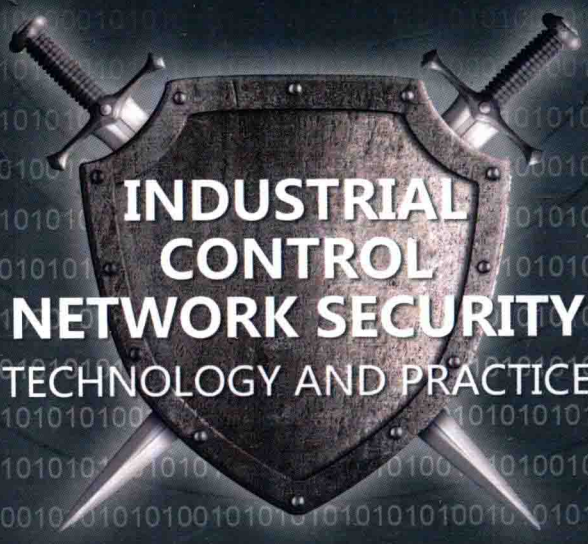
HZ BOOKS
华章教育

信息安全
技术丛书

- 国内首部面向初学者系统介绍工业控制网络安全的著作
- 工业控制网络安全领域的专家合作编写，从学术与工程视角全面涵盖工业控制网络的原理、技术与实践，帮助读者深度理解和掌握工业控制网络安全的精髓

工业控制网络安全技术与实践

姚羽 祝烈煌 武传坤 编著



机械工业出版社
China Machine Press

信息安全
技术丛书

工业控制网络安全技术与实践

姚羽 祝烈煌 武传坤 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

工业控制网络安全技术与实践 / 姚羽，祝烈煌，武传坤编著 . —北京：机械工业出版社，2017.5
（信息安全技术丛书）

ISBN 978-7-111-56907-7

I. 工… II. ① 姚… ② 祝… ③ 武… III. 工业控制计算机 – 计算机网络 – 信息安全 – 高等学校 – 教材 IV. TP273

中国版本图书馆 CIP 数据核字（2017）第 113756 号

本书是一本关于工业控制系统网络安全技术的专业教材。本书首先介绍工业控制系统与工业控制网络的概念、SCADA 和 DCS 两个典型的工业控制系统、一般工业控制系统的重要组成单元，然后介绍工业控制网络常见的安全威胁、工业控制系统各组成部分的脆弱性和安全防护技术、工业控制网络的常用通信协议和安全防护技术以及工业控制网络的漏洞特征、漏洞挖掘和攻击检测等技术，最后针对工业控制的几个典型领域进行了安全分析并给出了解决方案。

本书内容系统深入，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本科生和研究生的教材，也可以作为工业控制网络安全领域的研究人员和工程技术人员的培训用书及参考书。

工业控制网络安全技术与实践

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：余 洁 责任校对：殷 虹
印 刷：北京市荣盛彩色印刷有限公司 版 次：2017 年 7 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：16.5
书 号：ISBN 978-7-111-56907-7 定 价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

本书编写委员会

序 — *Foreword*

随着德国的“工业 4.0”、美国的“再工业化”风潮、“中国制造 2025”等国家战略的推出，以及云计算、大数据、物联网等新技术、新应用的大规模使用，工业控制系统逐渐由封闭独立走向开放、由单机走向互联、由自动化走向智能化。伴随这一趋势，工业控制系统网络安全的隐患日益凸显，伊朗核电站遭受“震网”攻击事件和乌克兰电网遭受持续攻击事件等更为我们敲响了警钟。工业控制系统已成为国家关键基础设施的“中枢神经”，其安全关系到国家的战略安全、社会稳定。

工业控制系统所面临的安全威胁是全世界面临的一个共同难题。工业设备的高危漏洞、后门、工业网络病毒、高级持续性威胁以及无线技术应用带来的风险，给工业控制系统的安全防护带来巨大挑战。

