工业控制系统信息安全指南

范科峰 高林 姚相振 周睿康 编著

科学出版社

工业控制系统信息安全指南

范科峰　高　林
姚相振　周睿康　编著

科学出版社
北京

内 容 简 介

随着工业化和信息化的迅猛发展，工业控制系统越来越多地采用信息技术和通信网络技术，工业控制系统信息安全问题面临严峻的挑战。本书全面阐述了工业控制系统相关信息安全概念，详细分析了工业控制系统信息安全脆弱性以及近年来相关安全事件，对国内外的工业控制系统信息安全发展现状做了介绍。同时本书提出了工业控制系统信息安全标准体系，对关键技术做了说明，还列举了一些行业的安全防护体系建设案例。最后总结了目前工业控制系统信息安全发展中存在的问题，综合分析了未来的发展趋势。

本书可以作为广大从事工业控制系统安全管理、应用开发、部署与管理工作的高级技术人员的参考书，也可以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的本科高年级学生、研究生的参考书。

图书在版编目（CIP）数据

工业控制系统信息安全指南 / 范科峰等编著. —北京：科学出版社，2016.12

ISBN 978-7-03-050925-3

Ⅰ. ①工… Ⅱ. ①范… Ⅲ. ①工业控制系统—信息安全—指南

Ⅳ. ①TP273-62

中国版本图书馆 CIP 数据核字（2016）第 287135 号

责任编辑：赵丽欣 张瑞涛 / 责任校对：刘玉靖

责任印制：吕春珉 / 封面设计：东方人华

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

三河市骏杰印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2016 年 12 月第 一 版 开本：787×1092 1/16

2016 年 12 月第一次印刷 印张：9 1/4

字数：225 000

定价：40.00 元

（如有印装质量问题，我社负责调换〈骏杰〉）

销售部电话 010-62136230 编辑部电话 010-62134021

序

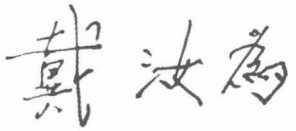
在我国社会主义现代化进程中，党中央高度重视网络安全和信息化工作。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上明确指出，“要做好信息化和工业化深度融合这篇大文章，发展智能制造，带动更多人创新创业”，同时“还要正确处理好安全和发展的关系”，保障我国工业信息化建设工作稳步推进。这是党中央从增强我国工业制造基础能力、保障国家安全、实现制造强国奋斗目标的战略高度作出的重要指示。

随着信息化和工业化的深度融合，工业控制系统技术和产品形态不断演进，从单机趋向互联，从封闭趋向开放，从自动化趋向智能化。工业控制系统在促进生产力显著提高的同时，面临着日益严峻的信息安全威胁。工业控制系统信息安全已经成为国家网络安全的重要组成部分，是推动“中国制造 2025”、制造业与互联网融合发展的基础保障。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，因此开展工业控制系统信息安全关键技术及标准研究显得尤为重要和迫切。

近年来，范科峰博士等人率领技术团队在工控系统安全标准研制和测评能力建设中一直不断学习，大胆实践创新，注意总结经验，取得了一定的研究成果，提出了一些新的理念和方法，本书反映了这支团队投身工控系统安全保障研究的进展。

本书深入浅出地剖析了当今影响工业控制系统信息安全保障的主要要素，从政策、标准、管理、技术等多角度分析了我国当前工业控制系统信息安全防护水平，并提供了参考案例。

吾生也有涯，而知也无涯。工控系统信息安全问题和对策是不断发展的，其信息安全保障工作需要不断创新发展。希望本书作者及其团队诸位同仁继往开来，努力耕耘，在工业控制系统两化深度融合的基础上向智能化发展，在信息安全保障领域取得更加丰硕的成果。



