文章编号:1672-3031(2018)05-0466-06

水利工控系统网络安全防护的问题与对策

郭 江,陈服军,张志华
(中国水利水电科学研究院 天津水利电力机电研究所,天津 301900)

摘要:近年来工控网络安全事件频繁发生,并且呈逐年递增趋势,造成的安全事件影响越来越大,甚至逐步威胁到国家安全。水利工程是国家关键基础设施的重要组成部分。随着"中国制造2025"和两化融合工作的推进,越来越多的智能设备、计算机技术和网络技术应用于工业控制系统,使工业控制系统极易遭到来自管理网或互联网病毒、木马以及黑客的攻击。文中主要介绍了水利工控网络安全的现状、在技术和管理方面存在的主要问题,以及引起水利工控网络安全问题的主要原因,重点阐述了水利工控系统网络安全防护工作要点及安全防护方案,并以水电厂工控系统为例给出了具体的防护措施。

关键词:水利工程工控系统;工控系统网络安全;安全防护;风险评估
中图分类号:TB114.2 **文献标识码**:A **doi**:10.13244/j.cnki.jiwhr.2018.05.016

1 引言

工业控制系统广泛用于电力、水利、污水处理、石油化工、冶金、汽车、航空航天、交通、通讯等诸多现代工业领域,众多关系到国计民生的关键基础设施,如水力发电、城市给排水等都依靠工业控制系统来实现生产过程自动化。随着两化(信息化与工业化)融合的推进,管理网络与生产网络的互联,使工控系统由原来相对封闭、稳定的环境变得更加开放、多变,工控系统的漏洞在互联网中暴露无遗,由于工控网络与传统的互联网有本质的不同,传统的互联网安全技术并不能保障工控网络安全,近年来工业控制系统的安全事件屡有发生(图1为近年来发生的工控网络安全事件趋势图),2012年全球工控网络安全事件为197件,并且呈逐年递增的趋势,到2015年工控网络安全事件已上升至295件[1],而且遭受攻击的目标多为国家重要基础设施或重要行业领域工业控制网络,安全事件影响越来越大,甚至逐步威胁到国家安全。国家基础设施的工控网络一旦受到攻击,将给社会稳定和经济健康发展造成不可估量的影响,如钢厂异常停机、石化工厂蠕虫泛滥等,给企业造成巨大的经济损失[2]。特别是2015年乌克兰电网事件,造成乌克兰140万名居民家中停电,为我国基础设施安全敲响了警钟,因此,国家关键基础设施的工控网络安全问题应该引起重点关注。

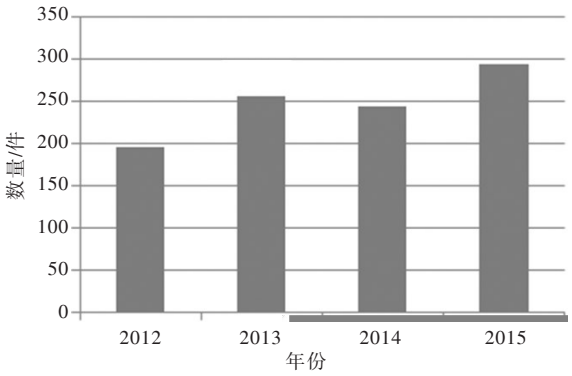

图1 工控网络安全事件趋势

水利工程是国家基础设施的重要组成部分,水利工程工控系统网络安全问题也逐渐引起重视,水利部下发《2017年水利信息化工作要点》,印发《水利网络安全顶层设计》,遵照《中华人民共和国网

收稿日期:2017-11-22
基金项目:水利部技术推介项目(SF-PX-201810)
作者简介:郭江(1965-),男,天津人,教授级高级工程师,主要从事水电站基础自动化和水利工控网络安全研究。
E-mail:guojiang@iwhr.com

