国家能源局文件

国能安全〔2015〕36号

国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知

各派出机构，各有关电力企业：

为了加强电力监控系统安全防护工作，根据《电力监控系统安全防护规定》（国家发展和改革委员会令2014年第14号），国家能源局制定了《电力监控系统安全防护总体方案》等安全防护方案和评估规范。现印发你们，请依照执行。

附件：1. 电力监控系统安全防护总体方案

2. 省级以上调度中心监控系统安全防护方案

3. 地（县）级调度中心监控系统安全防护方案

4. 发电厂监控系统安全防护方案

5. 变电站监控系统安全防护方案

6. 配电监控系统安全防护方案

7. 电力监控系统安全防护评估规范

国家能源局

2015年2月4日

抄送：中央网信办，国家发展改革委

附件 1:

电力监控系统安全防护总体方案

1 总则

1.1 为了保障电力监控系统的安全，防范黑客及恶意代码等对电力监控系统的攻击及侵害，特别是抵御集团式攻击，防止电力监控系统的崩溃或瘫痪，以及由此造成的电力设备事故或电力安全事故（事件），依据《电力监控系统安全防护规定》、《信息安全等级保护管理办法》及国家有关规定，制定本方案。

1.2 本方案确定了电力监控系统安全防护体系的总体框架，细化了电力监控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、配电等的电力监控系统安全防护方案及电力监控系统安全防护评估规范。

1.3 电力监控系统安全防护的总体原则为“安全分区、网络专用、横向隔离、纵向认证”。安全防护主要针对电力监控系统，即用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备，以及作为基础支撑的通信及数据网络等。重点强化边界防护，同时加强内部的物理、网络、主机、应用和数据安全，加强安全管理制度、机构、人员、系统建设、系统运维的管理，提高系统整体安

全防护能力，保证电力监控系统及重要数据的安全。

1.4　电力监控系统安全防护是复杂的系统工程，其总体安全防护水平取决于系统中最薄弱点的安全水平。电力监控系统安全防护过程是长期的动态过程，各单位应当严格落实安全防护的总体原则，建立和完善以安全防护总体原则为中心的安全监测、响应处理、安全措施、审计评估等环节组成的闭环机制。

1.5　本方案适用于电力监控系统的规划设计、项目审查、工程实施、系统改造、运行管理等。

2　安全防护方案

根据《电力监控系统安全防护规定》的要求，电力监控系统安全防护总体方案的框架结构如图 1 所示。

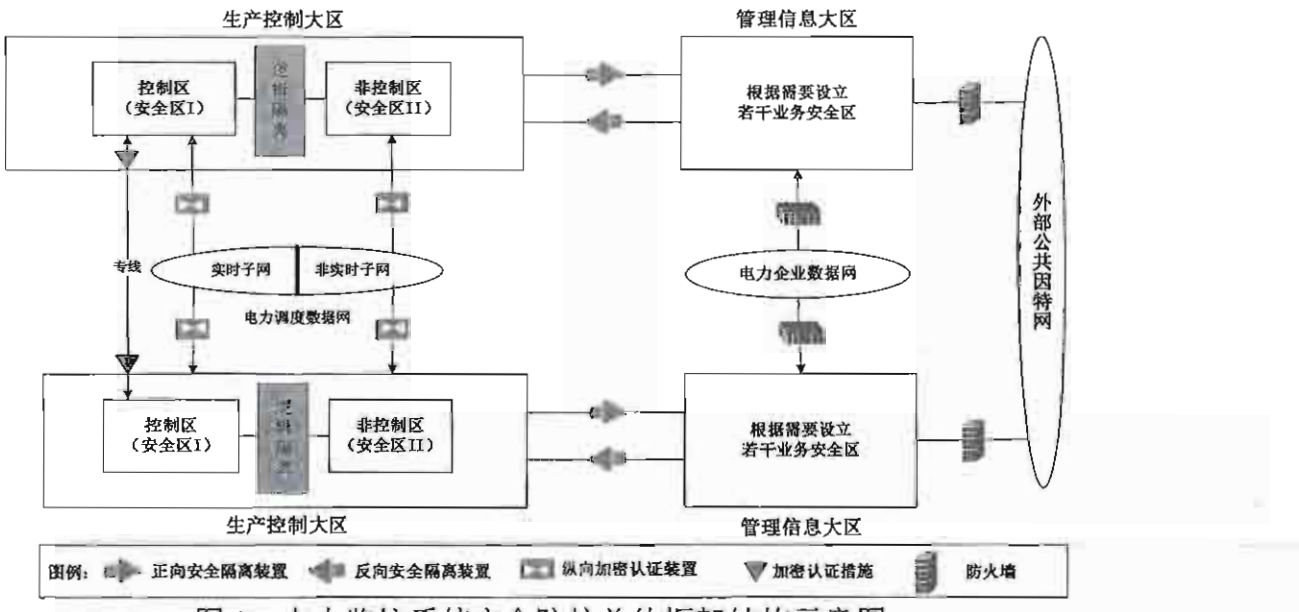

图 1　电力监控系统安全防护总体框架结构示意图

2.1 安全分区

安全分区是电力监控系统安全防护体系的结构基础。发

电企业、电网企业内部基于计算机和网络技术的业务系统，原则上划分为产控制大区和管理信息大区。生产控制大区可以分为控制区（又称安全区Ⅰ）和非控制区（又称安全区Ⅱ）。

在满足安全防护总体原则的前提下，可以根据业务系统实际情况，简化安全区的设置，但是应当避免形成不同安全区的纵向交叉联接。

2.1.1 生产控制大区的安全区划分

（1）控制区（安全区Ⅰ）：

控制区中的业务系统或其功能模块（或子系统）的典型特征为：是电力生产的重要环节，直接实现对电力一次系统的实时监控，纵向使用电力调度数据网络或专用通道，是安全防护的重点与核心。

控制区的传统典型业务系统包括电力数据采集和监控系统、能量管理系统、广域相量测量系统、配网自动化系统、变电站自动化系统、发电厂自动监控系统等，其主要使用者为调度员和运行操作人员，数据传输实时性为毫秒级或秒级，其数据通信使用电力调度数据网的实时子网或专用通道进行传输。该区内还包括有采用专用通道的控制系统，如：继电保护、安全自动控制系统、低频（或低压）自动减负荷系统、负荷控制管理系统等，这类系统对数据传输的实时性要求为毫秒级或秒级，其中负荷控制管理系统为分钟级。