目前，我国工业控制网络安全形势不容乐观，主要表现在：一是传统上注重硬件方面的投入，对工业控制安全的投入较少；二是工业控制网络安全软硬件和服务资源不足，工业控制网络安全从业人员的数量极度匮乏，难以满足行业需求；三是随着工业化和信息化的深度融合以及物联网的快速发展，工业控制系统以前所未有的速度发展，工业控制网络安全问题更加突出，对工业控制网络安全的技术、人才建设等不断提出新的要求。工业控制网络作为关键基础设施的重要组成部分，其安全问题不容忽视。从目前工业控制网络安全检查情况来看，行业一线真正懂得工业控制网络安全的人才非常缺乏，网络空间的竞争归根结底是人才竞争，要进一步推动工业控制网络安全事业的发展，关键在于加快相关人才的培养，让安全人才真正成为信息网络安全的核心驱动力量。

我们也要看到，工业控制网络安全是典型的工业自动化、通信网络、电子信息与行业融合的应用安全。工业控制网络安全涉及多领域知识的应用，有其特殊性，主要体现在：一是一般网络安全技术人员由于不了解工业控制现场，对工业控制理论和工业控制的实时、不可

停滞等特殊要求了解不深入，往往很难涉足工业控制安全领域；二是绝大多数工业控制自动化相关技术人员对网络安全了解不多，无法从事工业控制网络安全的相关工作。因此，工业控制网络安全人才的培养既迫切，又极具难度。我国网络空间安全学科建设刚刚起步，作为网络空间安全的重要部分，应该将工业控制网络安全纳入网络空间安全学科之中，以加快工业控制网络安全复合型人才的培养。

国内已有一批关注工业控制网络安全的教师和专家投入到工业控制网络安全人才培养工作中，但目前的问题是鲜有将工业控制和网络安全结合的书籍。本书基于作者在工业控制网络安全领域的研究成果和实践经验，系统地对工业控制系统网络基础知识、工业控制系统安全性及典型行业的工业控制网络安全应用案例进行了介绍，可帮助读者建立对工业控制网络安全的全面认知。该书既有工业控制网络安全前沿理论和技术的知识，又对当前常用工业控制技术和网络安全技术进行了总结，并有企业实战经验案例，特别适合高校教学和技术培训使用。希望本书的出版能对我国工业控制网络安全领域人才培养和工业控制网络安全技术发展起到积极作用，也希望更多的高校和企业加入到工业控制网络安全人才培养的队伍中来，产学合作，为我国网信事业发展培养更多优秀人才！

封化民

教育部高等学校信息安全专业教学指导委员会　秘书长

序　二 *Foreword*

工业控制网络安全正在成为网络空间对抗的主战场和反恐新战场，工业网络安全领域的对抗正在改变当今世界格局。

工业控制系统广泛应用于各个领域，包括基础设施（金融、能源、通信、电力、交通）、民生（水、电、燃气、医院、智慧城市、智能汽车）、工业生产（冶金、电力、石油化工、核能等）和军工等。超过 80% 的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业。网络信息安全防护理念正在发生深刻演变，以工业控制系统为中枢神经的国家关键基础设施安全和关键信息基础设施安全面临更为严峻的全新挑战。

当前，我国在工业控制系统安全的认知、感知、防护、标准等方面都存在很多亟待完善的地方。国内工业控制系统主要面临如下威胁：设备存在大量的高危漏洞，越来越普遍的设备后门实施，高级持续性威胁，无线技术的广泛应用给工业控制系统的安全防护带来巨大挑战。积极应对网络安全威胁，有效防范网络安全风险，是网络时代维护国家安全、社会稳定、公众利益的重要使命。

随着“中国制造 2025”和“智慧城市”建设的推进，网络安全问题随之产生，工业控制网络安全形势日趋严峻。近年来，世界各国发生了众多工业基础设施网络安全事件，工业控制系统安全已经由量变到了质变的阶段。以先进的网络技术攻击关键基础设施已经成为国家间攻防对抗以及恐怖主义威胁的新形式和新手段，看不见硝烟的战争已经打响，安全形势很严峻。

