工控系统脆弱性分析研究

李 实[1],万 睿[1],周 帅[2]

(1.大亚湾核电运营管理有限责任公司,广东 深圳 518124;2.华北计算机系统工程研究所,北京 100083)

摘 要:随着工业互联网新技术在工控领域的广泛应用,工控系统由以往的孤岛模式转变为开放系统,通过网络公开的工控态势平台,可以发现大量的工控设备暴露在互联网中,工控系统面临前所未有的安全危胁。通过对工控系统的安全现状与脆弱性进行分析,站在攻击者角度提出了工控系统面临的攻击威胁。结合真实的核电 DCS 系统,通过安全测试总结此系统的脆弱性,综合考虑安全防护策略的有效性和实际可用性,对系统中相应安全脆弱点部署安全设备,提出了一种针对核电 DCS 系统的安全防护方案。通过在实验室中部署验证,证明了该安全防护措施一定程度减轻了核电 DCS 系统的脆弱性,提升了系统的安全性。

关键词:工控协议;渗透测试;网络安全

中图分类号:TP393.08 文献标识码:A DOI:10.19358/j.issn.2096-5133.2022.03.005

引用格式:李实,万睿,周帅. 工控系统脆弱性分析研究[J].信息技术与网络安全,2022,41(3):26-31.

Research on vulnerability analysis of industrial control system

Li Shi[1], Wan Rui[1], Zhou Shuai[2]

(1.Daya Bay Nuclear Power Operations and Management Co., Ltd., Shenzhen 518124, China;
2.National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: With the wide application of new industrial Internet technologies in the field of industrial control, the industrial control system has been transformed from the previous island model to an open system. Through the industrial control situation platform exposed on the Internet, it can be found that a large number of industrial control devices are exposed to the Internet, and the industrial control system is facing unprecedented security threat. Through the analysis of the security status and vulnerability of the industrial control system, this paper puts forward the attack threats faced by the industrial control system from the attacker's point of view. Combined with the real nuclear power DCS system, the vulnerability of the system is summarized through safety tests, and the effectiveness and actual availability of the security protection strategy are comprehensively considered. It can make a protection plan by adding some safety equipment. Through the deployment and verification in the laboratory, the safety protection measures have reduced the vulnerability of the nuclear power DCS system and improved the security of the system.

Key words: industrial control system; penetration test; cyber security

0 引言

随着两化融合的深入,工控系统面临的网络安全风险越来越大[1],工控系统设计之初很少考虑网络安全的问题,物理隔离的作用有限,在信息系统中,必然存在因为设计考虑不周而产生的系统漏洞,而在全球化的大趋势下,“被后门”的存在使信息系统的弱点变得更加隐蔽,且被利用导致的破坏性更强,更有目的性。

在 2021 年上半年,关键基础设施相关漏洞公开披露了超过 600 个 ICS 漏洞,其中有 70%的漏洞被归类为高危或严重漏洞,涉及市面上大多数的供应商。2 月 5 日佛罗里达州的水处理设施遭受攻击,攻击者将饮用水中的氢氧化钠含量增加了 10 倍,被工作人员及时发现,没有造成严重后果;5 月 7 日美国东海岸石油天然气运输系统遭受俄罗斯网络犯罪集团的勒索病毒攻击,造成巨大损失;7 月 12 日伊朗铁路系统遭受网络攻击;10 月 27 日伊朗加油站信息系统遭受网络攻击,影响了全国 4 300 个加油站。全球

范围内的工控系统网络安全形势十分严峻。

网络攻击不仅会造成巨大经济损失，还有可能造成巨大人员安全事故。目前国内的工业控制领域相关技术，尚不能做到“泛在彻底”的自主安全，需要相当长的过渡与发展时间。本文通过对工控系统的安全现状与脆弱性进行分析，解析了工控系统存在的普遍问题，比如系统设计缺乏网络安全考虑，核心技术受制于人，人员制度管理不完善和安全防护设备不足等；以攻击者角度提出了工控系统面临的攻击威胁，最后结合实验室的核电 DCS 系统，进行安全测试发现系统安全问题，提出了一种安全可行的核电 DCS 系统安全加固方案。