（2）非控制区（安全区II）：

非控制区中的业务系统或其功能模块的典型特征为：是电力生产的必要环节，在线运行但不具备控制功能，使用电力调度数据网络，与控制区中的业务系统或其功能模块联系紧密。

非控制区的传统典型业务系统包括调度员培训模拟系统、水库调度自动化系统、故障录波信息管理系统、电能量计量系统、实时和次日电力市场运营系统等，其主要使用者分别为电力调度员、水电调度员、继电保护人员及电力市场交易员等。在厂站端还包括电能量远方终端、故障录波装置及发电厂的报价系统等。非控制区的数据采集频度是分钟级或小时级，其数据通信使用电力调度数据网的非实时子网。此外，如果生产控制大区内个别业务系统或其功能模块（或子系统）需使用公用通信网络、无线通信网络以及处于非可控状态下的网络设备与终端等进行通信，其安全防护水平低于生产控制大区内其他系统时，应设立安全接入区，典型的业务系统或功能模块包括配电网自动化系统的前置采集模块（终端）、负荷控制管理系统、某些分布式电源控制系统等，安全接入区的典型安全防护框架结构如图2所示。

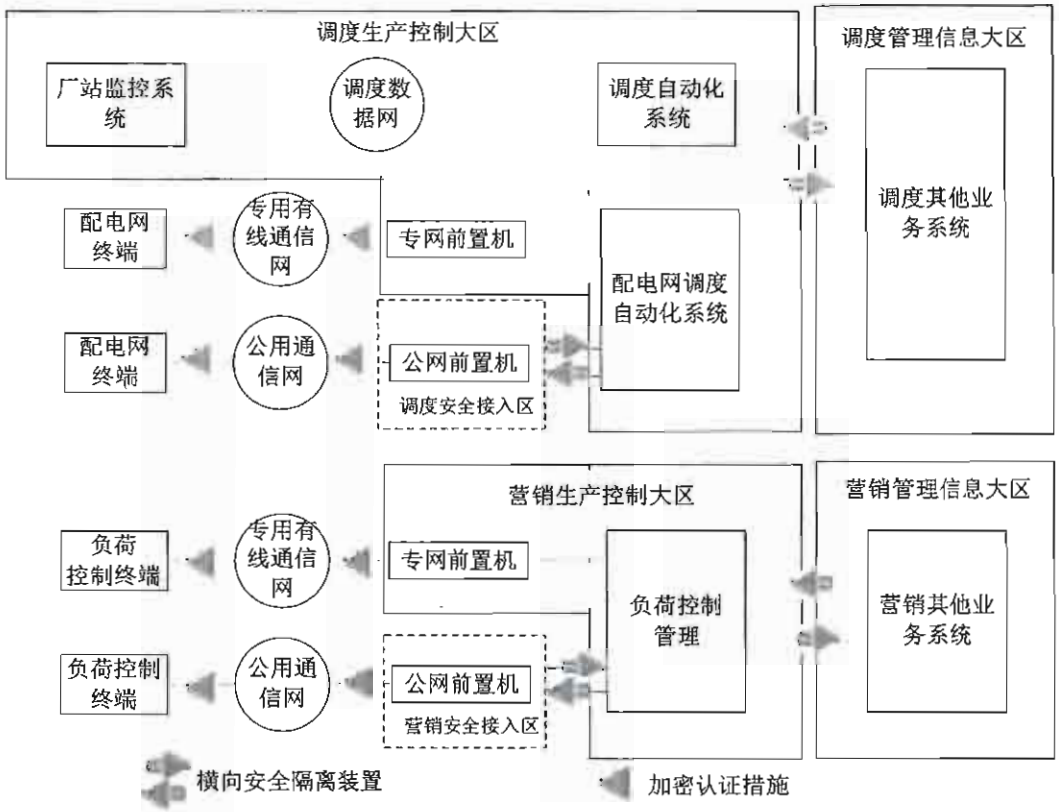

图 2　安全接入区的典型安全防护框架结构示意图

2.1.2　管理信息大区的安全区划分

管理信息大区是指生产控制大区以外的电力企业管理业务系统的集合。管理信息大区的传统典型业务系统包括调度生产管理系统、行政电话网管系统、电力企业数据网等。电力企业可以根据具体情况划分安全区，但不应影响生产控制大区的安全。

2.1.3　业务系统分置于安全区的原则

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、各业务系统间的相互关系、广域网通信方式以及对电力系统的影响程度等，按以下规则将业务系统

或其功能模块置于相应的安全区：

（1）实时控制系统、有实时控制功能的业务模块以及未来有实时控制功能的业务系统应当置于控制区。

（2）应当尽可能将业务系统完整置于一个安全区内。当业务系统的某些功能模块与此业务系统不属于同一个安全分区内时，可以将其功能模块分置于相应的安全区中，经过安全区之间的安全隔离设施进行通信。

（3）不允许把应当属于高安全等级区域的业务系统或其功能模块迁移到低安全等级区域；但允许把属于低安全等级区域的业务系统或其功能模块放置于高安全等级区域。

（4）对不存在外部网络联系的孤立业务系统，其安全分区无特殊要求，但需遵守所在安全区的防护要求。

（5）对小型县调、配调、小型电厂和变电站的电力监控系统可以根据具体情况不设非控制区，重点防护控制区。

（6）对于新一代电网调度控制系统，其实时监控与预警功能模块应当置于控制区，调度计划和安全校核功能模块应当置于非控制区，调度管理功能模块应当置于管理信息大区。

2.1.4 信息安全等级保护划分

根据不同安全区域的安全防护要求，确定其安全等级和防护水平。生产控制大区的安全等级高于管理信息大区，系统

定级按《电力行业信息系统安全等级保护定级工作指导意见》进行定级，具体等级标准见表1。

表 1　电力监控系统安全保护等级标准

类别	定级对象	系统级别	
		省级以上	地级及以下
电力监控系统	能量管理系统（具有 SCADA、AGC、AVC 等控制功能）	4	3
	变电站自动化系统（含开关站、换流站、集控站）	220 千伏及以上变电站为 3 级，以下为 2 级	
	火电厂监控（含燃气电厂）系统 DCS（含辅机控制系统）	单机容量 300MW 及以上为 3 级，以下为 2 级	
	水电厂监控系统	总装机 1000MW 及以上为 3 级，以下为 2 级	
	水电厂梯级调度监控系统	3	
	核电站监控系统 DCS（含辅机控制系统）	3	
	风电场监控系统	风电场总装机容量 200MW 及以上为 3 级，以下为 2 级	
	光伏电站监控系统	光伏电站总装机容量 200MW 及以上为 3 级，以下为 2 级	
	电能量计量系统	3	2
	广域相量测量系统（WAMS）	3	无
	电网动态预警系统	3	无
	调度交易计划系统	3	无
	水调自动化系统	2	
	调度管理系统	2	
	雷电监测系统	2	
	电力调度数据网络	3	2
	通信设备网管系统	3	2
	通信资源管理系统	3	2
	综合数据通信网络	2	
	故障录波信息管理系统	3	
	配电监控系统	3	
	负荷控制管理系统	3	
	新一代电网调度控制系统的实时监控与预警功能模块	4	3
	新一代电网调度控制系统的调度计划功能模块	3	2
	新一代电网调度控制系统的安全校核功能模块	3	2
	新一代电网调度控制系统的调度管理功能模块	2	

