江都水利枢纽工控系统网络安全关键技术设计

李景奇[1],孟 俊[2],黄 晋[3],张伟建[1],王 军[2],张玉倩[1]
(1.河海大学 网络安全与信息化办公室,江苏 南京 210024;2.江苏省江都水利工程管理处,江苏 扬州 225200
3.南京南瑞水利水电科技有限公司,江苏 南京 210000)

摘要:研究基于OODA态势感知循环模型,构建了江都水利枢纽工控系统网络安全体系,设计了水利工控系统网络态势感知平台及关键资产识别模型和自动化处置模型,为水利工控系统的网络安全管理提供借鉴。

关键词:水利工控系统;网络安全;态势感知;自动化处置
中图分类号:TV663 **文献标识码:**B **文章编号:**1007-7839(2023)11-0050-0005

Design of network security key technology of industrial control system of Jiangdu Water Conservancy Hub

LI Jingqi[1], MENG Jun[2], HUANG Jin[3], ZHANG Weijian[1], WANG Jun[2], ZHANG Yuqian[1]
(1. *Network Security and Information Technology Office, Hohai University, Nanjing* 210024, *China*;
2. *Jiangdu Water Conservancy Project Management Office of Jiangsu Province, Yangzhou* 225200, *China*;
3. *Nanjing NARI Water Resources Hydropower Technology Co., Ltd., Nanjing* 210000, *China*)

Abstract: Based on the OODA situational awareness cycle model, the overall network security architecture of the industrial control system of Jiangdu Water Conservancy Hub was constructed. The network situational awareness platform, key asset identification model, and automated disposal model of the water conservancy industrial control system were designed, providing reference for the network security management of the water conservancy industrial control system.

Key words: water conservancy industrial control system; network security; situation awareness; automated disposal

1 概 述

水利工控系统对水利工程管理和实际应用具有重要作用,水利关键信息基础设施对水利行业领域产生至关重要影响,是国家网络安全重点保护的对象,水利工控系统即是水利关键信息基础设施之一。本文以江都水利枢纽为例,对水利工控系统网络安全关键技术开展研究。

目前,水利网络安全方面仍存在问题,如网络安全管理制度不健全,网络安全防护措施不完备等,特别是水利工控系统缺少网络安全等级保护定级规范,而水利工控系统的封闭性及其与互联网物理隔离的特殊性,容易造成工作人员存有“物理隔离就绝对安全”“有防火墙,就不存在网络安全问题”等错误认识,这种网络安全意识容易造成水利工控系统的安全防范疏忽。从技术方面看,水利工

收稿日期:2023-07-24
基金项目:江苏省水利科技项目(2021067)
作者简介:李景奇(1980—),男,高级工程师,硕士,研究方向为计算机应用、网络安全。E-mail:147789024@qq.com

控系统存在网络安全设备不足、技术防范手段欠缺的问题，如水利办公网络和工控网络没有进行物理隔离、数据交换关键路径缺少防火墙或网闸、常用的入侵检测和漏洞扫描系统不能经常检测工控网络、对关键主机和终端没有有效保护、缺乏有效的监视手段、无法监控工作人员的安全风险等[1-3]。

2　网络安全需求及特点分析

传统的网络安全防御手段包括防火墙、入侵防御、安全审计等，主要基于已知威胁进行检测和安全处置，但对外部网络安全形势、内部网络安全威胁缺乏有效评估。现代信息技术的发展和应用越来越广泛，相应的网络攻击收益越来越多，网络攻击行为技术手段也越来越强、越来越隐蔽。尽早发现网络攻击，防患于未然，是抵御网络攻击的最直接方法。网络安全态势感知技术也受到越来越多的关注。

2.1　网络态势感知需求

网络安全态势感知需要把所有可获取的数据进行综合分析，并对网络的安全态势进行评估，快速响应提供网络安全处置决策依据，将风险和损失降到最低。因此，水利工控系统网络安全态势感知对提高工控网络的监控能力、应急响应能力和预测网络安全的发展趋势等具有重要意义。

2.2　网络安全特点分析

与水利办公系统网络相比，水利工控系统网络结构简单，但实时性要求高，以水利工程设备过程控制为主，主要通过控制终端PLC设备，实现调水目标。水利办公系统网络符合通用网络安全防御范畴，但水利工控系统网络具有行业网络防御特点。

