网络安全等级保护在大型水电站的实践

钟 健[1]，倪雅琦[2]
(1. 中国电力工程顾问集团公司西南电力设计院有限公司，四川 成都 610021；
2. 国网四川省电力公司信息通信公司，四川 成都 610041)

摘 要：按照《信息安全技术 网络安全等级保护基本要求》要求，对某大型水电站电力监控系统安全防护现状做出详细分析后，提出电力监控系统安全防护整改方案。整改方案严格遵守《信息安全技术 网络安全等级保护基本要求》《电力监控系统安全防护规定》等重要文件要求，涵盖了水电站主要的电力监控系统。在采取了有针对性的技术措施加强安全防护的同时，完善了水电站电力监控系统安全防护管理的建设。最后，对部分遗留问题进行了初步探讨，以便今后进一步完善电力监控系统安全防护体系建设。

关键词：电力监控系统；安全防护；网络安全等级保护；安全管理；水电站
中图分类号：TP309 **文献标志码**：B **文章编号**：1003－6954(2020)02－0084－07
DOI:10.16527/j.cnki.cn51-1315/tm.2020.02.019

Practice of Classified Protection of Cybersecurity in Large－scale Hydropower Station

Zhong Jian[1], Ni Yaqi[2]
(1. CPECC Southwest Electric Power Design Institute Co., Ltd., Chengdu 610021, Sichuan, China;
2. State Grid Sichuan Information and Telecommunication Company, Chengdu 610041, Sichuan, China)

Abstract: After a detailed analysis for the current situation of security protection in a hydropower station, the security architecture of power monitoring system in hydropower station is designed and proposed, which is strictly based on the "Information security technology－－Baseline for classified protection of cybersecurity" and "Regulations on security protection of power monitoring system" and covers the technology and management together. The design also involves most subsystems of the station, and is feasible to be put into practice. Finally, several remaining issues which need to be improved are discussed in order to enhance the security architecture.

Key words: power monitoring system; security protection; classified protection of cybersecurity; security management; hydropower station

0 引 言

随着计算机技术和通信技术在电力行业中的广泛应用，电力监控系统逐渐由传统生产控制设备范畴扩大到整个信息系统和通信网络，各系统之间的边界随着信息化逐渐模糊和融合，同时信息安全问题也从管理信息系统延伸到了生产控制系统的各个环节。因此，需要理清在《中华人民共和国网络安全法》、《信息安全技术 网络安全等级保护基本要求》(GB/T 22239－2019)(以下简称等保2.0)和国家发展和改革委员会颁布的《电力监控系统安全防护规定》等法律、标准要求下，如何组织实施电力行业网络安全防护，为发电企业等提供一个具备动态响应、持续进化的符合《中华人民共和国网络安全法》和等保2.0标准的整网安全保障体系。

1 电力监控系统安全防护与等保2.0的关系

《中华人民共和国网络安全法》自2017年6月1日开始施行。《信息安全技术 网络安全等级保护基本要求》自2019年12月1日开始施行，它是依据《中华人民共和国网络安全法》建立的国家层面的

网络安全标准体系，针对通用计算机信息系统，提出了安全技术应用、安全管理体系建设等方面普遍适用的规范要求[1]。

《电力监控系统安全防护规定》是国家能源局制定的网络安全行业标准，电力监控系统安全防护关注的重点是与电力安全生产中用于监视、测量、控制和调度电力生产及传输的业务系统和通信网络，并根据其对安全生产的重要性和业务特点，提出相关的安全防护措施和安全管理规范要求[2]。

电力监控系统安全防护的防护强度应满足或超过等级信息系统安全等级保护的要求。由于电力监控系统内部随着生产业务系统的升级也在不断更新、扩充、结合，安全要求也相应产生改变，《电力监控系统安全防护规定》其相关安全防护措施更加具有系统性、动态性和可持续性。因此，《信息安全技术 网络安全等级保护基本要求》是一个对信息网络系统安全防护体系建设通用的规范要求，也是对信息网络系统安全防护强度最基本的要求[3]；《电力监控系统安全防护规定》则是根据电力行业信息网络系统的特点，进行了有针对性的细化和加强，网络安全层级和界面清晰，操作性更强。

2 电力监控系统安全防护总体要求

电力监控系统安全防护的目的是防止电力监控系统的崩溃、误动和数据被非法访问，并造成电力设备故障或电力安全事故。电力监控系统安全防护的重点：一是防止来自系统外部非法访问获取信息和恶意攻击，特别是集团式攻击；二是防止内部非法访问和违规操作[4-6]。