2.1.5　生产控制大区内部安全防护要求

（1）禁止生产控制大区内部的 E-Mail 服务，禁止控制区

内通用的 WEB 服务。

（2）允许非控制区内部业务系统采用 B/S 结构，但仅限于业务系统内部使用。允许提供纵向安全 WEB 服务，但应当优先采用专用协议和专用浏览器的图形浏览技术，也可以采用经过安全加固且支持 HTTPS 的安全 WEB 服务。

（3）生产控制大区重要业务（如 SCADA/AGC/AVC、实时电力市场交易等）的远程通信应当采用加密认证机制。

（4）生产控制大区内的业务系统间应该采取 VLAN 和访问控制等安全措施，限制系统间的直接互通。

（5）生产控制大区的拨号访问服务，服务器和用户端均应当使用经国家指定部门认证的安全加固的操作系统，并采取加密、认证和访问控制等安全防护措施。

（6）生产控制大区边界上可以采用入侵检测措施。

（7）生产控制大区应当采取安全审计措施，把安全审计与安全区网络管理系统、综合告警系统、IDS 管理系统、敏感业务服务器登录认证和授权、关键业务应用访问权限相结合。

（8）生产控制大区内主站端和重要的厂站端应该统一部署恶意代码防护系统，采取防范恶意代码措施。病毒库、木马库以及 IDS 规则库应经过安全检测并应离线进行更新。

2.1.6 管理信息大区安全要求

应当统一部署防火墙、IDS、恶意代码防护系统及桌面终端控制系统等通用安全防护设施。

2.1.7 安全区拓扑结构

电力监控系统安全区连接的拓扑结构有链式、三角和星形结构三种。链式结构中的控制区具有较高的累积安全强度，但总体层次较多；三角结构各区可以直接相连，效率较高，但所用隔离设备较多；星形结构所用设备较少、易于实施，但中心点故障影响范围大。三种模式均能满足电力监控系统安全防护体系的要求，可以根据具体情况选用，见图 3。

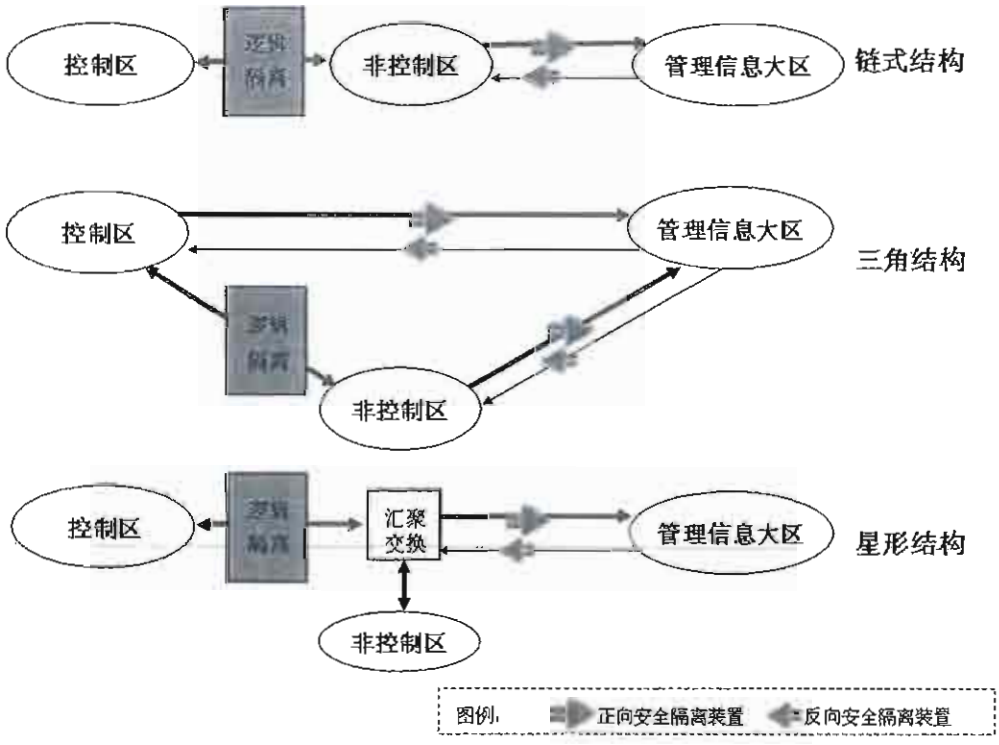

图 3 电力监控系统安全区连接拓扑结构

2.1.8 监管信息接入要求

按照国家有关规定，在满足电力监控系统安全防护要求的前提下，将相关信息接入电力监管信息系统。

2.2 网络专用

电力调度数据网是为生产控制大区服务的专用数据网络，承载电力实时控制、在线生产交易等业务。安全区的外部边界网络之间的安全防护隔离强度应该和所连接的安全区之间的安全防护隔离强度相匹配。

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，采用基于SDH/PDH不同通道、不同光波长、不同纤芯等方式，在物理层面上实现与电力企业其它数据网及外部公共信息网的安全隔离。当采用 EPON、GPON 或光以太网络等技术时应当使用独立纤芯或波长。

电力调度数据网划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。可以采用 MPLS-VPN 技术、安全隧道技术、PVC技术、静态路由等构造子网。

电力调度数据网应当采用以下安全防护措施:

（1）网络路由防护

按照电力调度管理体系及数据网络技术规范，采用虚拟专网技术，将电力调度数据网分割为逻辑上相对独立的实时子网和非实时子网，分别对应控制业务和非控制生产业务，保证实时业务的封闭性和高等级的网络服务质量。

（2）网络边界防护

应当采用严格的接入控制措施，保证业务系统接入的可信性。经过授权的节点允许接入电力调度数据网，进行广域网通信。

数据网络与业务系统边界采用必要的访问控制措施，对通信方式与通信业务类型进行控制；在生产控制大区与电力调度数据网的纵向交接处应当采取相应的安全隔离、加密、认证等防护措施。对于实时控制等重要业务，应该通过纵向加密认证装置或加密认证网关接入调度数据网。

