工业控制系统网络安全的主动防御技术研究与实践*

石永杰[1],于慧超[1],吕　峰[2],张　畅[3],吴亚萍[3]
(1.中国石油天然气股份公司西北销售公司,甘肃 兰州 730070;
2.中国石油天然气股份公司北京油气调控中心,北京 100007;
3.北京启明星辰信息安全技术有限公司,北京 100193)

摘　要:传统的以安全产品构成的"封、堵、查、杀"的被动式的安全防御难以面对日益严重的工业控制系统的定向网络攻击安全事件,构建以业务为核心的网络安全防御体系,方能确保所保护的工业控制系统应用环境的可用性与稳定性。从威胁主动发现、威胁主动抑制以及工业诱捕系统等技术进行研究,构建工业控制系统的主动防御系统,并实践于真实的工业控制系统应用环境。系统以面向业务安全运营的态势感知系统为控制中心,与融合 AI 技术的智能 AI 工业防火墙、智能主机安全防护系统、工控诱捕系统等智能检测与防御安全设备实现智能防御联动的威胁闭环控制与处理的机制。

关键词:工业控制系统;网络安全;主动防御;工控诱捕系统
中图分类号:TP393　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.04.003
引用格式:石永杰,于慧超,吕峰,等.工业控制系统网络安全的主动防御技术研究与实践[J].信息技术与网络安全,2020,39(5):13-18.

Research and practice of active defense technology in ICS cyber security

Shi Yongjie[1],Yu Huichao[1],Lv Peng[2],Zhang Chang[3],Wu Yaping[3]
(1.Petrochina Northwest Marketing Company,Lanzhou 730070,China;
2.Petrochina Oil & Gas Pipeline Control Center,Beijing 100007,China;
3.Beijing Venus Cyber Security Technology Co.,Ltd.,Beijing 100193,China)

Abstract:The traditional passive security defense of "sealing,blocking,checking,and killing" constituted by security products is difficult to face increasingly serious directed network attacks against the relatively closed industrial control system,and build a business-oriented network security defense system can ensure the availability and stability of the protected industrial control system application environment. We combine technologies such as active threat detection,active threat suppression,and industrial trapping systems to build an active defense system for industrial control systems and deploy it in a real industrial control environment to verify its effectiveness. Our system takes the situation-awareness system for business security operations as the control center,and combines intelligent detection and defense security equipment like industrial firewalls,host security protection systems and industrial control trapping systems that incorporate AI technology to achieve intelligent closed-loop threat control and processing.

Key words: industrial control system;network security;active defense;industrial control trapping system

0　引言

目前国际网络空间日益复杂。分析伊朗核电站、2019 年委内瑞拉电瘫痪等网络安全事件,从"网络利用"到"网络攻击",对目标工控网络进行破坏和摧毁的威胁越来越严重,网络攻击频次逐年增加,网络威胁程序长久潜在目标系统。我国工业控制系统目前主要依赖国外工业产品来构建,保护我国关键信息基础设施免受潜在的网路威胁显得十分急迫。传统的以安全产品构成的"封、堵、查、杀"的被动式的安全防御难以抵御潜伏的威胁,必须开展主动防御,面对高能力网络空间威胁行为体方能达到防患于未然。

*基金项目:工信部 2018 年工业互联网安全集成创新应用试点示范项目:面向油库安全运营的工业互联网态势感知系统。

www.pcachina.com

1 针对定向的工业控制系统的网络攻击特点与主动防御策略

1.1 新的网络空间时期的网络定向攻击的特点

在新的网络空间时期,网络攻击已成为另外一场没有硝烟的战场,其危害并不逊色于真实的物理战争,新的网络空间格局下的定向网络攻击的特点表现在:

(1)重大特殊时期的定向攻击的频次越来越高

2020 年 COVID-2019 疫情期间,有组织针对我国关键基础设施定向网络攻击频度增加,威胁越来越大,给我国的抗疫工作增加了严重的干扰,并造成损失。

(2)定向网络攻击的监测越来越高

随着有组织攻击技术手段不断提升、对社会工程学的利用以及攻击者的身份越来越隐蔽,使得网络攻击的实时监测与溯源变得越来越难。

(3)有组织网络攻击越来越明显

2019 年针对委内瑞拉的电力设施的攻击、2020 年新冠疫情期间针对我国的视屏系统的攻击等事件分析,一些敌对势力有组织入局、有目的和定向的攻击确定性越来越大。

(4)网络攻击的范围与涉及的领域越来越广

随着大规模定向网络攻击倾向越来越明显,涉及民生市政、核心工业生产、能源与军工,甚至太空领域的网络攻击屡见不鲜。美国国家基础设施咨询委员会(NIAC)多次公开强调"国家(美国)不足以抵抗敌对组织的针对关键基础设施等敏感网络系统的攻击性策略"已充分说明这一特性。

