

# 电力行业详细讲解以及方案



电力是以电能作为动力的能源。发明于 19 世纪 70 年代，电力的发明和应用掀起了第二次工业化高潮。成为人类历史 18 世纪以来，世界发生的三次科技革命之一，从此科技改变了人们的生活。20 世纪出现的大规模电力系统是人类工程科学史上最重要的成就之一，是由发电、输电、变电、配电和用电等环节组成的电力生产与消费系统。它将自然界的一次能源通过机械能装置转化成电力，再经输电、变电和配电将电力供应到各用户。

## 优点：

- 1、火力发电：燃料容易获取，热机效率高，调峰较易实现，建设成本低，容易与冶金、化工、水泥等高能耗工业形成共生产业链。
- 2、核能发电：基本不受自然资源产地限制，运行成本低，无温室气体排放。
- 3、水力发电：几乎完全无污染，运营成本低，便于调峰，可再生，有航运、水利等边际效益。
- 4、风力发电：无环境污染，运行成本低，可再生。
- 5、太阳能光伏发电：运行无污染，可再生，设备小型化，适合非集中供电。

## 弊端：

### 火力发电

烟气污染：煤炭直接燃烧排放的SO<sub>2</sub>、NO<sub>x</sub>等酸性气体不断增长，使我国很多地区酸雨量增加。全国每年产生 140 万吨SO<sub>2</sub>。

粉尘污染：对电站附近环境造成粉煤灰污染，对人们的生活及植物的生长造成不良影响。全国每年产生 1500 万吨烟尘。

资源消耗：发电的汽轮机通常选用水作为冷却介质，一座 100 万千瓦火力发电厂每日的耗水量约为 十万吨。全国每年消耗 5000 万吨标准。

### 水力发电

水力发电要淹没大量土地，有可能导致生态环境破坏，而且大型水库一旦塌崩，后果将不堪设想。另外，一个国家的水力资源也是有限的，而且还要受季节的影响。

## 风力发电

噪声，视觉污染。占用大片土地及林地，对植被破坏大。不稳定，不可控。成本仍然很高。

## 核能发电

要用反应堆产生核能，需要解决以下 10 个问题：

1. 为核裂变链式反应提供必要的条件，使之得以进行。
2. 链式反应必须能由人通过一定装置进行控制。失去控制的裂变能不仅不能用于发电，还会酿成灾害。
3. 裂变反应产生的能量要能从反应堆中安全取出。
4. 裂变反应中产生的中子和放射性物质对人体危害很大，必须设法避免它们对核电站工作人员和附近居民的伤害。
5. 核能电厂会产生高低阶放射性废料，或者是使用过之核燃料，虽然所占体积不大，但因具有放射线，故必须慎重处理，且需面对相当大的政治困扰。
6. 核能发电厂热效率较低，因而比一般化石燃料电厂排放更多废热到环境里，故核能电厂的热污染较严重。
7. 核能电厂投资成本太大，电力公司的财务风险较高。
8. 核能电厂较不适宜做尖峰、离峰之随载运转。
9. 兴建核电厂较易引发政治歧见纷争。
10. 核电厂的反应器内有大量的放射性物质，如果在事故中释放到外界环境，会对生态及民众造成伤害。

核电在正常情况下固然是干净的，但万一发生核泄漏，后果同样是可怕的。前苏联切尔诺贝利核电站事故，已使 900 万人受到了不同程度的损害，而且这一影响并未终止。

EMPPOWERED PERFORMANCE  
电力行业解决方案：

## 电力行业解决方案

### 一、项目背景

电力行业属于国有垄断性产业，是关系到国计民生的基础性行业，从组织上可划分为发电、调度两大系统和发电、输电、供电、用电四大环节，发电系统根据电厂的发电能级以及所处的位置分为跨网电厂、网级电厂、省级电厂、自备电厂及小水电等四个发电级别，统一向电网供电。供电系统实行分层次管理，即分为国家电网公司、网局/独立省局、地区和县电力公司四级；总体架构为金字塔形，上层对下层进行严密的控制。电力生产的产品是电能，其有着发、输、配、用电同时完成，不能储存的特点。电力生产的过程是：由发电系统向供电系统售电，供电系统将电经由高压电网送往全国各个城市并售给每个用电户，其中的资金结算由电网的计量关口电能表确定，整个过程复杂严密，对信息系统存在很大的依赖性。