纳入整改方案的电力监控系统安全防护分析的水电站核心电力监控系统包括：水电站计算机监控系统；相量测量装置(PMU)；安全自动装置系统；泄洪闸控制系统；船闸控制系统；消防火灾报警系统；110 kV 变电站监控系统；调功终端系统；电能量计量系统；故障信息处理系统；机组状态监测系统；水调自动化系统(水情自动测报系统)市场报价终端；大坝安全监测系统；工业电视系统；生产管理信息系统；临时接地线管理系统；办公 OA 系统；MIS 网。

整改思路主要为：

1) 调度数据网作为生产控制大区业务系统与调度端实时信息的专用通信通道，是电力监控系统安全防护纵向边界安全防护的一个着重点；电力监控系统与上级单位之间的纵向数据通信应作为纵向边界安全防护的一个重点；各电力监控系统之间的横向通信作为安全防护的另一个重点。

2) 水电厂各系统之间通过硬接线传输信号因不存在网络通信，应确认其为安全；而水电厂各系统之间的串行通信方式视其为安全。

3) 闸门控制系统实际包括泄洪闸控制系统、船闸控制系统以及进水口快速门。由于进水口快速门通过 I/O 口与计算机监控系统 LCU 相连实现远程控制，因此归入计算机监控系统。闸门控制系统在所提方案中由泄洪闸控制系统和船闸控制系统替代。

4) 严格禁止生产控制系统/装置的远程拨号维护接口。

5) 各业务系统内部的通信安全性应由生产厂家按照国家相关标准实施，在这里不再考虑。

根据上述思路，水电站电力监控系统安全防护边界防护和系统内部防护要求如下：

1) 通信安全需求

生产业务系统之间采用点对点串口通信应视为安全；生产业务系统设备之间网络通信需根据各业务系统安全分区的不同情况采取相应的横向隔离措施；生产业务系统/设备与调度端经调度数据网通信须采取纵向加密认证装置进行隔离；MIS 网与上级单位、调度端 DMIS 系统的网络通信应采取相应的隔离措施；出差人员与 MIS 远程拨号访问须采取 VPN 等技术和管理手段防止重要数据被窃取，防止该通道成为病毒传播和恶意攻击跨越防火墙的途径。通信网络连接图如图 1 所示。

2) 各电力监控系统安全需求

计算机监控系统内部应部署防病毒软件，防止病毒传播。系统主机和工作站的操作系统漏洞和应用系统漏洞存在被利用的风险，应及时封堵或升级，重要服务器和通信网关应进行主机加固。

水调自动化系统应具有病毒防护能力。

机组状态监测系统应部署防病毒软件，防止病毒传播。系统 Web 服务器与本系统的通信应进行物理隔离，实现数据单向传输，同时应保证 Web 数据与机组状态监测系统同步。

