高等学校网络空间安全专业“十三五”规划教材

工业控制系统信息安全

曹国彦　潘　泉
刘　勇　张定华　编

西安电子科技大学出版社
http://www.xduph.com

高等学校网络空间安全专业“十三五”规划教材

工业控制系统信息安全

曹国彦　潘　泉
刘　勇　张定华　编

西安电子科技大学出版社

内 容 简 介

本书是在我国高等教育对网络空间安全提出了更高要求的背景下编写而成的，是一本关于工业控制系统信息安全的基础教材。本书围绕工业控制系统信息安全的核心问题——防范性地化解工业控制系统风险，首先介绍了工业控制系统的基本组成单元及子系统(其资产性)，然后讨论工业控制系统的特性、脆弱性及所面临的威胁，引出工业控制系统所面临的风险及风险分析，最后在理解风险的基础上，从五个常用的安全控制角度介绍工业控制系统安全控制措施的基本思想、方法以及具体实现。

本书可作为信息安全和工业自动化等相关专业本科生的专业教材，也可作为工业控制系统信息安全的研究人员和工程技术人员的培训用书和参考书。

图书在版编目(CIP)数据

工业控制系统信息安全/曹国彦等编. —西安：西安电子科技大学出版社，2019.8
ISBN 978-7-5606-5340-2

Ⅰ. ① 工… Ⅱ. ① 曹… 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(2019)第 117391 号

策划编辑 陈 婷
责任编辑 盛晴琴 陈 婷
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限公司
版 次 2019 年 8 月第 1 版 2019 年 8 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 19
字 数 444 千字
印 数 1～3000 册
定 价 43.00 元
ISBN 978-7-5606-5340-2/TP
XDUP 5642001-1

高等学校网络空间安全专业“十三五”规划教材

编审专家委员会

前　言

工业控制系统信息安全的重要性不言而喻，它不仅关系到企业的正常生产运营、居民的基本生计生活需求，甚至在国家层面，也直接关系到国家工程、基础设施与稳定运行的安全。越来越多的工控系统安全事件让组织、企业、政府和国家认识到其重要性和危害性。

2014 年年底，德国联邦信息安全办公室发布了一份《2014 年信息安全报告》，这份 44 页的报告披露了一起针对 IT 安全关键基础设施的网络攻击事件，这个事件造成了重大物理伤害。受攻击的是德国的一个钢铁厂。钢铁厂遭到高级持续威胁(APT)攻击。攻击者使用鱼叉式钓鱼邮件和社会工程手段，获得了钢铁厂办公室网络的访问权。然后利用办公网络进入生产网络，操作控制网络，造成工控系统的控制组件和整个生产线被迫停止运转，从而给钢铁厂造成了重大破坏。2015 年 12 月，网络攻击者利用他们在乌克兰能源网络中的立足点关闭了三家电力配送公司，造成了持续几小时的停电。一年后，攻击者再次袭击了乌克兰的能源部门，将基辅市部分地区的电力中断了大约一个小时。著名的“震网”(Stuxnet)病毒被认为是工业控制系统攻击的典型代表。含有计算机病毒“震网”的 U 盘故意被伊朗核能设施的员工“意外”捡到，该员工把 U 盘插入内部网的计算机后，计算机组网中毒并迅速蔓延。之后通过设施内部往来陆续控制了德国西门子 PLC(可编程逻辑控制器)，让数千台离心机超载，造成物理性破坏，直接导致伊朗核开发推迟了四年之久。

众多针对工业控制系统的网络攻击让政府、组织、信息安全专业人员等认识到工业控制系统信息安全防护的重要性，在各政府与组织的主导下，相继发布了一系列针对工业控制系统安全的指导文件甚至安全标准。国际标准化组织(ISO)、国际电工委员会(IEC)、中国工业与信息化部等组织开发和发布的一系列信息安全标准和工业控制信息安全指导，用于规划、指导信息系统和工业控制系统建设与防护。这一系列标准主要有：

