工业控制系统信息安全防护指引

国家工业信息安全发展研究中心 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防护指引

国家工业信息安全发展研究中心 著

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

内容简介

为了指导全国各地方工信主管部门及工业企业更好地落实《工业控制系统信息安全防护指南》，提高广大从业人员工控安全防护意识和能力，国家工业信息安全发展研究中心组织人员编写了本书。本书详细介绍了我国有关工业信息安全的指导原则、方针政策和工作部署，强调了工业企业工控安全防护主体责任，提出了可供工业企业参考的防护策略、实施建议和解决方案。

图书在版编目（CIP）数据

工业控制系统信息安全防护指引 / 国家工业信息安全发展研究中心著 . -- 北京：电子工业出版社，2018.7

ISBN 978-7-121-31545-9

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

中国版本图书馆 CIP 数据核字 (2017) 第 108333 号

责任编辑：孙杰贤
印　　刷：北京虎彩文化传播有限公司
装　　订：北京虎彩文化传播有限公司
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：720×1 000　1/16　印张：13.25　字数：160 千字
版　　次：2018 年 7 月第 1 版
印　　次：2018 年 7 月第 1 次印刷
定　　价：54.00 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：(010) 88254287，xiongwei@phei.com.cn。

序

工业控制系统作为关键基础设施的重要组成部分，关乎企业安全、社会安全、经济安全乃至国家安全。随着制造强国建设稳步推进，制造业与互联网融合步伐不断加快，工业控制系统日趋数字化、网络化和智能化，在极大提高生产效率、提升创新能力、促进产业转型升级的同时，也面临着漏洞层出不穷、威胁加速渗透、攻击手段复杂多样等前所未有的信息安全挑战。自2010年“震网”事件爆发以来，德国钢铁厂遭受高级可持续性威胁(APT)攻击、乌克兰断电、美国网络瘫痪等事件屡屡发生，工业控制领域警钟长鸣。

党中央、国务院将工业控制系统信息安全（简称“工控安全”）作为网络空间安全的重要组成部分，给予高度重视，做出了一系列战略部署和政策指引。习近平总书记在党的十九大报告中全面系统深刻地论述了坚持总体国家安全观的重要思想，并在2018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强调指出，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”。《中华人民共和国网络安全法》对保障包括工业控制系统在内的关键信息基础设施安全做出明确规定。国务院先后颁布《中国制造2025》《关于深化制造业与互联网融合发展的指导意见》等指导性文件，围绕制造强国和网络强国建设战略目标，明确提出实施工业控制系统安全保障能力提升工程，为工控安全建设指明了方向。

当前，工控安全已成为实施制造强国和网络强国战略的重要保障，

是维护我国工业安全、经济安全乃至国家安全的关键一环，具有重大的战略意义。为科学构建工控安全防护体系，工业和信息化部于2016年10月正式印发《工业控制系统信息安全防护指南》，这是近五年来我国在工控安全领域发布的首个标志性、权威性指导文件，明确了工业企业工控安全防护的基本要求。

为加快落实文件各项要求，助力工控安全防护取得实效，国家工业信息安全发展研究中心组织编写了《工业控制系统信息安全防护指引》一书。该书是我国第一本较为全面地介绍工控安全形势、政策、防护技术与实践的综合性普及读本，在深入研究和系统分析的基础上，重点基于《工业控制系统信息安全防护指南》要求，从安全管理、运行维护、技术操作等多维度，系统地提出了具体可行的防护策略、实施建议和解决方案，为工业企业开展工控安全防护工作提供了有益的技术指导。

在《工业控制系统信息安全防护指引》付梓出版之际，仅以此序表示祝贺。在此，我衷心希望此书能为提升企业工控安全防护水平、推动全社会工控安全意识普及、提升国家工控安全综合保障能力发挥积极作用。

2018年5月

前 言

工业控制系统广泛运用于工业、能源、交通、水利以及市政民生等领域，对生产设备的正常运行发挥着至关重要的作用。随着我国信息化和工业化深入融合，以及物联网、云计算和大数据等新一代信息技术的飞速发展，工业控制系统逐步走向开放、互联、通用，产品越来越多地采用通用协议、通用硬件和通用软件，与企业网甚至互联网的一体化融合程度不断加深，传统的信息安全威胁不可避免地扩散到工业控制领域，工业控制系统信息安全面临着日益严峻的挑战，成为国家网络空间安全的重要组成部分。近年来，国内外发生的多起工控安全事件充分表明，工业控制系统越来越成为国家间网络对抗的领域和有组织黑客攻击的重要目标。工业控制系统外部安全威胁和自身存在的安全漏洞，客观上要求我们必须高度重视工业控制系统信息安全问题，在积极推进两化深度融合的同时，下大力做好工控安全建设。

