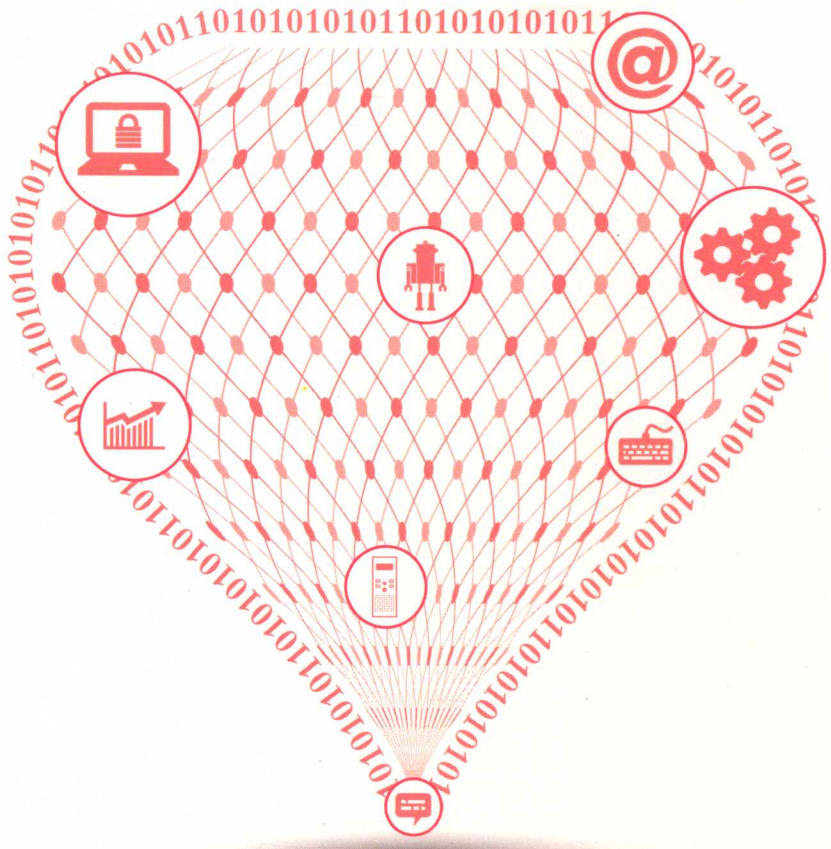

工业控制系统信息安全

（第2版）

肖建荣　编著

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

工业控制系统信息安全

（第2版）

肖建荣　编著

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

随着现代社会发展的迅速工业化和信息化，工业控制系统越来越多地采用信息技术和通信技术，工业控制系统信息安全面临严峻的挑战。本书简洁、全面地介绍了工业控制系统信息安全的概念和标准体系，系统地介绍了工业控制系统架构与漏洞分析，并且系统地阐述了工业控制系统信息安全的技术与方案部署、风险评估、生命周期、管理体系、项目工程、产品认证，工业控制系统的入侵检测与防护、补丁管理，工业控制系统信息安全软件与监控。本书以工业控制系统信息安全应用为导向，内容阐述深入浅出，问题分析清晰透彻，除系统地介绍相关技术与理论外，还有具体的工业控制系统信息安全应用举例，并且对未来进行了展望，可进一步加深读者对内容的理解和掌握。

本书可作为广大从事工业控制系统信息安全管理工程设计、应用开发、部署与管理工作的高级技术人员的参考书，也可作为高等院校工业自动化、计算机科学与技术、信息安全等相关专业的本科高年级学生、研究生的参考书。

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

工业控制系统信息安全 / 肖建荣编著. —2 版. —北京：电子工业出版社，2019.10

ISBN 978-7-121-37494-4

Ⅰ. ①工… Ⅱ. ①肖… Ⅲ. ①工业控制系统—信息安全 Ⅳ. ①TP273

中国版本图书馆 CIP 数据核字（2019）第 212664 号

策划编辑：陈韦凯
责任编辑：康　霞
印　　刷：天津千鹤文化传播有限公司
装　　订：天津千鹤文化传播有限公司
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：787×1 092　1/16　印张：15.75　字数：403.2 千字
版　　次：2015 年 9 月第 1 版
　　2019 年 10 月第 2 版
印　　次：2019 年 10 月第 1 次印刷
定　　价：65.00 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 zlts@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。