ISO/IEC 27001：2013 是 ISO 和 IEC 于 2013 年 10 月发布的 ISO/

IEC 27000 标准系列信息安全管理体系标准的组成部分，规定了一种管理系统，旨在明确管理控制下获取信息安全的指导。

北美电力可靠性协会(NERC)的 NERC1300 标准为关键基础设施提供保护。

国际自动化协会(ISA)安全合规研究所(ISCI)的 IEC－62443 工业和自动化控制系统(IACS)信息安全标准为第一个合格评定方案。这一标准在不断改进，并对工业控制系统及其安全进行了详细定义与指导，是最为重要的国际工业控制系统安全防护指导文件之一。

美国国家标准与技术研究所(NIST)发布的 800－12 对计算机安全和控制领域做了广泛的概述，强调了安全控制的重要性和实现安全控制的方法。NIST 于 2013 年发布的工业控制系统安全指导特别报告(NIST. SP800－82)指导怎样保护工业控制系统，包括主要的基础设施 SCADA 系统、分布式控制系统和可编程控制器。这个报告不仅提供了工业控制系统的基本拓扑、基本威胁和脆弱性识别，还提供了相应的降低风险的安全建议。这个指导报告基本奠定了工业控制系统的安全基石，很好地规范了行业。

我国工业与信息化部也相继参考国外标准发表了一系列关于工业控制系统信息安全的指导规范与标准，例如《工业控制系统信息安全防护指南》、《工业控制系统信息安全防护指引》、《工业控制系统安全控制应用指南》和《工业控制系统信息安全防护能力评价方法》等文件。我国工业与信息化部发布的系列标准与规范，为我国工业控制安全管理、运维和标准化建立了规范，极大地促进了我国工业控制系统信息安全的发展。

工业控制系统信息安全是传统的信息安全和网络安全的延伸，同时工业控制系统又具有很强的行业性。在智能制造系统中，由于新的数字制造的发展(如工业 4.0 或中国智能制造 2025)，传统的制造单元被系统地整合在智能网络里，通过局域网通信和控制链方式，显著降低了车间操作者的介入要求，增加了自动化程度，但客观上网络安全威胁蔓延至制造系统的控制单元与执行单元中，为安全生产带来了挑战。在能源工业控制系统中，能源系统的信息和物理组件深度融合，从而形成了一个通过网络通信和嵌入式实时系统组建的整合信息和物理方面的能源处理系统。能源系统的物理组件具有信息资源，当软件被嵌入到能源系统的子系统或物理组件中时，整个系统的资源可被网络攻击者利用，通过对子系统或者局部组件的攻击从而支配整个系统资源。智能电网

使用电脑网络控制电网发电、电能负载和配电资产，网络攻击者可能通过电脑硬件或者软件漏洞破坏发电的正常运行，从而危害负载以及相关配电资产。在交通系统中，交通系统是一个巨大的、开放的、相互依存的网络，承载着巨量的货运和亿万的乘客。交通系统组网包括信息和通信技术及其所需的基础设施、车辆和驾驶员、多种运输方式的接口等，一旦被专业的网络攻击者所利用，会损坏交通运输系统的基础设施安全以及数据安全。总而言之，工业控制系统信息安全迫在眉睫，这也是编写本书的直接背景。

本书从信息安全的角度出发，面向未来智能工业环境，讨论工业控制系统与相关应用的基本信息安全问题。本书以研究从基础知识到工业环境应用为立足点。本书的编写思想是：在美国 NIST 发布的 SP800-82《Guide to Industrial Control Systems Security》指导文件的基础上，梳理工业控制系统信息安全的主要问题，为工业控制安全分析奠定基础。同时，随着信息物理系统、物联网、嵌入式系统、射频识别、电力线通信、无线传感器、虚拟化和云计算平台等技术在工业控制系统中的应用越来越普及，本书加入了关于这些技术在工业环境应用中安全性的讨论。