（3）网络设备的安全配置

网络设备的安全配置包括关闭或限定网络服务、避免使用默认路由、关闭网络边界 OSPF 路由功能、采用安全增强的 SNMPv2 及以上版本的网管协议、设置受信任的网络地址范围、记录设备日志、设置高强度的密码、开启访问控制列表、封闭空闲的网络端口等。

（4）数据网络安全的分层分区设置

电力调度数据网采用安全分层分区设置的原则。调度数据网由骨干网和接入网组成。地级以上调度中心节点构成调度数据网骨干网（简称骨干网）。各级调度的业务节点及直调厂站节点构成分层接入网，各厂站按照调度关系接入两层接入网。

调度数据网未覆盖到的电力监控系统（如配电网自动

化、负荷控制管理、分布式能源接入等）的数据通信优先采用电力专用通信网络，不具备条件的也以可采用公用通信网络（不包括因特网）、无线网络（GPRS、CDMA、230MHz、WLAN等）等通信方式，使用上述通信方式时应当设立安全接入区，并采用安全隔离、访问控制、认证及加密等安全措施。

各层面的数据网络之间应该通过路由限制措施进行安全隔离。当县调或配调内部采用公用通信网时，禁止与调度数据网互联，保证网络故障和安全事件限制在局部区域之内。

企业内部管理信息大区纵向互联采用电力企业数据网或互联网，电力企业数据网为电力企业内联网。

2.3 横向隔离

2.3.1 横向隔离是电力二次安全防护体系的横向防线。采用不同强度的安全设备隔离各安全区，在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。电力专用横向单向安全隔离装置作为生产控制大区与管理信息大区之间的必备边界防护措施，是横向防护的关键设备。生产控制大区内部的安全区之间应当采用具有访问控制功能的网络设备、防火墙或者相当功能的设施，实现逻辑隔离。安全接入区与生产控制大区相连时，应当采用电力专用横向单向安全隔离装置进行集中互联。

2.3.2 按照数据通信方向电力专用横向单向安全隔离装置分为正向型和反向型。正向安全隔离装置用于生产控制大区到管理信息大区的非网络方式的单向数据传输。反向安全隔离装置用于从管理信息大区到生产控制大区的非网络方式的单向数据传输，是管理信息大区到生产控制大区的唯一数据传输途径。反向安全隔离装置集中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、内容过滤、有效性检查等处理后，转发给生产控制大区内部的接收程序。专用横向单向隔离装置应该满足实时性、可靠性和传输流量等方面的要求。

2.3.3 严格禁止 E-Mail、WEB、Telnet、Rlogin、FTP 等安全风险高的通用网络服务和以 B/S 或 C/S 方式的数据库访问穿越专用横向单向安全隔离装置，仅允许纯数据的单向安全传输。

控制区与非控制区之间应当采用具有访问控制功能的设备或相当功能的设施进行逻辑隔离。

2.4 纵向认证

2.4.1 纵向加密认证是电力监控系统安全防护体系的纵向防线。采用认证、加密、访问控制等技术措施实现数据的远方安全传输以及纵向边界的安全防护。对于重点防护的调度中心、发电厂、变电站在生产控制大区与广域网的纵向连接处应当设置经过国家指定部门检测认证的电力专用纵向加

密认证装置或者加密认证网关及相应设施，实现双向身份认证、数据加密和访问控制。安全接入区内纵向通信应当采用基于非对称密钥技术的单向认证等安全措施，重要业务可以采用双向认证。

2.4.2 纵向加密认证装置及加密认证网关用于生产控制大区的广域网边界防护。纵向加密认证装置为广域网通信提供认证与加密功能，实现数据传输的机密性、完整性保护，同时具有安全过滤功能。加密认证网关除具有加密认证装置的全部功能外，还应实现对电力系统数据通信应用层协议及报文的处理功能。

2.4.3 对处于外部网络边界的其他通信网关，应当进行操作系统的安全加固，对于新上的系统应当支持加密认证的功能。

2.4.4 调度中心和重要厂站两侧均应当配置纵向加密认证装置或纵向加密认证网关；小型厂站侧至少应当实现单向认证、数据加密和安全过滤功能。

2.4.5 传统的基于专用通道的数据通信可以逐步采用加密、身份认证等技术进行安全防护。

2.4.6 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。

2.5 电力调度数字证书系统

2.5.1　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，主要用于生产控制大区，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可靠的行为审计。

2.5.2　电力调度数字证书应当经过国家有关检测机构检测认证，符合国家相关安全要求，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、安全专用设备、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。

2.5.3　电力调度数字证书系统的建设运行应当符合如下要求：

（1）统一规划数字证书的信任体系，各级电力调度数字证书系统用于颁发本调度中心及调度对象相关人员、程序和设备证书。上下级电力调度数字证书系统通过信任链构成认证体系；

（2）采用统一的数字证书格式，采用满足国家有关要求的加密算法；

（3）提供规范的应用接口，支持相关应用系统和安全专用设备嵌入电力调度数字证书服务；

（4）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。

2.5.4 电力调度数字证书系统按照电力调度管理体系进行配置，省级以上调度中心和有实际业务需要的地区调度中心应该建立电力调度数字证书系统。

2.5.5 应当利用数字证书技术提高系统安全强度，新建设的电力监控系统应当支持电力调度数字证书的应用，现有应用系统的外部通信接口部分应当逐步进行相应的改造。

2.5.6 安全标签是具有数字签名的权限授权标记。安全标签应当纳入电力调度数字证书系统管理。新建设的电力监控系统，应当采用调度数字证书和安全标签实现安全授权的强制访问控制及强制执行控制。

3 通用安全防护措施

3.1 物理安全

电力监控系统机房所处建筑应当采取有效防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施，应当配置电子门禁系统以加强物理访问控制，必要时应当安排专人值守，应当对关键区域实施电磁屏蔽。

3.2 备用与容灾

电力企业应当定期对关键业务的数据与系统进行备份，建立历史归档数据的异地存放制度。关键主机设备、网络设备或关键部件应当进行相应的冗余配置。控制区的业务应当

采用热备用方式。重要调度中心应当逐步实现实时数据、电力监控系统、实时调度业务三个层面的备用，形成分布式备用调度体系。

3.3 恶意代码防范

应当及时更新经测试验证过的特征码，查看查杀记录。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。

3.4 逻辑隔离

控制区与非控制区之间应采用逻辑隔离措施，实现两个区域的逻辑隔离、报文过滤、访问控制等功能，其访问控制规则应当正确有效。生产控制大区应当选用安全可靠硬件防火墙，其功能、性能、电磁兼容性必须经过国家相关部门的检测认证。

3.5 入侵检测

生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，及时捕获网络异常行为、分析潜在威胁、进行安全审计。

3.6 主机加固

生产控制大区主机操作系统应当进行安全加固。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力、以及配置安全的应用程序。关键控制系统软件升级、补丁安装前要请专业技术机构进行安全评估和验