在智能化社会背景下，代码即武器。依靠工业控制系统实现自动化的基础设施和智能制造，以及在智慧城市建设中越来越普遍采用基于嵌入式技术的智能终端，都极有可能成为“武器”。在网络强国战略的背景下，工业控制系统网络安全、基础设施安全势必成为我国网络安全发展的主攻方向之一。目前，国内工业控制网络安全产业要解决的问题还很多，其中

一方面就是专业人才的培养，因为工业控制网络安全产业的发展离不开大量的专业技术人才。

本书的出版适逢其时，它填补了我国工业控制网络安全领域教材的空白。本书既有理论价值，又汇集了实践经验，可作为高等院校自动化类、信息安全类等相关专业的课程教材，也可作为工业控制网络安全培训教材以及专业教师、工业控制网络安全工程师的参考书。相信本书的出版能够给工业控制网络安全研究者提供有益的参考。

作为率先投身工业控制网络安全研究的专业人员与相关专业的企业领导者，我深知工业控制网络安全复合型人才的稀缺与企业对这部分人才的渴求。因此，该书必将为保障国家关键信息基础设施网络安全培养更多、更优秀、更专业的工业控制网络安全人才，对促进国内工业控制网络安全的研究与发展发挥重要的推动作用。

孙一桉

北京匡恩网络科技有限责任公司　技术委员会主席

前　言 Preface

随着信息技术和网络技术的迅猛发展，国家安全边界已经超越地理空间限制，延伸到信息网络，网络空间成为继陆、海、空、天之后的第五大国家主权空间。作为网络空间安全的重要组成部分，工业控制网络安全涉及国家关键基础设施和经济社会稳定，辐射范围广泛，应当予以充分重视。

工业控制系统广泛应用于电力、水利、污水处理、石油化工、冶金、汽车、航空航天等诸多现代工业，其中超过 80% 涉及国计民生的关键基础设施（如铁路、城市轨道交通、给排水、通信等）。随着工业化与信息化的深度融合、“互联网 +”及国务院“中国制造 2025”战略的提出，工业控制系统中信息化程度越来越高，通用软硬件和网络设施的广泛使用打破了工业控制系统与信息网络的“隔离”，带来了一系列网络安全风险。其中涉及的不仅仅是信息泄露、信息系统无法使用等“小”问题，而是会对现实世界造成直接的、实质性的影响，如设备故障、环境污染、人员伤亡甚至危害国家安全，其后果是无法预计的。

我国政府对工业控制系统的安全性予以高度重视，在国家战略、规范管理、信息共享、技术支撑等方面不断突破，致力于构建完善的工业控制网络安全保障体系。但是，目前国内网络安全研究团队的研究对象多集中在互联网和传统信息系统上，掌握工业控制网络安全知识、了解工业控制网络漏洞分析与安全防御技术的人极少，远不能满足各行业对工业控制网络人才的渴求，不能适应国家的发展战略。

本书围绕工业控制系统的安全，对工业控制系统、工业控制网络、工业控制系统整体安全性、SCADA 系统安全性、工业控制网络漏洞、工业控制网络协议、工业控制网络安全防御等进行了详细的阐述。最后列举了几个典型工业控制安全案例，旨在帮助读者全面了解工业控制系统安全领域的相关知识，建立防护意识。

本书共分为 8 章，各章主要内容概述如下：

第 1 章介绍了工业控制系统与工业控制网络的概念，描述了国内工业控制行业的现状及工业控制网络安全的趋势，并说明了工业控制系统中常用的术语。

第 2 章介绍了工业控制系统中 SCADA 与 DCS 这两个典型系统、控制器、现场设备，着重描述了 PLC 设备，并介绍了几种典型的工业控制网络。

第 3 章介绍了工业控制网络常见的安全威胁，并针对工业控制系统不同网络层的脆弱性进行了分析。

第 4 章介绍了 SCADA 系统的组成、安全需求、安全目标及脆弱性，描述了 SCADA 系统边界防护、异常行为检测、安全通信及密钥管理、风险评估与安全管理，介绍了 SCADA 系统安全测试平台，最后简要介绍了 SCADA 系统典型案例及发展趋势。

