工业控制系统脆弱性分析及漏洞挖掘技术研究综述

赖英旭[1,2], 刘 静[1,3], 刘增辉[4], 张靖雯[1]
(1. 北京工业大学信息学部, 北京 100124; 2. 信息保障技术重点实验室, 北京 100072;
3. 西安电子科技大学陕西省网络与系统安全重点实验室, 西安 710071; 4. 北京电子科技职业学院, 北京 100176)

摘 要: 针对工业控制系统信息安全问题的来源进行总结,对工业控制安全领域现有的脆弱性分析技术进行归纳、梳理. 根据所检测漏洞是否为已知漏洞,讨论工业控制系统漏洞检测技术和工业控制系统漏洞挖掘技术的发展现状和成果,分析当前研究存在的不足之处. 根据当前趋势进行展望,提出工业控制系统脆弱性分析和漏洞技术的未来发展方向.

关键词: 工业控制系统; 脆弱性分析; 漏洞挖掘; 漏洞检测; 协议分析; 模糊测试
中图分类号: TP 393.0 **文献标志码**: A **文章编号**: 0254-0037(2020)06-0571-12
doi: 10.11936/bjutxb2019120008

Review on Vulnerability Analysis and Vulnerability Mining Technology of Industrial Control System

LAI Yingxu[1,2], LIU Jing[1,3], LIU Zenghui[4], ZHANG Jingwen[1]
(1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China;
2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China;
3. Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an 710071, China;
4. Beijing Polytechnic, Beijing 100176, China)

Abstract: The sources of information security in industrial control systems and the existing vulnerability analysis techniques in industrial safety field were summarized. Based on whether the vulnerability detected is a known vulnerability, development status and results of the industrial control system vulnerability detection technology and vulnerability mining technology were discussed. The shortcomings of the current research were also analyzed. According to the current trend, the future development direction of vulnerability analysis and loophole technology of industrial control system were put forward.

Key words: industrial control system; vulnerability analysis; vulnerability mining; vulnerability detection; protocol analysis; fuzz testing

工业控制系统(industrial control system, ICS)是负责工业活动的各类控制系统的总称,负责监测和控制包括交通设施、水处理和配送、输配电和天然气管道等国家基础设施或工业过程. 随着计算机技术、通信和控制技术的发展,以及"两化"的融合与物联网的快速推进,现代工业控制系统已经成为诸

收稿日期: 2019-12-17
基金项目: 北京市自然科学基金-海淀原始创新联合基金资助项目(19L2020);信息保障技术重点实验室基金资助项目(614211204031117);工业和信息化部2018年工业互联网创新发展工程-面向电子行业安全技术典型应用推广项目(573007016201902)
作者简介: 赖英旭(1973—), 女, 教授, 主要从事可信计算、网络安全、工控网络安全方面的研究, E-mail: laiyingxu@bjut.edu.cn

如铁路、石油化工、电力、航空航天等国家关键基础设施领域的核心控制系统与中枢神经[1].

信息技术的应用使 ICS 由封闭走向开放,在提高生产作业效率的同时,也出现了针对工业控制系统的攻击行为. 2010 年,在伊朗发现了首个定向攻击真实世界中基础设施的蠕虫病毒“震网”(Stuxnet)[2],在此之后,又出现了 Conficker、Duqu、火焰(Flame)等病毒在工业领域肆虐横行的情况,这些安全事件造成了一定的财产损失和人员伤亡,保障工控安全已刻不容缓.

本文以维护 ICS 安全为目标,对当前研究进行归纳和分析. 首先介绍 ICS 的结构,接着分析脆弱性来源及评估技术,并对漏洞技术在 ICS 中的应用进行总结与分析,最后对 ICS 脆弱性评估与漏洞(vulnerability)技术的发展前景进行展望.

1 工业控制系统概述

通常情况下,不同企业可以搭建符合各自生产及管理要求的 ICS. 一个典型的现代 ICS 层次架构如图 1 所示.

部署现代 ICS 需要企业管理网络、监控网络和现场控制系统的共同参与. 在 ICS 的企业网络中,管理者通过获取监控网络提供的数据得知工厂内部情况,使用工厂信息管理系统(plant information management system,PIMS)对产品订单处理、生产调度等活动进行管理,部署先进过程控制(advanced process control, APC)系统处理复杂工业过程控制问题. 在监控网络中,操作员可以使用数据采集与监控(supervisory control and data acquisition,SCADA)系统对现场设备进行监视与控制. 现场控制层利用工业以太网协议与过程监控层进行通信,并使用分布式控制系统(distributed control system,DCS)、可编程逻辑控制器(programmabel logic controller,PLC)、远程终端单元(remote terminal unit,RTU)等部件进行工业现场设备的逻辑控制与指令运算[3]. 随着工业互联网的发展,“工业操作系统”+“工业 APP”的新型智能互联工厂建设架构的出现[4],通过互联网对 ICS 实施攻击的可能性越来越高,这些都为 ICS 带来巨大的安全隐患.

表 1 展示了 ICS 与传统信息系统的不同之处. 由于部件、协议及性能要求等方面存在差异,针对 ICS 脆弱性的攻击往往会造成更大的损失. 传统 IT 系统的防护手段对于 ICS 并不完全适用,需要制定符合工控要求的安全防护方案.

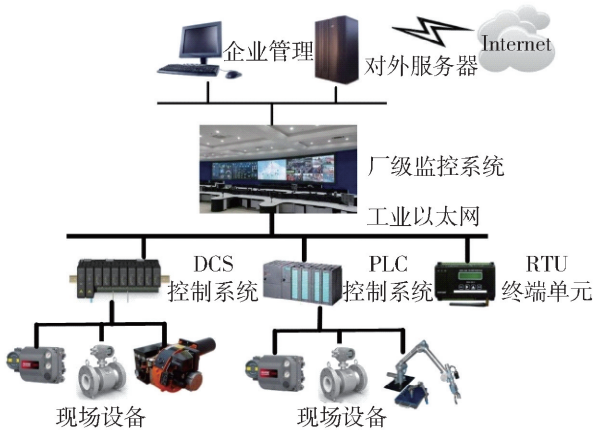

图 1 现代 ICS 层次架构

Fig. 1 Hierarchical architecture of modern ICS

表 1 工业控制系统与信息技术系统对比

Table 1 Comparison of ICS and information technology system

项目	传统 IT 系统	ICS
组成部件	单一(普通 PC 机)	多种(现场设备、PLC、RTU、DCS、SCADA 等)
操作系统	通用操作系统	嵌入式系统(VxWorks、WinCE 等)
通信协议	TCP/IP 协议	专用协议(OPC(object linking and embedding for process control)、Modbus TCP 等)
系统升级	软硬件升级简单	软硬件升级困难
实时性	允许传输延迟	高实时性
可用性	可停机或重启	难以停机或重启
安全性	较高	较低
生命周期	3 ~ 5 年	5 ~ 20 年

2 工业控制系统脆弱性研究

2.1 工业控制系统脆弱性概述

由于资源受限、环境封闭及高可用性要求等原因,ICS 设计之初缺乏对安全的充分考虑,这注定了 ICS 的脆弱性无法避免[5]. 现代 ICS 与信息技术结合发展,特别是工业互联网及人工智能技术的广泛应用,潜在安全问题逐渐被暴露出来. 分析 ICS 的脆弱性,研究有效的防护手段和工具,对于维护国家基础设施安全、避免安全损失等具有重要的意义.

