某电厂二次系统安全防护方案的设计与实现

曾 玉，马进霞，张立平

（中南电力设计院，湖北 武汉 430071）

摘要： 某电厂按照“安全分区、网络专用、横向隔离、纵向认证”的原则，对二次系统采用链式防护结构，在相关部位布置了防护设备。介绍了某电厂二次系统安全防护方案的设计与实现，并详述了该电厂二次系统安全防护设备的配置及对相关系统的改造。

关键词： 电厂； 二次系统安全防护； 改造

Design and implementation of secondary system security protection scheme of a power plant

ZENG Yu, MA Jin-xia, ZHANG Li-ping

(Central Southern Electric Power Design Institute, Wuhan 430071, China)

Abstract: According to the secondary system security protection principle “security location, network specialization, transverse isolation, longitudinal certification”, a power plant installs its protection devices on related systems. This paper describes the design and implementation of the scheme which uses chain-structure. Also, configuration scheme of the secondary system security protection and the reformation of the related secondary system are introduced detailedly.

Key words: power plant; secondary system security protection; reformation

中图分类号： TM76 文献标识码：B 文章编号： 1674-3415(2009)08-0072-07

1 总论

1.1 火电厂二次系统安全防护总体方案

根据《电力二次系统安全防护规定》的要求，火电厂二次系统原则上划分为生产控制大区和管理信息大区。生产控制大区可分为控制区（安全区 I）和非控制区（安全区 II）。安全防护的重点是保证电厂监控系统的安全可靠。总体目标包括：

(1) 防止发电厂监控系统服务等核心业务（即电力生产）中断。

(2) 防止发电厂监控系统本身崩溃。

(3) 抵御外部人员对发电厂监控系统发起的恶意破坏和攻击，及可能对相连的调度自动化系统的影响。

(4) 防止利用病毒、木马等恶意程序,从发电厂监控系统局域网内部发起的对电力生产及相连的调度自动化系统的恶意破坏和攻击。

(5) 保护发电厂监控系统实时和历史数据，主要防止数据被非授权修改。

火电厂二次系统安全防护总体方案如图 1 所示。

1.2 安全防护实施总体策略

1.2.1 安全分区

根据系统中业务的重要性和对一次系统的影响程度进行分区，所有的系统都必须置于相应的安全区内；对实时控制系统等关键业务采用认证、加密等技术实施重点保护。

1.2.2 网络专用

建立调度专用数据网络，实现与其它数据网络物理隔离。并以技术手段在专网上形成多个相互逻辑隔离的子网，以保障上下级各安全区的纵向互联在相同的安全区进行，避免安全区纵向交叉。

1.2.3 横向隔离

采用不同强度的安全隔离设备使各安全区中的业务系统得到有效保护，关键是将实时监控系统与管理信息系统等实行有效安全隔离，隔离强度应接近或达到物理隔离。

1.2.4 纵向认证

采用认证、加密、访问控制等手段实现数据的安全传输以及纵向界的安全防护。

2 某电厂二次系统安全防护方案

2.1 某电厂各二次系统业务需求

2.1.1 SIS 系统

厂级监控信息系统 SIS 主要是对全厂实时信息

的管理和显示。它接收由机组级 DCS 网络、辅助系统监控网络、电气网络控制系统 NCS、烟气脱硫 DCS、电气网络控制系统 FECS、机组振动监测 TDM 等系统来的信息并将相应的主要实时信息传送到厂级管理信息系统。

