1	希马公司的安全仪表产品介绍	(213)
5.5.2	基于 HIMA 安全仪表的废气站安全仪表系统组态	(216)
5.5.3	功能安全管理	(220)
5.5.4	项目实施	(221)
第 6 章	工业控制系统信息安全	(225)
6.1	工业控制系统信息安全问题	(225)
6.1.1	信息安全基础	(225)
6.1.2	工业控制系统信息安全概述	(226)
6.1.3	工业控制系统信息安全与 IT 系统信息安全的比较	(229)
6.2	网络控制协议解析与漏洞分析	(230)
6.2.1	Modbus/TCP 协议解析	(230)
6.2.2	IEC 60870-5-104 远动规约协议解析	(233)
6.2.3	工业控制系统的漏洞及其分析	(236)
6.2.4	工业控制系统的典型通信协议漏洞分析	(240)
6.2.5	网络扫描	(241)
6.3	针对工业控制系统的攻击手段与攻击过程	(242)
6.3.1	针对工业控制系统的攻击手段	(242)
6.3.2	针对工业控制系统的攻击过程	(246)
6.4	工业控制系统的安全监控工具	(248)
6.4.1	协议分析器	(248)
6.4.2	Libpcap 抓包框架	(249)
6.4.3	Snort 入侵检测框架	(250)
6.4.4	Wireshark 分析框架	(253)

6.5 工业控制系统信息安全防护	(256)
6.5.1 工业控制系统的典型架构及其安全防护技术	(256)
6.5.2 主要自动化公司的信息安全解决方案	(261)
6.5.3 电力二次系统安全防护	(268)
6.6 工业控制系统信息安全风险评估	(272)
6.6.1 信息安全风险评估的概念	(272)
6.6.2 典型风险评估方法及其对比	(272)
6.6.3 工业控制系统信息安全风险评估分析	(275)
6.7 工业控制系统信息安全标准	(280)
6.7.1 工业控制系统信息安全相关标准规范的制定历程	(280)
6.7.2 IEC 62443 的主要内容	(281)
6.8 工业控制系统入侵检测	(285)
6.8.1 入侵检测系统的基本原理、分类及评估指标	(285)
6.8.2 常用的入侵检测方法	(289)
6.8.3 工业控制系统入侵检测案例分析	(290)
6.9 一种控制器硬件的环工业控制系统测试床	(301)
6.9.1 测试床的总体结构与通信方案	(301)
6.9.2 测试床的被控物理过程介绍	(302)
6.9.3 测试床开发	(303)
6.9.4 测试床在工业控制系统信息安全中的作用	(313)
复习思考题	(314)
参考文献	(316)

第1章 绪 论

1.1 安全系统工程相关概念

1.1.1 安全与安全标准

一般来说,人们把“安全”和与其矛盾的术语“危险”联系起来。所谓安全,是指免遭不可接受的伤害,或者处于危险发生概率较小以至于可以接受的状态,也指处于一种伤害可接受的状态。安全是动态的,前一刻的安全并不表示后一刻也安全。安全是主观的,对于同一时刻同一事物是安全的还是危险的,不同的人有不同的观点。人们对安全的认知也是随着时间的变化而变化的,过去人们认为是安全的(如一些化工生产工艺),现在就可能认为是危险的。

人们生活的世界充满各种危险(雷击伤害、交通伤害、生产事故、电脑被勒索病毒攻击),这些危险既有自然灾害所造成的,也有人类活动引起的。因此,不存在绝对的安全,人们只能不断努力降低危险发生的概率,以提高安全性;用科学的方法正确理解与对待危险,把各种危险控制在可接受的水平。人们用危险性大小来衡量危险的相对程度,用危险概率和危险严重程度来表示危险可能的后果。危险概率是指危险发生的可能性,一般用单位时间内危险可能出现的次数描述,即危险发生的频度。危险严重程度是对危险造成的后果的评价。

由于安全是一个相对的、主观的概念,因此,评定状态是否安全需要一个标准,即通过与量化的危险概率或危险严重程度比较,从而判断状态是否达到人们可接受或期盼的安全程度,这个标准称为安全标准。当然,安全标准也是相对的,其受技术、资金等条件的制约。确定安全标准的方法有统计法和风险与收益比较法。

