DOI:10.7544/issn1000-1239.20211154
59(5):1035-1053,2022

# 工业控制系统安全综述

杨 婷[1,2] 张嘉元[2,3] 黄在起[1] 陈禹劼[1] 黄成龙[1] 周 威[4] 刘 鹏[5] 冯 涛[3] 张玉清[1,2,6]

[1](西安电子科技大学网络与信息安全学院 西安 710071)

[2](中国科学院大学国家计算机网络入侵防范中心 北京 101408)

[3](兰州理工大学计算机与通信学院 兰州 730050)

[4](华中科技大学网络空间安全学院 武汉 430074)

[5](美国宾夕法尼亚州立大学信息科学与技术学院 美国宾夕法尼亚州斯泰特科利奇 16802)

[6](海南大学计算机与网络空间安全学院 海口 570228)

(yangt@nipc.org.cn)

# Survey of Industrial Control Systems Security

Yang Ting[1,2], Zhang Jiayuan[2,3], Huang Zaiqi[1], Chen Yujie[1], Huang Chenglong[1], Zhou Wei[4], Liu Peng[5], Feng Tao[3], and Zhang Yuqing[1,2,6]

[1](*School of Cyber Engineering, Xidian University, Xi'an* 710071)

[2](*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing* 101408)

[3](*School of Computer and Communication, Lanzhou University of Technology, Lanzhou* 730050)

[4](*School of Cyber Science and Engineering, Huazhong University of Science & Technology, Wuhan* 430074)

[5](*College of Information Sciences and Technology, Pennsylvania State University, State College, PA, USA* 16802)

[6](*School of Computer Science and Cyberspace Security, Hainan University, Haikou* 570228)

**Abstract** In addition to the application of manufacturing industries, industrial control systems are also widely used in critical infrastructure such as transportation, energy, and water treatment industries. Accelerated application of digital, network, and intelligent technologies in industrial control systems, more and more smart devices are connected to it, leading to severe challenges to its security. Therefore, the security of industrial control systems has attracted the attention of researchers. In order to let the researchers systematically understand the current research progress, we have researched the core database of Web of Science, EI database, the network and information security related papers of CCF recommended international academic conferences and other high-level research work in the past three years. First, the architecture of industrial control systems is introduced, then the security threats that ICS faces are introduced. Moreover, according to the architecture of the industrial control systems, we divide the security research work into three parts: the communication security of industrial control system and cloud, the communication security of human machine interface (HMI) to device, the security of device firmware and other security research issues, analyze them from the perspective of attack and defense. Finally, we put forward the main challenges that security research faces, identify open problems for future research directions.

**收稿日期**:2021-11-16;**修回日期**:2022-01-20

**基金项目**:国家自然科学基金项目(U1836210);国家重点研发计划项目(2018YFB0804701)

This work was supported by the National Natural Science Foundation of China (U1836210) and the National Key Research & Development Program of China (2018YFB0804701).

**通信作者**:张玉清(zhangyq@ucas.ac.cn)

**Key words** industrial control systems security; Industry 4.0; industrial Internet of things; attack; countermeasures

**摘 要** 工业控制系统除了应用于生产制造行业外,还广泛应用于交通、水利和电力等关键基础设施.随着工业数字化、网络化、智能化的推进,许多新技术应用于工业控制系统,提高了工业控制系统的智能化水平,但其也给工业控制系统的安全带来严峻的挑战.因此,工业控制系统的安全倍受研究人员的关注.为了让研究人员系统化地了解目前的研究进展,调研了近 3 年 Web of Science 核心数据库、EI 数据库和 CCF 推荐网络与信息安全国际学术会议中发表的与工业控制系统安全相关论文以及其他相关的高水平研究工作.首先,介绍工业控制系统的体系结构及面临的威胁.然后,依据工业控制系统的体系结构,自上而下将其安全研究工作分为 ICS-云平台通信安全、HMI-设备通信安全、设备固件安全以及其他安全研究,并从攻击和防御角度进行分析和整理.最后,提出当前工业控制系统安全研究依然面临的主要挑战,并指出未来研究发展的方向.

**关键词** 工业控制系统安全;工业 4.0;工业物联网;攻击;防御

**中图法分类号** TP391

与传统网络安全相比,工业控制系统(industrial control system, ICS)在过去从未被认为存在潜在网络安全风险.在工业 4.0 时代[1],为了方便维护和管理,工业控制系统连接了越来越多的组件和设备.并且随着"中国制造 2025"的推进,工业控制系统将进一步地数字化、网络化和智能化[2].由于现有工业硬件无法轻易替换或更新,而将目前的安全功能集成到现有工业控制系统中极具挑战性(解决方案必须向后兼容几十年前的设备),工业控制系统正面临严重的安全威胁.如图 1 所示,总结了近 20 年影响力较大的工业控制系统安全事件,其中典型的安全事件是 Stuxnet 攻击伊朗核设备和 Industoryer 入侵乌克兰电网.Stuxnet 是第一个包含 PLC rootkit 的病毒,它将恶意代码注入到 PLC 程序中,使离心机以超出可接受范围的速度运行,从而破坏伊朗核计划.Industoryer 病毒是针对工业控制协议 IEC 60870-5-101,IEC 60870-5-104,OPC DA 和 IEC 61850 设计的.2016 年 12 月,Industroyer 攻击了乌克兰电网,它能够扫描工业控制系统的环境,直接向远程控制单元发送命令.综上所述,这些安全事件不仅会打乱人们正常的生活和生产秩序,还会造成公司商业资料的泄露和财产损失,严重的甚至会危及国家安全.

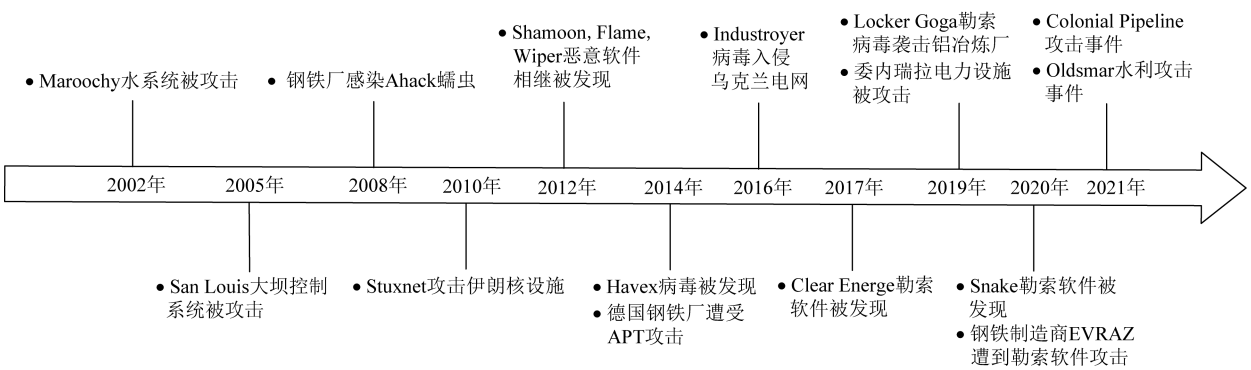


Fig. 1 Industrial control system cyber-attacks

图 1 工业控制系统安全事件

自 2019 年以来,全球范围内爆发新冠疫情,许多工作人员不得不在家办公,他们需要使用家庭计算机通过 VPN 连接到工业控制系统,因此增加了对工业控制系统连通性的需求.这加速了信息技术(information technology, IT)和操作技术(operation technology, OT)网络融合,促进了工业控制系统数字化转型.除此之外,在疫情中,原始设备制造商和系统集成商则受到了运输服务设备的限制,进入现场变得更加困难,因此也增加了对第三方安全远程访问的需求.通常,家庭网络比公司网络的安全标准

低,而且许多安全公司已经检测到这些家庭计算机被用来对工业控制系统网络执行不必要的扫描.根据 Kaspersky 统计[3],2021 年上半年期间,从工业控制系统的计算机设备上成功阻止了 5 150 种恶意软件.随着计算能力和存储能力的提高,网络攻击的复杂性将进一步增强,使用现代化的新技术和方法来检测和抵御攻击刻不容缓.

目前已有不少面向工业控制系统安全的综述研究.文献[4]分析了工业控制系统面临的典型威胁和攻击,讨论了尚未解决的安全问题及相应的工业控制系统安全解决方案,提供了未来的研究方向,但是没有对相关文献进行分析.文献[5]主要对工业控制系统中的安全解决方案进行了调研.文献[6]对工业控制系统漏洞报告进行了深入分析,衡量出工业控制系统的组件和安全策略受已知漏洞的影响.文献[7]分析了物联网和工业物联网都存在的安全挑战,以及工业物联网系统特有的安全挑战,并指出如何应对这些挑战.但是,工业控制系统攻击和防御技术迅速发展,有必要重新归纳和总结该领域近期的研究工作.

本文主要对近 3 年(2019-01—2021-10)Web of Science 核心数据库、EI 数据库、CCF 推荐网络与信息安全国际学术会议中发表的与工业控制系统安全相关论文,以及其他相关的高水平研究工作进行深入调研分析.图 2 展示了工业控制系统安全相关调研文献数量的逐年变化情况,可以看到,针对攻击的文献集中在 2018 年及以前,近 3 年的文献主要是防御方案,但也有新的攻击方法被提出.因此,基于这些新增加的文献,归纳和分析工业控制系统的研究现状与方向有着重要的现实意义.

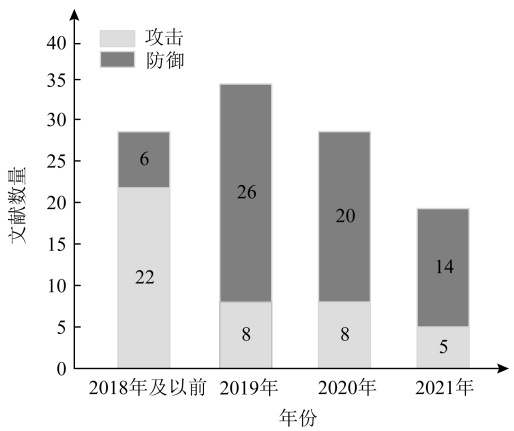


Fig. 2　Statistics of representative research on ICS security

图 2　工业控制系统安全代表性研究统计

本文根据工业控制系统的基本结构从攻击和防御 2 个角度,对近 3 年的工业控制系统安全研究工作进行了分析,主要贡献包括 3 个方面:

1) 介绍了工业控制系统基本的体系结构,依据工业控制系统的体系结构对各个组成部分面临的主要威胁展开全面讨论,剖析了威胁产生的原因及危害,展示了针对各种威胁现有的解决方案;

2) 深入分析了针对 ICS-云平台通信、HMI-设备通信和设备固件的具体攻击,并对不同攻击的检测、防御方案进行分类讨论,对类似的检测、防御方案进行了对比分析,展示了这些技术方案的效果;

3) 揭示了工业控制系统领域未来发展过程中将面临的挑战和机遇,并对工业控制系统安全未来的研究趋势进行展望.

## 1　工业控制系统体系结构及面临的威胁

本节首先介绍了工业控制系统的基本结构,然后从 ICS-云平台通行安全、HMI-设备通信安全和设备固件安全 3 个方向分析归纳了各结构部分面临的威胁.

