

工业控制系统关键组件安全风险综述

唐士杰^{1,2}, 袁方³, 李俊⁴, 丁勇^{5,6}, 王会勇⁷

- (1. 桂林电子科技大学计算机与信息安全学院, 广西 桂林 541004; 2. 桂林电子科技大学电子工程与自动化学院, 广西 桂林 541004;
3. 外交部通信总台, 北京 100016; 4. 国家工业信息安全发展研究中心, 北京 100040;
5. 桂林电子科技大学广西密码学与信息安全重点实验室, 广西 桂林 541004; 6. 鹏城实验室新型网络研究部, 广东 深圳 518055;
7. 桂林电子科技大学数学与计算科学学院, 广西 桂林 541004)

摘要: 随着现代信息技术与通信技术的快速发展, 工业控制(简称“工控”)系统已经成为国家关键基础设施的重要组成部分, 其安全性关系到国家的战略安全和社会稳定。现代工控系统与互联网越来越紧密的联系, 一方面促进了工控技术的快速进步, 另一方面为其带来了巨大安全问题。自“震网”病毒事件之后, 针对工控系统的攻击事件频发, 给全球生产企业造成了巨大经济损失, 甚至对很多国家和地区的社会稳定与安全造成重大影响, 引起人们对工控系统安全的极大关注。现代工控系统中自动化设备品类和专有协议种类繁多、数据流复杂且发展迅速等, 导致对工控关键组件安全的综述难度很大, 现有与此相关的综述性文献较少, 且大多较为陈旧、论述不全面。针对上述问题, 介绍了当前工控系统的主流体系结构和相关组件。阐述并分析了关键工控组件中存在的安全漏洞及潜在的威胁, 并重点针对数据采集与监视控制(SCADA)中的控制中心、可编程逻辑控制器、现场设备的攻击方法进行归纳、总结, 对近几年文献中实施攻击的前提条件、攻击的对象、攻击的实施步骤及其危害性进行了归纳与分析, 并从可用性、完整性和机密性的角度对针对工控网络的攻击进行了分类。给出了针对工控系统攻击的可能发展趋势。

关键词: 工控系统; 数据采集与监视控制; 可编程逻辑控制器; 攻击趋势

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022030

Review on security risks of key components in industrial control system

TANG Shijie^{1,2}, YUAN Fang³, LI Jun⁴, DING Yong^{5,6}, WANG Huiyong⁷

1. School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
2. School of Electronic Engineering and Automation, Guilin University of Electronic Technology, Guilin 541004, China
3. Communications Office of the Ministry of Foreign Affairs, Beijing 100016, China
4. National Industrial Information Security Development Research Center, Beijing 100040, China
5. Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China

收稿日期: 2021-10-18; **修回日期:** 2022-03-16

通信作者: 丁勇, stone_dingy@126.com

基金项目: 国家自然科学基金(61772150, 61862012, 61962012); 鹏城实验室重大任务项目(PCL2021A09)

Foundation Items: The National Natural Science Foundation of China (61772150, 61862012, 61962012), Pengcheng Laboratory's Major Task Project (PCL2021A09)

引用格式: 唐士杰, 袁方, 李俊, 等. 工业控制系统关键组件安全风险综述[J]. 网络与信息安全学报, 2022, 8(3): 1-17.

Citation Format: TANG S J, YUAN F, LI J, et al. Review on security risks of key components in industrial control system[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 1-17.

6. New Network Research Department of Pengcheng Laboratory, Shenzhen 518055, China

7. School of Mathematics & Computing Science, Guilin University of Electronic Technology, Guilin 541004, China

Abstract: With the rapid development of modern information technology and communication technology, industrial control system has become an important part of national key infrastructure, whose security is related to national strategic security and social stability. The close connection between modern industrial control system and Internet promotes the rapid progress of industrial control technology, meanwhile it brings serious security risks. Since the “Stuxnet” virus incident, attacks on industrial control systems have occurred frequently, which causes huge economic losses to global production enterprises. Besides, it also poses significant impact on the social stability and security to many countries and regions, which has aroused people’s great concern about the security of industrial control systems. Due to the wide variety of automation equipment and proprietary protocols, complex data flow and rapid development in modern industrial control system, it is very difficult to summarize the safety of key components of industrial control. There are few literatures related to this area, and most of them are old and incomplete. To solve the above problems, the mainstream architecture and related components of the current industrial control system were introduced. Then the security vulnerabilities and potential threats in the key industrial control components were analyzed. The attack methods of SCADA control center, programmable logic controller and field equipment were summarized. Furthermore, the preconditions, objects, steps and hazards of the attack in the literature in recent years were also analyzed. The attacks against industrial control network were classified from the perspective of integrity and confidentiality. Finally, the possible development trend of industrial control system attack was given.

Keywords: industrial control system, supervisory control and data acquisition, programmable logic controller, attack trend

0 引言

随着工业 4.0 的全面推进,越来越多的信息技术和通信技术被集成到现代工业控制(简称“工控”)系统(ICS, industrial control system)中。工控系统从单机走向互联,从封闭走向开放,从自动化走向智能化,为网络安全威胁向其加速渗透提供了条件^[1]。《2019—2021 年中国工控市场预测与展望数据》^[2]表明,发现 2019—2021 年,中国工控市场保持年均 12%以上的快速增长。到 2021 年,市场规模达到 2 600 亿元。在工控市场激增的同时,我国工控设备暴露数量明显上升。另外,工控系统需求的提升促进了数据采集与监视控制(SCADA, supervisory control and data acquisition)系统、控制器、高精度传感器等组件功能结构的更新变革。物联网、云计算和 5G 等新技术在工控系统中得到快速发展与应用,引入了新的安全风险,也意味工控安全将迎接更为严峻的挑战。

在文献[3]中,Babu 等概述了工控系统的新趋势:在工控的主要领域,从传统的机电系统逐步

转换到基于网络的数字系统,数字集成系统因其具有实时、可靠等特点,在工业和制造业中发挥着关键作用。Ayodeji 等^[4]也提到:“数字产品引入工控系统,以取代老化和过时的模拟控制系统。数字系统的共享兼容性使 IT 设备被大量用于 ICS。然而,共享设备暴露了传统信息物理系统控制中常见的不透明性。”

ICS 已从集中控制结构转变为当前的分布式控制结构,许多计算和信息传输功能已逐渐分散,从中央节点扩展到边缘节点。ICS 中的每个节点(如传感器、控制器或执行器)都可以配备物联网模块,从而具有计算和信息传输的能力^[5]。分布式控制一般采用冗余控制器体系结构,这是保证系统稳定性的一种实用方法,但这种体系结构扩大了系统攻击面,降低了对正在进行的网络攻击做出响应的敏感性^[6]。

工业 4.0 是以智能制造为主导的第四代工业革命,它将信息物理系统、物联网、云计算、工业集成、企业体系结构、面向服务的体系结构(SOA, service-oriented architecture)、业务流程管理、工业信息集成等技术结合应用,推动了制造

业向智能化转型^[7]。物联网云服务也正融入关键基础设施^[8], 新技术带来新的安全理念的同时, 带来了新的安全问题。例如, 云计算为 ICS 提供服务, 包括数据传输、存储、数据处理及分析, 这引起了人们对云环境数据安全性是否可信的担忧。物联网系统中设备、通信协议的异构性, 以及系统中节点的规模和数量, 使物联网系统的安全性比传统网络更具挑战性。

近年来, 很多学者从不同角度对工控系统的安全问题进行了归纳、总结。Asgar 等^[9]简要说明了 ICS 中存在漏洞和威胁, 重点论述了现有解决方案, 并对其分类。Upadhyay 等^[10]以标准漏洞数据库中报告的真实事件为例, 描述了各种类型的潜在 SCADA 漏洞。Nazir 等^[11]对模拟 SCADA 攻击进行了分类说明, 但其大部分参考文献是 2015 年以前的。Yadav 等^[12]对 2016 年前影响较大的 SCADA 真实攻击事件进行了分析, 将攻击分为 5 类, 即恶意软件、非网络攻击、未经授权的远程访问、服务中断和未知。Alladi 等^[13]分析了近 20 年 ICS 的重大攻击案例, 描述了案例中的攻击目标、攻击描述、结果及解决方案。冯涛等^[14]对工业以太网协议的脆弱性进行了分析, 并对主要防护技术进行论述。Sajid 等^[8]对基于云辅助互联网的工业 SCADA 系统的安全挑战进行了阐述, 并提出了 10 项建议来保护 SCADA 系统。

上述文献主要阐述工控网络安全的漏洞、脆弱性以及防御方法, 缺乏对 ICS 关键组件的攻击方法的总结归纳。针对上述问题, 本文分析了工控系统中存在的威胁, 对关键工控组件攻击方法进行了分析和分类。

1 工控系统

工控系统基本架构可分为 3 个层次, 如图 1 所示^[15]。

1) 公司网络层: 管理者可以远程访问监控计算机或人机界面(HMI, human machine interface)。

2) 逻辑控制层: 常见的系统有数据采集与监视控制系统和分布式控制系统(DCS, distributed control system)。该层用于监控生产状态, 并利用 HMI 实现人机交互, 其核心组件如下。

