新技术专家大讲堂系列丛书

工业控制系统信息安全的10堂课

让技术人员学习相关知识；
让企业找到解决方案；
让学生了解行业热点；
让大众紧跟技术发展。

肖建荣 编著

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

新技术专家大讲堂系列丛书

工业控制系统信息安全的10堂课

肖建荣 编著

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

内 容 简 介

本书以10堂课的形式全面、系统地对工业控制系统信息安全进行介绍。其中，第一堂课介绍工业控制系统信息安全概况，主要包括典型工业控制信息安全事件回顾、威胁分析、概念解析、基本需求、发展趋势等；第二堂课阐述工业控制系统信息安全标准体系；第三堂课介绍工业控制系统架构与漏洞分析；第四至八堂课是工业控制系统信息安全的技术部分，主要介绍工业控制系统信息安全技术、方案部署、风险评估、生命周期、管理体系等；第九堂课介绍工业控制系统信息安全产品认证；第十堂课分析未来趋势。全书内容以科普工业控制系统信息安全基础知识、基本原理为主，兼顾一门新兴专业课程和技术体系的严谨性和完整性。

本书可供工作中涉及工业控制系统信息安全领域的研发与技术人员参考，也可供欲了解工业控制系统信息安全的企业管理层与相关专业高校师生阅读。

图书在版编目（CIP）数据

工业控制系统信息安全的10堂课 / 肖建荣编著. —北京：电子工业出版社，2018.12
（新技术专家大讲堂系列丛书）
ISBN 978-7-121-35589-9

Ⅰ. ①工… Ⅱ. ①肖… Ⅲ. ①工业控制系统－信息安全－普及读物 Ⅳ. ①TP273-49

中国版本图书馆CIP数据核字（2018）第265067号

策划编辑：陈韦凯
责任编辑：康 霞
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
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：18.5　字数：362.6千字
版　　次：2018年12月第1版
印　　次：2018年12月第1次印刷
定　　价：58.00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）88254441；bjcwk@163.com。

前　言

工业控制系统信息安全（简称工控安全）作为国家网络安全的重要组成部分，已经上升为国家级信息安全战略，各国政府都在携手推进和积极应对，相关国际标准、国家标准、国家战略、指导方针、行动计划、行业准则等都已发布或正在制订过程中。与工业控制系统信息安全相关的用户、产品供应商、系统集成商、信息安全服务商、政府相关监管部门等，都在稳步推进新兴的工业控制系统信息安全专业建设。如何深入推进这门新兴专业学科的建设，是一个国际社会、国家区域、行业领域共同关注的课题。

● 工业控制系统信息安全的发起与发展

对于大多数人而言，工业控制系统信息安全的概念来自“震网”“黑暗力量”这些典型的工业控制信息安全事件。要想弄懂工业控制系统信息安全的概念，需要从这些典型工业控制信息安全事件开始分析、学习和探讨。

工业控制系统信息安全刚刚走过十几年，还处在发展过程中。如何建立一套全面的知识和实践应用体系，是我们面对的当务之急，这正是本书编写的出发点。虽然对其中的内容有些争议，但是我们希望在各方的共同参与下，在争议和发展中积极推进工业控制系统信息安全工作，做到在争论中不断发展、在实践中不断推进。因此，本书将给广大的工业控制系统用户一个全面和正确的指导，给广大从事工业控制系统设计、施工、调试和服务的用户一个强有力的支撑，同时可以给工业控制系统供应商提供参考，对政府一些职能部门的工作也有一定的参考性。

● 工业控制系统信息安全 10 堂课概要

本书以 10 堂课的形式全面、系统地对工业控制系统信息安全进行介绍。其中，第一堂课介绍工业控制系统信息安全概况，主要包括典型工业控制信息安全事件回顾、威胁分析、概念解析、基本需求、发展趋势等；第二堂课阐述工业控制系统信息安全标准体系；第三堂课介绍工业控制系统架构与漏洞分析；第四至八堂课是工业控制系统信息安全的技术部分，主要介绍工业控制系统信

息安全技术、方案部署、风险评估、生命周期、管理体系等；第九堂课介绍工业控制系统信息安全产品认证；第十堂课分析未来趋势。全书内容以科普工业控制系统信息安全基础知识、基本原理为主，兼顾一门新兴专业课程和技术体系的严谨性和完整性，同时，还单独阐述工业控制系统信息安全标准体系、工业控制系统架构与漏洞、工业控制系统信息安全产品认证和未来趋势等热点话题。通过介绍具有代表性和实用性的观点、硬件、软件、评估、管理、认证等内容，让读者能够在短时间内了解、认识、掌握和运用工业控制系统信息安全，并达到“让企业找到工业控制系统信息安全解决方案、让技术人员掌握工业控制系统信息安全知识、让学生了解工业控制系统信息安全专业课程、让普通大众跟进工业控制系统信息安全技术进步”的目的。