本书的主要组织及结构如下：

第 1 章介绍工业控制系统组网所用的主要通信协议与总线的基本知识，特别是针对工业控制系统的专有协议与总线。

第 2 章介绍工业控制系统的主要子系统及组件，如 SCADA 系统、DCS 系统和 PLC 等。

第 3 章建立在第 1 章和第 2 章的基础之上，介绍工业控制系统的基本架构及行业特点。

前三章构成本书的第一部分——工业控制系统基础介绍。

第 4 章介绍工业控制系统的特性、威胁和脆弱性，为第 5 章风险评估奠定基础。

第 5 章介绍工业控制系统信息安全的核心内容——风险评估，介绍风险评估的基本思想与方法，通过一个简单的实例，评价工业控制系统信息安全的风险。

第 4 章和第 5 章构成了工业控制系统信息安全分析的核心内容——信息的风险评估，为后续信息安全控制措施提供理论基础。

第 6 章介绍信息安全的最直接最有效的安全措施——隔离技术。隔离技术是工业控制系统信息安全最常用的防护手段，也是我国当前

工业控制系统安全防护最广泛使用的措施。本章最后介绍当前工业信息安全防护的纵深防御思想。纵深防御是当前工业控制系统安全防御的核心思想。

第7章至第10章分别从认证与权限、审计与数据安全、管理与运维和漏扫与靶场四个方面介绍工业控制系统信息安全防护的重要措施，从相应技术的基本原理到应用实现来介绍四个方面的具体思想与实现方式。

第11章从四个工业环境出发，介绍四个工业环境的信息安全实例，这四个行业分别为能源行业、电力行业、智能制造行业和交通行业。

特别感谢陕西思科瑞迪公司在本书编写过程中所提供的大力支持，同时还要特别感谢参与本书编写的王如月、梅欣、张愚等同仁。

由于作者水平有限，书中不足在所难免，敬请读者、专家批评指正。

作　者

2019年1月

目 录

第 1 章　工业控制系统通信及专有协议

1.1　数据通信

数据通信系统是指以计算机为中心，通过数据传输信道将分布在各处的数据终端设备连接起来，以实现数据通信为目的的系统。

数据通信系统由数据信息的发送设备、接收设备、传输介质、传输报文、通信协议等组成。香农定义的广义通信系统模型如图 1-1 所示。

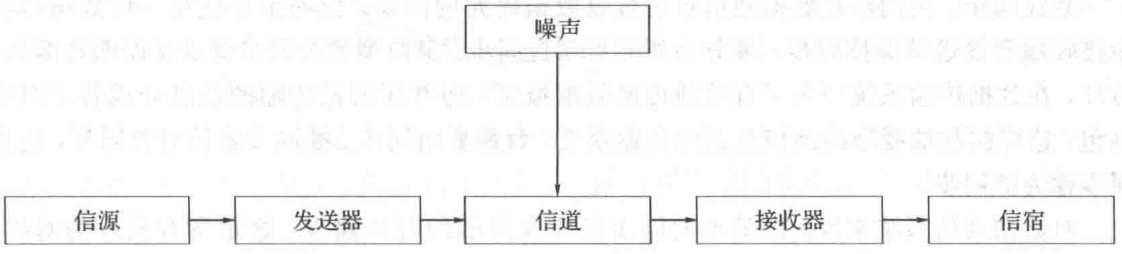

图 1-1　广义通信系统模型

图 1-1 中，信源是指传输数据信息的产生者；发送器将信息变换为适合于信道上传输的信号；信道是指发送器与接收器之间用于传输信号的物理介质(传输介质)。信号经过传输在接收器处变为信息。信宿是信息的接收者。通信传输过程会受到噪声的干扰，它往往会影响接收者正确地接收和理解所收到的信息。协议是数据通信规则的集合，目的是把接收到的信息还原为原有信息并为接收者所理解。如果没有协议，两台设备即使连接也无法通信。

发送设备、接收设备和传输介质是通信系统的硬件。发送设备将信源产生的数据经过编码变换为信号形式，送往传输介质；接收设备从带有干扰的信号中正确恢复出原有信号，并进行解码、解密等操作。

