基于网络安全攻防演习的纵深防御体系建设

张　伟，郭卫霞，杨国玉
（中国大唐集团科学技术研究院，北京 100043）

摘　要： 目前电力企业网络安全面临较多的威胁，电力监控系统信息安全保障能力不足，网络安全防护监测尤为重要。在此背景下，开展基于网络安全攻防演习的纵深防御体系建设，从技术和管理两方面进行部署和防护，将系统防护与企业管理、技术支撑相结合，解决不同层次的安全问题，加强企业整体网络安全防护能力，为今后的安全生产和管理奠定良好基础。

关键词： 电力监控；网络安全；攻防演习；纵深防御
中图分类号： TP309　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.201383

中文引用格式： 张伟，郭卫霞，杨国玉. 基于网络安全攻防演习的纵深防御体系建设[J].电子技术应用，2021，47(5)：25-28，34.
英文引用格式： Zhang Wei，Guo Weixia，Yang Guoyu. The construction of defense-in-depth system based on network security offensive and defensive exercises[J]. Application of Electronic Technique，2021，47(5)：25-28，34.

The construction of defense-in-depth system based on network security offensive and defensive exercises

Zhang Wei，Guo Weixia，Yang Guoyu
（China Datang Corporation Science and Technology Research Institute，Beijing 100043，China）

Abstract： At present，power companies face many threats to the network security，and the power monitoring system has insufficient information security capabilities. Network security protection monitoring is particularly important. In this context，the construction of a defense-in-depth system based on cyber security offensive and defensive exercises is launched，deployment and protection from both technical and management aspects are carried out and system protection is combined with corporate management and technical support，to solve solving security problems at different levels，strengthen the overall enterprise network security protection capabilities，and lay a good foundation for future safe production and management.

Key words： power monitoring；network security；offensive and defensive exercises；defense in depth

0 引言

十八大以来，以习近平同志为核心的党中央高度重视网络安全和信息化工作[1]，习近平总书记强调“没有网络安全就没有国家安全”，广大人民群众利益也难以得到保障，强调要把金融、能源、电力、通信、交通等领域的关键信息基础设施作为网络安全防护的重中之重[2]。电力系统作为现代社会的关键信息基础设施之一，是经济社会运行的神经中枢，也是网络攻击的重点目标[3]。近年以来，国内外网络安全形势不容乐观，面对复杂多变的国际形势以及国内社会转型期不断产生的新的社会冲突和矛盾，各类敌对势力一直妄图对我国关键信息基础设施进行破坏，以期造成不良社会影响。国外已经有了委内瑞拉人为造成接连两次发生大停电的例子，给当地百姓的正常生产、生活、社会稳定、国家安全造成极大影响，所以网络安全防护[4-6]迫在眉睫。对此，习近平总书记做出重要批示，要求防范电力战潜在重大风险。

目前电力行业的网络安全防护[7-10]仍面临着巨大的挑战。系统核心软硬件设备严重依赖国外厂商提供的软硬件产品；同时，电力监控系统信息安全防护薄弱，网络接入管理混乱；信息安全保障能力不足，核心系统依赖国外厂商运维；一线工业控制系统使用人员信息系统及信息安全方面的知识储备不足，信息安全意识淡薄，无完善的突发信息安全事件应急响应措施。总体来看，我国工业控制系统面临较多问题和威胁，急需加大工业控制系统信息安全方面的投入，全面提升工业控制系统信息安全防护水平。

切实加强网络安全防护，提高网络安全防护意识，必须从实践出发，熟知目前网络安全存在的问题和防护手段，才能兵来将挡，水来土掩，见招拆招。网络安全攻防演习的目的，一是及时整改深层次网络安全问题和隐患，提升综合防护能力和应急处置能力；二是加强参演各单位、社会力量与公安机关协同作战；三是提高攻防