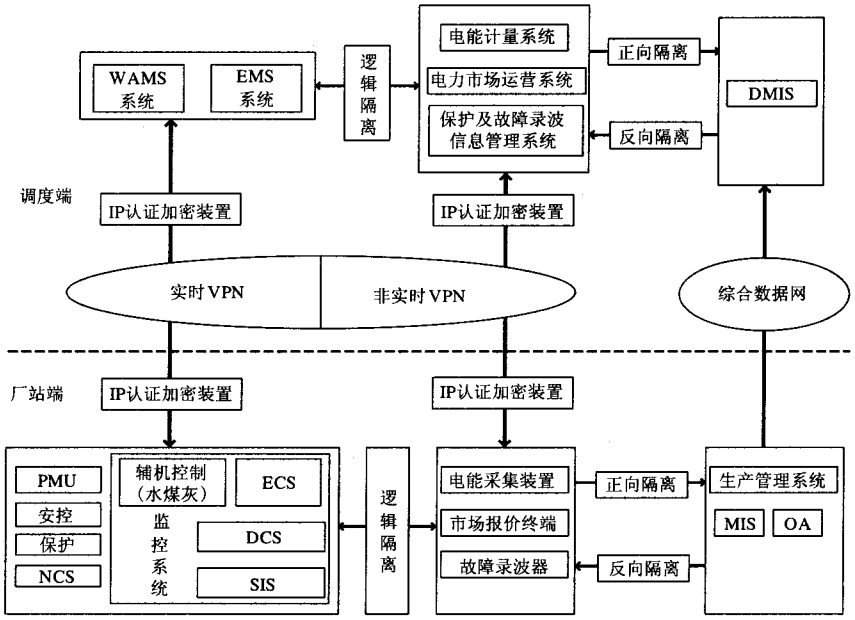

图 1　火电厂二次系统安全防护总体方案框图

Fig.1 Scheme of secondary system security protection for thermal power plant

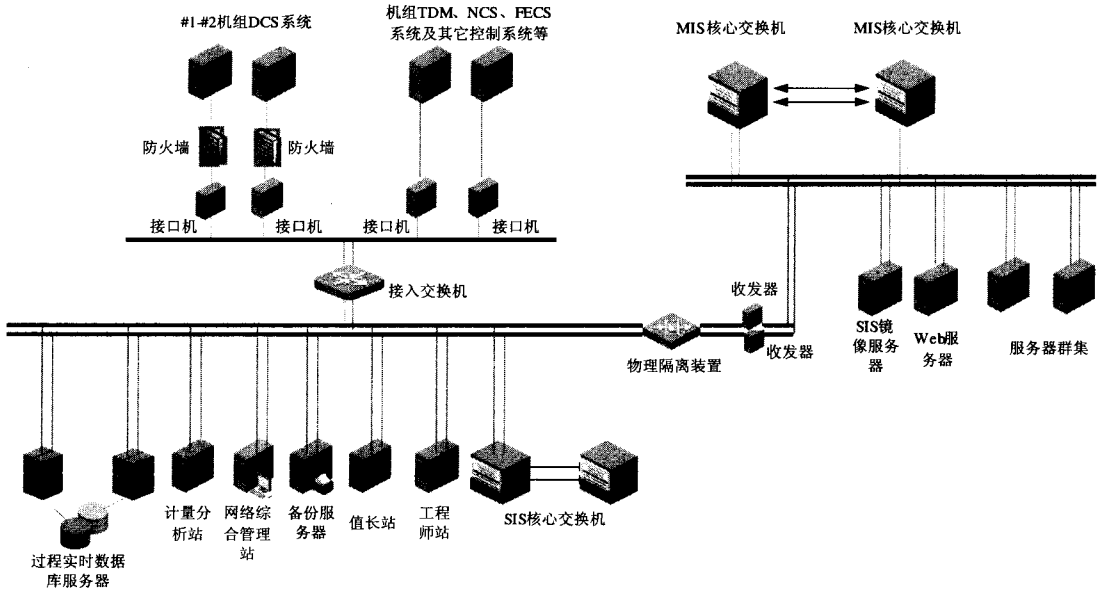

图2　某电厂SIS系统网络拓扑结构图

Fig.2 Network topology of the SIS system of a power plant

SIS 系统设置有接入交换机、过程实时数据服务器、核心交换机、网络综合管理站、值长站、工程师站、镜像服务器、WEB 服务器等。设备均布置于 SIS 间 SIS 机柜中。

