广西崇左蜜朋生物能源有限公司电力监控系统网络安全防护项目招标公告

（招标编号：CZBE201902）

项目所在地区：广西壮族自治区,崇左市,市辖区

一、招标条件

本电力监控系统网络安全防护项目已由项目审批/核准/备案机关批准，项目资金来源为其他资金*，招标人为广西崇左蜜朋生物能源有限公司。本项目已具备招标条件，现招标方式为公开招标。

二、项目概况和招标范围

规模：广西崇左蜜朋生物能源有限公司电力监控系统网络安全防护项目，数量：1项(详细技术要求见附件《广西崇左蜜朋生物能源有限公司电力监控系统网络安全防护项目技术规范》及《电力监控系统网络安全防护项目设备清单(广西崇左蜜朋生物能源有限公司)》)。

范围：本招标项目划分为1个标段，本次招标为其中的：

(001)电力监控系统网络安全防护项目;

三、投标人资格要求

(001 电力监控系统网络安全防护项目)的投标人资格能力要求：（一） 基本资格要求：

1、投标人须为国内依法注册的企业法人或者其他组织;

2、投标人在所提供的同类服务中未因该服务原因出现过重大及以上的质量问题或安全事故（以中华人民共和国工业和信息化部等有关主管部门网站公开通报为准）;

3、没有处于被责令停业，财产被接管、冻结及破产状态;

4、投标单位不能是正在接受国家有关部门审查、被吊销营业执照、被注销、资质证书过期、被其他企业兼并（或收购）或目前因重大经济纠纷涉讼的法人。

（二）专项资格要求：

提供自2015年以来具有成功实施并已投入使用的、且在大型企业案例业绩不少于3个（以提供客户属于大型集团企业的基本信息，以合同关键页、验收报告、材质报告、产地证明、材料检验单及合格证、需求报告或解决方案关键页为准）；案例资料与技术标书一并提交。;

本项目*不允许*联合体投标。

四、招标文件的获取

获取时间：从 2019 年 07 月 17 日 10 时 00 分到 2019 年 07 月 26 日 11 时 00 分

获取方式：东亚糖业网站下载 http://www.easugar.com/tender

五、投标文件的递交

递交截止时间：2019 年 07 月 26 日 12 时 00 分

递交方式：广西南宁市民族大道 136-5 号华润大厦 C 座 23 楼采购部纸质文件递交

六、开标时间及地点

开标时间：2019 年 07 月 26 日 15 时 00 分

开标地点：广西南宁市民族大道 136-5 号华润大厦 C 座 23 楼或 24 楼

七、其他

（一）广西崇左蜜朋生物能源有限公司招标，详细招标文件等信息请到东亚糖业官网获取 http://www.easugar.com/tender

（二）投标保证金：

投标保证金 请于 2019 年 7 月 25 日下午 17 时前以转账方式支付投标保证金 2 万元人民币，投标方可生效。如不中标凭退款申请函盖章原件 30 个工作日内退回投标保证金；中标后投标保证金转为履约保证金，验收合格后全额返还，不计利息；如中标者弃标，则不退回投标保证金。

保证金汇入账户：（注：汇款时请注明该款项为电力监控系统网络安全防护项目投标保证金）

单位名称：广西崇左蜜朋生物能源有限公司

开户行：中国建设银行广西区分行营业部

账号：45050159415100000606

退保证金申请函格式：　　退保证金申请函

XX 公司参与 XX 公司的电力监控系统网络安全防护项目投标于 XX 年 XX 月 XX 日支付贰万元投标保证金，因未中标原因申请退回贰万元投标保证金到 XX 公司以下账户：

单位名称：***

开户行名称：***

账　　号：***

银企直联代码：***

落款公司名称（加盖公章）

日期：XX 年 XX 月 XX 日

（三）投标要求：

1、技术标书与商务标书纸质版分开密封投标（技术投标书需应我司招标要求，如跟招标要求有偏离，请填写偏离表）。同时技术标书请发电子邮箱：yaoxiangyang@easugar.com

2、商务标书必须写明清楚竞标含税价格、税率、交货时间、质保期、付款方式(招标方要求的付款方式：验收合格付 90%，质保金 10%质保期满 1 年支付。)等商务条款，以及招标项目的详细价格清单。标书用信封装好并密封，信封头尾盖章并寄或送至以下地址：

广西南宁市民族大道 136-5 号华润大厦 C 座 23 楼采购部

收件人：姚向阳 ，联系电话：0771-5537112；13768809191

3、投标方参与投标过程中所产生的费用（含差旅、机票等）由投标方自行承担。

八、监督部门

本招标项目的监督部门为广西崇左蜜朋生物能源有限公司内审部。

九、联系方式

招 标 人：广西崇左蜜朋生物能源有限公司

地　　址：广西崇左市工业大道 35 号

联 系 人：姚向阳

电　　话：0771-5537112

电子邮件：yaoxiangyang@easugar.com

招标代理机构：

地　　址：

联 系 人：

电　　话：

电子邮件：

招标人或其招标代理机构主要负责人（项目负责人）：_____（签名）

招标人或其招标代理机构：_____（盖章）

电力监控系统网络安全防护项目
技术规范

广西崇左蜜朋生物能源有限公司

2019 年 6 月 26 日

目录

一、电力二次系统安全防护总体方案

1、总则

电力二次系统安全防护主要针对网络系统和基于网络的生产控制系统。安全防护的总体目标是保护电力监控系统及调度数据网络的安全，抵御黑客、病毒、恶意代码等的破坏和攻击， 防止电力二次系统的崩溃或瘫痪， 以及由此造成的电力系统事故或大面积停电事故。安全防护的基本原则为“安全分区、网络专用、横向隔离、纵向认证” 。安全防护的核心能力是“保护、检测、响应、恢复” 。

电力二次系统安全防护是一项系统工程，其总体安全防护水平取决于系统中最薄弱点的安全水平。各有关单位安全防护工作应当执行电力二次系统安全防护规定，遵守安全防护基本原则， 维护全网统一的安全防护结构和一致的安全策略。

2、安全防护目标

南方电网电力二次系统安全防护的总体目标是： 建立健全南方电网电力二次系统安全防护体系，在统一的安全策略下保护重要系统免受黑客、病毒、恶意代码等的侵害， 特别是能够抵御来自外部有组织的团体、拥有丰富资源的威胁源发起的恶意攻击，能够减轻严重自然灾害造成的损害，并能在系统遭到损害后， 迅速恢复主要功能， 防止电力二次系统的安全事件引发或导致电力一次系统事故或大面积停电事故，保障南方电网安全稳定运行。

南方电网电力二次系统安全防护工作的具体目标是：

（1）防范病毒、木马等恶意代码的侵害；

（2）保护电力二次系统的可用性和连续性；

（3）保护重要信息在存储和传输过程中的机密性、完整性；

（4）实现关键业务接入电力二次系统网络的身份认证，防止非法接入和非授权访问；

（5）实现电力监控系统和调度数据网安全事件可发现、可跟踪、可审计；

（6）实现电力监控系统和调度数据网络的安全管理。

3、安全防护设计原则

南方电网各级调度控制中心、配电中心（含负荷控制中心） 、变电站、各级调度控制中心直调电厂、电力通信机构在进行本单位电力二次系统安全防护方案设计时应遵守以下原则：

（1）系统性原则（木桶原理） ；

（2）简单性和可靠性原则；

（3）实时性、连续性与安全性相统一的原则；

（4）需求、风险、代价相平衡的原则；

（5）实用性与先进性相结合的原则；

（6）全面防护、突出重点的原则；

（7）分层分区、强化边界的原则；

（8）整体规划、分步实施的原则；

（9）不断完善的原则；

（10）下级服从上级，局部服从整体的原则；

（11）技术与管理相结合的原则。

4、安全防护总体策略

南方电网电力二次系统安全防护总体策略是南方电网各级调度控制中心、配电中心（含负荷控制中心）、变电站、各级调度控制中心直调电厂、电力通信机构开展电力二次系统安全防护工作必须遵守的原则。南方电网二次系统安全防护总体策略如下：

1） 安全分区

根据电力二次系统业务的重要性及其对电力一次系统的影响程度进行分区，南方电网电力二次系统分为生产控制大区和管理信息大区， 其中生产控制大区分为控制区（又称安全区 I）和非控制区（又称安全区 II） ，生产控制大区是电力二次系统重点防护对象。

2） 网络专用

南方电网各级电力调度数据网应当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综合业务数据网及外部公共信息网的安全隔离。该网可采用 MPLS-VPN 技术或类似技术划分两个相互逻辑隔离的业务子网，即实时 VPN 和非实时 VPN。实时 VPN 用于控制区业务系统的远程数据通信，非实时 VPN 用于非控制区业务系统的远程数据通信。

3） 横向隔离

南方电网各级运行维护单位的生产控制大区与管理信息大区之间应设置电力专用横向安全隔离装置实现物理隔离。生产控制大区和管理信息大区内部的安全区之间应采用防火墙或带有访问控制功能的网络设备实现逻辑隔离。