1.2 我国工业控制系统特有的威胁

目前,我国的工业控制系统尤其是在役的系统,绝大部分还是使用 Siemens、Honeywell、Rockwell、Yokogawa 等,即使目前我国的本土企业产品已在一些关键基础设施领域成功应用,能够解决我国"卡脖子"、"内置后门"等问题,但同样面临诸多漏洞等威胁,某种程度上存在比国外系统更多的安全隐患。诸如:

(1)操作系统、编译系统、IEC61131 设计软件等安全漏洞;

(2)防病毒及恶意软件的管控漏洞;

(3)使用 U 盘、光盘等外接设备的管控缺失;

(4)设备维修时,移动设备存在随意接入的情况;

(5)工控系统网络边界越来越模糊且防护不充分;

(6)访问和接触控制(包括远程访问、管理维护)薄弱;

(7)工控软件生命周期的安全管理漏洞;

(8)缺乏安全事件应急响应机制。

1.3 针对定向攻击的主动防御策略

目前,针对工业控制系统网络安全建设主要以满足 GB/T22239-2019 等保 2.0 标准体系的合规性为目的[1-3],但近几年的网络攻击更趋于定向性、隐蔽性,攻击手段多元化、技术多样化等特点,需要超越基础合规的主动动态防御策略:变被动防护为主动防护,变静态防护为动态防护,变单点防护为整体防控,变粗放防护为精准防护、粗粒度的防御能力转变为细粒度的主动防御能力,且具备事前预防、事中响应、事后审计的整体网络联动,能识别未知威胁并做研判,才能有效抵御有目的、定向的未知网络安全攻击。主要的策略包括如下几个方面:

(1)基于内生安全的基础安全

根据工控系统"高实时、资源受限、私有协议众多"的特点,梳理工控资源资产的数量、配置及策略,各资源资产的 CIA 关系;同时,从攻防视角,对工控系统脆弱性进行模块级分析,如对模块功能逻辑、执行语句进行数据篡改、伪造指令、实时欺骗以及获取超级权限等。同时,梳理工控网内完整的资产信息,确保无可利用"暗资产",利于漏洞应急和资产地图的快速查询筛选,并实时更新的列表。

(2)基于攻防与反制思维的网络安全建设

以攻击方、黑客入侵渗透的角色和思维,研究梳理工控系统的目标侦查、木马病毒投放、攻击漏洞利用、操作控制权获取、敏感数据窃取、攻击路线、攻击逃逸与证据销毁及其相应的反制技术,构建攻击与防御对抗的网络安全建设路线,并建立应急专家知识库。

(3)基于攻防的主动联控层面

网络安全主动防御的本质是对抗,而对抗的本质在攻防两端技术手段、资源整合、协调能力等方面的较量,以主动/被动采集、监测定向攻击轨迹、控制权获取等完整的情报收集,并以情报驱动的积极防御和进攻行动,做到实时的整体主动感知态势,并策略执行应急阻断和高效协同指挥决策,持续闭环的安全 PDCA 提升。智能联动闭环防御控制示意图如图 1 所示。

www.bcachina.com

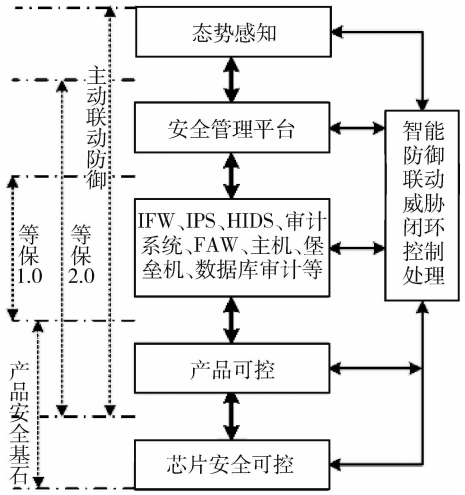

图 1　智能联动闭环防御控制示意图

2　工业控制系统主动防御的关键技术与具体措施

现代网络攻防空间中,有组织入局的攻击方具有较高的攻击成本资源,攻防双方往往处于绝对不对等的状态,产生的后果也往往是灾难性的。为此,在基础结构安全和全面纵深防御的基础上,建立并落实资产管理、漏洞管理、漏洞分析、补丁分析、补丁验证等全方位的安全运行机制,通过对信息的汇聚和分析,建设全面持续的动态监测系统,实现全天候全方位的态势感知能力[4-5],同时结合内外部威胁情报,及时发现威胁,通过将网络安全能力、信息技术基础设施和业务应用系统等深度融合,并依靠安全运营、应急响应与处置系统等手段进行威胁猎杀,达到及时止损的目的。在工业控制系统主动防御的实践中,每一个防御动作需要威胁辨识、分析、控制、排除威胁等包含终端以及网络的网元在内的协同。

