

电力自动化控制系统网络信息安全管理的研究与设计

针对目前电力系统对安全防护要求的逐步提升,对电力自动化控制系统网络信息安全管理进行了研究设计。结合某发电厂提出了安全防护策略,同时对其安全防护进行了设计,重点对网络、中调汇聚接入、控制区与非控制区的横向隔离、调度数据网与管理信息网隔离以及调度数据网边界入侵检测等进行了设计,为发电厂电力自动控制系统安全防护的设计实现奠定了基础。

李玉琛 杨 虎/国网宁夏电力公司中卫供电公司



李玉琛/工程师

关键词/Keywords

电力系统·
网络信息·
安全防护·

0 引言

网络技术随着信息技术的快速发展而逐步运用至各种电力控制系统内,这在很大程度上提升了电力系统的整体效率,此外电力系统的信息交换量也随之扩大,其对数据交换的安全性的要求也

随之升高。然而一些电力自动控制系统在构建时通常遗漏其数据网络的安全问题,如果无法提供安全防护保障就和本地的数据网络互连,这在很大程度上存留有很大的安全隐患^[1-2],所以亟待解决电力自动化控制系统网络信息的安全管理问题,因此本文对其进行了研究设计。

1 安全防护策略

1.1 安全防护风险分析

电力自动控制系统网络信息面临的主要安全风险如表1所示。

1.2 总体策略设计

总体策略设计图如图1所示。

表1 安全防护风险

风险	说明
旁路控制	破坏者对变电站及发电厂等输送非法操作指令,导致电力系统出现障碍严重的致使崩溃
完整性破坏	强行违规篡改电力控制中重要程序及配置
工作人员的随意行为	透露重要系统密码及信息,任意装置仪器或系统ACL
拦截/篡改	违规截获并篡改传输网中的设定参数及控制命令等数据
非法运用	不遵法运用网络系统计算机资源
信息泄露	证书及密码等重要资料泄露
欺骗	IP及Web欺骗等
伪装	黑客经过伪装利用合法身份入侵相关系统
分布式拒绝	服务攻击黑客经过调度网向相关系统输送很多垃圾数据致使拒绝服务,严重的导致系统崩溃
窃听	黑客在数据网上非法窃听明文传输数据

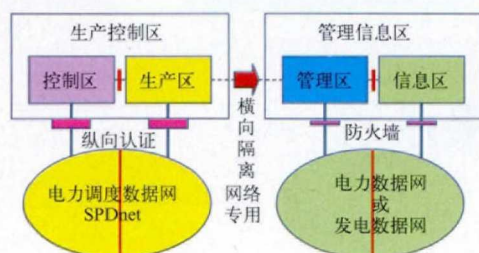


图1 总体策略

具体措施说明如表2所示。

2 电力自动化控制系统安全防护的设计

2.1 设计目标

电力自动化控制系统安全防护的关

表2 具体措施与说明

措施	说明
分区防护	针对干扰电力自动控制系统的强弱程度完成区域划分，防护电力生产及电力生产控制系统
总体安全防护	其包含全部满足方案要求的系统，一并置入安全区，以最大程度地完成对其的有效防护
横向隔离	运用隔离装置于不同安全区完成逻辑或物理横向隔离
网络隔离	运用技术完成多个相互逻辑隔离，完成电力调度数据网和电力数据通信网的多层次防护
纵向防护	运用认证加密及硬件防火墙等形式完成安全区的纵向安全防护

键就是分层分区完成防护，实行“安全分区、网络专用、横向隔离及纵向认证”安全策略^[3-4]，确保电力业务系统及调度数据网的安全运转。

某发电厂业务系统能够分成生产控制及管理信息两个大区，其中生产控制大区包含控制区（安全区I）和非控制区（安全区II），依照其系统的实时性、运用人员、关键功用、配置现场、调

度数据网通信形式以及对电力自动控制系统的干扰程度等因素，分别被置于与之对应的安全区^[5-6]。于生产控制和管理信息大区之间完成逻辑链路隔离，其设计目标如表3所示。