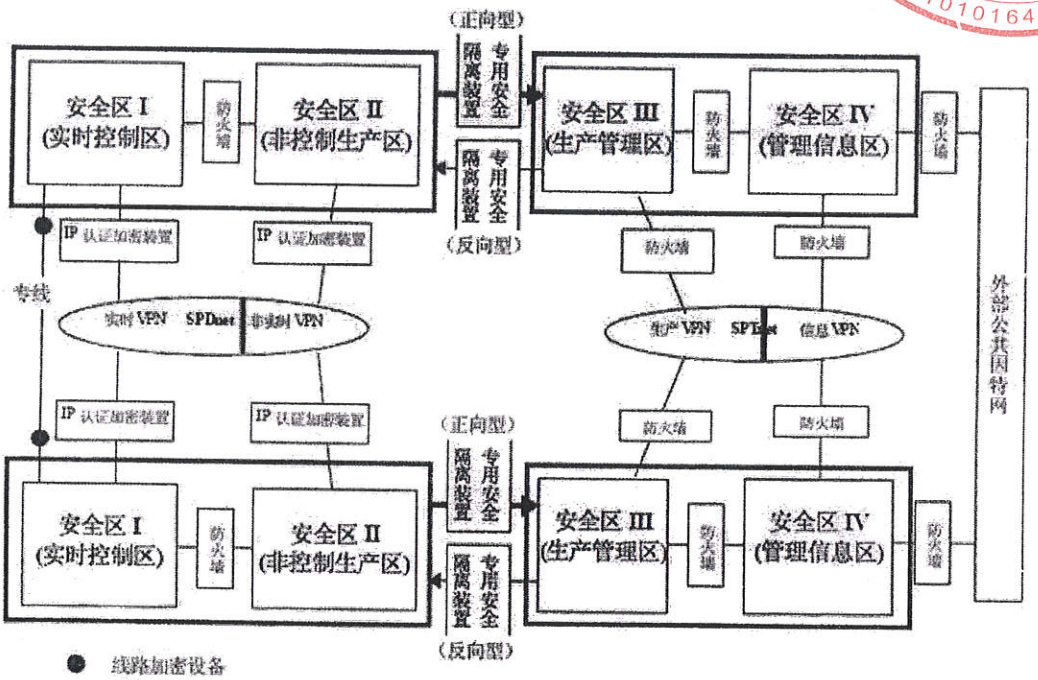
4） 纵向认证

南方电网各级运行维护单位在控制区与调度数据网的纵向连接处应部署电力专用纵向加密认证网关或加密认证装置， 非控制区与调度数据网的纵向连接处应部署电力专用纵向加密认证网关或防

火墙， 为上下级调度机构或主站与子站端的控制系统之间的调度数据网通信提供双向身份认证、数据加密和访问控制服务。

5、安全防护总体结构

1） 总体结构模型



该模型在技术上系统性地考虑了上下级各种数据业务的需求、网络的纵向互联、横向互联和数据通信的安全性问题，通过划分安全区、专用网络、专用隔离和加密认证等技术从多个层次构筑多道抵御网络黑客和恶意代码攻击的防线， 对电力实时监控系统等关键业务实施重点保护， 是构筑南方电网电力二次系统安全防护体系的基础。

生产控制大区的某些业务系统采用公用数据网络进行数据通信方式情况下，要求在主站端生产控制大区的通信出口采用物理隔离措施， 主站端和业务终端之间的数据通信采用加密认证措施。

2） 安全分区规则

南方电网各有关单位包括各级调度控制中心、配电中心（含负荷控制中心）、变电站、各级调度控制中心直调电厂内部基于网络的二次系统， 原则上划分为生产控制大区和管理信息大区。

a） 生产控制大区的划分

根据业务系统或其功能模块的实时性、使用者、主要功能、设备使用场所、各业务系统之间的相互关系、调度数据网通信方式以及对电力系统的影响程度等属性，生产控制大区原则上划分为控制区（安全区 I）和非控制区（安全区 II）。

➢ **控制区（安全区Ⅰ）**

控制区是电力二次系统各安全区中安全等级最高的分区，是必不可少的分区。该区中的业务系统与电力调度生产直接相关，有对一次系统的在线监视和闭环控制功能，且具有连续性、实时性（毫秒级或秒级）的特点以及高安全性、高可靠性和高可用性的要求。该区使用调度数据网络的实时 VPN 子网或专用通道与异地有关的控制区互联。

控制区的典型系统包括调度自动化系统（ SCADA/EMS ）、广域相量测量系统（WAMS）、自动电压控制系统（ AVC）、安稳控制系统、在线预决策系统、具有保护定值下发、远方投退功能的保信系统、配电自动化系统、变电站自动化系统、发电厂自动监控系统等，还包括使用专用通道的控制系统，如：安全自动控制系统、低频/低压自动减负荷系统、负荷管理系统等。

控制区业务系统的主要使用者为调度员、继电保护运行管理人员和运行操作人员。

➢ **非控制区（安全区Ⅱ）**

非控制区是电力二次系统各安全区中安全等级仅次于控制区的分区。该区的业务系统功能与电力生产直接相关，但不直接参与控制；系统在线运行， 与安全区Ⅰ的有关业务系统联系密切。非控制区的数据采集频度是分钟或小时级， 该区使用调度数据网络的非实时 VPN 子网或专用通道与异地有关的非控制区互联。

非控制区的典型系统包括调度员培训模拟系统、不带控制功能的继电保护和故障录波信息管理系统、水调自动化系统、电能量计量系统、电力市场运营系统、厂站端电能量采集装置、故障录波器和发电厂的报价终端等。

非控制区业务系统的主要使用者分别为调度员、水电调度员、继电保护人员及电力市场交易员等。

b） 管理信息大区的划分

根据业务系统或其功能模块的使用者、主要功能、设备使用场所、各业务系统之间的相互关系以及对电力系统的影响程度等属性， 管理信息大区原则上划分为生产管理区（安全区Ⅲ）和管理信息区（安全区Ⅳ）。

➢ **生产管理区（安全区Ⅲ）**

生产管理区是电力二次系统各安全区中安全等级次于非控制区的分区。该区中的业务系统与电力调度生产管理工作直接相关。该安全区使用企业综合业务数据网与异地有关的生产管理区互联。

生产管理区的典型系统包括电力调度运行管理系统（ OMS）、调度信息披露系统、雷电监测系统、生产控制大区系统（如 SCADA/EMS 、WAMS、电能量计量等）在管理信息大区的发布系统、调度

生产


GUANGXI CHONGZUO MIPENG BIO-ENERGY CO.,LTD
广西崇左蜜朋生物能源有限公司
4514021010164

管理用户终端等。

生产管理区业务系统的主要使用者为调度员和各专业运行管理人员。

➢ **管理信息区（安全区Ⅳ）**

管理信息区的业务系统主要用于生产管理和办公自动化。该安全区网络是本地办公环境下的局域网， 与个人桌面计算机直接相关。该安全区使用企业综合业务数据网与异地的管理信息区互联，并与 Internet 有互联关系。

管理信息区的典型业务系统包括管理信息系统（ MIS）、办公自动化系统（OA）、电网生产信息查询系统、统计报表系统、气象信息、客户服务系统、对外信息发布、Internet 业务等。

管理信息区业务系统的使用者为上下级管理部门和本单位内部工作人员。

3） 安全区互联结构

电力二次系统安全区域之间互联总体结构包括链式结构、三角结构和星形三种结构，其结构如图 2 所示：

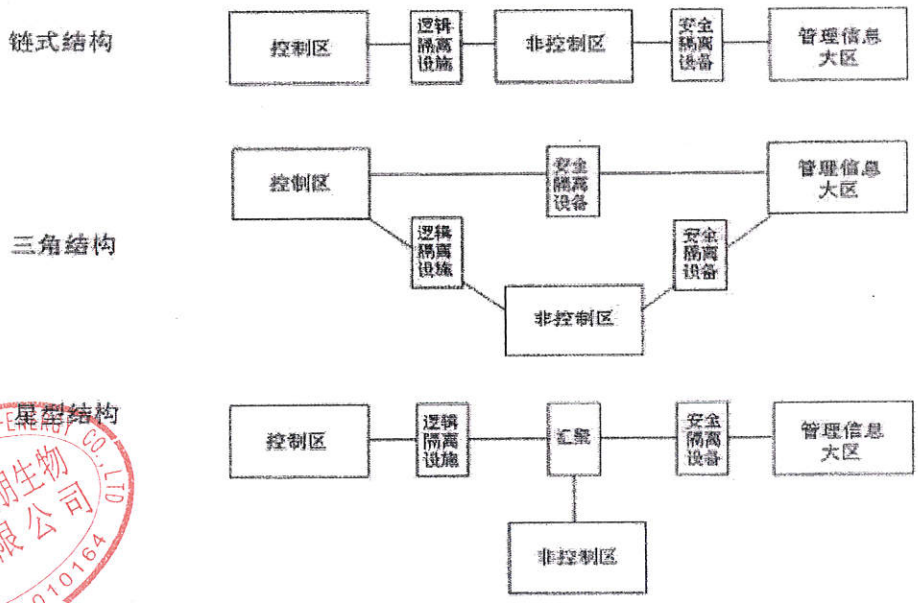


图 2 电力二次系统安全区互联总体结构

其中链式结构的控制区具有较高的累积安全防护强度，但总体层次较多， 三角结构具有较高的通信效率，但需要较多的安全隔离设施。可根据实际的系统现状和安全防护需求选择合适的互联结构。