双方技术能力；四是总结网络安全态势，形成网络安全评估报告，供上级决策。

1 网络安全隐患分析

通过各种防护监测可以发现企业存在较多安全隐患问题，其中急需解决的是针对企业内所有内外网设备进行杀毒处理。因为生产和办公的工作需要，大部分主机处于长时间运行并且防护手段甚微的状态，所以很有可能早已通过各种方式被种下病毒，潜伏在企业的内部网络中，时刻都可能对企业的系统造成威胁。安全防护设备还发现了各种操作系统以及个人邮箱仍存在许多弱口令现象，修改弱口令是最基本的网络安全防护意识，弱口令也是黑客入侵最简单常用的手段之一，从中获取内部信息和涉密文件。同时通过对内网流量的监测，发现有利用“QQ_TIM、WeChatVioceChat”协议进行登录外网的现象，普通员工的个人终端防护设备较低，又存在同时连接内外网的现象，很容易被黑客恶意利用并获取利益，这也是造成主机中毒的一种原因，如果中毒主机的使用者不注意，使用普通 U 盘给他人传递资料，那么很有可能造成大部分病毒传播。弱口令、个人终端同时连接内外网和 U 盘滥用的现象都可以通过提升管理手段和网络安全意识去杜绝，加强网络安全培训，建设网络安全考核制度都是有效的手段。

攻击方进攻企业系统可以总结为三种方式：社工入侵、系统入侵和口令破解。社工入侵指的是社会工程学攻击，企业通过日常的严格准入把控，可以杜绝身份不明人员乱入企业等现象。系统入侵大部分可以被入侵检测系统（主要为入侵检测软件和硬件的组合）所阻断，针对恶意 IP 能够通过各种防御设备拉黑、封禁，针对各个官网网站的攻击及时发现并处置，运维人员通过技术手段禁止远程软件的运行和操作，包括常用的 TeamViewer、QQ 远程以及系统自带远程工具等，可以有效地防止攻击者利用远程漏洞进行非法入侵。口令破解指的是针对各个操作系统或者邮箱进行口令的暴力破解，企业通过历年来对等级保护[11-12]和风险评估的重视，可以基本上杜绝弱口令的现象。

2 网络安全攻防演习战略体系

定期进行网络安全攻防演习对于企业来说是十分必要的，通过网络安全攻防演习，可以及时发现企业内现存的网络安全隐患，提上日程并及时处理，可以有效提升企业整体网络的安全防护能力。

在演习期间，实现具备全面的信息安全保障能力，具备全面的信息安全事件监控预警能力，在全面防护的同时实时监控信息安全态势[13]，发现安全事件立即处置，将各种威胁及风险降到最低，主要通过“人防+技防”综合防护手段进行保障本次工作。

网络安全攻防演习[14-15]主要通过技术和管理的方式进行安全防护建设，整体战略部署体系如图 1 所示，在管理方面需要事前划分工作小组，通过隐患排查、防护提升、实战保障等阶段各小组相互配合，保障网络安全；在技术方面主要体现为纵深防御体系的建设，通过治、梳、查、保、警等方面实现主动防御。

3 安全防护管理体系建设

网络安全攻防演习在管理方面的安全防护建设主要是通过事前清晰划分工作界面，将工作小组分为监测分析组、专家研判组、应急处置组、运维保障组和通信上报组，通过自我研发的工作上报平台，各工作小组各司其职，高效配合，以实现项目周期中有条不紊地开展工作。

