CCID Testing and Evaluation Technology for Intelligent Manufacturing
智能制造测试与评价技术丛书

工业控制系统测试与评价技术

中国电子信息产业发展研究院 | 编著

Testing and Evaluation Technology for Industrial Control System

工业控制系统（ICS）是由计算机设备与工业过程控制部件组成的自动控制系统

主要包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

工业控制系统测试与评价技术

Testing and Evaluation Technology for Industrial Control System

中国电子信息产业发展研究院 | 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

工业控制系统测试与评价技术 / 中国电子信息产业发展研究院编著. -- 北京 : 人民邮电出版社, 2017.2
（智能制造测试与评价技术丛书）
ISBN 978-7-115-43791-4

Ⅰ. ①工… Ⅱ. ①中… Ⅲ. ①工业控制系统－系统测试②工业控制系统－系统评价 Ⅳ. ①TP273

中国版本图书馆CIP数据核字(2016)第290067号

内 容 提 要

本书以工业控制系统（ICS）的测试与评价为主线，在论述 ICS 的概念与内涵及主要特征的基础上，给出了 ICS 测试与评价的技术框架，然后从 ICS 的硬件测评方法、软件测评方法、网络协议测评方法、安全测评方法与工程实战等多个角度论述了 ICS 测试与评价技术。

本书适合希望了解工业控制系统测试具体方法和过程的测试工程师阅读参考。

◆ 编　　著　中国电子信息产业发展研究院
责任编辑　杨　凌
责任编辑　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷
◆ 开本：700×1000　1/16
印张：25　　2017 年 2 月第 1 版
字数：410 千字　　2017 年 2 月河北第 1 次印刷

定价：99.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

丛书序言

在蒸汽机出现后的短短200多年间，工业文明所缔造的社会财富，远远超越过去数千年的总和。它是人类文明的精华，又创造了更璀璨的文明。这个世界从来没有像今天这样繁荣、昌盛和强大，但也从没有像今天这样迷茫和脆弱。能源危机、生态危机、金融危机、经济危机已在不断告诫人们历经三次革命的工业体系需要新的变革。工业改变世界，谁在改变工业？

进入21世纪以来，新一轮科技革命和产业变革正在孕育兴起，全球科技创新呈现出新的发展态势和特征。以智能制造为核心，信息技术、生物技术、新材料技术、新能源技术广泛渗透，带动几乎所有领域都发生了以数字化、网络化、智能化、绿色化、服务化为特征的群体性技术革命，这是新一轮的工业革命。

在新一轮的工业革命浪潮中，无论是德国的“工业4.0”、美国的“工业互联网”，还是日本提出的发展战略，都是在突出本国技术优势的基础上，力争抢占世界制造业的制高点。由于各国科技与工业发展的优势和基础不同，智能制造呈现出各自不同的特点。美国作为世界互联网的发源地，正在使用其强大的信息技术，提出了以信息物理系统（CPS）为主要特征的智能制造。德国依靠工业的厚重根基，提出了“工业4.0”的技术解决方案。日本始终不遗地坚持贯彻精益生产的理念。中国制定了符合我国情况的发展战略——“中国制造2025”，积极推动“互联网+”行动，破解制造业发展存在的若干问题，这是强国之策、利民之举！

智能制造是用人工智能技术解决制造的问题。摆在我们面前的问题，第一是要解决做什么，第二是解决怎么做。

做什么？《中国制造 2025》给出了行动纲领，它吸取了美国、德国、日本的所长，又结合了中国的特点，聚焦在五大工程——创新体系工程、智能制造工程、绿色制造工程、工业强基工程、高端装备工程。其中把智能制造工程作为主攻方向，以使我们的制造业由大变强。《中国制造 2025》明确要聚焦新一代信息技术产业、高档数控机床和机器人、航空航天装备、海洋工程装备及高技术船舶、先进轨道交通装备、节能与新能源汽车、电力装备、农机装备、新材料、生物医药及高性能医疗器械十大重点领域。

怎么做？习近平总书记强调，实施创新驱动发展战略，最根本的是要增强自主创新能力，最关键的是要把核心技术和关键技术牢牢掌握在自己手中，最重要的是要坚定不移地走中国特色自主创新道路。在日趋激烈的全球综合国力竞争中，我们没有更多选择，非走自主创新道路不可。