证。

3.7 安全 Web 服务

非控制区的接入交换机应当支持 HTTPS 的纵向安全 WEB 服务，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。

3.8 计算机系统访问控制

能量管理系统、厂站端生产控制系统、电能量计量系统及电力市场运营系统等业务系统，应当逐步采用电力调度数字证书，对用户登录本地操作系统、访问系统资源等操作进行身份认证，根据身份与权限进行访问控制，并且对操作行为进行安全审计。

3.9 远程拨号访问

需通过远程拨号访问生产控制大区的，要求远方用户使用安全加固的操作系统平台，结合数字证书技术，进行登录认证和访问认证。

对于通过拨号服务器(RAS)访问本地网络与系统的远程拨号访问的方式，应当采用网络层保护,应用 VPN 技术建立加密通道。对于以远方终端直接拨号访问的方式，应当采用链路层保护，使用专用的链路加密设备。

对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。

3.10 线路加密措施

对远方终端装置（RTU）、继电保护装置、安全自动装置、负荷控制管理系统等基于专线通道与调度主站进行的数据通信，应采用必要的身份认证或加解密措施进行防护。

3.11 安全审计

生产控制大区应当具备安全审计功能，可以对网络运行日志、操作系统运行日志、数据库重要操作日志、业务应用系统运行日志、安全设施运行日志等进行集中收集、自动分析，及时发现各种违规行为以及病毒和黑客的攻击行为。

3.12 安全免疫

生产控制大区具备控制功能的系统应当逐步推广应用以密码硬件为核心的可信计算技术，用于实现计算环境和网络环境安全可信，免疫未知恶意代码破坏，应对高级别的恶意攻击。

3.13 内网安全监视

生产控制大区应当逐步推广内网安全监视功能，实时监测电力监控系统的计算机、网络及安全设备运行状态，及时发现非法外联、外部入侵等安全事件并告警。

3.14 商用密码管理

电力监控系统中商用密码产品的配备、使用和管理等，应当严格执行国家商用密码管理的有关规定。

4 安全管理

4.1 安全分级负责制

国家能源局及其派出机构负责电力监控系统安全防护的监管，组织制定电力监控系统安全防护技术规范并监督实施。国家能源局信息中心负责承担电力监控系统安全防护监管的技术支持。电力企业应当按照“谁主管谁负责，谁运营谁负责”的原则，建立电力监控系统安全管理制度，将电力监控系统安全防护及其信息报送纳入日常安全生产管理体系，各电力企业负责所辖范围内电力监控系统的安全管理。各相关单位应当设置电力生产监控系统的安全防护小组或专职人员。

4.2 相关人员的安全职责

电力企业应当明确电力监控系统安全防护管理部门，由主管安全生产的领导作为电力监控系统安全防护的主要责任人，并指定专人负责管理本单位所辖电力监控系统的公共安全设施，明确各业务系统专责人的安全管理责任。

电力调度机构应当指定专人负责管理本级调度数字证书系统。

4.3 工程实施的安全管理

电力监控系统相关设备及系统应当采用安全可靠的软硬件产品，开发单位、供应商应以合同条款或协议的方式保证所提供的设备及系统符合《电力监控系统安全防护规定》和本方案以及国家与行业信息系统安全等级保护的要求，并在设备及系统全生命周期内对其负责。

电力监控系统专用安全产品的开发单位、使用单位及供应商，应当按国家有关要求做好保密工作，禁止安全防护关键技术和设备的扩散。

应当加强重要电力监控系统及关键设备全生命周期的安全管理，系统上线前应当由具有测评资质的机构开展系统漏洞分析及控制功能源代码安全检测。

电力企业各单位的电力监控系统安全防护实施方案必须严格遵守《电力监控系统安全防护规定》以及本方案的有关规定，并经过本企业上级专业主管部门、信息安全主管部门以及相应电力调度机构的审核，方案实施完成后应当由上述机构验收。

4.4 设备和应用系统的接入管理

接入电力调度数据网络的节点、设备和应用系统，其接入技术方案和安全防护措施必须经直接负责的电力调度机构同意。

生产控制大区的各业务系统禁止以各种方式与互联网连接；限制开通拨号功能；关闭或拆除主机上不必要的软盘驱动、光盘驱动、USB 接口、串行口、无线、蓝牙等，严格控制在生产控制大区和管理信息大区之间交叉使用移动存储介质以及便携式计算机。确需保留的必须通过安全管理及技术措施实施严格监控。

接入电力监控系统生产控制大区中的安全产品，应当获

得国家指定机构安全检测证明，用于厂站的设备还需有电力系统电磁兼容检测证明。

4.5 设备选型及漏洞整改

电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞和风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统及设备的运行管理和安全防护。生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备。

4.6 日常安全管理

电力企业应当建立电力监控系统安全管理制度，主要包括：门禁管理、人员管理、权限管理、访问控制管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等管理制度。

应当对关键安全设备、服务器的日志进行统一管理，及时发现安全管理体系中存在的安全隐患和异常访问行为。

应当特别加强内部人员的保密教育、录用离岗等的管理。包括对录用人员身份背景、专业资格和资质进行严格审查，关键岗位录用人员、接触内部敏感信息第三方人员应当签署保密协议；应当严格关键岗位人员离岗管理，取回各种

身份证件、钥匙、徽章等以及机构提供的软硬件设备，承诺调离后保密义务后方可离开。

4.7 联合防护和应急处理

建立健全电力监控系统安全的联合防护和应急机制。由国家能源局及其派出机构负责对电力监控系统安全防护的监管，电力调度机构负责统一指挥调度范围内的电力监控系统安全应急处理。各电力企业的电力监控系统必须制定应急处理预案并经过预演或模拟验证。

当电力生产控制大区出现安全事件，尤其是遭到黑客、恶意代码攻击和其他人为破坏时，应当立即向其上级电力调度机构以及当地国家能源局派出机构报告，同时按应急处理预案采取安全应急措施。相应电力调度机构应当立即组织采取紧急联合防护措施，以防止事件扩大。同时注意保护现场，以便进行调查取证和分析。事件发生单位及相应调度机构应当及时将事件情况向相关能源监管部门和信息安全主管部门报告。

5 安全防护评估

5.1 应当依据本方案的要求对电力监控系统的总体安全防护水平进行安全评估。安全防护评估贯穿于电力监控系统的规划、设计、实施、运维和废弃阶段。

5.2 应当建立健全电力监控系统安全防护评估制度，采取以自评估为主、检查评估为辅的方式，将安全防护评估纳入

电力系统安全评价体系。应当掌握基本的自评估技术和方法，配备必要的评估工具。

5.3 电力监控系统在上线投运之前、升级改造之后必须进行安全评估；已投入运行的系统应该定期进行安全评估，对于电力生产监控系统应该每年进行一次安全评估。评估方案及结果应当及时向上级主管部门汇报、备案。