络安全法》，结合水利网络安全现状，提出了统一水利网络安全策略、落实组织管理和监督检查两大保障，提升水利网络安全监测预警、纵深防御和应急响应三大能力的网络安全总体框架，并明确了相应的设计架构和主要内容，提出了保障措施。中国水利水电科学研究院天津机电所从2015年初开始进行水利工控网络安全方面的研究工作，对国内外工控网络安全动态、政策法规、防护技术等进行了详细的了解和研究，并调研了国内多个水电站、泵站等水利工程，充分了解水利工程工控系统网络安全现状，并建立了工控网络安全实验室，能够对水利工控系统进行漏洞挖掘和威胁检测，开展水利工控系统网络安全攻防研究，提供水利工控系统网络安全防护技术解决方案。

2　水利工控系统网络安全现状

2.1　典型工程工控系统测试分析　2015年12月，中国水利水电科学研究院天津机电所对天津市蓟州区某供水管理所和某水电站重要工控设备进行漏洞挖掘和安全检测，主要检测的设备包括供水管理所加压泵房中的PLC、计算机监控中心上位机PC及软件和水电站闸门控制系统中的PLC和调速器MSDSC-11微机控制器。测试通过漏洞挖掘检测设备和被测设备点对点直连方式进行连接(连接方式如图2所示)，漏洞检测平台置于被测设备和测试终端之间，测试终端通过预设的IP地址进入漏洞检测平台操作界面，漏洞检测平台和控制器通讯端口连接，测试数据在检测平台和被测设备之间交互。采用端口扫描、已知漏洞测试、Modbus TCP协议模糊分析、其他协议的模糊测试、风暴测试等方法进行测试。

(a) PLC检测连接方式　　(b) 调适器微机控制器检测连接方式

图2　漏洞检测设备和被测设备连接方式

对供水管理所工控系统测试中共发现15个漏洞，其中包含6个危急漏洞、9个高危漏洞，整体危险等级为危急。在对PLC测试中发现，发送畸形ARP和畸形IP报文可以导致被测设备失去响应甚至崩溃，该漏洞很容易被利用进行ARP欺骗窃取信息和攻击，导致PLC崩溃[3]。PLC一旦受到攻击崩溃将无法监测到各水井源的电流、电压、功率、压力、流量、液位等运行信息，更无法采取相应措施进行控制和处理异常情况，整个供水系统将遭到破坏，无法进行正常供水；在对上位机PC及组态软件测试中发现，组态软件所在PC开放了众多端口，开放的端口容易被扫描和利用进行设备登陆、控制、发起攻击等。同时发现组态软件和PC相关危急和高危漏洞，攻击者利用漏洞非常容易进行控制和执行相关操作。这些漏洞将会导致系统中上位机及监控组态软件遭到破坏或被控制，从而控制水源井控制系统中所有PLC设备，篡改采集的信息、随意下发控制指令，破坏供水系统。

在对某水电站工控系统的PLC测试中，由于现场条件不允许进行网口测试，只进行串口检测，发现发送相关畸形Modbus RTU报文容易导致被测设备产生崩溃。同时协议未进行加密认证，容易被攻击、进行信息窃取和伪造，另外还发现存在内存非法读写相关漏洞，攻击者可以轻易控制PLC。这些漏洞会导致水电站中闸门系统信息被窃取和遭到破坏以及崩溃。闸门系统一旦遭到破坏无法起到水位的调节和洪水期间泄洪等重要作用。调速器微机控制器MSDSC-11在测试中，由于现场条件不允许进行网口测试，只进行串口检测，发现发送相关畸形Modbus RTU报文容易导致被测设备产生

崩溃，同时协议未进行加密认证容易被攻击机进行信息窃取和伪造。此漏洞会导致水电站中调速系统遭到破坏甚至崩溃，从而无法起到调节水轮机转速、事故情况下紧急停机等作用，直接影响到水电站的发电系统，致使无法正常发电。