前　言

随着两化深度融合进程的快速推进，信息技术在智能电网、智能交通、工业生产系统等工业控制领域得到了广泛应用，极大地提高了企业的综合效益。为实现系统间的协同和信息共享，工业控制系统也逐渐打破了以往的封闭性：采用标准、通用的通信协议及软硬件系统，甚至有些工业控制系统也能以某些方式连接到互联网等公共网络中。这使得工业控制系统也必将面临病毒、木马、黑客入侵、拒绝服务等传统的信息安全威胁，而且由于工业控制系统多被应用在电力、交通、石油化工、核工业等国家重要领域中，其安全事故造成的社会影响和经济损失将更为严重。工业控制系统作为各国关键基础设施的重要组成部分，已逐渐成为黑客攻击的重点目标，也逐渐成为国与国之间博弈与较量的主战场，其重要性不言而喻。

本书全面介绍了工业控制系统信息安全相关的基本概念、安全技术和标准体系，系统阐述了国内外工业控制系统信息安全现状，系统分析了工业控制系统的脆弱性。本书主要从政策、标准、技术、方案等方面展开了针对性阐述，可以作为广大从事工业控制系统网络安全管理工程设计、应用开发、部署与管理工作的高级技术人员的参考书，也可以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的本科高年级学生、研究生的参考书。

为了方便读者阅读，下面对本书的框架作简单介绍。

第 1 章详细介绍了工业控制系统的基础概念，对 PLC、DCS、SCADA 进行了详细介绍，包括它们的基本结构、功能特点以及应用情况。

第 2 章对工业控制系统信息安全的脆弱性做了分析，阐述了国内外工业控制系统信息安全现状，对国内外的安全平台建设情况作了说明。

第 3 章介绍了工业控制系统信息安全标准体系及关键标准。

第 4 章对工业控制系统信息安全的关键技术以及这些技术的相关产品和测试工具等做了详细说明。

第 5 章对目前发生的工业控制系统信息安全事件进行了说明与分析，并进行了详细的对比。

第 6 章介绍了一些行业的工业控制系统信息安全防护体系的建设案例。

第 7 章简要说明了当前工业控制系统信息安全存在的主要问题，并对未来技术发展趋势作了说明。

本书受工业和信息化部工控安全评估专项（工信软函[2015]366 号、工信软函[2016]1181）、国家智能制造专项（京财经一指[2015]1170 号）、国家科技支撑计划课题（No.2012BAI23B07）的资助，并得到工业和信息化部信息化和软件服务业司有关领导、中央网信办网络安全协调局有关领导、中国电子技术标准化研究院有关领导的支持和指导，李琳、郑安兵、夏冀、苏树伟、高魏轩等科研人员也积极贡献他们的智慧和力量，在此一并表示感谢。

受时间及水平所限，本书内容难免有错漏之处，希望读者朋友批评指正。若有任何意见或建议，请发送邮件至 fankf@126.com。

目　录

第 1 章　工业控制系统技术基础

1.1　工业控制系统

1.1.1　工业控制

工业控制是指使用计算机、微电子、电气等技术手段，使工厂的生产和制造过程更加自动化、效率化、精确化，并具有可控性及可视性。工业控制技术的出现和推广带来了第三次工业革命，使工厂的生产速度和效率提高了 300%以上。20 世纪 80 年代初，国外先进工控技术被广泛引进我国，使用比较广泛的工业控制产品有可编程逻辑控制器（Programmable Logic Controller，PLC）、分布式控制系统（Distributed Control System，DCS）、数据采集与监视控制系统（Supervisory Control And Data Acquisition，SCADA）、变频器、触摸屏、伺服电机、工控机等。这些技术产品很大地推动了我国的制造业自动化进程，为我国现代化建设做出了巨大贡献。

工业控制在电力、石化、水利、航空航天、汽车等领域有着不可替代的优势。

1.1.2　工业控制系统

目前，在工业领域中使用的工控系统主要包括 SCADA、DCS、PLC、远程终端（Remote Terminal Unit，RTU）、智能电子设备（Intelligent Electronic Device，IED）等，统称为工业控制系统（Industrial Control System，ICS）。其中以远程数据采集为基础，对生产过程进行集中控制的 SCADA 系统是现代电力、石油、天然气、铁路、供水、化工等基础产业生产系统的神经中枢。