根据图 1 所示的现代 ICS 层次架构,ICS 脆弱性主要包括以下 3 个方面[6].

2.1.1　现场控制系统脆弱性

在现场控制系统网络中，各类工业设备、传感器通过现场总线与控制器进行连接通信. 现场控制系统往往位于生产第一线，无法避免如温度、粉尘、电磁干扰、不恰当人为操作等物理安全的威胁，特别是居心不测者对控制器进行信息盗取和参数篡改，将间接或直接影响到工业过程；工业无线传感器常被部署在难以到达的位置，虽然增加了现场控制系统的灵活性，但也相对容易被窃听[7]；工业生产在过程连续性和实时性等方面要求严格，ICS 需要对工业过程进行精确控制. 因此，即使发现工业控制设备存在安全隐患，也不能够立刻停机进行维护. 除此之外，工业通信协议在设计时欠缺对安全的周全考虑，不但缺乏安全认证和授权保护，而且通信过程中地址和命令大都采用明文传输，这使得攻击者很容易捕获数据并解析.

2.1.2　监控网络脆弱性

监控网络负责对工业生产过程进行管控，在现代 ICS 中具有非常重要的地位. ICS 的生命周期较长，工程师站和操作员站都相对固定，因此，工控计算机存在着操作系统漏洞过多而无法及时修复、登录认证方式过于简单、缺乏安全有效的防护工具等问题；相关人员在对 ICS 进行维护时往往采用远程访问或移动终端接入的方式，因此，存在着未授权访问和移动终端携带病毒的可能性；工业应用软件随着 ICS 需求的增多而逐渐复杂化，但缺乏有效的安全管理手段，带来了许多潜在危险；管理者在工业控制平台的操作权限过高，而缺乏必要的信息安全知识，也会给 ICS 安全运行带来安全隐患[8].

2.1.3　企业管理网络脆弱性

企业管理网络负责执行公司数据的处理、存储和检索. 为了提高企业的生产力和竞争力，企业网络开始与互联网进行连接[9]. 但同时，开放互联也增加了 ICS 被普通计算机网络中存在的恶意程序或者攻击造成破坏的可能性[10]. 各类联网用户的请求和应用进程间的通信为 ICS 带来了大量冲击性流量，也为通信流量的预测和识别带来了一定困难[11]. 此外，企业管理网络还存在防火墙配置不适当、缺乏安全边界控制、联网用户通过网络漏洞获取生产控制网络关键设备的运行控制数据等问题.

2.2　工业控制系统脆弱性分析方法

当前针对 ICS 脆弱性分析技术的研究仍处于起始阶段. 对 ICS 进行安全评估，根据评估结果对安全风险较大的部件进行重点防护，能够达到减轻攻击损失的效果[12]. 安全性评估包括定性评估和定量评估 2 种方式[13]. 定性评估是根据评估者的知识和经验对系统进行安全评估，评估结果用语言描述；定量评估往往借助工具进行计算，评估过程较为复杂，结果用数据表达. 目前，对 ICS 进行脆弱性分析常用的技术如表 2 所示.

表 2　ICS 脆弱性分析相关技术

Table 2　Related techniques of ICS vulnerability analysis

采用技术	定性/定量	定量方法	技术描述	相关文献
层次分析法(analytic hierarchy process，AHP)	结合使用	数学建模	将工业控制安全问题划分为不同因素，按照各因素的联系组合并从上到下划分为几个层次，各层权重都会影响结评估果	文献[14-16]
攻击树模型	定量评估	攻击模型	通过树形结构识别威胁和漏洞的方法，由表示攻击最终目标的根节点和表示用于实现给定目标的各种攻击方法的各种中间节点组成	文献[17-20]
攻击图模型	定量评估	攻击模型	利用有向图作为表示，为攻击者的攻击过程提供清晰描述的方法，攻击和条件作为顶点，攻击和条件之间的因果关系作为边	文献[23-25]
Petri 网模型	定量评估	攻击模型	用于解释 ICS 资源和进程之间的关系，并描述同步和异步元素的攻击信息流	文献[26-29]

2.2.1　层次分析法

AHP 是一种定量分析和定性分析相结合的脆弱性评估方法. 该方法在准确细致描述 ICS 脆弱性的基础之上，使用定性方法来补充说明脆弱性的特征和偶然关系. Markovic-Petrovic 等[14]采用定性方法建立真实水力发电 SCADA 系统的脆弱性的指标体系，各指标的权重由层次分析模型计算获得，最后通过 AHP 模糊评价的定性方法评估该 SCADA 系统

是否安全. Li 等[15]结合 ICS 安全需求的特殊性建立了 AHP 模型并获得各指标权重,采用灰色数学模型对评估结果进行计算,仿真结果显示作者提出模型具有很高的精度. Zhu 等[16]在使用层次分析法的基础上,使用熵值法和改进的约简因子优化模糊评价矩阵,有效地评估了系统资产的重要性、脆弱性的严重程度和所面临的威胁.

2.2.2 攻击模型法

针对 ICS 网络进行建立攻击模型建模,从而分析完整攻击过程,也是一种常用的脆弱性分析方法. 现有研究中使用到的攻击模型包括攻击树模型、攻击图模型和 Petri 网模型[17].

1) 攻击树模型. 攻击树模型用于进行网络攻击描述,具有直观、实用的优点. 黄慧萍等[18]不仅建立了攻击树模型,还结合了概率风险评估技术. 不足之处在于未对评分标准的建立进行深入研究,攻击成本属性、攻击难度及被发现可能性等叶节点属性由专家判断得出,未消除主观性. 李玲[19]采用攻击树方法,结合列控系统的典型特征,利用平台漏洞扫描结果,建模分析列控系统的信息安全风险. 王锋[20]从主动防御的角度,展开了对信号安全数据网的信息安全风险识别,根据挖掘出的端口及漏洞,利用攻击树模型分析网络内可能发生的攻击,根据攻击结果分析渗透攻击对网络造成的影响. Abdo 等[21]利用 Bowtie 风险模型分析工业安全事故,并引入攻击树来考虑可能影响系统安全的潜在恶意攻击. 这 2 种方法结合使用,从而考虑和识别了所有可能导致相同不良事件产生损害的所有安全事件和安全威胁. 文献[22]根据实际入侵场景设计根节点与多级叶节点,对可能存在的安全威胁及攻击手段进行了描述,直观说明该 SCADA 系统的防护重点.

2) 攻击图模型. 与攻击树模型相比,攻击图对网络攻击的描述能力更强,可以自动生成攻击路径来分析 ICS 网络的弱点. 通过可视化,攻击图可以向用户、管理员展示攻击的发生方式,然后采取防御措施,起到关于 ICS 安全防御预测的辅助功能. Yang 等[23]通过读取 ICS 网络资产分配文件构建原始网络拓扑模型,并根据属性将节点划分为权限节点、配置信息节点与攻击步骤节点. 黄家辉等[24]结合 ICS 特征,提出漏洞利用难度和漏洞危害性 2 个量化评估指标,攻击期望由二者量化后的乘积表示. 在真实控制系统案例中,计算出每个漏洞的攻击期望,并结合系统拓扑结构生成攻击图,从而获知该系统可被利用进行攻击的漏洞,计算出攻击期望最大的路径. Puys 等[25]设计了适用 ICS 的攻击场景制作(applicative attack scenarios production for industrial control system, A^2SPICS)方法,考虑了 Modbus 服务器进程的行为、攻击者可能攻击的元素以及网络拓扑信息建立攻击图.