● 感谢与沟通

本书在写作过程中，获得了来自机构、专业供应商、专业人士、学友等的很多宝贵意见和建议，在此深表感谢；感谢电子工业出版社策划编辑陈韦凯在作者写作过程中给予的沟通和理解。

本书在编写过程中，除引用了作者多年的工作实践和研究内容之外，还大量参考了一些国内外优秀论文、书籍，以及互联网上公布的相关资料，尽量在书后的参考文献中列出，但由于互联网上资料数量众多、出处引用不明确，可能无法将所有文献一一注明出处，对这些资料的作者表示由衷的感谢，同时声明原文版权属于原作者。

本书是一本工业控制系统信息安全前沿技术专业书，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高年级本科生、研究生的参考书。

工业控制系统信息安全是一门应用性很强的跨专业学科，在工业化和信息化大规模发展的今天已取得了一定的发展，本书尝试对此领域的理论和技术做一些归纳，以期有益于广大专业同行和关心工业控制系统信息安全的人士。由于工业控制系统信息安全技术在快速发展，加之作者水平有限，书中难免有一些缺点和错误，真诚希望读者不吝赐教，以期再版时修订。

作　者

目　录

第一堂课 工业控制系统信息安全概况

一、典型工业控制信息安全事件回顾

二、威胁分析

三、概念解析

四、基本需求

五、发展趋势

一、典型工业控制信息安全事件回顾

工业控制系统信息安全作为国家网络安全的重要组成部分，已然上升为国家级信息安全战略，各国政府都在积极应对这种挑战，但是对于与工业控制系统信息安全相关的用户、产品供应商、系统集成商、信息安全服务商、政府相关监管部门等，似乎对此有不同阐述，很显然，这就告诉我们新兴的工业控制系统信息安全专业术语不是那么容易能被解释清楚的，更何况这是一门新兴的专业学科！

对于大多数人而言，工业控制系统信息安全的概念来自“震网”、“黑暗力量”这些典型的工业控制信息安全事件。要想弄懂工业控制系统信息安全的概念，则不妨从这些典型工业控制信息安全事件开始，一边分析，一边学习，一边探讨。

（一）“震网”事件

2006 年，时任伊朗总统艾哈迈迪·内贾德突访纳塔兹地区的一个地下核工厂，借此向世界宣告伊朗核计划已经启动，这迅速引起了多国的反对。时任美国总统布什说，伊朗拥有核武器是不能被接受的。时任以色列总理内塔尼亚胡说，伊朗的核计划一定要制止，必须得制止，我们必须现在就要制止它。即便如此，伊朗的核发展计划仍在推进，并且在 2007 年动工建设布什尔核电站。

2010 年 9 月，正当布什尔核电站准备正式运行之际，伊朗官方宣布，境内诸多工业企业遭遇了一种极为特殊的计算机病毒袭击，该病毒能秘密改变核工厂离心机的转速，导致千余台离心机永久性损坏。随后伊朗数次推迟布什尔核电站的供电时间，伊朗核发展计划被迫延迟。伊朗官方 26 号证实，一种名为“震网”的计算机蠕虫病毒大范围爆发。某些组织甚至国家正在利用计算机技术限制伊朗发展核力量。

攻击者先感染核电站建设人员使用的互联网计算机或 U 盘，经 U 盘交叉使用侵入物理隔离的内网，通过内网找到 WinCC 服务器，通过修改 PLC 来改变工业生产控制系统的行为，包括拦截发送给 PLC 的读/写请求，以此判断系统是否为潜在的攻击目标，修改现有的 PLC 代码块，并且向 PLC 中写入新的代码块，利用 Rootkit 功能隐藏 PLC 感染，躲避 PLC 管理员或程序员的检测，最后实施破坏性攻击。其攻击事件流程图如图 1-1 所示。