2.2 设计方案

某发电厂网络拓扑图如图2所示。

表3 设计目标

序号	设计目标
a	调度数据网并行接入省骨干调度数据网
b	防止黑客及病毒等恶意代码攻击电力自动控制系统，从而致使电力系统故障
c	确保电力监控系统及调度数据网络的连续及可用性
d	完成电力调度关键信息在网络传输历程中的完好性
e	完成应用系统及设备连接电力自动控制系统的身份认证，从而在很大程度上避免非法连接及非授权访问

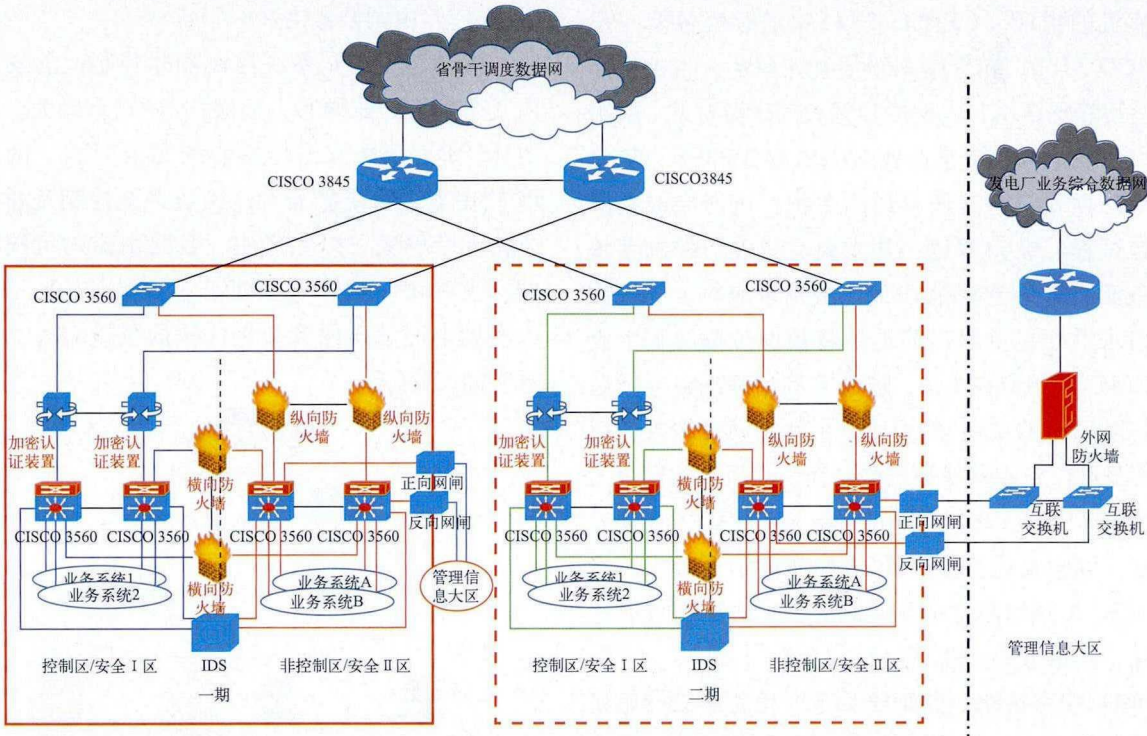


图2 某发电厂网络拓扑图

(1) 网络设计

1) 外网接入。发电厂调度数据网接入部分属于省调度数据网的接入层，一、二期调度数据网分别经过两台接入交换机CISCO 3560 (CE) 上连接核心路由器CISCO 3845 (PE)。其关键是兼顾冗余性，运用网络设备技术，在很大程度上确保发电厂数据网的链路容灾能力。

2) 内网访问与控制。设计内部网络的访问时要兼顾纵向及横向两方面，其设计如表4所示。

表4 内网访问与控制设计及说明

设计	说明
纵向访问	依照网络所属的区域装备加密认证及防火墙，全部纵向互联设计装备双系统及双链路冗余 运用HSRP于内部接入及汇聚的层次上完成热切换 上下级调度网络的互访，实时及非实时业务分别经过加密认证及防火墙完成控制保护
横向访问	于I、II区业务之间运用防火墙、VLIN、VPN及ACL等形式完成逻辑隔离 利用NAT形式完成 区向区主动的数据请求