根据网络攻击的一般过程和水利工控系统网络安全场景特点，水利工控系统网络攻击可能的手段和过程一般包括：(1)对办公网WEB服务器的探测和攻击；(2)对水利工控系统操纵终端进行社会工程化攻击；(3)通过暴力破解等方式，突破VPN等安全设备对操作终端的限制，从而完成对水利工控系统的攻击[4]。水利工控系统网络攻击过程如图1所示。

为防范网络攻击，根据水利工控系统攻击过程及特点，需要在办公网络和工控网络中部署日志采集设备和网络安全态势感知平台，采集网络攻击日志，基于系统安全规则，进行系统安全评估，并通过安全态势感知平台展现，实现对水利工控系统安全态势的观察和理解。

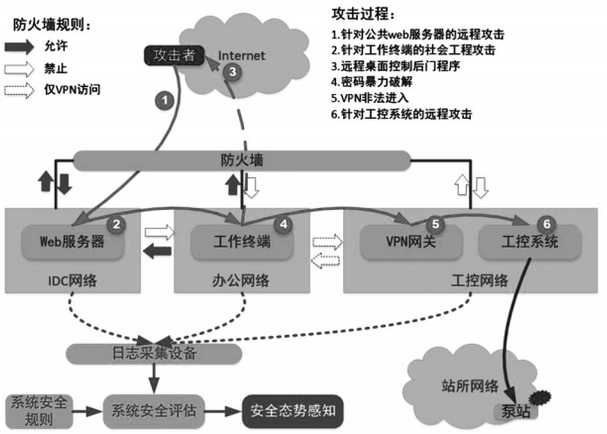

图1　水利工控系统网络安全攻击示意图

3　江都水利枢纽工控系统网络安全总体架构

根据江都水利枢纽对网络安全的总要求，紧密围绕办公网和工控网网络安全的现实需求和“十四五”国家信息化规划，充分考虑江都水利枢纽未来业务发展、技术发展和能力发展所面临的一系列安全风险威胁，以网络安全法、数据安全法、网络安全等级保护以及关键信息基础设施安全保护等法规要求为统揽，按照“一体化、集约化、运营化、专业化、数字化和服务化”的发展思路，在保障安全合规的同时，提升江都水利枢纽未来5年引入新业态、新技术带来的安全风险应对能力，以安全大数据为安全智能底座，以网络安全等级保护合规为基础、以安全能力建设为核心、以安全运营体系建设为抓手，建立全域覆盖、立体综合的江都水利枢纽网络安全技术体系和运营体系，打通江都水利枢纽网络安全风险评估、运维保障、监测预警、应急响应的运营流程，提高网络安全数据治理能力、数据安全管控和安全服务水平，实现“事前风险评估、事中安全防护、事后应急响应”的纵深防御体系，实现网络安全从被动向主动、从静态到动态、从事后到事前、从分散到集约的转变，全时域保障江都水利枢纽网络信息系统和数据安全可靠，发现和阻断已知网络攻击和未知入侵渗透，防范来自外部和内部多类型攻击和数据盗取行为，推动江都水利枢纽网络安全发展达到新高度。

江都水利枢纽按照国家对水利关键基础设施网络安全要求，从技术和管理2个方面进行顶层设计和应用实践，设计了江都水利枢纽网络安全总体

框架。如图2所示，江都水利枢纽工控系统网络安全总体框架由管理制度、态势感知平台、运营中心构成，管理制度和运营中心从制度和实施2个层面对网络安全的日常管理和运营提出具体要求，而核心是网络态势感知平台。网络态势感知平台基于OODA模型，从底层各类网络安全设备上采集数据，通过大数据平台进行归类和分析，构建网络安全模型，快速呈现网络安全态势。维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候会发生风险。这些态势能够感知到后，具体的风险处置则可以根据风险等级进行相应处理。

图2 江都水利枢纽工控系统网络安全体系

4 网络安全管理能力建设

江都水利枢纽网络安全管理体系对标《网络安全等级保护2.0》及《关键信息基础设施安全保护条例》，结合国家网络安全等级保护三级进行要求。明确网络安全管理机构、运营机构、业务主管部门和用户等各方的安全职责，坚持“谁主管谁负责、谁运行谁负责”的原则，各级单位分别做好所辖范围的网络安全工作，定期对各信息系统进行自查及抽查检测，必要时可以委托网络安全服务机构进行检测评估；定期开展网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；加强网络安全培训，不断提升网络安全意识和网络安全事件的应急处置能力；促进相关部门与网络安全服务机构之间的网络安全信息共享。