### 1.1　工业控制系统体系结构

工业控制系统的体系结构如图 3 所示,主要包括服务器/云平台、人机交互界面(human machine interface, HMI)、主终端装置(master terminal unit, MTU)、远程终端单元(remote terminal unit, RTU)、现场设备 5 部分.工业控制系统工作的大致流程:现场设备将生产过程中的实时数据传递到 PLC,PLC 根据预先设定好的程序对数据进行处理,然后对设备进行控制或者将数据上传到 MTU;用户可以根据人机交互界面上实时显示的数据来监控设备的状况或对设备进行操作;服务器或者云端会对这些设备数据进行存储,便于工作人员对数据汇总和分析.

#### 1.1.1　服务器/云平台

工业控制系统服务器会通过软件程序实时收集来自众多传感器、执行器、远程终端单元和实时的控制信息等,例如 CPU 的温度、风扇的转速、门阀的位置等.除此之外,其还可以对数据进行汇总和分析,例如平均值、标准偏差等.大型企业需要服务器实时组合和分析设备产生的数据来下达命令,这些数据使用标准格式进行存储,并通过数据分析和可视化显示结果,进而比较生产的效率和性能.

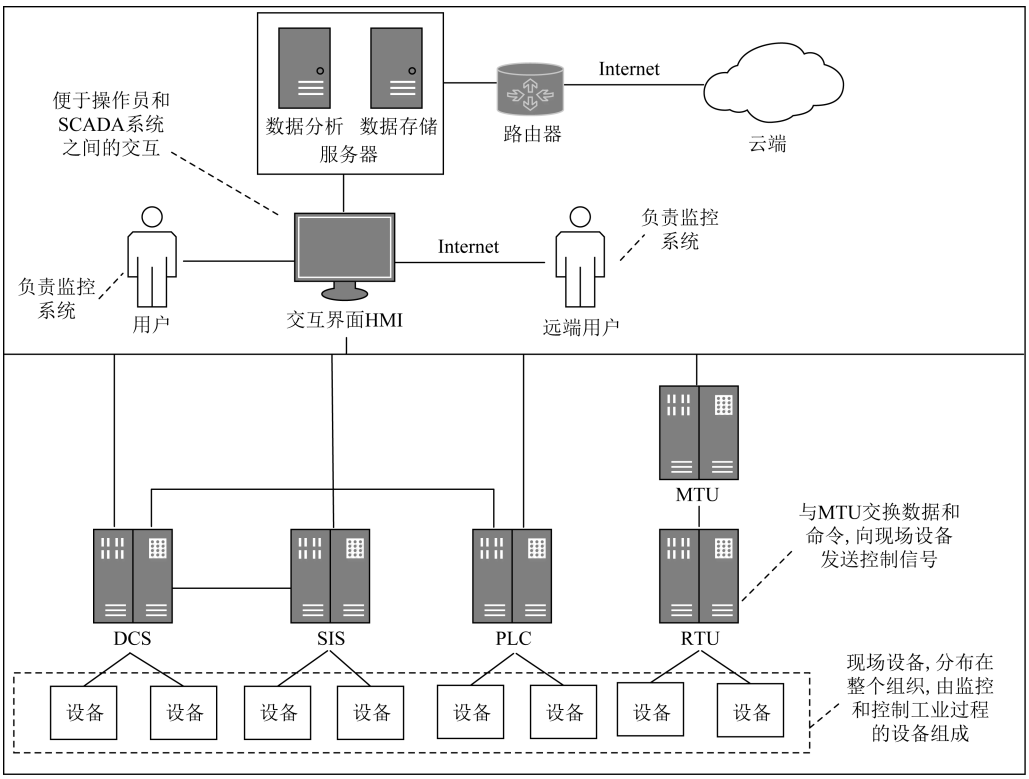


Fig. 3 The architecture of industrial control systems

图 3 工业控制系统基本架构

1.1.2 人机交互界面

工业控制系统通过人机交互界面对设备进行配置和操作,包括设备的运行、停止、更新、故障排除等.人机交互界面是通过网络与 MTU 连接的 1 台或多台计算机,可以在紧急或极端事件的情况下快速通知和错误报警.根据设备运行状况,展示设备的运行数据和状态.

1.1.3 主终端装置

MTU 负责从 RTU 收集数据并传输到 HMI 或服务器.MTU 和 RTU 之间是双向通信,MTU 和 RTU 之间的通信是由 MTU 发起的,可以通过控制人员操作触发,也可以设置周期性自动触发.

1.1.4 远程终端单元

RTU 是 PLC 技术的发展,既有 PLC 的传统功能,更有其独特的特点.RTU 和 PLC 通过现场总线或无线网络连接到传感器和执行器来收集实时信息,并操作和控制设备.

1.1.5 现场设备

现场设备是工业物联网系统中的数据来源,主要包括传感器和执行器.传感器用来收集设备状态的周期性数据,例如温度传感器、恒温器、压力传感器和 RFID 等;执行器主要用来执行控制命令.

## 1.2 工业控制系统面临的威胁

工业控制系统接入互联网后,攻击者可以利用已知的 IT 网络缺陷连接到控制台.工业控制系统对于安全防护的缺失(例如,对来自外部的控制进行适当身份验证),打开了工业控制系统的攻击面.工业控制系统既面临着传统 IT 的安全威胁,又面临着 OT 的安全威胁.本文只讨论工业控制系统中特有的 IT 和 OT 安全威胁.依据工业控制系统的体系结构,自上而下地将研究工作分为 ICS-云平台通信安全、HMI-设备通信安全、设备固件安全以及其他安全相关研究.

1.2.1 ICS-云平台通信安全

在传统的工业控制系统中,设备的控制和管理都是在本地进行的.近年来,工业控制系统逐渐从单片架构迁移到分布式云架构.云计算在工业自动化方向的市场潜力巨大.用户可以从云计算运营商租用硬件资源,例如服务器、存储、网络等,将软件放在这些资源上运行,通过网络获得应用软件所提供的信息与数据.用户只需投入少量的使用成本,即可得到与从前同功效、高质量的服务.因此,工业控制系统的数据逐步转变为云存储.但是,云平台的应用使工业控制系统的网络环境变得更加复杂(云平台

自身不安全,信息上下交互也不安全),工业控制系统和外部通信过程,除了要面临传统的 IT 威胁,还要面临新的安全威胁和漏洞,其中工业控制系统和云平台通信面临的安全威胁包括:云平台相关攻击、工业防火墙漏洞利用和端口扫描.

1.2.2　HMI-设备通信安全

在工业控制系统中,设备通过网络连接进行通信,进而协调整个生产制造过程.用户通过软件程序实时收集和存储工业控制系统中的运行数据,以便进一步的管理和分析.工业控制系统使用的通信协议在不同的行业、不同的地域或者不同的供应商之间差别很大,常用的工业通信协议包括 Modbus,Fieldbus 和 IEC 60870-5 等.工业通信协议设计时仅考虑运行在封闭的环境中,很少考虑到安全性,因此这些协议容易受到各种恶意攻击,如窃听、篡改和伪造等.PLC 是工业控制系统的核心部件,攻击者可以通过网络将恶意的逻辑代码注入到 PLC 的控制逻辑中来实现恶意攻击,例如病毒 Stuxnet 就是通过改变 PLC 的控制逻辑来实现攻击.除此之外,工业控制系统中存在着不同类型的传感器,攻击者可以利用电磁干扰来修改传感器读数.因此,人机交互界面和设备通信面临的安全威胁包括:PLC 控制逻辑注入攻击、ICS 专有通信协议攻击和传感器欺骗攻击.

1.2.3　设备固件安全

随着自动化和智能化技术的进步,工业控制系统之间的设备高度互连、相互依赖,越来越多的设备连接到工业控制系统.这些设备的微控制器芯片是由特定供应商提供,攻击者通过利用漏洞来劫持设备或恶意修改其固件对工业控制系统中的设备进行控制,尤其是 PLC 设备固件,它可根据系统输入来管理和控制现场设备,如果攻击者可以修改 PLC 设备固件,那么属于其权限范围内的任何物理系统组件都可以被完全控制.因此,设备固件安全威胁包括固件篡改和漏洞利用.

## 2　ICS-云平台通信安全

目前,大量基于云的技术被应用于工业控制系统,这给工业控制系统带来了新的安全威胁.本节将从攻击和防御 2 个角度对 ICS-云平台通信安全研究工作进行归纳和分析.

### 2.1　攻　击

2.1.1　针对云平台的攻击

工业控制系统的数据存储到云端,云平台利用虚拟技术实现多用户应用并发运行,用户对数据失去了控制,可能不会意识到详细的云平台安全策略、漏洞和恶意软件信息.文献[8]指出云平台面临不安全的 API 接口、内部攻击、数据泄露、服务劫持、账号盗用等安全问题.工业控制系统中关键数据的丢失和篡改都会给用户带来不可估量的损失,而这些问题都会使存储在其中的数据面临安全威胁.

**Table 1　Threats to Industrial Control Systems**

**表 1　工业控制系统面临的威胁**

| 分类 | 攻击 | 成因 | 危害 | 防御 |
|---|---|---|---|---|
| ICS-云平台通信安全 | 云平台相关攻击 | 安全策略不当,内部攻击 | 数据泄露,数据篡改 | 雾计算 |
| | | | | 区块链 |
| | 工业防火墙漏洞利用 | 程序漏洞,固件没有及时更新 | 程序崩溃,系统无法正常工作 | 安全测试 |
| | | | | 入侵检测 |
| | 端口扫描 | 攻击信息采集 | 漏洞利用 | 蜜罐 |
| | | | | 流量识别 |
| HMI-设备通信安全 | PLC 控制逻辑注入攻击 | 通过漏洞篡改逻辑控制程序 | PLC 无法正常工作 | 异常检测 |
| | | | | 远程认证 |
| | ICS 专有通信协议攻击 | 设计中没有考虑到安全性 | 窃听、篡改,中间人攻击 | 异常检测 |
| | | | | 协议模糊测试 |
| | 传感器欺骗攻击 | 传感器的通信信道安全性低 | 影响传感器的正常读数 | 欺骗攻击检测 |
| 设备固件安全 | 固件篡改或漏洞利用 | 程序编写不当或程序被篡改 | 设备不能正常运转,被攻击者控制 | 静态分析 |
| | | | | 保护固件更新过程 |
| | | | | 漏洞检测 |

2.1.2 工业防火墙安全

工业控制系统和云之间的网络连接可能会成为工业控制系统的后门,被攻击者利用[9].因此,互补的网络安全解决方案被引入到工业控制系统中,例如工业防火墙、工业网关.工业防火墙与传统的防火墙原理类似,通过监控和控制网络内部和网络之间的流量来抵御攻击.然而,工业控制系统的网络环境相对复杂,例如老化的工业设备、分布在多个地点的网络等.为了应对复杂的网络环境,工业防火墙增加了加密、VPN、深度包检测等功能.工业防火墙在工业控制系统的安全防护中扮演着重要的角色,但不能保证绝对的安全.2016 年,在施耐德电气的 ConneXium 防火墙产品中发现了一个缓冲区溢出漏洞,攻击者可以在 SNMP 的登录身份验证过程中执行代码[10].2019 年,美国电网遭到了与工业防火墙相关的攻击,攻击者利用防火墙固件中的一个漏洞强制防火墙在 10 h 的时间内持续重启,导致控制中心和受影响站点之间反复失去通信[11].

