信息安全保障人员认证培训教材

工业控制系统网络安全

GONGYE KONGZHI XITONG WANGLUO ANQUAN

中国信息安全认证中心

◎ 主　编 张　剑　◎ 副主编 王志威　张彬哲　张记卫　钱晓斌

★ ★ ★ CISAW ★ ★ ★

电子科技大学出版社

信息安全保障人员培训教程

工业控制系统网络安全

GONGYE KONGZHI XITONG WANGLUO ANQUAN

中国信息安全认证中心

◎主　编　张　剑　◎副主编　王志威　张彬哲　张记卫　钱晓斌

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

工业控制系统网络安全 / 张剑主编. - - 成都：电子科技大学出版社, 2017. 5

ISBN 978 - 7 - 5647 - 4500 - 4

Ⅰ. ①工… Ⅱ. ①张… Ⅲ. ①工业控制系统 - 信息安全 - 研究 Ⅳ. ①TP273

中国版本图书馆 CIP 数据核字 (2017) 第 109319 号

内容提要

本书全面阐述了工业控制网络和工业控制系统，论述了工业控制网络的特点和面临的安全威胁，给出了工业控制网络的风险评估方法和流程，阐述了工业控制网络中具体的安全防护体系和防护技术。本书介绍了工业控制网络相关的一些法律法规和标准规范，并结合典型行业应用中的工业控制网络，分析了安全防护体系和具体的安全防护技术。本书作为信息安全保障人员认证（CISAW）工业控制安全技术方向专业教材，与《信息安全技术》《信息安全技术应用》基础教材配套使用。

本书包括工业控制网络方面的基本概念、基本方法和较为深度的技术方法，适合不同层次的学员和相关领域的技术与管理人员使用。

工业控制系统网络安全

gōng yè kòng zhì xì tǒng wǎng luò ān quán

张剑 主编

王志威 张彬哲 张记卫 钱晓斌 副主编

策划编辑 万晓桐 徐守铭

责任编辑 万晓桐 徐守铭

出版发行 电子科技大学出版社

成都市一环路东一段 159 号电子信息产业大厦九楼 邮编 610051

主 页 www. uestcp. com. cn

服务电话 028 - 83203399

邮购电话 028 - 83201495

印 刷 成都市火炬印务有限公司

成品尺寸 185mm × 260mm

印 张 17. 5

字 数 448 千字

版 次 2017 年 5 月第一版

印 次 2017 年 5 月第一次印刷

书 号 ISBN 978 - 7 - 5647 - 4500 - 4

定 价 62. 00 元

丛书编委会

工业控制系统网络安全

主　编：张　剑

副主编：王志威　张彬哲　张记卫　钱晓斌

编　委：（以汉字拼音为序）

白　波　董黎芳　冯文博　冯显亮　何宛馨　黄　伟

马文杰　乔思远　王　行　王　亮　王　勇　王中东

武传坤　武　文　邢　鹏　杨　苹　杨　莹　张大江

张辉文　赵　杰　周家豪

序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材，其中包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3本基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12本专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10本应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完

整信息安全保障知识体系。既是广大CISAW认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏昊

2014年12月28日

前 言

2016年11月7日，第十二届全国人大常委会第二十四次会议表决通过了《网络安全法》，并将于2017年6月1日起施行。这标志着我国已经进入依法治理网络，依法保护网络安全的时代。

2015年6月，国务院学位委员会等机构批准成立“网络空间安全”一级学科。这意味着国家在培养网络空间安全人才方面将要加快步伐。网络安全的建设需要创新技术，更需要人才。为了能快速培养具有网络安全知识的人才，中国信息安全认证中心组织了多种课程的人才培训，效果明显。在网络安全相关领域的人才培训过程中，培训内容也在不断丰富和更新。但是，工业控制安全领域的人才培训仍然欠缺，其主要原因是工业控制安全领域是一个跨学科的领域，涉及工业控制领域与信息安全领域，而这两个领域的交叉存在一定难度。

工业控制网络安全是网络空间安全的重要组成部分，其安全隐患具有重要的社会影响。为了尽快完善网络安全认证工作，我们组织编写了这本培训教材。本书以工业控制网络安全的相关理论为基础，结合业界的实际操作经验，对工业控制网络安全的全生命周期进行了论述。

全书共分7章，第1章介绍了工业控制系统网络安全的发展历程，分析了工业控制系统网络存在的安全漏洞、由此导致的典型网络安全事故、我国工业控制系统网络安全面临的严峻形势等；第2章从技术上对工业控制系统进行了全面描述，包括常见的工业控制系统架构、典型工业控制协议、工业控制系统的网络架构等；第3章描述了工业控制系统风险评估，包括风险评估的概念、意义和方法，风险评估流程和实施，工控系统对风险的处置策略等；第4章介绍工业控制系统安全防御体系，从不同层面对工业控制系统网络安全的防御技术方法和策略进行了详细描述；第5章介绍了具体的工业控制系统网络安全防护技术，包括对结构安全的防护技术，对主机和设备安全的防护技术，对行为安全的防护技术，对基础软硬件安全的