SIS 信息需送至 MIS 系统，供厂级管理人员浏览。为此，设置了镜像服务器和 WEB 服务器，MIS 所需 SIS 信息均从此两服务器上读取。

某电厂 SIS 系统网络拓扑结构图参见图 2。

2.1.2 MIS 系统

厂级管理信息系统 MIS 主要是对全厂非实时信息的管理和显示(如人事管理、备品备件的管理)，它的终端在生产办公楼，为厂级管理人员服务的。

MIS 系统的中心交换机放置在化水车间三层，其它交换机放置在集控楼、行政办公楼、材料库、检修楼、输煤配电楼、检修公寓、运行公寓。

MIS 系统目前仅从 SIS 系统和电能计量系统读取相关数据。

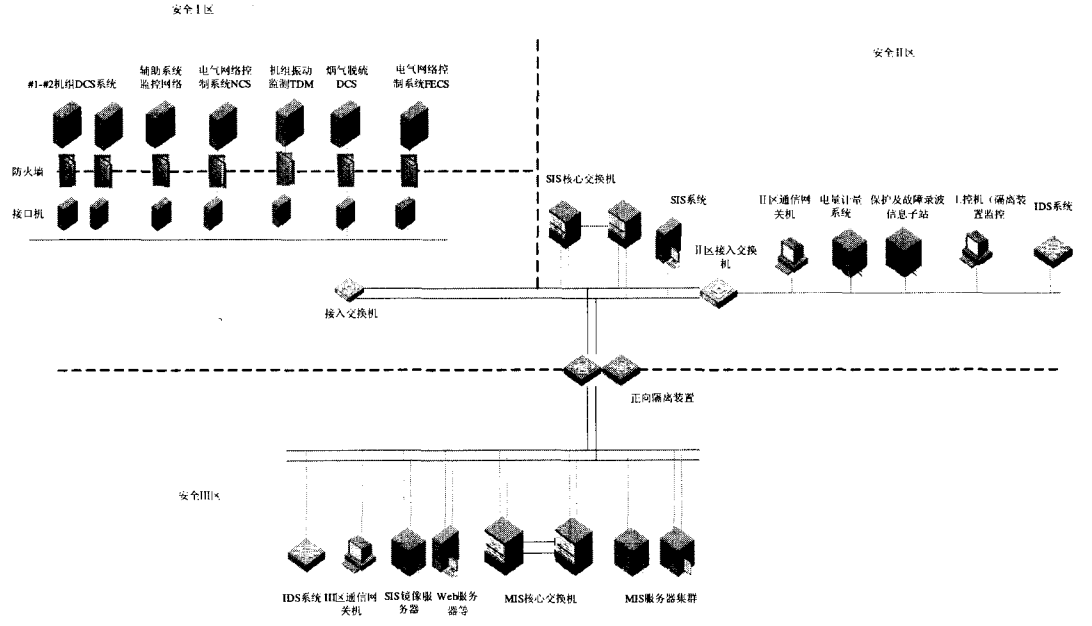

图 3 某电厂二次系统横向防护方案

Fig.3　Transverse protection scheme for a power plant

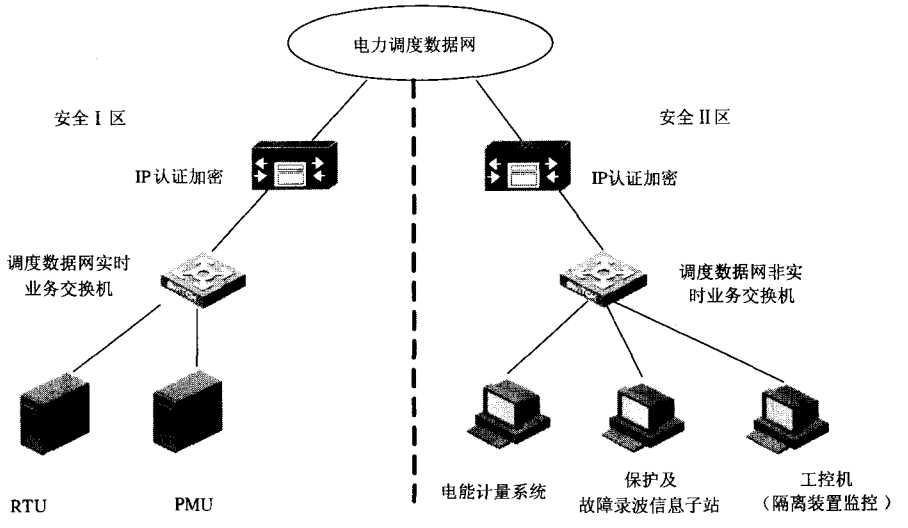

图 4 某电厂二次系统纵向防护方案

Fig.4 Longitudinal protection scheme for a power plant

2.1.3 RTU 系统

电厂配置一套上海惠安公司微机远动装置，采集电厂 500 kV 出线、发电机组、高压厂用变、高压公用变、起备变相关远动信息。远动信息通过电力调度数据网及专用通道送至华中网调及湖北省调，并接收网调的 AGC 命令。

RTU 系统与电厂其它系统目前暂无信息交换。

2.1.4 PMU 系统

电厂 PMU 采用 CSS-200 相量测量装置。采集电厂两回出线、升压变及机组信息。

PMU 采用电力调度数据网方式将相角信息传送至华中网调主站系统。

PMU 系统与电厂其它系统目前暂无信息交换。

2.1.5 保护及故障录波信息子站系统

电厂保护及故障录波信息子站系统采用武汉中元华电公司的 ZH-201 产品，实现对厂内保护和故障录波信息的统一管理，并将保护和故障录波信息通过电力调度数据网发送至调度端。

厂内保护装置(含发变组保护和起备变保护)、中元华电集中录波装置、通过以太网口接入保护及故障录波信息子站系统专网。

