

附件 3:

## 地（县）级调度中心监控系统安全防护方案

### 1 总则

1.1 为了加强地（县）级调度中心电力监控系统安全防护，保障电力监控系统的安全，依据《电力监控系统安全防护规定》和国家有关规定，制定本方案。

1.2 本方案是《电力监控系统安全防护总体方案》配套的系列文件之一，其它文件包括：《省级以上调度中心监控系统安全防护方案》、《变电站监控系统安全防护方案》、《发电厂监控系统安全防护方案》、《配电监控系统安全防护方案》和《电力监控系统安全防护评估规范》。

1.3 地（县）级调度中心电力监控系统安全防护目标是防范黑客及恶意代码等对电力监控系统发起的攻击和侵害，特别是抵御集团式攻击，防止地（县）级调度中心电力监控系统的瘫痪，并由此导致电力系统事故。地（县）级调度中心电力监控系统安全防护的重点是保障电网调度自动化系统及调度数据网络的安全。

1.4 本方案适用于地（县）级电力调度中心。大型地级电力调度中心安全防护方案可以参照《省级以上调度中心监控系统安全防护方案》执行。集控中心或集控站的集中监控系统的安全防护可以参照本方案执行。

## 2 典型结构

地（县）级调度中心监控系统主要包括调度自动化（包括监控和数据采集（SCADA）、电力系统高级应用软件（PAS）、调度员培训模拟等）、配电网调度自动化、负荷管理、电能量计量、调度生产管理、继电保护、故障信息管理、水库调度自动化、调度地理信息、电力调度数据网络及其他业务系统（如雷电监测、气象信息、变电站视频监视、配网生产抢修指挥等），根据安全分区原则，结合调度中心应用功能模块的特点，将各功能模块分别置于控制区、非控制区和管理信息大区。

地(县)级调度中心监控系统典型结构如图 1 所示：

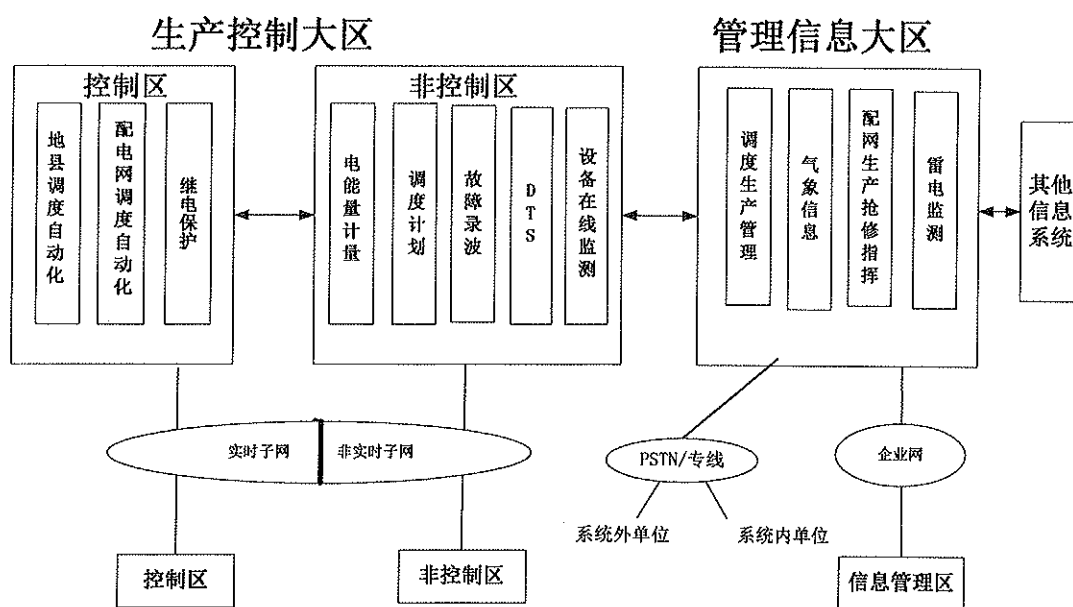


图 1 地（县）级调度中心监控系统典型结构示意图

随着技术的发展，地（县）级以上调度中心监控系统以及功能模块都会发生较大的变化，特别是在智能电网建设的



配电网实时监控、继电保护远方修改定值与远方投退、调度地理信息等业务和功能模块。

新一代电网调度控制系统的控制区主要包括：实时监控与预警类应用（电网运行稳态监控、电力监控设备在线监视与分析、自动电压控制、网络分析、综合智能告警分析）等业务和功能模块。