安全自动装置远方修改定值和控制的功能应屏蔽。故障信息处理系统 Web 服务应增加加密认证功能实现安全 Web，否则应关闭。

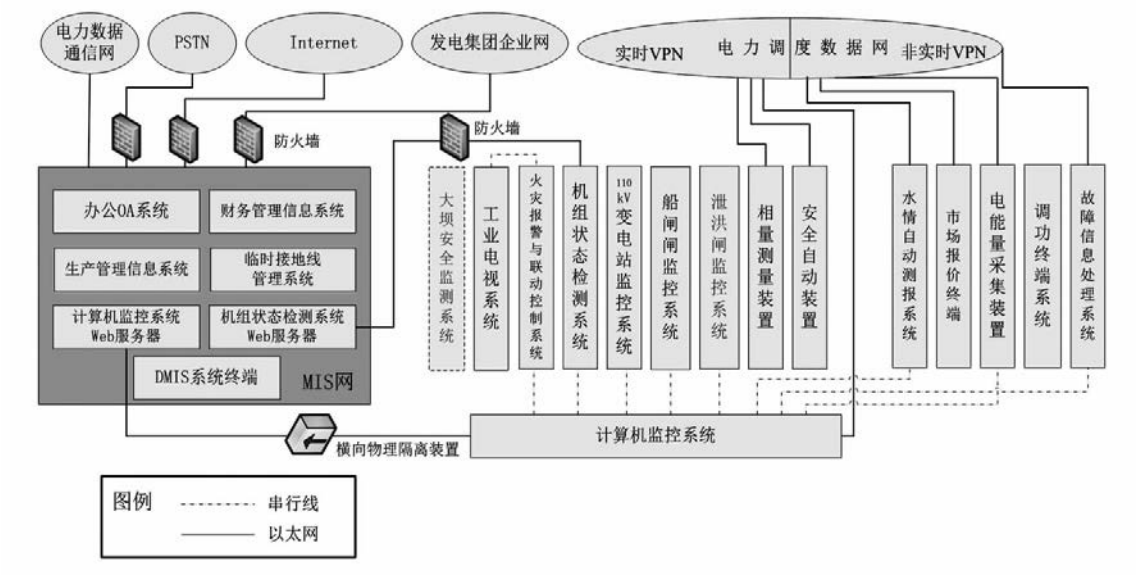

图 1　通信网络连接

市场报价系统作为电力市场运营系统的厂站侧组件，必须专机专用，与办公网络进行物理隔离；并配置防病毒系统。

MIS 网内重要服务器应采取有效的访问控制和隔离手段，封堵系统漏洞，过滤恶意代码病毒，阻挡网络攻击。各应用服务器应具有病毒防护能力。

移动设备是网络内部病毒传播的主要介质，应进行严格管理控制，采用比如安全 U 盘等措施。

各业务系统管理与操作人员、各终端使用人员的操作行为应得到有效监控，防护措施应能在一定程度上防止并可靠记录操作行为和恶意违规操作。

3) 全局安全需求

生产控制业务系统网络应能实时、可靠地响应安全事故，进行事故追忆，并具有学习功能。

水电站应定期对电力监控系统进行安全性评价，具有全面合理的电力监控系统安全防护管理体系。

3　业务系统保护等级测评

按照《信息安全技术 信息系统安全等级保护实施指南》(GB/T 25058 – 2010) 和《电力行业信息系统安全等级保护定级指导意见》确定水电站电力监控系统的安全保护等级。

电力监控系统的安全保护等级确定后，根据测评结果出具的信息安全等级保护测评报告，按照《信息安全技术 网络安全等级保护基本要求》管理规范和技术标准，开展电力监控系统安全建设工作，达到电站安全防护体系合规合法的总体目标。

4　电力监控系统安全防护措施

电力监控系统安全防护的总体策略是：安全分区、网络专用、横向隔离、纵向认证[2]。

针对水电站电力监控系统安全防护总体需求，同时遵循系统性、实用与先进结合、风险代价相平衡等原则，提出建立实时、主动、动态、由边界到核心的安全防护体系方案。

4.1　安全分区

防护方案所涵盖的电力监控系统依据《信息安全技术 信息系统安全等级保护实施指南》(GB/T 25058 – 2010) 和《电力行业信息系统安全等级保护定级指导意见》所确定的保护等级纳入相应的安全分区中。本期水电站业务系统划分为生产控制大区和管理信息大区两个大区。生产控制大区由具有实时控制功能的安全区Ⅰ和具有非实时控制功能的安全区Ⅱ组成，业务系统安全分区见图 2 所示。管理信息大区按照水电站业务管理需求划分为安全区Ⅲ、安全区Ⅳ[7]。业务系统安全分区如图 3 所示。

