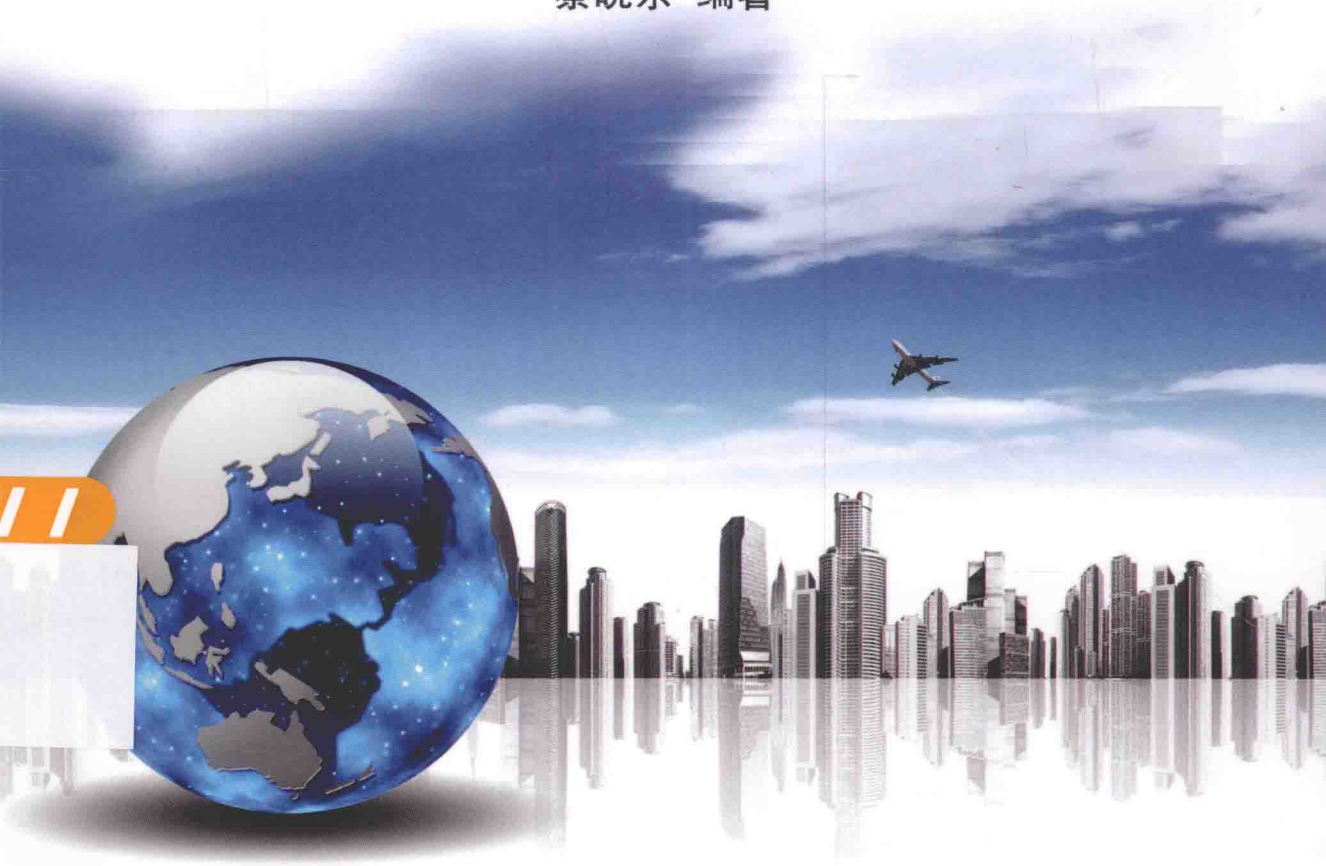
工业控制系统安全

等级保护方案与应用

Gongye Kongzhi Xitong Anquan Dengji Baohu Fangan Yu Yingyong

蔡皖东 编著



国防工业出版社
National Defense Industry Press

工业控制系统安全等级保护方案与应用

蔡皖东　编著

国防工业出版社

·北京·

内容简介

本书依据国家信息系统安全等级保护标准，并结合工业控制系统的基本特点，提出了工业控制系统安全等级保护方案，包括工业控制系统安全等级保护的定级方法、基本要求、安全设计、实施流程、系统测评以及应用示例等，可为工业控制系统安全等级保护工作提供参考和指南。