6、安全防护技术措施

1） 安全区间横向网络边界安全防护

安全区间横向网络边界隔离是电力二次系统安全防护的关键技术措施之一。通过采用不同强度的安全防护设备对安全区之间实施横向隔离保护，特别是对生产控制大区和管理信息大区之间的网络边界应实施物理隔离，其数据通讯采用严格的数据单向传输控制，以有效抵御病毒、黑客等对生产控制大区业务系统及其网络的各种攻击和渗透。

控制区与非控制区之间应采用硬件防火墙、具有 ACL 访问控制功能的交换机或路由器等设施进行逻辑隔离。逻辑隔离设施应具备状态检测、数据过滤和地址转换等基本功能，可以对传输的地址、协议、端口和数据流的方向进行控制。控制区与非控制区之间的访问控制策略原则上只允许控制区系统主动与非控制区系统建立连接，不允许从非控制区反向访问控制区系统。确有必要进行反向访问时，仅允许系统间的业务数据传输，且必须对访问的地址、协议和端口实施严格的访问控制，禁止任何远程登录类的反向访问。

生产控制大区与管理信息大区的网络边界处应设置电力专用安全隔离装置进行单向物理隔离。电力专用安全隔离装置通过“安全岛”数据摆渡和割断穿透性 TCP 连接等技术，实现数据的单向传输和网络边界的物理隔离。该装置分为正向型和反向型，其中正向型安全隔离装置用于生产控制大区到管理信息大区的单向数据传输。反向型安全隔离装置用于从管理信息大区到生产控制大区单向纯文本数据传输。反向安全隔离装置接收管理信息大区发向生产控制大区的数据，进行签名验证、编码转换、数据报文检查等处理后，转发给生产控制大区内的相关业务系统。

生产管理区与管理信息区之间应采用硬件防火墙、具有 ACL 访问控制功能的交换机或路由器等设施进行逻辑隔离。逻辑隔离设施应具备状态检测、数据过滤和地址转换等基本功能，可以对传输的地址、协议、端口和数据流的方向进行控制。生产管理区与管理信息区之间的访问控制策略原则上只允许生产管理区系统主动与管理信息区系统建立连接，不允许从管理信息区反向访问生产管理区系统。确有必要进行反向访问时，必须对访问的地址、协议和端口实施严格的访问控制。

2） 安全区纵向网络边界安全防护

在生产控制大区与调度数据网的网络边界部署电力专用纵向加密认证网关（对于非控制区，目前可用国产硬件防火墙替代），是电力二次系统安全防护的一项关键技术措施。

纵向加密认证网关采用电力专用密码与认证技术，为各级运行维护单位控制区的纵向数据通信提供认证与加密服务，实现数据传输的机密性、完整性保护。纵向加密认证网关还提供协议报文的过滤和处理功能，可实现端到端的选择性保护。

在生产控制大区与公用数据网络的网络边界部署公网专用安全通信网关或公网专用安全通信装置，是电力二次系统安全防护的另一关键技术措施。

公网专用安全通信网关和公网专用安全通信装置采用专用密码与认证技术，为运行维护单位控制区和业务终端的纵向数据通信提供网络隔离、认证与加密服务，实现数据传输的机密性、完整性保护。

在生产控制大区纵向网络边界上，应避免使用默认路由，仅开放特定通信端口，禁止开通 ftp、telnet、rlogin 、rsh、rcp、http、pop3 等高风险网络服务。

3） 调度数据网安全防护

电力调度数据网是生产控制大区专用的广域数据网络，承载电网的实时监控、在线稳定控制预决策、继保信息管理、电量采集、在线生产交易等业务。电力调度数据网应在专用通道上， 采用独立网络设备组网， 在物理层面上实现与综合业务网和公共信息网的安全隔离。各级运行维护单位应当避免通过调度数据网形成不同安全区的纵向交叉连接。网、省、地三级电力调度数据网严格禁止与企业综合业务数据网、公用数据网络和公用通信网络直接互联。各级调度数据网之间的互联应遵循《中国南方电网调度数据网互联管理办法》，调度数据网不允许远程拨号维护。

调度数据网的安全防护应采取下列技术和安全措施：

- **虚拟专网技术**

电力调度数据网应采用 MPLS VPN 技术或类似技术将电力调度数据网分割为逻辑上相对独立的实时 VPN 和非实时 VPN，分别对应控制业务和非控制生产业务，并部署 Qos 策略或其他技术手段，保证实时 VPN 中关键业务的带宽和服务质量

- **路由和交换设备的安全配置**

核心路由和交换设备的安全配置包括对核心路由器的访问采用基于高强度口令密码的分级登陆验证功能、对路由器和交换设备的网络服务和端口进行严格限定、避免使用默认路由、关闭调度数据网网络边界的 OSPF 路由功能、关闭路由器的源路由功能、采用增强的 SNMPv2 及以上版本的网管协议、设置受信的网络地址范围、开启访问控制列表、记录设备日志、封闭空闲的网络端口等。

- **核心和关键节点网络节点的可靠性配置**

对调度数据网络中的核心和关键节点网络设备，必须采用双机冗余备份机制，保证调度网络系统的高可靠性。

- **调度数据网的安全监控**

在调度数据网互联边界和关键节点可通过流量监控、入侵检测等技术手段实现“监控流量、预防攻击、隔离危险”， 实时发现网络安全威胁， 及时处理修复，杜绝调度数据网因外界攻击而大

面


GUANGXI CHONGZUO MIPENG BIO-ENERGY CO.,LTD
广西崇左蜜朋生物
能源有限公司
4514021010164

积瘫痪。

4） 公用数据网络安全防护

生产控制大区的某些业务系统采用公用数据网络进行数据通信方式的情况下，要求在主站端生产控制大区的通信出口采用物理隔离措施，实现生产控制大区业务系统与公用数据网络之间的物理隔离； 主站端和业务终端之间的通信采用加密认证措施， 实现数据通信的身份认证和数据加密。隔离措施的原则为业务系统设备以及认证加密设备（或功能模块）应位于物理隔离设备（或功能模块）的内网侧。

在主站端部署公网专用安全通信网关， 在业务终端部署公网专用安全通信装置。公网专用安全通信网关实现网络隔离、加密认证等功能；公网专用安全通信装置实现加密认证等功能。公网专用安全通信网关应能与相应业务终端的公网专用安全通信装置进行身份认证并建立加密数据通信通道， 实现业务系统的数据通信。

生产控制大区涉公用数据网络的业务系统（如：配电网自动化系统、电力负荷管理系统等），其使用公用数据网络的系统设备、业务终端按该业务系统所属安全分区的要求进行管理。

公用数据网络传输通道应当启用基础电信运营商可提供的安全措施，包括：

（1）优先选用 TD-SCDMA 等具有自主知识产权的技术和产品；

（2）利用 APN+VPN 或 VPDN 技术实现无线虚拟专有通道；

（3）通过认证服务器对接入终端进行身份认证和地址分配；

（4）在主站系统和公共网络采用有线专线+GRE 等手段。

5） 安全区内部安全防护

安全区内部的安全防护包括生产控制大区和管理信息大区的内部防护。

- **生产控制大区内部防护措施**

（1）禁止生产控制大区内部的 E-MAIL 服务。

（2）禁止控制区内通用的 WEB 服务。

（3）禁止生产控制大区以任何方式连接因特网。

（4）生产控制大区必须具有恶意代码措施。病毒特征库、木马库以及 IDS 规则库的更新应离线进行。

（5）控制区和非控制区内的业务系统之间应采用 VLAN 和访问控制安全措施，避免系统间的直接互通。

（6）生产控制大区重要业务系统的远程数据通信应采用加密认证措施。

（7）生产控制大区重要的服务器和通信网应使用国家指定部门认证的安全加固操作系统，并采

用加密、认证和访问控制等安全防护措施。

(8)省级及以上调度控制中心应在在控制区边界、非控制区边界独立部署入侵检测系统(IDS),地市级调度控制中心、单机装机容量 300MW 或全厂装机容量 1000MW 及以上的发电厂应在控制区边界部署入侵检测系统(IDS),可在非控制区边界独立部署入侵检测系统(IDS),实现对各个业务系统与横向、纵向网络边界的入侵检测。

(9)省级及以上调度控制中心和大型地市级调度控制中心可在生产控制大区部署综合安全监控及审计平台, 对各种网络设备运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全防护设备运行日志和告警信息等进行集中收集、分析、审计和告警处理。

- **生产管理区内部防护措施**

(1)生产管理区应根据业务系统划分安全区或安全网段(例如:服务器群网段、用户群网段),并通过交换机的 ACL 功能或防火墙对关键业务系统实施安全防护;

(2)生产管理区与管理信息区的横向互联边界应部署防火墙;