3) Petri 网模型. 在网络物理攻击中,攻击者通常采用网络和物理手段来实现协同攻击,从而使攻击进程既可以并发,也可以异步进行. 因此,Petri 网对于模拟网络物理攻击是可行的. Petri 网模型具有灵活性、细化性、可扩展性和动态性等特点,通过 Petri 网模型可以全面系统地分析 ICS 的动态和实时脆弱性. Fu 等[26]结合 Petri 网模型分析结果和 ICS 脆弱性的大数据分析结果,确定脆弱性指标及其权重,进一步利用径向基函数(radial basis function, RBF)神经网络模型构建评估模型. Li 等[27]开发一种基于随机 Petri 网的分析模型,用于评估和分析智能电网的系统可靠性. 所设计的分析模型准确获得了保守拓扑攻击、积极拓扑攻击、系统干扰和系统故障 4 种情况下的结果. Liu 等[28]利用概率 Petri 网及混合策略的攻击/防御模型进行 ICS 建模,使用纳什均衡来计算模型各攻击节点的权重. Mitchell 等[29]设计基于随机 Petri 网的分析模型,以捕捉攻击者行为与网络物理系统防御之间的动态关系,考虑了几种类型的故障,包括可能发生在网络物理系统中的损耗、渗透故障和渗漏故障.

3 工业控制系统漏洞技术

3.1 工业控制系统漏洞概述

漏洞是指系统中存在的一些功能性或安全性的逻辑缺陷,是系统在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷和不足[30].

3.1.1 工业控制系统漏洞现状

ICS 存在大量的安全漏洞与隐患,针对 ICS 发起的各类攻击,往往就是利用各类 ICS 软硬件中存在的安全漏洞来实现的[31]. 如图 2 所示,近几年来共发现了近千 ICS 漏洞,而且绝大部分是中高危漏洞. 攻击者可以利用这些漏洞获得某些系统权限,对系统执行非法操作,从而导致安全事件的发生,造成财产损失. 因此,应当大力加强针对 ICS 漏洞技术的研究工作,及时发现系统中存在的安全漏洞并尽早修补.

3.1.2 工业控制系统漏洞技术介绍

目前,ICS 的漏洞技术包括 ICS 漏洞检测技术与 ICS 漏洞挖掘技术[32]. ICS 漏洞检测技术是一种利用扫描等手段,发现 ICS 中存在的安全漏洞的技

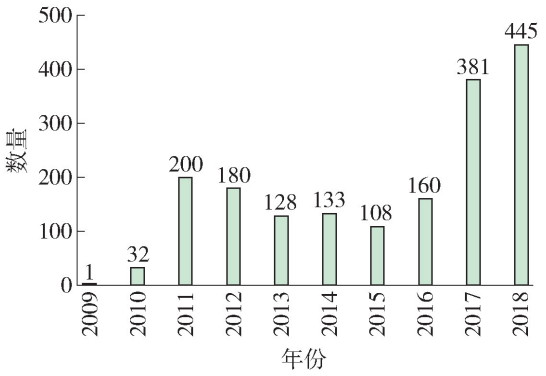

图 2　ICS 每年安全漏洞新增统计

Fig. 2　ICS annual incremental statistics of security vulnerabilities

术. 漏洞检测是一种主动防御手段，旨在发现漏洞并及时进行修补. ICS 漏洞挖掘技术以检测未知的安全漏洞为主要目的，核心技术是模糊测试(fuzzy testing)技术. 2 种技术具有不同的应用场景.

3.2　工业控制系统漏洞检测技术

检测 ICS 中是否存在已知的安全漏洞，往往采用安全扫描技术. 进行漏洞扫描首先需要收集漏洞并建立 ICS 漏洞数据库，数据库内存储 2 种信息：ICS 中主流控制设备的具体信息和当前已被漏洞平台公布的安全漏洞信息. 进行漏洞探测时，需要完成网络探测和系统探测. 网络探测负责捕获和解析广播包，解析得到工业控制交换机的站名称、地址以及系统的广播地址等基本信息. 系统探测则负责获取 ICS 中的工业控制设备以及其站类型、站名称、制造商标识、设备标识、MAC(media access control address)地址等具体信息[33]. 最后，把探测到的相关信息与数据库存储的内容进行匹配，继而得知被检测的工业控制设备是否存在已知漏洞.

3.2.1　工业控制系统漏洞检测技术研究现状

对现有文献及相关信息进行总结，目前针对 ICS 漏洞检测的相关工作如表 3 所示.

表 3　ICS 漏洞检测技术对比

Table 3　Comparison of ICS vulnerability detection technology

研究成果	成果描述	相关技术	优点
ICS 漏洞扫描系统[33]	基于网络的层次探测漏洞扫描系统	层次探测技术	专门针对 ICS 的漏洞扫描工具
ICS 漏洞检测系统[34]	基于国产化硬件平台的 ICS 漏洞检测工具	工控漏洞插件技术、硬盘加密技术、国产化技术	漏洞库容易扩展、高安全性保障
ICS 漏洞数据库系统[35]	设计了专门针对 ICS 的漏洞数据库	优化的漏洞评级方法(common vulnerability rating system，CVRS)	减少前期收集的工作量，提供漏洞分析平台
ICS 漏洞检测工具[36]	基于主机的集中式漏洞扫描系统	集中式技术	降低检测时间，适用于企业网络

王欢欢[33]根据 ICS 特性，设计了基于层次探测方法的 ICS 漏洞扫描系统. 首先根据发现和基本配置协议(discovery and basic configuration protocol，DCP)帧的结构特点对捕获的 PROFINET 数据包进行分析，获取所探测工业控制网络的基本信息. 然后构造 DCP 数据包，根据网络探测获得的广播地址进行广播发送并接收 ICS 设备的回复数据包，获取各设备详细信息，从而完成系统探测. 实验结果证明，该方法在网络探测过程中可以获得西门子交换机的具体信息；比对 Wireshark 与该方法探测得到的数据包，证明探测模块能够实现探测工业控制网络的功能；同时，将所获得的信息与漏洞数据库进行匹配，确定检测中存在已知漏洞.

张凤臣[34]设计了一种面向 ICS 的国产化漏洞分析系统. 该系统使用 1 024 位 AES 算法进行全盘加密，从而提高平台数据的安全性；进行漏洞扫描之前首先进行规则校验，校验成功之后安全加载规则漏洞库，并将规则整理为树型结构，然后逐级完成扫描. 文献[34]所使用的 ICS 漏洞数据库运用漏洞插件技术实现功能更新，并采用自学习模糊测试技术，保障了漏洞测试的高效性.

杨盛明[35]设计并实现了专门针对 ICS 的漏洞数据库系统，为工作人员前期搜集漏洞信息提供方便. 设计者对 ICS 漏洞进行了全面收集，采用 CVRS 对 ICS 漏洞进行重新评级，并对漏洞属性进行分析归纳，从而使具有多维属性的漏洞进行合理存储，有利于数据库的拓展和维护. 所实现系统还具备查询与共享功能，为相关人员研究 ICS 漏洞提供了良好的平台.