第 5 章详细介绍了四种常见的工业网络协议，并说明了各协议存在的安全问题，并有针对性地提出安全防护技术。

第 6 章介绍了工业控制网络漏洞的特征、分类、发布平台及态势，描述了针对已知漏洞的检测技术和针对未知漏洞的挖掘技术，分析了上位机、下位机及工业控制网络设备漏洞。

第 7 章全面介绍了工业控制网络安全防护技术，描述了工业控制安全设备的引入和使用方法，详细说明了对已知与未知工业控制安全威胁的处理方法。

第 8 章举例分析了几个典型的工业控制行业现状与安全趋势，并描述了相匹配的安全解决方案。

全书逻辑清晰，行文流畅，采用通俗易懂的方式介绍工业控制系统网络安全的相关知识，并提供了适当的图解，具有很强的可读性和实用性。

工业控制网络安全是集合了工业控制与网络安全的综合性、应用型方向，要求学习该方向的读者能够将系统知识与专业知识有机结合，在注重提升理论高度的前提下，将理论知识与工程实践紧密联系起来。本书结合工业控制网络安全领域的知识特点，充分考虑其知识体系、教育层次和课程设置，增设各行业典型实际案例，努力做到紧跟前沿技术的发展，使读者能够学以致用。教师可以基于本书增加实验课程，使学生更生动直观、深刻具体地掌握真实有效、切实可行的工业控制网络安全防护手段和思想。无论是初学者还是有一定经验的从业者，都可以从本书中找到所需要的内容。

本书可以作为高等院校自动化、计算机科学与技术、信息安全等相关专业的本科生、研究生教学用书，或工业控制系统安全相关人员的培训教材，也可以作为对工业控制网络安全感兴趣的普通读者和相关技术人员的参考资料。

希望更多的读者能通过学习本书更清晰、全面地掌握工业控制网络安全知识，为增强工业控制网络安全防护能力打下较为系统和扎实的基础。

在编写的过程中，本书除了借鉴多位专家的多年工作和研究内容外，还参考了大量的国内外优秀书籍、论文及网上公布的相关资料，并以参考文献的形式列出，可为读者进一步深入研究提供参考信息。

本书从策划到编写，得到了教育部高等学校信息安全专业教学指导委员会秘书长封化民教授的大力支持和指导，他对教材进行了审阅，提出了宝贵的建议，并欣然作序；解放军信息工程大学电子技术学院教授陈性元、北京航空航天大学博士生导师李春升、解放军电子工程学院博士生导师陆余良、国防科技大学电子工程所所长王伟、清华大学网络科学与网络空间研究院副研究员诸葛建伟、北京邮电大学副教授雷敏也审阅了本书，对本书内容提出了大量的意见和建议；机械工业出版社华章公司的各位编辑在本书的出版过程中给予了大力支持与帮助。在此深表感谢。

工业控制网络安全是自动化与信息安全结合演变的新兴领域，本书作为该领域的首本教材，在编写时虽力求全面、系统，但随着工业化和信息化大规模发展，工业控制系统网络安全技术日新月异，加之作者能力所限，书中难免有一些错误和不当之处，恳请读者提出宝贵意见，以期再版修订。