3.1 隐患排查

对集团公司总部保障对象与重要信息系统进行网络安全隐患排查，核实对于物理环境、通信网络、区域边界、计算环境层面的各项防护措施是否落实到位。

(1)各类场所物理防护检查，检查内容包括：物业、机房等场所的物理访问控制、防盗窃及防破坏、防火、电力供应、裸露设备接口管理、U 盘使用规定以及现场人员

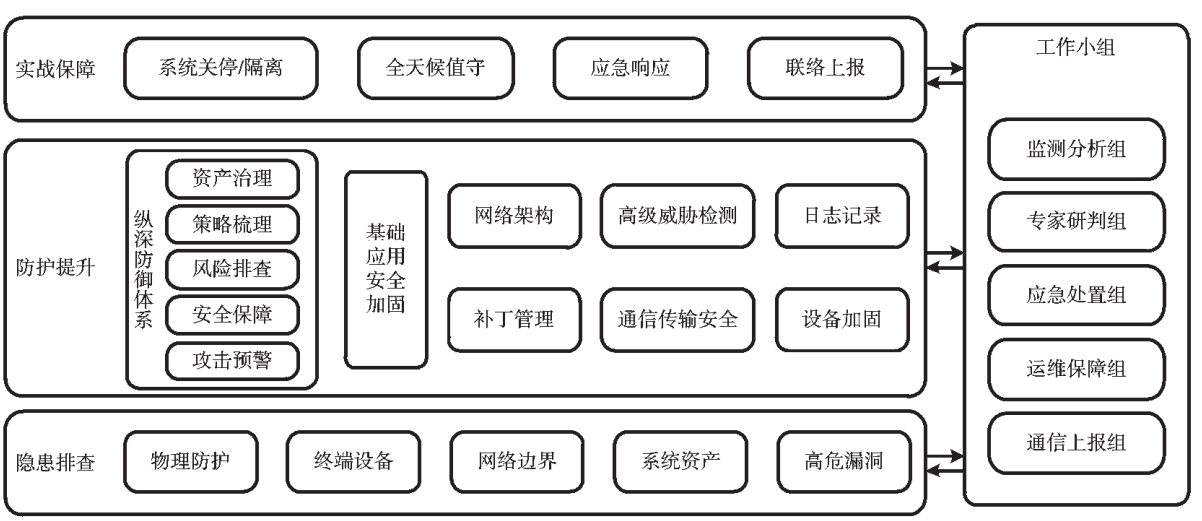

图 1 网络安全攻防演习战略体系

管理规定等情况。

(2)终端设备安全检查,检查内容包括:终端的物理防护、设备接口管控、桌面管控、防病毒软件的部署情况、接入内网的终端杀毒情况等。

(3)网络边界安全检查,检查内容包括:各生产大区与管理大区的物理隔离情况、互联网边界的安全防护情况、与第三方网络边界的安全防护情况、各类终端的安全接入情况,重要网络边界的防护设备策略配置规范、设备管理规范、操作规范、系统性能、账号与口令、日志与审计等。对互联网服务情况进行统计分析,根据各自的网络安全主体责任做好有效防护。

(4)系统资产的整体梳理,对内部资产情况进行摸底,重点是探知本单位资产情况,掌握资产分布情况,分别从互联网暴露面、内网资产、重点保护资产、僵尸网站、状态异常/不合规资产等方面进行梳理,梳理一共有多少资产(硬件资产、软件资产、信息数据资产等)、有多少种类型的资产、谁在使用这些资产、谁能使用这些资产、资产的对应责任人信息、是否满足等保要求、资产存在什么样的风险点、如何规避风险、有多少临时性资产等,通过对资产在线状态、设备指纹信息、服务端口信息和应用指纹信息画像,从而了解数据中心中资产分布状况。

(5)高危漏洞发现与处理,确保本单位漏洞扫描设备漏洞库已升级至最新,开展漏洞扫描及修复工作,对集团公司总部 11 个重要信息系统做了渗透测试,提供内外部攻防力量,对系统进行两轮渗透测试,充分发现信息系统安全隐患,切实整改。

3.2 防护提升

安全设备上线运行后,以最小化原则对所有安全设备防护策略进行梳理,重点核查远程连接等高危策略,去除冗余、过期、无效、重复的安全策略,加强内外网双向防护。建议对各单位强化公网准入控制,强化 SIM 卡准入机制,做好 APN 设置,针对遗失终端、嫌疑终端及时断网。

(1)采取纵深防御策略,综合利用多样化的防御手段,网络威胁情报联防处置平台(网盾 K01)—防火墙—Web 应用防护系统(Web Application Firewall,WAF),在多样化的纵深维度上布置层层防线,构建有效的纵深防御能力体系。

(2)构建合理的网络架构,通过合理的网络分区及在其上叠加的区域间数据流控制机制,可以有效防止恶意代码在网内的横向渗透与传播,也可以有效避免存在风险的终端或服务器被攻击者利用作为跳板对网内其他系统进行攻击试探。

(3)补丁管理,通过漏洞修复和补丁管理的动态机制,给出具体的建议操作和对应操作的预期结果,可有效同步漏洞信息、感知漏洞存在,进而实施漏洞修复和补丁管理,防御和缓解漏洞利用。

(4)通信传输安全,为保障数据通信传输安全,在通信前应当基于密码技术对通信的双方进行验证或认证;在数据的通信传输过程中,应当采用密码技术保证通信过程中数据的完整性、保密性。

(5)设备加固,网络层安全加固:主要从通信协议和服务、边界防护两方面进行加固。通信协议和服务:关闭网络不必用的功能和端口,关闭所有默认开启但是非必需的服务;常用协议的对应的端口要严格把控,避免未经授权的调用。边界防护:部署流量过滤设备,制定过滤策略,严格把控进出流量;部署流量监测设备,针对异常流量需及时报警、响应。无论是采用传统防火墙还是多重安全网关,抑或是网闸技术,都需要根据业务需求和实际网络情况及时更新规则和策略。