传输信道可以是简单的两条导线，也可以是由传输介质、数据中继、交换、存储、管理设备构成的网络。传输信道是为收发两地的数据流提供传输的信道，由传输介质和其他数据处理设备两部分组成。传输介质分为有线介质和无线介质两种，有线介质有双绞线、同轴电缆和光纤等，无线介质为空气，传输手段为微波、红外线、激光等。由光纤、同轴电缆、双绞线等有线介质构成有线通信，而由微波接力或卫星中继等方式通过大气层传输则构成无线通信。有线通信具有性能稳定、受外界干扰少、维护方便、保密性强等优点，但敷设工程量大，一次性投资也大。而无线通信利用无线电磁波在空气中传输信号，无需敷设有形介质，一次性投资相对较少，通信建立较灵活，但受空气环境影响较大，保密性较差。

1.1.1 数据传输的基本概念

1. 数据传输模式

1）传输模式

数据传输模式是指数据在信道上传输所采取的方式。数据传输模式有不同的分类方式：按照数据代码传输的顺序，可以分为并行传输和串行传输；按照数据传输的同步方式，可以分为同步传输和异步传输；按照数据传输的流向和时间关系，可以分为单工、半双工和全双工数据传输；按照数据信号的特点，可以分为基带传输、频带传输和数字数据传输。

2）同步技术

在数据通信系统中，通信系统的接收设备与发送设备的数据序列在时间上必须取得同步，以准确地接收发来的每位数据。这就要求接收设备按照发送设备所发送的每个位的重复频率及起止时间来接收数据，而且接收时还要不断校准时间和频率，这一过程称为同步。在数据通信系统中主要有载波同步、位(码元)同步和群(码组、帧)同步。

载波同步、位同步是数据通信系统接收数据码元的需要。位同步是使每一位数据传输中接收端和发送端保持同步，可分为外同步和自同步。最典型的自同步就是曼彻斯特编码。另外，在数据传输系统中为了有效地传递数据报文，通常还要把传输的信息分成若干组或打包，这样接收端要准确地恢复这些数据报文，就需要组同步、帧同步或信息包同步，这类同步称为群同步。

对数据通信系统来说，最基本的同步是收发两端的时钟同步，这是所有同步的基础。为了保证数据准确地传递，要求系统定时信号满足以下两点：

(1) 接收端的定时信号频率与发送端的定时信号频率相同。

(2) 定时信号与数据信号间保持固定的相位关系。

3）基带传输、频带传输和数字数据传输

基带传输是指原始信号不经调制，直接在信道上传输，即直接将计算机(或中断)输出的二进制“1”或“0”的电压(或电流)基带信号送到电路中进行传输。

频带传输是指把二进制“1”或“0”代表的信号，通过调制解调器变换成具有一定频带范围的模拟信号后进行传输，到达接收端后再把接收信号解调成原来的数字信号。

数字数据传输是利用数字话路传输数据信号的一种方式，这种方式效率高，传输质量较好。数字数据传输方式通常需要单独构成一个数字数据传输网(DDN)，因而初始投资较高，而采用模拟信道传输时完全可以利用已有的模拟电话网，只需在所用信道的两端各增设一个调制解调器作为数字传输用的数据电路终接设备(DCE)即可。同时，在DDN内部要求全网的时钟系统保持同步，否则在实现电路的转接和分支时就会有一定困难，在这一点上不如采用模拟信道传输灵活。

4）通信线路工作方式

单工通信是指通信只在一个方向上进行，在发送端和接收端之间有明确的方向性。如计算机向显示器传输数据采用的就是单工方式。

半双工通信是指通信可以在两个方向上进行，但不能同时进行传输，必须轮流进行。

全双工通信是指通信可以在两个方向上同时进行，当设备在一条线路上发送数据时，它也可以接收到其他数据。进行全双工通信时收发两端都需要安装调制解调器。

2. 数字数据传输

二进制数据可采用并行模式传输和串行模式传输两种方式进行传输。在并行模式下，每一个时钟脉冲有多位数据被传送；而在串行模式下，每一个时钟脉冲只发送一位数据。另外，发送并行数据只有一种方式，而对于串行传输则有两种方式——同步传输和异步传输。