(3)生产管理区应部署防病毒系统,并配置病毒库定期升级和定期扫描病毒等策略;

(4)省级及以上调度控制中心应在生产管理区边界部署入侵检测系统(IDS)。

6) 电力数字证书技术及应用

电力调度数字证书系统是南方电网电力二次系统安全防护的基础安全设施。电力调度数字证书系统是基于公钥技术的分布式的数字证书系统, 为电力监控系统及电力调度数据网上的关键应用、关键用户和关键设备提供数字证书服务, 实现高强度的身份认证、安全的数据传输以及行为审计。电力调度数字证书系统应按照南方电网电力调度管理体系进行配置, 省级及以上调度控制中心和有实际业务需要的地区调度控制中心应建立电力调度数字证书系统。

电力调度数字证书分为人员证书、程序证书、设备证书三类。人员证书指用户在访问系统、进行操作时对其身份进行认证所需要持有的证书; 程序证书指关键应用的模块、进程、服务器程序运行时需要持有的证书; 设备证书指网络设备、服务器主机等在接入本地网络系统与其它实体通信过程中需要持有的证书。

电力调度建设数字证书系统建设时,必须遵循如下原则:

(1)统一规划数字证书的信任体系。南网总调 CA 为一级 CA 系统;省级调度 CA 为二级 CA 系统;地、市级调度 CA 为三级 CA 系统。省调接受南网总调的证书管理, 负责所辖地调和直调厂站的证书管理; 地市级调度负责所辖县调及直调厂站的证书管理。上下级电力调度数字证书系统通过证书信任链构成认证体系。

(2)采用统一的数字证书格式和加密算法。数字证书格式遵循符合 X.509 V3 标准,证书格式

和加密算法应该严格按照电监会调度证书规范进行定义。

（3）电力调度数字证书的生成、发放、管理以及密钥的生成、管理应当脱离网络，独立运行。

7） 入侵检测措施

入侵检测是电力二次系统安全防护的重要技术措施。通过在生产控制大区和管理信息大区横向、纵向网络边界部署入侵检测系统， 可以实时监控关键业务系统和网络边界的关键路径信息，实现安全事件的可发现、可追踪、可审计。

入侵检测系统（ IDS）采用协议分析、模式匹配、异常检测等技术，通过将交换机上关键接入端口（例如各个安全区的纵向互联端口和横向互联端口）的数据报文镜像到 IDS 检测引擎（ IDS 探头）的接入端口，实现对网络流量、数据包的动态监视、记录和管理、对异常事件进行告警等。

8） 安全 WEB 服务

安全 II 区若有 WEB 服务，应采用支持 HTTPS 的安全 WEB 服务，其 WEB 服务器必须经过安全加固并采用电力调度数字证书对浏览器客户端访问进行身份认证及加密传输。

9） 防病毒措施

电力二次系统必须采用防病毒措施， 以及时发现网络和主机系统的安全漏洞和病毒入侵，消除电力监控系统的安全隐患。防病毒措施应遵循如下原则：

禁止生产控制大区与管理信息大区共用一套病毒代码管理服务器，对于生产控制大区的服务器和工作站应采用专用安全 U 盘等进行病毒代码的离线更新。

生产控制大区和管理信息大区防病毒策略的设定、病毒定义码的更新、病毒查杀记录的汇总以及事件报告等应纳入运行维护管理制度。

10） 综合审计平台

综合审计平台是二次系统安全防护的重要环节， 是保障二次系统安全运行的技术管理工具。省级及以上调度控制中心和大型地市级调度控制中心应在生产控制大区建立综合审计平台。综合审计平台应能全面收集、集中存储生产控制大区各种业务系统、网络设备、安全防护设备、机房设施等的运行日志、操作系统日志、数据库访问日志，并具备动态监视、故障分析、安全审计、事件预警及告警等功能。

综合审计平台由信息采集代理、事件管理和安全管理平台构成。信息采集代理支持网络、串口等通讯方式， 采用定制接口采集不同格式的日志信息和告警信息。事件管理主要用于存储各种日志信息、安全事件信息、操作系统信息、服务器信息等， 并对各种信息进行统一格式转换与存储。安全管理平台实现各种信息的告警管理，包括统计查询、报表、短信报警和系统管理等功能。

11） 远程拨号安全防护

电力二次系统应尽可能避免采用远程拨号方式维护系统，确有必要时，应采用电力专用安全拨号网关，实施网络层保护，并结合数字证书技术对远程用户进行客户端检查、登陆认证、访问控制和操作审计。

采用远程拨号方式维护系统时，必须采取下列管理控制措施：

（1）禁止生产控制大区与管理信息大区共用一套远程拨号设施。

（2）拨号设施平时应该关闭电源，开启拨号设施应履行审批手续。远程维护完毕后，应及时关闭拨号设施电源。

（3）对拨号登陆用户和密码应定期更换，对拨号人、拨号时间、事由、操作内容等必须详细记录。

（4）对远程拨号用户必须进行合理的权限限制，在经过认证的连接上应该仅能够行使受限的网络功能与应用。

（5）对远程拨号用户可使用定时限软证书和硬件证书进行身份认证。

12） 应用系统安全

对于应用系统本身的安全防护应满足下列要求：

（1）应用系统管理员账户、用户账户口令应定期进行变更；

（2）严格管理应用权限，制定权限赋予和权限变更的审核、批准、执行流程，依据最小化原则对用户赋予适当的权限，并定期进行权限复核；

（3）对应用系统应进行数据输入的合法性和参数配置的正确性检验；

（4）应用系统源代码应保存在专用开发系统中，不应与运行系统同机存放；

（5）定期对应用程序软件进行漏洞扫描，并修复所发现的漏洞；

（6）定期对应用系统以前发生的历史安全事件进行审计，分析总结安全事件的规律；

（7）对新上线的业务系统，应提供由专业安全机构出具的安全评估报告。

13） 操作系统安全

操作系统是承载业务应用、数据库应用的载体，是应用系统安全的基础。一旦操作系统的安全性出现问题，将对整体业务应用安全造成严重损害。操作系统应采取下列安全防护措施：

（1）系统应及时安装补丁，补丁安装前必须进行离线测试，确认对业务系统无影响后，方可进行安装；

（2）系统应进行安全加固，关闭非必须的服务，设置关键配置文件的访问权限，开启系统的日志审计功能；

（3）应制定用户管理策略、开户申请审批流程、定义用户口令管理策略，增强对关键账户文件

的保护，删除空口令账号；

（4）尽量限制管理员权限使用，一般操作中，尽量采用一般权限用户，仅在必要时切换至管理员账号进行操作；

（5）应当使用漏洞扫描工具定期对系统漏洞进行扫描，漏洞库应当及时更新，对于扫描出的漏洞应及时进行处理。

14） 支撑系统系统安全

数据库和各类中间件是各个业务系统的基础，数据完整性和合法存取会受到很多方面的安全威胁，包括密码策略、系统后门、数据库操作以及本身的安全方案。保证支撑系统安全的主要措施如下：

（1）及时更新经过测试的数据库最新安全补丁；

（2）对新安装的数据库，应及时修改所有账号的默认口令；

（3）及时删除无用和长久不用的账号；

（4）使用安全的口令策略，采用 8 位以上数字字符混合密码；

（5）使用安全账号策略，为不同的用户账号按需要授予相应的权限；

（6）加强数据库审核记录，并定期检查数据库审核记录；

（7）数据库中运行库和开发库应该进行分离。

15） 设备备用

地区级以上调度控制中心、500kV 变电站、集控站、各级调度控制中心直调电厂生产控制大区内部关键主机设备、网络设备或关键部件应采用冗余热备用方式，对管理信息大区内的设备可根据需要选用热备用、温备用或冷备用方式， 以保障系统的可用性。

16） 数据备份与恢复

数据备份是保证数据安全的关键技术措施。数据备份的内容包括操作系统、应用软件、业务系统数据、网络设备配置文件、安全防护设备配置文件等。数据备份应符合以下要求：

（1）规划设计新建系统时应考虑系统的备份需求，在系统投运前完成备份策略和恢复预案的制定并在系统投运后同时开始执行； 已投运系统备份需求发生变化时，要及时更新数据备份策略和恢复预案。

（2）备份系统的建设应统一纳入二次系统信息安全规划，备份系统及介质的选型要满足各系统的备份策略和数据备份及保存的要求， 包括安全可靠性、性能和服务质量、冗余等，省级及以上调度控制中心应建立集中备份系统， 确保通过数据备份能及时恢复各种故障情况下造成的数据丢失。

（3）应根据业务系统的需求制订备份策略，包括定期全备份与增量备份。电力二次系统关键数

据应定期作一次完全备份， 每当关键数据发生变化时， 应作一次增量备份。各有关单位在制订本单位的二次系统安全防护实施方案时， 必须制订备份系统具体的备份策略（包括全备份周期、增量备份周期、备份数据保留的时间等）。

（4）存储介质应存放在适于保存的安全环境（如防盗、防潮、防鼠害、磁性介质远离磁性、辐射性等），并有严格的存取控制,对备份了数据的存储介质要进行定期检查，确认所备份数据的完整性、正确性和有效性。