在发达国家，ICS 的技术发展已经较为纯熟，应用十分广泛。目前，全世界在线运行的 SCADA 系统已超过 300 万套。而 DCS 以及 PLC 的在线使用更是远超 SCADA，全世界大多数中小型工业企业都在其工业自动化方案中普遍使用了 DCS 和 PLC。

我国工业控制技术虽然起步较晚，但发展迅速，到“十二五”期间，ICS 已在能源工业、电力工业、交通运输业、水利事业、公用事业和装备制造企业得到广泛应用。国家关键基础设施对 ICS 已经形成不可分割的依赖关系，ICS 已成为我国现代工业自动化、智能化的关键。

工业控制系统的典型结构如图 1-1 所示。

1.1.3　工业控制系统与 IT 系统比较

最初的 ICS 与 IT 系统不具备相似性，ICS 是一个独立的系统，使用的是专用的控制协议以及特定的软硬件。但近年来，应用更广、成本更低的网络技术正在逐渐取代

这种专用的解决方案。目前 ICS 普遍采用 IT 解决方案来推动企业的互联和远程访问能力，一方面，这一技术路线使得 ICS 能够支持新的 IT 能力，打破了 ICS 的“信息孤岛”状态，实现了数据的共享联通。另一方面，ICS 的网络化也增加了其面临的信息安全风险。更为严重的是，当前在普遍应用中的信息安全解决方案都是用于解决典型 IT 系统的，因此把这些信息安全解决方案直接移植到 ICS 环境中要非常谨慎，必须全面考虑 ICS 的特殊性，形成符合 ICS 特性的信息安全解决方案。

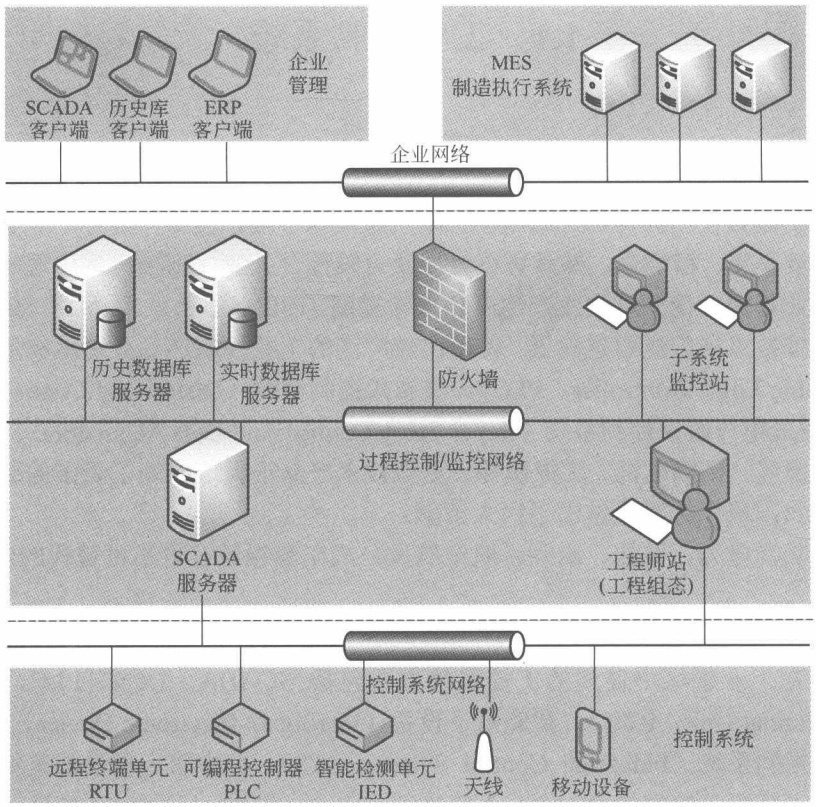


图 1-1　典型工业控制系统结构图

ICS 的特殊性要求包括以下几点。

1. 性能要求

ICS 与 IT 系统在性能要求上具有较大差异，ICS 通常采用实时通信。在系统设计与建设时，延迟和抖动都必须限定在可接受的范围内，因此对 ICS 来说，为保证其实时性，系统一般不能使用高流量的通信方式。与此相反，IT 系统通常要求高流量的通信方式，并且可以忍受很大程度上的延迟和抖动现象。

