# 浅谈枕头坝电站电力监控二次安全防护系统建设

靳 帅, 李 建 清
(国电大渡河枕头坝发电有限公司,四川 乐山 614700)

**摘 要**:随着计算机技术和网络通信技术在电力系统中的广泛应用,电力监控系统也逐步超越传统概念,与信息化网络结合得愈加紧密。网络技术的应用不仅给电力系统带来生产力的提高,同时也对电力监控系统的安全性提出了严峻的挑战。一旦电力生产控制系统网络遭到病毒或黑客的攻击,后果将不堪设想。本文结合枕头坝电站二次安全防护系统建设的经验,重点阐述了二次安全防护系统建设的原则、安防系统布置的方式,并结合具体实践提出了有效应对监控系统和工控网络安全威胁的管理方法。

**关键词**:安全防护系统;建设原则;系统布置;管理
**中图分类号**:[TM622];X924.3;S605+.3 **文献标识码**: B **文章编号**:1001-2184(2020)01-0091-04

## Discussion on Construction of the Secondary Safety Protection System for Power Monitoring of Zhentouba Hydropower Station

JIN Shuai, LI Jianqing
(Guodian Dadu River Zhentouoba Power Generation Co., Ltd., Leshan, Sichuan, 614700)

**Abstract**: As the wide application of computer technology and network communication technology in the power system, the power monitoring system gradually goes beyond the traditional concept, and is more and more closely combined with the information network. The application of network technology not only improves the productivity of power system, but also challenges the security of power monitoring system. Once the power production control system network is attacked by virus or hacker, the consequences will be unimaginable. Based on the experience of secondary safety protection system construction in Zhentouba Hydropower Station, this paper focuses on the principle of secondary safety protection system construction and the layout process of security system, and puts forward effective management methods to deal with the safety threats of monitoring system and industrial control network in combination with specific practice.

**Key words**: safety protection system; construction principal; layout of system; management

## 0 引 言

近年以来,工控领域发生了数起网络安全事故,电力监控系统的安全形势日益严峻,开展电力监控安防工作,提升工控系统整体安全防护水平,建立和完善电力监控二次安全防护系统,对保障电力系统的安全稳定运行具有重要的意义[1]。

枕头坝电站作为四川电网的骨干电源点,其安全生产对电网的稳定运行具有重要作用。通过电力监控二次安全防护系统建设,加强电站电力监控系统安全防护水平,抵御黑客及恶意代码等对电站电力监控系统进行的恶意破坏和攻击以及其它非法操作[2],以满足《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》(国能安全〔2015〕36 号)《电力监控系统安全防护规定》发改委 14 号令的相关要求和规定,从而有效地防止电站监控系统的瘫痪和失控及由此导致的电站一次系统事故和其他事故,以保障电力系统整体的安全运行。

## 1 安全防护系统建设原则

枕头坝电站按照“安全分区、网络专用、横向隔离、纵向认证”电力监控系统的安全防护总体原则,结合电站实际情况,根据能源监管办及国家电网公司相关文件要求,制定具体的建设原则,以保障电力监控系统和调度数据网络的安全[3]。

### 1.1 加固操作系统

**收稿日期**:2019-10-09

电站内监控系统关键应用系统的主服务器,以及网络边界处的通信网关机等,使用安全加固的操作系统。加固方式包括:关闭接口、清除弱口令、升级系统配置、安装系统补丁、采用专用加固软件强化操作系统、及时清除无用的应用程序等;非控制区的网络设备与安全设备采用身份鉴别、访问权限控制、会话控制等安全配置加固。对于外部存储器、打印机等外设的使用严格管理;对于闲置的数据接口采用物理封禁和软件封禁两种方式彻底断绝移动介质中的数据隐患带来的威胁。

### 1.2　布置网络入侵检测系统

在安全区 I 与安全区 II 分别布置网络入侵检测系统,保证安全防护能实时、动态应对安全事件,增强对网络行为的监察、控制和审计能力,检测探头布置在电力调度数据网接入交换机侧,及时捕获网络异常行为、分析潜在威胁、进行安全审计。