(6)日志记录,对所有网络设备及网络安全设备的运行情况、管理登录与操作情况、网络通信情况等信息进行日志记录,提供数据输出。对主机系统运行情况、用户访问情况等信息进行日志记录,并提供数据输出。对应用系统运行情况、用户访问情况等信息进行日志记录,并提供数据输出。日志需存储在指定位置,不得被越权访问。

(7)基础应用安全加固,基础应用(如邮件、Web 服务器)加固需要制定一套总领的安全加固规范,遵循安装与加固一体化的原则。

(8)高级威胁检测,采用高级威胁检测设备(APT),对网络中存在的各种病毒传输、攻击事件、可疑流量等进行实时监测,并输出网络流量日志与威胁检测结果。实现了基于网络的全局威胁检测,及对网络威胁行为的精细定位与溯源,快速处理网络威胁事件。

3.3 实战保障

各级指挥部集中监控指挥,各单位落实全天候重保工作要求,制定人员排班计划。

(1)落实特殊时段系统关停/隔离措施,根据前期制定的系统关停/隔离策略,结合特保时段和攻击强度对信息内、外网以及相关系统按照计划完成关停/隔离。

(2)全天候值守和应急响应,落实监控、应急方案和全天候值班计划,全力做好正式演习过程中的安全防护工作。各部门加强物理场所的安全巡视,尤其是户外场所、户外设备的安全巡视,确保万无一失,严格控制办公场所、营业场所中办公区域的人员出入,执行出入登记、人员接送制度,关键部位由安保部门确保安防措施到位、防范物理入侵。

(3)加强互联网边界、内外网边界、内网第三方边界等边界处的监测,具备异常流量发现能力。监控人员应具有基于流量的安全分析能力、具有对 APT 等特殊攻击行为的安全监测能力,确保网络攻击行为能够被记录,能够及时发现。第一时间收集网络攻击信息,通过录

屏、截屏等方式保存证据，并及时通报应急处置组和通信上报组，落实“零汇报”、事件快报制度，在每日攻击结束时以日报形式报送当天工作情况。

(4)充分研究攻击特征，精准定位攻击行为，加强对攻击事件的监测分析和应急处置。应急处置组对于发现的攻击行为通过网络阻断、物理隔离等方式及时处置各类攻击事件，对发现的问题及时处置整改。应急处置组根据发现的设备运行基线越限情况，及时进行比对、查杀、处理，将破坏降低到最小，避免数据泄露。同时做好内外部沟通联动工作。演习全程做好监控和应急工作的全过程记录。

(5)实施联络上报机制，信息中心做好与公安机关的对接与交流工作，对于非本次演习内的攻击行为联合公安机关做好发现攻击后的证据收集和举证。信息中心与公安机关保持密切联系，学习往年演习工作经验，向公司各单位实时通报演习注意事项、演习最新情报，合理利用演习规则，让公司在演习中掌握主动权。

4 纵深防御体系建设

网络安全攻防演习在技术方面的安全防护建设主要体现为纵深防御体系的建设[16-17]，分为事前和事中，事前通过“治”、“梳”、“查”，事中通过“保”、“警”，实现防御能力的建设。同时，结合后端情报系统提供的信息进行联动防御，主动封锁入侵路径。

(1)资产治理(治)。Web 应用安全综合治理系统利用被动自学习方式针对内部资产进行高效快速梳理，通过自动化检测僵尸网站、Webshell 等安全隐患，并利用应用间业务关系，关闭不必要的信息系统。

(2)策略梳理(梳)。梳理业务逻辑，规范安全设备防护策略配置，开展检查、监测、整改工作，针对边界防护策略进行梳理，原则上使用端口级的防火墙策略进行开放。

(3)风险排查(查)。采用一体化漏洞扫描开展高危端口治理排查梳理工作，形成高危端口台账，加强端口管控；开展操作系统及应用系统漏洞扫描和挖掘工作，建立漏洞隐患库，落实闭环整改要求。开展账号实名制、业务及平台类账号弱口令及权限最小化专项排查治理工作，包括但不限于办公终端、打印机等哑终端、自建系统、网络设备等。

(4)安全保障(保)。高级威胁分析系统、攻击防护、安全扫描、主机加固、失控主机发现、防火墙策略加固，信息安全评估、安全咨询、安全值守、资产梳理，应急响应、安全培训。