① SCADA 控制中心: 由主站单元、数据库服务器、应用程序服务器、工程师工作站、生产

调度工作站、诊断服务器等组件组成, 用于管理、协调和控制工控系统。

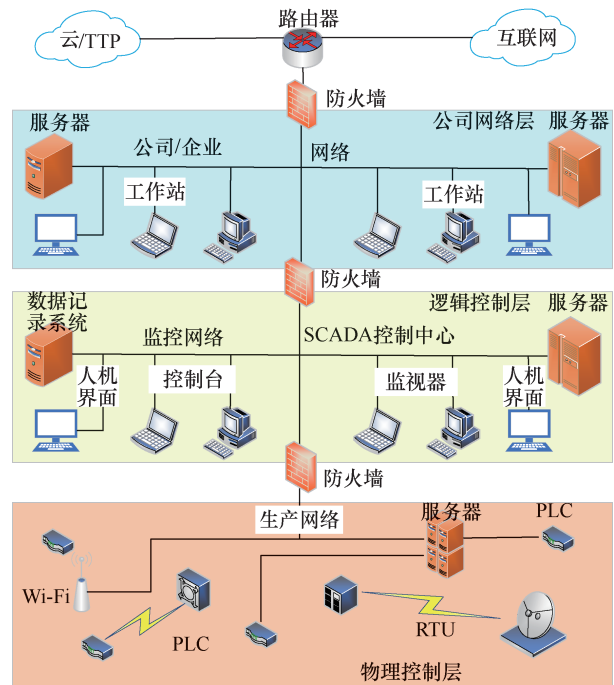


图1 工控系统基本架构
Figure 1 Basic architecture of industrial control system

② 人机界面: 一种图形用户界面系统, 能显示 ICS 环境中传感器收集的的设备状态和历史数据, 配置、变更控制算法和参数并将其部署到控制器, 监控整个 ICS。

3) 物理控制层: 由控制器和现场仪表组成。这层设备主要包括以下组件。

① 可编程逻辑控制器(PLC, programmable logic controller): 一种用于自动化控制的微控制器, 它能监视现场设备的状态, 可以根据工程师创建的控制逻辑, 实现对生产过程的自动控制。

② 远程终端单元(RTU, remote terminal unit): 能将远程传感器和执行器连接到中央系统, 但通常不支持控制回路。与 PLC 相比, RTU 不仅具有 PLC 的基本功能, 更适用于在远距离通信和恶劣温湿度环境下工作。

③ 仪表和执行器: 直接测量和执行控制命令的组件。

工控系统的通信至关重要。工业通信网络, 特别是监控网络, 大部分使用专有工控协议来交换信息和管理设备, 具有快速响应和较少网络故障的特性^[16-17]。常用的通信协议有 Modbus、

DNP3、Foundation Fieldbus、Profibus 等。

2 工控系统安全问题

工控系统是由工控组件构成的，几乎所有的组件可能遭受网络攻击。Gonzalez 等^[18]对由 277 个供应商开发的 988 个针对工控系统的漏洞咨询报告进行了深入分析。结果显示，人机界面、SCADA 软

件和 PLC 是受影响最大的组件。黄家辉等^[19]根据漏洞的危害性对各个因素进行了分级，如表 1 所示。表中的大、中、小分别代表如果组件被利用，对工控系统产生的影响大小（严重、一般、较小）。从表 1 可以看出，PLC、RTU 和服务器/数据库等组件在遭受到攻击时，对工控系统危害大。因此，本文详细讨论关键工控组件的安全问题。

表 1 漏洞危害性打分
Table 1 Score of vulnerability harmfulness

影响因素	等级细分	说明
SCADA 服务器	大	使整个控制系统和管理者的计算机能随时使用来自 SCADA 远程终端的重要信息
工程师站	中	既安装 STEP 7 编程组态软件，又安装 WinCC 监控操作组态软件
操作员站	小	仅需安装 WinCC 监控操作组态软件
用户机	小	存放传输给管理层的数据
Web 服务器	小	提供 Web 服务的功能，在某些工控系统中不是必需的
MES 服务器/数据库	大	存放制造执行层的重要数据
OPC 服务器/数据库	大	存放下位机采集的原始现场数据和上位机传来的指令
RTU	大	主要进行数据采集和本地控制，与传输可靠性、主机负担等相关
PLC	大	主要进行过程控制、信息控制和远程控制，是重要的下位机
PAC	小	作为开放型的自动化控制设备，其应用在工控系统中并不常见

2.1 工控设备存在的安全问题

2.1.1 SCADA 控制中心

控制中心的主机大多是通用的计算机，并使用通用操作系统，从而为 SCADA 中心带来了多种安全风险。首先，微软公司在 2014 年已经停止对 Windows XP 提供升级服务，但 Windows XP 的使用比例依然超过 40%；Windows 7 在 2020 年停止升级服务，但它的使用比例占据首位^[20]。即使采用了最新的操作系统，从可用性考虑，很多企业在使用过程中也较少使用补丁和安全更新，这意味着大多操作系统存在潜在漏洞风险。其次，控制中心的软件组件缺乏保护，很多主机未安装杀毒软件或安装了杀毒软件但使用过程中较少更新病毒库。杀毒软件升级更新可能与应用软件不兼容，导致出现应用软件“误杀”或冲突的情况。另外，随意使用不安全的移动设备，容易导致主机染上病毒，从而导致应用软件被病毒篡改或恶意卸载。

SCADA 软件产品也可能存在代码质量问题导致缺乏安全性。一些 SCADA 代码评审指出，

SCADA 系统的软件设计和实现通常不遵循安全的软件开发生命周期。专有应用程序中的不安全函数调用，尤其是 OPC 动态链接库（DLL）中的不安全函数调用，容易使 SCADA 系统受到攻击^[10]。SCADA 软件产品维护不善也会导致安全风险出现。补丁通常是在发现漏洞后发布的，新补丁与漏洞发布之间可能存在时间间隔。同时，很多工控用户不愿意打补丁，这归因于补丁修补程序失败率较高、有些补丁会由于未经适当测试引入新的未知漏洞或其他风险、打补丁的过程需要停机操作等。这使未打补丁的软件成为系统最大的漏洞之一。SCADA 软件趋于采用通用、标准的商用货架产品（COTS，commercial off-the-shelf）软件作为构成系统软件的基础，是使 SCADA 系统不安全的又一诱因^[21]。基于 COTS 的设计可能更便宜并可以减少设计时间，但会损害产品的整体安全性。而且，当出现新的漏洞时，通常很难在 SCADA 系统中修补此软件^[22]。

新一代的人机界面是基于 Windows 的操作系统，可配备触摸屏、ActiveX、数据库和远程访问

功能^[23]。HMI 用户可能使用默认密码和弱密码, 攻击者可以通过查阅用户指南、猜测、字典攻击或暴力攻击等方式破解; HMI 相关软件中可能存在漏洞, 包括为便于调试而故意留下的后门, 以及不良编程产生的无意漏洞^[24-25]; 通过 Web 浏览器连接可随时随地访问系统, 攻击者可以通过应用程序未经授权访问控制中心^[26], 从而带来 SQL 注入、目标遍历等其他与 Web 相关的风险。

2.1.2 控制器

控制器是基于微处理器的专用工控设备, 可以对其进行编程来自动监视和控制现场设备及过程。厂商在设计控制器时考虑的安全性, 更多是对受监视过程变化的实时响应以及在环境中工作的能力^[27], 很少会考虑抵御网络攻击的设计, 如身份验证机制、数据加密等。即使有些 PLC 有安全功能, 但它们通常会被忽略或禁用, 因为安全性通常与操作不一致^[28]。大多数 PLC 可以通过以太网连接到 ICS, 并间接连接到互联网。这大大增加了 PLC 被攻击的风险。在使用过程中, 控制器的 CPU 和内存资源限制、较长的生命周期以及严格的停机时间要求, 使得很难在现场修补现有设备, 也几乎不可能安装任何类型的端点保护^[29]。

控制器的固件存在安全风险。控制器基于专有操作系统设计, 有些修补程序仅仅适用于原始设备的生产商, 其安全升级一般由生产商修补^[10], 在远程更新时, 容易遭受攻击。有些供应商为方便用户自行更新, 在其网站上发布了固件更新的数据, 固件更新时, 有些控制器仅仅在客户端进行验证和加密, 攻击者可以采用软件逆向工程和协议逆向工程绕过它^[6], 加剧了安全隐患。

固件在更新操作时面临的威胁如下^[30-31]。

1) 逆向工程: 如果攻击者能够获取固件映像或相应的二进制文件, 可对固件的操作进行逆向工程, 以获取敏感信息。

2) 固件修改: 攻击者在固件中修改其内容, 以便执行未经授权的操作。

3) 获得访问授权: 某些设备在与外部设备通信时需要授权。如果攻击者可以获得该授权, 则能够对目标设备进行不同类型的攻击。

4) 安装未经授权的固件: 恶意方或具有恶意

目的的合法方会尝试将未经授权的固件安装到设备上。一旦在设备上安装了未经授权的映像, 攻击者便有可能进行其他攻击。

5) 未经授权的设备: 非法设备可能伪装成合法设备并取得真实固件的复件。

控制器的可编程区也是攻击者关注的目标之一。为获得对物理过程的控制权, 攻击者可能会伪造、篡改 PLC 的控制逻辑。此类攻击涉及的主要漏洞是 PLC 协议中缺少身份验证措施^[32-33]。控制器的控制逻辑在上载、下载操作时很少通过身份验证, 或者仅在上载、下载的一个方向上支持身份验证。攻击者可以通过对 PLC 的物理访问或通过网络来利用此漏洞, 并将恶意逻辑下载到 PLC 上。结构和设计不够完善的梯形图逻辑代码也会增加漏洞的风险。这方面的漏洞有: 使用重复的指令、使用硬编码值、缺乏详尽的诊断和警报消息、未使用的标签或操作数、程序模式等^[34]。