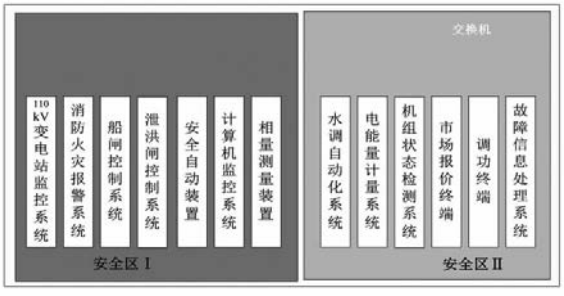

图 2　安全分区Ⅰ/Ⅱ

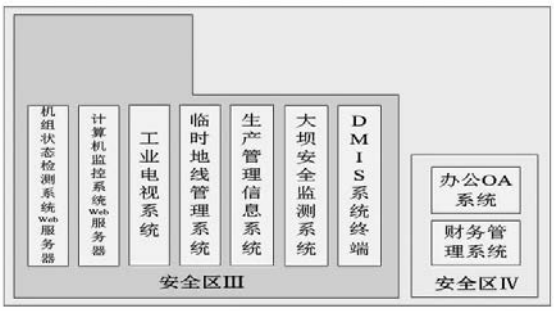

图3 安全分区Ⅲ/Ⅳ

水电站计算机监控系统和机组状态监测系统向MIS网提供的Web服务调整为独立的系统，迁移至安全区Ⅲ运行。

根据水电站的各业务网络连接情况，防护方案采用如图4所示链式拓扑结构实现安全区互连。

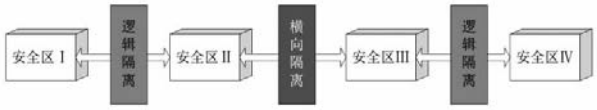

图4 链式结构

4.2 纵向通信防护

水电站纵向网络通信包括：1) 生产控制系统经调度数据网与调度端的通信；2) DIMS客户端经电力数据通信网与调度端通信；3) MIS网络经同集团公司通信。

第1项通信属于生产控制业务，远程通信采用纵向加密认证装置进行隔离；通过加密隧道、加载在加密隧道上的访问控制策略以及系统通信主机IP地址和端口的对应关系保证其传输数据的机密性、完整性。纵向加密认证装置可配置双机热备，确保设备高可靠性。

第2、第3项通信属于管理信息业务，采用国产硬件防火墙完成数据过滤和访问控制。防火墙应基于网络地址、通讯协议、通讯端口、用户、信息传输方向、操作方式、通讯时间、服务类型等因素配置控制策略，并能快速重组分片报文抵御分片攻击。

4.3 横向隔离

安全区Ⅱ和安全区Ⅲ区内交换机之间采用正向物理隔离装置实现数据以非网络方式从安全区Ⅱ发送到安全区Ⅲ，保证传输层以上数据完全单向传输，且最多返回1个字节的TCP应答数据。为确保设备高可用性，要求隔离装置采用双机网络热备份连接方式。同时，为提供安全区Ⅱ中水调自动化等系统从安全区Ⅲ获取数据的通道，须在安全区Ⅱ、Ⅲ区内交换机之间部署反向物理隔离装置，使用数字认证、病毒查杀和有效性检查等手段对纯文本数据进行过滤后将其从安全区Ⅲ摆渡到安全区Ⅱ。物理隔离装置的使用可极大提高生产控制大区的安全性，但同时也会造成FTP、SQL等应用层通信无法跨越隔离装置。因此必须对计算机监控系统和机组状态监测系统软件进行调整，以确保其Web功能的正常运行。

安全区Ⅰ、Ⅱ之间和安全区Ⅲ、Ⅳ之间采用国产防火墙逻辑隔离，对跨区的访问进行严格控制。

安全区Ⅳ采用国产防火墙与Internet隔离，配置完整的路由策略，对开放的协议、服务、端口、时段、用户、数据流向、连接数等进行严格控制。

4.4 入侵检测

生产控制大区统一部署一套分布式IDS，分别在安全区Ⅰ和安全区Ⅱ的区内交换机和调度数据网接入交换机镜像端口配置探测引擎，实时主动侦测攻击和非法操作。控制中心软件安装在安全区Ⅱ综合管理服务器上，接收扫描引擎事件上报并向扫描引擎下发安全策略。特征库的升级要求定期采用离线方式。

需要注意的是，目前商业化的入侵检测系统多数采用基于异常的检测方法，该检测方法误报率高，故不宜配置IDS与防火墙的联动策略。

4.5 病毒防护

由于安全区Ⅰ、安全区Ⅱ内的业务系统网络相对独立，不便于统一防病毒系统的形式，根据系统规模采用单机或网络方式的防病毒系统。

管理信息大区的应用基本上都建立在MIS网上，采用网络方式的防病毒系统。

病毒库由负责人定期采用离线方式升级。对UNIX或LINUX服务器和工作站以及嵌入式系统暂不考虑病毒防护。

4.6 漏洞扫描

漏洞扫描是一种主动的防范措施。漏洞扫描与防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络、主机和数据库的扫描，及时发现安全漏洞，评估网络风险；并根据扫描结果采取安装升级包、补丁包，修改各种网络隔离设备和数据库的访问控制策略等手段，避免非授权个人利用系统安全漏洞进行攻击或者非法访问。