3) 路由设计。去包：其主要完成地/省中调发出数据请求至电力控制系统设备，于PE路由器CISCO 3845中将目的地址指向两台控制区业务交换机的虚IP，CISCO 3845输送数据包至二层CISCO 3560，随之输送至主加密网关。主加密网关运用静态路由将内网的数据目的IP指向下一跳出接口。数据包输送至主业务CISCO 3560后，随之查找路由表以将其送至目的主机，进而完成全部去包过程。纵向回包：其主要完成电力控制系统设备反馈信息至地/省中调完成请求响应，主机接收请求后回包依照目的地址将数据包输送至主业务CISCO 3560的虚IP，随之其利用静态路由指向下一跳CISCO 3845的虚IP。主加密网关接收包后依照目的IP完成查找静态路由表，然后将其送至二层的CE交换机CISCO 3560，随之完成MAC地址表查找，同时发送至主PE路由器CISCO 3845上，然后CISCO 3845再完成路由表查找，进而完成回包过程。其示意图如图3所示。

4) 安全策略。其策略如下；①总体设计兼顾全部网络横向、纵向安全控制及业务区应用层的入侵检测，运用VLIN完成相异业务的隔离；②纵

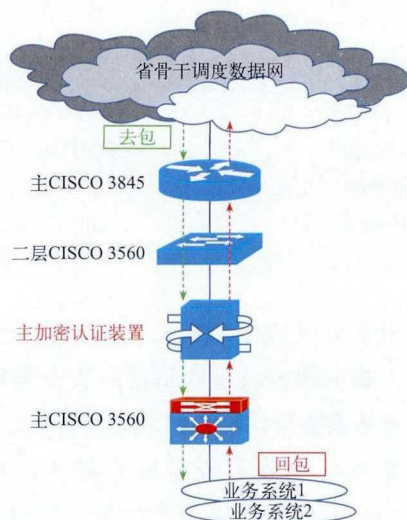


图3 路由示意图

向安全网关完成对进入实时区的控制，对应的服务应用端口在横向依照请求于I、II区装备相异级别的安全控制仪器，运用横向防火墙完成I、II区的逻辑隔离，同时运用NAT连接两个相异区域，并在内/外网口对源目标IP完成ACL控制；③控制及非控制区业务交换机和CE交换机间分别运用加密网关及防火墙，兼顾上级网络的配置外网接入运用MPLS VPN形式。

(2) 中调汇聚接入

该设计关键是解决控制和非控制区的安全接入冗余问题。兼顾其上连接HSRP冗余网关，故运用HSRP冗余协议当作核心的冗余形式，同时于PE路由器上设定静态的路由条目至控制及非控制区的冗余网关，以完成主、备路由器均可接收数据。运用MPLS VPN完成纵向数据的传输，这在很大程度上能够确保其数据传输的逻辑隔离，其示意图如图4所示。

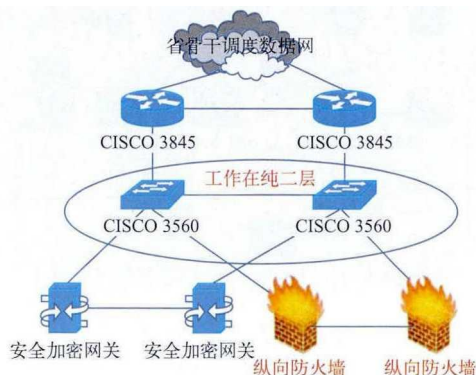


图4 中调汇聚接入示意图

中调汇聚接入及说明如表5所示。

表5 中调汇聚接入设计及说明

序号	说明
1	PE路由器CISCO 3845上层分别汇聚接入省调度网，下层分别接入两台工作在二层的CE交换机CISCO 3560
2	在两台PE路由器的内网接口上运用HSRP，上连接省调运用动态路由协议OSPF，下连接装置网关指向设定好的虚拟IP
3	于PE路由器上设定路由，当访问目的地址是实时及非实时区地址时，路由下一跳分别是控制及非控制区业务交换机的虚地址及纵向网关地址
4	CE交换机工作在二层，其作用是扩展PE路由器端口