2.1.3 端口扫描攻击

Shodan 是一款网络扫描工具,能够很容易地识别面向互联网的工业控制设备并询问可用服务,发现现有服务的相关漏洞.文献[12]从攻击者的角度利用搜索引擎 Shodan、漏洞数据库等公共工具发现工业设备,查找常用设备的漏洞,并对设备和漏洞进行映射.文献[13]通过 Shodan 搜索网络上的 PLC 设备,分析并验证了部分 PLC 漏洞.SHINE 项目使用 Shodan API 和 700 多个专门设计的询问来识别易受攻击的面向互联网的工业控制系统设备.该项目收集了超过 1 000 000 个 IP 地址,这些 IP 地址属于 SCADA 和控制系统及其相关的设备[14].除此之外,文献[15]展示了一种新的威胁向量,攻击者可以利用 PLC 作为 SNMP 扫描器通往内部工业控制系统网络的网关.文献[16]提出了一种通过 HMI 进行单点渗透的方案,使用机器学习模型作为选择识别工业控制系统流程的分类器,利用控制理论在工业控制系统中设计了通用的基于扰动的攻击,攻击者可以在没有先验知识的情况下进行高精确度的端到端攻击.

## 2.2 防 御

2.2.1 雾计算

雾计算是一种水平的系统架构,将计算、存储、控制和网络功能分布到更接近用户的地方[17].雾计算可以被认为是云计算的扩展.雾计算定义的系统要符合安全性、可伸缩性、开放性、自主性、可靠性等.雾节点可以放置在本地,是实现雾计算服务的物理和逻辑网络元素.当数据量特别大时,雾节点也可以作为外部云存储之间的中间件,对存储在云中的数据进行加密/解密.对于边缘设备则不需要知道底层存储和安全机制[18].雾计算可以缓解传统云计算模型中由于数据传输造成的高延迟问题,同时也有益于保持隐私数据及安全敏感数据的机密性[19].

2.2.2 蜜罐

蜜罐已经被证明是收集真实数据的非常有价值的工具,例如恶意软件的有效载荷,可以帮助更好地理解攻击者使用的攻击方法和策略.本文对基于蜜罐的防御方法进行了归纳总结,如表 2 所示,常见的研究角度有收集攻击数据、识别攻击源、分析攻击影响、交互扩展性和伪装真实设备.文献[20]提出了 HoneyPLC,它是一个高交互、可扩展和恶意软件收集的蜜罐,支持广泛的 PLC 模型和供应商.该工具表现出了高水平的伪装:它被多种广泛使用的侦察工具识别为真实设备,包括 Nmap,Shodan,Siemens Step7 Manager 等.文献[21]开发了几十个蜜罐来收集与工业控制系统相关的攻击数据,分析了工业控制系统面临的主要攻击方法和攻击模式,识别出 7 个确定的攻击源.文献[22]设计了一个高交互的工业控制系统蜜罐网络,可以识别和分析针对工业控制系统设备的攻击.在一年多的时间里,作者收集

**Table 2 The Work Comparison of Honeypot Defense**

**表 2 基于蜜罐的防御部分工作对比**

| 已有工作 | 研究角度 | | | | |
|---|---|---|---|---|---|
| | 收集攻击数据 | 识别攻击源 | 分析攻击影响 | 交互扩展性 | 伪装真实设备 |
| 文献[20] | √ | √ | × | √ | √ |
| 文献[21] | √ | √ | √ | × | × |
| 文献[22] | √ | √ | √ | √ | × |
| 文献[23] | × | √ | √ | × | × |

注:“√”表示文献中完成了该工作,“×”表示文献中未完成该工作.

了 80 000 个蜜罐交互,并进行了详细分析,其中只有 9 个针对工业控制系统的恶意攻击.恶意攻击包括 DOS、重放攻击、操纵逻辑、协议攻击和缓冲区溢出攻击.文献[23]设计了一种基于功能代码和流量特征的分层 DFA-SVM 识别模型来识别 Shodan 扫描,并从扫描时间、扫描频率、扫描端口、区域偏好、工业控制系统协议偏好、工业控制系统协议功能比例等方面评估 Shodan 扫描对工业控制系统的影响.

2.2.3　工业防火墙安全检测

文献[24]对 2 个商用工业控制系统防火墙进行安全测试,测试范围覆盖了功能测试、异常测试和渗透测试.文献[25]提出了一种主机入侵检测体系结构,允许执行 IDS 的多种常见功能(例如集中式 Host IDS 配置和管理、日志收集、系统审计、事件触发或监控分析),同时还支持被动入侵检测(例如日志和警报生成).

2.2.4　区块链技术的应用

文献[26]利用区块链保证数据的完整性,采用高效的复制机制实现数据备份,使数据在遭受攻击后能够恢复.文献[27]提出了一个基于区块链的工业控制系统通信协议,以处理通信安全和系统设备存储约束问题.文献[28]提出了一种新的用于硬实时控制系统数据完整性验证的递归水印算法,该文作者利用水印密钥,将水印噪声应用于硬实时信号,并通过未加密的硬实时通道发送,通过加密的非实时通道将相同的密钥传输给接收方,因此使用相同的密钥,接收方可以检测数据是否被攻击者修改.文献[29]提出了基于区块链的工业控制系统数据保护框架,该框架应用多签名技术完成多方认证,实验表明其适用于实时协同的工业控制系统.

## 3　HMI-设备通信安全

人机交互界面和设备的通信过程中存在较多的安全隐患,本节从攻击和防御 2 个角度对 HMI-设备通信安全进行了分析.

### 3.1　攻　击

3.1.1　控制逻辑注入攻击

现有的控制逻辑攻击侧重于通过网络向目标 PLC 注入恶意控制逻辑,在工业控制系统中,PLC 通常用于直接与传感器和执行器交互,并执行局部自动控制.PLC 上运行 2 种软件:固件(即操作系统)和控制逻辑(类似于应用程序),PLC 基本架构如图 4 所示.在 PLC 固件上运行的逻辑通常可以通过网络或本地 USB 进行修改.控制逻辑注入攻击面临 2 个关键问题:1)攻击 PLC 控制逻辑的程序;2)从控制中心中隐藏攻击.

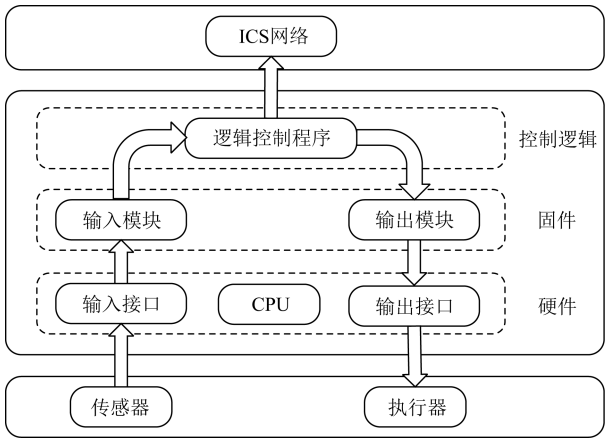


Fig. 4　PLC architecture

图 4　PLC 基本架构

文献[30]提出了一个工业控制系统勒索软件,它可以对文件和数据进行加密,修改 PLC 的逻辑控制.作者在 SIEMENS S7-300 PLC 上证明了攻击的可行性.文献[31]通过网络操纵传输到 PLC 的数据包,进而对控制逻辑进行修改,该文作者在 2 个不同厂商的 PLC 上实现了攻击,并证明这些攻击可以成功躲避入侵检测.文献[32]提出了梯形逻辑编写的恶意程序,通过持续改变行为或等待特定的触发信号来激活恶意程序,进而中断 PLC 的正常操作.文献[33]研究了 PLC 梯形逻辑代码或程序中存在的关键漏洞,并提出了相应的解决方案,以保证 PLC 的安全性.文献[34]提出了针对单个 PLC 的虚假数据注入攻击,攻击者通过分析目标 PLC 的 I/O 轨迹,以产生一组输入来控制 PLC 输出,只需要子系统的部分信息,就可以达到想要的恶意结果.文献[35]证明了 PLC 蠕虫的可行性,其中 PLC 是攻击的源头,可能会在 PLC 内部传播,不需要 PC 或服务器,因此不会被防病毒产品检测到.文献[36]分析了 XGB PLC 的内存和网络协议结构,并利用发现的漏洞发起重放攻击,在已有的存储结构的基础上,对 PLC 进行了内存调制攻击并造成了致命错误.文献[37]提出了一种针对 PLC 控制逻辑引擎的攻击,利用 PLC 固有的编程方式和启动/停止引擎的特点,通过网络攻击可以成功地使控制逻辑引擎失效.文献[38]提出了一种新的反编译工具,可以从网络捕获重构攻击代码.

3.1.2 ICS 专有通信协议攻击

工业控制系统专有协议用于工业软件和工业设备之间的通信,指定了消息到功能的映射关系.除了标准协议规定的功能外,许多工业制造商还对其产品的功能进行了扩展,超出了原协议规定的范围,同时这些操作很可能造成通信接口的暴露,在扩展功能实施的过程中没有很好地考虑安全问题.文献[39]通过对工业控制系统的重要组成部分 PLC 实施拒绝服务攻击、启动/停止攻击和中间人攻击来揭示攻击的结构.文献[40]通过操纵 HMI 和多个 PLC 之间的 Modbus 通信使人机界面显示一致的系统假视图,该攻击成功地欺骗了操作人员,并使系统处于停电状态.然而,文献[41]指出文献[40]中攻击者只是随机选择一些指令进行反向操作,并不能保证攻击目标的实现.因此,文献[41]设计了一种增强的、策略性的多级语义攻击,该攻击依赖系统状态转换规则来精确地决定要反转哪个控制指令,该方法可以在保持其隐蔽性的同时显著提高攻击成功率.文献[42]提出了启发式推理攻击,攻击者能够对来自 HMI 和 PLC 之间的网络请求和响应报文按照周期性发送顺序进行排序,再根据报文长度进行分类推断出 PLC 信号命令.

3.1.3 传感器欺骗攻击

基于声学、射频、激光和其他物理模式的模拟干扰会诱发故障,甚至控制传感器的输出.传感器输出的可用性和完整性受损,会给基于可靠传感器测量进行自动化决策的关键安全系统带来重大风险.文献[43]提出了一种传感器数据欺骗攻击,攻击者可以拦截传感器测量值,通过读取和修改通信信道中传感器读数,诱导系统达到不安全状态,从而对系统造成破坏.文献[44]在文献[43]的基础上提出了一种攻击方案,其放宽了攻击条件,允许更多类别的攻击策略.文献[45]提出了传感器数据欺骗隐形攻击,该攻击不会被操作人员发现.文献[46]提出并建立了离散事件系统的执行器攻击模型,证明了正态攻击者的存在性,并给出了其特征.文献[47]合成了 3 种传感器欺骗攻击,使用一个离散的结构来模拟监督者和环境的交互.文献[48]利用系统学习到的物理约束来操纵传感器读数的子集以躲避基于重构的异常探测器,从而隐藏攻击.文献[49]提出了第一个可证明的隐蔽通道,攻击者使用高质量/低噪声传感器和计算单元构造一个隐蔽传感器,隐蔽通信被编码在秘密传输传感器的输出噪声中,其分布与良性传感器(具有可比规格)难以区分.

### 3.2 防 御

3.2.1 基于协议分析的异常检测

文献[50]利用了工业控制系统特定应用程序操作的周期性,测量协议不同阶段执行中的偏差,以检测在工业控制系统体系结构中的各层次上的异常事件.文献[51]通过分析工业控制系统中网络数据包的结构,从中提取工业控制系统中协议的特征,并应用无监督学习神经网络方法进行工业控制系统异常检测.文献[52]提出了一种分析工业私有协议结构的方法,来提取控制设备的信息,实现对工业协议的有效网络流量监控.由于工业协议的多样性和缺乏统一的标准,使入侵检测技术适应大量不同的协议有很大的困难.文献[53]提出了将工业协议转换为抽象的协议消息,以实现基于不同工业协议的独立于协议的语义入侵检测.