Rakshit 等[36]实现了一种基于主机的集中式工业控制计算机系统漏洞检测系统. 该系统的漏洞扫描器安装在被测主机上,负责收集主机的相关信息;漏洞分析器位于服务器或服务器集群上,负责对接受到的信息执行分析匹配,并报告被测主机存在的漏洞. 文献[36]将该系统部署在工业控制企业网络上,并有效利用第三方安全知识,即使更新知识库,也不会增加终端主机的代码量,从而大大降低引入编程错误的可能性. 实验证明,在相同实验背景下,该集中式检测系统与开放漏洞评估语言(open vulnerability assessment language,OVAL)扫描器扫描到的漏洞个数相同,但所耗费的时间更少,因此,具有更好的性能.

3.3 工业控制系统漏洞挖掘技术

漏洞挖掘是一种针对未知漏洞的检测技术. 目前漏洞挖掘分析技术有多种,主要包括手工测试(manual testing)技术、Fuzzing 技术、比对和二进制比对(diff and bindiff)技术、静态分析(static analysis)技术、动态分析(runtime analysis)技术等[37]. 模糊测试技术是一种通过向目标系统提供非预期输入并监视异常结果来实现漏洞挖掘的方法[38],与传统的漏洞挖掘技术相比,模糊测试具有准确性较高、可用性强、对测试目标源码依赖性低等优点. 由于 ICS 的设备多由专门生产商提供,研究人员对内部结构了解不充分,多采用模糊测试技术对 ICS 进行漏洞挖掘.

3.3.1 ICS 漏洞挖掘技术研究现状

针对 ICS 漏洞挖掘主要集中在工业控制协议、工业控制软件、ActiveX 控件、人机界面(human machine interface,HMI)程序及工业控制设备等方向. 针对 ICS 漏洞挖掘技术的对比如表 4 所示.

表 4 ICS 漏洞挖掘技术对比

Table 4 Comparison of ICS vulnerability mining technology

改进方向/成果	测试用例来源	测试对象	部署模式	技术性能	不足
优化测试用例 设计 M-PEACH 测试框架[38]	Modbus/TCP 协议 Modbus ASCII 协议	SCADA 系统的 HMI 程序	普通模式	减少测试时间 检测出未知漏洞	无
优化测试用例 构建漏洞挖掘测试框架[39]	工业通信协议	Rockwell 工业控制器	普通模式	检测出未知漏洞 输入文件减少 29.6%	无
优化测试用例[40]	工业通信协议	工业控制设备	普通模式	代码覆盖率达到 100%	缺乏具体实验
构建通信协议状态模型[41]	工业通信协议	PLC 设备	普通模式	测试效率得到提高	缺乏检测数据支撑
优化测试用例 进行双向测试[42]	组态软件输入	监控组态软件 ActiveX 控件	内联模式 普通模式	测试用例冗余度降低 测试效率较高	功能实现不全
优化测试用例状态引导[43]	工业通信协议	SCADA 系统	内联模式	检测数量增加	模糊测试时间略长
模糊测试工具 MTF(modbus/TCP fuzzer)[44]	Modbus/TCP 协议	工业模拟设备	内联模式	减少检测时间	未对真实设备进行测试
模糊测试工具 LZFuzz[45]	工业通信协议	SCADA 系统	内联模式	提高测试性能	无
模糊测试工具 Smart Fuzzer 双向测试[46]	Modbus/TCP 协议	工业模拟设备	内联模式	发现未知漏洞 测试性能较好	未对真实设备进行测试
协议分析方法[47]	制造报文规范(manufacturing message specification,MMS)协议	智能电网	普通模式	检测出未知异常	不确定未知异常是否为漏洞
协议分析方法[48]	MMS 协议	智能电网	普通模式	基于字段分类的交叉领域模糊测试方法	不确定未知异常是否为漏洞
设计模糊测试框架[49]	OPC 协议	OPC 服务器	普通模式	能够针对协议特性进行测试	未进行测试效率的研究
改进模糊测试工具 优化测试用例[50]	工业控制软硬件编程数据	工业终端设备	普通模式	挖掘出设备漏洞	工作量大 漏洞分析困难

对现有研究成果进行总结对比可知，部分研究人员对测试用例进行研究，采用量化判定、遗传变异、深度学习等方法进行优化，提高漏洞挖掘的效率. 李志辉[37]基于深度对抗学习提出一种模糊测试用例生成方法，建立生成对抗网络中的生成模型和判别模型，用所获得的数据对模型进行训练得到特定的模型，用生成模型生成大量的测试用例数据，用生成的数据对系统进行压力测试引发系统异常. 最后，根据系统的异常，找到系统异常的原因，进行修补改进. 实际环境中的实验结果证明该方法表现出了较好的性能. 杨凯翔[38]为有效的对工业控制私有协议进行模糊测试，使用具有功能标识符特征的字节作为划分字节，对私有协议数据集进行分类，构建私有协议树，采用可变字节值概率统计方法、长度域学习方法、Apriori 和 Needleman/Wunsch 算法学习私有协议特征，依据协议特征学习结果进行模糊测试与异常监控. 张学聪[39]基于改进后的 Sulley 框架体系对电力行业 ICS 大量应用的 IEC60870-5-104 协议以及 Modbus_TCP 协议进行漏洞挖掘研究. 阮涛等[40]构造了由错误字段内容数据集以及协议裁剪和扩充数据集组成的模糊测试集，并更改取值步长和裁剪步长进行性能测试，得到测试用例结构与测试覆盖率之间的关系.

为了减少模糊测试前进行协议分析的工作量，尚文利等[41]首先利用有限状态机(finite state machine，FSM)建立工业协议状态模型，为生成测试用例提供条件；利用状态模型对协议脚本文件进行描述，再使用异常变异树进行变异，得到可以输入的测试用例，实现对 PLC 的未知漏洞挖掘. 吴波等[42]运用反汇编和数据包分析技术分析输入格式并进行二进制编码，采用轮盘赌选择和截段选择法进行遗传操作，使用单点交叉和本位变异进行选择交叉变异操作，生成了针对监控组态软件的测试用例，并通过统计测试数据触发的断点数量来计算算法的适应度值，将其作为下一轮测试中各项参数调整的依据. 张亚丰等[31]首先引入功能函数，构造了基于改进的扩展巴科斯范式(modified augmented Backus-Naur form，MABNF)语法的协议模型；将协议报文作为输入，根据模型转换为 MABNF 变异树，并生成 pit 文件；对变异树进行深度优先遍历，得到节点集合后再实施节点变异，获得了效果更好的测试用例集. 他们在后续研究中，又提出漏洞被发现是由于被测目标先处于一定的异常状态，才能由畸形测试报文触发的观点[43]，因此，建立了可扩展置标语言(extensible markup language，XML)协议模型，并使用基于协议状态机的测试序列生成算法(protocol state based test sequences generating method，PSTSGM)对被测目标状态加以引导. 测试用例依旧由 MABNF 范式语法模型生成，实现了模糊测试工具 SCADA-Fuzz.