(3) 控制区与非控制区的横向隔离

横向隔离务必要符合逻辑的数据隔离，与此同时能够避免低安全级数访问高安全级数区域的情况发生。运用防火墙NAT的形式阻滞非控制区给控制区发出的主动连接，其示意图如图5所示。

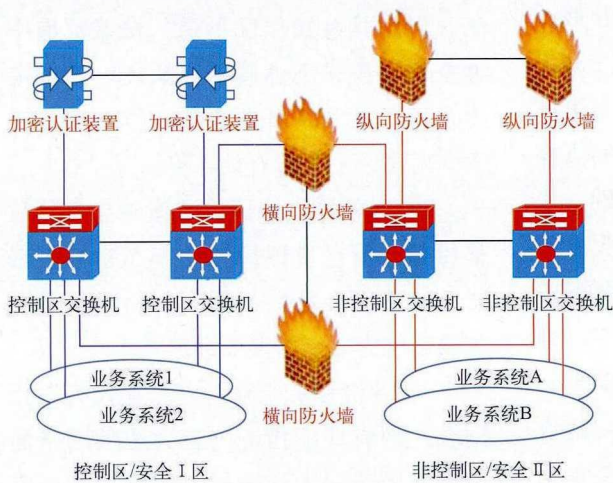


图5 控制区与非控制区横向隔离示意图

在安全区I、II间装备两台Eudemon 100E纵向互联硬件防火墙，以完成控制区访问非控制区的网络数据通信，同时运用NAT及ACL等完成：①两区的逻辑隔离，提升实时区的安全防护等级；②控制区相关业务系统能够同时运用实时及非实时VPN和中调完成数据传输，从而完成无缝连接。

(4) 调度数据网与管理信息网隔离

分别装备一台正向及反向隔离装置于非控制

区与管理信息大区之间，其中正向表示安全等级高到低的数据流方向，即非控制区至管理信息大区；反向则相反，反向传输务必要是单比特的纯文本或语言数据。

(5) 调度数据网边界入侵检测

装备一台四探针百兆入侵检测装置于调度数据网，其中每两个探针分别设定于安全I区及II区的两台纵向互联交换机，对其各自连接口完成端口镜像以连入IDS的扫描端口。因为IDS是被动式的，没有跳板性能，所以其没有恶意用户运用IDS为跳板访问控制及非控制区的出现。

3 结束语

以某发电厂的实际情况为研究背景，同时根据电力控制系统安全防护等各方面规定，对电力自动控制系统安全防护方案进行了研究设计，明确了设计目标，同时详细阐述了安全防护设计方案，这为以后其他发电厂电力自动控制系统安全防护的设计实现奠定了基础，同时为后续的进一步研究提供了科学理论。

参考文献

[1] 张敏, 张五一, 韩桂芬. 工业控制系统信息安全防护体系研究 [J]. 工业控制计算机, 2013 (10): 25-27.

[2] 卢山. 浅谈电力二次系统的安全防护 [J]. 企业技术开发, 2013 (18): 101-102.

[3] 岳宏亮, 陈鹏良, 楼书氢. 地区电网控制中心二次系统安全防护策略分析 [J]. 中国电力教育, 2014 (33): 180-181, 186.

[4] 王斯梁, 尹一桦. 工业控制系统安全防护技术研究 [J]. 通信技术, 2014 (2): 205-209.

[5] 邹春明, 郑志千, 刘智勇, 等. 电力二次安全防护技术在工业控制系统中的应用 [J]. 电网技术, 2013, 37 (11): 3227-3232.

[6] 牟善科, 秦莹. 省级电力调度中心二次系统安全防护设计方案 [J]. 电工技术, 2011 (4): 17-19.

(收稿日期: 2016-12-15) EA