### **3.2 非控制区**

传统电网调度自动化系统的非控制区主要包括：调度员培训模拟、水情信息采集与处理、电能量采集与处理、变电和输电设备状态信息采集、故障录波信息管理等业务和功能模块。

新一代电网调度控制系统的非控制区主要包括：调度计划类应用（申报发布、预测、检修计划）、水电及新能源监测分析、调度员培训模拟等业务和功能模块。

### **3.3 管理信息大区**

传统电网调度自动化系统的管理信息大区主要包括：调度生产管理、雷电监测、气象信息、变电站视频监视及配网生产抢修指挥等业务和功能模块。

新一代电网调度控制系统的管理信息大区主要包括：调度管理类应用（生产运行、专业管理、综合分析与评估、信息展示与发布、内部综合管理）等业务和功能模块。

各安全区的业务功能详见表 1 和表 2。

表 1 地（县）级调度中心传统电力监控系统业务功能安全分区表

| 序号 | 系统功能     | 控制区                   | 非控制区          | 管理信息大区             |
|----|----------|-----------------------|---------------|--------------------|
| 1  | 调度自动化    | 电网实时监控、AVC、PAS 等      | 调度员培训模拟       | WEB 发布             |
| 2  | 配电网调度自动化 | 配电网实时监控               |               |                    |
| 3  | 继电保护     | 继电保护远方修改定值、远方投退等控制功能。 |               |                    |
| 4  | 故障信息管理   |                       | 故障录波信息管理模块    |                    |
| 5  | 调度地理信息   | 地理信息数据、地理信息服务         |               |                    |
| 6  | 水库调度自动化  |                       | 水情采集、信息处理     |                    |
| 7  | 电能量计量    |                       | 电能量采集、处理      |                    |
| 8  | 输变电状态监测  |                       | 变电、输电设备状态信息传输 |                    |
| 9  | 调度生产管理   |                       |               | 数据统计、分析、报表、管理流程、发布 |
| 10 | 雷电监测     |                       |               | 采集、处理              |
| 11 | 气象信息     |                       |               | 接收、处理              |
| 12 | 变电站视频监视  |                       |               | 接收、处理              |
| 13 | 配网生产抢修指挥 |                       |               | 配网生产抢修，指挥          |

表 2 地（县）级调度中心新一代调度控制系统业务功能安全分区表

| 序号 | 业务功能         | 控制区         | 非控制区   | 管理信息大区 |
|----|--------------|-------------|--------|--------|
| 1  | 智能调度控制系统基础平台 | 基础平台        | 基础平台   | 基础平台   |
| 2  | 实时监控与预       | 电网运行稳态监控、二次 | 水电及新能源 |        |

| 序号 | 业务功能    | 控制区                            | 非控制区         | 管理信息大区                           |
|----|---------|--------------------------------|--------------|----------------------------------|
|    | 警类应用    | 设备在线监视与分析、自动电压控制、网络分析、综合智能告警分析 | 监测分析、调度员培训模拟 |                                  |
| 3  | 调度计划类应用 |                                | 申报发布、预测、检修计划 |                                  |
| 4  | 调度管理类应用 |                                |              | 生产运行、专业管理、综合分析与评估、信息展示与发布、内部综合管理 |