电力二次系统主要是指支撑电力调度任务的相关系统，包括电力监控系统、电力通信及数据网络等，其中电力监控是指用于监视和控制电网及电厂生产运行过程的、基于计算机及网络技术的业务处理系统及智能设备等。包括电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和自动装置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量计费系统、实时电力市场的辅助控制系统等；电力调度数据网络，是指各级电力调度专用广域数据网络、电力生产专用拨号网络等；电力二次系统是电力生产的重要环节，其信息网络也是电力行业信息化建设的重要组成部分。

国家对电力二次系统信息网络安全防护非常重视，2002年5月中华人民共和国国家经贸委30号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》（以下简称《规定》），对电力系统安全建设具有重要的指导意义。2006年电监会印发了《电力二次系统安全防护总体方案》，确定了电力二次系统安全防护体系的总体框架，细化了电力二次系统安全防护总体原则，定义了通用和专用的安全防护技术与设备，提出了省级以上调度中心、地县级调度中心、发电厂、变电站、配电等的二次系统安全防护方案。这些制度和方案对各省电力公司的安全体系建设起着指导意义。

XXXX电力集团公司是中央驻XXXX企业，是国家电网公司的所属企业，下属XX个市供电公司、超高压公司等XX家分公司，等多家全资（控股）子公司，对全省XX个县售电企业实行代管，其信息网络是非常庞大的，并且覆盖到生产、办公的各个领域，其电力二次系统包含了各级电力调度的能量管理系统、广域测量系统、电能量系统、调度计划系统、继电保护管理系统、调度员培训模拟系统、电力市场运营系统等，成为XXXX电力集团公司最核心的业务支撑平台，也是重点需要防护的信息网络系统。根据国家经贸委30号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》，同时参考电监安全[2006]34号文件《电力二次系统安全防护总体方案》提出的建设内容和目标，需要对电力二次系统整体安全保障进行全面的建设，确保电力监控系统及电力调度数据网络的安全，抵御黑客、病毒、恶意代码等各种形式的恶意破坏和攻击，防止电力二次系统的崩溃或瘫痪，保障电力应用系统的正常有序开展。为此，特编写此规划，针对XXXX电力集团公司电力二次系统的安全保障建设提出建设建议。

### 二、项目目标

本方案并根据我国电力系统的具体情况，结合 XXXX 电力公司二次系统的实际情况，参考国家经贸委[2002]第 30 号令《电网和电厂计算机监控系统及调度数据网络安全防护的规定》（以下简称《规定》）的要求，和电监安全[2006]34 号文件《《电力二次系统安全防护总体方案》》进行编写，目的是规范和统一 XXXX 电力二次系统安全防护的方案设计、工程实施和运行监管，重点防范对电网和电厂计算机监控系统及调度数据网络的攻击侵害及由此引起的电力系统事故，以保障我国电力系统的安全、稳定、经济运行，保护国家重要基础设施的安全。通过我们的分析认为，XXXX 电力二次系统安全防护的重点是确保电力实时闭环监控系统及调度数据网络的安全，目标是抵御黑客、病毒、恶意代码等通过各种形式对系统发起的恶意破坏和攻击，特别是能够抵御集团式攻击，防止由此导致一次系统事故或大面积停电事故，及二次系统的崩溃或瘫痪。从防护措施的角度，XXXX 电力二次系统安全防护应当包含以下五个部分：

- ★ 调度中心（地调及以上）二次系统安全防护体系；
- ★ 配电（含县调）二次系统安全防护体系；
- ★ 变电站二次系统安全防护体系；
- ★ 发电厂二次系统安全防护体系；
- ★ 电力二次系统安全管理。

### 三、网络架构描述

从系统总体结构上，XXXX 电力集团二次系统呈现为典型的横、纵式网状结构，从横向的角度，XXXX 电力集团二次系统可划分为生产控制大区和管理信息大区，其中生产控制大区又可分为控制区（安全区 I）和非控制区（安全区 II）；在不影响生产控制大区安全的前提下，管理信息大区又可划分为管理服务器区（安全区 III）和办公区（安全区 IV）。其中安全区 I 是 XXXX 电力集团生产的核心环节，直接实现对电力一次系统的实时监控，典型业务包括电力数据采集和监控系统等，纵向上利用电力调度数据网的实时子网进行通信，是 XXXX 电力集团二次系统中最重要、安全等级最高的信息系统，也是 XXXX 电力集团二次系统安全防护的重点与核心；安全区 II 则包括了 XXXX 电力生产的重要业务系统，其特点是在线运行但不具备控制功能，典型业务包括调度员培训模拟系统（DTS）等。纵向上利用电力调度数据网的非实时子网进行通信，其重要性仅次于安全区 I，也是 XXXX 电力集团二次系统安全防护的重点环节；安全区 III 主要包括 XXXX 电力生产所需的调度管理系统等，纵向上利用电力企业数据网进行通信，形式上主要采用 B/S 结构的方式，实现对相应业务的处理，是 XXXX 电力集团二次系统安全防护的重要环节，系统可用性的要求比较高；安全区 IV 则包括办公及 OA 系统，包含的业务有办公自动化系统（OA）、客户服务等。该区域与互联网存在接口，因此安全威胁来源比较多，也需要从边界防护的角度上进行对应的安全系统设计与建设。