1.1.2 安全系统

与安全问题相关的系统称为安全系统。安全系统是以人为中心,由安全工程、卫生工程技术、安全管理、人机工程等几个部分组成的,以消除伤害、疾病、损失,实现安全生产为目标的有机整体,是生产系统的重要组成部分。显然,安全系统是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结合成的具有特定功能的有机整体,这也导致了安全问题是一个复杂的系统工程问题,需要运用系统工程的理论和方法加以解决。

安全系统与一般系统既有共同点,也有其特殊性。

➤ 安全系统是以人为中心的人机匹配、有反馈过程的系统。因此,在系统安全模式中

要充分考虑人、机器与环境的互相协调。

- 安全系统是工程系统与社会系统的结合。在安全系统中处于中心地位的人受到社会、政治、文化、经济技术和家庭的影响，只有考虑以上各方面的因素，系统的安全控制才能更为有效。
- 安全事故（系统的不安全状态）的发生具有随机性。一是，事故的发生与否呈现不确定性；二是，事故发生后将造成什么样的后果事先不可能确切得知。
- 事故识别的模糊性。安全系统存在一些无法进行定量描述的因素，因此对系统安全状态的描述无法达到明确的量化。

针对安全系统，人们要根据以上特点来开展研究工作，寻求处理安全问题的有效方法。

1.1.3 系统工程

系统工程（System Engineering）是在现代化的“大企业”“大工程”“大科学”出现后，产品构造复杂、换代周期短、生产社会化、管理系统化、科学技术既高度分化又高度综合等历史背景下产生的。系统工程是指为了更好地实现系统的目标，对系统的组成要素、组织结构、信息流、控制机构等进行分析与研究的科学方法。它运用各种组织管理技术，使系统的整体与局部之间的关系相互协调和相互配合，实现总体的最优运行。系统工程不同于一般的传统工程，它所研究的对象不限于特定的工程物质对象，而可以是任何一种系统。系统工程是一种对所有系统都具有普遍意义的科学方法，属于工程技术的范畴，主要包括组织管理各类工程的方法论，是组织管理工程、解决系统整体及其全过程优化问题的工程技术。系统工程应用面广，研究安全科学必须与系统工程的理论和技术紧密结合。

系统工程的特点如下。

- 全局观，即把研究对象作为一个整体来分析。分析整体的各个部分之间的相互联系和相互制约关系，使整体的各个部分相互协调配合，服从整体优化要求；在分析局部问题时，应从整体协调的需要出发，选择优化方案，综合评价系统的效果。
- 具有较好的环境适应性。对系统的外部环境和变化规律及其对系统的影响进行分析，使得系统能适应外部环境的变化。
- 定性与定量相结合。综合运用各种科学管理技术和方法，定性分析和定量分析相结合。

1.1.4 安全系统工程

安全系统工程（Safety System Engineering）是以系统危险的形成、分布、转化，以及事故的孕育、产生、发展和终止变化规律为依据，以系统科学、安全科学、信息科学、控制科学、可靠性工程、人机工程等为基础，以安全管理、安全技术和职业健康为载体，对研究对象的风险进行辨识、评价、控制和消除，为安全预测和安全决策提供强有力的依据，以谋求整体安全的新兴学科。简单地说，安全系统工程就是使用系统工程的知识、方法和手段，解决生产中的安全问题，使系统可能发生的事故得到控制，并使系统的安全性达到最佳状态，最终能消除危险，防止灾害，避免损失，保证人身财产安全。它是研究系统安全、系统设计、工程技术手段及管理方法的技术科学。



我们可以从以下四个方面来理解安全系统工程的定义。

- ▶ 安全系统工程的理论基础是安全科学和系统科学，是系统工程在安全学中的应用，同时辅以信息论和控制论等相关学科。
- ▶ 安全系统工程的目标是追求整个系统及其全生命周期的安全。
- ▶ 安全系统工程的研究核心是系统危险因素的识别、分析，系统风险的预测、评价，系统安全预测、决策与事故控制。
- ▶ 安全系统工程的任务是实现最经济、最有效地控制事故和风险防范，最终使风险控制安全指标以下。