5.4 参与评估的机构及人员必须稳定、可靠、可控，并与被评估单位签署长期保密协议。对生产控制大区安全评估的所有记录、数据、结果等均不得以任何形式携带出被评估单位，按国家有关要求做好保密工作。

5.5 电力监控系统安全防护评估应当严格控制实施风险，确保评估工作不影响电力监控系统的安全稳定运行。评估前制定相应的应急预案，实施过程应当符合电力监控系统的相关管理规定。

6 附 则

本方案中下列用语的含义：

6.1 新一代电网调度控制系统：随着技术的发展，省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过程中，原有各个系统大多都集成为一个整体，并统称新一代电网调度控制系统。

6.2 重要厂站是指接入 220 千伏以上电网的发电厂和变电站（含开关站和换流站）；小型厂站是指接入 110/66 千伏

及以下电网的发电厂和变电站（含开关站和换流站）。

6.3　电力一次系统是构成电力系统的主体，它由直接生产、输送和分配电能的各种设备所构成，主要包括发电机、变压器、断路器、隔离开关、电力母线、输电线路和电力电缆等。

附录 1　相关安全防护法规和标准

《中华人民共和国保守秘密法》
《中华人民共和国计算机信息系统安全保护条例》
《电力监管条例》
《电力工业中涉及的国家秘密及具体范围的规定》
《计算机信息系统安全专用产品检测和销售许可证管理办法》
《计算机信息系统保密管理暂行规定》
《涉及国家秘密的通信、办公自动化和计算机信息系统审批暂行办法》
《计算机信息网络国际联网安全保护管理办法》
《信息安全等级保护管理办法》
《计算机信息系统安全保护等级划分准则》
《商用密码管理条例》
《计算机病毒防治管理办法》
《关于维护网络安全和信息安全的决议》
《电力监控系统安全防护规定》
《关于加强工业控制系统信息安全管理的通知》
GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南
GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南
GBT 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求.
IEC TR 62210 技术报告 电力系统控制和相关通信—数据和通信安全
ISO/IEC 17799 信息技术 保密安全技术 信息保密安全管理惯例法规
ISO/IEC13335-1 信息技术 安全管理指南 1 IT 安全的概念与模型
ISO/IEC13335-2 信息技术 安全管理指南 2 IT 安全管理与策划
ISO/IEC13335-3 信息技术 安全管理指南 3 IT 安全管理技术
ISO/IEC13335-4 信息技术 安全管理指南 4 防护措施的选择
ISO/IEC13335-5 信息技术 安全管理指南 5 网络安全管理指南
ISO 21827 系统安全工程 能力成熟度模型（SSE-CMM）
《信息安全风险管理指南》
《信息安全风险评估指南》

附录 2　主要术语中英文对照

AGC（Automatic Generation Control）：自动发电控制

CDMA(code-division multiple access) 码分多址

DAS（Distribution Automation Systtem）：配电网自动化系统

DCS（Distributed Control Systems）：分散控制系统

DMIS（Dispatch Management Information System)：调度生产管理系统

EMS（Energy Management System）：能量管理系统

EPON（Ethernet Passive Optical Network）：以太网无源光网络

GPON（Gigabit-Capable Passive Optical Network）：千兆比特无源光网络

GPRS（General Packet Radio Service) 通用分组无线服务技术

HTTPS（Hypertext Transfer Protocol Secure）：安全超文本传输协议

IDS（Intrusion Detection System）：入侵检测系统

MPLS-VPN（Multi-Protocol Label Switching - Virtual Private Networks）：多协议标记交换-虚拟专用网

PLC（Programmable Logic Controller）：可编程序逻辑控制器

PVC (Permanence Virtual Circuit)：永久虚电路

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

SDH/PDH（Synchronous Digital Hierarchy/Plesiochronous Digital Hierarchy）：同步数字传输体系/准同步数字体系

SNMP （Simple Network Management Protocol）：简单网络管理协议

TMR（Tele-Meter Reading）：电能量计量系统

USB（Universal Serial Bus）：通用串行总线

VLAN（Virtual Local Area Network）：虚拟局域网

VPN（Virtual Private Networks）：虚拟专用网

WAMS（Wide Area Measurement System）：广域相量测量系统

附件 2:

省级以上调度中心监控系统安全防护方案

1 总则

1.1 为了加强省级以上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:《地（县）级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》及《电力监控系统安全防护评估规范》。

1.3 调度中心电力监控系统安全防护目标是抵御黑客及恶意代码等通过各种形式对电力监控系统发起的恶意破坏和攻击，能够抵御集团式攻击，防止调度中心电力监控系统的瘫痪，并由此导致电力系统事故，特别是大面积停电事故。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 本方案适用于省级以上电力调度中心，大型地（市）电力调度中心可以参照执行。

2 典型结构

省级以上调度中心的传统电网调度自动化系统主要包

括能量管理系统、广域相量测量、电网动态监控系统、继电保护、故障录波信息管理系统、电力设备在线监测系统、电能量计量系统、实时和次日电力市场运营系统、调度员培训模拟系统、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。典型逻辑结构图见图 1。