本书分为7章，分别介绍了工业控制系统信息安全概论、工业控制系统安全等级保护定级、工业控制系统安全等级保护要求、工业控制系统等级保护安全设计、工业控制系统安全等级保护实施、工业控制系统安全等级保护测评和工业控制系统安全等级保护方案应用。

本书可作为工业控制系统安全等级保护方面的参考书以及培训教材。

图书在版编目(CIP)数据

工业控制系统安全等级保护方案与应用 / 蔡皖东编著. —北京：国防工业出版社，2015.3

ISBN 978-7-118-09974-4

Ⅰ.①工… Ⅱ.①蔡… Ⅲ.①工业控制系统-安全等级-保护-方案 Ⅳ.①TP273

中国版本图书馆CIP数据核字(2015)第043876号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号 邮政编码100048)

北京京华虎彩印刷有限公司印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 15 **字数** 342千字

2015年3月第1版第1次印刷 **印数** 1—1000册 **定价** 48.00元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

前　言

工业控制系统是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统，广泛应用于电力、水利、污水处理、石油天然气、化工、交通运输、制药以及大型制造等行业，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，工业控制系统已成为国家安全战略的重要组成部分。

2010年9月，伊朗布什尔核设施遭到震网（Stuxnet）病毒攻击，导致其核设施不能正常运行。震网病毒是世界上首个专门攻击工业控制系统的计算机病毒，引起国内外的广泛关注，信息安全界将震网病毒事件列为2010年十大IT事件之一。同时，震网病毒事件也引起了世界各国对工业控制系统信息安全的高度重视。

我国工业和信息化部于2011年9月专门发文《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451号），强调了加强工业信息安全的重要性、紧迫性，并明确了重点领域工业控制系统信息安全的管理要求，重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。

工业控制系统安全保护是一项系统工程，涉及安全技术和管理的方方面面，并非是信息安全技术和产品的简单应用，而是需要建立一套行之有效的系统安全保护体制和制度。

为了应对信息安全方面的挑战，我国制定了两种信息系统安全保护制度：信息系统安全等级保护制度和涉密信息系统分级保护制度。前者主要针对非密信息系统，后者针对涉密信息系统，并制定了一系列相关技术标准和法律法规，规范了信息系统的建设和管理。

工业控制系统处理和存储的信息通常是非密信息，应当按照等级保护标准进行安全保护。然而，等级保护标准是针对信息系统制定的，而工业控制系统与信息系统存在一定的差异，不能完全照搬等级保护标准，需要根据工业控制系统的特点，对等级保护标准进行适当修改和调整，使之适合于工业控制系统安全等级保护。

本书对工业控制系统安全等级保护方案进行了探讨，内容包括工业控制系统安全等级保护的定级方法、基本要求、安全设计、实施流程、系统测评以及应用示例等，可为工业控制系统安全等级保护工作提供参考和指南。

本书没有对相关的信息安全技术做详细的介绍，读者最好具有一定的信息安全基础知识，这样有助于理解和掌握本书的内容。

全书分为7章，第1章为工业控制系统信息安全概论，介绍了工业控制系统及通信协议、工业控制系统信息安全问题、工业控制系统信息安全标准、工业控制系统信息安全等级保护方案等内容；第2章为工业控制系统安全等级保护定级，介绍了系统定级原理和方

法及等级变更；第3章为工业控制系统安全等级保护要求，介绍了第一级到第三级系统的安全保护基本技术要求、基本管理要求、整体保护能力要求、基本安全要求的应用等内容；第4章为工业控制系统等级保护安全设计，介绍了第一级到第三级系统的安全保护环境设计技术；第5章为工业控制系统安全等级保护实施，介绍了工业控制系统的系统定级、总体安全规划、安全设计与实施、安全运行与维护、系统终止等工作流程；第6章为工业控制系统安全等级保护测评，介绍了第一级到第三级系统的单元测评、系统整体测评、等级测评结论等内容；第7章为工业控制系统安全等级保护方案应用，以一个工业控制系统安全等级保护方案为例，介绍了安全保护方案设计、安全风险评估方案等内容。