普通模式部署下，测试器充当客户端，测试目标作为服务器端；内联式的模糊测试器部署在服务器和客户端之间，实现双向测试. 吴波等[42]对监控组态软件和 ActiveX 控件进行模糊测试. 针对 ActiveX 控件的上层模糊测试器采用普通部署模式，下层的模糊测试器部署在现场设备与组态软件之间. Voyiatzis 等[44]提出并设计了一种内联模糊测试工具 MTF，该 Fuzzer 构建功能码为 43 的应用数据单元(application data unit，ADU)数据包向被测对象发送，然后捕获数据流量来识别被测系统相关信息，同时通过主动发送请求或被动捕获流量的方式，对 Modbus 数据类型进行探测. Shapiro 等[45]使用 arp-sk 工具执行地址解析协议(address resolution protocol，ARP)欺骗，从而使 LZFuzz 工具内联到主从端之间，在此基础上实现了 SCADA 客户端和服务器的双向测试. Xiong 等[46]专门提出了针对主机(客户端)的测试用例生成方法：利用 ARP 欺骗捕获从机发送的正常数据包，并对这些数据包以基于突变的方法进行测试用例的生成，再发送给主机.

ICS 内通信协议众多，因此，进行 ICS 漏洞挖掘时，也应考虑除 Modbus 之外的其他协议. Kim 等[47-48]对使用 MMS 协议的智能电网进行了编码特征分析，指出相关协议的语法相似性；然后根据工业协议特征及应用考虑，设计基于字段分类的交叉领域模糊测试方法. Wang 等[49]在分析 OPC 协议的基础上采用基于生成的方法生成测试用例，研究利用微软公共远程过程调用(remote procedure call，RPC)库来实现 OPC 客户端并构造合法数据包. 模糊器与目标建立连接，并进行参数解析；然后，将生成的测试用例发送给被测对象并进行异常捕获.

上述研究使用的测试用例大多来源于工业通信协议，这也是目前 ICS 漏洞挖掘技术的大趋势. 除此以外，还可以将软硬件间编程数据作为测试用例样本. 于长奇[50]针对多个 S7-300 系列 PLC 进行测试，使用嗅探技术抓取以太网通信数据包，采用逆向工程技术获取其中的原始编程数据，获得 50 个测试样本，进行交叉变异后得到 1 000 个测试用例. 结合实际情况对内存模糊器进行优化改进，提高了测试效率.

3.3.2　工业控制系统漏洞挖掘技术成果分析

虽然针对 ICS 的漏洞挖掘技术还处于起步阶

段,但也取得了一些令人欣慰的成果. 李志辉[37]将深度对抗学习方法应用到 ICS 漏洞挖掘中,而且所生成的模型在不同的 ICS 中均能获得较高的测试效果. 阮涛等[40]提出的研究方法可以帮助构建模糊测试错误集,并进行精确的异常定位,代码覆盖率理论上可达 100%. 尚文利等[41]提出针对工业嵌入式设备的漏洞检测分析系统的构造方法,实现的系统具有漏洞挖掘、漏洞扫描、漏洞分析等多种功能,为研究人员今后开发此类系统提供了借鉴.

文献[42-46]所设计的模糊测试器采用内联模式部署,针对监控组态软件、SCADA 系统等进行了双向测试. Voyiatzis 等[44]基于 Modbus/TCP 协议构建了 14 个维度的攻击向量,记录被测对象的状态或响应,决定下一步的变异策略,使 MTF 能够实现向导性 Fuzzing. Shapiro 等[45]设计名为 LZFuzz 的工具,采用改进的 Lempel-Ziv(LZ)压缩算法和突变模糊优化测试用例,使用 LZ 对比算法对截获的数据包进行来源判定. Xiong 等[46]设计的 Smart Fuzzer 可以通过优化测试数据生成机制来压缩测试空间的大小,使用 Modsim 和 Modscan 来模拟主从端,发现了大多数有代表性的漏洞,并成功检测到 0-day 漏洞. 张亚丰等[43]设计的 SCADA-Fuzz 对 SCADA 系统的 HMI 客户端和嵌入式设备进行了测试,结果证明其挖掘 ICS 未知漏洞的能力要强于 Peach. 上述进行了内联部署的网络协议模糊器不仅可以实现双向模糊测试,同时由于可截获实时数据包并从被测设备接收返回结果,从而进行动态变异策略调整,所以降低了模糊测试的时间,具有较好的测试效果.

部分研究所进行的漏洞挖掘有一些特定场景. 张亚丰等[43]利用 Peach 平台开发 M-Peach 工具,对 SCADA 系统的 HMI 程序进行漏洞挖掘测试,测试结果表明 M-Peach 在保证检测准确的同时,增强了测试用例有效性,并发现潜在的工业安全漏洞. Kim 等[47]所做的研究应用于智能电网领域,提出的分类方法对于基于 MMS 协议的测试用例构造有很大帮助,减少了因研究人员知识差异引起的测试差异. Wang 等[49]提出面向 OPC 的 Fuzzing 技术,使用 Fuzzing 平台 Peach 进行开发并进行实验,并对包括数据访问(data access,DA)、历史数据访问(history data access,HAD)、报警事件(alarms and events,AE)在内的不同 OPC 协议进行了模糊测试. 于长奇[50]提出针对 ICS 终端设备的漏洞挖掘技术,成功挖掘到了西门子 S7-300 系列 PLC 的拒绝服务漏洞,并将 Sulley 测试与该方法进行对比,证明该方法对工业控制终端硬件的漏洞挖掘更为有效.

3.3.3 工业控制系统漏洞挖掘技术研究局限性分析

虽然 ICS 的漏洞挖掘取得了一定的成果,但是当前研究仍存在着一定的不足:首先,部分研究缺乏有效的实验数据支撑. 例如:阮涛等[40]虽然对测试用例进行了优化,但并未设置对照组实验进行性能比对;Wang 等[49]未对客户端的测试用例进行优化,同时也缺乏对测试性能的研究. 其次,部分研究设计的模糊测试工具功能不全. 例如:吴波等[42]所提出的针对监控组态软件的测试方法,只实现了部分功能,测试工作仍需要大量的人工参与. 最后,部分研究存在工作量过大,漏洞分析困难的问题. 例如:于长奇[50]所提出的针对 ICS 终端设备的漏洞挖掘技术,实现所使用的内存模糊器需要复杂的步骤及其他工具的辅助,同时,虽然成功挖掘出了漏洞,但进行漏洞分析较为困难,只能交给专业厂商. 如何针对这些不足进行改进,提高 ICS 漏洞挖掘技术的性能,更好地保障工控安全,应当是研究人员未来考虑的重点.

4 工业控制系统脆弱性及漏洞技术展望

4.1 工业控制系统脆弱性分析技术研究趋势

随着工业化进程的不断推进,ICS 的复杂程度也在增加,这将会为脆弱性分析技术带来一定的挑战.

首先,ICS 复杂程度增加带来了安全评估指标的增加,这为基于层次分析的评估方法带来了困难,研究人员必须更谨慎考虑各指标的权重问题. 目前研究人员多采取如文献[13]与文献[24]提出的攻击图方法进行多属性指标决策,消除量化结果的片面性,但该方法能否满足更复杂的 ICS 的需求仍是未知的. 在未来,如果能够搜集到一定数量的 ICS 安全评估案例,可以考虑使用如神经网络算法的智能方法进行进一步的优化处理,使评估结果更加客观.