1 工业控制系统安全现状与脆弱性分析

1.1 工业控制系统安全现状

工控系统设计之初，由于其物理隔离的特性，系统设计时并没有重视网络安全问题[2]，随着越来越多新技术应用于工业场景中，工业系统逐渐暴露在互联网中[3]，据国家互联网应急中心相关监测统计，截至 2020 年 7 月暴露在互联网的工业设备已有 4 630 台，存在高危漏洞隐患的约占 40%，日均遭受超 2 万次的境内外扫描嗅探。

工控系统暴露在互联网上，造成巨大的工控安全风险，同时针对工控系统的攻击难度也越来越低，在互联网可以很轻松地找到数量众多的工控系统软硬件漏洞，诸多开源论坛、社区公开有大量的工控系统入侵案例，对攻击的详细步骤、攻击代码以及工具进行了详细说明。震惊全球的 WannaCry 病毒便是利用美国网络武器库泄露的漏洞以及工具实现的，其对超过 150 个国家，30 多万台电脑造成严重影响，直接损失超过 500 亿元。

工控系统广泛应用于涉及国计民生的关键基础设施中[4]，网络事件发生会导致严重后果，如2010 年伊朗核电站遭受震网病毒攻击，使其核计划大幅度推后；2015 年乌克兰电力系统遭受恶意软件攻击，大规模停电数小时。工控行业面临的威胁不仅仅是普通的网络攻击，由于国际形势的复杂性，“国家队”带来的威胁越来越大，例如近些年针对国内政府机构、电力与军工行业从业人员的代号为蔓灵花的攻击，其目的便以窃取敏感信息为主，具有很强的政治目的。