4.1 网络安全能力建设

通过部署各类网络安全设备，打通现有安全体系的认证、授权，实现各类网络安全设备的统一管理。建立网络安全服务目录，所有服务建立统一标准，实现统一注册、统一接口、统一调度。所有网络安全能力统一认证、授权，并与具体的安全执行组件、防护设备进行连接，实现对安全组件的编排和控制、运维等。

4.2 数据安全能力建设

从数据安全梳理、数据风险核查、数据安全监控、数据安全防护等各个维度提高江都水利枢纽的数据安全能力，进行数据资产价值评估、数据资产弱点评估、数据资产威胁评估，结合组织、制度、场景、技术、人员等，自上而下构建立体化的数据安全防护体系。

4.3 运营安全能力建设

网络安全运营中心是水利枢纽信息化建设、安全运营体系的核心平台。网络安全运营中心遵循“分层解耦、异构兼容”的原则，将安全能力和安全运营进行资源整合和智能联动，有效优化安全资源，强化风险防控能力，提升网络预警处置能力，打通工作协同机制，配合江都水利枢纽规范安全度量框架，保证业务系统的运行，及时掌握整体态势，切实保障水利枢纽工控系统的安全运行。

5 网络安全技术能力建设

水利工控系统网络安全关键技术包括水利工控系统的网络安全态势感知能力、威胁情报能力及网络安全管理平台设计。

5.1 网络安全态势感知平台

水利网络安全面临的最大问题是如何快速、有效地感知网络安全风险并处置网络安全事件。网络安全威胁情报，且事件类型多样、数量巨大，网络安全人员如何从海量网络攻击日志中筛选并快速判断出水利工控系统的网络安全问题，从而进行针对性处置，是现在面临的最急迫、最需要解决的问题。

水利工控系统网络安全态势感知平台（Water Conservancy Industrial Control System Network Security Situation Awareness Platform，WCICS-NSSA）[5]分为数据来源、数据采集及预处理、态势数据计算和存储、态势数据理解和态势呈现5个层次。数据来源包括水利工控系统网络中的各类网络安全设备中存储的各类数据，如防火墙、入侵检测系统、防病毒、流量控制、日志审计等系统存储的各类数据，这些数据既有网络攻击日志，又有工作人员的操作日志。数据采集和预处理是指通过ETL工具或syslog方法采集各类安全设备数据，并进行数据预处理，然后通过大数据平台，自动呈现各类网络安全设备（防火墙、入侵检测系统等）的运行状况，并对有效

数据和结果进行分类存储。态势数据理解需要通过模式识别、关联分析等技术手段，把数据转化为更易于理解、更符合认知的网络安全防护报告。态势呈现有利于网络安全人员直接感知，呈现内容包括水利工控系统网络攻击态势、威胁情报态势、资产风险态势、安全处置态势4个部分，实现对水利工控网络安全的总体感知和预警。

当前网络安全态势感技术发展迅速，与流域数字孪生技术相结合，成为水利信息化工作的重要一环。

5.2　网络安全态势监控

WCICS-NSSA从安全设备、网络设备、操作系统、应用系统中采集网络攻击数据和用户行为数据，形成网络安全大数据。基于网络安全大数据的分析，WCICS-NSSA形成网络攻击的态势图，方便网络安全人员直观观察、分析和处置。网络安全最大的风险是不知道风险在哪里，而通过WCICS-NSSA监控技术，把不可观的网络攻击行为抽象化，形成可视化的、图像化的网络攻击态势图。

WCICS-NSSA威胁情报态势内容包括水利行业网络安全威胁、工控系统内部网络安全风险、水利网络安全知识图谱、水利网络安全知识管理。水利行业网络安全威胁数据可以直接从外部网络安全公共平台抓取或采集，可以作为安全威胁趋势的感知。工控系统内部网络安全风险数据主要通过网络安全事件处置情况、网络安全等级保护测评报告和定期的网络安全测评获得。水利网络安全知识图谱通过网络安全日志、安全事件，攻击源和攻击对象之间的关系及攻击态势进行关联分析，形成知识图谱。知识图谱有利于逐步形成水利网络安全全景关系图，提高水利网络安全攻击趋势的预测。水利网络安全知识管理则是将相应的网络安全处置方法、处置的过程进行记录，为后续的网络安全处置和网络安全分析提供相关的经验和技巧。WCICS-NSSA威胁情报态势，通过大数据分析技术，结合水利工控系统资产信息，分析研判水利工控系统网络安全状态和形势，并及时发布预警信息[6]。