4.7 安全审计

纵向加密认证装置、横向物理隔离装置、防火

墙、入侵检测、防病毒系统、主机、工作站等电力监控系统安全防护设备以及调度数据网接入设备本身都会产生自身运行状况和系统安全的日志。生产控制大区应建立安全审计管理平台，方便运行维护人员集中管理日志信息，借助相应工具分析、判断、预防和及时响应处理系统的安全事件，完成全面的日志分析、告警和综合安全管理[2]。

安全审计管理平台部署在安全区Ⅱ和管理信息大区的MIS网内，通过SNMP协议或SYSLOG等方式获取安全设备(如纵向加密认证装置、横向物理隔离装置、防火墙、IDS、防病毒系统等)、调度数据网接入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。通过合理的事件配置为管理人员提供及时、可靠的告警，实现全网的实时安全检测，清晰的记录可为安全审计提供有力的支持，统一标准化的管理功能可有效的整合生产控制大区的安全防护体系，衔接安全技术和安全管理，从全局高度维护网络的安全性。

4.8 主机加固

防火墙、IDS等网络安全产品解决了当前网络系统的一些问题，但由于这些安全产品大多独立于应用系统之外，并不能完全防护外部的入侵行为，也不能防止内部用户的破坏行为。而且通过渗透攻击，黑客最终将获得服务器系统管理员的权限，基于网络的安全产品将不再起作用。

水电站重要的主机(如：监控主服务器、重要的工作站/操作员站、通信服务器)运行的是实时系统的重要数据和业务进程，对可靠性要求更高。一旦出现了事故，事后无法追查、判断责任，无法迅速找到解决方案。因此主机加固做为核心防护是一项必须的措施，要保证重要的业务不停顿，重要的数据不被更改、删除、非法拷贝。除加强操作系统补丁管理、安全配置外，在核心系统上部署主机加固防护产品，对计算机监控系统、110 kV变电站监控系统、船闸控制系统、泄洪闸控制系统、水调自动化、生产管理信息系统的服务器、操作员站和通信服务器等进行安全配置和主机加固。

4.9 MIS网安全监控

水电站MIS网与Internet连接，且涉及的业务量大，终端多，用户类型相对复杂。虽然MIS网重要性不及生产控制系统，但由于内部存在相当数量的企业级保密数据且网络化的管理和办公方式日益深入，维护其安全将是电厂生产管理工作正常运行的重要保障。

管理信息大区应配置一套内网安全管理系统，实现严格可靠的网络管理，形成健康有序的网络环境，避免内部安全隐患造成边界防护的失效。

内网安全管理系统不间断监测服务器和网络设备的运行状况，采集相关运行日志，实现网络资源状态的集中监管；对重点业务系统进行精细化的监管；将网络设备、关键服务器及业务整合，发生故障时，及时告知故障点及故障可能波及的范围，尽可能减少故障修复时间和关键数据的损失；能够对内部网络操作进行监控和管理；具备远程监测和报警功能；并提供详细的网络性能和网络行为报告。

4.10 网络安全设置

在维护网络安全的同时，安全设备以及组网设备自身应由专人执行严格的安全设置，采取建立强健的身份认证、合理分配管理权限、限制不安全应用协议、关闭默认设置、信息加密等措施确保网络及安全设备的安全可靠。

5 建立安全管理机制

“技术是基础，日常管理是根本”，健全的管理是人与技术设备协调统一的保证。所提方案对水电站电力监控系统安全管理提出了以下几个方面的建议：1) 建立完善的安全管理组织机构和责任制度；2) 设备、应用及服务的接入管理；3) 建立日常运行的安全管理制度；4) 工程实施过程中的安全管理；5) 建立快速的安全事件响应机制；6) 建立分级的安全评估制度。

前3个方面对安全管理组织安排、安全职责划分、系统接入管理、人员管理、资源管理、保密工作、访问控制、系统维护、安全审计、应急备份、安全培训等提出了全面的建议，是安全管理工作的基础，更详细的内容可参考《信息系统安全管理要求》(GB/T 20269－2006)、《信息安全实用管理规则》(GB/T 19716－2005)等标准，作为安全管理机制基本思路和建设框架的参考，通过实际的执行、调整应尽早形成初步可行的电力监控系统安全防护管理规范。

6 安全评估

电力监控系统安全防护是一个长期动态的过程,方案设计仅是处在安全防护的初级阶段,在安全防护的基础框架上,定期的安全评估可促使新问题的发现和及时修正,在不断的循环中完善防护体系。