2.2　水利工控网络安全特点　水利工控系统网络安全的特点主要表现在以下5个方面：(1)水利工控网络大多采用IEC61158中提供的20种工业现场总线标准，如Modbus系列、Profibus系列等，这些都是若干年前设计的，根本没有考虑安全性问题[4]，黑客通过现场总线这种网络结构，便很容易获得控制区及执行器的控制权，进而控制整个水利工控系统。(2)水利工控系统中的控制器等设备大多采用西门子、GE、施耐德等公司产品，这些通用控制器所具有的漏洞极易成为恶意攻击的突破口[5]。(3)水利工控系统的软件升级困难。水利工控系统网络以稳定性为基础，如果频繁升级补丁软件，将给系统的稳定性带来严重威胁，如果升级失败或出错，将造成整个工控系统的不可用，给用户带来巨大的损失；(4)控制病毒的手段缺乏。水利工控系统中很多控制设备单元都是相对封闭的系统，无法通过病毒软件进行病毒清理，同时缺少控制病毒在工控系统网络中传播的手段，工控系统一旦感染病毒将传播到整个工控网络；(5)水利工控系统中的设备具有多样性。水利工控系统中的设备多种多样，每种设备都具有各自的特点，设备的安全等级参差不齐，给水利工控系统安全防护带来非常大的困难[6]。

3　水利工控系统网络安全存在的主要问题

3.1　从技术层面上考虑　水利工控系统网络安全存在的主要问题表现在以下5个方面：(1)网络结构上存在的安全问题。水利工控系统网络内部虽然采取了一些安全隔离或者访问认证的措施增加网络安全，如横向隔离、纵向加密等措施，但仍缺乏全面有效的网络边界防护、访问加密认证等安全防护措施。有些水利工控生产控制网和管理网直接连接，只采用传统的防火墙进行边界防护，生产控制网和管理网在同一网段内，管理网直接访问生产控制网等[7]。(2)设备本体存在的安全问题。水利工控系统中的工控机、PLC、移动介质、交换机等大多采用国外品牌，这些设备存在大量漏洞未修复或未及时修复，并且缺乏必要的有效措施进行防护，这些漏洞大多为拒绝服务、远传代码执行和缓冲区溢出等，这些漏洞如果被黑客利用，将引起设备故障或非法操作[8]。(3)行为审计方面存在的安全问题。现有的水利工控系统大多缺乏必要的技术手段对工控网络进行监测和审计；未部署监测审计设备，不能及时监测工控网络中的异常流量；未对工控系统账户进行定期审计，并且缺乏对违规操作、越权访问等行为的监测审计。(4)维护严重依赖系统集成商。有的虽然开放远程维护端口，但缺乏监测审计，对系统集成商没有进行严格的管控，事故发生后不能有效的对关键操作行为进行溯源和定位。(5)自主可控方面存在的安全问题。水利工控系统普遍缺乏自主可控的设备对工控网络安全进行防护，工控网络的大部分工控设备及服务由国外主导，无法实现自主可控。还无法在工控设备的应用层、内核层、硬件层等的设计和生产过程中加入自主可控的可信软硬件，建立系统的主动免疫机制，提高对恶意代码攻击的防护能力[9]。

3.2　从管理层面上考虑　水利工控系统网络安全存在的主要问题主要表现在以下3个方面：(1)管理机制不健全，生产管理部门注重工控系统的功能性而忽略行为安全性，普遍缺乏完善的风险评估、运行维护、安全审计、突发事件的应急处理方案等，现场运行人员安全意识薄弱，很少进行专业培训，违规操作现象经常发生。(2)维护行为严重依赖系统集成商，对其行为没有进行有效监管，甚至出现系统集成商私自对设备进行远程维护而没有通知生产管理部门的现象，造成生产运行异常。(3)缺乏行业标准，水利工程主管部门没有出台相应的法律法规和政策标准，使生产管理部门在进行监督管理和执法检查时缺乏相应的政策和法律依据。