WCICS-NSSA资产风险态势通过对水利工控系统的网络设备、服务器的软硬件资源评估，明确各类资产的重要性、威胁情况、脆弱性、供应链安全等，进行信息资产的分级分类，定义各类资产的安全等级。网络安全态势监控的关键是厘清监控的对象的范围及风险等级。信息资产可以根据受到攻击后可能带来的资产损失来确定资产的价值，也可以按评分量表进行打分来相对评估。因此，网络安全态势监控包括：(1)确立信息资产的风险等级；(2)确定相应等级的网络安全保障策略；(3)确定相应等级的网络安全处理方式。水利工控系统监控信息通过网络安全态势感知平台展现，并能充分被网络安全管理员、业务管理员和系统管理员共享。

WCICS-NSSA的信息资产风险评估的关键要素包括威胁程度、资产脆弱度、资产价值、供应链风险程度、运维制度缺失度等[7-8]。水利工控系统信息资产风险评估如式(1)如示。

$$R=f(A,T,V,C,M) \tag{1}$$

式中：R为风险评估值，A为资产价值，T为威胁指数，V为脆弱性指数，C为供应链风险指数，M为运维制度缺失度。所有指标都与评估值成正比，指标越高，风险评估值越高。因此应采取的安全保护措施等级就越高。这5项因素以量表的形式进行评估，各项之间进行加总来计算分值。资产价值主要考虑该资产的价格、功能、用途。威胁指数主要考虑外部攻击的频次和攻击强度。脆弱性指数主要考虑信息设备本身的漏洞、密码等内部全性问题。供应链风险指数从供应链的角度来评估供应商的能力及供应产品的可替代程度。不可替代设备的风险度明显会高于可替代设备。运维制度缺失度主要考察工控系统设备的各项运维制度是否齐全，能否做到按时维修、巡检等。

5.3　网络安全事件处置

网络安全事件处置的关键是如何高效完成对网络安全事件的处理，减少受攻击时间，减少对水利工控系统的影响。对此，WCICS-NSSA从3个方面来支持网络安全事件处置工作：一是呈现安全处置态势，直观展示网络安全风险处置情况；二是支持处置流程及其监督处置进展；三是支持对网络安全事件处置的评估，并形成知识经验。在水利工程工控系统中，一般会通过“镜像”方式捕获并分析水利工控网络和设备运行数据，同时监测通信行为、控制指令、网络流量的异常，辨别恶意代码传播、网络扫描渗透等行为，感知水利工控网络安全态势。而对水利工控系统终端，可以通过安全配置、端口绑定等各种方式对系统终端进行加固[9]。

基于WCICS-NSSA的网络安全处置流程包括：(1)防火墙设备根据设定的阈值进行自动处置，当感知到攻击时，网络安全设备第一时间进行阻断；(2)人工复核，由网络安全人员确认网络安全事件等级；(3)通报网络安全事件，及时通过短信、微信、

邮件等途径，督促业务部门进行处置，把安全的情况自动发送给网络安全人员；(4)形成处置报告，将处置的方法形成知识文档，作为网络安全知识管理的重要内容加以保存，为其他网络安全事件处置提供经验支持。

对于网络安全事件处置，根据“OODA环”，安全事件从感知到分析到决策再到处置，是一个较长的过程，如何达到时间最短、结果最优，是实际处理工作中迫切需要解决的问题，其中最主要的是能对安全攻击进行快速阻断，这需要安全设备能够支持网络攻击熔断技术，其关键在于：(1)如何快速识别网络安全事件。目前主要基于特征值，如应用防火墙，可直接阻断攻击；(2)如何立即处置安全攻击，拒绝访问。对于防火墙而言，网络攻击的识别方法需要有明确并可执行的规则，而最简单最快捷的规则就是访问次数。因此，WCICS-NSSA选择访问次数为网络攻击熔断的关键指标。在网络攻击事件处置可以通过分析网络安全大数据，然后发送一键断网指令到防火墙设备，由防火墙来实施攻击拦截。而如何测算网络访问量达到多大才是攻击，需要通过对资产对象的了解和一定的算法来实现。自适应熔断算法通过计算访问次数，采取随攻击数量而逐步增加拒绝该源地址访问链接的概率，直到应用完全不通访问，达到应急网络安全防范的目的。当访问量下降，防火墙自动逐步恢复接受访问链接。