本书在国家相关标准的基础上，结合工业控制系统的基本特点，提出了工业控制系统安全等级保护方案，这里谨向相关标准制定者表示敬意和感谢。希望本书能够对工业控制系统安全等级保护工作起到有益的作用。

最后，感谢西北工业大学专著出版基金对本书的大力资助。

作 者

2015年元月于西安

目　录

第 1 章　工业控制系统信息安全概论

1.1　引　　言

随着工业化与信息化的深度融合，越来越多的信息技术应用到了工业领域。目前，工业控制系统已广泛应用于电力、能源、化工、水利、制药、污水处理、石油天然气、交通运输以及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，工业控制系统安全关系到国家的战略安全。

另一方面，由于工业控制系统越来越多地采用了通用的硬件、软件以及网络设施，并且与企业管理信息系统实现了系统集成和网络互连，与互联网存在直接和间接的联系，打破了工业控制系统原来的自我封闭状态，系统越来越开放，加之运营工业控制系统的企业安全意识普遍比较淡薄，缺乏有效的安全防护，给病毒传播、远程攻击以及非法入侵等网络攻击创造了可乘之机。

2010 年 9 月 24 日，伊朗布什尔核设施遭到震网（Stuxnet）病毒攻击，导致其核设施不能正常运行。震网病毒是世界上首个专门攻击工业控制系统的计算机病毒，震网病毒通过 U 盘“摆渡”到内部网络进行传播，进而攻击与内部网络相连的工业控制系统。震网病毒事件引起国内外的广泛关注，信息安全界将震网病毒事件列为 2010 年十大 IT 事件之一。

2011 年出现的毒区（Duqu）病毒和 2012 年出现的火焰（Flame）病毒等都是专门攻击工业控制系统的计算机病毒，说明计算机病毒已经成为一种强大的网络战武器。

根据权威的工业安全事件信息库（Repository of Industrial Security Incidents，RISI）统计，截至 2011 年 10 月，全球已发生 200 余起针对工业控制系统的攻击事件。2001 年后，通用开发标准与互联网技术的广泛使用，使得针对工业控制系统的攻击事件出现大幅度增长，工业控制系统信息安全问题变得日益突出。

根据美国计算机应急响应小组（US－CERT）下属的专门负责工业控制系统安全的应急响应小组 ICS－CERT 的统计，2009 年和 2010 年发生的工业控制系统相关安全事件分别为 9 起和 41 起，2011 年则为 198 起，呈现大幅度上升趋势。这些安全事件的发生集中于能源、水利、化工以及核设施等领域，其中能源行业的安全事件在三年间共发生 52 起，占安全事件总数的 21%。