保护及故障录波信息子站同时通过以太网口接入厂内 NCS，实现信息共享。

保护及故障录波信息子站系统与厂内其它系统目前暂无信息交换。

2.1.6 电能计量系统

电厂配置了一套电能计量系统，采用北京煜邦电力技术有限公司产品。电能计量系统以电力调度网络和拨号方式将电能量数据上传至调度端。

电能计量系统数据需送至 MIS 系统，供厂级管理人员浏览。

2.1.7 辅助报价决策系统

辅助报价决策系统的主要功能包括：市场外部信息分析（包括负荷分析）、负荷预测、报价决策、结算/评估、预调度计划、风险分析、敏感性分析、机组安全域分析、机组组合、与管理信息数据接口软件（包括：合同管理、成本分析、燃料管理、检修计划）等。

辅助报价决策系统需读取电能计量系统数据。

因华中电网电力市场技术支持系统的方案还未确定，某电厂尚未建立此系统。

2.2 二次系统的安全区划分

根据二次系统的特点，各相关业务系统的重要程度、数据流程、目前状况和安全要求，将某电厂整个二次系统分为两个大区：生产控制大区和管理信息大区。

2.2.1 生产控制大区

（1）安全区 I：实时控制区

安全区 I 的典型系统包括机组 DCS、水煤灰系统、烟气脱硫 DCS、机组振动监测系统 TDM、电气网络控制系统 FECS、RTU、PMU、NCS。其主要使用者为调度员和运行操作人员，数据实时性为秒级。

安全区 I 是电力二次系统中最重要的系统，安全等级最高，是安全防护的重点与核心。

（2）安全区 II：非实时控制生产区

安全区 II 的系统包括厂级监控系统 SIS、保护及故障录波信息子站系统、电能量计量系统等。该区数据的实时性为分钟级、小时级。

安全区 II 的 SIS 系统需采集安全区 I 的 DCS、水煤灰系统、烟气脱硫系统、TDM、FECS 等系统的信息。

2.2.2 管理信息大区

目前仅考虑安全区 III。该区中的业务系统或功能模式的典型特征为：实现电力生产的管理功能，但不具备控制功能，不在线运行，该区包括管理信息系统（MIS）、办公自动化系统（OA）客户服务、辅助报价决策系统等。该区的外部通信边界为发电企业的广域网络及因特网。