第二,随着工业控制网络规模的扩大,基于攻击模型的评估算法的时间复杂度急剧增加. 因此,需要根据大规模工业控制网络的性质,研究攻击模型生成算法,降低算法的复杂度,提高其在大规模网络中的适用性. 如使用节点聚合算法[23]对拓扑节点信息进行聚合及使用规约减少攻击图的规模[51]等方法. 如何在适当减少工作量的基础上,获得准确、合理的评估结果,是脆弱性分析技术研究的趋势之一.

第三,思考如何建立成熟完善的 ICS 安全评估标准. Zhu 等[16]充分考虑 ICS 安全评估需求的特殊性,建立了符合要求的安全指标体系和评估细则.

所建立的评估细则结构完整、内容详细、等级划分清晰，从而使评估人员可以根据现场情况应用标准直接进行评估. 完善的评估标准能够为 ICS 脆弱性分析工作提供科学的参考依据，对于评估工作的顺利开展至关重要.

最后，工业控制环境并不是一成不变的，因此，每隔一段时间就需要对 ICS 重新进行脆弱性评估，否则就可能产生安全隐患. 工信部于 2017 年发布了《工业控制系统信息安全防护能力评估工作管理办法》[52]，特别强调了全生命周期评估，指出防护能力评估是对工业、企业 ICS 规划、设计、建设、运行、维护等全生命周期各阶段开展的安全防护能力综合评价.

4.2　工业控制系统漏洞检测技术研究趋势

如何更好地进行漏洞检测，减少存在的漏洞数量，降低 ICS 被攻击的风险，研究人员们做出了许多努力.

首先是建立完善的 ICS 安全漏洞库. 杨盛明[35]指出，不仅应当及时从国家信息安全漏洞共享平台(China national vulnerability database，CNVD)、美国工程系统网络紧急应变小组(industrial control systems cyber emergency response team，ICS-CERT)等 ICS 漏洞平台上搜集发布的工业控制漏洞，也需要留意 ICS 生产商官网，确保漏洞收集的完整性. 对所收集的漏洞进行合理评价与分类整理，尽可能完善漏洞信息，也会为提高漏洞扫描准确性带来帮助. 张凤臣[34]使用了 ICS 漏洞插件技术实现了漏洞数据库的快速更新. 漏洞数据库是进行漏洞检测的基础，探测到的信息需要与漏洞数据库进行匹配，才能确定被测系统是否含有漏洞. 因此，ICS 漏洞数据库的完善程度对于漏洞扫描的结果至关重要.

其次，应当致力于从 ICS 的实际情况出发进行研究. 王欢欢[33]注意到传统的漏洞扫描工具难以满足 ICS 漏洞检测的需求，因此，设计了层次探测漏洞扫描系统. 该系统既可以获取工业控制交换机的信息，提高漏洞探测阶段获取信息的全面性和准确性，又满足了 ICS 漏洞检测的要求. Rakshit 等[36]考虑到现代 ICS 与企业网相连的特点，设计的基于主机的集中式漏洞扫描系统，可以应用于企业网络，有效保障了现代 ICS 的网络安全.

除此以外，王欢欢[33]指出，不同的 ICS 所使用的设备可能由不同的生产厂商提供，因此，支持的工业控制协议可能会有差异，应当增加扫描系统支持的工业控制协议；提高漏洞扫描的性能，降低检测时间，并及时进行漏洞修补，对于维护 ICS 安全也十分重要.

4.3　工业控制系统漏洞挖掘技术研究趋势

基于模糊测试的 ICS 漏洞挖掘研究都有一个共同的目标，就是提高漏洞挖掘的性能，从而更好地保障 ICS 安全.

为了实现这个目标，研究人员们对测试过程进行了多方面优化改进. 首先是实现协议格式分析上的优化. 对通信协议进行充分分析将有利于构造更有效的测试用例，然而目前对协议分析多采用人工手段，工作量较大[53]. 不同的 ICS 网络支持的通信协议可能不同，这更增加了测试人员的负担. 张亚丰等[31]采用了 MABNF 模型对工业通信协议进行统一描述，并由该模型生成了代码覆盖率较高的测试用例. 尚文利等[41]也使用了 FSM 模型对协议脚本文件进行描述，为生成测试用例提供条件. 由此可见，采用统一的模型描述工业协议，实现协议格式的自动化分析，减少测试开发人员的负担，将是 ICS 漏洞挖掘技术未来发展的一个可行方向.

研究人员在测试用例生成及优化方面也做了相关工作. 现有研究表明，改进现有的组合方法，并利用其他技术进行模糊测试是可行的[54]. 机器学习技术有助于自动生成基于语法的模糊测试的输入，尚文利等[41]和吴波等[42]使用的遗传变异方法，减少了检测时间，提高漏洞挖掘的性能，故未来也需要继续进行这方面的研究. 研究人员应当选择合理有效的测试用例生成算法，降低测试用例的冗余度，提高测试命中率；同时也需要保证测试用例的有效性，否则即使生成了大量的畸形测试数据，也会被校验机制检测丢弃，测试效率无法得到提高.

除此之外，双向测试似乎是一个新的研究趋势. 由于工业控制报文大多采用明文传输，使用中间人方式捕获并变异是完全可行的. 文献[42－46]均采用了内联模式部署模糊测试器，不仅可以实现对客户端和服务器的双向测试，还可以截获实时数据包并从被测设备处接收返回结果. 根据获得的信息判断被测设备是否出现异常，进行动态变异策略调整. 然而，张亚丰等[43]通过对实验结果分析指出，这种实时测试的方式需要占用一定的处理器资源，模糊测试的时间可能略有延长，需要多加考虑优化问题.

5　结论

1) 我国正处于工业转型升级的关键期，工业技术发展带来了生产力的提高，但安全问题也随之而来. 本文以保障 ICS 安全为目标，探讨了 ICS 脆弱

性的主要来源,对现有的 ICS 脆弱性评估技术和漏洞技术进行了总结阐述. 脆弱性来源分析揭示了 ICS 安全问题频繁发生的根本原因,ICS 脆弱性评估技术的归纳总结为研究人员进行改进提供了指导意义. 从 ICS 漏洞的防护角度,总结了当前 ICS 漏洞检测技术和漏洞挖掘技术的研究成果,并讨论了这些成果的优点和不足.

2) 最后结合当前信息技术的发展趋势对所提及的安全技术进行了展望,提出了一些可能的发展方向,以期为工业控制领域的安全研究人员带来参考,从而更好地维护 ICS 安全.

参考文献:

[1] 张翔宇, 路来顺. 工业控制系统网络安全分析与研究[J]. 网络空间安全, 2019, 10(5): 114-120.
ZHANG X Y, LU L S. Network security analysis and research of industrial control system [J]. Cyberspace Security, 2019, 10(5): 114-120. (in Chinese)

[2] CLAYTON M. Stuxnet malware is weapon out to destroy Iran's bushehr nuclear plant[N/OL]. [2020-01-31]. The Christian Science Monitor. https://www.questia.com/newspaper/1P2-32547540/stuxnet-malware-is-weapon-out-to-destroy-iran-s.