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 版前言

工业控制系统信息安全事件的频繁发生，吸引了全球人的目光，因为现代工业控制系统普遍采用数据采集与监控（SCADA）系统、分布式控制系统（DCS）、可编程逻辑控制器（PLC）系统，以及其他控制系统等，并且已广泛应用于电力、水利、石化、钢铁、医药、食品、汽车、航天等工业领域，成为国家关键基础设施的重要组成部分，其是否能够安全、稳定运行，已经关系到国家的战略安全。

世界各国政府、专家都在积极开展广泛合作，已经制定出一些相关的国际标准和规范，也在组织本国的人力、物力，制定相应的国家标准和规范，做到未雨绸缪，竭尽全力地做好工业控制系统信息安全工作。

工业控制系统信息安全工作刚刚走过十几年，还处在发展过程中。建立一套全面的知识和应用体系是我们的当务之急，这正是编写本书的出发点。虽然对其中的内容有些争议，但是我们希望在各方的共同参与下，积极推进工业控制系统信息安全工作，做到在争论中不断发展，在实践中不断推进。因此，本书将给广大工业控制系统用户一个全面和正确的指导，给广大从事工业控制系统设计、施工、调试和服务的用户以强有力的支撑，同时也可以给工业控制系统供应商提供参考，对政府相关职能部门的工作也有一定的参考价值。

本书分为 12 章。第 1 章介绍工业控制系统信息安全现状、威胁与发展趋势、定义与要求，以及标准体系；第 2 章介绍工业控制系统架构与漏洞分析；第 3 章介绍工业控制系统信息安全技术与部署中的工业防火墙技术、虚拟专用网技术、控制网络逻辑分隔、网络隔离，以及纵深防御架构；第 4 章介绍工业控制系统信息安全风险评估的系统识别、区域与管道的定义、信息安全等级、风险评估过程，以及风险评估方法；第 5 章介绍工业控制系统生命周期、信息安全程序成熟周期，以及信息安全等级生命周期；第 6 章介绍工业控制系统信息安全管理体系的安全方针、组织与合作团队、资产管理、人力资源安全、物理与环境管理、通信与操作管理、访问控制、信息获取与开发维护、信息安全事件管理、业务连续性管理，以及符合性；第 7 章介绍工业控制系统信息安全项目工程的规划设计、初步设计、详细设计、施工调试、运行维护，以及升级优化；第 8 章介绍工业控制系统信息安全产品认证机构、产品认证，以及产品认证趋势；第 9 章介绍工业控制系统入侵检测与防护；第 10 章介绍工业控制系统补丁定义、补丁管理系统设计、补丁管理程序，以及补丁管理实施；第 11 章介绍工业控制系统信息安全软件与监控的两个常见应用实例，即工厂信息管理系统和远程访问系统；第 12 章介绍工业发展趋势、工业控制系统发展趋势，以及工业控制系统信息安全展望。

本书在编写过程中，除引用了作者多年的工作实践和研究内容之外，还参考了一些国内外优秀论文、书籍，以及互联网上公布的相关资料，虽已尽量在书后的参考文献中列出，但由于互联网上资料数量众多、出处引用不明确，可能无法将所有文献一一注明出处，对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。

本书是一本工业控制系统信息安全前沿技术专业书，可作为广大从事工业控制系统和网络安全管理工程设计、应用开发、部署与管理工作的高级技术人员的参考书，也可作为高等院校工业自动化、计算机科学与技术、信息安全等相关专业的本科高年级学生、研究生的参考书。

工业控制系统信息安全是一门应用性很强的跨专业学科，在工业技术和信息技术大规模发展的今天迅速发展，本书尝试对此领域的理论和技术做了一些归纳，与广大同行和关心工业控制系统信息安全的人士分享。由于工业控制系统信息安全技术在快速发展，加之作者的水平有限，书中难免有缺点和错误，真诚希望读者不吝赐教，以期修订时更正。