#### 4 安全部署

根据总体方案要求，结合地（县）级调度中心监控系统的安全分区和安全区域边界条件，确定地（县）级调度中心监控系统安全防护的总体逻辑结构如图 3。

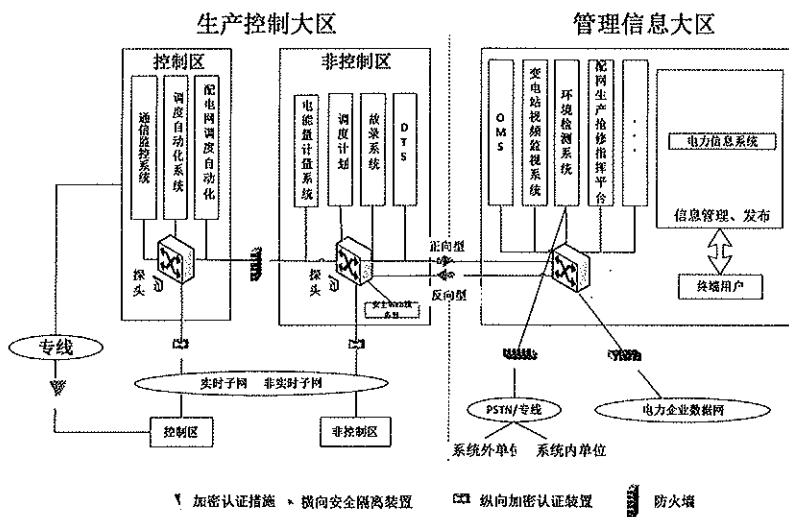


图 3 传统地（县）级调度中心调度自动化系统安全防护总体部署示意图

新建调度控制系统安全防护总体逻辑结构如下图所示。

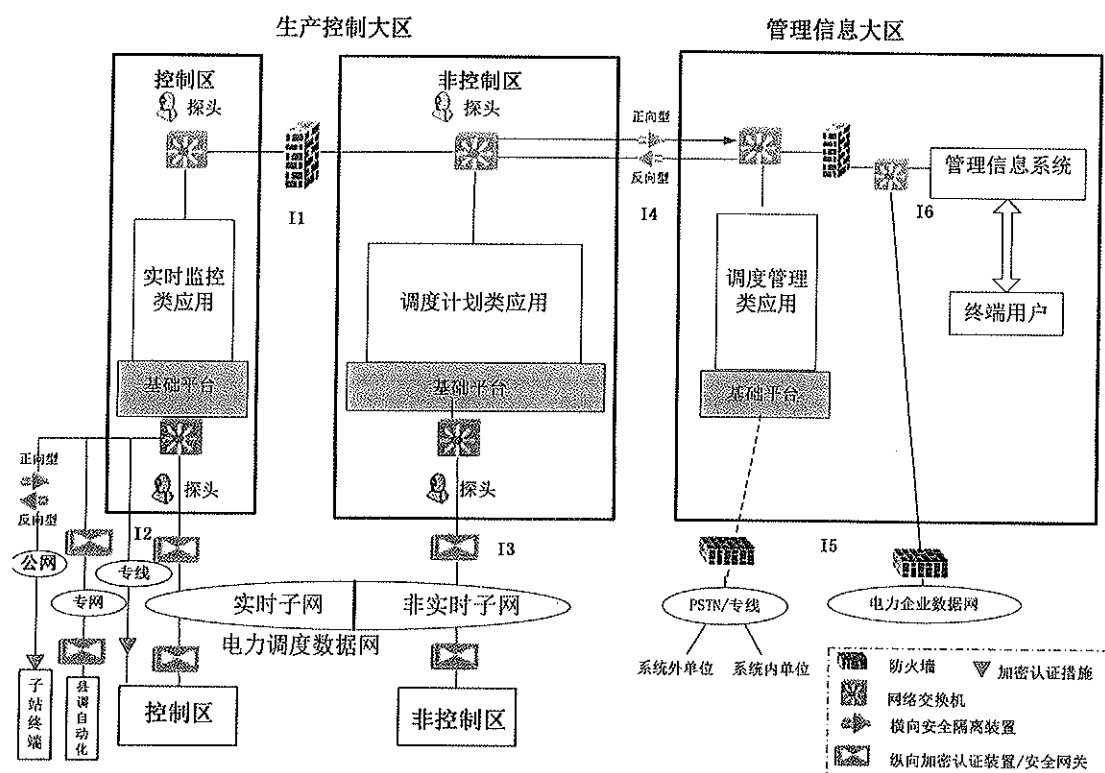


图4 新一代地（县）级调度中心调度控制系统安全防护总体部署示意图

安全部署示意图中所指的逻辑接口（I1-I6）的描述见表

3。

表 3 电网调度自动化系统的逻辑接口

| 接口 | 名称              | 数据类型                                                                  | 通信方式及协议           |
|----|-----------------|-----------------------------------------------------------------------|-------------------|
| I1 | 控制区与非控制区横向边界    | 数据类型不定。                                                               | 本地局域网<br>TCP/IP   |
| I2 | 控制区纵向边界         | 1. 遥信、遥测及计算数据；<br>2. 电网模型数据等                                          | 电力调度数据网<br>TCP/IP |
| I3 | 非控制区纵向边界        | 1. 负荷需求数据<br>2. 发电计划数据<br>3. 联络线数据<br>4. DTS 相关数据<br>5. 市场交易安全校核等相关数据 | 电力调度数据网<br>TCP/IP |
| I4 | 生产大区与管理信息大区横向边界 | 电网模型、图形、历史数据、准实时数据                                                    | 本地局域网<br>TCP/IP   |