提出建立分级的安全评估制度,水电站作为基层单位首先必须配合上级的安全工作,定期进行全面安全评估,同时需建立可行的自评估办法,利用自评估逐步规范和加强安全管理,促进安全意识、机制的建立。同时自评估项目和标准也应不断完善和提高。

7 待进一步探讨的问题

所提水电站电力监控系统安全防护方案仅处于安全防护体系生命周期的初步建设阶段。从效率、安全等角度看,该方案尚存在以下需进一步研究和解决的问题:

1) 所提方案关注的主要是边界防护和核心防护两方面的安全需求。《信息安全技术 网络安全等级保护基本要求》已经将信息网络扩展到工业控制网络,其中安全计算环境关系到工控系统的主机应用安全、数据存储保护,是网络安全等级保护中三重防护重要组成部分。这将是下一步水电站电力监控系统安全防护的重点内容[4]。

2) 漏洞扫描、安全审计、入侵检测系统等安全防护设备提供了详细的资料辅助安全策略制定。但由于电厂安全防护负责人员大多只是电力专业背景,在缺乏专门训练的情况下,面对庞大的分析数据要坚持长期跟踪变化并实时做出应急反有一定的困难。可以考虑建设网络安全态势感知体系,实现对主机设备、网络设备、安防设备等的实时告警与运行状态在线监测,从静态布防到实时管控转变[5],达到以下目标:①外部侵入有效阻断。对外部侵入行为能够实时监视,及时阻断危害链路,保证电力监控系统不受入侵事件影响。②外力干扰有效隔离。对于外部产生紧急威胁事件,能够通过有效手段对涉及主机或设备进行有效隔离,保证威胁事件不会扩散传播。③内部违规及时发现。对于内部的越权访问和恶意操作,可及时发现并预警。

3) 区域电力数字证书系统的缺乏使得要在电厂等基层单位实现统一的身份认证机制和普及加密通信还需时日。

8 结 语

水电站电力监控系统安全防护实施方案如图5所示。方案严格地执行了相关文件的规定,符合电力监控系统安全防护和信息安全的原则性要求。尽管如此,上述问题仍应该在今后的生产管理中继续

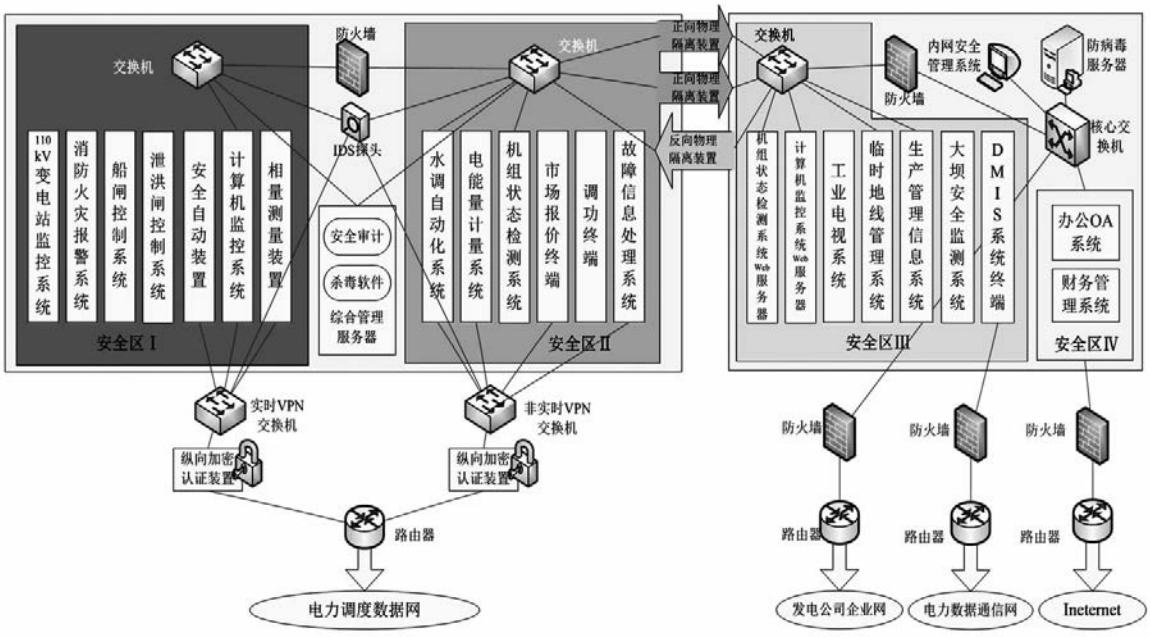

图5 电力监控系统安全防护实施方案

得到高度关注和进一步研究，根据技术的发展、环境因素的改变对方案做出合理的调整，以保证跟上安全形势的变化；为水电站提供一个具备动态响应、持续进化的符合《中华人民共和国网络安全法》和《信息安全技术 网络安全等级保护基本要求》的整网安全保障体系。