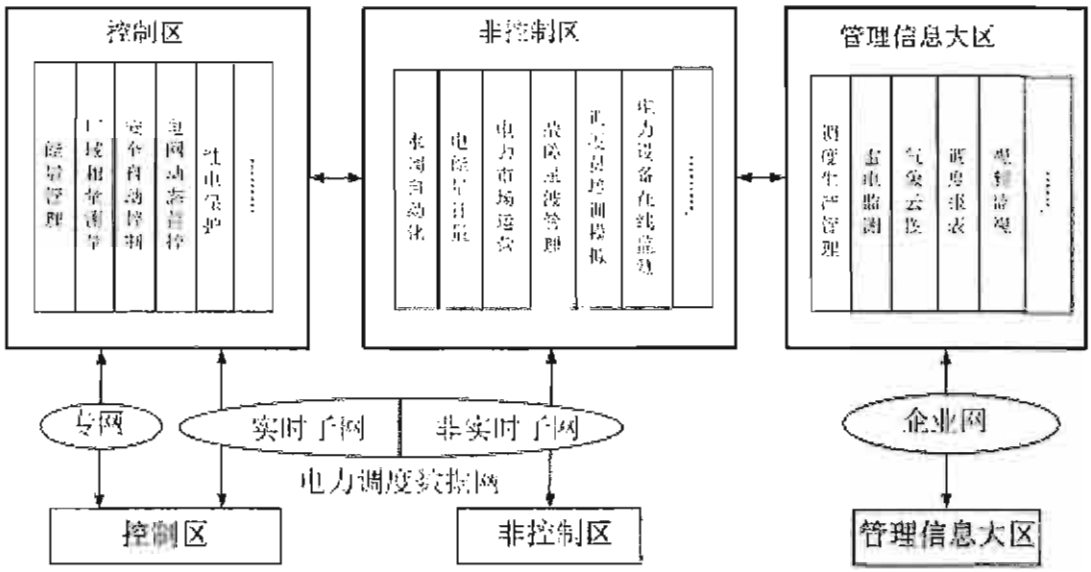

图 1 传统电网调度自动化系统典型逻辑结构图

随着技术的发展，省级以上调度中心监控系统以及功能模块发生较大变化，上述所列系统大多集成为一个整体，并统称新一代电网调度控制系统。典型的新一代电网调度控制系统，通常由一个基础平台和实时监控、安全校核、调度计划和调度管理四类应用构成。典型逻辑结构见图 2。

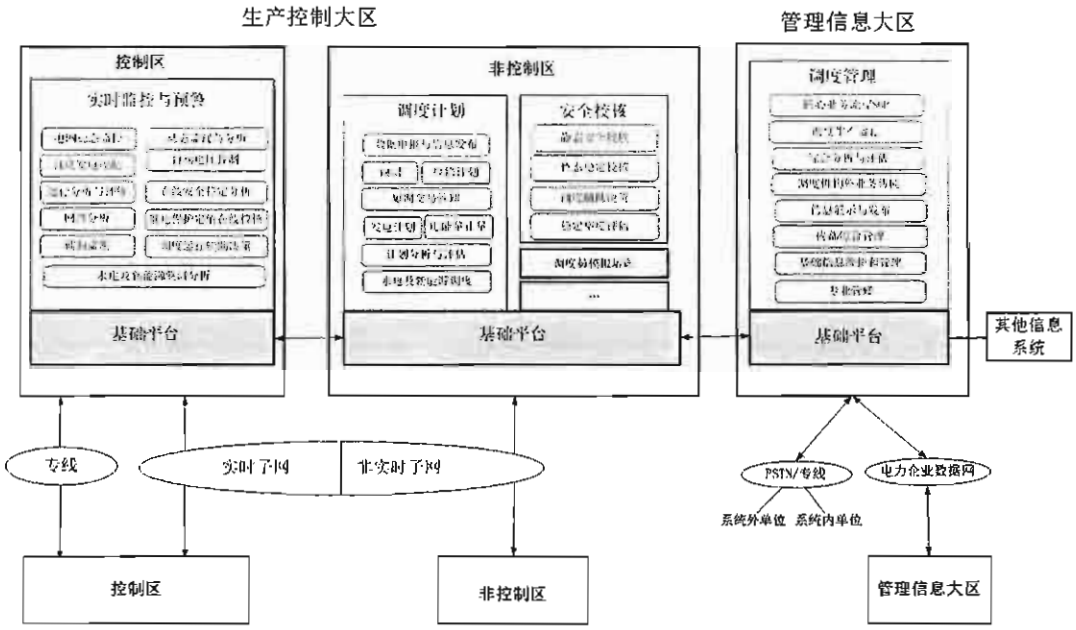

图 2 新一代电网调度控制系统典型逻辑结构图

3 安全分区

3.1 控制区

传统电网调度自动化系统的控制区主要包括：能量管理、广域相量测量、安全自动控制、继电保护等业务和功能模块。

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（电网稳态监控、动态监视与分析、自动发电控制、自动电压控制、运行分析与评价、在线安全稳定分析、网络分析、继电保护定值在线校核、辅助监测、调度运行辅助决策、水电及新能源监测分析）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：故障录波信息管理、电力设备在线监测、实时和次日电力市场运

营、调度员培训模拟、水库调度自动化、电能量计量等业务和功能模块。

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（数据申报与信息发布、预测、检修计划、短期交易管理、发电计划、电能量计量、计划分析与评估、水电及新能源调度），安全校核类应用（静态安全校核、暂态稳定校核、调度辅助决策、稳定裕度评估），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/卫星云图、视频监视、调度信息发布、办公自动化等业务和功能模块。

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（调度生产运行、综合分析与评估、调度机构外业务协同、信息展示与发布、内部综合管理、基础信息维护和管理、专业管理）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 省级以上调度中心传统电力监控系统业务功能安全分区表

序号	业务系统	控制区	非控制区	管理信息大区
1	能量管理	电网和设备监控、AGC、AVC、安全分析等		WEB发布
2	广域相量测量系统	动态数据采集、实时数据处理、分析等		
3	安全自动控制系统	稳定分析、决策生成和下发		

序号	业务系统	控制区	非控制区	管理信息大区
4	通信监控系统	通信监控信息采集、监视		
5	继电保护	继电保护远方修改定值、远方投退等控制功能。		
6	故障录波信息管理系统		故障录波信息管理模块	
7	电力设备在线监测		信息采集、处理	信息采集、处理
8	实时和次日电力市场运营系统	在线安全稳定校核	交易、结算、考核、内网报价	外网报价、公众信息发布
9	调度员培训模拟系统		调度员培训模拟	
10	水库调度自动化系统		水情信息采集、处理	
11	电能量计量系统		电能量采集、处理	
12	电网动态监控系统	在线监控、稳定计算等		
13	电力市场监管信息系统接口			向电力市场监管系统发布有关信息
14	调度生产管理系统			数据统计、分析、报表、管理流程
15	雷电监测系统			采集、处理
16	气象/卫星云图系统			接收、处理
17	视频监视系统			接收、处理
18	调度信息发布			WEB 服务
19	办公自动化			MIS、OA
20	电力调度数据网络	实时子网	非实时子网	

表 2 省级以上调度中心新一代电网调度控制系统业务功能安全分区表

序号	业务系统	控制区	非控制区	管理信息大区
1	基础平台	基础平台	基础平台	基础平台
2	实时监控与预警类应用	电网稳态监控、动态监视与分析、自动发电控制、自动电压控制、运行分析与评价、在线安全稳定分析、网络分析、继电保护定值在线校核、辅助监测、调度运行		

序号	业务系统	控制区	非控制区	管理信息大区
		辅助决策、水电及新能源监测分析		
3	调度计划类应用		数据申报与信息发布、预测、检修计划、短期交易管理、短期交易管理、发电计划、电能量计算、计划分析与评估、水电及新能源调度	
4	安全校核类应用		静态安全校核、暂态稳定校核、调度辅助决策、稳定裕度评估	
5	其它应用		调度员培训模拟等	
6	调度管理类应用			调度生产运行、综合分析与评估、调度机构外业务协同、信息展示与发布、内部综合管理、基础信息维护和管理、专业管理