4　水利工控系统网络安全问题的原因

从水利工控系统网络安全现状和网络安全存在的主要问题看出，水利工控系统网络安全风险主

要表现在：网络边界防护安全问题、主机、服务器安全问题、流量行为安全问题、管理和运维安全问题等4个方面。

4.1　网络边界防护安全问题　(1)除了横向隔离和纵向加密装置外，其他防护措施不足；(2)在生产控制大区之间虽然部属了传统防火墙，但无法识别专有工控协议，不能提供明确的允许/拒绝访问的能力。

4.2　主机、服务器安全问题　(1)采用传统网络防病毒软件(部分主机甚至无法安装杀毒软件)，无法及时更新恶意代码库，且容易误杀控制程序；(2)主机和服务器采用通用的操作系统，其漏洞直接影响系统的安全运行；(3)无法对重要程序的完整性进行检测，并在检测到完整性受到破坏后不具有恢复能力；(4)缺乏有效的技术措施切断病毒和木马的传播与破坏路径，如非法进程的运行、非法网络端口的打开与服务、非法USB设备的接入等[10]。

4.3　流量行为安全问题　(1)缺乏对非授权设备私自联到内部网络的行为进行检查、定位和阻断的能力；(2)无法有效的检测到网络攻击行为，并对攻击源IP、攻击类型等信息进行记录；(3)无法在网络边界处对恶意代码进行检测和告警，更新恶意代码库不及时；(4)缺乏有效的安全审计功能。

4.4　管理和运维安全问题　(1)未设立专门的信息安全岗位，信息安全管理和维护由业务部门按照自己的理解进行管理和维护，同时信息安全制度不完善。(2)在日常运行维护过程中普遍存在诸如介质未采用有效的手段进行管理和防护，容易造成病毒入侵和敏感信息泄露的风险。(3)存在账号共享、弱口令、未定期更改密码的问题，例如信号系统的用户权限普遍缺乏定期回顾检查，容易造成越权、权限滥用导致的安全事故。(4)安全防护应急预案存在事故预想不全面、内容不完整、相关要求缺乏可操作性等问题，缺少演练、培训和更新的相关内容，无法在真正的事故中及时响应和恢复系统[11]。

5　水利工控系统网络安全防护对策

水利工控系统网络安全与传统的互联网安全具有本质区别，甄别水利工控系统网络存在的安全风险与安全隐患，实施相应的安全保障策略是确保水利工控系统网络安全的有效手段。水利工控系统网络安全防护需要覆盖控制系统整个生命周期，具备自动学习、自动适应，自动生成防御策略的工业等级的全网安全监控的保护系统；要具有全面覆盖西门子、施耐德等全球主流厂商设备的安全数据库(包括设备漏洞库、网络模型库、设备风险统计)；同时，必须向基础设施企业提供漏洞挖掘、渗透攻击、安全策略、技术培训的全方位安全服务[12]。以水电站工控系统网络安全防护为例，从以下5个环节简要介绍水利工控系统网络安全防护技术解决方案，图3为水电厂工控系统网络安全防护技术解决方案原理图。水电厂的网络结构采用分层分布开放式运行方式设计，整个系统分为主控层、通讯层和现地层3个层级。主控层采用以太网通讯结构，设置操作员站、工程师站、数据服务器、通讯工作站、打印机等。通信层采用通信管理机、交换机等实现规约转换和设备通信，网络结构为双环网冗余结构。现地层主要包括机组LCU、公用LCU、闸门LCU等现地控制单元。

5.1　关键节点防护　在水电厂的现地层机组LCU、公用LCU、闸门LCU等现地控制单元与通信层环网之间部署智能保护终端，通过智能保护终端对工控系统现地层的关键LCU进行安全防护，利用已公开漏洞的攻击行为和流量信息进行有效识别和拦截。允许从受信的上位机发送的合规操作流量通过，基于动态学习和自适应的防护策略，达到对关键LCU、RTU的防护效果。