3.2.2 基于机器学习算法的异常检测

目前主要的基于机器学习算法的异常监测工作如表 3 所示,具体描述如下.文献[54]利用卷积神经网络提出了特征处理算法,将传统 IT 网络的异常检测知识转移到工业控制系统网络中,能够充分挖掘

**Table 3 Comparison of Attack Detection Based on Machine Learning Algorithm**

**表 3 基于机器学习算法的异常检测工作对比**

| 已有工作 | 测试数据集 | 算法 | 精确度/% | 准确率/% | 召回率/% |
|---|---|---|---|---|---|
| 文献[54] | 沙箱模拟 | CNN | | 95.53 | 71.10 |
| 文献[55] | 天然气管道数据集 | LSTM | 90.68 | 90.42 | 90.68 |
| | | GRU | 91.70 | 91.77 | 91.70 |
| 文献[56] | SwaT 数据集 | CNN+ LSTM | 97.20 | | 77.30 |
| 文献[57] | WADI 数据集 | LSTM | | | 47.44 |
| | SwaT 数据集 | LSTM | | | 78.81 |
| 文献[58] | WADI 数据集 | DIF | 76.50 | | 57.40 |
| | SwaT 数据集 | DIF | 93.50 | | 83.50 |

流量数据的特征,并准确地识别异常行为.文献[55]提出利用递归神经网络对工业控制系统的网络流量进行建模和预测,并用于异常检测,以天然气管道数据集为例,对2种递归神经网络结构(LSTM和GRU)进行了测试.文献[56]提出了一种基于深度神经网络的集成电路异常检测框架,该框架使用扩张卷积和长短期记忆(LSTM)层来学习工业控制系统中传感器和驱动器数据的时间特征,在安全水处理试验台上得到了验证.文献[57]提出了一个异常检测框架,利用机器学习和数据挖掘技术,从工业控制系统操作数据日志中提取规则,进行异常检测.文献[58]提出了一种新型的半监督双隔离森林攻击检测系统,该系统由2个独立的隔离森林模型组成,分别使用归一化原始数据(执行器信号和传感器测量的正常数据)和主成分分析对数据进行预处理,通过分离异常来检测攻击.

3.2.3　基于软件定义网络的异常检测

文献[59]提出了基于云的入侵检测和防御系统,利用软件定义网络和网络功能虚拟化来检测任何恶意网络活动.文献[60]针对工业控制系统的通信需求设计了一个基于软件定义网络和网络功能虚拟化的通信基础设施,开发了一种针对双向工业控制系统流的攻击检测和定位算法,并设计了一种最佳干预策略,以满足工业应用的通信和安全需求.文献[61]在SDN控制器上执行深度包检测来识别恶意网络数据包.

3.2.4　基于流量和日志分析的异常检测

文献[62]提出了一种通过流量识别工业控制系统网络攻击的方法,该方法还可以通过流量分析评估恶意攻击的意图并提出了防御攻击的建议.文献[63]研究了影响工业系统的4种攻击类型:直接攻击、顺序攻击、时间攻击和超请求攻击,通过分析发送数据顺序,提出了基于滤波器的攻击检测方法,并且具有良好的检测结果.文献[64]提出了一种基于行为模型的异常检测方法,该方法从工业控制网络流量中提取行为数据序列,建立控制器和工业控制系统受控过程的正常行为模型,并比较测试行为数据和预测行为数据,以检测异常.文献[65]提出了一种用于工业PLC的时序指纹识别技术,通过对PLC的输入/输出作为请求/响应消息的函数进行建模,从而对扫描周期和控制逻辑之间的关系进行建模来检测重放攻击.文献[66]提出了一种新的方法对IEC-60870-5-104网络中自发事件的时序特性进行建模,并利用该模型进行异常检测.文献[67]中基于自回归综合移动平均的流量预测模型可以对工业控制系统网络的短期流量进行预测,并根据流量模式的异常变化准确检测渗透攻击.此外,该异常检测模型采用单类支持向量机,能够通过分析以太网/IP数据包中的关键字段来检测恶意控制指令.文献[68]提出了一种主机异常检测系统,通过该系统可以实施过滤策略,以保护网络主机.

文献[69]提出了一种基于自编码器的新方法,用于检测工业控制系统运行中的异常情况,并且训练了几个基于具有不同架构的自动编码器的神经网络,并评估了它们中的每一个在检测过程控制系统工作中的异常问题中的有效性.文献[70]提出了一种基于时域和频域分析的数据驱动入侵检测方法,利用了闭环控制所需的传感器测量,不消耗额外的系统资源,也不依赖系统模型,同时提取时域和频域特征,利用工业控制系统正常运行条件下的特征向量建立隐式马尔可夫模型用于实时入侵检测.文献[71]以系统的监控控制和数据采集日志作为输入,利用数据驱动结构学习将系统的控制不变量抽象为控制图,然后监控图边缘的权值以检测异常.文献[72]提出了一种基于复合自编码器模型的学习正态模式的异常检测方法,与一般的自编码器神经网络对数据进行预测和重构不同,该模型对输入数据同时进行预测和重构,克服了单独使用每一个数据的缺点,此外,利用模型得到的误差,提出一个变化率来定位最可能受到攻击的设备.

3.2.5　传感器欺骗攻击检测

文献[73]提出了检测传感器欺骗攻击的检测模型,传感器系统通过关闭传感器来监测传感器输出中的攻击信号,一旦微控制器检测到攻击信号的存在,微控制器就拒绝进一步处理传感器输出.与其他检测方法相比,该方法不仅成本低、节省空间,而且部署速度快.文献[74]采用概率有限状态自动机进行系统建模,根据成功达到不安全状态的可能性,从概率的角度量化攻击策略.文献[75]提出了一种全分布式自适应控制策略,并获得了渐近输出一致性.文献[76]提出了一种混淆方法,使控制器对执行器使能攻击具有弹性,从而保持原有闭环系统的行为.

3.2.6　工业控制系统协议模糊测试

工业控制系统协议模糊测试可以有效地检测协议的漏洞,表4对相关的研究工作进行了比较.文献[77]介绍了一种基于差异感知的工业控制系统协议模糊种子选择方法DSS.DSS比较工业控制系统消息以确定它们是否触发相同的执行路径,从而选择

包含少量种子但获得高边缘覆盖率的高质量种子集.文献[78]在目前应用最广泛的协议模糊测试工具 Peach 的基础上构建了 Peach*,并在 Modbus 和 DNP3 等多个工业控制系统协议上进行了实验.结果表明,与原 Peach 相比,Peach* 的速度更快,发现的路径更多.文献[79]提出了一个函数代码感知的模糊框架 Polar,该框架通过实现新的语义感知突变和选择策略对模糊过程进行优化.与 AFL 和 AFLFast 相比,Polar 以 1.5～12 倍的速度实现相同的代码覆盖率和错误检测数量,在 24 h 内发现的路径数量增加了 0～91%.文献[80]提出了一个模糊系统 ICPFuzze,该系统使用长短期记忆网络学习协议的特征并自动生成突变测试数据,还利用测试的响应,调整权重策略,以发现更多导致异常连接状态的数据.通过与开源和商用模糊测试工具的比较,验证了该方法的有效性.

**Table 4 Comparison of Fuzzing ICS Communication Protocols**

**表 4 ICS 通信协议模糊测试工作比较**

| 已有工作 | 优化策略 | 测试协议 | 效果 |
|---|---|---|---|
| 文献[77] | 种子选择 | Modbus, S7comm | 使用较少的种子,可以达到相同的覆盖率 |
| 文献[78] | 代码覆盖率 | Modbus, DNP3 | 速度提高 1.2～25 倍,覆盖率增加 8.35%～36.84% |
| 文献[79] | 种子突变 | Modbus, IEC104, IEC61850 | 速度提高 1.5～12 倍,覆盖率增加 0～91% |
| 文献[80] | 种子突变 | Modbus, DLMS | 在短时间内发现更多崩溃 |

#### 3.2.7 远程认证技术

文献[81]提出了一种将混合远程认证技术与基于物理的模型相结合的方法,以保持工业控制系统的控制行为完整性,并评估了它对针对安全水处理设施的各种攻击的有效性.文献[82]提出了一种用于工业控制系统控制过程的新型远程认证方案,它将基于软件的认证与物理行为关联.该方案能够检测到在训练阶段未见过的攻击,并通过计算控制过程验证产生的加密哈希距离来测量异常.文献[83]提出、实现并评估了一种委托认证协议,它是第一种用于缺乏对远程认证硬件支持的商品设备的安全远程认证技术,以实现对可能受到损害的远程嵌入式设备的软件状态进行安全远程验证.

## 4 设备固件安全

在 3.1.1 节中描述的控制逻辑注入攻击的主要目标是工业控制系统中的控制软件及其通信过程,而不是直接修改底层设备固件.本节重点介绍了通过修改设备固件来执行远程触发攻击以及针对此类攻击的缓解方案.

### 4.1 攻 击

攻击者通过发现易受攻击的程序内存,进而劫持程序的执行流程.哈佛结构的 CPU 广泛应用于工业物联网设备,文献[84]利用程序漏洞永久地将任何代码片段注入到哈佛结构的 CPU 程序内存中.文献[85]研究了 PLC 固件漏洞,提出了一种通用的固件分析和远程代码注入攻击方法,并进行实验来演示如何更新和上传固件.文献[86]通过远程修改目标 PLC 中运行的控制逻辑以自动中断物理进程,还采用了一种新的虚拟 PLC 方法,通过将工程软件与捕获的原始控制逻辑的网络流量结合起来,隐藏恶意修改操作.文献[87]提出了一种对 PLC 的攻击,进而实现了对电网控制系统的物理感知隐身攻击.该程序可以在 PLC 的输出模块将控制命令发送到物理设备执行器之前修改控制命令,以最大限度地破坏物理电源设备,导致设备大规模故障.文献[88]展示了攻击者如何利用嵌入式设备引脚控制设备操作和相关的硬件中断,篡改嵌入式系统 I/O 的完整性和可用性.文献[89]介绍了针对智能电网的固件修改攻击,通过修改中继上运行的固件,进而利用中继的设计缺陷使设备级联断电.在文献[90]中,作者演示了如何使用常用的工具将固件加载到 2 个不同的现场设备的以太网卡,并指出攻击者可以编写自己的恶意固件,然后恶意固件加载到现场设备以太网卡,进而可以对被控制的进程、其他现场设备和控制系统网络上的其他系统发起攻击.

### 4.2 防 御

本文对设备固件安全相关的研究工作进行了归纳和整理,具体如表 5 所示.

#### 4.2.1 静态分析

文献[91]将 3.2 万份固件图像分解成 170 万个独立文件,然后对其进行静态分析,在超过 693 个固件映像中发现了 38 个以前未知的漏洞.文献[92]介绍

了工业物联网领域的静态程序分析工具,并对 PLC 程序进行了安全测试.文献[93]开发了模块化的工业控制程序逆向工程框架,用于工业控制系统二进制程序逆向分析.文献[94]提出了一种 PLC 固件分析技术,将可疑的固件与原始固件进行静态分析,检测代码差异,例如删除、添加和修改函数等.文献[95]提出了一种基于程序分析和时间上下文的自动安全审查方法,通过执行静态程序分析创建定时事件因果关系图,分析 PLC 代码和事件之间的因果关系,生成事件序列,可用于自动检测隐藏的安全违规.