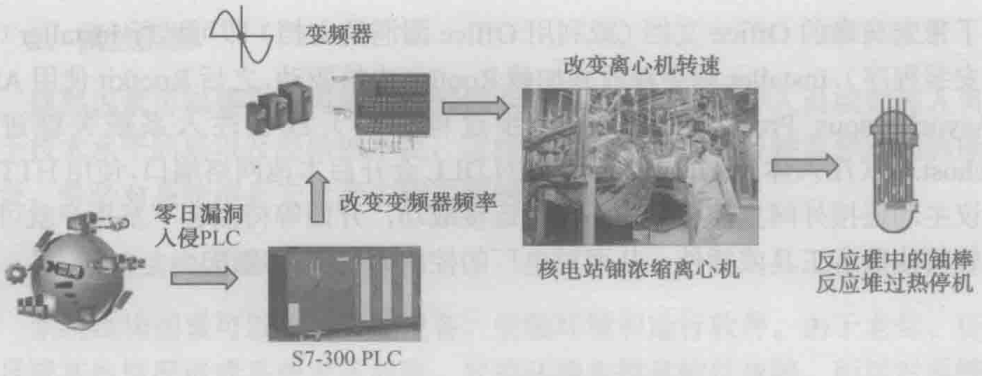

图 1-1　“震网”攻击事件流程图

（二）“黑暗力量”事件

2015 年 12 月 23 号下午，乌克兰西部伊万诺-弗兰科夫斯克地区的居民们结束一天的工作陆续回家，在当地的电力供应控制中心，运维人员也即将完成自己的本次轮班。然而，平静被打破了。一位当值人员在整理桌上文件时，突然发现计算机屏幕上的光标开始不受控制地四处游移，他目睹着光标完成断电操作，而自己却无能为力。一瞬间，数以百万计的居民陷入黑暗，恐慌如潮水一般淹没城市。很快，这被证实是一起针对电厂的网络攻击行为，黑客利用欺骗手段，让电力公司员工下载了一款名为“黑暗力量”（Black Energy）的恶意病毒软件，并最终获得了电厂系统的控制权。和历史上多次网络攻击事件一样，乌克兰电厂的幕后黑手迄今逍遥法外。

图 1-2 展示了 Black Energy 入侵目标主机的过程。黑客通过收集目标用户邮箱，然后向其定向发送携带恶意文件的 Spam 邮件，疏于安全防范的用户打

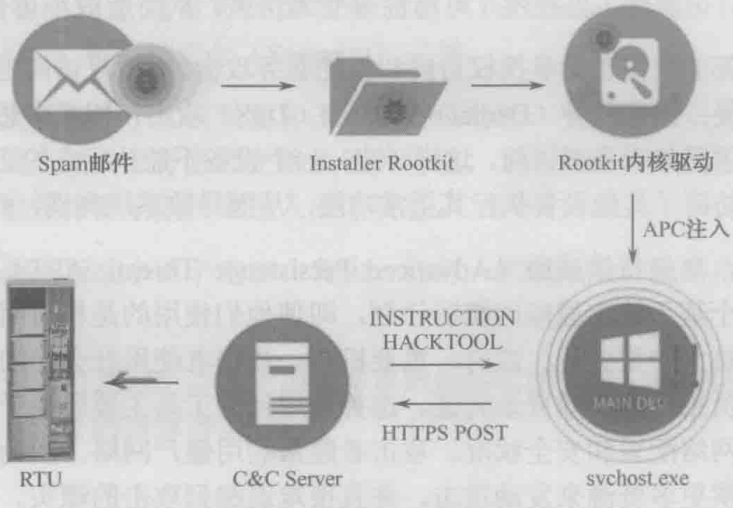

图 1-2　Black Energy 感染流程图

开了带宏病毒的 Office 文档（或利用 Office 漏洞的文档）即可运行 Installer（恶意安装程序），Installer 则会释放并加载 Rootkit 内核驱动，之后 Rootkit 使用 APC（Asynchronous Procedure Call，异步过程调用）线程注入系统关键进程 svchost.exe（注入体 MAIN.DLL），MAIN.DLL 会开启本地网络端口，使用 HTTPS 协议主动连接外网主控服务器，一旦连接成功，开始等待黑客下发指令就可以下载其他黑客工具或插件，从而对电厂的控制系统实施攻击。

二、威胁分析

工业控制系统信息安全的威胁主要来自敌对因素、偶然因素、系统结构因素和环境因素。

1．敌对因素

敌对因素可以是来自内部或外部的个体、专门的组织或政府，通常采用包括黑客攻击、数据操纵（Data Manipulation）、间谍（Espionage）、病毒、蠕虫、特洛伊木马和僵尸网络等进行攻击。

黑客攻击通过攻击自动化系统的要害或弱点，使得工业网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，从而造成不可估量的损失。

来自外部的攻击包括非授权访问和拒绝服务攻击。非授权访问是指一个非授权用户的入侵；拒绝服务（Denial of Service，DoS）攻击，即黑客想办法让目标设备停止提供服务或资源访问。这样一来，一个设备不能执行它的正常功能，或者它的动作妨碍了其他设备执行其正常功能，从而导致系统瘫痪，停止运行。