5.2　边界隔离防护　在水电厂生产控制大区与生产非控制大区之间部署智能工业防火墙，通过智能工业防火墙抵御来自外界伪基站接入渗透控制系统的风险。能够对控制源身份的合法性进行有效判断，对非法IP发送的数据包能够有效甄别和拦截，为控制系统网络边界提供全天候实时动态安全防护。

5.3　上位机防护　在水电厂主控层的工程师站、操作员站、OPC服务器以及SIS接口机上部署工控卫士，通过应用程序、网络、USB移动存储的白名单策略，防止用户的违规操作和误操作，阻止不明程序、移动存储介质和网络通信的滥用，有效提高工控网络的综合“免疫”能力。

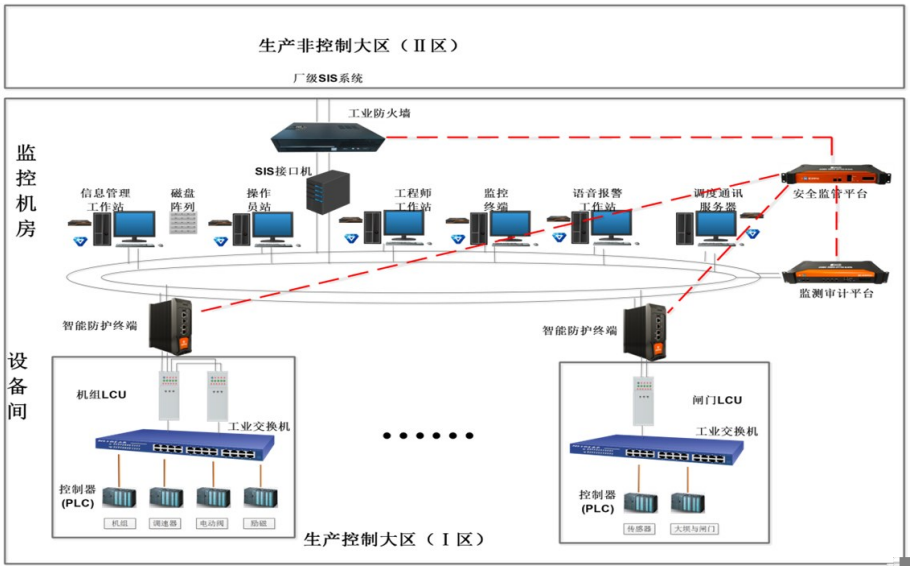

图3　水电厂工控系统网络安全防护技术解决方案原理

5.4　网络安全监测审计　在水电厂生产控制大区通信层环网、LCU子网旁路部署监测审计平台，对网络通信流量进行有效监视和威胁检测。对向工控网进行的生产数据非法收集、恶意攻击、数据篡改、违规操作进行告警和审计，为网络安全管理人员提供线索依据和事件还原功能，对违规操纵和网络攻击行为可实时告警。

5.5　集中安全监管　安全监管平台对部署在整个工控系统的安全设备实现统一化安全监管和运维。实时收集现场安全设备信息、分析威胁情报信息，基于安全分析模型，实现全局的态势安全预警与策略动态响应，实时发送现场的安全告警信息。

6　结论

（1）现阶段我国水利工控系统网络安全在技术方面和管理方面都存在较多问题。在技术方面主要存在网络结构安全、设备本体安全、行为审计安全、维护严重依赖系统集成商、缺乏自主可控防护手段等主要问题；在管理方面主要存在管理机制不健全、无法对系统集成商进行有效的监管、缺乏相应的政策和法律依据等问题[13]。

（2）引起此类问题的主要原因是在技术方面缺乏全面有效的网络边界防护、访问加密认证等安全防护措施；未部署监测审计设备，不能及时监测工控网络中的流量异常；设备存在大量漏洞未修复或未及时修复，并且缺乏必要的有效措施进行防护；大量采用国外品牌设备等。在管理方面安全制度不完善，安全防护应急预案存在事故预想不全面、内容不完整等。