2.1　基于 AI 技术的轻量级工业主机主动安全防御技术

在工业控制系统中,工业主机由于大部分采用通用架构与通用操作系统等,同时由于其特殊使用用途和要求,一般不会轻易进行系统升级以及补丁更新等,往往就成为被病毒感染与遭受网络攻击的主要目标,如蠕虫病毒攻击过程首先是感染目标主机,再自动扫描、发现漏洞、自动传播等。从纵深与主动防御的角度,工业主机安全防护应当具备查、杀病毒功能,并同时具备“黑名单”和“白名单”,为了保持控制系统的可用性,不能采用实时采样及全盘扫描技术,在隔离离线杀毒过程中又不能破坏原有应用程序完整性,可以基于 AI 自学习自动分类建模生成白名单规则库,根据规则进行智能匹配,以此更准确、更高效地建立工业控制系统的可信系统,能最大程度降低误报和误判,避免误将病毒木马等加入白名单的风险。基于 AI 分类建模算法可以实现“自动策略生成、数据正向反馈、AI 干涉修正、威胁情报辅助”的全闭环管理模式,以此保障工控工作站、服务器的可用性、可靠性和可信性。

另外,采用基于主机的入侵检测技术,实时监控目标主机所在网络的实时连接情况和审计处理系统日志。通过对进入目标主机的所有数据流量实时采集、分析,并与攻击特征库进行匹配,一旦发现异常行为特征,及时报警处理或阻拦,以达到保护目标主机的目的。

2.2　工控诱捕系统技术

为实现主动防御,需要在工业互联网企业的入口处以及工业控制系统的入口处分别部署诱捕系统,构成联动的诱捕网络。由于工控诱捕系统的特殊性,本文仅就工控诱捕系统进行阐述。

工业控制系统的“白名单”策略只隔离了不信任的行为数据,缺乏对这些数据的分析和研究,造成与攻击者的信息不对称的情况;工控安全审计检测旁路部署,存在流量丢包、类型不全和误报率高而难以防范复杂攻击。工业环境网络相对隔离,无法自动实时更新特征库,也会造成攻击检测的严重滞后。工控诱捕系统便可作为以上防护不足的有效补充,通过模拟工控系统网络运行环境,构建陷阱主机,提供陷阱网络服务,诱导诱惑内外部入侵者进行攻击,以此捕获攻击方式与路径,延缓对真实工控系统的入侵,发挥着主动防御的作用。

工控诱捕系统以诱捕系统技术和主机监控技术为基础,结合流量转发技术和软件定义网络(SDN),构建前端部署轻量化可定制的流量探针节点,将可疑和攻击流量转发至后端诱捕系统集群网络。工控诱捕系统由仿真诱捕系统资源层、数据层和平台层三部分构成,如图 2 所示。其中,仿真诱捕系统资源层起到吸引和诱捕攻击作用,并将攻击数据发送到数据层进行分析和存储;数据层用于对攻击数据进行存储和分析、对接安全情报数据,聚合形成攻击事件和数据统计报分析;平台层用于对数据进行展示,管理系统各个节点。工控诱捕系统的技术架构与分析引擎分别如图 2、图 3 所示。