图 1－1（a）为 RISI 统计的工业控制系统攻击事件，图 1－1（b）为 ICS－CERT 统计的工业控制系统攻击事件。

与互联网上所发生的信息系统安全事件相比，针对工业控制系统的安全事件数量要少得多，但工业控制系统涉及国计民生，每一次安全事件的发生都会带来很大的影响和

危害。

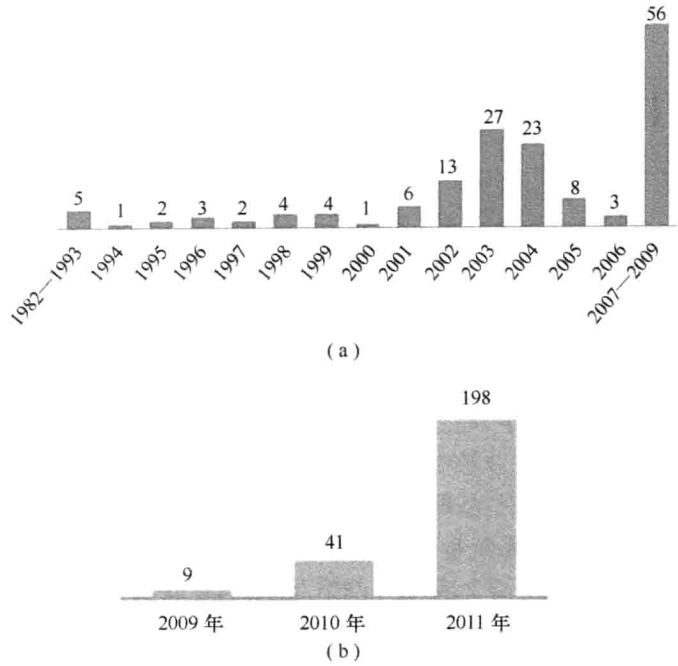


图 1-1　有关组织统计的工业控制系统攻击事件

(a) RISI 统计的工业控制系统攻击事件；(b) ICS-CERT 统计的工业控制系统攻击事件。

下面是各个工业领域所发生的典型工业控制系统安全事件。

1. 能源、石油化工控制系统安全事件

1994 年，美国亚利桑那州的盐河工程被黑客成功入侵。

2000 年，俄罗斯天然气公司 Gazprom 的网络被黑客入侵，在公司内部人员的帮助下，黑客突破了该公司网络的安全防护措施，通过木马程序修改了底层控制指令，致使该公司的天然气流量输出一度控制在外部用户手中，对企业和国家造成了巨大的经济损失。

2001 年，黑客入侵了美国加州监管电力传输系统的独立运营商计算机控制系统。

2008 年，黑客入侵并劫持了南美洲某国的电网控制系统，敲诈该国政府，在遭到拒绝后，攻击了电力传输系统，导致长时间的电力中断。

2008 年，美国国土安全局针对电力系统的一次渗透测试中，一台发电机组在其控制系统遭到攻击后发生物理损坏。

2011 年，出现了一种叫做 Night Dragon 的蠕虫病毒，专门窃取能源和石化公司的油田投标及数据采集与监控(SCADA)系统运作等敏感数据。

著名的信息安全公司 McAfee 在一份报告中披露，黑客曾入侵了 5 家跨国石油天然气公司，窃取其商业机密。

2. 水利控制系统安全事件

2001 年，澳大利亚昆士兰 Maroochy 污水处理厂的内部人员多次非法入侵 SCADA 系统，该厂发生了 46 次不明原因的控制设备功能异常事件，导致数百万升的污水流入了该地区的供水系统。

2005 年，由于工业控制系统漏洞，导致美国路易斯安那州索克水库的水量监控数据与远程监控站获得的数据不一致，致使意外排放出 10 亿加仑的水。

2006 年，美国宾夕法尼亚州哈里斯堡污水处理厂的计算机系统被一台维修用的笔记本电脑感染了病毒，导致该计算机系统被黑客入侵和控制，致使该地区农作物的灌溉大受影响。

2007 年，攻击者入侵加拿大的一个水利 SCADA 系统，通过安装恶意软件破坏了用于控制萨克拉门托河河水调度的计算机系统。

3. 核工业控制系统安全事件

1992 年，立陶宛 Inalina 核电站的计算机中心员工因对管理当局不满，故意在电厂控制程序内植入恶意程序，使控制系统功能异常。

2003 年，美国俄亥俄州 Davis Besse 核电站进行维修时，维护人员自行搭接对外连接链路，以方便在厂外进行远程维护工作。维修计算机接入核电站网络时，该计算机上携带的 SQL Server 病毒传入核电站网络，致使该核电站的控制网络全面瘫痪，系统停机将近 5 小时。

2006 年，美国 Browns Ferry 核电站因其控制网络上的通信信息过载，导致控制水循环系统的驱动器失效，使反应堆处于“高功率、低流量”的危险状态，核电站工作人员不得不全部撤离，直接经济损失达数百万美元。

2010 年，德国安全专家发现了专门攻击工业控制系统的震网病毒，该病毒感染了全球超过 45000 个网络，其中伊朗最为严重，直接造成伊朗布什尔核电站推迟发电。震网病毒专门针对西门子公司的数据采集与监控系统 SIMATIC WinCC 进行攻击，通过直接篡改 PLC 控制代码实施。而 SIMATIC WinCC 系统在中国的多个重要行业应用广泛，如钢铁、电力、能源、化工等行业。

4. 交通控制系统安全事件

1997 年，一个十几岁的少年入侵美国纽约的航空管理系统，干扰了航空与地面通信，导致马赛诸塞州的 Worcester 机场被迫关闭 6 小时。

2003 年，美国 CSX 运输公司的计算机系统因为外接移动设备感染了病毒，导致华盛顿特区的客货运输中断。

2003 年，19 岁的黑客入侵了美国休斯敦渡口的计算机控制系统，导致该系统全面停机。

2008 年，黑客攻击了波兰 LodZ 市的城市铁路系统，用一个电视遥控器改变了轨道扳道器的运行，导致 4 节车厢脱轨。

5. 制造业安全事件

1992 年，美国汽车制造公司雪弗莱的前雇员入侵了该公司的报警控制系统，通过修改程序参数，关闭了该公司位于 22 个州的应急警报系统，直到一次紧急事件发生后才被发现。