工控系统面临巨大安全风险，分析工控系统的普遍脆弱性，研究工控系统的安全防护方案，对工控安全有着重大意义。

1.2 工控系统的安全性分析

工业以太网技术的应用使工控系统的弱点越来越多，图 1 展示了工控系统的风险点。

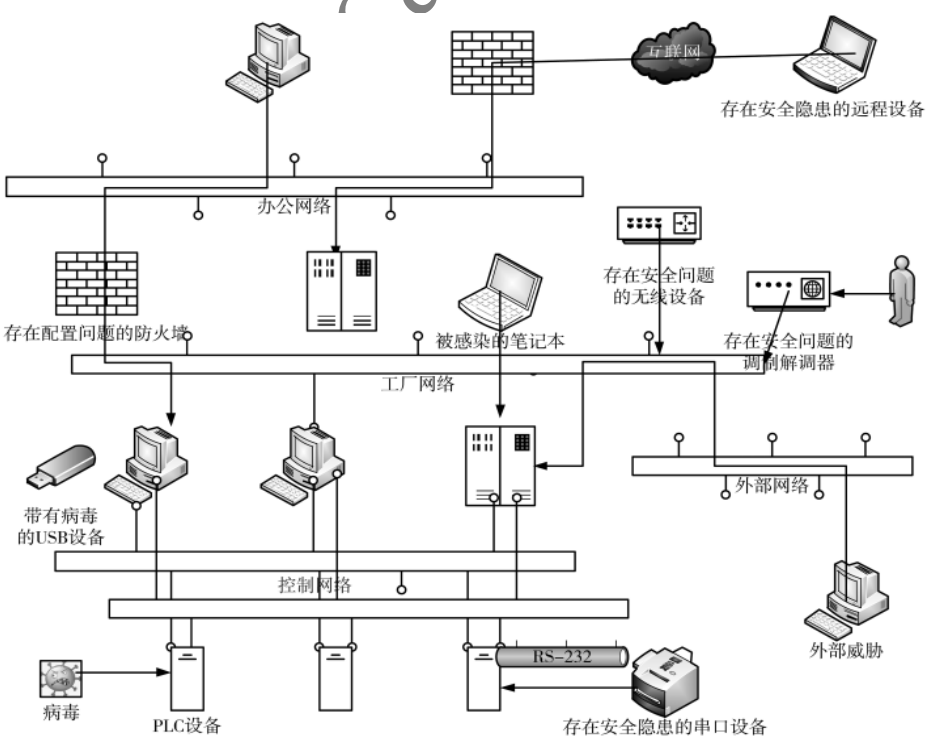

图 1 工控系统风险点

工控系统在设计之初，便欠缺信息安全方面的考虑，没有顶层的安全架构设计，缺乏整体、长远的规划[5]，核心技术尚不能做到自主安全，这些是工控系统安全的基本问题。

工控系统人员与制度管理存在脆弱性[6]。首先人作为最大的弱点，不健全的规章制度，会导致对信息系统的各种安全保护前功尽弃，目前工控系统中人员缺乏安全培训与安全意识，人员制度的管理是工控安全的关键问题。

工控系统平台安全防护设备相关的安全问题是重点问题[7]，安全防护设备不全，设备的未授权非法访问，设备通信协议的漏洞，设备的访问控制策略与设备配置不当，存储介质缺乏管理，都对工控系统平台造成了巨大威胁。工控网络方面的风险点主要在于网络机构不合理，网络边界缺失，边界防护设备设置不当，网络安全相关审计不足，无线网络[8]的安全风险等。

2 攻击者角度的脆弱性分析

工控系统由于复杂的现场与不完备的安全机制，攻击面较传统网络也更大[9]，下面讨论了几种工控系统的典型攻击点。

(1)对终端设备的直接攻击

当攻击者取得生产控制网络的权限后，便可以对终端控制设备进行直接攻击，从而导致生产失控、设备损坏等严重后果，图 2 为其攻击示意图。

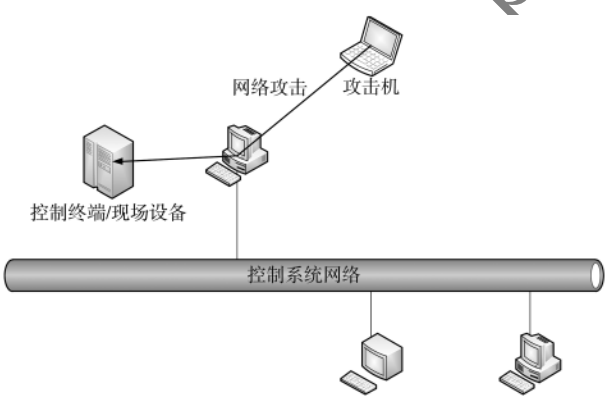

图 2 对终端控制设备进行攻击

(2)对人机接口进行攻击

HMI 在内网中，当攻击者对人机接口进行攻击后，便可获取到网络中的敏感信息，或者直接对上位工程师站、操作员站进行远程控制，从而对与其相关的设备进行攻击。其攻击示意图如图 3 所示。

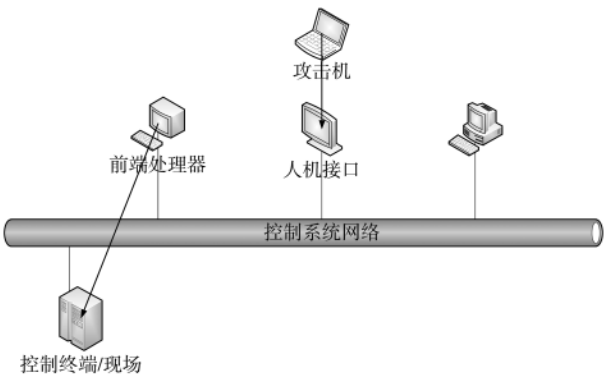

图 3 攻击 HMI 接口

(3)攻击数据库

工控系统数据库中保存系统的重要数据，并且有些工控设备运行需要的数据也保存在数据库中，对数据库进行攻击，可篡改其中数据，对控制系统造成攻击，其攻击示意图如图 4 所示。