电厂的 SIS 镜像服务器、WEB 服务器也位于安全区 III，实现对 II 区 SIS 系统数据库的同步。辅助报价决策系统需读取 II 区电能计量系统及发电报价终端系统的数据。

2.3 二次系统安全防护方案

电厂二次系统横向安全防护方案如图 3 所示。

电厂二次系统纵向安全防护方案如图 4 所示。

电厂二次系统安全防护采用链式结构。在安全区 II 与管理信息大区之间部署专用隔离装置，安全区 I 与管理安全区之间禁止直接的信息访问，安全区 I 和安全区 II 之间采用防火墙等隔离设备实现互连。

2.3.1 横向安全防护方案

(1) 厂内安全 I 区的 NCS、DCS、TDM、水煤灰系统、烟气脱硫系统、FECS 均需接入位于安全 II 区的 SIS 系统，根据 SIS 系统已有结构，并考虑对现有 SIS 系统进行尽可能少的改造工作，在各系统与接口机之间布置分散的防火墙。各业务系统通过防火墙接入 SIS 交换机后，实现信息的互联。

(2) 厂内线路保护装置、断路器保护装置、母线保护装置、发变组保护装置、起备变保护装置等位于安全 I 区。上述保护装置需接入位于安全 II 区的保护及故障录波信息子站。目前上述保护装置中线路保护装置、断路器保护装置、母线保护装置采用以太网口方式接入以太网交换机，发变组保护装置、起备变保护装置经 RS485/以太网转换装置后也采用以太网方式接入交换机。在以太网交换机与 II 区之间装设防火墙，实现保护信息的安全接入。

(3) 厂内的电力市场报价终端部署在安全区 II，与运行在管理信息大区的报价辅助决策系统的信息交换需通过专用的横向隔离装置。

(4) 厂内 MIS 系统、生产管理系统均部署在管理信息大区，对厂内 SIS 系统及其它位于生产控制大区的系统的信息访问需通过专用的安全隔离装置。

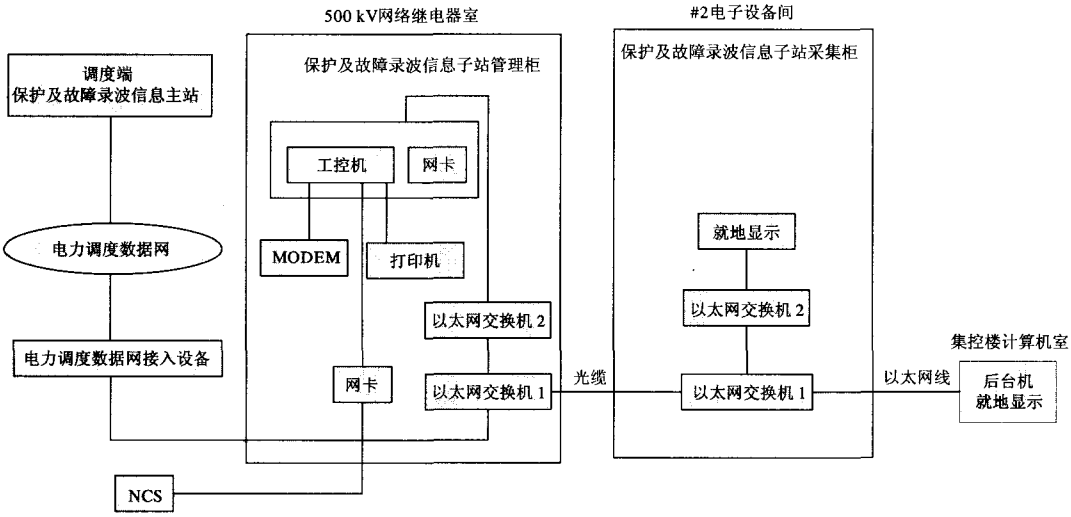

图 5 某电厂保护及故障录波信息子站联系图

Fig.5 Connection diagram of the relay protection and fault information system of a power plant