编著者

2015 年 4 月

第 2 版前言

本书第 1 版自 2015 年出版以来，其系统性、实用性和前瞻性得到了电力、水利、石化、钢铁、医药、食品、交通、航天等工业领域从事工业控制系统信息安全技术管理和从事工业控制系统信息安全服务、建设、研发等的专业人员的广泛关注。同时，作为国内工业控制系统信息安全领域第一本系统、实用、先进的专业图书，本书被多家培训机构选为工业控制系统信息安全专业培训的首选教材，受到相关读者的一致好评。

随着国家网络安全战略规划建设的大力推进和社会各界从事工业控制系统信息安全工作人士的共同参与，工业控制系统信息安全在法律法规、标准规范、信息安全技术、行业应用等方面正在快速发展，结合工业控制系统信息安全专业培训经验与建议，本书的再版势在必行。

在本书编写过程中，主要对第 1 版第 1 章中的工业控制系统信息安全标准体系和第 3 章工业控制系统信息安全技术与部署进行了补充和修改，并将第 11 章改编为工业控制系统信息安全软件与监控。近年来，国际上通用的工业控制系统信息安全标准陆续发布，国内的工业控制系统信息安全法律法规、标准规范也在不断制定和发布。因此，本书第 1 章中的工业控制系统信息安全标准体系必须紧跟行业步伐。此外，近些年出现的工业控制系统信息安全技术对目前工作有很好的指导作用，因此，第 1 版第 3 章工业控制系统信息安全技术与部署需要进行补充和修改。再有，近些年涌现出的工业控制系统信息安全软件与监控是工业控制系统信息安全的重要组成部分，因此，将本书第 11 章改编为工业控制系统信息安全软件与监控。另外，对一些章节中的有关部分也进行了修改，使之更贴近工业控制系统信息安全应用和研究指导。

工业领域是国家关键基础设施的重要组成部分，工业控制系统信息安全关系着国家的战略安全。因此，从事工业控制系统信息安全相关工作的人员应担负其重任，不断补充工业控制系统信息安全知识，努力做好工业控制系统信息安全工作。

本书可作为广大从事工业控制系统和网络安全管理工程设计、应用开发、部署与管理工作的高级技术人员的参考书，也可作为高等院校工业自动化、计算机科学与技术、信息安全等相关专业的本科高年级学生、研究生的参考书。

工业控制系统信息安全是一门快速发展的跨专业学科。在工业技术和信息技术大规模发展的今天，通过广大专业同行和关心工业控制系统信息安全人士的不懈努力，工业控制系统信息安全技术已取得了一定的成效。由于工业控制系统信息安全技术还在飞速发展，加之作者的水平有限，书中难免存在错漏和不足之处，请广大读者批评指正，以便不断完善。

编著者

2019 年 8 月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　工业控制系统信息安全简介

1.1　工业控制系统信息安全现状、威胁与发展趋势

随着现代社会发展的迅速工业化和信息化，工业控制系统产品越来越多地采用以信息技术为基础的通用协议、通用硬件和通用软件，并广泛应用于电力、冶金、安防、水利、污水处理、石油天然气、化工、交通运输、制药，以及大型制造等行业中。同时，为了满足当前工业控制的需求，提高工厂或公司管理的运作效率，工业控制系统通过各种方式与互联网等公共网络连接，使病毒、木马等威胁向工业控制系统扩散有了可乘之机。由于工业控制系统的产品特性及网络连接，工业控制系统正面临巨大的威胁，因此工业控制系统信息安全受到越来越多的关注。

1.1.1　工业控制系统信息安全现状

2001 年后，通用开发标准与互联网技术的广泛使用使针对工业控制系统的攻击行为出现大幅增长，工业控制系统信息安全形势变得日益严峻。

据权威工业安全事件信息库（Repository of Industrial Security Incidents，RISI）统计，截止 2011 年 10 月，全球已发生 200 余起针对工业控制系统的攻击事件。据美国 ICS-CERT 报告，2012 年工业控制安全事件 197 起，2013 年工业控制（简称工控）安全事件 248 起，其统计图如图 1-1 所示。