[3] 王玉敏, 丁露. 工业控制系统(ICS)概述和与 IT 系统的比较[J]. 中国仪器仪表, 2012(2): 37-43.
WANG Y M, DING L. Industry Control System (ICS) overview and comparison with the IT system[J]. China Instrumentation, 2012(2): 37-43. (in Chinese)

[4] 褚健, 谭彰, 杨明明. 基于工业操作系统的智能互联工厂建设探究[J]. 计算机集成制造系统, 2019, 25(12): 3026-3031.
CHU J, TAN Z, YANG M M. Construction of intelligent Internet factory based on industrial operating system[J]. Computer Integrated Manufacturing System, 2019, 25(12): 3026-3031. (in Chinese)

[5] 姚羽, 祝烈煌, 武传坤. 工业控制网络安全技术与实践[M]. 北京: 机械工业出版社, 2017.

[6] VARGAS C, LANGFINGER M, VOGEL-HEUSER B. A tiered security analysis of industrial control system devices [C]// IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, Jul 24-26. Piscataway: IEEE, 2017: 399-404.

[7] SHEELA S J, SURESH K V, DEEPPAKNATH T. Security of industrial wireless sensor networks: a review [C]// 2015 International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15). Bangalore, India, Dec 21-22. Piscataway: IEEE, 2015: 1-6.

[8] 陈星, 贾卓生. 工业控制网络的信息安全威胁与脆弱性分析与研究[J]. 计算机科学, 2012, 39(增刊 2): 188-190.
CHEN X, JIA Z S. Industrial control network information security threats and vulnerability analysis and research [J]. Computer Science, 2012, 39(Suppl 2): 188-190. (in Chinese)

[9] PIRES P S M, OLIVERIRA L A H G. Security aspects of SCADA and corporate network interconnection: an overview[C]// International Conference on Dependability of Computer Systems. Szklarska Poreba, Poland, May 25-27. Los Alamitos: IEEE Computer Society, 2006: 127-134.

[10] 姜伟伟, 刘光杰, 戴跃伟. 基于 Snort 的 Modbus TCP 工控协议异常数据检测规则设计[J]. 计算机科学, 2015, 42(11): 212-216.
JIANG W W, LIU G J, DAI Y W. Design of Modbus TCP industrial control network protocol abnormal data detection rules based on snort[J]. Computer Science, 2015, 42(11): 212-216. (in Chinese)

[11] 赖英旭, 高春梅. 工业控制网络流量特性分析与建模[J]. 北京工业大学学报, 2015, 41(7): 991-999.
LAI Y X, GAO C M. Industrial control network traffic characteristic analysis and modeling [J]. Journal of Beijing University of Technology, 2015, 41(7): 991-999. (in Chinese)

[12] 赵勇, 廖建华, 沈昌祥. 基于访问验证的工业控制系统安全保障方法[J]. 北京工业大学学报, 2013, 39(12): 1861-1867.
ZHAO Y, LIAO J H, SHEN C X. Industry control system security assurance method based on access verification [J]. Journal of Beijing University of Technology, 2013, 39(12): 1861-1867. (in Chinese)

[13] 黄家辉. 基于攻击图的变电站控制系统脆弱性量化分析[D]. 杭州: 浙江大学, 2016.
HUANG J H. Quantitative analysis for the vulnerability of substation control system based on attack graph [D]. Hangzhou: Zhejiang University, 2016. (in Chinese)

[14] MARKOVIC-PETROVIC J, STOJANOVIC M, BOSTJANCIC R S. A fuzzy AHP approach for security risk assessment in SCADA networks[J]. Advances in Electrical and Computer Engineering, 2019, 19(3): 69-74.

[15] LI M, LI W J, YU P, ZHOU F Q. Risk prediction of the SCADA communication network based on entropy-gray model[C]// International Conference on Network and Service Management, Tokyo, Japan, Nov. 26-30. Piscataway: IEEE, 2017: 1-5.

[16] ZHU H, FU J, BAO W, et al. Quantitative safety assessment method of industrial control system based on reduction factor[C]// 1st International Conference on Intelligent Manufacturing and Internet of Things (IMIOT)/5th International Conference on Computing for Sustainable Energy and Environment (ICSEE),

Chongqing, China, Sep. 21-23. Berlin: Springer, 2018: 191-201.

[17] FU R, HUANG X, XUE Y, et al. Security assessment for cyber physical distribution power system under intrusion attacks[J]. IEEE Access, 2018, 7: 75615-75628.

[18] 黄慧萍，肖世德，孟祥印. 基于攻击树的工业控制系统信息安全风险评估[J]. 计算机应用研究，2015，32(10)：3022-3025.
HUANG H H, XIAO S D, MEMG X Y. Attack tree-based method for assessing cyber security risk of industrial control system[J]. Application Research of Computers, 2015, 32(10): 3022-3025. (in Chinese)

[19] 李玲. 列控系统信息安全渗透测试技术研究[D]. 北京：北京交通大学，2018.
LI L. Research of the penetration test on the security of the train control system[D]. Beijing: Beijing Jiaotong University, 2018. (in Chinese)

[20] 王锋. 信号安全数据网信息安全防御方案研究[D]. 北京：北京交通大学，2018.
WANG F. Research on information safety defense scheme of railway signal [D]. Beijing: Beijing Jiaotong University, 2018. (in Chinese)

[21] ABDO H, KAOUK M, FLAUS J M, et al. A safety/security risk analysis approach of industrial control systems: a cyber bowtie - combining new version of attack tree with bowtie analysis[J]. Computers & Security, 2017, 72: 175-195.

[22] VEERAMANY A, HUTTON W J, SRIDHAR S, et al. A framework for development of risk-informed autonomous adaptive cyber controllers[J]. Journal of Computing and Information Science in Engineering, 2019, 19(4): 041004-1-041004-10.

[23] YANG Y L, WANG J T, XU G A. The implementation of a vulnerability topology analysis method for ICS[J]. MATEC Web of Conferences. Paris: EDP Sciences, 2016, 44: 02032-1-02032-4.

[24] 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. A method for quantifying vulnerability of industrial control system based on attack graph[J]. Acta Automatica Sinica, 2016, 42(5): 792-798. (in Chinese)

[25] PUYS M, POTET M L, KHALED A. Generation of applicative attacks scenarios against industrial systems[C]//10th International Symposium on Foundations and Practice of Security (FPS), Nancy, France, Oct. 23-25. Berlin: Springer-Verlag, 2017: 127-143.

[26] FU Y, ZHU J, GAO S. CPS Information security risk evaluation system based on petri net[C]//IEEE Second International Conference on Data Science in Cyberspace. Shenzhen, China, June 26-29. Piscataway: IEEE, 2017: 541-548.

[27] LI B, LU R, CHOO K K, et al. On reliability analysis of smart grids under topology attacks: a stochastic petri net approach[J]. ACM Transactions on Cyber-Physical Systems. 2018, 3: 1-25.

[28] LIU X, ZHANG J, ZHU P. Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory[J]. International Journal of Critical Infrastructure Protection, 2017, 16: 13-25.

[29] MITCHELL R, CHEN I R. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems[J]. IEEE Transactions on Reliability, 2015, 65(1): 350-358.