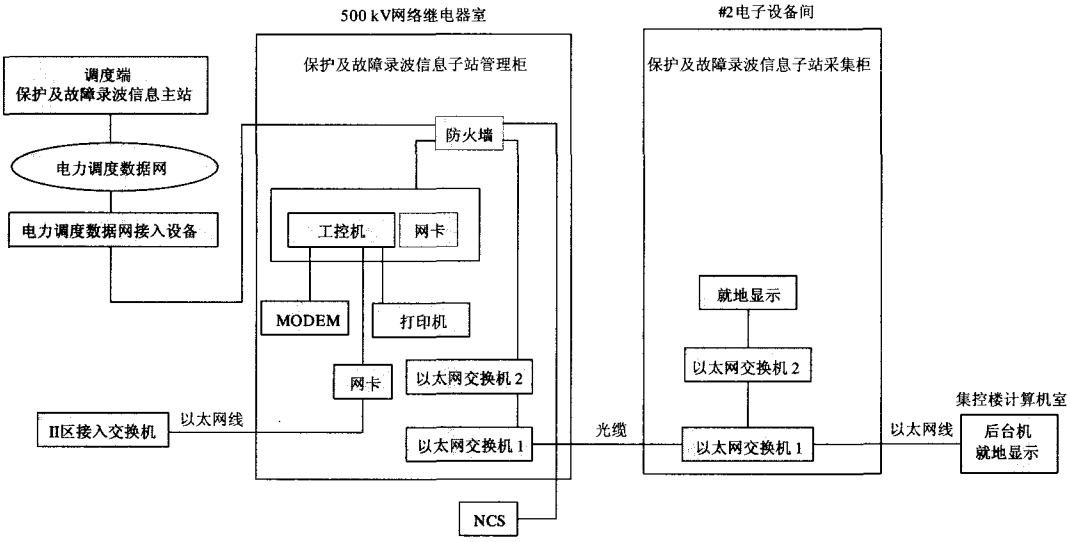

图 6 改造后某电厂保护及故障录波信息子站联系图

Fig.6 Connection diagram of the relay protection and fault information system of a power plant after reformation

2.3.2 纵向安全防护方案

RTU、PMU 等实时信息系统属于安全区 I 内的系统，接入电力调度数据网接入设备 VPN1；保护及故障录波信息子站、电能量计量系统等系统属于安全区 II 内的系统，接入电力调度数据网接入设备 VPN2，在纵向上均需加装 IP 认证加密装置（本期工程预留费用，与华中公司同步建设）。

2.3.3 其它防护

(1) 在安全区 II、III 区统一部署一套 IDS(入侵检测)管理系统。IDS 探头主要部署在安全区 II、III 的边界点。

(2) 在 II、III 区各部署一套网络防病毒系统，具体的防病毒服务器升级中心可设置在 II 区、III 区的通信网关机上，并且必须以手工方式下载病毒库经严格检验后以光盘或其它移动设备方式更新，禁止跨区连接更新，II 区内所有机器分别连接到相应的防病毒服务器进行病毒库的更新；安全 III 区的防病毒服务器可直接连接到 Internet 上更新病毒库，

III区内所有网关机和主站等直接连接到防病毒服务器自动更新病毒库。

(3) 在 II 区配置工控机，并在该工控机上安装专用的物理隔离装置监控程序，实时收集监控物理隔离装置的状态信息，同时将物理隔离装置的工作信息通过调度数据专网实时传送到华中网调的安全集控中心，以便实时掌握物理隔离装置的工作状态和网络流量情况。

(4) II 区和 III 区分别配置通信网关机，在这些通信网关机上安装专用的跨物理隔离传输软件，用于构建 II 区和 III/IV 区之间的文件和数据单向传输通道。

(5) 建立完善的安全管理组织机构。

3　相关系统改造及设备布置

3.1 SIS 系统改造

原 SIS 系统中仅机组 DCS(#1 机组 DCS、#2 机组 DCS、公用 DCS)与接口机之间布置了防火墙，本次安全系统改造需在水煤灰辅助系统监控网络、NCS、FECS、TDM 与接口机之间各增加 1 套防火墙。新增防火墙安装于 SIS 接口机柜上。