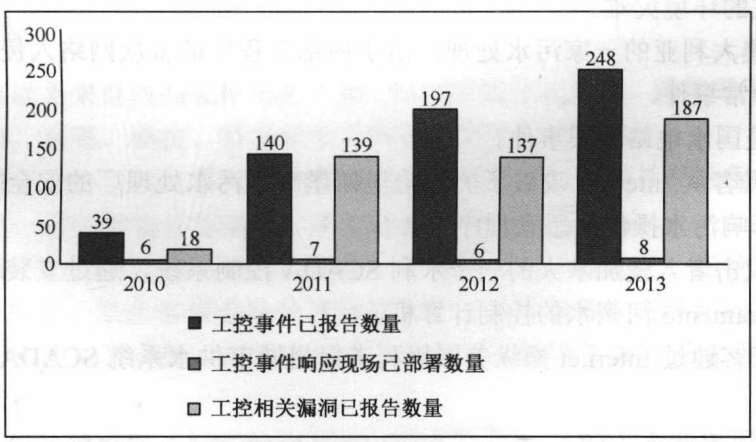

图 1-1　ICS-CERT 工业控制系统信息安全事件统计图

由此可见，近几年工业控制系统信息安全事件呈明显增多趋势。同时，ICS-CERT 安全报告指出，工业控制系统信息安全事件主要集中在能源、关键制造业、交通、通信、水利、核能等领域，而能源行业的安全事故超过一半。

近年来，典型工业控制系统入侵事件出现在能源、水利与水处理、交通运输、制造等行业。

1. 能源行业

1994 年，美国亚利桑那州 Salt River Project 被黑客入侵。

2000 年，俄罗斯政府声称黑客成功控制了世界上最大的天然气输送管道网络（属于 GAzprom 公司）。

2001 年，黑客侵入了监管加州多数电力传输系统的独立运营商。

2003 年，美国俄亥俄州 Davis-Besse 的核电厂控制网络内的一台计算机被微软的 SQL Server 蠕虫病毒感染，导致其安全监控系统停机将近 5 小时。

2003 年，龙泉、政平、鹅城换流站控制系统发现病毒，后发现是由外国工程师在系统调试中用笔记本电脑上网所致。

2007 年，在美国国土安全局的“Aurora”演习中，针对电力控制系统进行渗透测试，一台发电机在其控制系统受到攻击后被物理损坏。

2010 年，“网络超级武器”Stuxnet 病毒有针对性地入侵工业控制系统，严重威胁到伊朗布什尔核电站核反应堆的安全运营。

2012 年，美国国土安全局下属的 ICS-CERT 称，自 2011 年 12 月以来，已发现多起试图入侵几大输气公司的黑客活动。

2012 年 4 月 22 日，伊朗石油部和国家石油公司的内部计算机网络遭病毒攻击，为安全起见，伊朗方面暂时切断了海湾附近哈尔克岛石油设施的网络连接。

2. 水利与水处理行业

2000 年，一个工程师在应聘澳大利亚的一家污水处理厂被多次拒绝后，远程入侵该厂的污水处理控制系统，恶意造成污水处理泵站故障，导致超过 1000m^3 的污水被直接排入河流，造成了严重的环境灾难。

2001 年，澳大利亚的一家污水处理厂由于内部工程师的多次网络入侵而发生了 46 次控制设备功能异常事件。

2005 年，美国水电站溢坝事件。

2006 年，黑客从 Internet 攻破了美国哈里斯堡一家污水处理厂的安全措施，在其系统内植入了能够影响污水操作的恶意程序。

2007 年，攻击者入侵加拿大的一个水利 SCADA 控制系统，通过安装恶意软件破坏了用于控制从 Sacramento 河调水的控制计算机。

2011 年，黑客通过 Internet 操纵美国伊利诺伊州城市供水系统 SCADA，使得其控制的供水泵损坏。

3．交通运输行业

1997 年，一个十几岁的少年入侵纽约 NYNES 系统，干扰了航空与地面通信，导致马萨诸塞州的 Worcester 机场关闭 6 小时。

2003 年，CSX 运输公司的计算机系统被病毒感染，导致华盛顿特区的客货运输中断。

2003 年，19 岁的 Aaron Caffrey 入侵 Houston 渡口的计算机系统，导致该系统停机。

2008 年，攻击者入侵波兰某城市地铁系统，通过电视遥控器改变轨道扳道器，导致四节车厢脱轨。

4．制造行业

2005 年，在 Zotob 蠕虫安全事件中，尽管在 Internet 与企业网、控制网之间部署了防火墙，但还是有 13 个美国汽车厂由于被蠕虫感染而被迫关闭，50 000 生产线上的工人被迫停止工作，预计经济损失超过 1 400 000 美元。