1.2 安全系统工程的研究对象、内容与特点

1.2.1 安全系统工程的研究对象

在安全生产领域中，任何一个生产系统都包括三部分内容，即从事生产活动的操作人员、管理人员和设计人员，生产必需的机器设备、厂房、工具等物质条件，以及生产活动所处的环境。安全系统工程同样也包括三部分内容，即人子系统、机器子系统、环境子系统，它们构成了安全系统工程的研究对象。图 1.1 给出了三个子系统之间的关系。

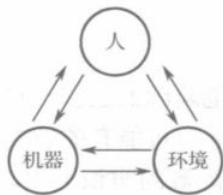


图 1.1 人-机器-环境关系图

1. 人子系统

人子系统的安全与否涉及人的生理因素和心理因素，以及规章制度、规程标准、管理手段、管理方法等是否适合人的特性，是否易于被人们接受；涉及人对机器的适应性及人对环境的适应性。人的行为学作为一门科学，从社会学、人类学、心理学、行为学角度来研究人在生产中的安全性，不仅将人子系统作为系统固定不变的组成部分，还将人看作自尊自爱、有感情、有思想、有主观能动性的人。

2. 机器子系统

对于机器子系统，我们不仅要从材料设备的可靠性角度来考虑安全性，同时还要考虑仪表操作对人提出的要求，以及人体测量学、生理学、心理与生理过程有关参数对仪表和操作部件的设计提出的要求。例如，中央控制室操作台的设计要求包括操作员具有一定的操作控制系统的的能力，如各类报警信号的处理、在紧急情况下的安全停车等；操作台在设计上便

于操作员操作,具备人机友好等特点。

3. 环境子系统

环境子系统考虑环境的理化因素和社会因素,其中环境的理化因素是指噪声、振动、粉尘、有毒气体、射线、光、温度、湿度、压力、热、化学有害物质等;环境的社会因素是指管理体制、工时定额、班组结构、人际关系等。

三个子系统之间相互影响、相互作用的结果是使系统整体的安全性处于某种状态。例如,环境的理化因素影响机器的寿命、精度甚至损坏机器;机器产生的噪声、振动、湿度主要影响人和环境;人的心理状态、生理状态往往是引起错误操作的主要原因;环境的社会因素又会影响人的心理状态,使系统安全具有潜在危险。只有从三个子系统之间的这些关系出发,才能真正解决系统的安全问题。

1.2.2 安全系统工程的内容

安全系统工程专门研究如何用系统工程的原理和方法确保系统安全功能的实现,其内容主要包括危险源辨识和控制、系统安全分析、系统安全评价、系统安全预测、安全决策与措施等。安全系统工程除了研究机械设备的可靠性与安全性,还研究人、材料、环境及人机系统和它们之间的相互作用可能造成的损失,以保护整个系统的稳定运行及人类的自身安全和健康。

1. 危险源辨识和控制

危险源辨识是发现、识别系统中危险源的工作,它是一项非常重要的工作,是危险源控制的基础,只有辨识了危险源之后,才有可能有的放矢地考虑如何采取措施控制危险源。以前,人们主要根据事故经验来进行危险源的辨识工作。20世纪60年代以后,人们根据标准、规范、规程和安全检查表辨识危险源。例如,美国职业安全卫生管理局等安全机构编制、发行了各种安全检查表,用于危险源辨识。

危险源控制主要通过技术手段来实现,包括防止事故发生的安全技术和减少或避免事故损失的安全技术。前者用于约束、限制系统中的能量,防止发生意外的能量释放;后者用于避免或减轻意外释放的能量对人或物的作用。管理也是控制危险源的重要手段,通过一系列的管理活动,控制系统中人的因素、物的因素和环境因素,以便有效地控制危险源。

2. 系统安全分析

系统安全分析是采用系统工程的原理和方法对存在的危险因素进行辨识、分析,并根据需要进行定性或定量描述的一种技术方法。其中,危险源辨识是发现、识别系统中危险因素的重要工作,是控制危险源的基础。通过安全分析,人们可以掌握影响系统安全的危险因素及其对系统安全的影响程度。

目前,系统安全分析有多种多样的形式和方法,我们在使用中应注意每一种安全分析方法都有其自身的特点和局限性,应根据系统的特点和分析的要求,采取不同的分析方法。由于系统的安全性是人、机器、环境等多种因素耦合作用的结果,所以,系统安全分析也可以