www.bcachina.com

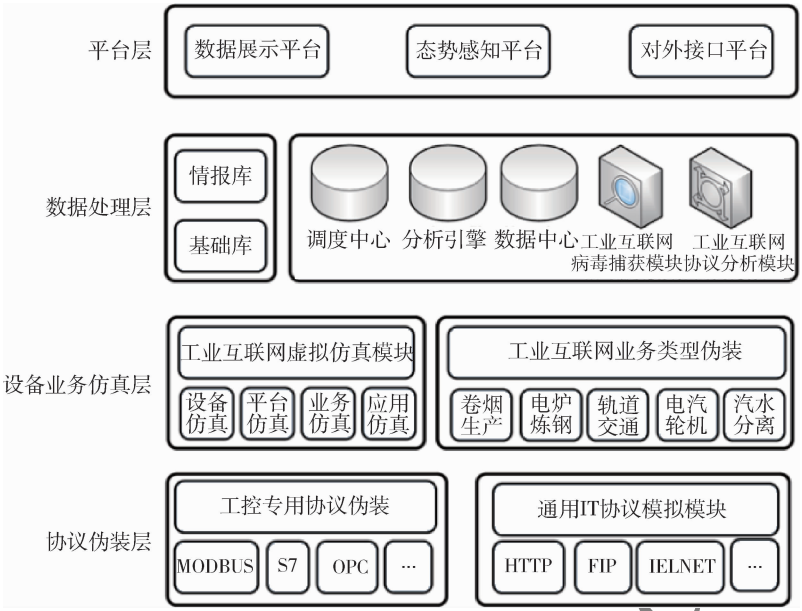

图 2　工控诱捕系统技术架构图

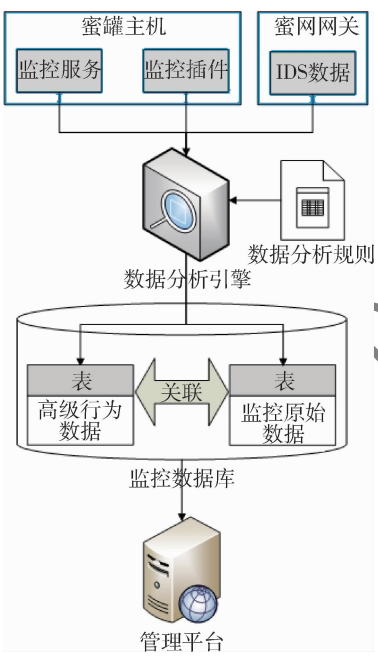

图 3　工控诱捕捕系统数据分析引擎

流量探针节点将网段内可疑访问流量(例如特定目的 IP、端口或协议的)引导至到后端诱捕网络的主机,实现诱捕系统网络的轻量级快速部署和可控性,增大诱捕攻击面,有效降低诱捕网络的部署和维护成本。

诱捕网络由大量的诱捕探针节点和路由网关构成,以高仿真高交互蜜罐技术为基础,并结合自身业务特性组成。模拟工控系统真实的应用业务环境,同时诱捕网与真实内网环境相互协调,以此提升欺骗环境真实性,快速精准定位攻击事件,并结合流量分析设备,降低攻击定位中存在的滞后性及误报高等问题,起到真正的诱捕作用,保护正常业务。

诱捕系统机包括高交互诱捕系统和低交互诱捕系统,根据下发的业务方针策略自动构建的业务仿真环境,包括操作系统、应用软件、开放服务及端口等内容,是迷惑诱捕攻击者的核心关键。特别是以捕获深度真实攻击行为为主要目的的高交互诱捕系统主机,还包括文件监控、进程监控、网络监控和控制台监控等,可在驱动层实现主机数据监控,包括样本上传、创建可疑进程、非授权网络访问以及远程 SHELL 交互内容等关键数据项监控。

2.3　自适应动态策略 AI 边界防护技术

工业控制系统内部的访问与连接相对固定,通信流量具有周期性的变化等特点,使得在工业控制系统网络内部建立自适应动态策略 AI 边界防护成为可能。由于工控系统的内网节点访问关系相对固定,使得高级威胁入侵者一旦进入控制系统内网就会导致任何单点环节失陷或失效;同时随着两化融合的深度推进,分系统之间的边界越来越模糊,高级威胁入侵造成的危害更大,借助于自学习的模式,采用人工智能技术,实现自适应动态策略的 AI

边界防护势在必行。

自适应动态策略的 AI 边界防护的核心是边缘安全的智能化,就需要工业防火墙内置基于神经网络构建的 AI 高级威胁检测模型,不再依赖外部部署的大数据分析平台,在防火墙本地即可精准发现高级威胁,需要包括 ECA(恶意加密流量不解密)识别、恶意软件非法连接远控服务器行为识别、暴力破解恶意行为识别、工业协议深度解析(DPI)、工业流量深度解析(DFI)等,以此提高威胁检出率和降低误报率,确保与管理中心、IPS、诱捕系统等智能联动。另外,动态策略调整需要通过安全管理中心远程遥控方式下发新的防护策略和应用能力,保证安全业务按需动态调整,需要工业 AI 防火墙内置轻量诱捕系统,并通过安全管理中心协同联动,实现大规模轻量诱捕、动态引流与诱捕蜜网深度融合联动,实现针对不存在 IP 和未开放端口诱骗的全面监控,提升对更隐蔽、更致命的威胁的辨识与处理。联动闭环控制图如图 4 所示。