2. 可靠性要求

为保证生产过程连续性，最大程度降低生产成本，ICS 大多要求全年不间断工作，因此 ICS 非预期停机带来的经济损失是不可接受的。一般情况下，ICS 的停机必须提前

规划并按照规划时间表严格执行，在 ICS 部署上线前，必须完成详尽的测试工作，确保 ICS 可用性。另外，ICS 通常都会进行冗余设计，通过备份来增加系统的可靠性，备份系统并行运行以防止 ICS 出现未知故障。相对而言，IT 系统中的传统技术如重启系统等是 ICS 不可接受的解决方案。

3. 风险管理要求

IT 系统信息安全防护最需要关注的是数据的保密性和完整性，而对于 ICS 而言，更需要关注的是人员安全、生产安全、环境危害等，这就要求 ICS 的运行、维护、管理人员要深刻领悟功能安全和信息安全之间的重要关系。

4. 体系结构要求

在 IT 系统中，无论集中式还是分布式操作系统，其信息安全防护工作主要关注的是 IT 资产中存储与传输的数据信息。对于 ICS，PLC、DCS 控制器、操作员站等系统核心终端需要特别防护。IT 系统和 ICS 在体系结构的防护对象和防护目标上存在本质不同。

5. 物理安全要求

传统 IT 系统对环境一般没有特殊影响，而 ICS 在物理上会产生较为复杂的相互作用，例如由于系统漏洞引发的信息安全威胁，可能会对环境产生恶劣影响，从而引发安全生产事故。因此，对于 ICS 所集成的信息安全功能必须通过严格的上线检测，从而保证这些新技术、新功能不会影响正常的 ICS 功能。

6. 时间响应要求

传统 IT 系统在实现安全访问控制时可以不必过分要求系统的时间响应，但是对一些 ICS 而言，自动响应时间或者人机交互响应时间要求是非常苛刻的，例如为保证 HMI 设备的终端安全，需要使用密码授权和身份认证，但是这些安全功能不能阻碍或干扰 ICS 的紧急动作，要确保关键紧急动作的信息流不被中断或干扰。

7. 操作系统安全要求

传统的 IT 系统安全控制措施不完全适用于 ICS 操作系统，工业网络通常更为复杂，由于实时性、可用性、可靠性的要求，ICS 中的软硬件很难及时进行补丁升级。

8. 运算资源要求

ICS 通常为资源受限系统，在设计之初并不包含典型的信息安全防护功能，ICS 组件没有可用于实现信息安全防护功能的资源。此外，在某些情况下，根据供应商许可和售后服务协议，ICS 不允许使用第三方信息安全技术解决方案进行安全加固。如果用户在未经供应商许可的情况下使用了第三方信息安全技术解决方案，可能导致供应商停止提供后续运维服务。

9. 通信要求

ICS 在工业现场使用的通信协议与传统 IT 系统存在巨大差别，尤其在工业现场总线层面，数据传输大多数依赖专用协议，目前主流专用协议包括 Modbus、Profibus、DNP、IEC 60870-5-104、OPC 等。

10. 配置变更要求

对于 ICS 而言，未进行补丁管理是造成信息安全问题的主要原因之一。对于传统 IT 系统，安全运维人员基于自动工具，可以将正确的安全策略和规程通过补丁进行及时更新，有效弥补系统中存在的安全防护问题。但 ICS 的软硬件补丁更新往往无法及时完成，一是 ICS 提供商需要根据生产业务流程对补丁进行完备的可用性测试，确保补丁更新不会影响企业正常业务。二是 ICS 进行补丁更新须明确列入系统计划时间表，等待系统停机检修，补丁时效性往往无法有效保障。三是多数 ICS 连续运行时间长，使用的信息化软硬件设备版本过旧，供应商不再支持提供补丁更新，企业运维人员进行配置变更、缺陷修复、策略调整等工作时，需要控制工程师、安全工程师进行有效指导，系统评估变更管理工作。