### 1.3　配置漏洞扫描系统

安全 I 区与安全 II 区配置漏洞扫描系统,定期扫描主机服务器系统、数据库及系统配置并进行加固;定期对网络的不同断面进行漏洞扫描,及时发现安全隐患。

### 1.4　布置恶意代码防护系统

生产控制大区内统一布置恶意代码防护系统,采取防范恶意代码措施。对生产控制大区中的所有计算机统一进行病毒定义码更新、防病毒政策设定、病毒情况监控,手动、定时病毒扫描及清除、病毒日志及汇总报表以及集中隔离未知病毒,并隔离有病毒的客户端,手工定期升级恶意代码防护系统病毒库。

### 1.5　采取安全审计措施

生产控制大区采取安全审计措施,把安全审计与安全区网络管理系统、综合告警系统、IDS 管理系统、敏感业务服务器登录认证和授权、关键业务应用访问权限相结合。

### 1.6　设置安全隔离装置

在生产控制大区与管理信息大区之间设置经国家指定部门检测认证的电力专用横向单向安全隔离装置,隔离强度接近物理隔离。电力专用横向单向安全隔离装置作为生产控制大区与管理信息大区之间的必备边界防护措施,是横向防护的关键设置。生产控制大区内部的安全区之间采用具有访问控制功能的网络设备、防火墙的设施,实现逻辑隔离。

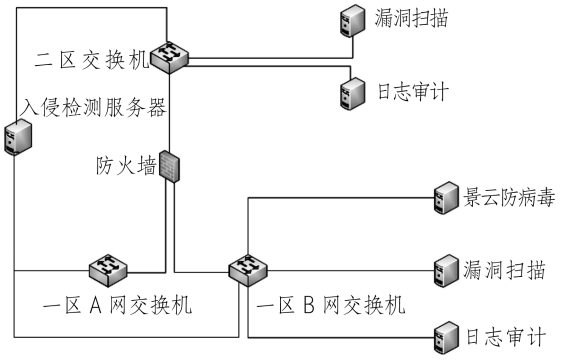


图 1　枕头坝电站二次安防系统链路图

## 2　安全防护系统布置

### 2.1　安全分区

按照《电力监控系统安全防护总体方案》:将电站基于计算机及网络技术的业务系统划分为生产控制大区和管理信息大区,并根据业务系统的重要性和对一次系统的影响程度将生产控制大区划分为安全控制 I 区和安全控制 II 区,重点保护生产控制以及直接影响电力生产与机组运行的系统,该分区原则满足安全可靠的要求[4]。枕头坝电站安全分区情况见表 1:

**表 1　枕头坝电站安全分区情况**

| 序号 | 安全区 | 系统名称 | 备注 |
|---|---|---|---|
| 1 | 安全Ⅰ区 | 电站计算机监控系统 | |
| 2 | | 主设备状态监测系统 | |
| 3 | | 微机五防系统 | |
| 4 | | 电能量计量系统 | |
| 5 | 安全Ⅱ区 | 保护信息子站系统 | |
| 6 | | OMS 系统 | |
| 7 | 管理信息大区 | 电站 MIS 系统 | |
| 8 | | ON－CALL 系统 | |

### 2.2　网络专用

调度数据网是与生产控制大区相连接的专用网络,承载电力实时控制、在线生产交易等业务。电站端的电力调度数据网在专用通道上使用独立的网络设备组网,在物理层面上实现与电力企业其他数据网及外部公共信息网的安全隔离。电站端的电力调度数据网划分为逻辑隔离的实时子网和非实时子网,分别连接控制区和非控制区,符合网络专用的原则。

### 2.3　横向通信防护

横向隔离是电力监控系统安全防护体系的横向防线。枕头坝电站高度重视网络边界的安全防护，为满足电站 ON－CALL 系统数据传输的需要，在生产控制大区与信息管理大区之间布置了一台南瑞正向隔离装置，取消了原设计中的反向隔离装置，只允许业务数据从生产控制大区向信息管理大区单向传送；在控制区与非控制区之间布置硬件防火墙实现逻辑隔离，同时根据业务需要对防火墙进行策略配置，以确保控制区内数据的绝对安全。

### 2.4　纵向通信防护

纵向加密认证是电力监控系统安全防护体系的纵向防线。电站生产控制大区与调度数据网的纵向连接处设置经过国家指定部门检测认证的电力专用纵向加密认证装置，实现双向身份认证、数据加密和访问控制。