防护技术，并介绍了工控系统中特有的安全白名单技术和常见的工控系统网络安全检测工具；第6章针对电力行业和石油化工行业，描述了工业控制系统网络安全典型应用案例；第7章介绍了工业控制系统网络安全相关法律法规和标注等。

本书在编写过程中得到《信息安全保障人员认证考试用书》编委会的指导，同时得到中国信息安全认证中心、北京匡恩网络科技有限责任公司、国卫信安教育科技（北京）有限公司和四川省中认信安技术服务有限公司的大力支持，在此表示衷心感谢。

由于我们水平有限，错误之处在所难免，欢迎读者批评指正，帮助我们在以后的培训中进行修改，提高教材的质量。

张剑

2017年2月

目 录

第 1 章

工业控制系统网络安全发展历程

工业控制系统网络安全是集成了信息系统网络安全技术与工业自动化控制技术的跨学科的全新领域，是网络安全在工业控制领域的延续。工业控制系统网络安全与国家安全、经济安全和民生安全息息相关，是信息时代国家经济和社会建设的基础性问题，也是当前加快推进产业转型升级、维护社会和谐稳定的最迫切的现实问题。

1.1 网络安全技术发展历程

随着互联网的普及和信息化建设步伐的加快，人们的工作、生活已严重依赖于网络，互联网已成为国家的重要基础设施。然而，互联网在带给人们极大便利的同时也带来了许多网络安全问题，网络安全问题正成为制约互联网、工业生产、关键基础设施的发展，甚至国家安全的重要因素。

1.1.1 网络安全的起源

1968 年，美国国防部高级研究计划局组建了一个计算机网，名为 ARPANET（英文 Advanced Research Projects Agency Network 的缩写，又称“阿帕”网）。按央视的数据，新生的“阿帕”网获得了国会批准的 520 万美元的筹备金及两亿美元的项目总预算，是当年中国国家外汇储备的 3 倍。时逢美苏冷战，美国国防部认为，如果仅有一个集中的军事指挥中心，万一被苏联摧毁，全国的军事指挥将处于瘫痪状态，所以需要设计一个分散的指挥系统。它由一个个分散的指挥点组成，当部分指挥点被摧毁后其他点仍能正常工作，而这些分散的点又能通过某种形式的通信网取得联系。

1969 年，“阿帕”网第一期投入使用，有 4 个节点，分别是加利福尼亚大学洛杉矶分校、加利福尼亚大学圣巴巴拉分校、斯坦福大学以及位于盐湖城的犹它州州立大学。

位于各个结点的大型计算机采用分组交换技术，通过专门的通信交换机（IMP）和专门的通信线路相互连接。一年后“阿帕”网扩大到 15 个节点。1973 年，“阿帕”网跨越大西洋利用卫星技术与英国、挪威实现连接，扩展到了世界范围。

1975 年，“阿帕”网由美国国防部通信处接管。在全球，已有大量新的网络出现，如计算机科学研究网络（Computer Science Research Network，CSNET）、加拿大网络（Canadian Network CDnet）、因时网（Because It's Time Network，BITNET）等。

1982 年中期“阿帕”网被停用过一段时间，直到 1983 年“阿帕”网被分成两部分，即用于军事和国防部门的军事网（MILNET）以及用于民间的“阿帕”网版本。用于民间的“阿帕”网改名为互联网。

1986 年，一家巴基斯坦电脑公司为了防止自己出售的软件被非法拷贝而编写了“大脑（Brain）”程序。该程序运行在 DOS 操作系统下，通过软盘在不同的计算机之间传播。该程序能够追踪到有多少人在非法使用该公司的软件，成为世界上公认的第一个在个人电脑上广泛传播的计算机病毒。

1988 年，美国人罗伯特·莫里斯把一个“蠕虫”病毒程序放到了互联网上。该病毒迅速扩散蔓延，最终导致了数千台连接互联网的计算机瘫痪。这个被称为“莫里斯（Morris）蠕虫”程序的出现使相关人员意识到互联网并不是他们想象中的那样安全，从此以后计算机网络安全问题得到了越来越多的关注与重视，网络安全技术的研究得以广泛开展，网络安全革命也随之爆发。

1.1.2 网络安全技术发展历程

网络安全技术的发展经历了面向信息的安全保障和面向业务的网络安全保障、面向服务的安全保障三个阶段。[1]

1.1.2.1 面向信息的安全保障

从计算机诞生一直到 20 世纪 90 年代末期，这段时间计算机网络刚刚兴起，各行各业的信息正在陆续实现电子化，不同行业和领域的业务系统相对独立。在需要交换信息时，通常通过建立特定的数据格式和文件格式，以及数据交换区的形式来实现。这个阶段的信息量相对较小，复杂程度也较低，因此能够实现对信息进行直接的安全保障。

面对信息的安全保障，体现在对信息的产生、传输、存储、使用过程中的保障，主要的技术是信息加密，保障信息不外露在“光天化日”之下。因此，信息安全保障设计的理念是以风险分析为前提，如 ISO13335 风险分析模型，找到系统中的“漏洞”，分析漏洞能带来的威胁，评估堵上漏洞的成本，再“合理”地堵上“致命”漏洞，威胁也就消失了。

在此阶段，安全技术一般采用防护技术，加上人员的安全管理，出现的最多的是