2005 年，在 Zotob 蠕虫病毒事件中，尽管在互联网与企业网、控制系统网络之间部署了防火墙，但美国还是有 13 个汽车厂因被蠕虫病毒感染而被迫关闭，50000 名生产工人被迫停止工作，直接经济损失超过 140 万美元。

2005 年的 InfraGard 大会上，BCIT 科学家 Eric Byres 声称在用普通扫描器扫描某著名

品牌的可编程逻辑控制器(PLC)时导致其崩溃,可见工业控制系统的脆弱性。

随着工业化和信息化的深度融合,工业控制系统的安全漏洞和攻击事件还会不断地增长,工业控制系统信息安全任重道远。

1.2 工业控制系统及通信协议

工业控制系统信息安全问题与工业控制系统组成及通信协议密切相关,为了更清楚地了解工业控制系统所面临的安全风险、安全需求以及工业信息安全技术,有必要对工业控制系统及通信协议做简单的介绍。

1.2.1 工业控制系统简介

工业控制系统(Industrial Control Systems,ICS)是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件,共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统,其核心组件包括数据采集与监控(SCADA)系统、分布式控制系统(DCS)、PLC、远程终端(RTU)、智能电子设备(IED)以及各个组件通信接口等。

目前,工业控制系统广泛应用于电力、能源、化工、水利、制药、污水处理、石油天然气、交通运输以及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,工业控制系统已是国家安全战略的重要组成部分。

一次典型的ICS控制过程通常由控制器、人机接口(HMI)、远程诊断与维护软件三部分组件共同完成,见图1-2。控制器执行控制逻辑运算,HMI执行信息交互,远程诊断与维护软件在出现异常的操作时进行诊断和恢复。

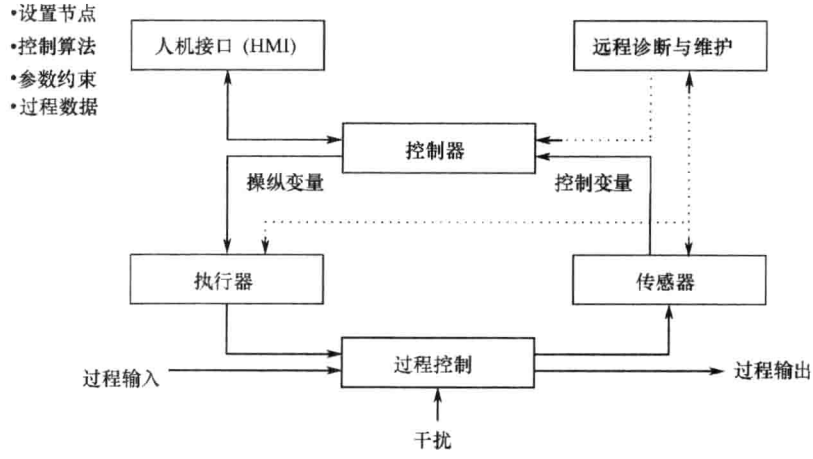


图1-2 典型的ICS控制过程

SCADA系统是工业控制系统的重要组件,通过与数据传输系统和HMI交互,SCADA系统可以对现场的运行设备进行实时监视和控制,以实现数据采集、设备控制、数据测量、参数调节以及各类信号报警等各项功能,SCADA系统总体布局如图1-3所示。SCADA系统是一种分布式计算机系统,用于控制地理上分散的设备,这些设备有时分散于数千平

方千米范围内，集中的数据采集和控制是系统运行的关键。一个 SCADA 系统控制中心通过远程通信链路对场地实行集中监视和控制，包括监视报警和过程状态数据。根据从远程工作站点收到的数据，以自动或人工方式发出管理指令，操控远程站点的控制设备。现场设备控制本地操作，例如开启和关闭阀门及断路器，采集数据和监视报警条件的本地环境。目前，SCADA 系统广泛应用于水利、电力、石油化工、电气化、铁路等分布式工业控制系统中。