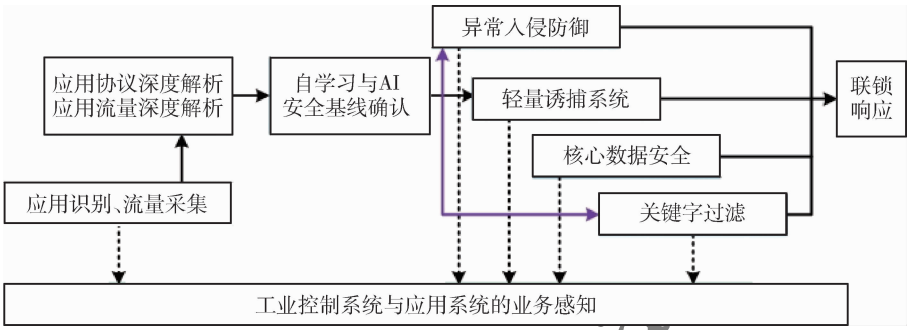

图 4　诱捕蜜网与自适应动态策略的边界防护联动控制图

2.4　主动安全防御体系的态势感知

工控态势感知集检测、预警、响应处置等功能于一身,是主动防御体系中的安全大脑和“指挥中心”,实现对攻击、威胁、流量、行为、运维和合规等态势进行全维度的感知,实现全网的安全风险态势感知、事件响应以及资源协同联动,实现“预知未来、主动发现、协同防御、智能进化”的智能主动安全防御能力[3]。

针对工控网络高实时、资源受限、私有协议众多的特点,需要多视角态势感知方法(如基于控制系统内生安全、CPS 异常检测[6]、APT 攻击检测和仿真诱捕产生的报警信息),通过多视图学习方法从多源报警中提取并优化攻击策略,降低单种类型报警系统的误报率。围绕攻击网络存在的漏洞,通过建立攻击者、防御者和内部人员三方博弈的动态数学模型,预测攻击者的最佳攻击时机[7-8]。基于工控业务背景、攻击时机和系统风险构建工控网络安全态势,监控网络内的敏感操作行为,如图 5 所示。

3　工业控制系统主动防御之实践

为进一步提升油库发油生产系统的安全防护能力,中国石油西北销售公司成功申报了工信部 2018 年工业互联网试点示范项目《面向油库安全运营的工业互联网安全态势感知系统》[6],采用基于工控诱捕系统、基于 AI 技术的主机防御等技术,在核心业务多样性、攻击事件频发的大背景下,快速实现业务性能异常检测。其中业务性能监控包括日志数据、应用系统追踪文件和全面的性能监控指标等,通过对这些数据的实时分析和回溯分析,实现细粒度的实时监控和全栈式视图保障其核心业务的稳定运营以及智能化的安全运营。

安全运营的核心是提升安全智能运维的水平,提高企业网络安全应急处理的能力。在大量数据分析的场景下,结合机器学习、深度学习等技术,利用海量、实时、全栈的监控数据,通过 AI 算法,提出问题定位和运维决策的建议,缩短 MTTR(平均故障恢复时间),并通过迭代提高分析和决策的准确性,快速定位网络威胁点并予以智能消除,以此克服网络安全运维部门面对海量采集数据大量依赖人工分析的瓶颈。

在油库发油工控系统中的流量异常以及应用服务异常现象中,常常潜伏着一些攻击行为或安全事件,系统通过对发油工业控制系统进行全流量数据采集分析,并智能调用安全规则库,对异常行为进行报警。通过结合大数据挖掘和智能化分析技术,将攻击者的整个攻击过程归纳为侦察扫描、定