当前防火墙都具备根据访问量自动丢包的功能，但还需要根据水利工控系统的访问量和访问范围，制定更有针对性的访问规则和网络安全策略，实现既能在防火墙上自动拦截，也能在网络安全态势感知平台上呈现和告警，减少对应用系统的影响。该策略设置可以参考如式(2)所示的自适应熔断算法来计算丢弃请求的概率。

$$P=\max\left(0,\frac{R_{\text{requests}}-K\times A_{\text{accepts}}}{R_{\text{requests}}+1}\right) \tag{2}$$

式中：R_{requests}为窗口时间内的请求总数；A_{accepts}为正常请求数量；K为敏感度，K越小越容易丢请求，一般推荐1.5~2之间。正常情况下$R_{\text{requests}}=A_{\text{accepts}}$，所以概率是0。随着正常请求数量减少，当达到$R_{\text{requests}}=K\times A_{\text{accepts}}$继续请求时，概率$P$会逐渐比0大开始按照概率逐渐丢弃一些请求，如果故障严重则丢包会越来越多，假如窗口时间内$A_{\text{accepts}}=0$则完全熔断。当应用逐渐恢复正常时，A_{accepts}、R_{requests}同时都在增加，但是$K\times A_{\text{accepts}}$会比$R_{\text{requests}}$增加得更快，所以概率很快就会归0，关闭熔断。

网络安全事件处置需要技术人员检查、备份、修复和处理，这些操作是非常严谨而专业的，既要能把网络安全风险解除，又不能影响水利工控系统的正常运转，所以技术人员需要对水利工控系统非常了解，以保障问题处理不会影响业务运行。因此需要加强知识管理，积累安全知识，支持后续的网络安全事件分析和处理，为类似安全问题处置提供经验和方法。基于WCICS-NSSA对水利工控系统网络安全问题和威胁情况的综合分析，逐步形成水利工控系统网络安全知识图谱，及时对水利工控设备风险进行溯源分析，了解相关关系，从而对水利工控系统网络威胁的处置提供决策支持。

6 结 语

江都水利枢纽工控系统网络安全需要从管理和技术2个角度出发，不断完善网络安全防护体系。一方面要完善管理制度，配置网络安全人员，构建网络安全管理中心；另一方面部署综合态势感知平台，通过防火墙、VPN、上网行为分析等安全设备采集网络安全大数据并进行分析，实现水利工控系统的网络安全态势感知。凭借WCICS-NSSA，构建2层深度防御技术体系，实现“边界→网络→终端”的立体防御。

梳理水利工控系统网络路径，明确路径中的节点存在的网络安全隐患，根据安全需求差异性划分不同的安全区域，并在不同区域之间利用专用防火墙、隔离网闸等进行防护，通过物理隔离、逻辑隔离等方式防护水利工控系统。水利工控系统安全体系要重视网络安全管理，并充分应用网络安全态势感知等先进技术，保障水利工控系统的安全运营。本文基于OODA态势感知模型，提出了基于OODA的水利工控系统网络安全总体框架，设计了关键资产识别模型和自适应熔断模型，从网络安全大数据识别出攻击，并进行自动阻断，提升网络安全防护能力和水平。

参考文献：

[1] 蔡阳. 贯彻《网络安全法》构建水利网络安全保障体系[J]. 水利信息化，2017(3)：1-4，15.

[2] 詹全忠. 水利网络与信息安全资源整合共享探讨[J]. 水利信息化，2014(6)：22-26.

[3] 杨旭，谢丰，任旭诚. 水利工程工业控制系统网络安全研究[J]. 水利信息化，2017(3)：20-23.