是几种方法的综合,以取长补短或相互比较,使得分析结果有一定的科学性和可信性。另外,对现有的分析方法不能生搬硬套,必要时应根据具体情况进行改进。

系统安全分析的主要步骤如下。

- 把所研究的生产过程或作业形态作为一个整体,确定安全目标,系统地提出问题,确定明确的分析范围。
- 将工艺过程或作业形态分成几个单元或环节,绘制流程图,选择评价系统功能的指标或顶端事件。
- 确定终端事件,应用数学模型或图表形式及有关符号,以使系统定型化或数量化;将系统的结构和功能加以抽象化,将其因果关系、层次及逻辑结构变换为图像模型。
- 分析系统的现状及其组成部分,测定与诊断可能发生的事故的危险性、灾害后果,分析并确定导致危险的各个事件的发生条件及其相互关系,建立数学模型或进行数学模拟。
- 对已建立的系统,综合采用概率论、数理统计、模糊技术、最优化技术等数学方法,对各种因素进行定量描述,分析它们之间的数量关系,观察各种因素的变化规律。根据数学模型的分析结果及因果关系,确定可行的措施方案,建立消除危险、防止危险转化或条件耦合的控制系统。

系统安全分析的最优化利用因果关系、逻辑推理、数学模型进行安全分析和决策判断。它是指在一定条件下,当评价函数、要素指数或目标值(或顶端事件)达到理想状态时,一系列可调因素变量所得出的最佳结果;或者是指通过明确系统各因素或目标值(或顶端事件)的关系,收集尽可能完善的相关信息和资料,分析各种可选用的方案,以便选择最佳控制手段,有效地改进控制系统的功能。

3. 系统安全评价

系统安全分析的目的是进行安全评价。系统安全评价是对系统的危险性进行定性和定量分析,得出系统发生危险的可能性及其程度的评价,以寻求最低事故率、最小损失和最优安全投资效益。系统安全评价是安全决策的重要依据。

系统安全评价可分为定性安全评价和定量安全评价两大类。定性安全评价通过定性分析系统中的危险性,能揭示系统中的危险因素并对危险性的重要程度进行分类。与传统方法相比,定性安全评价的准确性已有了很大提高。但是,只有经过定量安全评价才能充分发挥安全系统工程的作用。当系统安全评价的结果表明需要改进系统的安全状况时,就必须采取安全措施,以减少危险因素及其发生概率,重新进行系统安全评价,直到达到安全要求。

系统安全评价又分为对系统本质安全的评价和对人的行为安全的评价。系统本质安全是指20世纪60年代,起源于电子工业电气系统的自我保护功能的设计。在安全工程方面,系统本质安全主要是指装备、机具等物质运转系统对其异常、超载、形变、故障、失效、超限等非寻常状态具有自我调节、转换、联锁、保护的功能。例如,在化工、石化等易燃易爆场合使用的本质安全仪表就属于这方面的内容。人的行为安全主要是指对系统中参与者的相关行为与制度的执行情况的评价,包括系统执行机构的建立、系统制度和系统操作规程的制定及其执行。在实际工作中应该把人的行为方式、情绪状态、心理素质等也作为评价的内容。

系统安全评价内容包括危险有害因素识别与分析、危险性评价、确定可接受风险和制定

安全对策措施四个方面。在实际的系统安全评价过程中，这四个方面的工作是不能截然分开、孤立进行的，而是相互交叉、相互重叠于整个管理工作中的。

系统安全评价方法很多，如逐项赋值评价法、火灾爆炸危险评价法、可靠性评价法、模糊综合评价法等。系统安全评价方法要根据评价对象的特点、规模、评价的要求和目的等进行选择。

4. 系统安全预测

系统安全预测是对系统未来的安全状况进行预测，预测有哪些危险及其危险程度，以便对可能发生的事故进行预防和预报。通过系统安全预测，我们可以掌握事故的变化趋势，认识危险的客观规律，从而制定相应的策略、发展规划及技术方案，以此来控制事故的发生和发展趋势。

系统安全预测根据预测对象的不同，可以分为宏观预测和微观预测；根据应用的理论原理，可以分为白色理论预测、灰色理论预测和黑色理论预测。系统安全预测的主要方法有回归分析预测法、马尔柯夫预测法、灰色系统预测法和德尔菲预测法等。