SIS 与 MIS 之间原已布置了正向物理隔离装置（与 SIS 系统配套购置），光电转换装置分别布置于相应系统的屏上，光缆也已敷设，本次改造，为增强安全性，新增 1 套正向物理隔离装置。

3.2 保护及故障录波信息子站系统改造

原保护及故障录波信息子站各套保护装置通过以太网交换机与子站相连，NCS 与子站直接相连以及以太网交换机直接接入电力调度数据网接入设备，从而造成 I、II 区的直接跨区互联。本次改造，在子站与以太网交换机之间新增 1 套防火墙，布置于保护及故障录波信息子站管理屏上。原子站与 NCS 之间的连接改至 NCS 经防火墙与子站相接。原子站经以太网交换机直接接入电力调度数据网接入设备，改造后经防火墙再接入电力调度数据网接入设备。

新增防火墙电源取至屏顶 UPS。

改造前保护及故障录波信息子站系统联系图如图 5 所示。改造后保护及故障录波信息子站系统联系图如 6 所示。

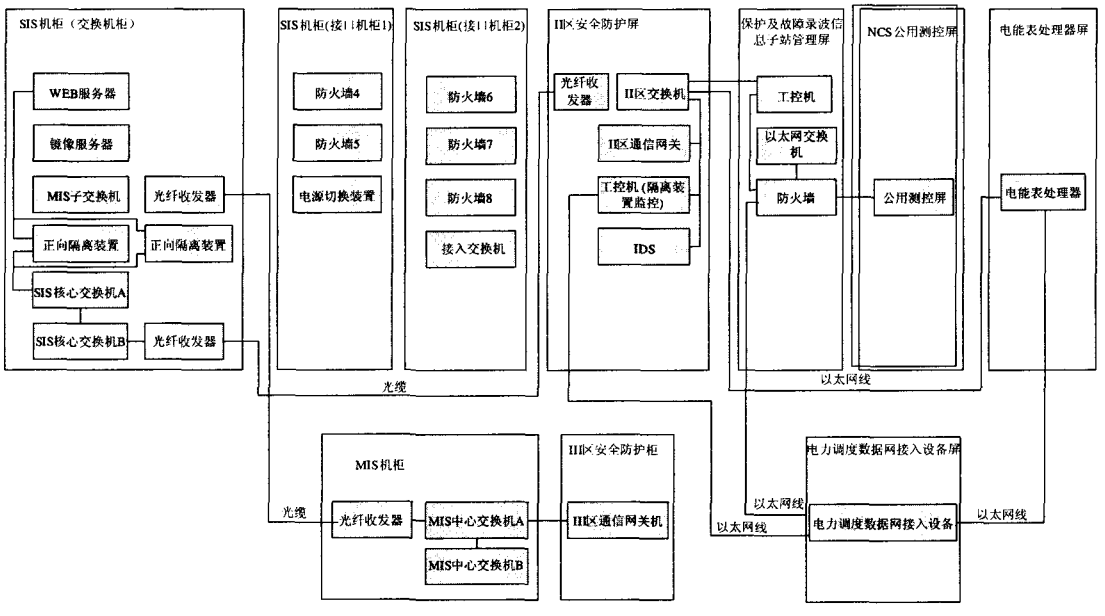

图 7 某电厂二次系统安全防护系统设备联系图

Fig.7 Connection diagram of the secondary system security protection devices of a power plant

3.3 新增屏柜

在 500 kV 网络继电器室新增 1 面 II 区安全防护屏，装设 II 区交换机、II 区通信网关、隔离装置监控工控机、IDS 、电源切换装置及光电转换装置和光纤接口盒。从屏顶小母线各引 1 路 UPS 电源及 1 路 220 V 交流电源至切换装置，经切换后供各设备使用。