**Table 5　Summary of Device Firmware Security**

**表 5　设备固件安全研究工作汇总**

| 防御方法 | 已有工作 | 研究内容 |
|---|---|---|
| 静态分析 | 文献[91] | 对固件图像分解成独立文件进行静态分析发现漏洞 |
| | 文献[92] | 对工业控制系统静态程序分析工具进行了介绍 |
| | 文献[93] | 对工业控制系统二进制程序进行逆向分析 |
| | 文献[94] | 对 PLC 固件进行静态分析,检测代码差异 |
| | 文献[95] | 基于程序分析和时间上下文的自动安全审查方法 |
| 固件安全更新 | 文献[96] | 通过提取传输的固件信息来识别和组织篡改固件 |
| | 文献[97] | 通过模糊测试来评估 PLC 二进制文件和控制器交互的安全性 |
| | 文献[98] | 利用固件的物理特性和加密模块进行身份验证 |
| | 文献[99] | 监控固件更新命令和捕获固件进行验证 |
| | 文献[100] | 基于硬件原语和加密模块实现嵌入式系统固件安全更新 |
| 其他 | 文献[101] | 通过测量固件执行中的低级硬件事件来检测固件恶意篡改 |
| | 文献[102] | 在 PLC 固件使用行为监控检测恶意负载异常 |
| | 文献[103] | 分析已知漏洞补丁包来检测未知漏洞 |

#### 4.2.2　固件安全更新

文献[96]提出了一个确保固件更新的完整性和真实性的工具,该工具能够成功提取正在传输的固件信息,及时识别和阻止被篡改的固件.文献[97]开发了一个工业控制系统模糊测试框架,用于评估 PLC 二进制文件和控制器交互的安全性.文献[98]利用设备固有的物理特性和集成的加密模块对固件包进行身份验证,以确保固件的保密性和完整性.文献[99]提出了一个确保 PLC 固件更新完整性的方案,通过监控固件更新命令,进而捕获固件,在固件传递给 PLC 之前进行验证.文献[100]提出了一个嵌入式系统固件安全更新的框架.该框架基于硬件原语和加密模块,可以部署在通信通道不安全的环境中.

#### 4.2.3　其他方法

文献[101]通过测量固件执行过程中发生的低级硬件事件的数量来检测嵌入式控制系统固件中的恶意修改.文献[102]提出对合法的 PLC 有效负载程序的运行行为进行建模,并在 PLC 固件中使用运行行为监控来检测有效负载攻击,并通过监控 I/O 访问模式、网络访问模式以及负载程序的时序特征,检测恶意 PLC 负载的异常行为.文献[103]提出了 VulHunter,即在分析已知漏洞补丁包的基础上发现未知漏洞,设计并实现了二进制比较、包提取和背景语义求解等算法.文献[104]提出了一个分布式工业控制系统的控制行为完整性解决方案,该方案可以精确地模拟所有 PLC 的状态,通过监控整个 ICS 的输入和输出行为,检测出 PLC 行为中的不一致性.

## 5　其他研究

### 5.1　高级持续威胁的防护

高级持续威胁是一种针对特定组织的复杂攻击类型,攻击者拥有丰富的经验和资源,可以在长时间不被发现的情况下渗透到受害者网络[105].文献[106]提出一种基于意见动力学的新技术,该技术允许跟踪攻击的所有阶段,通过关联不同的异常测量随时间的变化,从而估计威胁的持久性和资源的临界值.由此产生的信息对于监测控制系统的整体健康状况和部署相应的响应程序至关重要.文献[107]建立了传播模型来探索 PLC-PC 蠕虫在 PLC-PC 耦合网络中的传播行为,并提出了抑制 PLC-PC 蠕虫传播和降低工业控制系统网络安全威胁的建议.

### 5.2 对抗样本攻击

基于机器学习的入侵检测系统的普及和应用使得工业控制系统的网络攻击检测更加灵活和高效.然而,也引入了一个额外的攻击向量——对抗样本攻击.目前关于对抗机器学习的研究主要集中在互联网领域,它给 CPS 应用带来的风险还没有得到很好的研究.文献[108]利用生成对抗网络和工业控制系统的攻击数据自动生产攻击.文献[109]研究了应用于 CPS 的机器学习的潜在漏洞,提出了约束对抗机器学习算法,该算法可以有效地生成对抗性的样本,即使在实际约束下也会显著降低机器学习模型的性能.文献[110]通过使用基于雅可比矩阵的显著映射攻击生成对抗样本,同时探索分类行为,探讨了对抗学习如何用于目标监督模型.

### 5.3 工业控制系统实验台

在实际操作现场开发或验证安全技术是相当困难的,为了保证工业控制系统的安全性,需要创建与实际环境相似的实验环境.数学模型能够准确量化维持特定工业控制系统的系统动态和控制回路稳定性所需的开销.文献[111]设计了基于实际工业控制系统的实验测试平台,提出了用数学模型来评估工业控制系统中安全解决方案的效率和弹性,并对所提出模型的有效性进行了评估.文献[112-113]针对各种攻击场景的工业控制系统数据集进行了比较分析,并讨论了将数据集应用于工业控制系统安全研究的注意事项,建立了用于实验环境的工业控制系统试验台,为应用机器学习和人工智能算法的 IDS 系统提供数据集.文献[114]设计了一个配电自动化实验平台,并利用该平台发现多个 SCADA 基础设施漏洞.

### 5.4 软件定义网络安全

软件定义网络(software defined network, SDN)允许软件对网络流进行实时控制.在工业控制系统中,SDN 可以提供负载均衡、防火墙、流量监控等常规路由之外的特定功能.现在越来越多的研究中使用了 SDN.文献[115]对现有的 SDN 攻击进行了整理,通过 SDN 测试台来评估这些攻击的严重性.文献[116]研究了工业控制系统环境中 SDN 的攻击.网络控制的集中化使工业控制系统成为主要的攻击目标,可能导致系统内出现单点故障,控制 SDN 控制器的攻击者几乎获得对网络的完全控制,作者描述并演示了一些简单但高效的攻击.

## 6 工业物联网安全的挑战与机遇

本节基于第 5 节中对安全威胁以及相应的防御方案的分析,提出当前研究面临的挑战和机遇.图 5 中展示了挑战和机遇的对应关系.

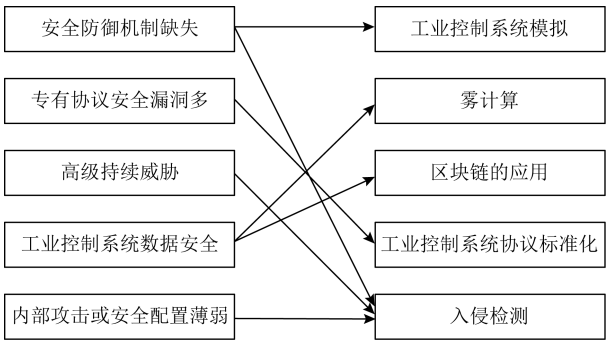


Fig. 5 Challenges and opportunities

图 5 挑战与机遇

### 6.1 目前面临的主要挑战

#### 6.1.1 安全防御机制缺失

由于早期设计过程中工业控制系统与互联网隔离,因此安全机制没有被详细地考虑,同时工业设备的硬件无法轻易地被替换,导致现有的部分设备没有通信加密和认证方案.文献[117]调研了美国工业控制系统网络应急响应小组发布的关于 277 家供应商工业控制系统设备的 988 份漏洞报告,发现最常见的漏洞与“输入验证不当”有关,其次是“网页生成过程中输入中和不当”和“认证不当”.除此之外,工业控制系统的生命周期比标准计算机系统长,随着攻击技术不断进化,势必将对工业控制系统安全造成严重的威胁.

#### 6.1.2 工业控制系统专有协议安全漏洞较多

文献[118]指出目前仍有大部分设备使用 Modbus TCP, EtherNetIP, Profinet 和 DNP3 协议,在网络上很容易扫描到这些设备.由于协议存在认证缺失、权限管理缺失、加密缺失等安全问题,设备很容易被攻击者控制.文献[119]总结了针对工业通信协议“Modbus 协议”的安全攻击,包括拦截、中断、修改、伪造.除此之外,在工业控制系统中,部分工业控制系统协议通常是设备专有的,是由供应商或利益相关方保密的,确切的协议规范是不开放的.这给安全人员分析协议的安全性带来了一定的困难.

#### 6.1.3 高级持续威胁

目前工业控制系统面临许多安全威胁,其中危害最大的是 APT 攻击[120],并且针对工业控制系统

的大型攻击都属于 APT 攻击,例如 Stuxnet,Flame 和 Havex.APT 攻击的参与者往往是组织良好的且可能是由政府资助的黑客和专业人士,他们有能力开发和维护专门为自己的目的而设计的恶意软件,并能解读窃取到的数据.通常 APT 的攻击方式较复杂,攻击范围相对于其他普通的攻击方式来说较窄,但是能在更长的时间内保持不被发现,因此使得 APT 攻击更难检测和防御.目前,工业控制系统的安全防御措施并不能有效地抵御 APT 攻击,在未来的研究工作中可以结合工业控制系统的特点,制定有针对性的防御方案.

#### 6.1.4　工业控制系统数据安全

数据是第 4 次工业革命的核心,数字化、自动化、智能化的背后都依赖数据的分析和处理.由于连接的工业设备种类和数量的增加,工业控制系统产生并需要处理的数据在快速增长.工业 4.0 中最大的问题之一就是如何在不影响系统完整性、不泄露数据隐私和不增加成本的情况下管理大量冗余数据.工业控制系统数据安全主要包括数据存储安全、数据访问安全和数据传输安全.如果任何环节出现问题,都会给公司带来巨大的损失,例如,未经授权的访问或者越权访问敏感数据,就会导致数据泄露给公司带来严重影响.

#### 6.1.5　内部攻击或安全配置管理环节薄弱

内部攻击是指组织内部人员使用工具对工业控制系统发起一系列违规的操作.内部人员对工业控制系统有一定的权限,因此内部攻击的危害远大于外部攻击.工作人员的安全意识薄弱,会导致工业防火墙配置不当、使用设备出厂时统一的安全口令或者密码强度较弱、没有及时更新固件或未打补丁的固件等,这些都会给工业控制系统带来严重的安全威胁.

### 6.2　未来研究机遇

#### 6.2.1　工业控制系统模拟

对于大多数研究机构来说,为网络安全研究构建工业控制系统的成本太高,难以实现.然而,模拟方法允许研究人员轻松部署工业控制系统,以分析它对攻击的反应.文献[121]讨论了使用 Node-RED(一种开源软件)来模拟工业控制系统的环境,以处理可编程逻辑控制器的任务,并更新和管理 Modbus TCP/IP 服务器.文献[122]提出了工业控制系统网络靶场的开发,该靶场基于实时攻防游戏模型,结合典型工业系统的动态仿真模型.当系统的单个部件因故障或其他原因而无法运行时,由于替换组件与初始组件不同,需要一个完整的工作周期来验证可替换组件的可用性.将数字双胞胎包含在对象及其控制系统的生命周期中,可以有效地解决在这种情况下系统修改(单个组件更换)的问题.数字双胞胎是一个更便宜的模拟系统,可以用于测试.由于某些属性允许对多个副本进行并行测试,并在某些限制内影响模型时间,因此它提供了更高质量的测试.数字双胞胎是工业控制系统的虚拟实体,它为安全研究提供了新的平台,例如模拟和复制系统行为[123].文献[124]提出了一种基于数字双胞胎的入侵检测算法实现方案,通过数字双胞胎可以精确地反映物理系统的内部行为.该算法放置在数字双胞胎中能够及时检测攻击,对不同类型的攻击进行分类,而不会对实际系统造成负面影响.