作　者

2017 年 5 月

Suggestion 教学 / 学习建议

如采用本书作为课程教材或培训教材，可参考本部分给出的建议安排教学内容和授课时长。读者也可依据本部分的建议和进度安排进行自学。

章节	教学 / 学习要求	课时
第 1 章 绪论	熟悉工业控制系统概念 熟悉工业控制网络与传统 IT 信息网络的异同 了解工业控制系统的威胁、脆弱点 了解典型工业控制系统事件	1
第 2 章 工业控制系统基础	了解工业控制系统的内容 了解 SCADA 系统的组成部分及主要功能 熟悉 DCS 的组成部分及特点	1
	熟悉 PLC 的主要功能 熟悉 PAC 的主要功能及优点 了解 RTU 的主要功能及优点 熟悉 IED 的工作机制 熟悉 HMI 的组成及特点	2
	了解 PLC 的产生原因及特点 熟悉 PLC 的结构及工作原理 掌握 PLC 的主要指令系统类别 熟悉 PLC 的通信技术规程 熟悉 PLC 的接口电路要求	2
	了解钢铁、石化、电力、市政交通行业的主要系统组成及结构	1
第 3 章 工业控制网络安全威胁	了解工业控制网络结构与组成 熟悉常见的安全威胁 掌握现场总线控制网络的脆弱性 掌握过程控制与监控网络的脆弱性 掌握企业办公网络的脆弱性	3

（续）

章节	教学 / 学习要求	课时
第 4 章 SCADA 系统安全分析	掌握 SCADA 系统组成 熟悉 SCADA 系统安全需求 熟悉 SCADA 系统安全目标 熟悉 SCADA 系统脆弱性 掌握安全域及边界防护 掌握异常行为检测技术 掌握安全通信及密钥管理 掌握风险评估与安全管理要点	2
	了解 SCADA 系统安全测试平台 了解电力 SCADA 系统安全防护技术 了解 SCADA 系统安全发展趋势	1
第 5 章 工业控制网络通信协议的安全性分析	了解 Modbus 总线协议 掌握 Modbus 协议安全缺陷 掌握 Modbus 协议安全防护技术 了解 DNP3 协议 掌握 DNP3 协议安全缺陷 掌握 DNP3 协议安全防护技术	3
	了解 IEC 系列协议 掌握 IEC 系列协议安全缺陷 掌握 IEC 系列协议安全防护技术 了解 OPC 协议 掌握 OPC 协议安全缺陷 掌握 OPC 协议安全防护技术	3
第 6 章 工业控制网络漏洞分析	掌握工控安全漏洞特征 掌握工控安全漏洞分类 了解工控安全漏洞标准化工作 了解工控安全漏洞态势分析 掌握已知漏洞的检测技术 掌握未知漏洞的挖掘技术	3
	掌握上位机概念与安全分析 掌握下位机概念与安全分析 掌握工控网络设备安全与漏洞分析	4
第 7 章 工业控制网络安全防护技术	了解传统信息系统与工业控制网络安全的不同侧重点 熟悉边界防护的主要安全设备 熟悉准入控制的主要设备类型 精通安全设备的选择方法 精通防火墙设备的配置方法 精通边界隔离与访问控制原理 精通防火墙技术原理 掌握漏洞发现技术原理 掌握补丁管理方法	3

（续）

章节	教学 / 学习要求	课时
第 7 章 工业控制网络安全 防护技术	了解工业控制网络行为安全定义 了解工业控制网络中的行为类型 熟悉可信计算的内容 熟悉加解密算法原理 熟悉安全开发流程的内容 掌握运营安全的重要性 掌握运营安全的日常内容 熟悉违规行为分析方法 熟悉违规行为处理方法 掌握异常参量和异常行为的定义 掌握异常行为的分析方法 熟悉工业控制网络中白名单技术的应用原理 熟悉常用白名单技术类型 熟悉智能列表定义 熟悉事件关联技术的类型 熟悉系统关联的定义 了解蜜罐技术的意义 了解蜜罐技术的组成部分	2
第 8 章 综合案例分析	了解数控制造业工控网络安全现状及解决方案 了解城市燃气行业工控网络安全现状及解决方案 了解石油化工行业工控网络安全现状及解决方案	1
总课时	第 1 ～ 8 章建议课时	32
	综合实训课时	8

说明：1）建议课堂教学全部在实验室内完成，实现“讲－练”结合。

2）建议教学分为核心知识技能模块和技能提高模块，其中核心知识技能模块建议课时为 24，技能提高模块建议课时为 8，不同学校可以根据各自的教学要求和计划课时数对教学内容进行取舍。

目　录 *Contents*