1）并行传输

并行传输(Parallel Transmission)是将由“1”和“0”组成的二进制数每 n 位组成一组，在发送时 n 位同时发送，即数据以成组的方式在两条以上并行信道上同时传输。在传输过程中，使用 n 根线路同时发送 n 位，每一位都有自己独立的线路，并且一组中的所有 n 位都能够在同一个时钟脉冲从一个设备传送到另一个设备上。

2）串行传输

串行传输(Serial Transmission)是使数据流以串行方式在一条信道上一位接一位地传输。通常情况下，采用串行传输的线路，在设备内部都采用并行通信方式，这就需要在发送端和通信线路之间以及通信线路和接收端之间进行转换。

在进行串行传输时，接收端正确地划分串行数据码流中的传输数据，并采取一定措施发送一个个字符的传输方式，称为字符同步。根据实现字符同步的方式不同，串行数据传输可分为异步传输和同步传输。

3. 同步传输与异步传输

同步传输是以一定时钟节拍来发送数据信号的。这个时钟可以是参与通信的那些设备或器件中的一台产生的，也可以是外部时钟信号源提供的。时钟可以有固定的频率，也可以间隔不固定的周期进行转换。所有传输的数据位都和这个时钟信号同步。在进行同步传输时，不是独立地发送每个字符，而是连续地发送位流，并且不需要每个字符都有自己的开始位和停止位，而是把它们组合起来一起发送，这些组合称为数据帧，简称为帧。

在异步传输中，每个节点都有自己的时钟信号，每个通信节点必须在时钟频率上保持一致，并且所有的时钟必须在一定误差范围内相吻合。异步传输并不要求在传送信号的每一数据位时收发两端都同步。

4. 差错控制

在数据通信过程中，由于各种干扰及传输线路本身的因素，在传输过程中会不可避免地发生错误，特别是随着无线通信应用的增多，无线通信的差错率要远高于有线通信。为了提高通信系统的传输质量而采取的检测与校正方法就是差错控制。

差错控制的工作方式有两类：一类是接收端检测到接收的数据有差错时，接收端自动纠正差错；另一类是接收端检测出错误后不是自动纠错，而是反馈给发送端一个表示错误的应答信号，要求重发，直到正确接收为止。目前常用的差错控制方式有以下三种。

1）反馈纠错

反馈纠错是指发送端发送的码字具有检错能力，接收端根据协议对所接收的码字检测

是否有错误，然后通过反馈信道将判决结果反馈给发送端，要求发送端重传出错信息，直到正确为止。

2）前向纠错

前向纠错指发送端将信息码元按照一定规则加上监督信息，构成纠错码（纠错码的纠错能力有限），当接收的码字中有差错且在该码字的纠错能力之内时，接收端会自动纠错，但当错误超过码字的纠错能力时将无法纠错。

3）混合纠错

混合纠错是反馈纠错和前向纠错两种方式的结合。当接收端收到码字后首先判断有无差错，如果差错在编码的纠错能力之内，则自动纠错；如果超过编码的纠错能力，则通过反馈信道命令发送端重发以纠正错误，直到正确为止。

差错检测就是监视收到的数据并判别是否发生了传输错误，它仅仅识别出现错误现象而不识别错误发生在哪位或哪几位。差错检测常用的方法有以下两种：

（1）奇偶校验码。奇偶校验码是指通过增加冗余位来使得码字某些位中“1”的个数保持为偶数或奇数的编码方式。

（2）循环码（Cyclical Redundancy Check，CRC）。CRC 码是一种检错率高、编码效率高的检错码。CRC 码的原理是：任何一个由二进制数位串成的代码都可以与一个只有“1”和“0”为系数的多项式建立一一对应关系。

CRC 校验码的检错能力很强，除了能检查出离散错外，还能检查出突发错。其检错能力如下：

- 能检查出全部单个错。
- 能检查出全部离散的二位错。
- 能检查出全部奇数个数。
- 能检查出全部长度小于或等于 k 位的突发错。
- 能以 $1-(1/2)^{k-1}$ 的概率检查出长度为 $k+1$ 位的突发错。