#### 6.2.2　雾计算

雾计算除了能够实现工业控制系统到云端的数据安全存储外,还能实现流量监控和分析.文献[125]提出了一种基于雾计算的分布式 DDoS 防御方案,该方案将流量分析工作负载灵活分配到多个分布式位置并根据需要分配虚拟化的网络计算功能.雾节点由于不受计算资源的严格限制,并且响应时间短,因此能够对本地的安全事件及时响应,更好地维护工业控制系统的安全.

#### 6.2.3　区块链的应用

区块链被广泛应用于金融领域,例如比特币、以太坊.区块链能够有效地记录分布式点对点网络上 2 个或多个参与方之间的交易,存储的数据由网络中的所有成员共同拥有,并且永久不可修改[126].区块链为多个实体进行数据交互提供了一个可信和安全的平台,可以用于工业控制系统中数据的收集和存储,例如智能能源[127].除此之外,区块链还可以用于工业控制系统中的安全通信[128]、设备管理[129]、异常检测[130].在过去的几年中出现了许多区块链项目,但目前区块链的研究还处于起步阶段,它还面临可扩展性、能源和成本效率、资源约束等挑战.

#### 6.2.4　工业控制系统协议标准化

目前工业控制系统中使用的通信协议存在较多的安全隐患,研究人员除了对当前使用的协议进行安全测试来修复漏洞,还可以根据需求设计安全的通用协议来解决当前面临的困境.国家相关的部门也可以出台相应的政策对工业控制系统通信协议进行标准化.

6.2.5 入侵检测

虽然现在已经有多种入侵检测方案被提出,例如基于协议分析的检测方案、基于流量和数据分析的检测方案等,但是随着计算能力和攻击技术的进步,新型攻击会不断出现,例如针对机器学习算法的毒化攻击[131].因此要实时关注攻击者的动向,更新入侵检测技术,才能更好地抵御攻击者的进攻.

## 7 总 结

由于工业控制系统的开放性、复杂性和多样性,所以在其发展过程中不可避免地面临各种各样的安全威胁,针对各类安全威胁的有效防御是保障工业控制系统安全的重要方式和手段.本文调研了近3年工业控制系统安全研究中的代表性工作,依据工业控制系统的体系结构,从攻击和防御的角度分别阐述其中的主要类型,并以此为基础分析了当前工业控制系统领域面临的挑战.工业控制系统的模拟、雾计算、区块链的应用以及工业控制系统协议的标准化的进步给未来研究带来了机遇.随着"工业4.0"的不断推进,相应的安全研究也必将不断深入,为工业控制系统的发展提供保障.

**作者贡献声明**:杨婷设计论文整体调研方案及论文撰写;张嘉元负责论文部分撰写及画图;黄在起、陈禹劼、黄成龙负责论文素材整理及论文部分撰写;周威、刘鹏、冯涛负责最终论文的审核及修订;张玉清提出论文整体研究思路,及最终论文的审核与修订.

## 参 考 文 献

[1] Lasi H, Fettke P, Kemper H G, et al. Industry 4.0 [J]. Business & Information Systems Engineering, 2014, 6(4): 239-242

[2] Zhou Ji. Intelligent manufacturing-main direction of "Made in China 2025"[J]. China Mechanical Engineering, 2015, 26(17): 2273-2284 (in Chinese)
(周济. 智能制造——"中国制造2025"的主攻方向[J]. 中国机械工程, 2015, 26(17): 2273-2284)

[3] Kaspersky ICS CERT. Threat landscape for industrial automation systems [EB/OL]. [2021-11-13]. https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-statistics-for-H1-2021-En.pdf

[4] Panchal A C, Khadse V M, Mahalle P N. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures [C] //Proc of 2018 IEEE Global Conf on Wireless Computing and Networking (GCWCN). Piscataway, NJ: IEEE, 2018: 124-130

[5] Asghar M R, Hu Q, Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges [J]. Computer Networks, 2019, 165: 106946

[6] Thomas R J, Gardiner J, Chothia T, et al. Catch me if you can: An in-depth study of CVE discovery time and inconsistencies for managing risks in critical infrastructures [C] //Proc of the 2020 Joint Workshop on CPS&IoT Security and Privacy. New York: ACM, 2020: 49-60

[7] Yu Xingjie, Guo Huaqun. A survey on IIoT security [C] //Proc of 2019 IEEE VTS Asia Pacific Wireless Communications Symp (APWCS). Piscataway, NJ: IEEE, 2019: 1-5

[8] Singh A, Chatterjee K. Cloud security issues and challenges: A survey [J]. Journal of Network and Computer Applications, 2017, 79: 88-115

[9] Sajid 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

[10] Schneider Electric. Security Notification-ConneXium [EB/OL]. [2021-11-13]. https://www.se.com/uk/en/download/document/SEVD-2016-035-01/

[11] Western Electric Coordinating Council. Lesson learned: Risks posed by firewall firmware vulnerabilities [EB/OL]. [2021-11-13]. https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf

[12] Anton S D D, Fraunholz D, Krohmer D, et al. The global state of security in industrial control systems: An empirical analysis of vulnerabilities around the world [J]. IEEE Internet of Things Journal, 2021, 24(8): 7525-17540

[13] Lee T, Kim S, Kim K. A research on the vulnerabilities of PLC using search engine [C] //Proc of 2019 Int Conf on Information and Communication Technology Convergence (ICTC). Piscataway, NJ: IEEE, 2019: 184-188

[14] Byres E. Project shine: 1,000,000Internet-connected scada and ICS systems and counting [EB/OL]. [2021-11-13]. https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting

[15] Klick J, Lau S, Marzin D, et al. Internet-facing PLCs as a network backdoor [C] //Proc of 2015 IEEE Conf on Communications and Network Security (CNS). Piscataway, NJ: IEEE, 2015: 524-532

[16] Sarkar E, Benkraouda H, Maniatakos M. I came, I saw, I hacked: Automated generation of process-independent attacks for industrial control systems [C] //Proc of the 15th ACM Asia Conf on Computer and Communications Security. New York: ACM, 2020: 744-758

[17] OpenFog Consortium. IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing [S]. Piscataway, NJ: IEEE, 2018: 1-176

[18] Atieh A, Nanda P, Mohanty M. Context-Aware fog computing implementation for industrial Internet of things [C] //Proc of 2021 Int Wireless Communications and Mobile Computing (IWCMC). Piscataway, NJ: IEEE, 2021: 598-603

[19] Ning Zhenyu, Zhang Fengwei, Shi Weisong. A study of using TEE on edge computing [J]. Journal of Computer Research and Development, 2019, 56(7): 1441-1453 (in Chinese)
(宁振宇, 张锋巍, 施巍松. 基于边缘计算的可信执行环境研究[J]. 计算机研究与发展, 2019, 56(7): 1441-1453)

[20] López-Morales E, Rubio-Medrano C, Doupé A, et al. HoneyPLC: A next-generation honeypot for industrial control systems [C] //Proc of the 2020 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2020: 279-291

[21] Li Ke, You Jianzhou, Wen Hui, et al. Collaborative intelligence analysis for industrial control systems threat profiling [C] //Proc of the Future Technologies Conf. Switzerland: Springer, Cham, 2018: 94-106

[22] Dodson M, Beresford A R, Vingaard M. Using global honeypot networks to detect targeted ICS attacks [C] //Proc of 2020 12th Int Conf on Cyber Conflict (CyCon). Piscataway, NJ: IEEE, 2020, 1300: 275-291

[23] Chen Yongle, Lian Xiaowei, Yu Dan, et al. Exploringshodan from the perspective of industrial control systems [J]. IEEE Access, 2020, 8: 75359-75369

[24] Nguyen T D, Austin S C, Irvine C E. Astrategy for security testing industrial firewalls [C] //Proc of the 5th Annual Industrial Control System Security (ICSS) Workshop. New York: ACM, 2019: 38-47

[25] Martinez C V, Vogel-Heuser B. A host intrusion detection system architecture for embedded industrial devices [J]. Journal of the Franklin Institute, 2021, 358(1): 210-236

[26] Maw A, Adepu S, Mathur A. ICS-BlockOpS: Blockchain for operational data security in industrial control system [J]. Pervasive and Mobile Computing, 2019, 59: 101048

[27] Brandão R. A blockchain-based protocol for message exchange in a ICS network: Student research abstract [C] //Proc of the 35th Annual ACM Symp on Applied Computing. New York: ACM, 2020: 357-360

[28] Song Z, Skuric A, Ji K. A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement [J]. IEEE Transactions on Automation Science and Engineering, 2020, 17(2): 1030-1043

[29] Rahman Z, Khalil I, Yi Xun, et al. Blockchain-based security framework for a critical industry 4.0 cyber-physical system [J]. IEEE Communications Magazine, 2021, 59(5): 128-134

[30] Zhang Yipeng, Sun Zhonghao, Yang Liqun, et al. A11 your PLCs belong to me: ICS ransomware is realistic [C] //Proc of 2020 IEEE 19th Int Conf on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway, NJ: IEEE, 2020: 502-509

[31] Yoo H, Ahmed I. Control logic injection attacks on industrial control systems [C] //Proc of IFIP Int Conf on ICT Systems Security and Privacy Protection. Switzerland: Springer, Cham, 2019: 33-48

[32] Govil N, Agrawal A, Tippenhauer N O. On ladder logic bombs in industrial control systems [M] //Computer Security. Switzerland: Springer, Cham, 2017: 110-126

[33] Serhane A, Raad M, Raad R, et al. PLC code-level vulnerabilities [C] //Proc of 2018 Int Conf on Computer and Applications (ICCA). Piscataway, NJ: IEEE, 2018: 348-352

[34] McLaughlin S, Zonouz S. Controller-aware false data injection against programmable logic controllers [C] //Proc of 2014 IEEE Int Conf on Smart Grid Communications (SmartGridComm). Piscataway, NJ: IEEE, 2014: 848-853

[35] Spenneberg R, Brüggemann M, Schwartke H. PLC-blaster: A worm living solely in the PLC [J]. Black Hat Asia, 2016, 16: 1-16

[36] Lee J C, Choi H P, Kim J H, et al. Identifying and verifying vulnerabilities through PLC network protocol and memory structure analysis [J]. CMC-Comput Mat Contin, 2020, 65(1): 53-67

[37] Qasim S A, Ayub A, Johnson J, et al. Attacking the IEC 61131 logic engine in programmable logic controllers [C] //Proc of Int Conf on Critical Infrastructure Protection. Switzerland: Springer, Cham, 2021: 73-95

[38] Senthivel S, Dhungana S, Yoo H, et al. Denial of engineering operations attacks in industrial control systems [C] //Proc of the 8th ACM Conf on Data and Application Security and Privacy. New York: ACM, 2018: 319-329

[39] Yılmaz E N, Sayan H H, Üstünsoy F, et al. ICS cyber attack analysis and a new diagnosis approach [C] //Proc of the Int Conf on Artificial Intelligence and Applied Mathematics in Engineering. Switzerland: Springer, Cham, 2019: 127-141

[40] Kleinmann A, Amichay O, Wool A, et al. Stealthy deception attacks against SCADA systems [M] //Computer Security. Switzerland: Springer, Cham, 2017: 93-109

[41] Hu Yan, Sun Yuyan, Wang Youcheng, et al. An enhanced multi-stage semantic attack against industrial control systems [J]. IEEE Access, 2019, 7: 156871-156882

[42] Choi T, Bai G, Ko R K L, et al. Ananalytics framework for heuristic inference attacks against industrial control systems [C] //Proc of 2020 IEEE 19th Int Conf on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway, NJ: IEEE, 2020: 827-835