2.1.3 现场设备

现场设备通常是功能和资源有限的较低级别的组件。随着嵌入式技术的快速发展, 智能设备逐渐增多, 使现场设备也能进行本地存储和少量的数据处理。攻击者开始关注对低级设备的攻击, 这可能会对物理工业系统造成直接损害, 并且难以发现^[6]。对现场设备进行防护的最大困难之一是资源限制: 现场设备通常没有足够的内存和资源来执行安全功能, 存在物理直接暴露或远程非法访问的威胁; 此外, 现场设备可以运行数年而无须重新启动, 会造成碎片积累, 从而导致设备存在缓冲区溢出问题。还有一个问题是关键组件缺乏冗余, 如发电机或不间断电源 (UPS) 缺乏备用电源^[22]。

2.2 工控网络

传统的 ICS 网络与互联网是完全隔离的, 其底层专有通信协议在设计之初以功能为主要目的进行设计, 协议缺乏内置的安全性设计^[35], 如缺乏认证机制、过时的授权服务、没有权限区分、弱口令、不必要的端口与服务、明文传输数据等。Modbus 协议是在工控系统中应用较多的一种专有协议。该协议采用轮询方式查询数据, 每个请求之间会有一个小的时间间隔, 从而为劫持通信留下一个很小的但可用的时间窗口。此外, 它没

有用于身份验证、授权和加密的内置机制,使攻击者有可能分析出 Modbus 消息中来自物理过程的关键信息^[36]。Biham 等^[37]指出西门子 PLC S7-1200 使用的 P2 协议(S7 协议版本 2)在下载消息时不受完整性保护,且不对运行对象加密。作者模拟了 TIA 与 S7-1200 之间的通信,以纯文本形式发送运行对象,攻击者在分析运行对象的结构后,确定其指令和操作数,能很容易地修改现有的运行对象来构建具有某些功能的控制程序。此外,其他的协议存在类似的安全性问题。

在现代工控系统中,随着全球互联网技术的发展,工控协议趋于开放和透明。基于 TCP/IP 或 UDP/IP 技术的工控协议陆续推出并成功应用。施耐德公司推出了基于 TCP/IP 以太网的 Modbus TCP。它是第一家采用 TCP/IP 以太网并用于工业自动化领域的标准协议,其 TCP 端口是 502。除此之外,还有 PROFINET、OPC UA、Ethernet/IP、POWERLINK 和 HART/IP 等协议,还有些设备使用现有的 IP 网络(包括 Internet)进行通信^[38]。这些新的变化,使 ICS 组件以及通信协议遭受外部黑客攻击的风险比传统 IT 系统高^[39]。

数据加密和身份认证是传统互联网络采用的保护数据完整性和机密性的有效手段。为了保护 ICS 免受网络攻击,一些学者尝试将其引入工控系统^[40-42]。加密技术的引入,极大地减少了重放和窃听攻击^[43]。智能电网中的大多数电子设备有望具有轻量级的加密功能^[44]。

目前针对密码学在工控系统中的应用研究仍处于起步阶段^[42]。加密传输应用于工控系统还有很多问题没有得到很好的解决。

1) 实时响应问题。ICS 是硬实时系统^[45],在特定时间范围内没有发出控制信号或完成某项操作,可能会导致生产安全方面的重大损失。

2) 有限的计算能力。工控系统中控制器及现场智能设备的内存和计算能力有限,而加解密算法的实现需要比较大的开销。

3) 系统稳定性问题。Wei 等^[46]通过实验说明消息加密和解密导致的额外时延可能会导致智能电网的电压崩溃概率变为原来的 10 倍。这说明加解密算法可能带来不小的负面影响,甚至严重的后果。

4) 系统可维护性问题。加密会大大增加故障排除和恢复的成本,与未加密的网络相比,未加密网络中的问题(如通信故障、重传、设备故障等)可以更快、更轻松地被识别^[47]。

无线技术在控制系统中的应用越来越多。工业无线通信是数字化转型的关键要素,但也可能带来一些挑战。传统的 Wi-Fi(802.11)可用于在工程便携式计算机、移动 HMI、PLC 等之间建立连接。但如果配置不正确(即安全性和传输范围),它们可能会在现场站点的物理范围之外引发额外的风险^[48]。无线传输极易受到来自各种来源的干扰和影响,如电磁辐射、热噪声、快速移动的设备等,这会导致传输错误。

随着工业互联网的快速发展,云计算为工控系统带来了很多好处。基于公共、私有或混合的云服务,使使用者可以在任何时间和任何地点方便地访问 ICS 操作数据^[49],简化了工业管理的流程,提高企业的经济效益。但是,云计算的大规模发展也带来了许多问题。国家互联网应急中心在 2020 年上半年数据分析报告中指出^[50]:我国根云、航天云网、OneNET、COSMOPlat、奥普云、机智云等大型工业云平台持续遭受来自境外的网络攻击,平均攻击次数达到 114 次/日,同比上升 27%。工业云平台承载着大量接入设备、业务系统,以及企业、个人信息等重要数据,使其成为网络攻击的重点目标。这使 ICS 面临如下新的安全问题^[8,51]。

1) 云通信的加入使 SCADA 系统更加开放,在通信过程中可能存在数据嗅探、数据泄露、数据修改、数据丢失或数据欺骗。

2) SCADA 系统和云之间的网络连接可能会打开 ICS 的后门,攻击者可以利用这些后门进行攻击。

3) 运行在云上的 SCADA 系统应用程序很容易被攻击者搜索和滥用。

4) 云和外部个别服务提供商都有自己的安全漏洞。

3 工控系统攻击分类

3.1 SCADA 控制中心

控制中心的工程师工作站可将控制程序下载到 PLC 中执行控制命令。因此,工程师工作站

是部署恶意活动的主要目标。Biham 等^[37]创建了恶意工作站，并伪装成工程师工作站，实现了对 PLC 远程启动/停止攻击和程序下载攻击。作者构建了两种恶意工作站。

1) “流氓”工作站：利用伪造的工作站，自行构建或读取原有的 S7 数据包，修改后发送给 PLC，执行 PLC 的启动/停止攻击。

2) 高级“流氓”站：利用现有工作站，采用中间人攻击，用代理工作站接管现有工作站，并从中接收会话密钥；能独立修改下载消息所包含控制逻辑的两个副本（源代码和二进制代码）；能够按工程师期望的方式维护源程序，同时对 PLC 进行编程以运行工程师永远不会看到的恶意二进制文件。

Zhang^[52]设计了两种针对工程师工作站的攻击方案，其攻击路径如图 2 所示。一种是数据泄露。攻击者通过网络钓鱼攻击，在工程师工作站与外部恶意服务器之间建立服务器-客户端协议，从工程师工作站窃取关键信息。另一种是恶意数据注入攻击。如图 2 中 E 所示，攻击者将虚假数据注入工程师工作站和数据存储器，以覆盖攻击者的踪迹。其错误注入攻击步骤如表 2 所示。

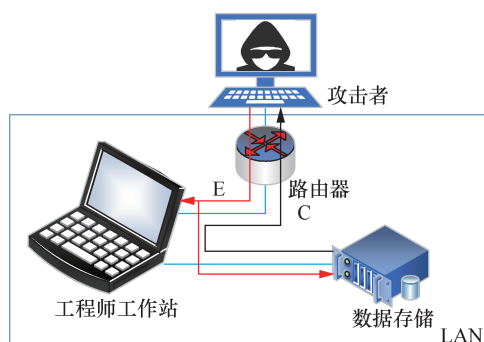


图 2 对工程师工作站的攻击场景

Figure 2 Attack scenario on engineer workstation

表 2 错误注入攻击步骤
Table 2 False data injection attack steps

开始时间 (观察序号)	结束时间 (观察序号)	攻击描述
600 s(150)	630 s(158)	网络发现
840 s(210)	1 020 s(255)	利用 Ettercap 实施中间人攻击
1 020 s(255)	1 020 s(255)	恶意代码注入
1 200 s(300)	2 400 (600)	恶意代码运行 LabVIEW 模型

HMI 也是常见攻击目标之一。HMI 容易遭受密码窃取攻击^[3]。大多数 HMI 存在没有账号和密

码管理措施、用户账号权限分配不当、密码采用弱密码或初始密码或长期保持不变等问题。

针对 HMI 的隐形欺骗攻击也较为常见。攻击者利用虚假信息，让操作员将错误的情况视为真实情况。Kleinmann 等^[53]提出了一种基于语义网络的攻击，攻击工具的架构如图 3 所示。在劫持 HMI 和 PLC 之间的通信通道后，攻击者仅替换消息内容，而不注入、删除、扩展或压缩消息，同时使 HMI 呈现虚假的工业过程视图，从而欺骗操作员采取不适当和有害的手动操作。但由于被攻击者替换的消息的大小、时间及命令序列等都是 100%合法的信息，攻击是完全隐身的，很难检测到此类攻击。Hu 等^[54]也做了相似的研究。

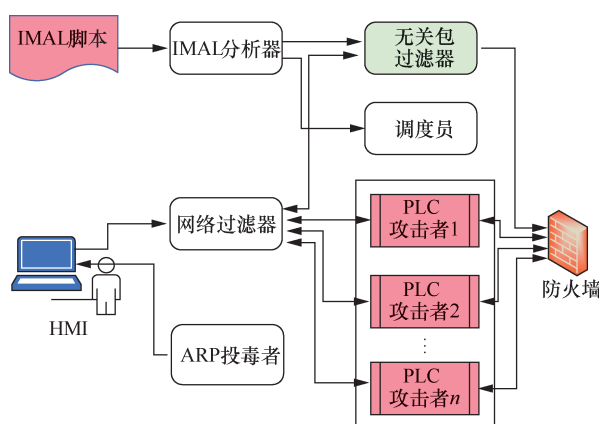


图 3 攻击工具的架构

Figure 3 The architecture of attack tool

3.2 PLC

可编程逻辑控制器是工控系统中使用最广的一种控制器。对 PLC 的攻击会影响物理过程，为工控系统带来灾难性的后果。对 PLC 的常见攻击有如下几种。

1) 固件修改攻击（firmware modification attack）：固件是嵌入式设备的底层软件，PLC 固件为系统输入和物理输出之间提供了软件驱动的接口^[55]。现在很多 PLC 控制器具有固件更新的功能，可以在无须对硬件进行物理变动的情况下，使用软件更新包来修补漏洞或升级功能。攻击者可以利用这一更新过程，通过逆向工程获取固件更新包，然后利用重启系统的控制器漏洞，获取 PLC 的访问权限，再通过远程或本地重启固件更新将恶意代码注入，可执行未经授权的操作。