11. 技术支持要求

传统 IT 系统具备良好的可扩展性，能够支持多元化的技术路线。而 ICS 技术服务大多数由单独的供应商提供，不同供应商之间的技术方案无法进行有效融合和扩展，在安全技术支持上，运维和管理人员需要进行系统评估，确保技术方案的可实施性。

12. 系统生命周期要求

传统 IT 系统的生命周期受技术发展约束较大，一般来说生命周期在 3～5 年内。对于 ICS，由于系统的设计、研发、使用与现实生产工艺结合紧密，使用场景具有很强的特定性，因此 ICS 的生命周期一般在 15～20 年，甚至更长。这就要求系统在连续运行能力上有更为完备的设计和集成工艺。

13. 访问连接要求

传统 IT 系统通常能够进行直接有效的连接访问，但是 ICS 的访问往往存在地域上的分离，需要使用特殊的设备和技术进行安全远程访问。

对 IT 系统和 ICS 的不同之处总结见表 1-1。

表 1-1　IT 系统和 ICS 对比

分　类	IT 系统	ICS
性能要求	非实时性 响应必须是持续性的 需要高吞吐量 高的延迟和抖动是可接受的	实时性 实时响应 一定程度的吞吐量是可接受的 高的延迟或抖动是不可接受的
可用性要求	重新启动是可以接受的 根据系统操作要求，可用性的不足通常是可以容忍的	由于生产过程可用性要求，类似重新启动这样的响应是不能接受的 根据可用性要求，需要冗余系统 断电要提前数天/数周进行计划和确定时间表 高可用性要求进行完全彻底的测试

续表

分　类	IT 系统	ICS
风险管理要求	首先保证数据保密性和完整性 故障容忍不是第一重要的；瞬间停机不是主要风险 主要风险来自商业动作的延迟或中断	首先保证人身安全，其次才是保护生产过程 第一重要的是故障容忍，甚至瞬间停机也是不能接受的 主要风险是监管违规，环境破坏，人、财、物的损失
体系结构的信息安全焦点	主要是保护 IT 资产，以及在这些资产中存储或传输的信息 中央服务器需要更多保护	主要目标是保护现场系统（如 PLC、DCS 等） 对中央服务器的保护也很重要
非预期后果	传统 IT 系统有信息安全解决方案	一定要测试信息安全工具（ICS 的离线测试），以确保它们不会影响到正常的 ICS 操作
时间关键相互作用	很少关键紧急事件 限制访问控制可以通过对信息安全要求的程度来实现	对人员和其他紧急事件的响应是非常关键的 对 ICS 的访问要控制，但不应阻碍或干扰到人机交互
系统操作	使用典型的操作系统 应用自动化工具进行系统的直接升级	不同的或者专用的操作系统，通常没有内在的信息安全能力 更改软件要非常慎重，通常由软件供应商进行，因为涉及特定的控制算法以及可能会修改相应的硬件和软件
资源限制	系统由足够的资源以支持诸如来自第三方的信息安全解决方案	系统支持固定的工业生产过程，因而没有足够的内存或资源支持信息安全能力
通信	标准的通信协议 主要是有线网络，局部可能会有无线通信能力 典型的 IT 网络规程	很多专用的和标准的通信协议 多种类型的通信媒介，包括有线和无线（无线电和卫星） 网络结构复杂（现场层，控制层，管理层等）
变更管理	软件变更多样性，并且有着很好的信息安全策略和规程。过程是自动进行的	软件更新要进行测试并且逐步布置到系统中，以确保控制系统的可维护性。ICS 的断电要进行计划和确定时间表。ICS 也可能使用没有技术支持的操作系统
技术支持	允许多样化的服务	技术支持只有供应商独立进行
部件生命周期	一般是 3～5 年	一般是 15～20 年
部件访问	通常是本地，并且易于访问	通常是分离的、远程的，并且需要其他的物理媒介才能够进行访问

