国之重器出版工程

制造强国建设

智能工业丛书

Decoding: Industrial Cyber Security

解码：工业信息安全

尹丽波　国家工业信息安全发展研究中心　主编

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

国之重器出版工程

制造强国建设

智能工业丛书

解码：工业信息安全

Decoding：Industrial Cyber Security

尹丽波　国家工业信息安全发展研究中心　主编

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

图书在版编目（CIP）数据

解码：工业信息安全 / 尹丽波，国家工业信息安全发展研究中心主编. —北京：电子工业出版社，2019.9
ISBN 978-7-121-37079-3

Ⅰ. ①解… Ⅱ. ①尹… ②国… Ⅲ. ①工业安全—信息安全—概论 Ⅳ. ①X931

中国版本图书馆 CIP 数据核字（2019）第 144526 号

策划编辑：董亚峰
责任编辑：刘小琳　　文字编辑：邓茗幻　　特约编辑：许波建
印　　刷：固安县铭成印刷有限公司
装　　订：固安县铭成印刷有限公司
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：720×1 000　1/16　印张：14　字数：260 千字
版　　次：2019 年 9 月第 1 版
印　　次：2019 年 9 月第 1 次印刷
定　　价：68.00 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：liuxl@phei.com.cn，（010）88254538。

《国之重器出版工程》
编辑委员会

专家委员会委员（按姓氏笔画排列）：

于　全　中国工程院院士

王少萍　“长江学者奖励计划”特聘教授

王建民　清华大学软件学院院长

王哲荣　中国工程院院士

王　越　中国科学院院士、中国工程院院士

尤肖虎　“长江学者奖励计划”特聘教授

邓宗全　中国工程院院士

甘晓华　中国工程院院士

叶培建　中国科学院院士

朱英富　中国工程院院士

朵英贤　中国工程院院士

邬贺铨　中国工程院院士

刘大响　中国工程院院士

刘怡昕　中国工程院院士

刘韵洁　中国工程院院士

孙逢春　中国工程院院士

苏彦庆　“长江学者奖励计划”特聘教授

屈贤明　国家制造强国建设战略咨询委员会委员、工业和信息化部智能制造专家咨询委员会副主任

项昌乐　“长江学者奖励计划”特聘教授，中国科协书记处书记，北京理工大学党委副书记、副校长

柳百成　中国工程院院士

闻雪友　中国工程院院士

徐德民　中国工程院院士

唐长红　中国工程院院士

黄卫东　“长江学者奖励计划”特聘教授

黄先祥　中国工程院院士

黄　维　中国科学院院士、西北工业大学常务副校长

董景辰　工业和信息化部智能制造专家咨询委员会委员

焦宗夏　“长江学者奖励计划”特聘教授

本书编写组

国家工业信息安全发展研究中心

监测预警所

组　长：刘　迎

成　员：郭　娴　刘京娟　程薇宸　黄　丹　张慧敏

杨帅锋　杨佳宁　陈柯宇　余章馗　刘文胜

曹　凯　狄晓晓　唐漪浓

前言

工业信息安全是实施制造强国和网络强国战略的重要保障，是支撑中国制造实现高质量发展的关键要素，对于切实维护工业生产安全、促进两化融合健康发展具有重要意义。当今世界，工业信息安全越来越受到各国特别是发达国家的高度重视，成为网络空间安全的一大焦点领域。近年来，伴随着现代制造业数字化、智能化、网络化的快速发展，我国工业信息安全领域的政策标准、工作机制、保障技术、组织架构等逐步完善，呈现出健康发展的良好势头。但是，我们也要清醒地认识到，由于工业信息安全的复杂性，我国工业信息安全形势十分严峻，面临着系统安全脆弱性凸显、网络安全威胁加速渗透、攻击手段复杂多变等一系列深刻挑战。

习近平总书记在党的十九大报告中全面系统地论述了坚持总体国家安全观的重要思想，在 2019 年 4 月 20—21 日召开的全国网络安全和信息化工作会议上更进一步指出，要“树立正确的网络安全观，加强信息基础设施网络安全防护”。工业信息安全作为国家安全体系的重要组成部分，党中央、国务院高度重视，做出一系列战略部署和政策指引，着力全方位构建工业信息安全保障体系。《中华人民共和国网络安全法》从关键信息基础设施保护的角度，明确了工业信息安全的基本要求。国务院先后颁布《关于深化制造业与互联网融合发展的指导意见》《关于深化“互联网+先进制造业”发展工业互联网的指导意见》等指导性文件，为我国工业信息安全的建设和发展提出了新课题，提供了新机遇，