[30] 迟强，罗红，乔向东. 漏洞挖掘分析技术综述[J]. 计算机与信息技术，2009(增刊2)：93-95.
CHI Q, LUO H, QIAO X D. Summary of defect excavation analysis technology [J]. Computer & Information Technology, 2009 (Suppl 2): 93-95. (in Chinese)

[31] 张亚丰，洪征，吴礼发，等. 基于范式语法的工控协议 Fuzzing 测试技术[J]. 计算机应用研究，2016，33(8)：2433-2439.
ZHANG Y F, HONG Z, WU L F, et al. Form-syntax based fuzzing method for industrial control protocols[J]. Application Research of Computers, 2016, 33(8): 2433-2439. (in Chinese)

[32] 孙易安，胡仁豪. 工业控制系统漏洞扫描与挖掘技术研究[J]. 信息安全与技术，2017，8(1)：75-77.
SUN Y A, HU R H. Research on vulnerability scanning and discovering technology of industrial control system [J]. Information Security and Technology, 2017, 8(1): 75-77. (in Chinese)

[33] 王欢欢. 工控系统漏洞扫描技术的研究[D]. 北京：北京邮电大学，2015.
WANG H H. Research on vulnerability scanning technology of industrial control system [D]. Beijing: Beijing University of Posts and Telecommunications, 2015. (in Chinese)

[34] 张凤臣. 工业控制设备漏洞检测系统浅析[J]. 科技与创新，2016(24)：106-107.
ZHANG F C. Analysis of vulnerability detection system for industrial control equipment [J]. Science and Technology & Innovation, 2016 (24): 106-107. (in Chinese)

[35] 杨盛明. 工业控制系统漏洞库设计与实现[J]. 电子质量，2015(12)：56-60.
YANG S M. Design and realization on industrial control system vulnerability database[J]. Electronics Quality, 2015(12): 56-60. (in Chinese)

[36] RAKSHIT A, OU X M. A host-based security assessment architecture for Industrial control systems [C] //

International Symposium on Resilient Control Systems. Idaho Falls, USA, Aug. 10-12. Piscataway: IEEE, 2010: 13-18.

[37] 李志辉. 基于对抗学习的工业控制协议漏洞挖掘技术研究[D]. 上海: 华东师范大学, 2019.
LI Z H. Vulnerability mining of industrial control protocol based on deep adversarial learning[D]. Shanghai: East China Normal University, 2019. (in Chinese)

[38] 杨凯翔. 基于模糊测试的工控网络协议漏洞挖掘方法研究[D]. 北京: 北京工业大学, 2018.
YANG K X. A vulnerability mining method for industrial control network protocol based on fuzz tesing [D]. Beijing: Beijing University of Technology, 2018. (in Chinese)

[39] 张学聪. 基于 Fuzzing 测试的电力工控系统漏洞挖掘技术研究[D]. 南昌: 南昌航空大学, 2018.
ZHANG X C. Research on vulnerability discovery of power industrial control system based on fuzzing testing [D]. Nanchang: Nanchang Hongkong University, 2018. (in Chinese)

[40] 阮涛, 钟晨, 陈银桃, 等. 一种应用于工业控制系统的模糊测试方法[J]. 自动化应用, 2015(6): 42-44.
RUAN T, ZHONG C, CHEN Y T, et al. A fuzzing method applied to industrial control system [J]. Automation Application, 2015(6): 42-44. (in Chinese)

[41] 尚文利, 万明, 赵剑明, 等. 面向工业嵌入式设备的漏洞分析方法研究[J]. 自动化仪表, 2015, 36(10): 63-67.
SHANG W L, WAN M, ZHAO J M, et al. Study on the vulnerability analysis method for industrial embedded devices[J]. Process Automation Instrumentation, 2015, 36(10): 63-67. (in Chinese)

[42] 吴波, 云雷, 金先涛, 等. 工业监控组态软件模糊测试方法研究[J]. 电子产品可靠性与环境试验, 2016, 34(3): 33-38.
WU B, YUN L, JIN X T, et al. Research on the fuzzing test method of industrial configuration software [J]. Electronic Product Reliability and Environmental Testing, 2016, 34(3): 33-38. (in Chinese)

[43] 张亚丰, 洪征, 吴礼发, 等. 基于状态的工控协议 Fuzzing 测试技术[J]. 计算机科学, 2017(5): 132-140
ZHANG Y F, HONG Z, WU L F, et al. Protocol state based fuzzing method for industrial control protocols[J]. Computer Science, 2017(5): 132-140. (in Chinese)

[44] VOYIATZIS A G, KATSIGIANNIS K, KOUBIAS S. A Modbus/TCP fuzzer for testing internetworked industrial systems[C]//2015 IEEE 20th Conference on Emerging Technologies & Factory Automation. Luxembourg, Sep. 8-11. Piscataway: IEEE, 2015: 1-6.

[45] SHAPIRO R, BRATUS S, RPGERS E, et al. Identifying vulnerabilities in SCADA Systems via fuzz-testing[M]// Critical Infrastructure Protection V. Berlin: Springer, 2011: 57-72.

[46] XIONG Q, LIU H, XU Y, et al. A vulnerability detecting method for Modbus-TCP based on smart fuzzing mechanism [C] // IEEE International Conference on Electro/information Technology. Dekalb, IL, USA, May 21-23. Piscataway: IEEE, 2015: 404-409.

[47] KIM S J, JO W Y, SHON T. A novel vulnerability analysis approach to generate fuzzing test case in industrial control systems [C] // IEEE Information Technology, Networking, Electronic and Automation Control Conference. China, May 20- 22. Piscataway: IEEE, 2016: 566-570.

[48] KIM S J, SHON T. Field classification-based novel fuzzing case generation for ICS protocols[J]. Journal of Supercomputing, 2018, 74(9): 4434-4450.

[49] WANG T, XIONG Q, GAO H, et al. Design and implementation of fuzzing technology for OPC protocol[C] // Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE Computer Society, Beijing, China, Oct. 16-18. Los Alamitos: IEEE Computer Society, 2013: 424-428.

[50] 于长奇. 工控设备漏洞挖掘技术研究[D]. 北京: 北京邮电大学, 2015.
YU C Q. The study of industrial control system device vulnerability discovery[D]. Beijing: Beijing University of Posts and Telecommu-nications, 2015. (in Chinese)

[51] 高梦州, 冯冬芹, 凌从礼, 等. 基于攻击图的工业控制系统脆弱性分析[J]. 浙江大学学报(工学版), 2014, 48(12): 2123-2131.
GAO M Z, FENG D Q, LING C L, et al. Vulnerability analysis of industrial control system based on attack diagram[J]. Journal of Zhejiang University (Engineering Edition), 2014, 48(12): 2123-2131. (in Chinese)

[52] 工业和信息化部. 工业和信息化部关于印发《工业控制系统信息安全防护能力评估工作管理办法》的通知[EB/OL]. [2017-09-09]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5761045/content.html.

[53] 李舟军, 张俊贤, 廖湘科, 等. 软件安全漏洞检测技术[J]. 计算机学报, 2015, 38(4): 717-732.
LI Z J, ZHANG J X, LIAO X K, et al. Survey of software vulnerability detection techniques[J]. Chinese Journal of Computers, 2015, 38(4): 717-732. (in Chinese)

[54] LIANG H, PEI X, JIA X. Fuzzing: state of the art[J]. IEEE Transactions on Reliability, 2018, 67(3): 1199-1218.

(责任编辑 梁 洁)