[43] Su Rong. Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations [J]. Automatica, 2018, 94: 35-44

[44] Góes R M, Kang E, Kwong R, et al. Stealthy deception attacks for cyber-physical systems [C] //Proc of 2017 IEEE 56th Annual Conf on Decision and Control (CDC). Piscataway, NJ: IEEE, 2017: 4224-4230

[45] Zhang Qi, Li Zhiwu, Seatzu C, et al. Stealthy attacks for partially-observed discrete event systems [C] //Proc of 2018 IEEE 23rd Int Conf Emerging Technologies and Factory Automation (ETFA). Piscataway, NJ: IEEE, 2018: 1161-1164

[46] Lin Liyong, Thuijsman S, Zhu Yuting, et al. Synthesis of supremal successful normal actuator attackers on normal supervisors [C] //Proc of 2019 American Control Conf (ACC). Piscataway, NJ: IEEE, 2019: 5614-5619

[47] Meira-Góes R, Kang E, Kwong R H, et al. Synthesis of sensor deception attacks at the supervisory layer of cyber—physical systems [J]. Automatica, 2020, 121: 109172

[48] Erba A, Taormina R, Galelli S, et al. Constrained concealment attacks against reconstruction-based anomaly detectors in industrial control systems [C] //Proc of Annual Computer Security Applications Conf. New York: ACM, 2020: 480-495

[49] Herzberg A, Kfir Y. The chatty-sensor: A provably-covert channel in cyber physical systems [C] //Proc of the 35th Annual Computer Security Applications Conf (ACSAC'19). New York: ACM, 2019: 638-649

[50] Bolboacă R, Genge B, Haller P. Using side-channels to detect abnormal behavior in industrial control systems [C] //Proc of 2019 IEEE 15th Int Conf on Intelligent Computer Communication and Processing (ICCP). Piscataway, NJ: IEEE, 2019: 435-441

[51] Si Wen, Li Jianghai, Huang Xiaojin. Features extraction based on deep analysis of network packets in industrial control systems [C] //Proc of Int Symp on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant. Berlin: Springer, 2019: 524-529

[52] Shim K S, Sohn I, Lee E, et al. Enhance the ICS network security using the Whitelist-based network monitoring through protocol analysis [J]. Journal of Web Engineering, 2021, 20(1): 1-32

[53] Wolsing K, Wagner E, Henze M. Facilitating protocol-independent industrial intrusion detection systems [C] //Proc of the 2020 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2020: 2105-2107

[54] Hu Yibo, Zhang Dinghua, Cao Guoyan, et al. Network data analysis and anomaly detection using CNN technique for industrial control systems security [C] //Proc of 2019 IEEE Int Conf on Systems, Man and Cybernetics (SMC). Piscataway, NJ: IEEE, 2019: 593-597

[55] Sokolov A N, Alabugin S K, Pyatnitsky I A. Traffic modeling by recurrent neural networks for intrusion detection in industrial control systems [C] //Proc of 2019 Int Conf on Industrial Engineering, Applications and Manufacturing (ICIEAM). Piscataway, NJ: IEEE, 2019: 1-5

[56] Sapkota S, Mehdy A K M, Reese S, et al. FALCON: Framework for anomaly detection in industrial control systems [J]. Electronics, 2020, 9(8): 1192-1212

[57] Feng C, Palleti V R, Mathur A, et al. A systematic framework to generate invariants for anomaly detection in industrial control systems [C/OL] //Proc of NDSS. 2019 [2021-11-13]. https://www.ndss-symposium.org/wp-content/uploads/ndss2019_07A-3_Feng_slides.pdf

[58] Elnour M, Meskin N, Khan K, et al. A dual-isolation-forests-based attack detection framework for industrial control systems [J]. IEEE Access, 2020, 8: 36639-36651

[59] Brugman J, Khan M, Kasera S, et al. Cloud based intrusion detection and prevention system for industrial control systems using software defined networking [C] //Proc of 2019 Resilience Week (RWS). Piscataway, NJ: IEEE, 2019, 1: 98-104

[60] Sándor H, Genge B, Szántó Z, et al. Cyber attack detection and mitigation: Software defined survivable industrial control systems [J]. International Journal of Critical Infrastructure Protection, 2019, 25: 152-168

[61] Sainz M, Garitano I, Iturbe M, et al. Deep packet inspection for intelligent intrusion detection in software-defined industrial networks: A proof of concept [J]. Logic Journal of the IGPL, 2020, 28(4): 461-472

[62] Sheng Chuan, Yao Yu, Yang Wei, et al. How to fingerprint attack traffic against industrial control system network [C] //Proc of 2019 1st Int Conf on Industrial Artificial Intelligence (IAI). Piscataway, NJ: IEEE, 2019: 1-6

[63] Sicard F, Zamaï É, Flaus J M. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems [J]. Reliability Engineering & System Safety, 2019, 188: 584-603

[64] Song Zhanwei, Liu Zenghui. Abnormal detection method of industrial control system based on behavior model [J]. Computers & Security, 2019, 84: 166-178

[65] Ahmed C M, Ochoa M, Zhou Jianying, et al. Scanning the cycle: Timing-based authentication on PLCs [C] //Proc of the 2021 ACM Asia Conf on Computer and Communications Security. New York: ACM, 2021: 886-900

[66] Lin C Y, Nadjm-Tehrani S. Timing patterns and correlations in spontaneous SCADA traffic for anomaly detection [C/OL] //Proc of the 22nd Int Symp on Research in Attacks, Intrusions and Defenses. 2019 [2021-11-13]. https://www.usenix.org/system/files/raid2019-lin-chih-yuan.pdf

[67] Yu Wenbin, Wang Yiyin, Song Lei. A two stage intrusion detection system for industrial control networks based on ethernet/IP [J]. Electronics, 2019, 8(12): 1545-1562

[68] Colelli R, Foglietta C, Panzieri S, et al. The smart extension approach for securing industrial control systems [J]. IFAC-PapersOnLine, 2020, 53(2): 11207-11212

[69] Pyatnisky I A, Sokolov A N. Assessment of the applicability of autoencoders in the problem of detecting anomalies in the work of industrial control systems [C] //Proc of 2020 Global Smart Industry Conf (GloSIC). Piscataway, NJ: IEEE, 2020: 234-239

[70] Huang Dajian, Shi Xiufang, Zhang Wenan 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

[71] Yang Zeyu, He Liang, Cheng Peng, et al. PLC-Sleuth: Detecting and localizing PLC intrusions using control invariants [C/OL] //Proc of the 23rd Int Symp on Research in Attacks, Intrusions and Defenses (RAID 2020). 2020: 333-348. [2021-11-13]. https://www.usenix.org/system/files/raid20-yang.pdf

[72] Wang Chao, Wang Bailiang, Liu Haikuo, et al. Anomaly detection for industrial control system based on autoencoder neural network [J]. Wireless Communications and Mobile Computing, 2020, 2020: 1-10

[73] Zhang Youqian, Rasmussen K. Detection of electromagnetic interference attacks on sensor systems [C] //Proc of 2020 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2020: 203-216

[74] Meira-Góes R, Kwong R, Lafortune S. Synthesis of sensor deception attacks for systems modeled as probabilistic automata [C] //Proc of 2019 American Control Conf (ACC). Piscataway, NJ: IEEE, 2019: 5620-5626

[75] Gao Rui, Huang Jianghuai, Wang Lei. Leaderless consensus control of uncertain multi-agents systems with sensor and actuator attacks [J]. Information Sciences, 2019, 505: 144-156

[76] Zhu Yuting, Lin Liyong, Su Rong. Supervisor obfuscation against actuator enablement attack [C] //Proc of 2019 18th European Control Conf (ECC). Piscataway, NJ: IEEE, 2019: 1760-1765

[77] Bai Shuangpeng, Wen Hui, Fang Dongliang, et al. DSS: Discrepancy-Aware seed selection method for ICS protocol fuzzing [C] //Proc of Int Conf on Applied Cryptography and Network Security. Switzerland: Springer, Cham, 2021: 27-48

[78] Luo Zhengxiong, Zuo Feilong, Shen Yuheng, et al. ICS protocol fuzzing: Coverage guided packet crack and generation [C] //Proc of 2020 57th ACM/IEEE Design Automation Conf (DAC). Piscataway, NJ: IEEE, 2020: 1-6

[79] Luo Zhengxiong, Zuo Feilong, Jiang Yu, et al. Polar: Function code aware fuzz testing of ICS protocol [J]. ACM Transactions on Embedded Computing Systems, 2019, 18 (5s): 1-22

[80] Lin P Y, Tien C W, Huang T C, et al. ICPFuzzer: Proprietary communication protocol fuzzing by using machine learning and feedback strategies [J]. Cybersecurity, 2021, 4 (1): 1-15

[81] Salehi M, Bayat-Sarmadi S. PLC defender: Improving remote Attestation techniques for PLCs using physical model [J]. IEEE Internet of Things Journal, 2020, 8(9): 7372-7379

[82] Ghaeini H R, Chan M, Bahmani R, et al. PAtt: Physics-based attestation of control systems [C/OL] //Proc of the 22nd Int Symp on Research in Attacks, Intrusions and Defenses (RAID 2019). 2019: 165-180. [2021-11-13]. https://www.usenix.org/system/files/raid2019-ghaeini.pdf

[83] Ammar M, Crispo B, De Oliveira Nunes I, et al. Delegated attestation: Scalable remote attestation of commodity CPS by blending proofs of execution with software attestation [C] //Proc of the 14th ACM Conf on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2021: 37-47

[84] Francillon A, Castelluccia C. Code injection attacks on harvard-architecture devices [C] //Proc of the 15th ACM Conf on Computer and Communications Security. New York: ACM, 2008: 15-26

[85] Basnight Z, Butts J, Lopez Jr J, et al. Firmware modification attacks on programmable logic controllers [J]. International Journal of Critical Infrastructure Protection, 2013, 6(2): 76-84

[86] Kalle S, Ameen N, Yoo H, et al. Clik on PLCs! attacking control logic with decompilation and virtual PLC [C/OL] //Proc of Binary Analysis Research (BAR) Workshop, Network and Distributed System Security Symp (NDSS). 2019 [2021-11-13]. https://www.ndss-symposium.org/wp-content/uploads/bar2019_74_Kalle_paper.pdf

[87] Garcia L, Brasser F, Cintuglu M H, et al. Hey, my malware knows physics! attacking PLCs with physical model aware Rootkit [C/OL] //Proc of NDSS. 2017 [2021-11-13]. https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_08-1_Garcia_paper.pdf

[88] 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

[89] Konstantinou C, Maniatakos M. Impact of firmware modification attacks on power systems field devices [C] //Proc of 2015 IEEE Int Conf on Smart Grid Communications (SmartGridComm). Piscataway, NJ: IEEE, 2015: 283-288

[90] Peck D, Peterson D. Leveraging Ethernet card vulnerabilities in field devices [C] //Proc of SCADA Security Scientific Symp. 2009: 1-19. [2021-11-13]. https://icscsi.org/library/Documents/ICS_Vulnerabilities/DigitalBond-Leverage Ethernet Vulnerabilities in Field Devices.pdf

[91] Costin A, Zaddach J, Francillon A, et al. A large-scale analysis of the security of embedded firmwares [C] //Proc of the 23rd USENIX Security Symp (USENIX Security'14). Berkeley, CA: USENIX Association,2014: 95-110