满足文件要求不是最终目的，安全工作要努力实现的是人员安全意识的提高、安全机制的建立和事故保障体系的完善，最终形成渗入生产管理各个细节的安全体系，而不仅仅是浮于文字的规定。

参考文献

[1] 中华人民共和国网络安全法[Z]. 2016.
[2] 中华人民共和国国家发展和改革委员会. 电力监控系统安全防护规定[Z]. 2014.
[3] 国家市场监督管理总局中国国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239－2019[S]. 北京: 中国标准出版社, 2019.
[4] 电力监控系统安全防护总体方案[S], 2015.
[5] 何占博, 王颖, 刘军. 我国网络安全等级保护现状与2.0标准体系研究[J]. 信息技术与网络安全, 2019, 38(3): 9－14.
[6] 赵志远. 等保2.0安全扩展要求讲了些什么[J]. 网络安全和信息化, 2019(6): 42－43.
[7] 周双进. 亭子口水电站二次系统安全防护方案[J]. 四川水利, 2018(5): 32－36.
[8] 国家能源局. 电力信息系统安全等级保护实施指南: GB/T 37138－2018[Z]. 2019.

作者简介:

钟 健(1972)，高级工程师，从事电力调度自动化、电力监控系统安全防护、网络通信等工作；

倪雅琦(1976)，高级工程师，从事电力调度自动化、电力信息系统建设、信息化产品研发等工作。

(收稿日期: 2019－12－26)

(上接第23页)

3 结 语

瞬时性故障的保护是MMC在柔性直流输电和直流电网领域应用必须解决的关键问题。前面提出了一种具备直流故障清除能力的三电平子模块拓扑，该拓扑无需任何附加的保护功率器件。经仿真验证了所提MMC拓扑在直流短路故障发生时能够在5 ms以内实现短路故障电流的自清除。

参考文献

[1] 徐政. 柔性直流输电系统(第二版)[M]. 北京: 机械工业出版社, 2016.
[2] International Electrotechnical Commission. High－voltage Direct Current (HVDC) Transmission Using Voltage Sourced Converters (VSC) [C]. IEC Tech. Rep. TR－62543, 2011.
[3] Soto－Sanchez D, Green T. Control of A Modular Multilevel Converter－based HVDC Transmission System[Z]. IEEE, 2011: 1－10.
[4] Norrga S, Xiaoqian L, Angquist L. Converter Topologies for HVDC Grids: Energy Conference(ENERGYCON) [C]. IEEE International, Cavtat, 2014.
[5] Marquardt R. Modular Multilevel Converter Topologies with DC－Short Circuit Current Limitation: Power Electronics and ECCE Asia (ICPE & ECCE) [C]. 2011 IEEE 8th International Conference on, Jeju, 2011.
[6] 薛英林, 徐政. C－MMC直流故障穿越机理及改进拓扑方案[J]. 中国电机工程学报, 2013, 33(21): 63－70.
[7] 薛英林, 徐政. 适用于架空线路输电的新型双极MMC－HVDC拓扑[J]. 高电压技术, 2013, 39(2): 481－487.
[8] Solas E, Abad G, Barrena J A. Modular Multilevel Converter with Different Submodule Concepts－Part I: Capacitor Voltage Balancing Method[J]. IEEE Transactions on Industrial Electronics, 2013, 60(10): 4525－4535.
[9] Solas E, Abad G, Barrena J A. Modular Multilevel Converter with Different Submodule Concepts－Part II: Experimental Validation and Comparison for HVDC Application[J]. IEEE Transactions on Industrial Electronics, 2013, 60(10): 4536－4545.

作者简介:

常 非(1986)，博士，工程师，研究方向为电力电子技术在电力系统中的应用与继电保护。

(收稿日期: 2020－01－16)