赋予了新动能。

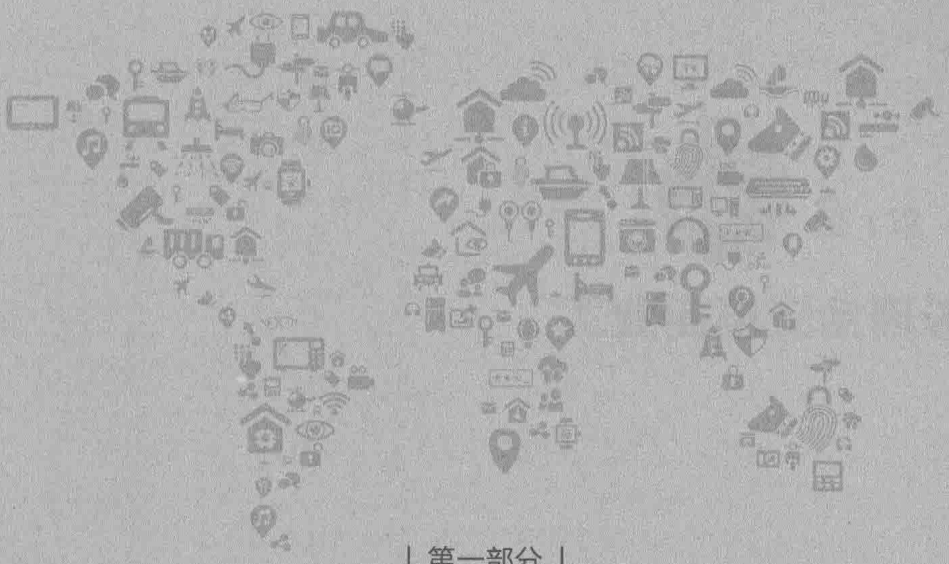
工业信息安全是一个全新安全领域。为推动工业信息安全的实践探索和理论研究，为相关机构、从业人员开展工业信息安全工作提供学习参考和学术咨询，国家工业信息安全发展研究中心会同浙江大学、战略支援部队信息工程大学、东北大学、北京理工大学等高等院校，组织撰写了《解码：工业信息安全》一书。本书作为一本系统讲解工业信息安全的综合性普及读物，对工业信息安全的定义、发展现状、演进趋势、政策环境、应用形态和技术实践等各个方面进行了较为全面的介绍。全书共包含三个部分、十个章节，第一部分 概述篇详细介绍了工业信息安全的定义、重要性及发展演进趋势；第二部分 基础篇较为全面地向读者普及了工业信息安全涉及的各类基础知识，涵盖工业信息安全的对象主体、风险来源、防护措施等各个方面；第三部分 应用篇则选取工业控制系统信息安全、工业互联网安全、工业云和工业大数据安全等工业信息安全的主要组成部分和技术实践，对其逐一进行讲解与剖析。

实践在发展，理论在更新。随着工业领域新技术发展和工业信息安全形势变化，本书的内容将适时更新和完善。恳请广大读者提出宝贵意见。

本书编写组

2018 年 10 月

目 录



| 第一部分 |

概述篇

第1章

工业信息安全概述

工业信息安全是一个全新的工业安全领域，包含工业数字化、网络化、智能化运行过程中的各个要素、各个环节的安全。本书所称工业信息安全是指工业企业的设备设施、控制系统、信息系统受到保护，连续、可靠、正常运行，数据不因偶然或恶意原因遭受破坏、更改、泄露，以及工业生产所需的公用通信网和互联网服务不中断。工业控制系统信息安全（以下简称工控安全）、工业互联网安全、工业大数据安全、工业云安全等均是工业信息安全的重要组成部分。与传统网络安全相比，工业信息安全须适应工业环境下系统和设备实时性、高可靠性及工业协议众多等特征，防护难度更大。当前，新一代信息技术在加速信息化与工业化深度融合发展的同时，也带来了日趋严峻的工业信息安全问题，工业信息安全重要性日益凸显。

一、工业信息安全的起源与发展

随着现代社会信息化的迅猛发展，工业化和信息化不断深入融合，工业控制系统（以下简称工控系统或ICS）作为工业领域的核心部分，成为钢铁石化、高端装备、电力系统、轨道交通、核设施等重点工业领域关键基础设施的“神经中枢”，其安全性受到越来越多的关注。从21世纪初开始，随着数字化、网络化、智能化在工业领域的普及和深化，业界对工控系统安全的认识和理解不断拓展和加深。在工业安全实践中，工业信息安全的概念逐步清晰和确立。在国际上，虽然中外在表述上有所不同，但对工业信息安全研究的范围、关注领域、制定的安全防护策略大体是一致的。近年来，在习近平总书记制造强国和网络强国思想的指引下，我国不断建立完善工业信息安全的总体布局，明确指导原则和工作重点，组建国家级工业信息安全技术支撑机构，全面提升工业信息安全保障水平。

工控安全是最早被关注的工业信息安全关键领域。2010年发生的伊朗核电站受“震网”（Stuxnet）蠕虫病毒攻击导致重大损失的事件震惊全球，把工控安全带入公众视野。工控系统作为信息系统与现实世界连接的纽带，被广泛应用于关系国计民生的诸多领域。工控安全风险所带来的，不仅是信息泄露、信息系统无法使用等“小”问题，也会对现实世界造成直接的、实质性的影响，如设备运行异常（交通瘫痪、城市运行停滞、生产制造不达标）、设备运行停滞（停水、停电、停气、停供暖、生产制造系统停滞）、设备损坏（零部件损坏甚至火灾爆炸）、环境污染乃至人员伤亡等。对于那些应用于国家层面及军工领域的工控系统，其信息安全风险更会对国家安全造成直接影响，工控系统的安全要得到世界范围的高度重视。美国国家标准技术研究院（NIST）于2011年6月公开发布了《工业控制系统安全指南》（SP 800-82），该指南文件概述了工控系统、典型系统拓扑结构及其重要性，阐述了其安全需求的基本原理；探讨了工控系统与传统IT信息系统的区别，阐述了威胁、脆弱性与安全事件的差异；简要介绍了旨在消减脆弱性的工控安全项目的开发与部署，并对在工控系统典型网络设计中如何整合安全性要素提出了建议。

我国高度重视工控安全。2011年9月，工业和信息化部发布《关于加强工