电站生产控制大区所连接的广域网为电力调度数据网 SPDnet，采用 MPLS－VPN 技术为安全区Ⅰ、Ⅱ分别提供两个逻辑隔离的 VPN。在生产控制大区内，分别配置了 2 套电力专用纵向加密认证装置，实现网络层双向身份认证、数据加密和访问控制，满足电力监控系统防护的要求[5]。

### 2.5　综合安全防护体系

综合防护是结合国家信息安全等级保护工作的相关要求对电力监控系统从主机、网络设备、恶意代码防范、应用安全控制、审计、备份及容灾等多个层面进行信息安全防护的过程。

#### 2.5.1　防病毒系统

在电站安全Ⅰ区、II 区中分别布置一套景云网络防病毒系统。对生产控制大区中的所有计算机统一进行病毒定义码更新、防病毒策略设定、病毒情况监控，手动、定时的病毒扫描及清除、病毒日志及汇总报表以及集中隔离未知病毒，并能隔离有病毒的客户端。每月由专人定期升级防病毒系统病毒库，提高抗病毒能力。

#### 2.5.2　安全审计系统

在安全Ⅰ区和安全 II 区分别配置一套启明星辰 TSOC－SA2100 安全审计装置。通过 SNMP 协议的方式获取安全设备（如防火墙、IDS 、专用隔离设备、防病毒系统等）和调度数据网设备的安全事件信息，对网络安全事件信息进行集中分析过滤、处理、保存。

#### 2.5.3　主机加固

按照二次安防对生产大区的核心服务器配置主机加固的要求，对全站具备操作系统的主机或服务器中统一配置一套北京信达主机加固软件，强化操作系统访问控制能力以及配置安全的应用程序。并在日常工作中加强对服务器登录账户和口令的管理和优化，注重对操作系统的异常情况分析检测，及时发现和排查系统漏洞和问题[6]。

#### 2.5.4　漏洞扫描系统

在安全Ⅰ区和安全Ⅱ区分别配置一套启明星辰 CSNS－H3 漏洞扫描系统。对安全Ⅰ区和安全Ⅱ区的服务器、数据库、主机和网络设备定期手动扫描弱配置并进行加固；每月由专人定期对网络的不同断面进行漏洞扫描，及时发现安全隐患。

#### 2.5.5　入侵检测装置

枕头坝电站分别在生产控制区和调度数据网分别布置一套启明星辰网络入侵检测系统。生产控制区入侵检测装置检测探头布置于工程师站、两台集控通讯服务器、Ⅱ区接入交换机进行实时检测；调度数据网入侵检测装置检测探头布置于省调接入网实时和非实时交换机进行检测[7]。从而保证安全防护系统能实时、动态应对安全事件，增强对网络行为的监察、控制和审计能力。

#### 2.5.6　网络机柜

为保证二次安防系统的安全高效运行，配置一套标准网络机柜用于布置二次安防设备，做到专柜专用，同时提供两路冗余电源，保证供电电源的可靠。

## 3　安全防护系统管理

为充分发挥综合安全防护系统作用，提高抵御网络安全风险的能力，枕头坝电站在系统建设中制定了严格的管理规定，定期开展相关作业，不断升级优化系统功能，以保证安全防护体系能够有效应对监控系统和工控网络安全威胁，时刻发挥出最大的作用。