Basnight 等^[55]介绍了一种通用的固件分析方

法, 通过实验演示了如何更新修改固件版本, 说明了对 PLC 进行固件修改攻击的可行性。Garcia 等^[56]通过修改 PLC 固件, 实现了对 PLC 输入输出的控制。Ma 等^[6]验证了分布式系统中冗余控制器体系结构的缺陷, 对控制器成功进行了隐形攻击, 其攻击过程如下。敌手首先对备用控制器 B 发起固件修改攻击。攻击备用控制器不会引起控制系统状态的任何变化, 因此不会引起管理员或其他监控系统的注意。接着, 敌手攻击主控制器 A, 产生系统故障的假象, 激活切换机制。然后, 敌手对主控制器 A 发起固件修改攻击并注入恶意代码, 再次激活切换机制。在经过两次切换控制器后, 攻击者能够成功控制主控制器。

2) 有效负载攻击 (payload attack): PLC 中的控制程序称为有效负载。通过修改或替换 PLC 的有效负载, 可以获得对执行器的控制权, 破坏生产过程, 可能导致工控系统中断、设备损坏等严重事故。

Govil 等^[33]讨论了梯形逻辑炸弹 (LLB, ladder logic bomb), 即以梯形逻辑编写的恶意软件, 描述了三类 LLB: 拒绝服务 LLB、用于处理传感器读数和命令的 LLB、用于秘密数据记录的 LLB。由于在将新逻辑下载到 PLC 之前缺乏安全性检查和身份验证, 攻击者可将这类恶意软件插入 PLC 的现有控制逻辑中, 然后持续更改行为, 或者等待特定的触发信号来激活恶意行为。

Yoo 等^[32]提出了两种新的控制逻辑注入攻击。① 数据执行攻击。如图 4 所示, 攻击分为两步: 首先, 攻击者将恶意控制逻辑代码传输到目标 PLC 的数据块, 因其不在代码块的地址范围内, 因此不受签名的限制; 其次, 攻击者修改指向恶意控制逻辑代码基址的指针, 从而将 PLC 的系统控制流重定向到恶意逻辑, 并迫使 PLC 执行攻击者的逻辑。② 碎片和噪声填充攻击。该攻击通过在控制逻辑包中附加一系列填充字节来破坏深度包检查。这两种攻击在不中断数据包的传输过程也不修改 PLC 固件的情况下, 操纵控制逻辑数据包, 隐秘地将逻辑传输到 PLC。

Li 等^[57]通过仿真实验证明错误的顺序逻辑攻击会导致严重的过程中断或设备损坏。实施此类攻击的基本要求如下: 物理过程是周期性的,

多个控制组件彼此关联; 控制操作有严格的顺序要求且控制命令有数量限制; 攻击者可以获得足够的知识和背景信息 (如系统拓扑), 并能够更改网络控制系统中工厂与控制器之间交换的数据等。为了成功实施该类攻击, 至少要解决 3 个问题。首先, 攻击者需要渗透目标系统以收集所需信息, 如系统结构、现场设备的配置和参数。其次, 攻击者需要了解组件中使用的专有数据, 以构建恶意有效负载。最后, 需要将恶意有效负载部署到最终目标。这些挑战使在实践中难以成功实施此类攻击。

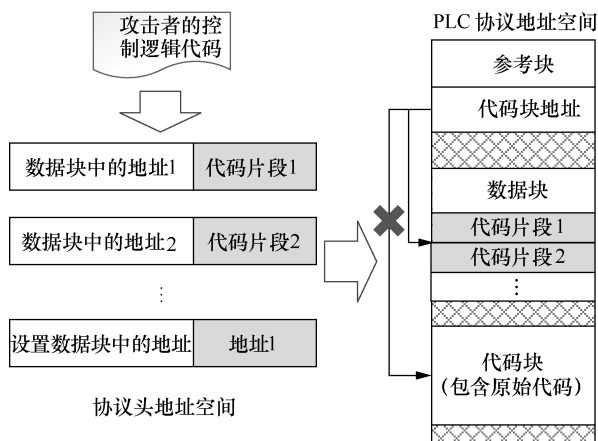


图 4 对协议头检测的数据执行攻击
Figure 4 Data execution attack on protocol header inspection

有些学者通过将工程软件与原始 (未感染) 控制逻辑结合使用, 采用中间人攻击的方式隐藏恶意修改。Kalle 等^[58]设计了一种对 PLC 控制逻辑实施远程攻击的方法 (CLIK)。攻击过程如图 5 所示, 共分为 4 个步骤。① 利用零日漏洞破坏 PLC 的安全措施, 从目标 PLC 窃取原始控制逻辑。② 将窃取的控制逻辑的二进制文件反编译为其高级源代码。③ 通过基于规则的自动化方法感染源代码, 将代码编译为二进制表示, 再传回 PLC 以感染控制逻辑。④ 使用虚拟 PLC 向控制中心的工程软件提供虚假信息。当工程软件尝试从 PLC 获取控制逻辑时, 虚拟 PLC 会截取该请求, 然后使用捕获的流量发送原始控制逻辑进行响应。虚拟 PLC 从工程软件的角度模拟未感染的真实 PLC 的行为。作者在 52 个控制逻辑程序上进行测试, 结果表明 CLIK 能成功地处理不同的逻辑程序。平均而言, CLIK 不到 1 min 即可完成攻击周期并感染目标控制逻辑。

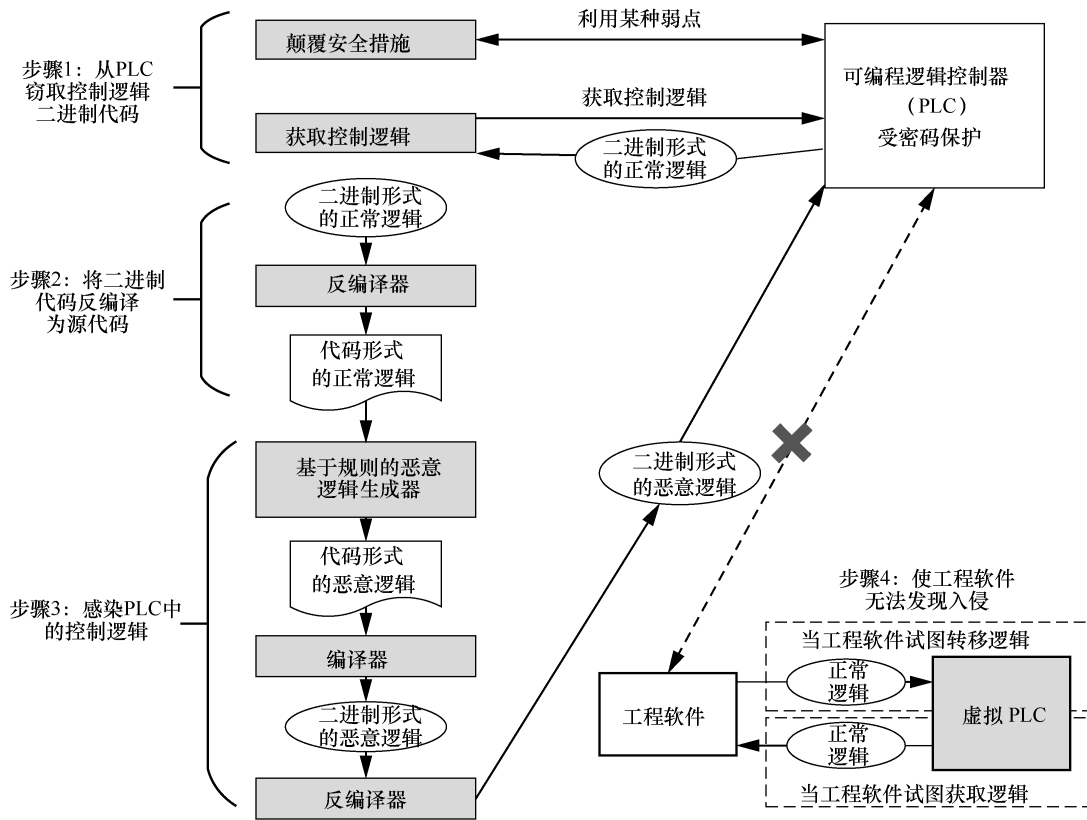


图 5 控制逻辑感染攻击链 CLIK 的高级总览
Figure 5 High-level overview of CLIK, a control logic infection attack

Senthivel 等^[59]在 PLC 和运行 PLC 编程软件的工作站之间实施了中间人操作。当梯形逻辑程序被从编程软件下载到 PLC 时,攻击者将原来的梯形逻辑的一部分替换为受感染的逻辑。当工程师试图将(感染的)程序从 PLC 上传到编程软件时,攻击者将拦截流量并用原始逻辑替换感染的部分。因此,该软件显示正常的程序,以达到欺骗工程师的目的,如图 6 所示。

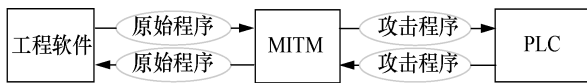


图 6 DEO 攻击 1-从工程软件中隐藏受感染的梯形图逻辑
Figure 6 DEO attack 1-hiding infected ladder logic(running in a target PLC) form the engineering software