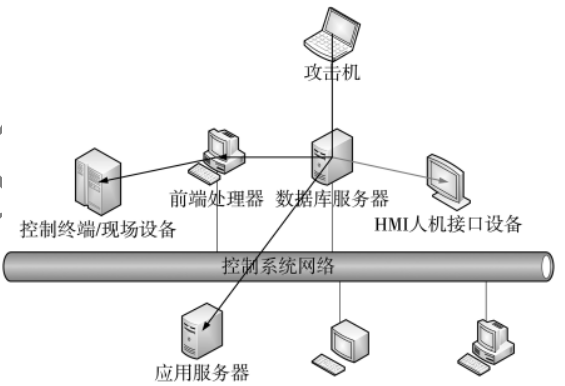

图 4 攻击数据库服务器

(4)中间人攻击

中间人攻击是一种间接入侵攻击，将攻击者控制的机器放置到两台通信设备中，对通信的两端分别建立独立的联系，并交换其所收到的数据，对通信数据进行非法篡改，使操作员无法及时看到设备实时状态，实现非法目的。其攻击示意图如图 5 所示。

(5)虚假数据注入

虚假数据注入能够利用系统对数据合法性检测不足的漏洞，篡改状态结果，特别对于电力行业[10]，后果会很严重。虚假数据注入主要是在量测值中注入虚假数据攻击向量，使非法数据可以通过数据监测，从而使系统运行在错误的状态，而数据监测并没有报警。

(6)PLC 蠕虫病毒[11]

工控内网环境下，由于缺乏杀毒措施，病毒的

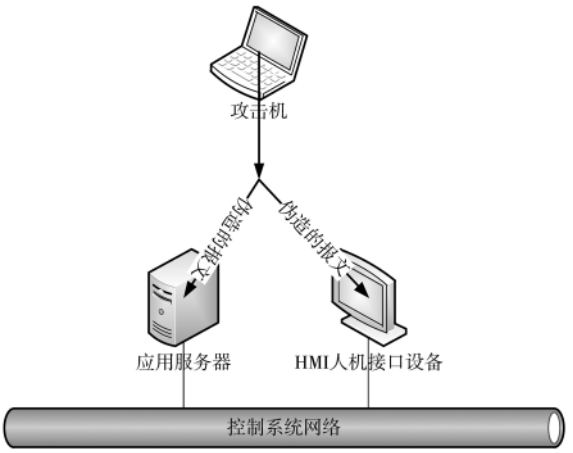

图 5 中间人攻击

破坏力十分巨大，一些经过设计的蠕虫病毒，会在内网中自动传播复制，造成网络与设备故障。蠕虫病毒首先选择 IP 尝试连接，如果建立连接成功，则检查其是否已被感染；若连接不成功或者已被感染，则选择新的 IP 重新尝试连接；若未被感染，则下装病毒程序，重启目标 PLC 重复此过程。

3 工控系统安全防护

3.1 核电 DCS 系统结构

上文对工控系统的脆弱性进行了分析，本节结合实验室环境，对核电行业工控系统进行安全分析。实验室核电 DCS 系统[12]整体结构主要包括法国 AREVA 提供的安全相关仪控系统 TXS 与德国西门子的正常仪控系统 SPPA-T2000，其结构图如图 6 所示。

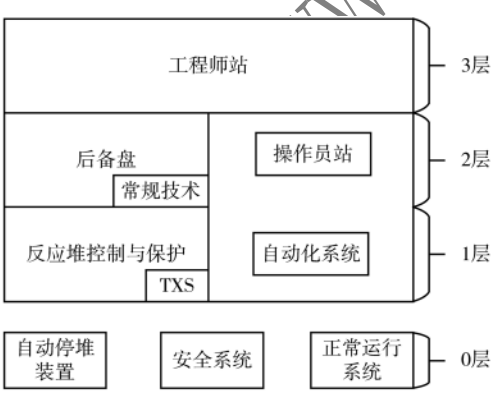

图 6 核电 DCS 系统

其中 0 层为现场接口层；1 层为系统自动化层，主要执行现场设备的数据采集与处理，对现场设备自动控制；2 层为机组监督控制层，是一个人机接口层，对机组进行监测控制与信息显示；3 层为厂级管理层，通过采集实时数据，为全厂生产过程提供综合优化服务及实时监控信息。