|    |                   |                    |                           |
|----|-------------------|--------------------|---------------------------|
| I5 | 管理信息大区纵向边界        | 卫星气象云图、气象实况、水文信息等  | 电力企业数据网、PSTN/专线<br>TCP/IP |
| I6 | 调度生产管理系统与管理信息系统边界 | 生产管理 PMS 数据、办公自动化等 | 本地局域网<br>TCP/IP           |

调度中心的安全区域之间可以采用链式、三角或星形结构，此处仅以链式结构示意图。

我国不同地区的地、县级调度中心在规模和业务系统的配置上具有很大的差别，在安全工程具体实施时可以根据应用系统实际情况，确定安全实施方案，并报上级调度中心审核。采用地（县）调一体化模式部署的系统，推荐采用纵向连接的通信方式，并应采用纵向加密认证装置进行防护。不推荐使用局域网延伸的通信方式，已采用此方式的应及时进行技术改造，同时在过渡期内应通过安全审计等方式加强管理，并采用必要的安全加密措施。

生产控制大区中各业务功能根据电力行业等级保护要求，在物理、安全设备、操作系统、数据、应用等方面进行全面防护。

具有远方遥控功能的业务（如 AGC、AVC、继电保护定值远方修改）应采用加密、身份认证等技术措施进行安全防护。

地级调度中心应当部署内网安全监视应用，实现对监控系统中运行的安全设备实时监视和纵向加密认证装置统一

远程管理功能；应当部署支持符合国家要求的算法、具备签发安全标签功能的电力调度证书系统，形成地级调度中心独立的数字证书认证体系。地级调度中心应当具备关键应用功能备用和关键数据备份功能。

县级及以上调度中心应当具有病毒防护措施，地区和大型新建 SCADA、AVC 和新一代调度控制系统等具有控制功能的业务系统应当满足利用电力调度数字证书进行加密认证的要求。

## **5 主要业务功能安全防护方案**

本章仅对地（县）级调度中心的主要业务系统的安全防护进行描述，不再重复《电力监控系统安全防护总体方案》已规定的公共防护措施部分。新一代电网调度控制系统中各安全区的防护参照图 4 地（县）级以上调度中心安全部署中描述的方案进行安全防护。传统电网调度自动化系统的安全防护方案如以下所述。

### **5.1 调度自动化系统安全防护**

调度自动化系统实现对实时运行的电力系统进行数据采集、监视、控制和安全分析功能，是地、县级调度中心最重要的系统；系统主体位于控制区，WEB 浏览功能模块置于管理信息大区。