1.1.4　工业控制系统的关键组件

为了便于后面的讨论，本小节将描述用于 ICS 的关键组件。其中一些组件广泛应用于 SCADA、DCS 和 PLC，而另一些组件只能用于某一类特殊行业的 ICS。

1. 控制组件

下面介绍一些 ICS 的主要控制组件。

1）控制服务器

控制服务器载有 DCS 或 PLC 监控软件，监控软件可与较低级别的控制设备进行通信。通过工业网络，控制服务器可访问辅助控制模块。

2）SCADA 服务器或主终端单元（MTU）

SCADA 服务器是 SCADA 系统的主控制设备（Master）。远程终端单元（MTU）和 PLC 设备通常作为伺服控制（Slave）位于远程现场。

3）远程终端装置（RTU）

远程终端装置（RTU）也称为远程遥测装置，是一种用于支持 SCADA 远程工作站

的具有特殊用途的数据采集和控制装置。当有线通信方式实现困难时，RTU 常常配备无线接口以便于现场支持远程通信。

4）可编程逻辑控制器（PLC）

PLC 是一个小型工业计算机，通过硬件设备，如继电器、开关、定时器或计数器实现逻辑功能。PLC 能够实现复杂的过程控制，大量用于 SCADA 系统和 DCS 系统中。其他用于现场设备的控制器如 RTU 等。能够提供和 PLC 相似的功能，但却是为特殊应用设计的。在 SCADA 环境中，PLC 经常被当作现场控制设备，因为它们更经济，功能更多样，使用灵活，比起特殊用途的 RTU，配置更容易。

5）智能电子设备（IED）

IED 能够采集和传输现场数据，并能根据控制指令执行控制任务。IED 可以在一个装置中整合模拟信号的输入/输出设备、低级别控制器、通信设备和存储器。SCADA 和 DCS 系统中的 IED 通常用于实现现场自动控制。

6）人机界面（HMI）

HMI 是一种允许人工操作控制过程的软硬件集合，能够快速修改控制设置，从而改变控制目标，在紧急情况下，通过 HMI 可以进行手动控制操作确保安全。一方面，HMI 允许控制工程师或操作员配置控制器的设定点、控制算法和控制参数。另一方面，HMI 还能够显示进程的状态信息、历史信息和报告，并且可以将某些控制信息共享给操作员、管理员等其他授权用户。

7）历史数据库（data historian）

历史数据库是一种集中数据库，记录 ICS 上所有过程的信息数据。在此数据库中存储的信息可以支持从统计过程控制到企业层面规划的各类分析工作。

8）输入/输出（I/O）模块

I/O 模块可以从 PLC、RTU 和 IED 中进行数据信息收集、缓冲和传输。I/O 模块可以配置在控制服务器或单独的计算机平台上，也可以用于 HMI 等第三方控制元件。

2. 网络组件

在工业网络层次结构中，每一层网络都具有不同的特性。随着信息化程度的不断加深，控制工程师可以通过企业内网对 ICS 进行全面监控，这种方式可以让企业高层决策者及时获得设计、研发、生产、运维等数据信息。下面介绍普遍应用于各种工业网络结构的 ICS 网络组件。

1）现场总线网络

现场总线网络将传感器、数控机床、工业机器人等现场设备连接到 PLC 或其他控制器，现场总线技术的广泛使用消除了控制器和每个设备之间点到点的连接方式。控制设备使用各种专用协议与现场设备进行通信，根据控制设备和现场设备之间传递的消息内容，控制设备可识别出发送或接收该消息的现场设备身份。

2）控制网络

控制网络用于连接高级别的控制设备模块和低级别的控制模块。

3）通信路由

通信路由用于实现不同网络间的消息传递。如局域网向广域网传递数据，在 SCADA

系统中通过远距离通信媒介连接 MTU 和 RTU。

4）防火墙

防火墙通过自定义的安全防护策略检测和控制数据包，以保护网络资产安全性，防火墙有助于实现 ICS 网络安全管理及网络隔离策略。

5）调制解调器

调制解调器转换串行数字信号和网络传输信号。调制解调器通常用于 SCADA 系统，使 MTU 和远程现场设备能够进行远距离串行通信，也可以使 DCS 和 PLC 能够操作和维护现场设备。