二、火电厂二次系统安全防护结构规范

1、火电厂二次系统安全防护总体逻辑结构

火电厂二次系统安全防护总体逻辑结构如图 16。该图示意了二次系统安全区域的划分、安全区域之间横向互联的逻辑结构、安全区纵向互联的逻辑结构以及网络安全防护设备的总体部署。图中虚线框和虚线部分表示不一定存在。

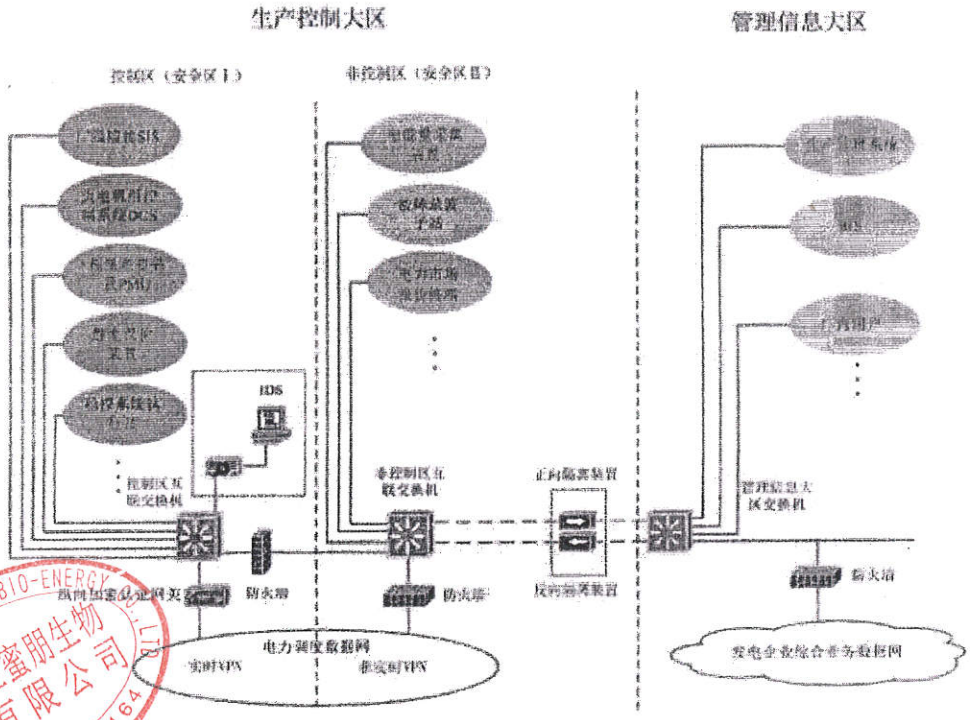


图 16　火电厂二次系统安全防护总体逻辑结构示意图

火电厂的二次系统分为生产控制大区和管理信息大区，其中生产控制大区分为控制区（安全区 I）和非控制区（安全区 II ），管理信息大区可根据需要划分安全区或安全网段。对于不属于省级及以上调度机构直调的小型火电厂，其生产控制大区可以不再细分，安全防护设备设施可相应进行简化。

控制区的主要业务系统包括厂级监控 SIS、火电机组控制系统 DCS、调速系统和自动发电控制功能、励磁系统和无功电压控制功能、网控系统、远动终端、AVC 子站、稳控系统执行站、相量测量装置 PMU、各种控制装置(电力系统稳定器 PSS、快关汽门装置)、五防系统、继电保护装置、具有设置功能的保信子站等。

非控制区的主要业务包括电能量采集装置、故障录波子站、无设置功能的保信子站、电力市场报价终端等。

管理信息大区的主要业务系统包括生产管理系统、MIS、OA 等。

该结构规范给出了生产控制大区中可能存在的业务系统及功能模块，未包括火电厂的所有业务系统， 各火电厂应结合实际情况并遵照二次系统安全防护规定实施具体配置。

各安全区内具有纵向、横向数据通信业务的业务系统汇集接入各自安全区的互联交换机；各安全区的互联交换机各自通过相应安全强度的安全防护设备横向连接不同的安全区域，纵向连接不同的广域网络。

火电厂二次系统安全区横向及纵向互联方案 1 实施细节

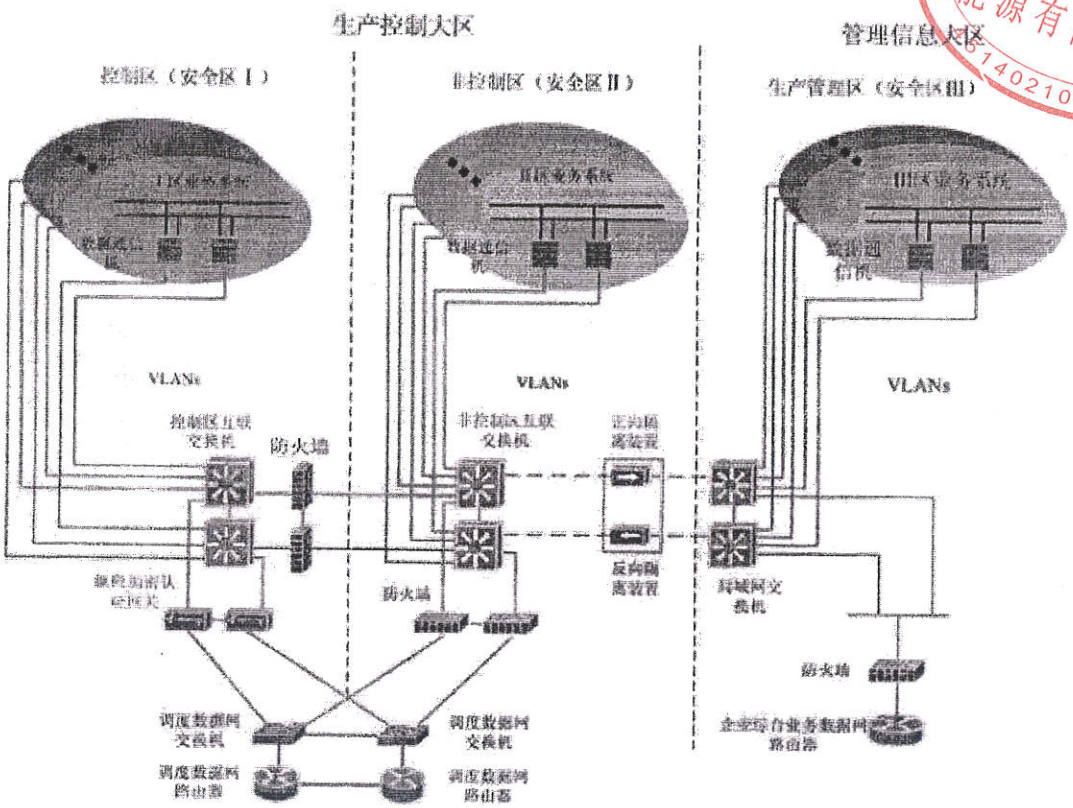


图 17　火电厂二次系统安全区横向及纵向互联方案　　1 拓扑结构图

横向和纵向互联的主要设备包括各业务系统的数据通信机、互联交换机、横向互联硬件防火墙、正、反向隔离装置、控制区纵向加密认证网关、非控制区纵向加密认证网关（硬件防火墙） 以及调度数据网网络设备。这些设备均可采取冗余备用结构。对正、反向隔离装置，可根据具体业务需求，适当增加配置数量。

数据通信机用于业务系统之间的横向及纵向数据通信。

互联交换机用于有纵、横向数据通信的业务系统的汇集接入、接入系统之间的访问控制和安全

区的横向及纵向互联。

横向互联硬件防火墙部署在控制区与非控制区的网络边界上，用于控制区与非控制区网络的逻辑隔离， 实现控制区有关业务与其它区域相关业务系统的横向数据通信。

正向隔离装置和反向隔离装置部署在控制区、非控制区与管理信息大区的网络边界，用于生产控制大区网络与管理信息大区网络的物理隔离，正向隔离装置实现生产控制大区有关业务系统以正向单向方式向管理信息大区相关业务系统发送数据；反向隔离装置实现管理信息大区有关系统以反向单向方式向生产控制区相关业务系统导入纯文本数据。

控制区纵向加密认证网关部署在控制区与调度数据网实时 VPN 之间，用于本地控制区与远端控制区相关业务系统或业务模块之间网络数据通信的身份认证、访问控制和传输数据的加密与解密，保障系统连接的合法性和数据传输的机密性及完整性。

非控制区纵向加密认证网关（硬件防火墙）部署在非控制区与调度数据网络非实时 VPN 之间，用于本地非控制区与远端非控制区相关业务系统或业务模块之间网络数据通信的访问控制。

火电厂二次系统安全区横向及纵向互联方案 1 的配置要点如下：

（1）在控制区互联交换机上划分若干实时业务 VLAN ，各 VLAN 地址为调度数据网实时 VPN 的业务段地址， 实时 VLAN 中，有两个 VLAN 分别用于控制区的横向互联和纵向互联，其余 VLAN 分别用于控制区内不同类别业务系统的接入。