3.2 核电 DCS 系统脆弱性

结合工控系统的安全性分析与攻击者角度的脆弱性分析，本节针对实验室的 DCS 系统进行脆弱性分析。

(1)DCS 终端控制器遭受攻击

通过对实验室的终端控制器进行安全分析，发现部分设备通过西门子的专用通信模块进行网络交互，通过 MAC 地址进行寻址，而通信明文传输，对通信协议没有解析过滤，可构造异常数据对终端控制器直接进行攻击。

(2)工程师站存在漏洞

对系统中的主机进行扫描探测，主机存在多种可利用漏洞，由于业务稳定性需求，尚未进行漏洞修复，在内网中可利用其漏洞对工程师站进行攻击。

(3)工控设备无认证加密

上位机与下位机通信缺乏必要的身份鉴别和认证机制，只要能够从协议层面与下位机建立连接，就可以对下位机进行修改，缺乏对系统最高权限的限制，高权限账号往往具有掌控系统和数据的能力，因此，任意一种非法操作都会导致系统瘫痪。缺乏有效的审计和事后追溯工具，责任划分和威胁追踪十分困难。

(4)终端主机无安全防护

系统中主机对传入文件缺乏审计与控制，对系统中传入可执行文件，未能及时隔离处置，可随意执行。

(5)未限制接入地址且部分主机存在弱口令

未对设备接入地址进行限制，接入设备设置 IP 在同一网段中，便可访问其他设备；部分设备存在弱口令，通过口令爆破可获得其权限。

3.3 系统安全防护

工控系统安全防护存在很多难点[13]，工控系统对安全性、鲁棒性、实时性、可用性要求较高。系统更新修复困难，一般不允许重启关机，一但停止运行后果可能是无法接受的。工控场景中设备计算能力、存储资源都有限，环境也较为恶劣，设备都要求简单可靠，难以添加复杂的安全设备。

通过对系统中的设备进行安全测试，发现系统存在的安全问题，总结防护增强点[14]，并在实验室中部署相关安全设备，图 7 为实验室安全设备接入拓扑示意图。

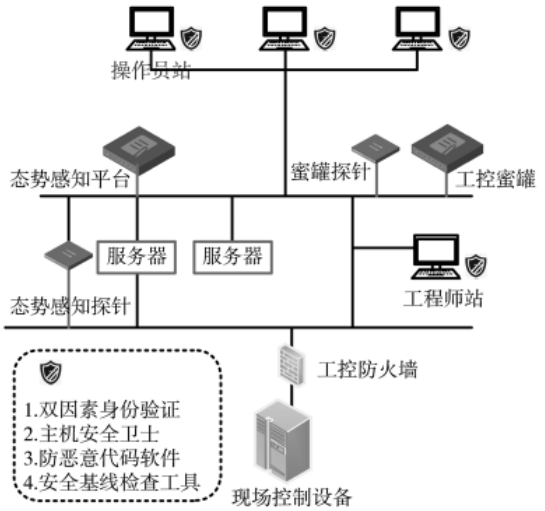

图 7 实验室安全设备接入拓扑示意图

(1)面对工控终端设备被直接攻击的威胁,需要对终端设备进行一定防护,比如在终端设备设置工控防火墙、工控蜜罐等安全设备。

在二层部署 MongoDB 蜜罐,诱导攻击者对蜜罐发起攻击,在实验室中通过正常连接 MongoDB 数据库,在蜜罐中可检测到对 MongoDB 蜜罐的具体操作行为,图 8 为部署工控蜜罐检测到的信息。

通过在攻击者入侵的关键路径上部署诱饵和陷阱(蜜罐),诱导攻击者转移攻击目标,进入与真实网络隔离的蜜网,让攻击者在蜜网中攻击“假”目标,获取虚假数据,从而拖延攻击时间,间接保护真实资产。在此过程中,蜜罐能完整记录攻击者行为,捕获高级未知攻击(比如基于 0day 的 APT),并且可以对攻击者做身份溯源,为防守方提供先人一步的主动防御手段。