(5)攻击预警(警)。基于部署的高级可持续性威胁检测系统针实时监测发现的恶意文件、远程控制、僵尸网络、Webshell 探测等风险状况，针对攻击事件一点发现，通过利用 Web 应用防火墙和 K01 等安全防护产品实现全网阻断。

通过“资产治理，外防内控”达到实现信息安全的动态防御及主动防护要求(主动出击)，实现将信息安全运维服务和安全设备能力进行有机融和，提升整体系统的信息安全运维服务的能力，切实保障信息安全和各业务系统能安全可靠运行，通过专业安全服务力量提供针对信息系统保障安全解决方案，最大限度降低业务的安全风险，提高业务系统安全运营和防护水平。

5 结论

本文对目前电力企业存在的网络安全问题进行了剖析，总结分析出企业在安全设备维护不到位、人员行为操作不规范以及安全防护意识薄弱等方面存在的安全隐患，使得企业存在可能会被黑客或病毒入侵的风险。同时，针对于上述安全风险和隐患，本文提出了一种基于网络安全攻防演习的纵深防御体系，主要体现在管理和技术两方面，通过“人防+技防”进行综合的安全防护建设，保障企业网络安全。

网络安全攻防演习对于企业来说不能仅仅只是一次演习行动，更应该对未来的安全生产运行提供前车之鉴和保底机制，将通过网络安全攻防演习发现的问题提上日程并及时处理才是网络安全攻防演习的目的所在。通过网络安全攻防演习，可以有效提升企业整体网络的安全防护能力，为今后的安全生产和实战奠定良好的基础。

参考文献

[1] 刘剑，苏璞睿，杨珉，等.软件与网络安全研究综述[J].软件学报，2018，29(1)：42-68.
[2] 王栋，陈传鹏，颜佳，等.新一代电力信息网络安全架构的思考[J].电力系统自动化，2016(2)：6-11.
[3] 高昆仑，王志皓，安宁钰，等.基于可信计算技术构建电力监测控制系统网络安全免疫系统[J].工程科学与技术，2017，49(2)：28-35.
[4] 彭道刚，卫涛，姚峻，等.能源互联网环境下分布式能源站的信息安全防护[J].中国电力，2019，52(10)：11-17，25.
[5] 李田，苏盛，杨洪明，等.电力信息物理系统的攻击行为与安全防护[J].电力系统自动化，2017，41(22)：162-167.
[6] 朱海鹏，赵磊，秦昆，等.基于大数据分析的电力监控网络安全主动防护策略研究[J].电测与仪表，2020，57(21)：133-139.
[7] 郑国军，杨鹏洁，李秀琼，等.一种基于模糊理论的电力网络安全防护诊断系统及方法：201911008234.X[P]，2020-02-11.
[8] 张涛，赵东艳，薛峰，等.电力系统智能终端信息安全防护技术研究框架[J].电力系统自动化，2019，43(19)：1-8，67.
[9] 常方圆，李二霞，亢超群，等.配电终端可信安全防护方案研究[J].计算机应用研究，2020，37(S2)：256-259.
[10] 周慎学，范渊，夏克晁，等.台二电厂工控系统信息安全防护体系的建设[J].中国电力，2017，50(8)：53-57.
[11] 马民虎，赵光.等级保护与关键信息基础设施保护的竞

(下转第 34 页)