根据调度自动化系统的特点和电力监控系统安全防护

总体方案的要求，其物理边界及安全部署如图 5。

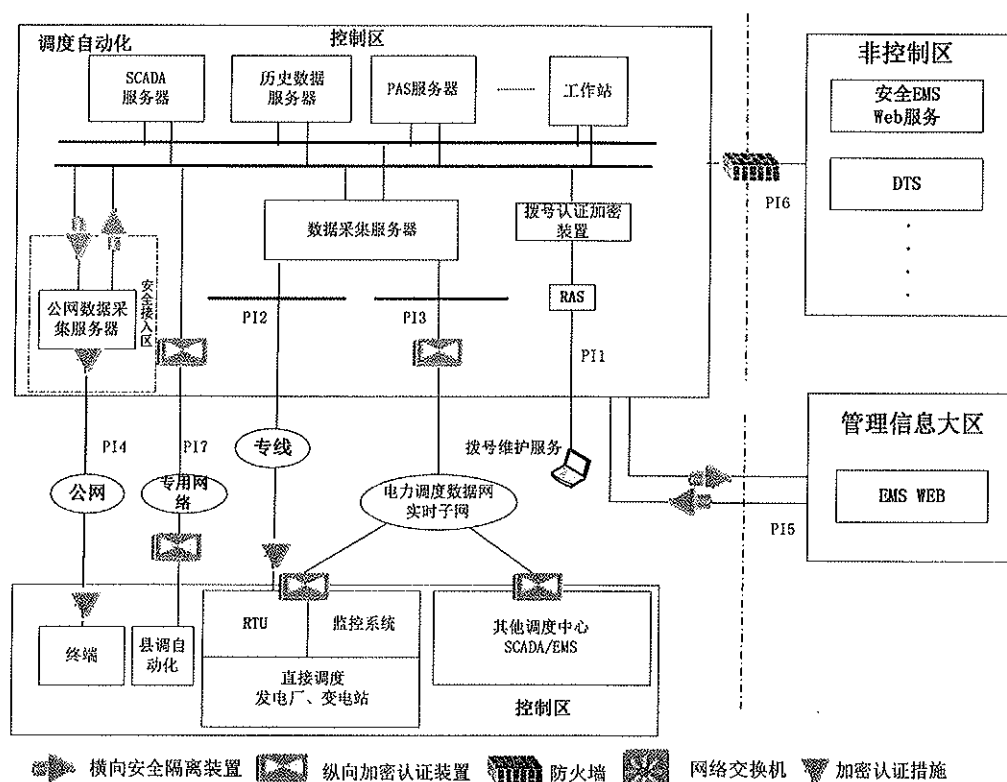


图 5 调度自动化系统的物理边界及安全部署示意图

调度自动化系统的物理边界为：拨号网络边界（PI1）、传统专用远动通道（PI2）、纵向网络边界（PI3，PI7）、公网通信边界（PI4）、横向网络边界（PI5、PI6）。这七个边界的安全防护措施按照总体方案实施。并要求新建调度自动化系统的控制功能模块应当支持认证加密机制，对已有系统应当逐步进行改造。