党中央、国务院高度重视工控安全建设，《国家网络空间战略》、《国家网络安全法》高度概括了工业信息安全对于保障关键国家信息基础设施正常运行、社会稳定和国家安全的重大意义，提出了指导原则。国务院先后发布《中国制造 2025》、《国务院关于深化制造业与互联网融合发展的指导意见》等重要文件，对加强工控安全保障工作做出具体部署。

2016 年 10 月，工业和信息化部为了贯彻落实党中央、国务院有关文件精神，提升工业控制系统信息安全防护水平，保障工业控制系统安全，在深入调查研究、广泛征求意见的基础上，发布了《工业控制系统信息安全防护指南》，分别从管理、技术角度系统地提出了十一个方面的安全防

护工作要求，并在全国范围内大力开展宣贯培训工作，取得积极成果，获得热烈反响。

为帮助全国各地方工信主管部门及工业企业更好地贯彻落实《工业控制系统信息安全防护指南》（简称《防护指南》），提高广大从业人员工控安全防护意识和能力，在工业和信息化部指导下，我们编写了《工业控制系统信息安全防护指引》作为与《防护指南》相配套的技术读本。全书分为四个章节，第一章深刻阐述了工业信息安全的重大意义；第二章详细介绍了我国关于工业信息安全的指导原则、方针政策和工作部署，特别强调了工业企业在工控安全防护中的主体责任；第三章有针对性地普及了工控安全相关基础知识，对概念、知识点、通用防护措施以及技术手段作了通俗解释；第四章围绕《指南》所涉及的十一项防护要求，结合工控安全领域目前的主要做法，提出了可供工业企业参考的防护策略、实施建议和解决方案。

本书适用于面向地方、行业及企业开展工控安全防护技术培训，也适用于工业企业管理人员、技术人员以及高校、研究机构相关人员学习参考。

为适应工业领域新技术高速发展和工控安全形势的不断变化，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。

编者著

2018 年 2 月

目 录

第一章 工业信息安全的重大意义 / 1

第一节 工业信息安全是助力两化深融的基础保障 / 3

第二节 工业信息安全是实现制造强国战略的重要支撑 / 4

第三节 工业信息安全是建设网络强国的必然要求 / 5

第二章 国家关于工业信息安全的政策及部署 / 7

第一节 习近平总书记的重要论述 / 9

第二节 国家立法强化关键信息基础设施安全 / 10

第三节 国务院关于工业信息安全的相关政策 / 12

一、《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》 / 12

二、《中国制造 2025》 / 12

三、《国务院关于深化制造业与互联网融合发展的指导意见》 / 13

四、《国务院关于积极推进“互联网 +”行动的指导意见》 / 14

第四节 政府主管部门对工业信息安全的工作部署 / 15

一、《关于加强工业控制系统信息安全管理的通知》 / 15

二、《信息化和工业化深度融合专项行动计划（2013—2018）》 / 16

三、《工业和信息化部贯彻落实〈国务院关于积极推进“互联网 +”行动的指导意见〉的行动计划（2015—2018 年）》 / 17

四、《工业控制系统信息安全防护指南》 / 18

第五节 工业企业的主体责任 / 19

一、工业信息安全是现代企业核心竞争力的关键要素 / 19

二、企业应认真落实工业信息安全各项职责 / 20

三、增强意识是做好工业信息安全的首要前提 / 20

四、健全队伍是保障工业信息安全的基础条件 / 21

第三章 工业控制系统信息安全基础知识 / 23

第一节 工业控制系统相关基本概念 / 24

一、工业控制系统定义、主要类型及架构 / 24

二、工业控制系统与 IT 系统的区别 / 25

第二节 工业控制系统存在的主要安全问题 / 27

一、核心技术产品受制于人 / 27

二、安全防护水平相对落后 / 28

三、网络攻击风险持续加剧 / 28

四、安全管理机制尚待健全 / 29

第三节 技术防护手段及方式 / 29

一、常用技术防护手段 / 29

二、工控安全防护流程 / 35

第四节 工业控制系统相关标准介绍 / 39

一、国际工业控制系统信息安全标准 / 39

二、我国工业控制系统信息安全标准 / 47

三、工业控制系统信息安全标准体系框架 / 54

第四章 《指南》解读及主要做法 / 57

第一节 编制背景及依据 / 59

一、编制背景 / 59

二、编制依据 / 60

第二节 安全软件选择与管理 / 61

一、目的 / 61
二、内容要求 / 61
三、实施建议 / 62
第三节 配置和补丁管理 / 65
一、目的 / 65
二、内容要求 / 65
三、实施建议 / 67
第四节 边界安全防护 / 71
一、目的 / 71
二、内容要求 / 71
三、实施建议 / 72
第五节 物理和环境安全防护 / 77
一、目的 / 77
二、内容要求 / 77
三、实施建议 / 78
第六节 身份认证 / 79
一、目的 / 79
二、内容要求 / 80
三、实施建议 / 82
第七节 远程访问安全 / 86
一、目的 / 86
二、内容要求 / 86
三、实施建议 / 88