FIR filter design[J].Circuits Systems and Signal Processing, 2018, 37(10): 4409-4430.
[30] VASUNDHARA, MANDAL D, KAR R, et al.Digital FIR filter design using fitness based hybrid adaptive differential evolution with particle swarm optimization[J].Natural Computing, 2014, 13(1): 55-64.
[31] LIU M, CHEN L.A novel evolutionary method of structure-diversified digital filter design and its experimental study[J].Soft Computing, 2018, 22(7): 2381-2401.
[32] SHI Y.A modified particle swarm optimizer[C].Evolutionary Computation Proceedings, 1998: 69-73.
[33] 方正华.粒子群算法研究及在FIR数字滤波器中的应用[D].南京: 南京信息工程大学, 2014.
[34] HUANG W P, ZHOU L F, QIAN J X.FIR filter design: frequency sampling filters by particle swarm optimization algorithm[C].Proceedings of 2004 International Conference on Machine Learning and Cybernetics, 2004.
[35] 李辉, 张安, 赵敏, 等.粒子群优化算法在FIR数字滤波器设计中的应用[J].电子学报, 2005(7): 1338-1341.
[36] 周飞红, 刘辉.粒子群优化算法在FIR数字滤波器设计中的应用[J].计算机工程与应用, 2008(33): 83-85, 95.
[37] ABAB N E H, JEHAD I A, BATAINEH M H.Linear phase FIR filter design using particle swarm optimization and genetic algorithms[J].Digital Signal Processing, 2007, 18(4): 657-668.
[38] SUN J, FENG B, XU W.Particle swarm optimization with particles having quantum behavior[C].Proceedings of Congress on Evolutionary Computation.IEEE, 2004.
[39] SUN J, FENG B, XU W.A global search strategy of quantum-behaved particle swarm optimization[C].Proceedings of IEEE Conference on Cybernetics & Intelligent Systems, 2004.
[40] 吕国, 李艳芳, 钟晓春, 等.QPSO算法在FIR数字滤波器设计中的应用[J].通信技术, 2009, 42(6): 194-196.
[41] 梁慧, 彭世国.基于混沌粒子群优化算法的FIR数字滤波器设计[J].微型机与应用, 2010, 29(23): 41-43, 46.
[42] ZHAO Z, GAO H, LIU Y.Chaotic particle swarm optimization for FIR filter design[C].International Conference on Electrical & Control Engineering.IEEE, 2011.
[43] KAR R, MANDAL D, MONDAL S, et al.Craziness based particle swarm optimization algorithm for FIR band stop filter design[J].Swarm & Evolutionary Computation, 2012, 7: 58-64.
[44] 赵安新, 陈明, 张钟华, 等.采用综合学习粒子群算法的有限冲激响应数字滤波器设计[J].西安交通大学学报, 2012, 46(8): 71-75.
[45] KUMAR P U, KALADHARA S, DAS S M, et al.Design of optimal digital fir filter using particle swarm optimization algorithm[C].Advances in Computational Science, Engineering and Information Technology, 2013: 187-196.
[46] AGGARWAL A, RAWAT T K, UPADHYAY D K.Design of optimal digital FIR filters using evolutionary and swarm optimization techniques[J].AEUE-International Journal of Electronics and Communications, 2016: 373-385.
[47] SHAO P, WU Z, ZHOU X, et al.FIR digital filter design using improved particle swarm optimization based on refraction principle[J].Soft Computing, 2017, 21(10): 2631-2642.
[48] ZHANG C, YUE Z, WANG F, et al.A novel framework for FIR digital filter design based on P system with PSO[C].2018 International Conference on Information Systems and Computer Aided Education(ICISCAE), 2018.

(收稿日期: 2020-10-13)

作者简介:
张书玉(1995-), 女, 硕士研究生, 主要研究方向: 数字滤波器优化设计。
王婷(1980-), 通信作者, 女, 博士, 副教授, 主要研究方向: 信号处理, E-mail: chunchun1010@163.com。

扫码下载电子文档

(上接第28页)

合及解决路径[J].西安交通大学学报(社会科学版), 2018, 38(4): 16-22.
[12] 徐洋, 谢晓尧.信息安全等级保护测评量化模型[M].武汉: 武汉大学出版社, 2017.
[13] 龚俭, 臧小东, 苏琪, 等.网络安全态势感知综述[J].软件学报, 2017, 28(4): 1010-1026.
[14] 李经纬.网络攻防技术研究及企业实训平台设计[D].北京: 华北电力大学, 2018.
[15] 武泽慧, 魏强, 王清贤.基于OpenFlow的SDN网络攻防方法综述[J].计算机科学, 2017, 44(6): 121-132.
[16] 肖鹏, 周继翔, 刘宏春, 等.纵深防御和多样性策略在安全级数字化控制系统研发中的应用[J].上海交通大学学报, 2018(1): 14-19.
[17] 蒋宁, 林浒, 尹震宇, 等.工业控制网络的信息安全及纵深防御体系结构研究[J].小型微型计算机系统, 2017, 38(4): 830-833.

(收稿日期: 2021-02-07)

作者简介:
张伟(1976-), 男, 硕士, 高级工程师, 主要研究方向: 网络安全。
郭卫霞(1994-), 女, 硕士, 助理工程师, 主要研究方向: 深度学习、信息安全。
杨国玉(1980-), 男, 硕士, 高级经济师, 主要研究方向: 信息化与网络安全管理。

扫码下载电子文档

版权声明