（2）在非控制区互联交换机上划分若干非实时业务 VLAN，各 VLAN 地址为调度数据网非实时 VPN 的业务段地址，非实时 VLAN 中，有两个 VLAN 分别用于非控制区的横向互联和纵向互联，其余 VLAN 分别用于非控制区内不同类别业务系统的接入。

（3）在控制区互联交换机和非控制区互联交换机上使用 ACL 功能对各 VLAN 实施访问控制，避免安全区域内各 VLAN 间业务系统直接互通。

（4）对于控制区具有横向数据通信的系统，可将其数据通信机上实时 VPN 业务段的 IP 地址通过横向互联的防火墙转换为非实时 VPN 业务段的地址，并且使用防火墙访问控制功能对转换后的地址实施访问限制。

（5）在正、反向隔离装置上配置内外网的业务系统虚拟访问地址及相应安全控制规则。

（6）控制区纵向加密认证网关和非控制区纵向加密认证网关（硬件防火墙）均采用透明工作方式。

（7）在控制区纵向加密认证网关和非控制区纵向加密认证网关（硬件防火墙）上配置安全控制规则。

（8）控制区和非控制区各业务系统通信机的网关地址为该机所接入 VLAN 的网关地址；控制区

互联交换机上路由到非控制区业务网段的网关地址为横向互联防火墙的内部网口地址，路由到调度数据网实时 VPN 的下一跳地址为调度数据网网络设备上的实时 VPN 业务段连接地址；非控制区互联交换机上路由到调度数据网非实时 VPN 的下一跳地址为调度数据网网络设备上的非实时 VPN 业务段连接地址。

（9）在控制区，若存在某些业务系统同时具有实时类数据（或控制类数据）和非实时类数据的纵向传输（例如： 一体化系统保信子站， 其接收主站下发的设置指令为控制类数据，而上传主站召唤的录波数据为非实时类。又如： PMU 子站，其上传主站的相量和频率数据为实时类数据， 而上传主站召唤的历史数据和录波数据为非实时类数据），为了使控制区的这些业务系统既可使用实时 VPN 传输实时类数据（或控制类数据）又可使用非实时 VPN 传输非实时类数据且不形成 VPN 之间纵向交叉连接，可采取如下方法：

1）将控制区具有非实时数据传输的业务系统通信机外网口 IP 地址通过横向互联防火墙由实时 VPN 业务段地址转换为非实时段的地址；

2）通过防火墙对转换后的地址实施严格的访问控制，其访问控制策略为，只允许主站有通信需求的非实时 VPN 业务段地址（主机地址）及业务 TCP 端口访问转换后的地址。

2、公网业务终端二次系统安全防护结构规范

公网业务终端所属安全分区与其所连接的主站系统的安全分区相同。公网业务终端通过相应安全强度的安全防护设备纵向连接不同的广域网络。

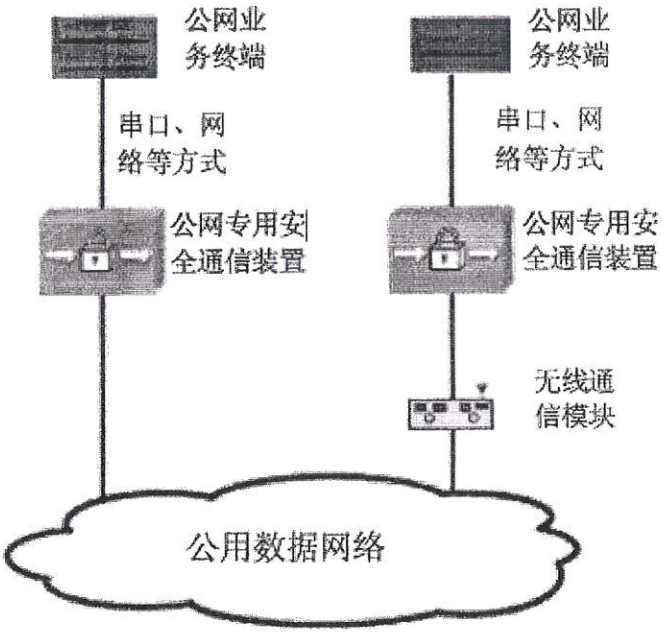


图 22　公网业务终端二次系统安全防护拓扑结构示意图

公网业务终端纵向互联的主要设备包括各业务系统的公网业务终端、公网专用安全通信装置、无线通信模块，这些设备均可采取冗余备用结构。

公网业务终端用于业务系统的数据采集。

公网专用安全通信装置部署在业务终端与公用数据网络之间，用于本地公网业务终端与远端生产控制大区涉公用数据网络的业务系统之间网络数据通信的身份认证和传输数据的加密与解密，保障系统连接的合法性和数据传输的机密性及完整性。

当采用的公用数据网络为无线网络时， 可采用无线通信模块。无线通信模块部署在公网专用安全通信装置部署与公用数据网络之间， 用于无线电信号的发射与接收。

公网业务终端纵向互联的配置要点如下：

（1）公网专用安全通信装置采用透明工作方式。

（2）公网专用安全通信网关应能与相应子站的公网专用安全通信装置进行身份认证并建立加密数据通信通道，实现业务系统的数据通信。

三、设备选型规范

1、网络交换机

本处所指网络交换及是用于生产控制大区横向和纵向网络边界互联的交换机，其设备选型应符合下列基本要求：

（1）网络接口：10/100M 以太网电接口≥ 24 个； 1000M 以太网光接口≥ 2 个。

（2）设备可安装于 19 英寸标准机柜。

功能及性能要求

（1）支持静态、RIP 等路由协议。

（2）备板交换能力：≥ 32Gbps。

（3）二、三层包转发能力≥ 6.5Mbps。

（4）支持 VLAN 间的访问控制列表。

（5）支持 MPLS VRF Lite 或与之类似的逻辑隔离功能。

（6）支持 VLAN 数目≥ 1000。

（7）支持本机和远端交换机的端口镜像功能。

（8）支持路由冗余负载均衡 VRRP 功能。

2、网络安全监测装置

序号	项目	子项	标准参数值	投标人保证值
1	硬件配置	内存	内存不低于 4GB	（投标人填写）
2		硬盘容量	不低于 250GB	（投标人填写）
3		存储方式	固态硬盘	（投标人填写）
4		网卡	具备不少于 4 个 10M/100M/1000M 自适应以太网电口	（投标人填写）
5	技术要求	一般要求	在故障、重启的过程中不引起数据重发、误发、漏发	（投标人填写）
6			有明显的接地标志	（投标人填写）
7			有安全警示标识	（投标人填写）
8			应具备装置故障告警信号输出接点，装置运行灯灭时应导通装置故障接点	（投标人填写）

9			应采用无风扇、无旋转部件硬件设计	（投标人填写）
10		正常工作大气条件	大气压力： 70～106kPa	（投标人填写）
11		性能要求	采集信息吞吐量≥600 条/s； 支持监测对象数量≥100； 对上传事件信息的处理时间≤1s； 对远程调阅的处理时间≤3s； 应支持上传事件信息的本地存储，保存至少一年的上传事件信息； 本地日志审计记录条数≥10000 条； 通过 IRIG-B 同步，对时精度≤1ms， 通过 SNTP 同步，对时精度≤100ms； 在没有外部时钟源校正时，24 小时守时误差应不超过 1s； 平均故障间隔时间（MTBF）≥30000h。	（投标人填写）
12		贮存、运输极限环境温度	装置的贮存、运输极限的环境温度－25℃～＋70℃，相对湿度不大于85%，不应出现异常情况。温度恢复正常后装置的功能和性能应符合要求。	（投标人填写）
13		绝缘电阻要求	在正常试验大气条件下额定绝缘电压 U_i≤60V，绝缘电阻要求≥5 MΩ（用 250V 兆欧表）；U_i＞60V，绝缘电阻要求≥5 MΩ（用 500V 兆欧表）	（投标人填写）
14		冲击电压	在正常试验大气条件下装置的电源输入回路、交流信号输入回路、信号输出触点等各回路对地、以及回路之间，应能承受 1.2/50μs 的标准雷电波的短时冲击电压试验，当额定绝缘电压大于 60V 时，开路试验电压为 5kV；当额定绝缘	（投标人填写）

			电压不大于 60V 时，开路试验电压为 1kV。试验后装置应无绝缘损坏和器件损坏。	
15		电磁兼容要求	电磁兼容应满足 GB/T 17626 标准	（投标人填写）
16		机械性能要求	正弦稳态振动、冲击、自由跌落的参数等级见 GB/T 2423.10 中规定； 装置防护性能：符合 GB/T 4208 规定的 IP20 级要求； 箱体抗盐蚀能力：满足 GB/T 10125 标准的中性盐雾试验 96h 试验周期无锈蚀。	（投标人填写）
17	外观接口	外形尺寸	应符合 GB/T 19520.12 的规定，应采用 1U 整层机箱。	（投标人填写）

注 1 项目单位对标准技术参数表中参数有差异时，可在项目需求部分的项目单位技术差异表中给出，投标人应对该差异表响应。差异表与标准技术参数表中参数不同时，以差异表给出的参数为准。参数名称栏中带*的参数为重要参数。如不能满足要求，将被视为实质性不符合招标文件要求。