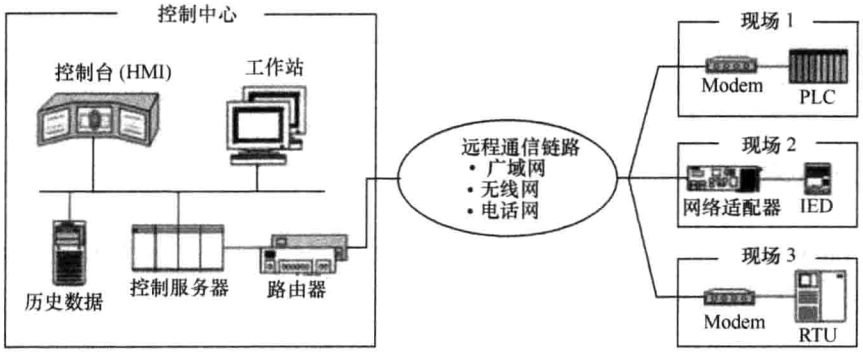


图 1－3　SCADA 系统总体布局

DCS 用于工业过程控制，主要应用于基于流程控制的行业，例如电力、石化等行业的分布式作业，实现对各个子系统运行过程的管控。DCS 是一个综合的体系结构，包含多个综合的负责局部过程任务控制的子系统和一个用于监视这些子系统的控制管理系统。

PLC 是用于控制工业设备和过程的电子装置，主要实现工业设备的具体操作与工艺控制。在 SCADA 系统和 DCS 中广泛使用 PLC 作为控制系统的执行部件，它们通过调用各个 PLC 组件来为其分布式业务提供基本的操作控制，例如汽车制造流水线等。

综上所述，DCS 和 PLC 是面向过程的，由过程驱动，能够实现闭环实时过程的控制；而 SCADA 系统是面向数据采集的，由事件驱动，SCADA 系统通常被认为是一个协同配合系统，但是一般不以实时方式进行过程控制。由于工业过程控制比分布式过程监视控制更为复杂，因此与 SCADA 系统相比，DCS 和 PLC 在更大程度上使用闭环控制。然而，实际的工业控制系统可能具有 DCS 和 SCADA 系统的双重特征，使两者的界线比较模糊，例如一个中小城市供水系统中所使用的工业控制系统可能并不严格区分 DCS 和 SCADA 系统。

SCADA 系统、DCS 和 PLC 之间还有一个区别：DCS 和 PLC 所控制的设备通常分布在工厂或车间的有限区域内，而 SCADA 系统则分布在更大的地理范围内。在通信方式上，DCS 和 PLC 通常使用工业局域网技术来实现，而 SCADA 系统通常使用远程通信技术来实现，并且需要解决由远程链路所产生的通信延迟、数据丢失等问题。

1.2.2　工控通信协议简介

在工业控制系统中，通常采用现场总线和工业以太网技术进行组网，实现网络通信。现场总线是一种传统的工业控制系统组网技术，网络传输速率较慢。工业以太网是新兴的工业控制系统组网技术，大大提高了网络传输速率，成为工业控制系统组网的主流

技术。

在工业控制系统组网中，常用的工控通信协议和标准有：MODBUS、PROFIBUS、DNP3（Distributed Network Protocol 3）、IEC 60870－5－101/104、TASE. 2（Tele－control Application Service Element 2）和 IEC 61850 等。

（1）MODBUS 协议：是由法国施耐德电气公司发明的工业控制现场总线协议，随着工业自动化的发展和互联网的广泛应用，MODBUS 协议也在不断地发展，出现了由多个 MODBUS 协议组成的 MODBUS 协议集。例如使用串行链路的现场总线协议 MODBUS RTU、MODBUS ASCII、MODBUS PLUS 以及基于以太网的 MODBUS TCP 等。MODBUS 协议采用主－从结构，提供连接到不同类型总线或者网络设备之间的客户机－服务器通信功能。客户机（主站）使用不同的功能码请求服务器（从站）执行不同的操作，服务器执行功能码定义的操作并向客户机发送响应，或者在操作中检测到差错时发送异常响应。