6）远程接入点

远程接入点是工业网络中为实现系统远程访问控制而配置的设备。如智能终端连接远程接入点访问控制 ICS。

1.1.5　工业控制系统的发展趋势

ICS 的快速发展综合利用了电子信息、自动控制和通信技术，集成化、网络化、智能化是 ICS 的重点发展方向。

1. 基于虚拟仪器的工业控制系统

虚拟仪器（Virtual Instruments）是在以工业 PC 为核心的硬件平台基础上利用高性能、低成本的模块化硬件（例如插入式板卡）及驱动软件，结合高效灵活的开发软件（例如 Lab VIEW），实现测量和控制的一种仪器系统。基于虚拟仪器的 ICS 的研究将对传统的工业测控系统产生巨大的影响。

虚拟仪器有以下四大优势。

1）性能高

在以工业 PC 作为硬件平台的虚拟仪器系统中，计算机卓越的处理器和文件 I/O 功能，使得数据和信号的存储、分析、处理可以实时进行。此外，随着计算机网络技术的发展，仪器使用联接功能来分配工作任务也变得越来越普遍（最典型的例子就是超级计算机、分布式监控设备及数据/结果远程可视化），越加成熟的计算机网络使得虚拟仪器展现出更强大的优势。

2）扩展性强

1986 年，美国国家仪器公司首先提出虚拟仪器的概念，并以“软件就是仪器”作为虚拟仪器的重要标志。随着现代工业的快速发展，系统应生产要求进行不断变化、改进，其中，虚拟仪器可扩建功能已成为工程师开发测控系统必须考虑的问题。通过使用以功能强大的开发软件（例如 Lab VIEW）为基础的虚拟仪器，只需用户更新计算机或测量硬件，就能以最少的硬件投资和极少的、甚至无需软件升级即可改进整个系统。

3）开发简单

在驱动和应用两个层面上，软件所具有的一个重要优势就是模块化，它可以将复杂的大问题轻松地划分为若干个容易解决的小问题。虚拟仪器高效的软件构架能与计算机、仪器仪表和通信方面的最新技术结合在一起。简单直观的编程方式、众多的设备驱动程序、多样实用的分析表达和支持功能，可以帮助用户轻松地配置、创建、发布、维

护和修改高性能、低成本的测量和控制解决方案。

4）无缝集成

虚拟仪器从本质上说是一个集成的软硬件概念。虚拟仪器软件的高效率来自软件本身与硬件的无缝集成（例如 Lab VIEW 带有大量多样即用的函数库用于集成各种测量仪器）。旨在开发测试、测量和控制系统的虚拟仪器软件还具有广泛的 I/O 功能，帮助用户轻松地集成多个测量设备，降低系统的复杂性。由于基于虚拟仪器构建的工业控制系统具有控制性能优良、设备使用灵活、系统开发方便、经济效益突出等优势，因而它的应用特别适合于当前复杂的工业现场对工业控制系统更高更新的要求。基于虚拟仪器的控制系统具有很好的发展趋势。

2. 基于现场总线的工业控制系统

分布式控制系统（Distributed Control System，DCS）作为主流的工业控制系统，为用户提供了管理与控制相分离的有效方法，但是其封闭式结构导致的不可互操作性和造价高等缺点已经不能满足用户对控制系统开放性和低成本的迫切需要，现场总线控制系统（Fieldbus Control System，FCS）正是在这种情况下应运而生的。现场总线控制系统就是用现场总线这一开放的、具有互操作性和标准化的通信网络将现场各智能设备和控制设备连接构成的工业控制系统。

从 20 世纪 80 年代开始，各种现场总线相继产生，现已有 40 余种。较为普遍的有：基金会现场总线 FF（Foundation Fieldbus）、控制局域网络 CAN（Controller Area Network）、局部操作网络 Lon Works（Local Operating Network）、过程现场总线 Profibus（Process Fieldbus）和 HART（Highway Addressable Remote Transducer）、DeviceNet、ControlNet、P-NET。现场总线标准有：丹麦国家标准 DSF21906、德国国家标准 DIN19245、日本 JEMA 标准、美国国家标准 ANSI/NEMA 以等同方式支持的 ISA/IEC 标准草案和欧洲标准 EN50254（CLC65CX）等。多种现场总线标准并存的局面除了技术上的竞争外，商业利益上的激烈竞争也是其主要的原因。