(2)面对 HMI 接口设备的攻击威胁,工控系统人机接口设备需要部署安全软件,防止遭受攻击被控制,导致敏感信息泄露或者对系统进行非法操作。同时系统需要部署安全检测平台例如态势感知平台,对系统中的非法操作进行及时报警,及时处理。

在系统中部署态势感知平台,并且接入蜜罐接口信息,对整个系统的行为进行监控审计,当人机接口等内部设备面对攻击行为时,及时给予报警并及时处置。

工业网络安全态势感知平台能够识别到 PLC 的漏洞、固件版本、代码、配置变更、状态信息等一系列有价值的内容,从而获得对资产的可视化、漏洞风险评估能力以及掌控能力。

(3)工控系统中的数据库与数据如果被攻击、篡改或者遭虚假数据注入,可能对工控系统造成巨大影响。在数据传输中,可采用国密算法对数据进行加密,考虑到传输与加密的消耗,可采用对数据部分字段加密的方法,保证数据传输与存储的安全性;为增强信息系统的“安全可控”,在系统中采用应用国密算法的设备,推动国产密码在重要领域的应用。实验室中终端设备应用基于国密算法的 USBkey。

密码算法是保障信息安全的核心技术,为从根本上摆脱对国外密码技术和产品的过度依赖,采用基于国密算法的设备对系统的安全性有着极其重大的意义。

(4)面对 PLC 蠕虫病毒在内网的传播,内网设备可以配置主机安全软件,通过对系统中的文件、程序进行审计,并安装防病毒软件定期进行补丁更新,确保系统的安全性。

在工控系统中应用主机卫士,采用白名单策略对系统中的应用进行管理,可以有效降低恶意程序在系统中的传播。实验室中通过安装主机卫士,勒索病毒、蠕虫木马在系统中都无法执行,系统安全

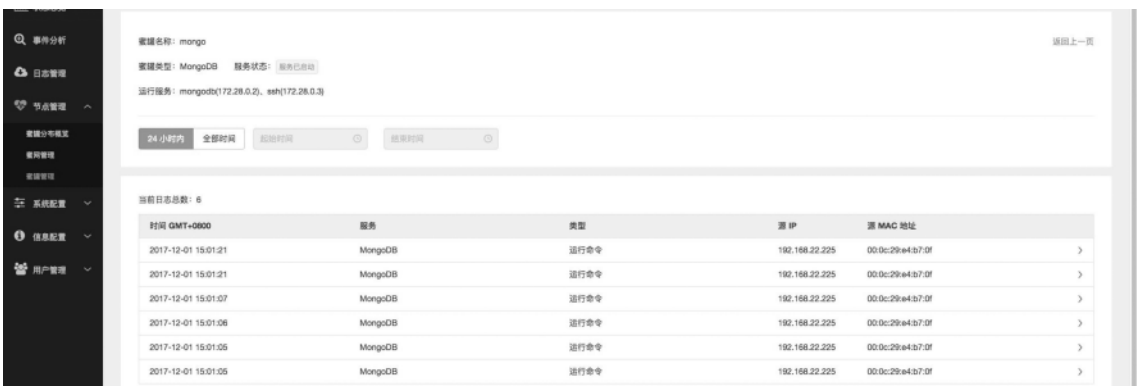

图 8 mongodb 蜜罐攻击检测

性得到提高。

核电站网络中的应用系统存在的任何不合规配置以及安全风险，一旦被恶意攻击者利用将导致严重的灾难性后果，而网络中的不合规配置与风险暴露面正是会造成这种风险的最大问题之一，安全基线设置是否严格以及是否产生变化成为防范恶意攻击的最后一道防线。实验室中通过基线检测工具对系统进行扫描，发现系统配置问题，对其进行整改，进一步提高系统的安全性。