3、纵向加密装置

配置要求

（1）至少具备 2 个 10/100M 网络接口。

（2）具备双机热备接口。

（3）具备 1 个 RS232 配置接口+ 1 个 IC 卡读卡器接口。

（4）具备双电源。

（5）装置可安装于 19 英寸标准机柜。

安全性要求

（1）必须通过国家密码管理委员会办公室组织的安全性审查和技术鉴定。

（2）具备公安部销售许可证。

（3）通过南方电网公司组织的功能与性能测试。

（4）采用专用服务器硬件和代码可控的安全操作系统。

（5）本身应能够一定程度防御常见的网络攻击，包括 ARP Attack 、Ping Attack 、Pingof Death Attack 、Smurf Attack 、Unreachable Host Attack 、Land Attack 、Teardrop Attack 、Syn Attack 等。

（6）支持设备密钥、工作参数的备份与恢复。

可靠性要求

（1）应通过有关部门组织的电磁兼容性检测。

（2）应支持双机热备功能，在任一设备出现故障时，自动切换。

（3）应具有自动旁路功能，在紧急故障状态下，可以旁路所有安全功能，作为透明桥接设备工作，必要时允许通过网线旁路。在旁路状态下，设备应有明显的警告提示。

功能要求

（1）采用国家密码管理局批准的电力专用密码算法对传输的数据进行保护，保证数据的真实性、机密性和完整性。

（2）加密认证装置或加密认证网关之间支持基于电力数字证书的双向认证。

（3）支持透明工作方式与网关工作方式，支持 NAT。

（4）具有基于 IP 、传输协议、应用端口号的综合报文过滤与访问控制功能。

（5）加密认证网关支持对电力应用协议的特殊报文进行选择性加密保护。

（6）符合《IP 加密认证装置技术规范》的技术要求，支持不同厂家设备的互联互通。

（7）装置必须能够识别、处理网络正常运行所需要的路由协议报文、及其他协议报文。

（8）装置必须能够识别、过滤、转发 Trunk 协议的报文， 装置本地配置功能必须支持设置 VLanID。

性能要求

（1）最大并发加密隧道数： 300 条

（2）100M LAN 环境下，加密隧道建立延迟：＜ 1s

（3）明文数据包吞吐量： 40Mbps （50 条安全策略， 1024 报文长度）

（4）密文数据包吞吐量： 20Mbps （10 条安全策略， 1024 报文长度）

（5）数据包转发延迟：＜ 2ms （50%密文数据包吞吐量）

（6）满负荷数据包丢弃率： 0

纵向加密装置（普通型）

序号	参数名称	单位	招标人要求	投标人保证值
1	*网络接口	个	100M 网卡接口≥4 个	（投标人填写）
2	外设接口	个	终端接口(RS232) 1 个 智能 IC 卡接口 1 个	（投标人填写）

序号	参数名称	单位	招标人要求	投标人保证值
3	设备厚度	U	1U	（投标人填写）
4	平均无故障时间(MTBF)	h	>60000h(100%负荷)	（投标人填写）
5	最大并发加密隧道数	条	1024 条	（投标人填写）
6	*明文数据包吞吐量	Mbps	95Mbps(50 条安全策略，1024 报文长度)	（投标人填写）
7	*密文数据包吞吐量	Mbps	25Mbps(50 条安全策略，1024 报文长度)	（投标人填写）
8	*数据包转发延迟	ms	＜1ms	（投标人填写）
9	*100M LAN 环境下，加密隧道建立延迟	ms	＜1ms（50%数据吞吐量）	（投标人填写）
10	满负荷数据包丢弃率	%	0	（投标人填写）

注 1 项目单位对标准技术参数表中参数有差异时，可在项目需求部分的项目单位技术差异表中给出，投标人应对该差异表响应。差异表与标准技术参数表中参数不同时，以差异表给出的参数为准。参数名称栏中带*的参数为重要参数。如不能满足要求，将被视为实质性不符合招标文件要求。

纵向加密装置（增强型）

序号	参数名称	单位	招标人要求	投标人保证值
1	*网络接口	个	1000M 网卡接口≥4 个	（投标人填写）
2	外设接口	个	终端接口(RS232) 1 个 智能 IC 卡接口 1 个	（投标人填写）
3	设备厚度	U	1U	（投标人填写）
4	平均无故障时间(MTBF)	h	>100000h(100%负荷)	（投标人填写）
5	最大并发加密隧道数	条	2048 条	（投标人填写）
6	*明文数据包吞吐量	Mbps	340Mbps(100 条安全策略，1024 报文长度)	（投标人填写）
7	*密文数据包吞吐量	Mbps	80Mbps(50 条安全策略，1024 报文长度)	（投标人填写）
8	*数据包转发延迟	ms	＜1ms	（投标人填写）
9	*1000M LAN 环境下，加密隧道建立延迟	ms	＜1ms（50%数据吞吐量）	（投标人填写）

序号	参数名称	单位	招标人要求	投标人保证值
10	满负荷数据包丢弃率*	%	0	（投标人填写）

注 1 项目单位对标准技术参数表中参数有差异时，可在项目需求部分的项目单位技术差异表中给出，投标人应对该差异表响应。差异表与标准技术参数表中参数不同时，以差异表给出的参数为准。参数名称栏中带*的参数为重要参数。如不能满足要求，将被视为实质性不符合招标文件要求。

4、安全隔离装置

配置要求

（1）网络接口： 10/100M 接口 2 个（内网） +10/100M 接口 2 个（外网） +1 个 10/100M 双机热备接口。

（2）外设接口： 2 个终端接口(RS232)+ 读写器接口。

（3）电源接口：配置双电源。

（4）装置可安装于 19 英寸标准机柜。

安全性要求

（1）具有电力专用安全防护设备的检测证明。

（2）具备公安部销售许可证。

（3）反向隔离装置必须通过国家密码管理委员会办公室组织的安全性审查和技术鉴定。

（4）采用非 INTEL 指令系统的（及兼容）的 RISC 微处理器构筑内网隔离系统。

（5）采用嵌入式安全操作系统， 去除 TCP/IP 协议栈和其它不需要的系统服务， 保证系统安全程度最大化。

（6）能抵御除已知的网络攻击。

可靠性要求

（1）装置应支持双机热备方式工作，在设备出现故障，能自动切换。

（2）装置应具备双路电源，并支持主备电源的在线无缝切换。

（3）装置支持多种连接方式，可以根据现场安装情况，选择支持“单进单出” 、“双进单出”、“双进双出”等接入模式运行。

（4）隔离设备的关键芯片和元器件都进行产品老化试验，所有的隔离设备在出厂前必须经过不少于 72 小时地连续通电测试，并提供相关质量报告。

功能要求

- **正向隔离装置**

（1）实现两个安全区之间的物理安全的数据交换，并且保证安全隔离装置内外两个处理系统不同时连通。

（2）表示层与应用层数据完全单向传输， 即从安全区 III 到安全区 I/II 的 TCP 应答禁止携带应用数据。

（3）透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址。

（4）基于 MAC、IP 、传输协议、传输端口以及通信方向的综合报文过滤与访问控制。

（5）支持 NAT。

（6）防止穿透性 TCP 联接：禁止两个应用网关之间直接建立 TCP 联接，应将内外两个应用网关之间的 TCP 联接分解成内外两个应用网关分别到隔离装置内外两个网卡的两个 TCP 虚拟联接。隔离装置内外两个网卡在装置内部是非网络连接，且只允许数据单向传输。

（7）具有可定制的应用层解析功能，支持应用层特殊标记识别；

（8）安全、方便的维护管理方式：基于证书的管理人员认证，图形化的管理界面。

（9）支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时， 可通过隔离装置专用的告警串口或网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准。

- **反向隔离装置**

（1）实现两个安全区之间的物理安全的数据交换，并且保证安全隔离装置内外两个处理系统不同时连通。

（2）具有基于数字证书的数据签名/ 解签名功能， 具有电力加密算法进行数字加密的功能。

（3）具有应用数据内容有效性检查功能。

（4）具有纯文本编码检查功能。

（5）实现两个安全区之间的物理安全的数据传递。

（6）支持透明工作方式：虚拟主机 IP 地址、隐藏 MAC 地址。

（7）支持 NAT。

（8）基于 MAC、IP 、传输协议、传输端口以及通信方向的综合报文过滤与访问控制；

（9）防止穿透性 TCP 联接。

（10）基于数字证书的图形化界面，通过专用智能 IC 卡进行身份认证，保证配置管理的安全。

（11）支持系统告警，支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时， 可通过隔离装置专用的告警串口或网络向第三方日志告警管理系统输出报警信息，日志格式遵循 Syslog 标准。

性能要求

- 正向隔离装置

（1）百兆状态下数据包吞吐率≥ 40Mbps（100 条安全策略， 1024 字节报文长度）

（2）数据包转发延迟：＜ 10ms（100%负荷）

（3）满负荷数据包丢弃率为 0

（4）平均无故障时间(MTBF) ＞60000 小时(100%负荷)