（2）PROFIBUS 协议：是由德国联邦科技部组织西门子等十几家公司以及多个研究机构制定的关于现场总线的德国国家标准。开始时，在 PROFIBUS 标准中只有 PROFIBUS－FMS 协议，后来先后制定了 PROFIBUS－DP 协议、PROFIBUS－PA 协议以及基于以太网的 PROFINET 协议等，形成了 PROFIBUS 协议集，目前广为使用的是 PROFIBUS－DP 协议。

（3）DNP3 协议：是由美国通用电气－哈里斯加拿大子公司基于 IEC 60870－5 标准开发的一种现场总线协议，专用于满足北美地区的应用需求。DNP3 协议定义了数据链路层、伪传输层和应用层，并使用串行链路进行数据通信。在 DNP3 协议中，只有被指定的主站能够发送应用层的请求报文，而从站则只能发送应用层的响应报文（包括主动响应报文）。DNP3 协议在 TCP/IP 协议上实现时，将 DNP3 协议的整个链路数据单元作为 TCP/IP 协议的应用层数据进行传输。

（4）IEC 60870－5－101/104 标准：IEC 60870－5－101 标准是远动设备及系统传输规约中基本远动任务配套标准，适用于串行数据传输的远动设备和系统；而 IEC 60870－5－104标准则是基于标准传输规约集的 IEC 60870－5－101 网络访问标准，即 IEC 60870－5－104 是 IEC 60870－5－101 在 TCP/IP 协议上的实现。DNP3 协议和 IEC 60870－5－101/104 标准都遵从 IEC 60870－5 标准的数据链路帧格式（IEC 60870－5－1）和链路传输过程（IEC 60870－5－2），两者之间存在很多相似之处。

（5）TASE. 2 标准：也称为 ICCP（Inter Control－center Communication Protocol），是一种工业控制系统底层网络通信协议，已经成为国际标准，主要用于在多个控制中心之间通过局域网或广域网实现实时数据及其他信息的相互传输。

（6）IEC 61850 标准：是一种针对变电站自动化的数据通信标准，以支持不同厂商变电站自动化系统和产品的互操作性。IEC 61850 标准按照变电站自动化系统所要完成的控制、监视和继电保护三大功能，从逻辑上将系统分为三层，即变电站层、间隔层和过程层，并定义了三层间的 10 种逻辑接口。

随着 TCP/IP 协议的广泛应用，工控通信协议对 TCP/IP 协议的支持成为必然的发展趋势，同时也引入了由此而带来的工业控制系统信息安全问题。

1.2.3　OPC 标准简介

为了支持工业控制应用软件和硬件产品之间的互操作性，需要在应用层面上解决系统集成和数据通信问题。对此，相关国际组织制定了 OPC（Object Linking and Embedding for Process Control）标准。

OPC 标准是一个工业标准，由 OPC 基金会负责制定和管理，OPC 基金会现有会员已超过 220 家，遍布全球，包括世界上所有主要的自动化控制系统、仪器仪表及过程控制系统的公司。OPC 标准基于微软公司的 OLE（Object Linking and Embedding）、COM（Component Object Model）和 DCOM（Distributed COM）技术，包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统中。OLE 也就是现在的 Active X。

OPC 标准为基于 Windows 的应用程序和现场过程控制应用建立了桥梁。在过去，为了存取现场设备的数据信息，每一个应用软件开发商都需要编写专用的接口函数。由于现场设备的种类繁多，且产品的不断升级，往往给用户和软件开发商带来很大的工作负担。系统集成商和开发商迫切需要一种具有高效性、可靠性、开放性、可互操作性的即插即用的设备驱动程序。在这种情况下，OPC 标准应运而生。

OPC 标准以微软公司的 OLE 和 COM 技术为基础，COM 是一种为了实现与编程语言无关的对象而制定的标准，该标准将 Windows 下的对象定义为独立单元，可以不受程序限制来访问这些单元。这种标准可以使两个应用程序通过对象化接口通信，而不需要知道对方是如何创建的。例如，用户可以使用 C ++ 语言创建一个 Windows 对象，它支持一个接口，通过该接口，用户可以访问该对象提供的各种功能，用户可以使用 Visual Basic、C/C ++ 、Pascal、Smalltalk 或其他语言编写对象访问程序。在 Windows NT 4.0 操作系统及其以后的版本中，COM 规范被扩展到可访问本机以外的其他对象，一个应用程序所使用的对象可分布在网络上，这种 COM 扩展被称为 DCOM。