3) 引脚控制攻击 (pin control attack)^[60]: 该攻击在不修改 PLC 逻辑指令或固件的前提下,滥用控制器的引脚控制功能,来操作物理过程。引脚控制主要由引脚多路复用和引脚配置两方面组成。攻击者通过更改引脚寄存器修改引脚的多路复用功能,通过将引脚连接到另一个外围设备,

来阻止控制器与外围设备的通信,并对其进行物理损坏。攻击者也可以通过引脚配置攻击,将引脚模式从输入更改为输出,反之亦然,以控制合法进程从该引脚写入或读取信息。由于引脚配置的更改不会产生中断,在运行时复用或重新配置引脚时,系统会像往常一样继续其任务,但输入和输出可能会产生意想不到的结果。

4) 虚假数据注入 (FDI, false data injection) 攻击:可以分为两类:一类是攻击者已经知道 PLC 中的一些关键控制点,并恶意修改其值,从而导致控制混乱,如强制对寄存器地址执行写操作,以覆盖寄存器的当前值;另一类是攻击者向 PLC 注入虚假的传感器测量数据,使 PLC 根据虚假测量数据启用不适当的控制操作。

Gönen 等^[61]通过内部人员对 Schneider M241 PLC 进行错误数据注入攻击。如果内部人员获取了寻址映射,就可以读取寄存器地址的状态,并向内存地址发送新值以更改这些地址的值。对 PLC 设备进行 FDI 攻击的步骤如图 7 所示。

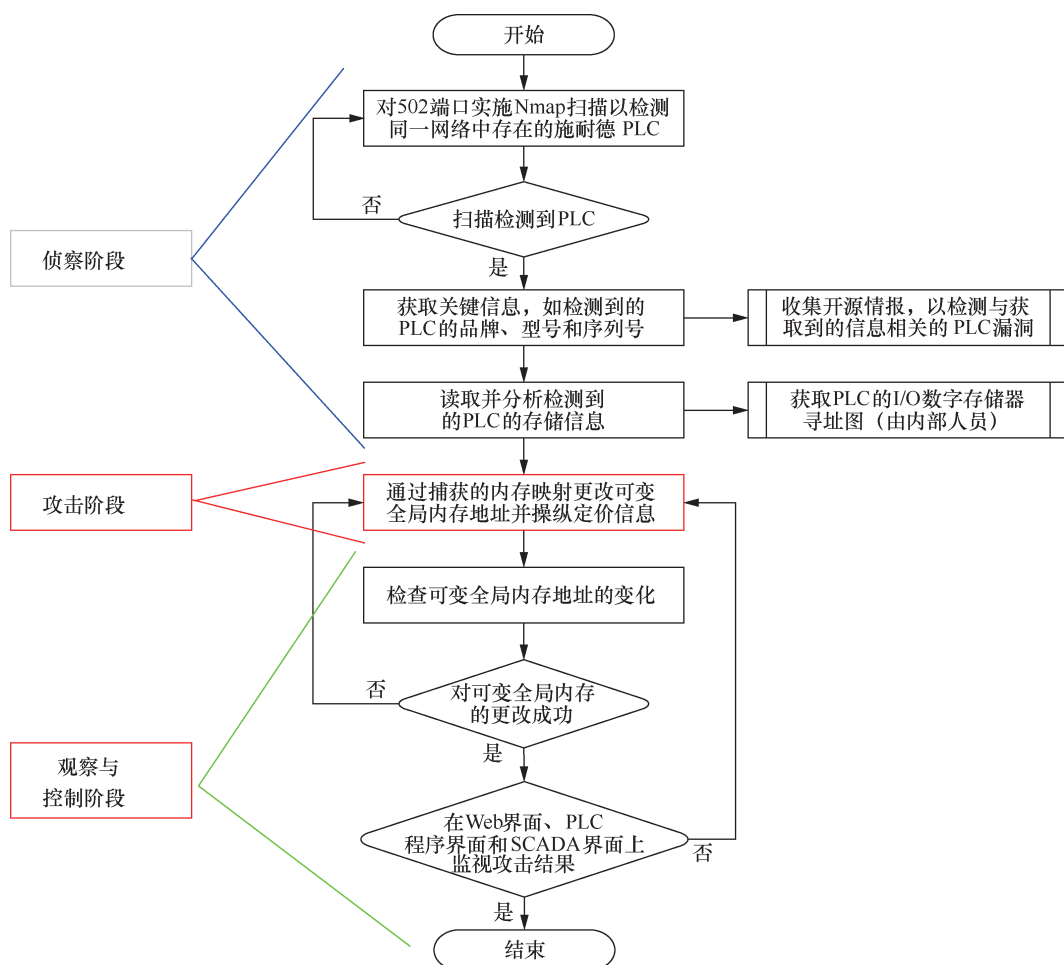


图 7 对 PLC 设备进行 FDI 攻击的步骤
Figure 7 Steps of FDI attack on PLC equipment

Roomi 等^[62]开发了一种可模拟攻击的网络范围, 如图 8 所示: 通过直接篡改受感染设备(继电器、频率监视器和温度传感器等)的数据或返回值, 将其存储在 FDI 攻击配置中, 攻击者可以将伪造的数据动态地注入 PLC, 来模拟 FDI 攻击。但 cyber range 的模拟是轮回进行的, 平均每个回合需要 4.2 s, 无法提供瞬态或实时行为, 但仍可以模拟预先编程的 FDI 攻击。

5) 蠕虫病毒攻击: Spenneberg 等^[63]基于 SIMATIC S7-1200 演示了 PLC 蠕虫攻击的可行性。只需引入受感染的 PLC, 即可使该蠕虫在工控网络中传播。蠕虫感染目标 PLC 的执行步骤如图 9 所示。首先, 蠕虫启动与可能目标的连接。一旦建立了连接, 蠕虫先检查目标是否已经被感染。如果未检测到感染, 蠕虫将停止执行已安装的程序, 并传输自己的代码。然后, 再次启动目

标 PLC。该蠕虫仅使用 PLC, 不需要任何 PC 或服务器即可传播, 且在重启和断电后仍然存在。这些特性使其很难被追踪。

针对 PLC 攻击的分类如表 3 所示。

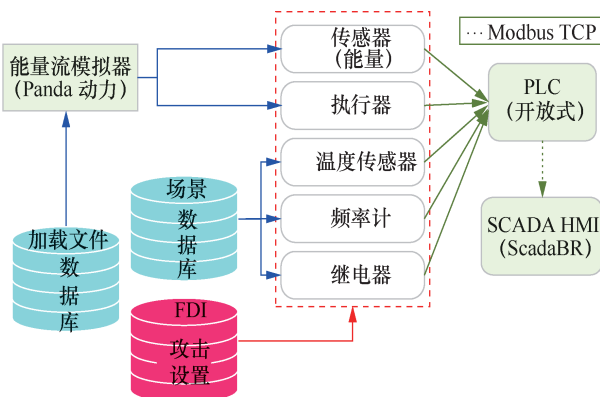


图 8 FDI 网络范围示意
Figure 8 Schematic view of FDI cyber range

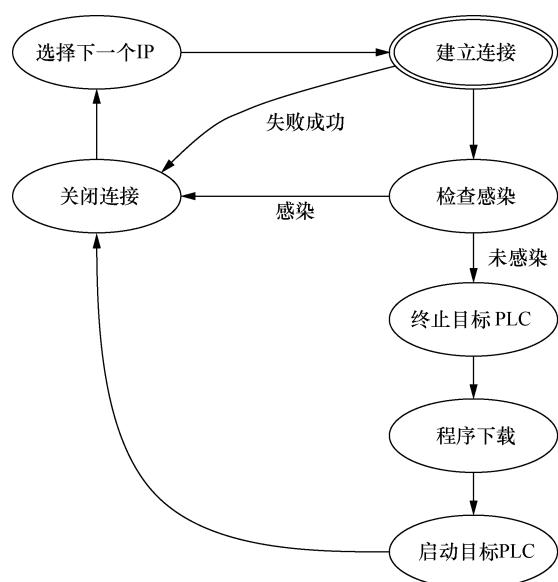


图9 蠕虫的工作顺序
Figure 9 Execution sequence of the worm

3.3 现场设备

传感器数值替换攻击 (sensor spoofing attack): 一种是直接替换, 即攻击者用恶意传感器替换一个或多个传感器, 攻击者可以操纵传感器读数, 将虚假数值反馈到系统; 另一种是间接替换, 即将来自另一个进程的传感器测量值代替目标传感器的测量值。

故意电磁干扰 (IEMI, intentional elec-

tro-magnetic interference) 攻击: 通过有意地引入噪声, 干扰系统的正常运行, 或者向常用的电子系统中注入虚假数据, 使攻击者具有独立控制电子系统的能力。Selvaraj 等^[64]证明了可以使用低功率 IEMI 影响传感器/驱动系统输出的直流或平均电压, 从而允许对模拟和数字系统进行任意虚假数据注入。

缓冲区溢出攻击 (buffer overflow attack): 攻击者可以通过拒绝服务攻击创建溢出。当数据超出分配的内存空间时, 数据的完整性将被破坏。

3.4 工控网络攻击

工控网络信息安全的基本属性包括可用性、完整性和机密性。可用性在保证 ICS 正常运行的重要条件, 意外中断是不可接受的。在 ICS 中, 可用性完整性通常比机密性更重要。本文根据攻击破坏工控网络信息安全的基本属性对攻击进行分类。

3.4.1 可用性攻击

可用性攻击旨在恶意占用网络资源或干扰网络数据, 从而导致数据延时到达或传输中断。常见的可用性攻击有: DoS (denial of service) 攻击^[65]、勒索软件攻击 (ransomware attack)^[15,66]、干扰攻击 (jamming attack)^[67]等。