（下转第63页）

控制柜,通过安装各类传感器、搭建现场通讯网络,实现了前池水位的自动测量以及水泵和电磁阀电气参数的实时监测、远程控制。同时,搭建了以4G模块和无线专网为基础的传输平台,将现场数据实时传输至集控中心工业互联网平台[4]。

远程监控应用App是在工业互联网平台提供的开发工具基础上,根据现场实际需求,开发出的集数据展示、统计、远程控制等功能为一体的应用平台。主要功能有总貌展示、导航菜单、地图导览。设计了园区城市排涝泵站总貌界面,将泵站公司管理园区的9个雨水排涝泵站整体信息进行大屏展示,开发了导航菜单和地图导览,进行沉浸式交互。

泵站运行状态实时显示将当前泵站运行过程中的重要运行参数以及运行环境信息进行实时大屏展示。同时应用在界面上方设计了信息切换栏导航,方便管理值班人员实时切换查看各类信息的详细报表。 远程监控应用App的数据报表功能是对运行状态实时显示功能的补充,前者更适用于大屏展示,而数据报表则可以让管理值班人员了解当前泵站运行时泵房和机组的各类详细信息。远程控制模块包括水泵机组控制以及泵房设施控制2个部分。水泵机组控制可通过Web或移动端交互界面,点击操作按钮实现水泵机组的远程启停。泵房设施的控制则是泵房照明、排气扇的开关控制。远程控制模块信息传输通过专用网络独立进行,避免其他干扰,实现泵站的远程值班、无人值守。

5　结　语

研究提出了一种城市排涝泵站远程集控智能化改造方案,并以某城市排涝泵站为例,改造并实现了基于工业互联网平台的城市排水泵站运行的远程集控。主要成果如下:

(1)现场设备的智能化信息监测。通过对现场原有老旧设备的智能化改造,实现了泵房运行环境和水泵机组的智能化信息监测,实现了部分设备的自动启停和联动控制,改善了排水泵站运行条件,实现排水泵站的“智能运行和无人值守”。

(2)现场运行和管理的远程集控。通过搭建工业互联网平台网络架构和应用开发,实现整个系统运行状态的实时监测。开发了远程控制功能,可对水泵机组和泵房设施实现远程控制,从而实现了“无人值守和远程值班”。

(3)优化运行成本,减员提效。通过改造,实现了由24 h专人值守向远程值班和定期巡检的转变,原有值班人员由9人专人值守加管理室4人变为2人巡检加集控中心2人,大大缩减了泵站管理公司的运维成本,取得良好的经济效益。

城市排涝泵站远程集控智能化改造是一项兼具社会效益和经济效益的重要工作,涉及多学科、多领域专业知识的综合应用,同时也是一项繁琐复杂的工程。本项目以公司所管理的某科创园区内城市排涝泵站为例,在传统老旧排水泵站的智能化改造和优化运行的方案架构设计、网络平台搭建、现场施工以及远程集控的实现等方面进行探索,并取得了一定的成果。目前该泵站已经进行了无人值守、远程集控值班的试运行。本项目实施方案的相关经验,对其他中小型泵站的智能化改造和远程集控运行具有借鉴意义。

参考文献:

[1] 房灵常,唐炜,陈金水. 智能泵站关键技术研究[J]. 中国农村水利水电,2020(12):73-76.

[2] 唐鸿儒,赵林章,朱正伟,等. 智能泵站研究[J]. 中国农村水利水电,2022(8):128-131.

[3] 樊锦川,黄蔚,冯宛露,等. 基于工业互联网操作系统的泵站一体化运维平台建设[J]. 江苏水利,2022(8):40-44.

[4] 王飞,张峻瑞,叶鑫. 智慧化工园区系统的设计与建设展望[J]. 化工自动化及仪表,2023,50(3):365-370.

(上接第54页)

[4] 张亮,屈刚,李慧星,等. 智能电网电力监控系统网络安全态势感知平台关键技术研究及应用[J]. 上海交通大学学报,2021,55(增刊2):103-109.

[5] 李景奇,夏方坤,张伟建,等. 水利工控系统网络安全态势感知平台设计与应用[C]//2022年(第十届)中国水利信息化技术论坛论文集,2022:1-10.

[6] 詹全忠,蔡阳. 水利关键信息基础设施保护的思考[J]. 水利信息化,2017(3):16-19,28.

[7] 李程雄. 网络安全态势感知系统关键技术研究[J]. 电子技术与软件工程,2021(23):231-233.

[8] 邹立刚,张新跃. 关键信息基础设施保护思考[J]. 网络空间安全,2020,11(12):44-48.

[9] 杨旭,谢丰,任旭诚. 水利工程工业控制系统网络安全研究[J]. 水利信息化,2017(3):20-23.