通过 DCOM 技术和 OPC 标准，完全可以创建一个开放的、可互操作的控制系统软件。OPC 标准采用客户/服务器模式，开发访问接口的任务主要由硬件生产厂家或第三方厂家来完成，以 OPC 服务器的形式提供给用户，解决了软、硬件厂商的矛盾，很好地解决了系统集成问题，提高了系统的开放性和互操作性。

OPC 服务器通常支持两种类型的访问接口：自动化接口和自定义接口。它们分别为不同的编程语言环境提供访问机制。自动化接口是为脚本编程语言而定义的标准接口，可以使用 Visual Basic、Delphi、Power Builder 等编程语言开发 OPC 服务器的客户应用。而自定义接口是专门为 C ++ 等编程语言而制定的标准接口。

现在 OPC 标准已成为工业控制系统互连和系统集成的首选方案，为工业控制编程带来了很大的便利，用户不用为通信协议和互操作性的难题而苦恼。目前，绝大多数的自动化软件解决方案的提供者都全方位地支持 OPC 标准，否则就会被淘汰。

在工业控制领域中，系统通常由若干分散的子系统构成，并且各个子系统往往采用不同厂家的设备和方案。用户需要将这些子系统集成起来，架构成一个统一的实时监控系统。这样的实时监控系统需要解决各个分散子系统间的数据共享问题，各个子系统需要统一地协调相应的控制指令。另外，考虑到实时监控系统通常需要升级和调整，这就要求各个子系统具备统一的开放接口。

OPC 标准提供了这样的开放接口，通过这个接口，基于 Windows 的软件组件能够方便地交换数据。OPC 标准为数据源（OPC 服务器）和数据使用者（OPC 应用程序）之间的连接提供了软件接口，数据源可以是 PLC、DCS、条形码读取器等控制设备，作为数据源的 OPC 服务器既可以是和 OPC 应用程序运行在同一台计算机上的本地 OPC 服务器，也可以是运行在另一台计算机上的远程 OPC 服务器。

OPC 标准具有广泛的适用性，既适用于通过网络把最下层控制设备的原始数据提供给作为 OPC 应用程序的 HMI、SCADA、批处理等自动化程序，以至更上层的历史数据库等应用程序；也适用于应用程序和物理设备的直接连接。

基于 OPC 标准的工业控制系统主要由两部分组成（图 1-4）：

（1）OPC 服务器：OPC 服务器通常是按照各个供应厂商的硬件开发的，通过 OPC 接口屏蔽了各个供应厂商硬件和系统的差异，从而实现不依赖于硬件的系统架构。同时利用 OPC 接口的 Variant 数据类型，提供不依赖于硬件中固有的数据类型，按照应用程序的要求提供数据格式，实现数据采集等服务。

（2）OPC 应用程序：由供应厂商或第三方开发的应用程序，通过 OPC 标准接口来访问 OPC 服务器，实现数据采集、系统监视、趋势分析等服务。

图 1-4　基于 OPC 的工业控制系统组成

1.3　工业控制系统信息安全问题

1.3.1　工业控制系统安全风险

与传统的信息系统安全需求不同，工业控制系统系统设计需要兼顾应用场景与控制管理等多方面因素，以优先确保系统的高可用性和业务连续性。在这种设计理念的影响下，缺乏有效的工业安全防护措施使很多工业控制系统面临着很大的安全风险。

1. 工业控制系统潜在的风险

（1）操作系统的安全漏洞问题。由于考虑到工业控制软件与操作系统补丁兼容性的问题，在系统运行后一般不会对 Windows 平台打补丁，导致系统带着漏洞运行。

（2）杀毒软件安装及升级更新问题。用于生产控制系统的 Windows 操作系统，基于工业控制软件与杀毒软件的兼容性的考虑，通常不安装杀毒软件，给病毒与恶意代码传染与扩散留下了可乘之机。

（3）使用 U 盘、光盘导致的病毒传播问题。由于工业控制系统中的管理终端一般没有采用安全保护措施对 U 盘和光盘的使用进行有效的管理，导致因外设的滥用而引发的安全事件时有发生。

（4）设备维修时笔记本电脑的随意接入问题。在工业控制系统维护时，随意将没有安全保护措施的笔记本电脑接入工业控制系统，将笔记本电脑中存在的病毒或木马程序