本丛书在当前发展智能制造为迫切任务之时，应时推出，给出了智能制造的基本概念及主要内容介绍，为广大读者作向导，实为难得。尤其本丛书聚焦智能制造关键应用的测试与评价技术，有望为智能制造提出一套建设参考标准和规范，更是智能制造规范发展的重要工作。丛书由中国电子信息产业发展研究院卢山院长和黄子河副院长牵头，研究院及中国软件评测中心四十多位一线有丰富检测评估经验的专家和技术人员参与了本套丛书的撰写工作。目前该丛书已经完成《智能制造测试与评价概论》《工业控制系统测试与评价技术》《工业机器人测试和评价技术》《智能网联汽车测试与评价技术》《工业大数据测试与评价技术》及《FPGA 软件测试与评价技术》的编写工作。尽管可能有些人对书中的一些具体概念、提法、重点把握及技术细节会有不同的看法，但我认为，一方面，学术需要争论，另一方面，我们会通过智能制造的实践与发展逐步走向共识和更正确、更深刻。智能制造与制造业的产品和服务一样，需要高质量实施。因此，这一套丛书在我国是先行的、引领性的、有重要价值的。相信本书能为中国制造从数量到质量，从制造到智造发挥重要作用。

中国工程院院士 卢第柏

2017 年 2 月 20 日于西安交通大学

《工业控制系统测试与评价技术》

编 委 会

前　言

制造业是国民经济的主体，是立国之本、兴国之器、强国之基。自 18 世纪中叶开启工业文明以来，世界强国的兴衰史和中华民族的奋斗史一再证明，没有强大的制造业，就没有国家和民族的强盛。打造具有国际竞争力的制造业，是我国提升综合国力、保障国家安全、建设世界强国的必经之路。

随着新一代信息技术与制造业深度融合，各国都在加大科技创新力度，推动 3D 打印、移动互联网、云计算、大数据、生物工程、新能源、新材料等领域取得新突破。技术进步正在引发影响深远的产业变革，形成新的生产方式、产业形态、商业模式和经济增长点。特别是国际金融危机发生后，发达国家纷纷实施“再工业化”战略，制定以重振制造业为核心的再工业化战略。美国发布《先进制造业伙伴计划》《制造业创新网络计划》，德国发布《工业 4.0》，日本发布 2014 年度版《制造业白皮书》，英国发布《英国制造 2050》等。

新中国成立尤其是经过改革开放 30 多年的发展，我国制造业持续快速发展，建成了门类齐全、独立完整的产业体系，产业规模达到整个世界制造业的 20% 左右，有力推动了工业化和现代化进程。但与世界先进水平相比，我国制造业自主创新能力不足，关键核心技术受制于人，品牌质量水平不够高，产业结构不尽合理，仍然“大而不强”。在当前全球产业竞争格局发生重大调整的背景下，我国于 2015 年 5 月印发了《中国制造 2025》，旨在紧紧抓住这一重大历史机遇，实施制造强国战略，加强统筹规划和前瞻部署，把我国建设成为引领世界制造业发展的制造强国。

工业控制系统经过几十年的发展，系统结构从最初的CCS（计算机集中控制系统），到第二代的DCS（分散控制系统），发展到现在流行的FCS（现场总线控制系统）。同时，随着工业化与信息化进程的不断交叉融合，工业控制系统已广泛应用于电力、水力、石化、医药、食品制造、交通运输、航空航天等工业领域，其中超过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。工业控制系统已经成为国家关键基础设施的重要组成部分，工业控制系统的安全可靠关系到国家的战略安全。

在智能制造体系下，工业控制系统与信息系统高度集成，打破了工业控制系统的封闭环境，工业控制系统呈现开放性，基于PC架构的计算机普及与应用，Windows平台的广泛应用，基于IEEE 802.3的工业以太网普及，大量采用TCP（UDP）/IP网络协议，各种工控协议交互和兼容，传统的控制领域正经历着一场前所未有的变革。对诸如图像、语音信号等大数据量、高速率传输的要求，又催生了当前在商业领域风靡的以太网与控制网络的结合，这股工业控制系统网络化浪潮又将诸如嵌入式技术、多标准工业控制网络互联和无线技术等多种当今通用技术融合进来，使得当前的工业控制系统越来越复杂化、信息化和通用化。但是，工业控制系统在全球化、开放、互通的信息网络环境下，基础网络、关系国家安全的重要信息系统的运行以及其中的大量数据信息存在着重大的安全隐患，一旦工业控制系统信息安全出现漏洞，将对工业生产运行和国家经济安全造成重大威胁，而且随着工业控制系统的复杂化，工业控制系统安全防护、漏洞检测将变得越来越难，从而加剧了工业控制系统的安全隐患。

为了保障工业控制系统的安全可靠运行，对其进行系统评测并定期开展安全检查和安全评估是十分必要的。中国软件评测中心作为我国权威的第三方软、硬件产品及系统工程质量安全与可靠性检测机构，基于长期以来在工业控制系统安全攻防的研究和质量、安全测评领域积累的理论和工程实践经验，组织编写了本书，并编入《智能制造测试与评价技术丛书》中。