表3 针对 PLC 攻击的分类
Table 3 Classification on attacks towards PLC

攻击类型	参考文献	控制器	攻击的实验
固件修改攻击	文献[55]	ControlLogix L61	伪造了固件的版本号
	文献[6]	NA400-0501 UWNTEK UW5101 FM802 CPU	对 3 种控制器进行逆向工程并找到所需的漏洞, 来攻击冗余控制器
	文献[56]	Allen Bradley PLC	通过修改 PLC 的固件, 在不改变 PLC 控制逻辑的情况下操作 PLC 的输入和输出值
有效负载攻击	文献[58]	Schneider Electric Modicon M221 PLC	设计了一个完整的控制逻辑感染攻击链, 包括漏洞攻击、反编译、恶意逻辑生成和隐藏感染
	文献[59]	Allen-Bradley Micrologix 1400-B PLC	设计了 3 种控制逻辑攻击场景, 称为 DEO (denial of engineering operations) 攻击, 可能严重影响控制中心操作员的态势感知, 以产生安全隐患
	文献[33]	工控系统测试平台	进行了 4 种 LLB 的实验及评估
	文献[32]	Modicon M221 MicroLogix 1400	提出了两种新的控制逻辑注入攻击: 数据执行攻击; 碎片和噪声填充攻击
引脚控制攻击	文献[60]	Wago 750-8202 PLC	通过更改引脚相关寄存器修改引脚的功能和配置, 实施引脚控制攻击
虚假数据注入攻击	文献[61]	Schneider M241 PLC	使用错误数据注入进行寄存器操纵
蠕虫病毒攻击	文献[63]	SIMATIC S7-1200	演示了 PLC 蠕虫的可行性

1) DoS 攻击: DoS 攻击指耗尽被攻击对象的资源,以阻止授权个人或实体访问某些资源(如设备、网络等)。此类攻击容易导致系统在有效时间范围内难以执行控制任务。针对 ICS 的 DoS 攻击可能旨在破坏 SCADA 主设备与从设备之间的通信,这可能导致 SCADA 主设备失去对本地控制系统和执行器的控制^[68]。针对控制器的 DoS 攻击,可能会耗尽控制器的计算、存储和网络资源,干扰控制器及时发出控制命令。

2) 勒索软件攻击:勒索软件是一种恶意软件,使用加密等手段劫持工控系统中的重要资源和服务,致使受攻击的对象无法访问。然后攻击者向受害者索要金钱以换取被锁定的数据。基于云的文件共享技术使用广泛,云上勒索软件攻击可以在一次攻击中加密无数文件,意味着它的传播速度更快、危害更大。

勒索软件攻击可以分为两类^[66-69]。锁定勒索软件攻击(locker ransomware attack):这种类型的勒索软件会阻止受害者访问他自己的设备,即在支付赎金之前,不允许用户访问他的系统或设备。Zhang 等^[70]构造一种勒索软件 ICS-BROCK,其攻击步骤如下:通过漏洞检测发现易受攻击的工作站,并尝试感染它和 PLC 的上位机,然后将逻辑炸弹写入 PLC 并锁定,被锁定的 PLC 需要解锁密钥才能正常工作。该方法能用较少的信息完成勒索攻击,更接近真实的攻击场景。加密勒索软件攻击(crypto ransomware attack):此类攻击会搜索用户的有用数据并对其进行加密,除加密文件之外,用户可以不受限制地访问并操作系统。Zimba 等^[15]对多阶段加密勒索软件攻击进行了建模。通过静态恶意软件分析说明,勒索软件可采用不同的技术,在不同的网络分区传播和攻击关键基础设施。

3) 干扰攻击:由于无线媒体的开放性,无线通信容易受到无线电干扰的攻击。当恶意设备发出高功率干扰信号时,其附近的所有无线设备可能无法通信^[71]。Adepu 等^[67]在安全水处理(SWAT, secure water treatment)实验台上实现了对工控系统的网络干扰攻击。作者通过使用可配置的射频设备、通用软件无线电外设(USRP, universal software radio peripheral)来阻塞通信信

道,实现了干扰攻击。

3.4.2 完整性攻击

完整性攻击试图在从源头传输到目的地的过程中插入、更改或删除数据,从而破坏数据交换和决策。常见的完整性攻击有:重放攻击(replay attack)^[53,72]、节点复制攻击(node replication attack)^[73]等。

1) 重放攻击:攻击者可以在不篡改任何数据的情况下,将另一时段从网络上窃听的数据包发送出去,达到欺骗系统的目的。由于工控系统中传输的数据包没有时间戳,只要数据格式正确,很难判断数据包的真假^[74]。

重放攻击是 PLC 中典型的攻击方式之一,攻击包括 3 个步骤^[75]:① 启动 Wireshark,捕获数据包;② 过滤掉不属于流量命令中的指令包;③ 通过取得命令包的格式对 PLC 进行重放攻击。HMI 也是重放攻击的常见目标。在劫持 HMI 和 PLC 之间的通信通道后,攻击者可以仅替换消息内容,使 HMI 呈现历史数据视图从而欺骗操作员^[53]。

2) 节点复制攻击:在无线工业网络中,通常会复制一些真实节点,以增强节点的处理能力。但攻击者可以使用捕获的真实节点中的信息来创建恶意节点。

文献[73]利用 NIST 开放数据集进行汽车装配环境下复制攻击的仿真实验。攻击者首先劫持合法节点,并提取其 ID、密钥、控制信息、数据信息等有关的敏感信息。随后,攻击者根据提取的信息来复制节点,并部署在工业无线网络中。然后,复制的节点可以充当合法节点与其他节点进行数据交互。当无线网络中存在大量复制节点时,它们可以通过连续发送访问请求始终占据通信通道来发起拒绝服务攻击。攻击者还可通过在网络中广播恶意信息,以注入恶意数据或更改合法节点的传输信息,来破坏数据的完整性。

3.4.3 机密性攻击

机密性攻击指未经授权的实体嗅探、网络数据窃取或流量分析。常见的机密性攻击有:窃听攻击(eavesdropping attack)^[76]、中间人攻击(man-in-the-middle attack)^[77-78]、位置欺骗攻击(location spoofing attack)^[79]等。

窃听攻击：窃听攻击是一种被动攻击，攻击者可以嗅探网络通信通道，以捕获网络通信上正在发送和接收的信息。窃听攻击不会导致工控系统产生不正常的现象，因此很难被检测到。

中间人攻击：攻击者进入两台设备之间的对话，并在交换数据和控制消息的同时让两端认为他们正在与对方直接对话。中间人攻击有主动和被动两种攻击方式^[80]。被动方式是监控控制器通信流量并获取数据。主动方式是通过篡改数据和命令，干扰系统的正常运行。Urbina 等^[77]展示了如

何在 ICS 现场总线网络中，采用中间人攻击从被窃听的信息中获取传感器读数，并伪造传感器和执行器命令。此外，作者讨论了设置中间人攻击存在的一些挑战以及如何克服这些挑战。

位置欺骗攻击：通过伪造无线电信号，一方面，攻击者可以误导定位到一个错误的结果，这将对依赖于位置信息的工业系统造成威胁^[79]；另一方面，攻击者若伪装成具有高访问权限的位置，则可能非法访问机密资源。

针对工控网络攻击的分类如表 4 所示。

表 4 针对工控网络攻击的分类
Table 4 Classification on attacks towards industrial control net

基本属性	攻击类型	文献	简要描述
可用性	DoS 攻击	文献[65]	通过使用 Hping、SmootSec IDS 和 Wireshark 等工具对 PLC 和 TIA Portal 应用程序进行 DoS 攻击。作者侧重于检测 PLC 设备和 TIA Portal 应用程序的漏洞，并进行安全分析来确定解决方案
	勒索软件攻击	文献[15]	模拟来自 CI (critical infrastructure) 中 3 种渗透源的不同加密勒索软件多级攻击。通过静态恶意软件分析说明，勒索软件采用不同的技术，在不同的网络分区传播和攻击 CI 组件
		文献[66]	对物联网环境中勒索软件的演变、预防和缓解进行了全面调查
	干扰攻击	文献[67]	在安全水处理 (SWAT) 实验台上实现了对工控系统的网络干扰攻击
完整性	重放攻击	文献[53]	在劫持 HMI 和 PLC 之间的通信通道后，在 HMI 中重放先前获得的消息
		文献[72]	在配水 (WADI) 工厂试验台发起重放攻击，研究在什么情况下，攻击者/攻击可以在盗取水时不被发现
	节点复制攻击	文献[73]	利用 NIST 开放数据集进行汽车装配环境下复制攻击的仿真实验
机密性	窃听攻击	文献[76]	模拟无线网络中的窃听攻击，同时考虑了信道条件和天线模型。分析了路径损失效应、阴影衰落效应与窃听攻击的概率
	中间人攻击	文献[77]	讨论了对 ICS 现场总线通信的中间人攻击，给出了有关典型拓扑和此类设置中使用协议的详细信息
	位置欺骗攻击	文献[78]	利用 COPS SCADA Lab kit、Ettercap、Wireshark 等工具对 SCADA 网络实施中间人攻击
		文献[79]	采用 Matlab 仿真位置欺骗攻击

4 未来攻击趋势

未来针对工控系统攻击的主要发展趋势主要如下。

(1) 针对工控攻击的门槛降低

攻击者发动 ICS 攻击变得越来越容易，这归因于越来越多的工具或示例可供使用，从而降低了入侵者所需知识和技能^[81]。信息技术 (IT) 和运营技术 (OT) 领域的融合将成为常态，入侵者甚至可以绕开工控底层专业知识，采用常规手段组合式攻击来直接攻击控制系统。