1.1.2 串行通信

几乎所有的仪表、控制设备都配置有串行接口。串行通信接口中有两个重要的概念，即数据终端设备（Data Terminal Equipment，DTE）和数据电路终接设备（Data Circuit-terminating Equipment，DCE）。在通信线路的两端都要有 DTE 和 DCE。DTE 用于产生数据并且将数据传输到 DCE，而 DCE 将此信号转换成适当的形式在传输线路上进行传输。在物理层，DTE 可以是终端、微机、打印机、传真机等其他设备，但是一定要有一个转接设备才可以通信。DCE 是指可以通过网络传输或接收模拟数据或数字数据的任意一个设备，最常用的设备就是调制解调器。

1. 串行通信的主要参数

串行通信中，交换数据的双方利用传输在线路上的电压变化来达到数据交换的目的，但是如何从不断改变的电压状态中解析出其中的信息，就需要双方共同决定如何发送数据和命令。因此，为了进行通信，双方必须遵守一定的通信规则，这个通信的规则就体现在对通信端口参数的初始化上。利用通信端口的初始化可实现对以下四项的设置。

1）数据的传输速度

要使双方的数据读取正常，就要考虑到传输速率——波特率(Baud Rate)，它代表的意义是每秒所能产生的最大电压状态改变率。由于原始信号经过不同的波特率取样后，所得到的结果完全不一样，因此通信双方采用相同的通信速度非常重要。

2）数据的发送单位

一般串行通信端口所发送的数据是字符型的，这时一般采用 ASCII 码或 JIS(日本工业标准)码。若用来传输文件，则会使用二进制的数据类型。

3）起始位及停止位

由于异步串行传输中没有使用同步时钟脉冲作为基准，因此接收端完全不知道发送端何时将进行数据的发送。为了解决这个问题，就在发送端要开始发送数据时，将传输在线路上的电压由低电位提升至高电位(逻辑 0)，而当发送结束后，再将高电位降至低电位(逻辑 1)。接收端会因为起始位的触发而开始接收数据，并因停止位的通知而确知数据的字符信号已经结束。起始位固定为 1 位，而停止位则有 1、1.5 及 2 位等多种选择。

4）校验位的检查

校验位是用来检查所发送数据正确性的一种校验码，分为奇校验(Odd Parity)和偶校验(Even Parity)，分别检查字符中“1”的数目是奇数个还是偶数个。

2. 串行通信的流量控制

在串行通信中，当数据要由 A 设备发送到 B 设备前，数据会先被送到 A 设备的数据输出缓冲区，接着再由此缓冲区将数据由线路发送到 B 设备；同样，当数据利用硬件线路发送到 B 设备时，数据会先被发送到 B 设备的接收缓冲区，而 B 设备的处理器再到接收缓冲区将数据读取并进行处理。

流量控制就是为了保证传输双方都能正确地发送和接收数据而不会漏失。如果发送的速度大于接收的速度，而接收端的处理器来不及处理，则接收缓冲区在一定时间后会溢出，造成以后发送来的数据无法进入缓冲区而漏失。解决这个问题的方法是让接收端通知发送端何时发送以及何时停止发送。流量控制又称握手(Hand Shaking)，常用的方式有硬件握手和软件握手。

下面简要介绍工业通信领域主要的串行通信的标准，包括 RS－232C、RS－422 和 RS－485。

1）RS－232C 串行通信

RS(Recommended Standard)代表推荐标准，232 是标识号，C 代表 RS－232 的最新一次修改。RS－232C 是用于数字终端设备 DTE 与数字电路终端设备 DCE 之间的接口标准。该标准所定义的内容属于国际标准化组织 ISO 所指定的开放式系统互连参考模型中的最底层——物理层所定义的内容。

RS－232C 被定义为一种在低速率串行通信中增加通信距离的单端标准。RS－232C 采取不平衡传输方式，即所谓的单端通信。收、发端的数据信号是相对于信号的，如从 DTE 设备发出的数据在使用 DB25 连接器时 2 脚相对 7 脚(信号地)的电平。典型的 RS－232C 信号在正负电平之间摆动，在发送数据时，发送端驱动器输出正电平为＋5～＋15 V，负电平