2010 年我国某石化、2011 年某炼油厂的某装置控制系统分别感染 Conficker 病毒，都造成了控制系统服务器与控制器通信不同程度的中断。

2014 年，某钢铁厂遭到攻击，攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，造成重大损失。

5．跨行业

2011 年，微软公司警告称，最新发现的 Duqu 病毒可从工业控制系统制造商那里收集情报数据。

2012 年，发现攻击多个中东国家的恶意程序——Flame 火焰病毒，能收集各行业的敏感信息。

1.1.2　工业控制系统信息安全威胁

工业控制系统信息安全威胁主要来自敌对因素、偶然因素、系统结构因素和环境因素。

1．敌对因素

敌对因素可以是来自内部或外部的个体、专门的组织或政府，通常采用包括黑客攻击、数据操纵、间谍、病毒、蠕虫、特洛伊木马和僵尸网络等进行攻击。

黑客攻击通过攻击自动化系统的要害或弱点，使得工业网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，从而造成不可估量的损失。

来自外部的攻击包括非授权访问，是指一个非授权用户的入侵；拒绝服务（Denial of Service，DoS）攻击，即黑客想办法让目标设备停止提供服务或资源访问。这样一来，一个设备不能执行它的正常功能，或者它的动作妨碍了其他设备执行正常功能，从而导致系统瘫痪，停止运行。

近年来，高级持续威胁（Advanced Persistence Threat，APT）不断出现。攻击者有一个基于特定战略的缜密计划，其攻击对象是大中型企业、政府、重要机构。攻击者使用社会

上的工程技术和/或招募内部人员来获取有效登录凭证。选择使用何种工具主要取决于他们的攻击目标是什么，以及其网络配置和安全状况。攻击者经常利用僵尸网络，因为僵尸网络能够给他们提供更多资源来发动攻击，并且很难追踪到攻击的源头。

2．偶然因素

偶然因素可以来自内部或外部的专业人员、运行维护人员或管理员。由于技术水平的局限性及经验不足，这些人员可能会出现各种意想不到的操作失误，势必对系统或信息安全产生较大影响。

3．系统结构因素

系统结构因素可以来自系统设备、安装环境和运行软件。由于设备老化、资源不足或其他情况造成系统设备故障、安装环境失控及软件故障，从而对系统或信息安全产生较大影响。

4．环境因素

环境因素可以来自自然或人为灾害、非正常的自然事件（如太阳黑子等）和基础设施破坏。这些自然灾害、人为灾害、非正常的自然事件和基础设施破坏对工业控制系统信息安全产生较大影响。

1.1.3 工业控制系统信息安全发展趋势

工业控制系统信息安全发展趋势主要有3个：全行业覆盖趋势、经济越发达安全事件越多趋势和日益增多趋势。

1．全行业覆盖趋势

目前，工业控制系统广泛应用于我国电力、冶金、安防、水利、污水处理、石油天然气、化工、交通运输、制药，以及大型制造等行业中，据不完全统计，超过80%涉及国计民生的关键基础设施是依靠工业控制系统来实现自动化作业的，工业控制系统已是国家安全战略的重要组成部分。因此，工业控制系统信息安全有全行业覆盖的趋势。

2．经济越发达安全事件越多趋势

国家经济越发达，工业控制系统应用越广泛；国家经济越发达，工业管理要求越高，工厂信息化建设越多。因此，工业控制系统信息安全有国家经济越发达工业控制系统安全事件就越多的趋势。

3．日益增多趋势

新技术新应用层出不穷，云计算、移动互联网、大数据、卫星互联网等领域的新技术

此为试读，需要完整PDF请访问：www.ertongbook.com