（3）针对水利工控系统网络安全存在的问题，应采取以下防护手段或措施：通过智能保护终端对工控系统现地层的关键LCU进行安全防护，对非法操作进行有效拦截；在网络边界部署智能工业防火墙，抵御来自外界伪基站接入渗透控制系统的风险；在主控层的工程师站、操作员站、OPC服务器以及SIS接口机上部署工控卫士，防止误操作和违规操作；对网络通信流量进行有效监视和威胁检测，对违规操纵和网络攻击行为实时告警；最后通过安全监管平台，对部署在整个工控系统的安全设备实现统一化安全监管和运维。

参　考　文　献：

[1]　2016年工业控制网络安全态势报告[R]. 北京匡恩网络科技有限公司，2016.
[2]　郭娴. 互联网+时代下工业控制系统网络安全[J]. 自动化博览，2015(7)：64-65.

[3] 张志华，秦继伟，郭江．水电站控制系统网络安全现状及安全对策[J]．水电站机电技术，2017，40(5)：64-67．
[4] 郭江，张志华．工控系统网络安全现状及风险分析[C]//抽水蓄能电站自动控制技术应用研讨会-2016年学术交流会论文集．2016．
[5] 胡明远，张志华．水电站工控网络安全现状及解决方案[C]//2017年学术交流会论文集．北京：中国水力发电工程学会信息化专委会、中国水力发电工程学会水电控制设备专委会，2017．
[6] 胡明远，张志华．泵站工控网络安全现状及解决方案[C]//中国水利学会泵及泵站专业委员会-2017年学术年会．2017．
[7] STOUFFER K A，FALCO J A，SCARFONE K A．SP800-82．Guide to Industrial Control Systems(ICS)Security：Supervisory Control and Data Acquisition(SCADA)systems，Distributed Control Systems(DCS)，and other control system configurations such as Programmable Logic Controllers(PLC)[M]．National Institute of Standards & Technology，2011．
[8] 郭江，张志华，张志民．水利工业控制系统网络安全问题初探[C]//中国水利学会泵及泵站专业委员会-2015年学术年会论文集．2015．
[9] 王孝良，崔保红，李思其．关于工控系统信息安全的思考与建议[J]．信息网络安全，2012(8)：36-37．
[10] 刘威，李冬，孙波．工业控制系统安全分析[J]．信息网络安全，2012(8)：41-43．
[11] 熊琦，彭勇，戴忠华，等．工业控制系统的安全风险评估[J]．中国信息安全，2012(3)：57-59．
[12] 高洋，彭勇，谢丰．美国工控安全保障管理的启示[J]．中国信息安全，2012(3)：44-47．
[13] 郭江，张志华．水电厂工控系统网络安全风险评估概述[J]．水电站机电技术，2018，41(2)：68-70．

Problems and countermeasures of cybersecurity on industrial control systems in water projects

GUO Jiang，CHEN Fujun，ZHANG Zhihua

(*Tianjin Instiute of Hydroelectric and Power Research*，
China Institute of Water Resources and Hydropower Research，*Tianjin* 301900，China)

Abstract：In recent years，industrial control network security incidents have happened frequently，and increased year by year. The impact of security incidents is more and more serious，which even threatens national security gradually. Water projects are an important part of the national key infrastructure. With the development of "China made 2025" and "two integration"，more and more intelligent equipment，computer technology and network technology are applied to industrial control system，which make the industrial control system vulnerable to management network，Internet virus，Trojan horse and hacker. This paper introduces the main problems existing in the aspects of technology and management status，and the main cause of water industrial network security problems，focusing on the protection and safety of water work points of industrial control system network and security solutions，and with the control system of water power plant as an example gives the specific protection measures.

Keywords：Industrial control systems in hydro projects；industrial control systems cybersecurity；aggregated security countermeasure；risk assessment

(责任编辑：杨　虹)