(2) 针对设备的攻击有所上升

工控设备使用年限较长，软硬件存在安全漏洞、设备缺乏认证和授权管理、数据加密和完整性检查欠缺等问题。工控设备所处的环境安全、设备安全和管理安全任何一方面遭受攻击，可能对整个工控系统造成巨大的损坏。特别是随着智能设备大规模部署，互联互通已成为必然趋势，工控安全问题也会随着连接性的增长而增加。

(3) 勒索软件攻击日渐频繁

近几年，针对工控系统的勒索软件攻击逐渐上涨，其原因可能有两个方面：一方面，经济利益是吸引攻击者使用该类攻击的首要因素，

黑客组织采用钓鱼邮件、软件捆绑、鱼叉式攻击等方式向企业发起勒索攻击，索要高昂的赎金；另一方面，数字货币的出现及使用，如比特币，可使攻击者轻松获得非法报酬，而不必担心真实身份的暴露，有利于匿名“安全”支付^[82-83]。这可能是勒索软件攻击在数字货币出现之后越发流行的原因之一。

(4) 高级可持续威胁攻击日趋严重

高级可持续威胁攻击仍将是复杂性和最棘手的工控攻击之一，它采用多种攻击方式来渗透和分析目标，具有极强的隐蔽性和持久性，使防御者难以检测和防御。APT 攻击的目的性很强，对石油、化工、电力、核能等国家关键基础设施的安全构成严重威胁。

(5) 针对企业上云的安全问题日益突出

工业和信息化部印发了《推动企业上云实施指南（2018—2020 年）》，并表示上云比例和应用深度显著提升，使云计算在企业中广泛普及。随着企业上云的普及，攻击者利用云计算资源攻击企业或云服务提供商也会增多，如分布式拒绝服务攻击、网络钓鱼活动、恶意托管、数据盗取等。

5 结束语

工控系统是电力、交通、石化等国家关键基础设施的重要组成部分。对工控系统的攻击，会扰乱系统的运行，对工业生产的经济效益产生很大影响，甚至造成人员伤亡。本文对工控系统中关键组件面临的安全问题和攻击方法相关文献进行了综述：首先介绍了 ICS 的基本概念；然后对关键工控组件的安全问题进行了分析，重点从控制中心、PLC、现场设备、工控网络，对现有文献的攻击方法进行分类、总结；最后，指出了未来工控攻击的发展趋势。

参考文献：

- [1] 工业和信息化部. 关于印发信息化和工业化融合发展规划(2016—2020 年)的通知[EB]. Ministry of industry and information technology. Notice on printing and distributing the integrated development plan of informatization and industrialization (2016—2020) [EB].
- [2] 赛迪顾问. 2019—2021 年中国工业控制市场预测与展望数据[EB]. CCID Consultant. 2019—2021 Forecast and prospect data of China's industrial control market[EB].
- [3] BABU B, IJYAS T, MUNEEER P, et al. Security issues in SCADA based industrial control systems[C]//2017 2nd International Conference on Anti-Cyber Crimes (ICACC). 2017: 47-51.
- [4] AYODEJI A, LIU Y, CHAO N, et al. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems[J]. Nuclear Engineering and Technology, 2020, 52(12): 2687-2982.
- [5] HUANG D, SHI X, ZHANG W A. False data injection attack detection for industrial control systems based on both time-and frequency-domain analysis of sensor data[J]. IEEE Internet of Things Journal, 2020, 8(1): 585-595.
- [6] MA R, CHENG P, ZHANG Z, et al. Stealthy attack against redundant controller architecture of industrial cyber-physical system[J]. IEEE Internet of Things Journal, 2019, 6(6): 9783-9793.
- [7] XU L D, XU E L, LI L. Industry 4.0: state of the art and future trends[J]. International Journal of Production Research, 2018, 56(8): 2941-2962.
- [8] SAJJID A, ABBAS H, SALEEM K. Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges[J]. IEEE Access, 2016, (4): 1375-1384.
- [9] ASGHAR M R, HU Q, ZEADALLY S. Cybersecurity in industrial control systems: issues, technologies, and challenges[J]. Computer Networks, 2019, (165).
- [10] UPADHYAY D, SAMPALLI S. SCADA (supervisory control and data acquisition) systems: vulnerability assessment and security recommendations[J]. Computers & Security, 2020, (89).
- [11] NAZIR S, PATEL S, PATEL D. Assessing and augmenting SCADA cyber security: a survey of techniques[J]. Computers & Security, 2017, (70): 436-454.
- [12] YADAV G, PAUL K. Architecture and security of SCADA systems: A review[J]. International Journal of Critical Infrastructure Protection, 2021.
- [13] ALLADI T, CHAMOLA V, ZEADALLY S. Industrial control systems: cyberattack trends and countermeasures[J]. Computer Communications, 2020, 155: 1-8.
- [14] 冯涛, 鲁晔, 方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报, 2017, 38(Z2): 185-196.
FENG T, LU Y, FANG J L. Overview of vulnerability and security protection technology of industrial Ethernet protocol[J]. Journal of communications, 2017, 38 (Z2): 185-196.
- [15] ZIMBA A, WANG Z, CHEN H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems[J]. Ict Express, 2018, 4(1): 14-18.
- [16] XU Y, YANG Y, LI T, et al. Review on cyber vulnerabilities of communication protocols in industrial control systems[C]//2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). 2017: 1-6.
- [17] WAN M, LI J, LIU Y, et al. Characteristic insights on industrial cyber security and popular defense mechanisms[J]. China Communications, 2021, 18(1): 130-150.
- [18] GONZALEZ D, ALHENAKI F, MIRAKHORLI M. Architectural security weaknesses in industrial control systems (ICS) an empirical study based on disclosed software vulnerabilities[C]//2019 IEEE International Conference on Software Architecture (ICSA). 2019: 31-40.
- [19] 黄家辉, 冯冬芹, 王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报, 2016, 42(5): 792-798.

- HUANG J H, FENG D Q, WANG H J. Vulnerability quantification method of industrial control system based on attack graph[J]. *Journal of Automation*, 2016, 42 (5): 792-798.
- [20] 工业互联网产业联盟. 工业互联网安全风险态势报告 2019 [R]. Industrial Internet industry alliance. Industrial Internet security risk situation report 2019[R].
- [21] ANI U P D, HE H, TIWARI A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective[J]. *Journal of Cyber Security Technology*, 2017, 1(1): 32-74.
- [22] KALAM A A E. Securing SCADA and critical industrial systems: From needs to security mechanisms[J]. *International Journal of Critical Infrastructure Protection*, 2021, (32).
- [23] SERHANE A, RAAD M, RAAD R, et al. Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats[J]. *SN Applied Sciences*, 2019, 1(8): 1-12.
- [24] WEERATHUNGA P E, CIORACA A. The importance of testing Smart Grid IEDs against security vulnerabilities[C]//2016 69th Annual Conference for Protective Relay Engineers (CPRE). 2016: 1-21.
- [25] WANG J, SHI D. Cyber-attacks related to intelligent electronic devices and their countermeasures: a review[C]//2018 53rd International Universities Power Engineering Conference (UPEC). Glasgow, Scotland: IEEE, 2018: 1-6.
- [26] FILLATRE L, NIKIFOROV I, WILLETT P. Security of SCADA systems against cyber-physical attacks[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2017, 32(5): 28-45.
- [27] AHMED I, OBERMEIER S, SUDHAKARAN S, et al. Programmable logic controller forensics[J]. *IEEE Security & Privacy*, 2017, 15(6): 18-24.
- [28] KLICK J, LAU S, MARZIN D, et al. Internet-facing PLCs-a new back orifice[J]. *Blackhat USA*, 2015: 22-26.
- [29] FORMBY D, BEYAH R. Temporal execution behavior for host anomaly detection in programmable logic controllers[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 15: 1455-1469.
- [30] MANSOR H, MARKANTONAKIS K, AKRAM R N, et al. Don't brick your car: firmware confidentiality and rollback for vehicles[C]//2015 10th International Conference on Availability, Reliability and Security. 2015: 139-148.
- [31] BETTAYEB M, NASIR Q, TALIB M A. Firmware update attacks and security for IoT devices: Survey[C]//Proceedings of the ArabWIC 6th Annual International Conference Research Track. 2019: 1-6.
- [32] YOO H, AHMED I. Control logic injection attacks on industrial control systems[C]//IFIP International Conference on ICT Systems Security and Privacy Protection. 2019: 33-48.
- [33] GOVIL N, AGRAWAL A, TIPPENHAUER N O. On ladder logic bombs in industrial control systems[M]// *Computer Security*. Berlin, Heidelberg: Springer, 2017.
- [34] SERHANE A, RAAD M, RAAD R, et al. PLC code-level vulnerabilities[C]//2018 International Conference on Computer and Applications (ICCA). 2018: 348-352.
- [35] CERON J M, CHROMIK J J, SANTANNA J, et al. Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands[J]. *arXiv preprint arXiv:2011.02019*, 2020.
- [36] ROSA L, CRUZ T, SIMÕES P, et al. Attacking SCADA systems: A practical perspective[C]//2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). 2017: 741-746.
- [37] BIHAM E, BITAN S, CARMEL A, et al. Rogue7: Rogue engineering-station attacks on S7 Simatic PLCs[J]. *Black Hat USA*, 2019, 1-21.
- [38] DODSON M, BERESFORD A R, THOMAS D R. When will my PLC support Mirai? The security economics of large-scale attacks against Internet-connected ICS devices[C]//2020 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2020: 1-14.
- [39] DRIAS Z, SERHROUCHNI A, VOGEL O. Taxonomy of attacks on industrial control protocols[C]//2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS). 2015: 1-6.
- [40] DRIAS Z, SERHROUCHNI A, VOGEL O. Identity-based cryptography (IBC) based key management system (KMS) for industrial control systems (ICS)[C]//2017 1st Cyber Security in Networking Conference (CSNet). 2017: 1-10.
- [41] YANG L, SHANG W, CHEN C, et al. Authentication technology in industrial control system based on identity password[C]//2020 39th Chinese Control Conference (CCC). 2020: 7677-7684.
- [42] 梁耀, 冯冬芹, 徐珊珊, 等. 加密传输在工控系统安全中的可行性研究[J]. *自动化学报*, 2018, 44(03): 434-442.
- LIANG Y, FENG D Q, XU S S, et al. Feasibility study of encrypted transmission in industrial control system security[J]. *Journal of automation*, 2018, 44 (3): 434-442.
- [43] ELMRABET Z, ELGHAZI H, KAABOUCH N, et al. Cyber-security in smart grid: Survey and challenges[J]. *Computers & Electrical Engineering*, 2018, 67: 469-482.
- [44] GUNDUZ M Z, DAS R. Cyber-security on smart grid: threats and potential solutions[J]. *Computer Networks*, 2020(169): Article No. 107094.
- [45] SILBERSCHATZ A, GALVIN P B, GAGNE G. Operating system concepts[M]. New Jersey: John Wiley & Sons, 2006.
- [46] WEI M, WANG W. Safety can be dangerous: secure communications impair smart grid stability under emergencies[C]//2015 IEEE Global Communications Conference (GLOBECOM). 2015: 1-6.
- [47] FAURI D, WIJS B D, HARTOG J D, et al. Encryption in ICS networks: a blessing or a curse?[C]//2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). 2017: 289-294.
- [48] GREEN B, KNOWLES W, KROTOFIL M, et al. PCaAD: towards automated determination and exploitation of industrial processes[J]. *arXiv preprint arXiv:2102.10049*, 2021.
- [49] ADEYANJU I A, EMAKE E D, OLANIYAN O M, et al. Digital industrial control systems: vulnerabilities and security technologies[J]. *Current Applied Science and Technology*, 2021: 188-207.
- [50] 国家互联网应急中心. 2020 年我国互联网网络安全态势综述[R]. National Internet Emergency Center. Overview on China's Internet network security situation in 2020[R].
- [51] BHAMARE D, ZOLANVARI M, ERBAD A, et al. Cybersecurity for industrial control systems: a survey[J]. *Computers & Security*, 2020, 89: 101677.