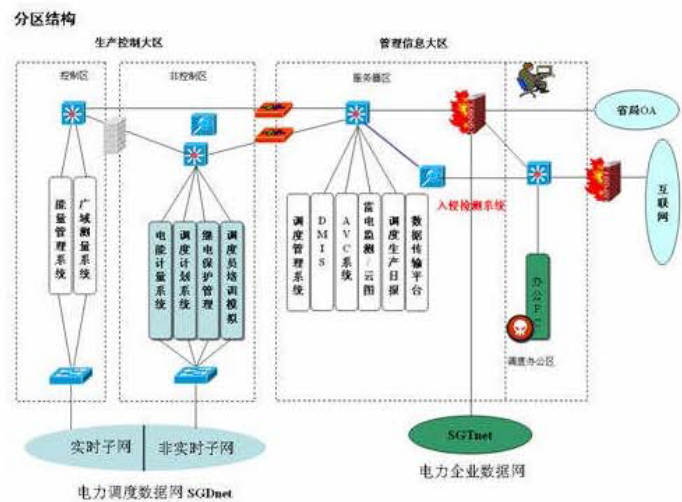


图 2.1a XXXX 电力全省二次系统横向分区结构示意图

此外，从纵向的角度，根据 XXXX 电力二次系统又可分为省调度中心（省调）；地市级调度中心（地调，包括了××个市级供电公司）；县级调度中心（县调）；以及变电站、发电厂和集控站等环节，纵向上根据横向的四个安全区，分别通过电力调度数据网以及电力企业数据网实现了各级电力二次系统的业务访问和处理

#### 四、调度中心二次系统安全防护方案

XXXX 电力的调度中心又可划分为省级调度中心（省调），地市级调度中心（地调）以及县区级调度中心（县调），这里我们以省调为例描述其按照“安全分区、网络专用、横向隔离、纵向认证”的建设原则，结合典型电力二次系统的防护技术和国家经贸委[2002]第 30 号令、电监安全[2006]34 号文件要求，确定的整体安全防护方案。地调和县调可参考省调进行建设，并根据投资情况适当调整部分的安全措施。

省调二次系统主要包括能量管理系统、广域相量测量系统、电网动态监控系统、继电保护和故障录波信息管理系统、电能计量系统、电力市场运营系统、调度员模拟系统、水库调度自动化系统、调度生产管理系统、雷电监测系统和电力调度数据网络等，针对调度中心采取防护措施主要包括防火墙、入侵检测、入侵防护、病毒防护、漏洞扫描、服务器核心防护、日志审计系统、专用安全隔离装置、专用数字证书、IP 认证加密装置、SSL VPN、终端安全管理、安全管理平台等系统，实现全面的防护，具体部署方式如下：



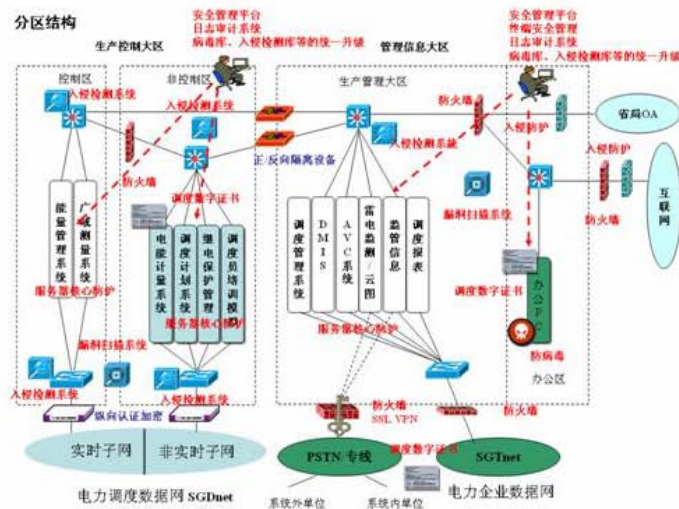


图 4.3 XXXX 电力二次系统调度中心安全防护部署图

说明:

从横向隔离的角度:

★ 生产控制大区和管理信息大区之间部署电力专用安全隔离装置，两大区之间只能有数据的交换，其他所有访问均不能直接在两个大区之间进行；

★ 防火墙则在安全隔离的基础上，隔离控制区和非控制区、生产管理区和办公区、办公区与省局 OA 区、办公区和互联网区域，进行严格的访问控制，防范非授权和越权的访问；

★ 在互联网以及省局 OA 边界，部署入侵防护系统，在防火墙的基础上进一步对访问数据包进行检测，有效防范外部攻击，阻断恶意代码；

从纵向隔离的角度:

★ 针对生产控制大区的纵向连接，采取 IP 认证加密设备进行纵向隔离，实现对下级单位访问用户的严格身份认证，同时利用加密确保数据的传输安全；

★ 在管理信息大区则采取防火墙实现纵向隔离。

从内部防护的角度:

★ 在生产控制大区的控制区、非控制区，以及管理信息大区核心部分，引入入侵检测系统，对安全区核心部位的数据包进行有效侦听，防范恶意攻击行为；

★ 针对重要的服务器，采取服务器核心防护技术，提升服务器的抗攻击能力；

★ 终端安全管理则主要作用于办公区内的终端，能够有效提高终端的抗攻击能力防止终端成为安全防护的短板；

★ 在生产控制大区和管理信息大区引入的漏洞扫描系统，通过对网络、服务、主机系统的实时扫描和分析，发觉系统存在的安全隐患，并提供给系统管理人员使其有针对性地采取措施，将安全隐患弥补在被利用之前；

★ 部署的全网病毒防护系统则有效实现对病毒的查杀，防止病毒在调度中心信息网络中大面积地传播。

从应用安全的角度

★ 通过专用调度数字证书，实现对应用系统访问的强身份认证，确保只有合法用户，才能在许可的

访问内访问各类业务应用系统。

★ 通过日志审计系统，对网络运行日志、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、安全设施运行日志等进行统一安全审计，及时自动分析系统安全事件，实现系统安全运行管理。

从安全管理的角度：

通过安全集中管理平台，实现对调度中心的安全管理，并通过对日志的分析，能够及时了解网络的活动状态，并对可能存在的安全事件进行迅速定位，防止安全事件的进一步发展。

## 五、安全建设效果

本方案根据国家经贸委[2002]第 30 号令和电监安全[2006]34 号文件的要求，总体上按照“安全分区、网络专用、横向隔离、纵向认证”的原则进行了设计和规划，具体包括：

### 满足安全分区的要求

根据 XXXX 电力二次系统的特点，和各相关业务系统的重要程度和数据流程、目前状况和安全要求，将整个电力二次系统分为两个大区，包括生产控制大区和管理信息大区，其中生产控制大区可划分为控制区（安全区 I）和非控制区（安全区 II），管理信息大区可划分为生产管理区（安全区 III）和管理信息区（安全区 IV）。不同的安全区确定了不同的安全防护要求，从而决定了不同的安全等级和防护水平。其中安全区 I 的安全等级最高，安全区 II 次之，其余依次类推，并按照分区进行边界防护以及部署其他安全产品。

### 满足横向隔离的要求

★ 在安全区 I、II 之间；安全区 III、IV 之间；以及安全区 IV 和互联网之间的网络节点上，部署硬件防火墙系统，并执行严格的访问控制，并且防火墙系统采取集中管理的方式，确保访问控制策略的有效性，杜绝非授权或非法的访问；

★ 在生产控制大区和管理信息大区边界部署专用安全隔离装置，实现更为安全的隔离，保障生产控制大区和管理信息大区只有数据被传递，任何直接的访问均被禁止。

### 满足纵向认证的要求

★ 针对生产控制大区（包括安全区 I、II），纵向认证主要通过国调统一部署的纵向安全认证装置来实现认证、加密、访问控制一体化的建设目标，针对管理信息大区（包括安全区 III、IV），纵向上采取防火墙实现隔离，形成多级隔离体系，防止下级单位的安全隐患传播到上级单位，造成大规模的安全事故；

★ 在省、地调之间的管理信息大区内则通过部署防火墙实现纵向隔离；

★ 对远程访问则通过 SSL VPN 结合 RADIUS 认证的方式实现安全访问。