### 3.1　口令更新

针对系统加固，采用定期对关键服务器、边界防护设备等系统用户口令进行更新，口令不少于十位，并采用字母大小写加数字加至少三位特殊字符的组合。

### 3.2　漏洞扫描

定期对漏洞扫描系统漏洞库进行离线更新，

并手动对相关系统进行漏洞扫描。

3.3　记录备份

定期对入侵检测规则库进行离线更新,及时处理入侵报警信息,对装置运行记录进行备份。

3.4　手动查杀

定期对日志审计系统的日志审计记录进行核查并进行备份,对防恶意代码系统病毒库进行离线更新,并对相关系统进行手动查杀。

3.5　升级更新

定期对网络边界防护装置如防火墙、隔离装置、纵向加密装置的配置文件及配置策略进行一次备份,当系统网络结构或业务内容发生变化时,及时对配置策略升级更新。

3.6　异地存放备份文件

对监控机房内各计算机节点的软件、配置文件、数据、日志审计系统的审计日志等重要信息进行备份并异地存放,确保系统一旦发生故障时能够快速恢复。

## 4　结　语

枕头坝电站电力监控系统二次安防系统的建设,完善了电站电力监控系统及调度数据网络的安全防护体系,满足电力二次安防相关的要求。同时也大大提高了抵御黑客及恶意代码等外部攻击和入侵对电力监控系统进行的恶意破坏和攻击,以及其他非法操作的能力,可有效防止系统瘫痪和失控、及由此导致的电站生产事故,从而有力地保障了枕头坝电站监控系统和工控网络的安全运行。

**参考文献:**


[]　骆文忠.电力二次系统安全防护体系运行分析[J].宁夏电力,2008,2008 年增刊:27－28.

[2]　《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》,国能安全〔2015〕36 号文.

[3]　杨　非;戴承栋;李东风.水电厂二次自动化系统安全防护的设计与研究[J].水电厂自动化,2011,32(3):46－50.

[4]　孙娅苹;李强;罗成 等.核电站电气二次系统信息安全防护策略研究[J].电信网技术,2017,(4):18－20.

[5]　陈玉平.电力调度自动化二次系统安全防护初探[J].自动化技术与应用,2009,28(8):132－134.

[6]　钱　明.风电企业信息网络安全防护体系建设探讨[J].科技创新与应用,2014,(7):52－53.

[7]　王　群;潘亮.紫坪铺水电厂二次系统安全防护简介[J].水电与新能源,2013,(1):52－56.



**作者简介:**

靳　帅(1990-),男,河南南阳人,助理工程师,从事水电站运行维护技术管理工作;

李建清(1975-),男,四川仁寿人,高级工程师,从事水电站管理工作.


**(责任编辑:卓政昌)**

(上接第 90 页)

看出:跌坎型消力池可以明显地降低临底流速,减小消力池底板因传统平底消力池高流速直接冲刷和高流速空化空蚀而导致的破坏。为了节约工程投资,跌坎也不能太高,否则开挖量过大,故应将跌坎的高度和入池水流流速及入池角度综合考虑。入池角度如果为仰角,虽然可以明显降低临底流速,但消力池内水流波动震荡较大。为了既降低消力池底板临底流速又减小池内壅水和水面波动,根据计算结果分析,跌坎消力池水流入池角度以俯角十度以内为宜。

**参考文献:**


[1]　四川大学水力学与山区河流开发保护国家重点实验室编,水力学,下册,第五版,91－102.

[2]　周立本.五强溪水电站右消力池修复设计[J].水力发电,2002,(5):25－28.

[3]　孙双科 ,柳海涛 ,夏庆福 ,王晓松.跌坎型底流消力池的水力特性与优化研究[J].水利学报,2005, 36(10):1188－1193.

[4]　张建民,李艳玲,杨永全,许唯临,曾雄辉,程浩.多股多层水平有压淹没射流消能特性研究[4].水利水电技术,2004,35(11):30－33.

[5]　黄秋君,冯树荣,李延农,吴建华.多股多层水平淹没射流消能工水力特性试验研究[J].水动力学研究与进展,A 辑,2008,23(6):694－701.

[6]　Lannder B E, Spalding D B.MathematicalModels of Turbulence [M] .Academic Press, London and New Tork, 1972:90－110.



**作者简介:**

刁　奕(1999-),女,四川成都人,四川农业大学水利水电学院水利水电工程专业 2017 级;

杨思远(1999-),男,湖南岳阳人,四川农业大学水利水电学院农业水利工程专业 2017 级;

龚月婷(1997-),女,四川绵阳盐亭县人,四川农业大学水利水电学院水利水电工程专业 2017 级;

郑　果(1997-),男,重庆潼南人,四川农业大学水利水电学院农业水利工程专业 2017 级;

杨　敏(1980-),女,陕西西安人,工学硕士,讲师,从事水利水电工程教学和科研工作.


**(责任编辑:吴永红　卓政昌)**