在 SIS 交换机柜上新增 1 套光电转换装置及 1 套正向隔离装置，在 SIS 接口机柜 1 上新增 2 套防火墙设备、1 套电源切换装置；在 SIS 接口机柜 2 上新增 3 套防火墙设备。从#1 电子设备间 UPS 公用屏引 1 路 UPS 电源，另从屏顶引 1 路 220 kV 电

源至电源切换装置，切换后的电源供新增防火墙设备及光电转换装置使用。光纤接口盒则利用屏上已有光纤接接口盒。

在化水车间三层新增 1 面 III 区安全防护屏。屏上装设III区通信网关机及IDS。电源取自MIS 机房 UPS 电源。

电厂二次系统安全防护系统设备联系图如图 7 所示。

4 结语

电厂按照“安全分区、网络专用、横向隔离、纵向认证”的原则，对二次系统进行了安全分区，采用链式防护结构，在相关部位布置了防火墙、安全装置、安全文件传输系统、通信网关机等防护设备。目前，该系统已投入运行，有效地提高了电厂二次系统数据通信和监控过程的安全性，与即将实施的纵向安全防护体系一起，构成电厂较为完善的安全防护体系。

参考文献

[1] 电力二次系统安全防护规定(电监会5 号令)[S]. 2004.

[2] 电力二次系统安全防护总体方案(电监安全[2006]. 34 号)[S]. 2006.

收稿日期：2008-06-10；　修回日期：2008-08-11

作者简介：

曾　玉（1973-），女，硕士，高级工程师，主要从事电力系统二次设计工作；E-mail: zengyu@csepdi.com

马进霞（1957-），女，教授级高工，主要从事电力系统二次项目管理工作；

张立平（1973-），男，高级工程师，主要从事电力系统二次设计工作。

（上接第 41 页　continued from page 41）

参考文献

[1] 张学松，柳焯，于尔铿，等. 配电网潮流算法比较算法[J]. 电网技术,1998,22(4):45-49.
ZHANG Xue-song,LIU Zhuo, YU Er-keng，et al.A Comparison Power Flow Calculation Methods for Distribution Network[J]. Power System Technology, 1998,22(4):45-49.

[2] Ghosh S,Das D.Method for Load-flow Solution of Radial Distribution Networks[J]. IEE Proceedings Gener，Trans, and Distrib,1999,146(6).

[3] 于继来,王江,柳焯.电力系统潮流算法的几点改进[J].中国电机工程学报,2001,21(9)：88-93.
YU Ji-lai,WANG Jiang,LIU Zhuo. Improvements on Usual Load Flow Algorithms of Power System[J]. Proceedings of the CSEE，2001,21(9)：88-93.

[4] 谢开贵,周家启.树状网络潮流计算的新算法[J].中国电机工程学报,2001,21(9)：116-120.
XIE Kai-gui,ZHOU Jia-qi.A New Load Flow Algorithm for Radial Distribution Networks[J]. Proceedings of the CSEE, 2001,21(9)：116-120.

[5] 曹亮,孔峰,陈昆薇.一种配电网的实用潮流算法[J].电网技术, 2002,26(11):58-60.
CAO Liang,KONG Feng,CHEN Kun-wei.A Practical Algorithm of Load Flow Calculation for Distribution Networks[J].Power System Technology, 2002,26(11):58-60.

[6] 颜伟，刘芳.辐射型网络潮流分层前推回代算法[J].中国电机工程学报，2003，23（8）:76-80.
YAN Wei,LIU Fang.Layer-by-layer Back/forward Sweep Method for Radial Distribution Load Flow[J]. Proceedings of the CSEE, 2003，23（8）:76-80.

[7] Dattatri K. C++面象对象高效编程[M]. 北京：人民邮电出版社,2000.
Dattatri K. C++ Effective Object-Oriented Software Construction[M]. Beijing:People's Posts & Telecom Press,2000.

收稿日期：2008-09-02；　修回日期：2008-09-21

作者简介：

董张卓(1962-)，男，博士，高级工程师，主要从事电力自动化方面科研教学工作；E-mail:dongzzxa@qq. com

刘　雪（1983-），女，硕士研究生，从事电力系统分析研究工作。