第八节 安全监测和应急预案演练 / 90
一、目的 / 90
二、内容要求 / 90
三、实施建议 / 92
第九节 资产安全 / 98
一、目的 / 98
二、内容要求 / 98
三、实施建议 / 99
第十节 数据安全 / 101
一、目的 / 101
二、内容要求 / 101
三、实施建议 / 102
第十一节 供应链管理 / 106
一、目的 / 106
二、内容要求 / 106
三、实施建议 / 107
第十二节 落实责任 / 109
一、目的 / 109
二、内容要求 / 109
三、实施建议 / 110
附录 I 相关政策文件综述 / 113
附录II 重大工业控制系统信息安全事件一览 / 197
附录III 标准术语一览表 / 203

1 第一章

工业信息安全的重大意义

第一节　工业信息安全是助力两化深融的基础保障

第二节　工业信息安全是实现制造强国战略的重要支撑

第三节　工业信息安全是建设网络强国的必然要求

第一章 工业信息安全的重大意义

工业信息安全是网络强国战略的重要组成部分，是保障国家总体安全的重要内容，是实施制造强国战略和推进“互联网+”行动计划的基础条件。习近平总书记在中央网络安全和信息化领导小组第一次会议上强调，“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业”。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上再次强调，“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进”。习近平总书记从战略高度充分阐述了安全与发展的辩证关系，为做好工业信息安全工作指明了方向。

第一节 工业信息安全是助力两化深融的基础保障

工业化和信息化的融合发展是新时期我国促进工业由大变强，支持国民经济顺利转型升级、提质增效的核心举措，是保障互联网与制造业融合创新的重要途径，是我国工业化与信息化发展面临的关键机遇。在推动两化深度融合发展的过程中，工业信息安全具有重要意义，提升工业信息安全保障能力显得尤为重要。

工业控制系统是我国工业的核心组成部分，是钢铁石化、高端装备、电力系统、轨道交通、核设施等重点工业领域的核心中枢。工业控制系统

信息安全事关经济发展、社会稳定和国家安全。随着工业 4.0、两化深度融合、“互联网 +”、“中国制造 2025”、“智能制造”等战略的提出，工业化和信息化的融合发展不断深入，工业控制系统面临的各类安全问题和风险愈发凸显。因此，在推进两化深度融合发展中，必须将工业信息安全摆上战略位置，提高思想重视程度，推进落实各项工作，为两化深度融合提供安全保障。

第二节 工业信息安全是实现制造强国战略的重要支撑

工业信息安全的保障能力和水平是制造强国战略顺利实施的基础条件，是新一轮制造业科技革命和产业变革的根本支撑。《中国制造 2025》强调指出，要以加快新一代信息技术与制造业深度融合为主线，以推进智能制造为主攻方向，推动我国从制造业大国向制造业强国转变。该文件明确提出，要加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系，并加强安全产品、技术、标准的研发，实施一批安全工程，这标志着安全能力建设已成为制造强国建设的重要内容。随着《中国制造 2025》全面推进实施，工业信息安全的重要性日益凸显。没有工业信息安全，“中国制造 2025”宏伟目标将难以顺利实现。

保障工业控制系统的安全可靠是实现工业智能化发展的关键环节，自主可控的设备产品、技术和服务是保障重点行业工业控制系统信息安全的根本。当前，我国重要关键设备和基础软件绝大多数采用国外产品，安全基础不牢，核心技术产品受制于人，安全风险不容忽视。只有牢牢抓住工业信息安全的主动权、控制权，推动实现重要工业控制设备、系统和平台的安全可控，才能有效推进《中国制造 2025》战略目标的落地实施，才能缔造真正意义上的制造强国。

第三节 工业信息安全是建设网络强国的必然要求

我国已经发展为网络大国，正在为实现网络强国的战略目标而不懈努力。工业企业是国民经济的主体，事关经济的健康发展和社会的稳定，是立国之本、兴国之器、强国之基。工业领域的信息安全是工业经济发展的安全屏障，是网络安全的重要组成部分，也是建设网络强国的题中应有之义。

当前，我国工业与信息化的关联度越来越紧密，在“中国制造2025”、“互联网 +”等行动计划推动下，工业信息化水平大幅提升，工业信息安全成为网络强国建设中不可回避的重要内容和新的课题。近年来，国内外工业信息安全形势十分严峻，来自外部的网络攻击愈发严重，震网（Stuxnet）、Duqu、火焰、Shamoon 和 Havex 等信息安全威胁频现，攻击范围和影响程度愈加广泛。随着城市基础设施越来越依赖网络和计算机控制系统，其遭受网络攻击的风险也在加剧。城市基础设施一旦遭受攻击，必然会对人们的日常生活造成直接影响，甚至引起社会恐慌，尤其是在电力、能源、供水等领域，极容易引发灾难性后果。因此，大力提升工业信息安全能力，健全工业信息安全环境，是支撑网络强国建设稳步推进的必然要求。