近年来，高级持续威胁（Advanced Persistence Threat，APT）不断出现。攻击者有一个基于特定战略的缜密计划，即使他们使用的是相对简单的机制。其攻击对象是大中型企业、政府、重要机构。攻击者使用社会上的工程技术和招募内部人员来获取有效登录凭证。选择使用何种工具主要取决于攻击目标是什么，以及网络配置和安全状况。攻击者经常利用僵尸网络，因为僵尸网络能够给他们提供更多资源来发动攻击，并且很难追踪到攻击的源头。

2. 偶然因素

偶然因素可以是来自内部或外部的专业人员、运行维护人员或管理人员。由于技术水平的局限及经验的不足，这些人员可能会出现各种意想不到的操作失误，势必对系统信息安全产生较大影响。

3. 系统结构因素

系统结构因素可以来自系统设备、安装环境和运行软件。由于老化、资源不足或其他情况造成系统设备故障、安装环境失控及软件故障，所以对系统信息安全产生较大影响。

4. 环境因素

环境因素可以来自自然或人为灾害、非正常的自然事件（如太阳黑子等）和基础设施破坏。这些自然灾害、人为灾害、非正常的自然事件和基础设施破坏，对工业控制系统信息安全产生较大影响。

三、概念解析

工业领域的安全通常可分为功能安全（Functional Safety）、物理安全（Physical Safety）和信息安全（Security）三类。

功能安全是指为了实现设备和工厂的安全功能，受保护的安全相关部分和控制设备的安全相关部分必须正确执行其功能。当失效或故障发生时，设备或系统必须仍能保持安全条件或进入安全状态。

物理安全是指减小由于电击、着火、辐射、机械危险、化学危险等因素造成的危害。

信息安全的范围较广，大到国家军事政治等机密安全，小到防范企业机密的泄露、个人信息的泄露等。

1. ISO 对工业控制系统信息安全的定义

在 ISO/IEC 27002 中，信息安全的定义是“保持信息的保密性、完整性、可用性，另外也可包括真实性、可核查性、不可否认性和可靠性等。”

2. IEC 对工业控制系统信息安全的定义

工业控制系统信息安全是工业领域信息安全的一个分支，是最近发展起来的一个热点名词。事实上，工业控制系统信息安全早就存在，只是当时人们并没有意识到。

工业控制系统信息安全与通用信息技术（IT）安全有一定区别，也有一定共性，有时也存在一定交集，取决于工业控制系统的架构。

在 IEC 62443 中对工业控制系统信息安全的定义：①保护系统所采取的措施；②由建立和维护保护系统的措施所得到的系统状态；③能够免于对系统资源的非授权访问和非授权或意外的变更、破坏、损失；④基于计算机系统的能力，能够保证非授权人员和系统既无法修改软件及其数据又无法访问系统功能，而能够保证授权人员和系统不被阻止；⑤防止对工业控制系统的非法或有害入侵，或者干扰其正确和计划的操作。

四、基本需求

1. 3 个基本需求

工业控制系统信息安全是针对工业控制系统的信息保护而言的，其信息安全的 3 个基本需求如下。

1）可用性

工业控制系统信息安全必须确保所有控制系统部件可用、运行正常及功能正常。

工业控制系统的过程是连续的，不能接受意外中断。如果需要人为中断，必须提前计划和安排。具体实施前的测试是必须的，以确保工业控制系统的高

可用性。除了意外中断，为了保证生产连续，许多控制系统不允许随便启动和停止。在某些情况下，生产的产品或使用的设备比信息的中断更重要。因此，采用典型的IT策略，如重新启动一个组件，通常在工业控制系统中是不能被接受的，会对系统的可用性、可靠性和可维护性要求产生不利影响。有些工业控制系统采用冗余组件并行运行，在主组件出问题时可以切换到备份组件，保证连续性。

2）完整性

工业控制系统信息安全必须确保所有控制系统信息的完整性和一致性。工业控制系统信息的完整性和一致性分为如下两方面：

（1）数据完整性，即系统未被未授权篡改或损坏。

（2）系统完整性，即系统未被非法操纵，按既定的目标运行。

3）保密性

工业控制系统信息安全必须确保所有控制系统部件可用，运行正常及功能正常。

工业控制系统信息安全必须确保所有控制系统信息安全，配置必要的授权访问，防止工业信息盗取事件的发生。

除上面介绍的3个基本需求外，工业控制系统信息安全还有其他方面的需求，这些需求将在第三堂课中介绍。

2. 工业控制系统信息安全与信息技术系统安全的比较

与工业控制系统信息安全相比，信息技术系统安全也有上面提到的3个需求。两者对这些需求的优先级是有区别的，其区别如图1-3所示。

图1-3　工业控制系统信息安全与信息技术系统安全的比较图