尽管多种现场总线标准并存的局面将会在一段较长的时期内存在，但是相对于 DCS 而言，FCS 仍然具有巨大的优势。FCS 采用公开化的通信协议，遵守同一通信标准的不同厂商的设备之间可以互连互通实现信息交换。用户可以灵活选用不同生产厂家的现场总线产品来组成实际的控制系统，使系统具有较好的开放性和互操作性。智能化的现场设备具有独立自动控制的基本功能，从而实现了结构上的彻底分散，简化了系统结构，提高了系统的可靠性，降低了开发成本，另外 FCS 对多变的工业环境还具有高度适应性。近年来，为了加快新一代系统的开发，工控界正在着力于工业以太网与现场总线相结合的研究。业界普遍认为，FCS 取代 DCS 将成为可能。

1.2　可编程逻辑控制器

可编程逻辑控制器（PLC）是一种专为在工业环境应用而设计的数字运算操作系统。它采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、

计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械或生产过程。

PLC 已广泛应用于钢铁、石油、化工、建材、机械制造、汽车、轻纺、交通运输、环保等各个行业，控制内容由最初的开关量的逻辑控制增加到模拟量控制、运动控制、过程控制、数据处理、通信与联网等。在 SCADA 系统中，PLC 提供与远程终端单元 RTU（Remote Terminal Unit）同样的功能。在 DCS 中，PLC 在一个监管控制序列中作为本地控制器使用。在小型控制系统中，PLC 还常常作为主控制组件。

PLC 采用可编程的存储器，用来执行特殊指令，如 I/O 控制、逻辑、定时、计数、PID（比例-积分-微分）控制、通信、算法等。图 1-2 表示 PLC 通过现场总线控制制造过程。PLC 通过工程工作站的程序接口访问局域网上的历史数据。

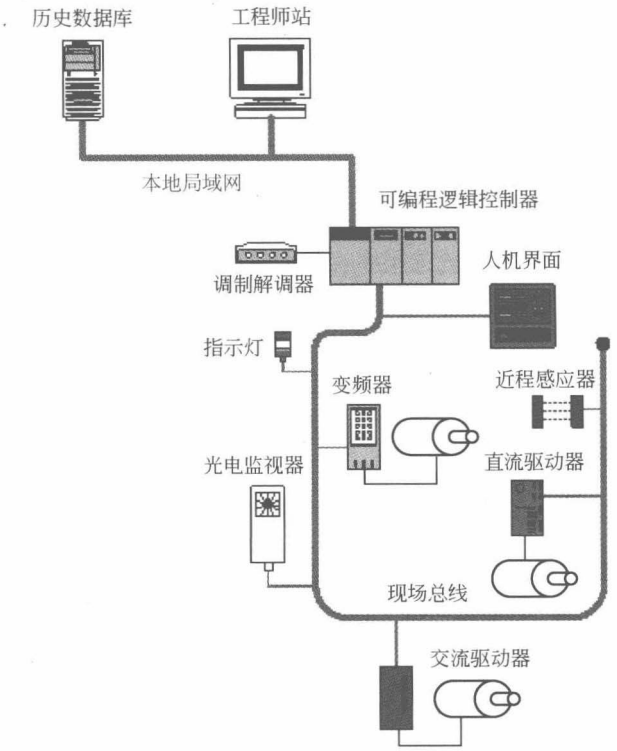


图 1-2　PLC 控制系统示例图

1.2.1　基本结构

可编程逻辑控制器实质是一种专用于工业控制的计算机，其硬件结构基本上与微型计算机相同，基本构成如下。

1. 电源

可编程逻辑控制器的电源起着十分重要的作用。控制器的正常工作是建立在一个良好、可靠的电源基础上的，因此，可编程逻辑控制器的制造商对电源的设计和制造也十分重视。一般交流电压波动在+10%（+15%）范围内，可以不采取其他措施而将 PLC 直