5. 安全决策与措施

安全系统是一个不确定的系统，受多种因素的影响，所以要以最低的成本达到最优的安全水平，就要进行安全决策。安全决策是针对生产活动中需要解决的特定安全问题，根据安全标准、规范和要求，运用现代科学技术知识和安全、科学的理论与方法，提出各种安全措施方案。安全决策的最大特点是从系统的完整性、相关性、有序性角度出发，对系统实施全面、全过程的安全管理，实现对系统的安全目标的控制。

安全措施主要有两个方面：一是预防事故发生的措施，即在事故发生前加以防范，排除危险因素；二是控制事故损失扩大的措施，即在事故发生后采取补救措施，防止事故扩大，降低事故造成的损失。

1.2.3 安全系统工程的特点

在工业等领域内引进安全系统工程的方法是有许多优越性的。安全系统工程使安全管理工作从过去的凭直观经验进行主观判断的传统方法，转变为定性与定量分析。它具有以下五个特点。

- 运用系统安全分析方法，了解系统的薄弱环节及其可能导致事故的条件，从而采取相应的措施，预防事故的发生。定性分析可以找到事故发生的真正原因，找出系统的危险程度。另外，定量分析能够预测事故发生的可能性和事故后果的严重性，从而可以采取相应的预防措施，以防止事故的发生、发展。
- 现代生产的特点是大型化、连续化和自动化，生产关系日趋复杂，各子系统相互联系、相互制约。安全系统通过全面、系统的安全分析、评价和优化选择，找出适当的方法使各子系统之间达到最佳配合状态，即用最少的投资达到最佳的安全效果，大幅度地减少伤亡事故的发生。
- 安全系统不仅适用于工程技术，还适用于安全管理，在实际工作中已经形成安全系

统工程与安全系统管理两个分支。它的应用范畴可以归纳为发现事故隐患、预测故障引起的危险、设计和调整安全措施方案、实现安全管理最优化、不断改善安全措施和管理方法五个方面。

- 促进各项安全标准的制定和有关可靠性数据的收集。安全系统工程既然需要评价,就需要各种标准和数据,如允许安全值、故障率数据,以及安全设计标准、人机工程标准等。
- 安全系统工程的开发和应用可以迅速提高安全技术人员、操作人员和管理人员的业务水平和系统分析能力。

1.3 工业生产安全

1.3.1 工业生产安全问题

安全问题无处不在,小到日常生活中燃气泄漏引发的爆炸,大到核电站核泄漏事故导致的灾难。本书侧重于工业生产领域,特别是流程工业中的安全问题。

工业革命以来,工业化的推进为人类生活提供了丰富的物质资料,极大地提高了人类的生产和生活水平。但工业生产的大量安全事故又严重威胁了人身健康、环境和财产安全。特别是改革开放以后,伴随着我国工业化进程的加快,大规模的资源开采和工业化生产使得安全生产问题日益突出,安全形势日益严峻,成为社会关注的焦点问题,也是政府监控和管理的重点。

以现代工业控制系统为主的信息技术在安全生产领域发挥了不可替代的作用。各类安全技术和产品的大量涌现为安全生产提供了技术保障,而安全标准的制定为安全生产提供了指南和法律依据。这些技术和安全标准有力地促进了安全生产水平的提高,在保护人民生命财产和环境安全方面起到了重要作用。

然而,随着我国“两化融合”的不断推进,特别是互联网和移动互联网与工业生产融合的加深,工业生产安全又面临了新的挑战,有了新的态势。以“震网”病毒为代表的网络攻击对关键基础设施的严重破坏进一步表明了信息时代安全保障的迫切性、必要性和复杂性。伴随着以工业 4.0、工业物联网为代表的新型工业生产模式的出现,工业生产信息系统与物理过程的融合构成了信息物理系统,目前非常有必要加强信息物理系统的安全研究。

1.3.2 工业生产安全的主要保障措施

工业生产安全主要从工业生产的安全需求角度出发,依据相关的法律法规,开展工业生产的安全风险评估,确定相关的安全保障技术措施和管理手段,实施全生命周期的安全管理,以达到降低事故风险、实现安全生产的目的。

对于安全保障技术措施而言,除了设计层面的固有安全设计外,在实际生产过程中实施的安全保障技术措施主要包括参数报警、常规控制功能、故障诊断、常规控制系统的工艺联