- 反向隔离装置

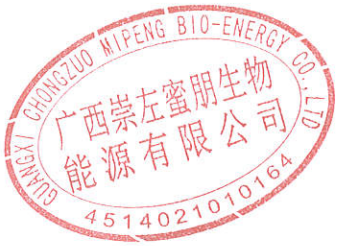
（1）百兆状态下的密文有效网络吞吐率≥ 20Mbps

（2）数字签名速率大于 60 次/ 秒

（3）数据包转发延迟＜ 30ms

（4）满负荷数据包丢弃率为 0

（5）平均无故障时间(MTBF) ＞60000 小时(100%负荷)



5、硬件防火墙

生产控制大区的硬件防火墙选型应符合下列基本要求：

安全性要求

（1）具有自主知识产权的国产设备。

（2）具备公安部颁发的《计算机信息系统安全专用产口销售许可证》。

（3）具备中国国家信息安全测评认证中心颁发的《国家信息安全认证产品型号证书》。

（4）支持 VPN 功能的，需要采用通过国家密码管理局鉴定的密码算法，并提供国家密码管理局的技术鉴定证书。

（5）采用专用服务器硬件和安全操作系统。

功能要求

（1）可以基于网络地址、通讯协议、通讯端口，用户账号，信息传输方向、操作方式、网络通讯时间、网络服务等进行综合过滤与访问控制。

（2）支持动态网络地址转换（ NAT）。

（3）支持 IP 和 MAC 地址绑定。

（4）支持应用层协议的内容过滤： 对 HTTP 过滤做到命令级包括 URL 和脚本（Java Applet 和 ActiveX ）两种类型的请求过滤、页面内容过滤； 对 FTP 过滤功能的特性支持命令级控制，以及基于命令级控制实现的对目录和文件的访问控制； 对 SMTP 过滤功能特性支持主题过滤、正文过滤、附带文件过滤、地址过滤、防止邮件炸弹、限制邮件大小、限制 Relay 等功能。

（5）支持路由及交换两种工作模式； 在交换模式下支持多 VLAN 之间代理路由功能，方便各区域中不同网段数据的转发。

（6）支持 IEEE802.1q 的 Trunk 封装协议。

（7）提供网络信息自动收集功能，如共享资源信息、IP/MAC 地址信息、开放端口信息等。

（8）提供基于 IP 地址及用户的最大流量控制功能，提供基于优先级的宽带管理功能。

（9）具有一次性口令用户身份认证功能， 并通过标准的 RADIUS 协议支持第三方的认证。

（10）具有安全的自身防护能力， 可以实时防止多种网络攻击和扫描； 当出现异常情况时可发出告警信息。

（11）防火墙上的配置信息、过滤规则可以方便的下载并保存在软盘或某 PC 机中，以供备份，需要时再上载或恢复。

（12）支持多机热备份功能，切换时间不能超过 1 秒。

（13）日志系统支持网络和本地两种存取方式， 日志包括事件日志和访问日志。日志应可方便导出。

（14）具有中文 GUI 界面，通过 GUI 能够完成全部防火墙的集中配置、管理工作；对防火墙的管理可以划分多级访问权限， 对不同的网管人员分配不同的管理权限， 提供灵活的管理、监控机制。

（15）采用简化方案对横向互联防火墙和纵向互联防火墙进行合并的还需支持虚拟防火墙功能。

性能要求

- **百兆硬件防火墙**

（1）网络吞吐率≥ 100Mb

（2）最大并发连接数＞ 200000

（3）新建连接速率＞ 3000 连接/ 秒

（4）平均无故障时间≥ 60000 小时

- **千兆硬件防火墙**

（1）网络吞吐率≥ 1000Mb

（2）最大并发连接数＞ 1000000

（3）新建连接速率＞ 20000 连接/ 秒

（4）平均无故障时间≥ 60000 小时

6、入侵检测系统

入侵检测系统可部署在省级及以上调度控制中心的安全区 I 和安全区 II 的网络边界上，对横向

和纵向网络边界实施检测，对安全事件进行记录和审计。

安全性要求

（1）具有自主知识产权的国产设备。

（2）具备公安部颁发的《计算机信息系统安全专用产口销售许可证。

（3）具备中国国家信息安全测评认证中心颁发的《国家信息安全认证产品型号证书》

功能要求

（1）系统具备完整的规则库，至少能检测超过 100 种的网络应用层协议。

（2）系统支持采用模式匹配、协议识别、协议异常检测、关联分析等多种技术识别各种攻击。

（3）系统支持对常用的应用协议包括 HTTP、FTP、SMTP、POP3、TELNET 等数据连接的内容恢复的功能，能够完全记录通信的过程与内容，并将其回放。

（4）系统支持 IP 碎片重组和 TCP 流会话重组技术。

（5）支持与通用的防火墙进行联动并协同防御。

（6）系统内置基于状态检测的防火墙，支持地址转换功能，具有流量管理功能，对于可能出现的异常流量，提供抗拒绝服务攻击功能。

（7）系统具备入侵警报实时通知功能，保证管理员能够及时发觉网络中的入侵行为以采取相应的措施来保护网络的安全。

（8）系统具备灵活的查询和报表功能，可对网络中的攻击事件，访问记录进行查询，并可根据查询结果输出直观的报表。

（9）系统支持多种管理方式，包括单级管理、主辅管理、多级管理等，并提供图形化的监测主机系统配置工具，灵活支持对监测主机的系统及网络配置进行修改和配置。

（10）系统支持手动或自动备份事件数据库，并具备完善的事件审计功能。

性能指标要求

- 百兆 IDS

（1）系统检测率＞ 98%（100%负荷）

（2）系统误报率＜ 1%（100%负荷）

（3）最大检测能力＞ 90Mb

（4）最大并发连接数＞ 30000/ 秒

（5）平均无故障时间＞ 60000 小时

- 千兆 IDS

（1）系统检测率＞ 98%（100%负荷）

（2）丢包误报率＜ 1%（100%负荷）

（3）最大检测能力＞ 900Mb

（4）最大并发连接数＞ 600000/ 秒

（5）平均无故障时间＞ 60000 小时

7、综合审计平台

平台应能全面收集，集中存储生产控制大区、管理信息大区各种业务系统、网络设备、安全防护设备、机房设施等的运行日志、操作系统日志、数据库访问日志、即时告警信息，具备动态监视、故障分析，安全审计、事件预警及告警功能。

平台的设计方案必须符合二次系统安全防护的总体策略及相关的安全要求。

安全性要求

具有自主知识产权的国产设备。

功能要求

（1）能够以图、表等方式显示设备工作状态、系统拓扑图、系统日志、告警信息、统计和审计结果等。

（2）支持基于角色（如系统管理员、系统安全员、值班员）的权限管理；并支持系统及设备分类管理。

（3）可对不同产品的系统日志、告警信息进行集中收集。

（4）可对告警信息进行分级、分类，具有告警过滤功能。

（5）支持对跨设备的大量事件进行关联分析，及时判断并分析在网络中发生的违反安全策略和未经授权的行为。

（6）提供丰富灵活的方式对告警信息和日志信息进行查询。

（7）可辅助分析安全状态和安全事件原因。

（8）具备完整的统计报表，且可灵活定制报表。

（9）支持按系统或设备类别生成审计报告。

（10）支持通过声响、手机短信、移动电话等方式的即时告警功能。

（11）具备良好的可扩展性，可方便实现新增系统或设备接入。

广西崇左蜜明生物能源有限公司 GUANGXI CHONGZUO MIFENG BIO-ENERGY CO.,LTD 4514021010164

工段长：2019.6.26.　　技术部工程师：2019.6.26.

部门经理：2019.6.26　　生产总经理：2019-6-26

广西崇左蜜朋生物能源有限公司
电力监控系统网络安全防护项目设备清单

序号	名　称	生产厂家	型式、规格、性能参数	单位	数量	备注
一	**态势感知装置**	许继昌南	PSSEM-2000S	台	1	
二	**数据网接入设备柜**			套	1	
1	接入交换机	华为	S3700-28TP-SI-AC	台	1	
2	纵向加密装置	科东	Pstunnel-2000；支持SM2加密算法	台	2	
3	防病毒系统	瑞星	瑞星杀毒软件	套	1	
4	主机加固	北京信达		套	1	
5	探针软件	许继昌南		套	3	
6	安装机柜	许昌许继	2260×800×600(高×宽×厚)	面	1	
7	配套线缆及附件	许昌许继		套	1	
8	杀毒U盘	金士顿	瑞星杀毒软件	个	1	
9	安全U盘	金士顿	企业级硬件加密64G	个	1	
10	杀毒电脑	联想	Thinkpad笔记本	台	1	
三	产品调试与验收	许继昌南		项	1	

备注：1、供方提供的软件硬件确保能够接入许继CBZ8000后台系统；
2、供方负责与供电局进行对接，确保产品能通过供电局检测与验收。

生产总经理：　　部门经理：　　工段长：

2019-6-26　　2019.6.26　　2019.6.26

GUANGXI CHONGZUO MIPENG BIO-ENERGY CO.,LTD
广西崇左蜜朋生物能源有限公司
4514021010164

请购单：11000 62307