www.pachina

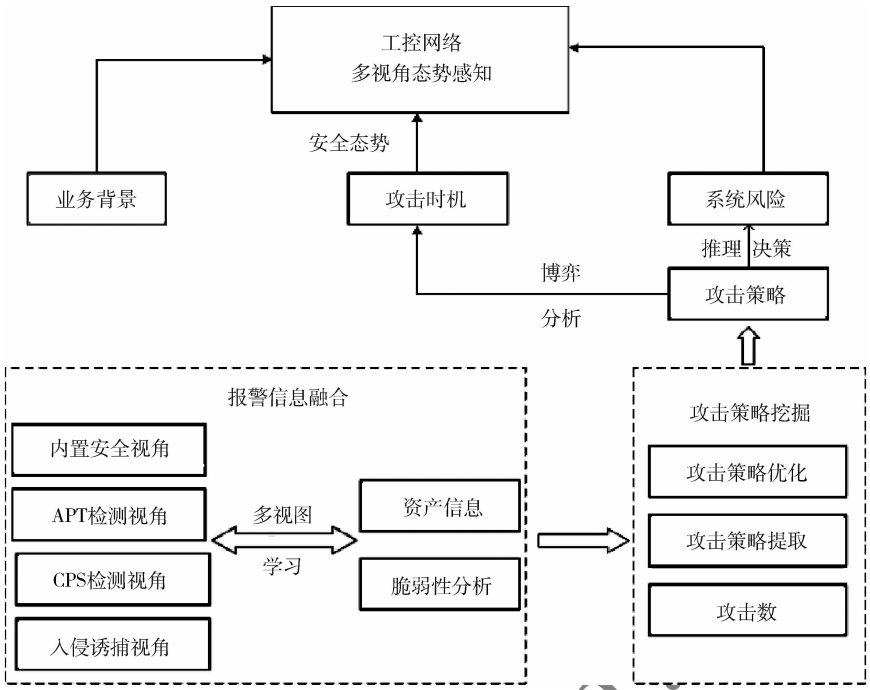

图 5　主动防御体系的工控态势感知系统

向攻击、攻陷入侵、工具安装、恶意行为五个阶段，展示整个动态攻击过程和攻击效果，实现基于全网络的流量安全监测分析。另外，系统结合漏洞库对扫描到的各类资产进行漏洞分析并告警；利用高速率报文存储检索系统完成对历史网络流量的回放和追溯，快速还原攻击过程，为网络管理人员及时调整管理策略提供技术支撑。

2019 年，中石油针对该公司管辖下的三座油库进行实战攻防，利用相关技术构建的工业互联网态势感知系统能够实时感知威胁攻击，并对某些隐蔽的、未知类型的攻击进行实时跟踪与取证，予以有效拦截，有力阻断了针对实际生产环境的工业控制系统的定向攻击，达到了智能安全运营的目的。

4　结束语

工业控制系统安全防护的重点需要以其业务运行安全为中心，以保障其可用性为前提，其主动安全防御能力需要与物理、网络、系统、应用、数据与用户等各个层级深度结合，并将网络安全防御能力部署到信息化基础设施和信息系统的每一个业务环节，建设以态势感知为核心的威胁情报驱动的动态主动防御能力体系，将安全管理与防护措施落实到其全生命周期的每一个阶段，并将态势感知驱动的实时防护机制与系统运行维护过程深度融合，实现主动协同联动的实战化运行和现常态化的威胁主动发现与自适应智能响应处置，渐进提升整个工控网络安全主动防御水平。

参考文献

[1] GB/T. 22239-2019. 信息安全技术网络安全等级保护基本要求[S]. 2019.
[2] GB/T. 25070-2019. 信息安全技术网络安全等级保护安全设计技术要求[S]. 2019.
[3] GB/T. 28448-2019. 信息安全技术网络安全等级保护测评要求[S]. 2019.
[4] 石永杰. 工业互联网环境下 IT /OT 融合的安全防御技术研究[J]. 信息技术与网络安全,2019,38(7):1-5
[5] 陶耀东,贾新桐,崔君荣. 工业互联网 IT/OT 一体化的安全挑战与应对策略[J]. 电信网技术,2017(11):8-12.
[6] 彭浩,阚哲. 蓄意攻击策略下信息物理系统的级联失效及安全评估[J]. 郑州大学学报,2019(51):13-21.
[7] 张大松,姜洪朝,吴云峰. 火电工控系统网络安全防护方案设计[J]. 信息技术与网络安全,2020,39(3):17-22.
[8] 江泽鑫. 电力物联网信息安全防护技术研究[J]. 信息技术与网络安全,2020,39(2):31-36.

(收稿日期:2020-03-28)

作者简介:

石永杰(1967 -)男,硕士,高级工程师,主要研究方向:成品油库自控系统、工控防护、信息安全规划等。

于慧超(1986 -),男,本科,工程师,主要研究方向:信息安全、工控安全防护及系统运维等。

吕峰(1969 -),男,硕士,高级工程师,主要研究方向:油气管道自控系统和网络安全。

www.pcachina.com

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