## 5.2 电能量计量功能的安全防护

电能量计量功能通过电能量终端装置采集电能量数据，作为计量和结算的依据，原始数据禁止修改。该系统属于非控制区。

根据电能量计量功能的特点和电力监控系统安全防护总体方案的要求，物理边界及安全部署如图 6。

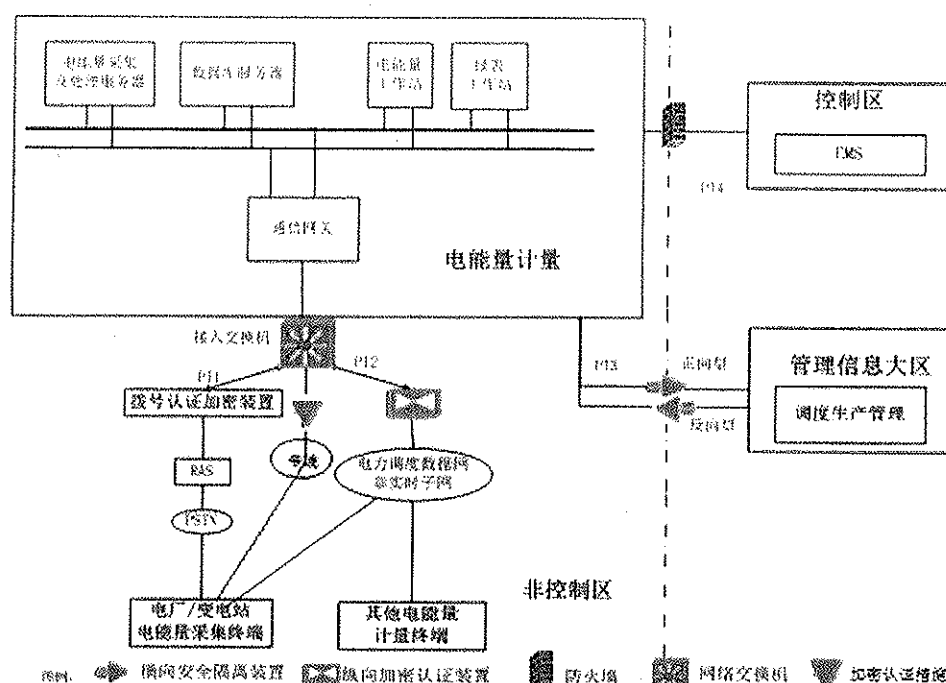


图 6 电能量计量功能的物理边界及安全部署示意图

电能量计量功能的物理边界为：拨号网络边界（PI1）、纵向网络边界（PI2）和横向网络边界（PI3，PI4）。这四个边界的安全防护措施按照总体方案实施。

地级调度中心的电能量计量功能主体应当位于非控制区，当下级厂站端或调度机构只有控制区时，计量数据需通过控制区传输。

推荐采用网络方式采集电能量数据，也可以采用以下两种拨号通信方式：

单向拨号方式。从主站端向厂站端单向拨号，避免拨号转移。厂站端的电能量采集装置与当地的其它系统需有效隔

离。

拨号服务器方式。该方式要求通过拨号服务器（RAS）接入非控制区的接入交换机，在 RAS 和接入交换机之间部署拨号认证加密装置，拨号访问应当使用电力调度数字证书。

若无条件实现上述安全防护时，则禁止开通拨号访问。

### 5.3 调度生产管理功能的安全防护

调度生产管理功能主要包括调度生产数据服务、调度报表管理、调度检修管理等多种业务，系统主体位于管理信息大区。

调度生产管理功能使用电力企业数据网的生产 VPN 进行广域网通信，并采用硬件防火墙实现安全隔离。

地级调度中心调度生产管理功能应当在管理信息大区部署网关机，承载生产控制大区与管理信息大区的数据交互及与上级调度生产管理功能通信功能。

调度生产管理功能与生产控制大区之间的数据通信必须采用专用横向单向安全隔离装置实现强隔离。通过正向型电力专用横向单向隔离装置从生产控制大区向管理信息大区传输实时数据和交易信息等。通过反向型电力专用横向单向隔离装置从管理信息大区向生产控制大区传输计划数据和气象信息等。调度生产管理功能的安全防护部署如图 7。

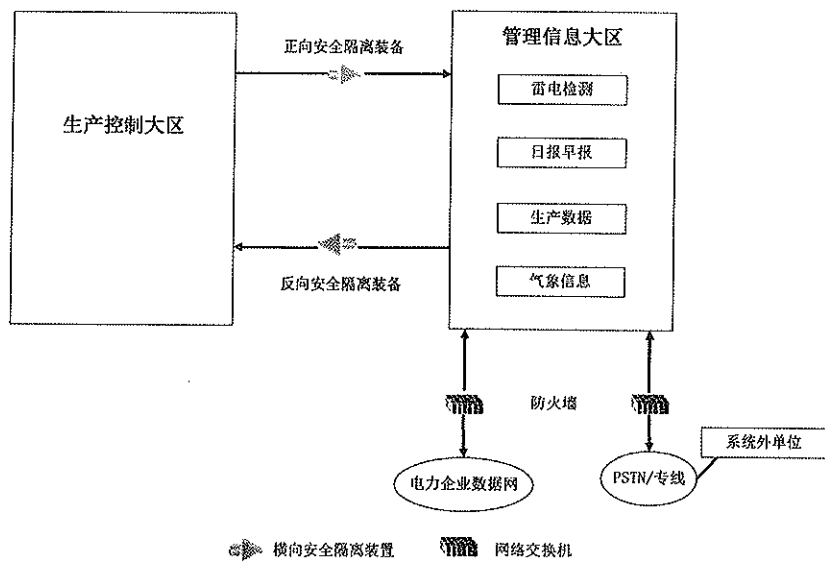


图 7 调度生产管理功能安全部署示意图

## 附录主要术语中英文对照

DTS(Dispatcher Training Simulator): 调度员培训仿真系统  
PSTN (Public Switched Telephone Network): 公用交换电话网  
RAS (Remote Access Server): 远程访问服务器  
RTU (Remote Terminal Unit): 远方终端装置  
SCADA/EMS (Supervisory Control And Data Acquisition/Energy Management System): 监控和数据采集/能量管理系统  
TCP/IP (Transaction Control Protocol/Internet Protocol): 互联网传输协议  
VPN (Virtual Private Networks): 虚拟专用网  
AGC (Automatic Generation Control): 自动发电控制  
AVC (Automatic Voltage Control): 自动电压控制