(5)工控系统的防护还需要禁止非法外联。由于工控系统的特殊性，首先要对系统从规章制度和地址限制两方面进行管理，避免非法外联。

双因素身份认证系统在边界层设置凭证，防止入侵者通过网络化和非网络化方式非法进入终端系统。这一层的防御构架具有强口令身份认证识别功能。通过在实验室部署基于国密算法的双因素身份验证系统，实现对系统登录使用的管理，有效控制了系统非法操作。

4 结论

本文通过对工控系统进行安全性分析，指出工控系统的一些易受攻击的脆弱点，包括工控设备与工控终端安全防护不足，数据传输过程保密性完整性验证缺失，人员访问控制管理存在漏洞，内网设备对文件的上传缺乏管控等；并结合实验室环境中的核电 DCS 系统，对其进行安全测试，总结核电工控系统的脆弱性与修复方案；最后在实验室中针对系统的安全问题，提出了一套核电 DCS 系统的加固方案，包括终端节点的蜜罐旁路部署，工控防火墙的加装，态势感知平台的部署，设备主机卫士的安装，系统中设备的基线扫描，以及双因素登录验证，对工控系统进行全方位的安全加固。

工控系统有其独有的特点，对于工控内网的网络防护，需要慎之又慎[15]。工控系统的安全防护，既要考虑安全性，还要考虑对系统业务的影响，需要经过严格的实验测试，进行可行性验证。核电领域生产运行严重依赖国外的设备与技术，基于工控系统脆弱性研究，在核电领域构建全面整体的信息安全防护体系有着重大意义。

参考文献

[1] 张东华.火电行业工控系统信息安全关键技术研究[J].物联网技术，2021，11(9)：79-81，86.

[2] 王文宇，刘玉红.工控系统安全威胁分析及防护研究[J].信息安全与通信保密，2012(2)：33-35.

[3] 徐伟，孔坚，毛庆梅，等.工业控制系统安全现状及应对策略[J].网络安全技术与应用，2021(9)：115-117.

[4] 卢慧康.工业控制系统脆弱性测试与风险评估研究[D].上海：华东理工大学，2014.

[5] 晋成龙，桂宗能，王媛媛.水利工程工控系统网络安全及防护设计[C]//2021(第九届)中国水利信息化技术论坛论文集，2021.

[6] 尹峰.浅析电力企业工控系统风险和防御[J].大众用电，2017(S1)：148-150.

[7] MCLAUGHLIN S，KONSTANTINOU C，WANG X，et al. The cybersecurity landscape in industrial control systems[J].Proceedings of the IEEE，2016，104(5)：1039-1057.

[8] LI X，LI D，WAN J，et al.A review of industrial wireless networks in the context of Industry 4.0[J]. Wireless Networks，2017，23(1)：23-41.

[9] ATTAULLAH H M，KHAN R A，MUGHAL S.Cyber security for industrial control system-a survey[J].iKSP Journal of Emerging Trends in Basic and Applied Sciences，2021，1(1)：15-21.

[10] 赵俊华，梁高琪，文福拴，等.乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J].电力系统自动化，2016，40(7)：149-151.

[11] 张帆.PLC 蠕虫病毒的实现与防护[J].信息与电脑(理论版)，2019，31(21)：183-185.

[12] 黄辉明.EPR 核电机组 DCS 控制系统构架及设计[J].中国新通信，2020，22(4)：104-106.

[13] 陶海.工控系统安全防护问题对策研究[J].现代工业经济和信息化，2017，7(19)：54-55.

[14] 张敏，张五一，韩桂芬.工业控制系统信息安全防护体系研究[J].工业控制计算机，2013(10)：25-27.

[15] 王云龙.工业控制系统添加信息安全设备的兼容性研究及测试[J].电子技术与软件工程，2021(5)：238-240.

(收稿日期：2021-11-16)

作者简介：

李实(1985-)，男，硕士研究生，高级工程师，主要研究方向：工业自动化、网络安全。

万睿(1976-)，男，本科，工程师，主要研究方向：工业自动化。

周帅(1994-)，男，硕士研究生，助理工程师，主要研究方向：工控信息安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所