- [52] ZHANG F. Cybersecurity solutions for industrial control systems and key equipment[D]. Knoxville: University of Tennessee, 2019.
- [53] KLEINMANN A, AMICHAY O, WOOL A, et al. Stealthy deception attacks against SCADA systems[M]// Computer Security. Berlin Heidelberg: Springer, 2017.
- [54] HU Y, SUN Y, WANG Y, et al. An enhanced multi-stage semantic attack against industrial control systems[J]. IEEE Access, 2019, 7: 156871-156882.
- [55] BASNIGHT Z, BUTTS J, JR J L, et al. Firmware modification attacks on programmable logic controllers[J]. International Journal of Critical Infrastructure Protection, 2013, 6(2):76-84.
- [56] GARCIA L, BRASSER F, CINTUGLU M H, et al. Hey, my malware knows physics! attacking plcs with physical model aware rootkit[C]//NDSS. 2017: 1-15.
- [57] LI W, XIE L, DENG Z, et al. False sequential logic attack on SCADA system and its physical impact analysis[J]. Computers & Security, 2016, 58: 149-159.
- [58] KALLE S, AMEEN N, YOO H, et al. Klik on plcs! Attacking control logic with decompilation and virtual plc[C]//Binary Analysis Research (BAR) Workshop, Network and Distributed System Security Symposium (NDSS). 2019:1-12.
- [59] SENTHIVEL S, DHUNGANA S, YOO H, et al. Denial of engineering operations attacks in industrial control systems[C]//Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018: 319-329.
- [60] ABBASI A, HASHEMI M. Ghost in the plc designing an undetectable programmable logic controller RootKit via pin control attack[J]. Black Hat Europe, 2016, 2016: 1-35.
- [61] GÖNEN S, SAYAN H H, YILMAZ E N, et al. False data injection attacks and the insider threat in smart systems[J]. Computers & Security, 2020, 97: 101955.
- [62] ROOMI M M, BISWAS P P, MASHIMA D, et al. False data injection cyber range of modernized substation system[C]//2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). 2020: 1-7.
- [63] SPENNEBERG R, BRÜGGEMANN M, SCHWARTKE H. Plc-blasters: A worm living solely in the PLC[J]. Black Hat Asia, 2016, 16: 1-16.
- [64] SELVARAJ J, DAYANIKLI G Y, GAUNKAR N P, et al. Electromagnetic induction attacks against embedded systems[C]//Proceedings of the 2018 on Asia Conference on Computer and Communications Security. 2018: 499-510.
- [65] YILMAZ E N, CIYLAN B, GÖNEN S, et al. Cyber security in industrial control systems: analysis of DoS attacks against PLCs and the insider effect[C]//2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). 2018: 81-85.
- [66] HUMAYUN M, JHANJHI N Z, ALSAYAT A, et al. Internet of things and ransomware: evolution, mitigation and prevention[J]. Egyptian Informatics Journal, 2021, 22(1): 105-117.
- [67] ADEPU S, PRAKASH J, MATHUR A. Waterjam: An experimental case study of jamming attacks on a water treatment system[C]//2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). 2017: 341-347.
- [68] ZHANG F, KODITUWAKKU H A D E, HINES J W, et al. Multi-layer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data[J]. IEEE Transactions on Industrial Informatics, 2019, 15(7): 4362-4369.
- [69] SAJJAN R S, GHORPADE V R. Ransomware attacks: Radical menace for cloud computing[C]//2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). 2017: 1640-1646.
- [70] ZHANG Y, SUN Z, YANG L, et al. A11 Your PLCs Belong to me: ICS ransomware is realistic[C]//2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2020: 502-509.
- [71] PIRAYESH H, SANGDEH P K, ZENG H. Securing ZigBee communications against constant jamming attack using neural network[J]. IEEE Internet of Things Journal, 2020, 8(6): 4957-4968.
- [72] PALLETI V R, MISHRA V K, AHMED C M, et al. Can replay attacks designed to steal water from water distribution systems remain undetected?[J]. ACM Transactions on Cyber-Physical Systems, 2020, 5(1): 1-19.
- [73] CHEN S, PANG Z, WEN H, et al. Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks[J]. IEEE Transactions on Industrial Informatics, 2020, 17(3): 2041-2051.
- [74] QIAN J, DU X, CHEN B, et al. Cyber-physical integrated intrusion detection scheme in SCADA system of process manufacturing industry[J]. IEEE Access, 2020, 8: 147471-147481.
- [75] 陆冠竹, 刘奕贤, 刘宗晔, 等. 工业控制系统安全之探讨——以西门子 S7 系列为例[C]//TANET2019. 2019: 715-719.
- LU G Z, LIU Y X, LIU Z C, et al. Discussion on the safety of industrial control system — Taking Siemens S7 Series as an example[C]//TANet 2019. 2019: 715-719.
- [76] LI X, XU J, DAI H N, et al. On modeling eavesdropping attacks in wireless networks[J]. Journal of Computational Science, 2015, 11: 196-204.
- [77] URBINA D I, GIRALDO J A, TIPPENHAUER N O, et al. attacking fieldbus communications in ICS: applications to the SWaT testbed[C]// Proceedings of the Singapore Cyber-Security Conference (SG-CRC). 2016: 75-89.
- [78] DEB D, CHAKRABORTY S R, LAGINENI M, et al. Security analysis of MITM attack on SCADA network[C]//International Conference on Machine Learning, Image Processing, Network Security and Data Sciences. Abu Dhabi, The United Arab Emirates: Springer. 2020: 501-512.
- [79] LIU D, XU Y HUANG X. Identification of location spoofing in wireless sensor networks in non-line-of-sight conditions[J]. IEEE Transactions on Industrial Informatics, 2017, 14(6): 2375-2384.
- [80] PAN X, WANG Z, SUN Y. Review of PLC security issues in industrial control system[J]. Journal of Cybersecurity, 2020, 2(2): 69-83.
- [81] DI PINTO A, DRAGONI Y, CARCANO A. TRITON: The first ICS cyber attack on safety instrument systems[C]//Proc. Black Hat. 2018: 1-26.
- [82] AHMED Y A, KOCER B, HUDA S, et al. A system call refinement-based enhanced minimum redundancy maximum relevance

method for ransomware early detection[J]. Journal of Network and Computer Applications, 2020, 167: 102753.

- [83] GAZZAN M, ALQAHTANI A, SHELDON F T. Key factors influencing the rise of current ransomware attacks on industrial control systems[C]//2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). 2021: 1417-1422.

[作者简介]



唐士杰（1980-），女，广西灌阳人，桂林电子科技大学讲师，主要研究方向为工控安全。



李俊（1986-），男，江西吉安人，国家工业信息安全发展研究中心高级工程师，主要研究方向为工控安全、工业互联网安全、新一代信息技术安全。



丁勇（1975-），男，四川潼南人，桂林电子科技大学教授、博士生导师，主要研究方向为网络信息安全、工控安全、密码学。



袁方（1980-），男，江苏沛县人，外交部通信总台高级工程师，主要研究方向为专用通信建设、信息化应用、信息安全、密码应用、网络安全。



王会勇（1977-），男，山东诸城人，桂林电子科技大学副教授，主要研究方向为网络信息安全与隐私保护。