本书以工业控制系统测评技术为主线，共分为8章。

第1章概要介绍了工业控制系统的基本概念、典型架构、关键技术、应用现状和发展趋势等，并通过对近年来工业领域内发生的事故分析了工业控制系

统安全可靠的重要性，以及开展工业控制系统评测的意义和必要性。

第 2 章主要介绍工业控制系统测评的基础理论和方法，对测评标准、测评体系、测评方法和过程管理等进行了重点阐述。通过本章，读者可以直观了解工业控制系统测评。

第 3 章主要介绍在工业控制系统领域开展测评的国内外的实验室建设情况，并介绍了几款专业测评工具。

第 4 至 7 章分别从软件、硬件、网络和信息安全等角度对工业控制系统的方法进行了具体阐述，并在第 8 章通过具体的案例对工业控制系统测评的实操过程进行了剖析，通过直观的感受引导读者准确把握系统测评的过程。

限于时间、条件与水平，本书还存在需要进一步完善提高的地方，衷心希望广大读者与各界人士给予批评指正。

作者

2016 年 10 月于北京

目 录

Chapter 1 第1章 工业控制系统概述

1.1 工业控制系统的基本概念

工业控制系统（Industrial Control System，ICS）是用于工业生产的多种控制系统的统称，包括监控和数据采集（Supervisory Control And Data Acquisition，SCADA）系统、分布式控制系统（Distributed Control System，DCS）、可编程逻辑控制器（Programmable Logic Controller，PLC）等，按照实现功能和通信网络的不同，可以分为管理调度层、网络通信层、集中监控层、现场控制层和采集执行层。

工业控制系统在几十年之内已经完成了多次更新换代：第一次是从20世纪50年代开始，由之前的气动、电动单元组合式模拟仪表、手动控制系统升级为使用模拟回路的反馈控制器，形成了使用计算机的集中式工业控制系统。第二次大约是在20世纪60年代，工业控制系统开始由计算机集中控制系统升级为集中式数字控制系统。系统中的模拟控制电路开始逐步更换为数字控制电路，并完成了继电器到可编程逻辑控制器的全面替换。由于系统的全面数字化，工业控制系统使用更为先进的控制算法与协调控制，从而使工业控制系统发生了质的飞跃。但由于集中控制系统直接面向控制对象，因此在集

中控制的同时也集中了风险。第三次始于20世纪70年代中期，由于工业设备大型化、工艺流程连续性要求增加以及工艺参数控制量的增多，已经普及的组合仪表显示已经不能满足工业控制系统的需要。集中式数字控制系统逐渐被离散式控制系统所取代。大量的中央控制室开始使用CRT显示器对系统状态进行监视。越来越多的行业开始使用最新的离散式控制系统，包括炼油、石化、化工、电力、轻工以及市政工程。第四次是在20世纪90年代后期，集计算机技术、网络技术与控制技术于一体的全分散、全数字、全开放的工业控制系统——现场总线控制系统（FCS）应运而生。相比之前的分布式控制系统，现场总线控制系统具有更高的可靠性、更强的功能、更灵活的结构、对控制现场更强的适应性以及更加开放的标准。不同时期的工业控制系统如图1-1所示。

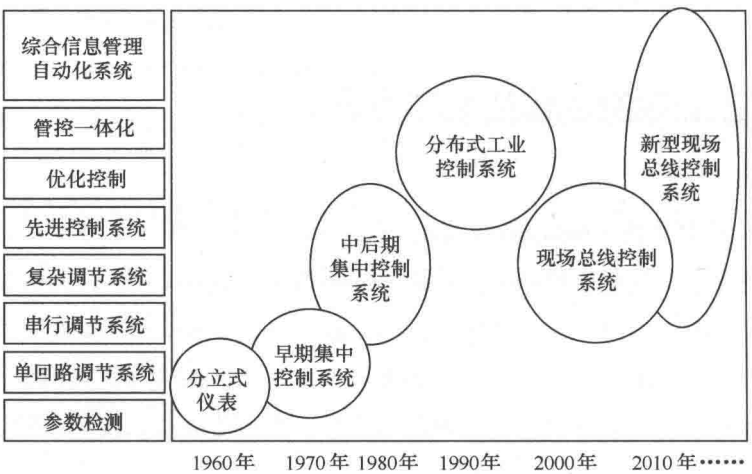

图1-1　不同时期的工业控制系统

1.2　工业控制系统的典型架构

工业控制系统一般分为5层，包括管理调度层、网络通信层、集中监控层、现场控制层和采集执行层，如图1-2所示。