[92] Florin I L, Bălan T. Vulnerability remediation in ICS infrastructure based on source code analysis [C] //Proc of 2020 19th RoEduNet Conf: Networking in Education and Research (RoEduNet). Piscataway, NJ: IEEE, 2020: 1-6

[93] Keliris A, Maniatakos M. ICSREF: A framework for automated reverse engineering of industrial control systems binaries [J]. arXiv preprint, arXiv:1812.03478, 2018

[94] Garcia Jr A M. Firmware modification analysis in programmable logic controllers [C/OL] //Proc of Int Conf on Cyber Warfare and Security. 2014 [2021-11-13]. https://apps.dtic.mil/sti/pdfs/ADA599675.pdf

[95] Zhang Mu, Chen C Y, Kao Binchou, et al. Towards automated safety vetting of PLC code in real-world plants [C] //Proc of 2019 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2019: 522-538

[96] Benkraouda H, Chakkantakath M A, Keliris A, et al. Snifu: Secure network interception for firmware updates in legacy PLCs [C] //Proc of 2020 IEEE 38th VLSI Test Symp (VTS). Piscataway, NJ: IEEE, 2020: 1-6

[97] Tychalas D, Benkraouda H, Maniatakos M. ICSFuzz: Manipulating I/Os and repurposing binary code to enable instrumented Fuzzing in ICS control applications [C] //Proc of the 30th USENIX Security Symp (USENIX Security'21). Berkeley, CA: USENIX Association, 2021: 2847-2862

[98] Falas S, Konstantinou C, Michael M K. A hardware-based framework for secure firmware updates on embedded systems [C] //Proc of 2019 IFIP/IEEE 27th Int Conf on Very Large Scale Integration (VLSI-SoC). Piscataway, NJ: IEEE, 2019: 198-203

[99] Benkraouda H, Chakkantakath M A, Keliris A, et al. Snifu: Secure network interception for firmware updates in legacy PLCs [C] //Proc of 2020 IEEE 38th VLSI Test Symp (VTS). Piscataway, NJ: IEEE, 2020: 1-6

[100] Falas S, Konstantinou C, Michael M K. A modular end-to-end framework for secure firmware updates on embedded systems [J]. ACM Journal on Emerging Technologies in Computing Systems, 2021, 18(1): 1-19

[101] Wang Xueyang, Konstantinou C, Maniatakos M, et al. Confirm: Detecting firmware modifications in embedded systems using hardware performance counters [C] //Proc of 2015 IEEE/ACM Int Conf on Computer-Aided Design (ICCAD). Piscataway, NJ: IEEE, 2015: 544-551

[102] Yang Huan, Cheng Liang, Chuah M C. Detecting payload attacks on programmable logic controllers (PLCs) [C] // Proc of 2018 IEEE Conf on Communications and Network Security (CNS). Piscataway, NJ: IEEE, 2018: 1-9

[103] Fu Xiao, Sha Letian, Yuan Zaiping, et al. VulHunter: A discovery for unknown bugs based on analysis for known patches in industry Internet of things [J]. IEEE Transactions on Emerging Topics in Computing, 2017, 8 (2): 267-279

[104] Adepu S, Brasser F, Garcia L, et al. Control behavior integrity for distributed cyber-physical systems [C] //Proc of 2020 ACM/IEEE 11th Int Conf on Cyber-Physical Systems (ICCPS). New York: ACM, 2020: 30-40

[105] Singh S, Sharma P K, Moon S Y, et al. A comprehensive study on APT attacks and countermeasures for future networks and communications:Challenges and solutions [J]. The Journal of Supercomputing, 2019, 75(8): 4543-4574

[106] Rubio J E, Roman R, Alcaraz C, et al. Tracking advanced persistent threats in critical infrastructures through opinion dynamics [C] //Proc of European Symp on Research in Computer Security. Switzerland: Springer, Cham, 2018: 555-574

[107] Yao Yu, Sheng Chuan, Fu Qiang, et al. A propagation model with defensive measures for PLC-PC worms in industrial networks [J]. Applied Mathematical Modelling, 2019, 69: 696-713

[108] Umer M A, Jilani M T, Ahmed C M, et al. Attack rules: An adversarial approach to generate attacks for industrial control systems using machine learning [C] //Proc of CPSIoTSec. New York: ACM, 2021: 35-40

[109] Li Jiangnan, Yang Yingyuan, Sun J S, et al. Conaml: Constrained adversarial machine learning for cyber-physical systems [C] //Proc of the 2021 ACM Asia Conf on Computer and Communications Security. New York: ACM, 2021: 52-66

[110] Anthi E, Williams L, Rhode M, et al. Adversarial attacks on machine learning cybersecurity defences in industrial control systems [J]. Journal of Information Security and Applications, 2021, 58: 102717

[111] Chekole E G, Huaqun G. ICS-sea: Formally modeling the conflicting design constraints in ICS [C] //Proc of the 5th Annual Industrial Control System Security (ICSS) Workshop. New York: ACM, 2019: 60-69

[112] Choi S, Yun J H, Kim S K. A comparison of ICS datasets for security research based on attack paths [C] //Proc of Int Conf on Critical Information Infrastructures Security. Switzerland: Springer, Cham, 2018: 154-166

[113] Fujdiak R, Blazek P, Mlynek P, et al. Developing battery of vulnerability tests for industrial control systems [C] //Proc of 2019 10th IFIP Int Conf on New Technologies, Mobility and Security (NTMS). Piscataway, NJ: IEEE, 2019: 1-5

[114] Negi R, Kumar P, Ghosh S, et al. Vulnerability assessment and mitigation for industrial critical infrastructures with cyber physical test bed [C] //Proc of 2019 IEEE Int Conf on Industrial Cyber Physical Systems (ICPS). Piscataway, NJ: IEEE, 2019: 145-152

[115] Yoon C, Lee S, Kang H, et al. Flow wars: Systemizing the attack surface and defenses in software-defined networks [J]. IEEE/ACM Transactions on Networking, 2017, 25 (6): 3514-3530

[116] Gardiner J, Rashid A, Nagaraja S, et al. Controller-in-the-middle: Attacks on software defined networks in industrial control systems [C] //Proc of the 2nd Joint Workshop on CPS & IoT Security and Privacy (CPSIoTSec'21). New York: ACM, 2021: 63-68

[117] Gonzalez D, Alhenaki F, Mirakhorli M. Architectural security weaknesses in industrial control systems (ICS) an empirical study based on disclosed software vulnerabilities [C] //Proc of 2019 IEEE Int Conf on Software Architecture (ICSA). Piscataway, NJ: IEEE, 2019: 31-40

[118] Irmak E, Erkek İ. An overview of cyber-attack vectors on SCADA systems [C] //Proc of 2018 6th Int Symp on Digital Forensic and Security (ISDFS). Piscataway, NJ: IEEE, 2018: 1-5

[119] Huitsing P, Chandia R, Papa M, et al. Attack taxonomies for the Modbus protocols [J]. International Journal of Critical Infrastructure Protection, 2008, 1: 37-44

[120] Grooby S, Dargahi T, Dehghantanha A. Protecting IoT and ICS platforms against advanced persistent threat actors: Analysis of APT1, silent chollima and molerats [M] // Handbook of Big Data and IoT Security. Switzerland: Springer, Cham, 2019: 225-255

[121] Day S, Smallwood W, Kuhn J. Simulating industrial control systems using Node-RED and unreal engine 4 [C] //Proc of National Cyber Summit. Switzerland: Springer, Cham, 2021: 13-21

[122] Khan S, Volpatto A, Kalra G, et al. Cyber range for industrial control systems (CR-ICS) for simulating attack scenarios [C/OL] //Proc of the CEUR Workshop. 2021: 246-259. [2021-11-13]. http://ceur-ws.org/Vol-2940/paper21.pdf

[123] Dietz M, Pernul G. Unleashing the digital twin's potential for ICS security [J]. IEEE Security & Privacy, 2020, 18(4): 20-27

[124] Akbarian F, Fitzgerald E, Kihl M. Intrusion detection in digital twins for industrial control systems [C] //Proc of 2020 Int Conf on Software, Telecommunications and Computer Networks (SoftCOM). Piscataway, NJ: IEEE, 2020: 1-6

[125] Zhou Luying, Guo Huaqun, Deng Gelei. A fog computing based approach to DDoS mitigation in IIoT systems [J]. Computers & Security, 2019, 85: 51-62

[126] Alladi T, Chamola V, Parizi R M, et al. Blockchain applications for industry 4.0 and industrial IoT: A review [J]. IEEE Access, 2019, 7: 176935-176951

[127] He Yujun, Gong Guocheng. A summary of research on block chain technology in the security field of IoT [J]. Telecom Engineering Technics and Standardization, 2017, 30(5): 12-16 (in Chinese)
(何渝君, 龚国成. 区块链技术在物联网安全相关领域的研究[J]. 电信工程技术与标准化, 2017, 30(5): 12-16)

[128] Afanasev M Y, Fedosov Y V, Krylova A A, et al. An application of blockchain and smart contracts for machine-to-machine communications in cyber-physical production systems [C] //Proc of 2018 IEEE Industrial Cyber-Physical Systems (ICPS). Piscataway, NJ: IEEE, 2018: 13-19

[129] Lauer H R, Salehi S A, Rudolph C, et al. User-centered attestation for layered and decentralized systems [C/OL] //Proc of Workshop on Decentralized IoT Security and Standards. 2018 [2021-11-13]. https://researchmgt.monash.edu/ws/portalfiles/portal/273194581/269534447_oa.pdf

[130] Golomb T, Mirsky Y, Elovici Y. CIoTA: Collaborative IoT anomaly detection via blockchain [J]. arXiv preprint, arXiv: 1803.03807, 2018

[131] Kravchik M, Biggio B, Shabtai A. Poisoning attacks on cyber attack detectors for industrial control systems [C] //Proc of the 36th Annual ACM Symp on Applied Computing. New York: ACM, 2021: 116-125

**Yang Ting**, born in 1994. PhD candidate. Her main research interest is Internet of things security.
**杨　婷**,1994 年生.博士研究生.主要研究方向为物联网安全.

**Zhang Jiayuan**, born in 1997. Master candidate. Her main research interest is information security.
**张嘉元**,1997 年生.硕士研究生.主要研究方向为信息安全.

**Huang Zaiqi**, born in 1997. Master candidate. His main research interests include Internet of things security and artificial intelligence security.
**黄在起**,1997 年生.硕士研究生.主要研究方向为物联网安全、人工智能安全.

**Chen Yujie**, born in 1998. Master candidate. His main research interests include Internet of things security and artificial intelligence security.
**陈禹劼**,1998 年生.硕士研究生.主要研究方向为物联网安全、人工智能安全.

**Huang Chenglong**, born in 1999. Master candidate. His main research interests include Internet of things security and Web security.
**黄成龙**,1999 年生.硕士研究生.主要研究方向为物联网安全、Web 安全.

**Zhou Wei**, born in 1993. PhD, associate professor. His main research interests include Internet of things security and systems security.
**周　威**,1993 年生.博士,副教授.主要研究方向为物联网安全、系统安全.

**Liu Peng**, born in 1971. Professor. His main research interest is cyber-security.
**刘　鹏**,1971 年生.教授.主要研究方向为网络安全.

**Feng Tao**, born in 1970. PhD, professor. His main research interests include network and information security.
**冯　涛**,1970 年生.博士,教授.主要研究方向为网络与信息安全.

**Zhang Yuqing**, born in 1966. PhD, professor, PhD supervisor. His main research interest is information security.
**张玉清**,1966 年生.博士,教授,博士生导师.主要研究方向为信息安全.