4 安全部署

根据总体方案要求，结合调度中心监控系统的安全分区和安全区域边界条件，典型的传统电网调度自动化系统安全防护的总体安全部署如图 3，新一代电网调度控制系统的安全防护的总体安全部署如图 4。

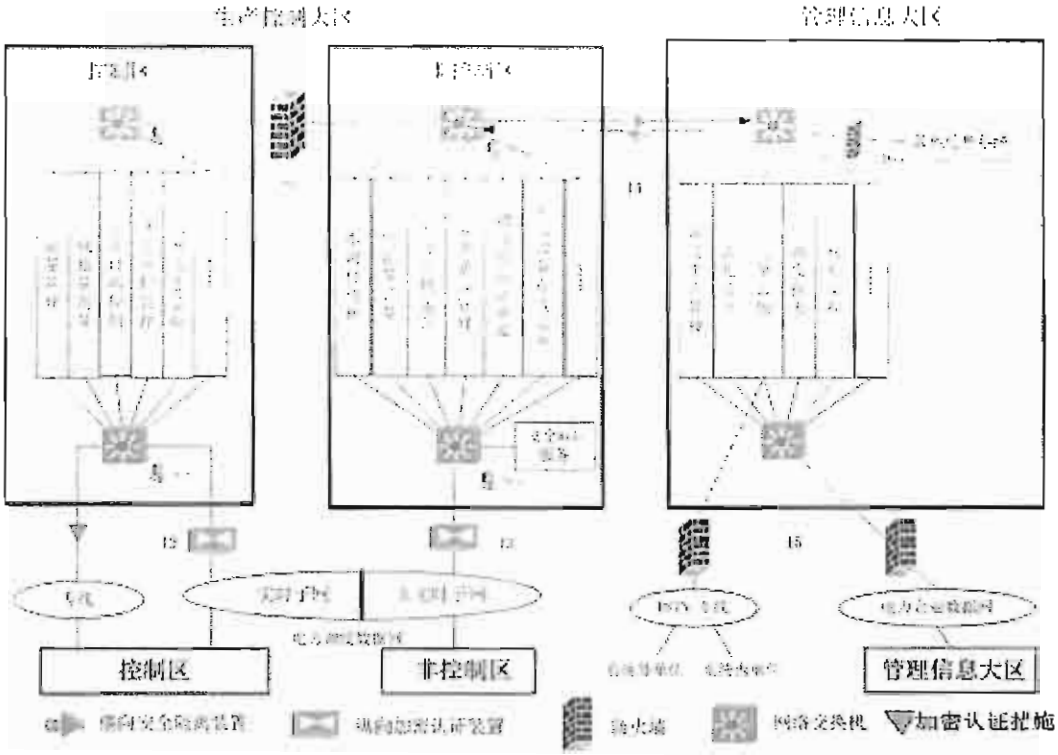

图 3 传统电网调度自动化系统安全防护总体安全部署示意图

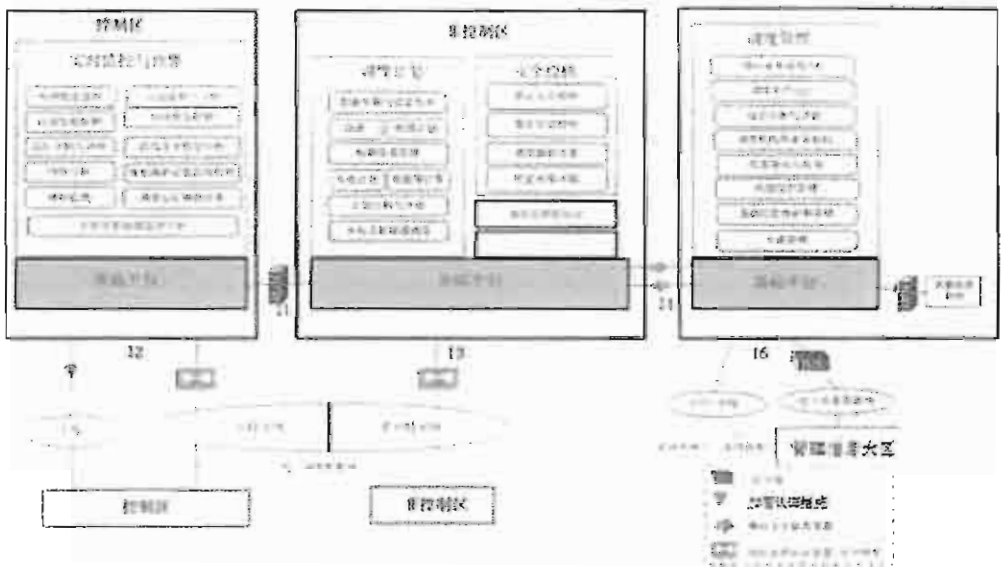

图 4 新一代电网调度控制系统安全防护总体安全部署示意图

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 TCP/IP
I2	控制区纵向边界	1.遥信、遥测及计算数据; 2.电网模型数据等	电力调度数据网 TCP/IP
I3	非控制区纵向边界	1.负荷需求数据 2.发电计划数据 3.联络线数据 4.DTS 相关数据 5.市场交易安全校核等相关数据	电力调度数据网 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 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 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 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。

各安全区均分别配置了前端交换机和后端交换机，是调度中心监控系统安全防护的典型模式。

调度中心应当采用病毒防护、入侵检测、安全审计和安全管理平台等安全防护手段，提高电力监控系统整体安全防护的管控能力。生产控制大区的安全管理平台不应当与管理信息大区的安全管理平台互联。

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。

省级以上调度中心应当部署内网安全监视应用，实时监测电力监控系统的计算机、网络及安全设备运行状态，对纵向加密认证装置进行统一管理，及时发现非法外联、外部入

侵等安全事件并告警。

省级以上调度中心应该建立支持国密算法、具备安全标签功能的电力调度数字证书系统，负责所辖调度范围及下级调度机构的电力调度数字证书的颁发、维护和管理。能量管理系统和电力市场运营系统应当逐步采用数字证书技术实现加密认证机制。对于遥控和定值设置等功能必须使用加密认证手段来传输控制命令。

省级以上调度中心应当建立备用调度中心，做到关键应用的应用级备用和一般应用的数据备份，备用调度中各系统的安全防护措施应当和主系统完全一致。

生产控制大区中各业务系统根据行业信息安全等级保护要求，在物理、安全设备、操作系统、数据、应用等方面进行全面防护。

5 主要业务功能安全防护方案

本章仅对省级以上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 省级以上调度中心新一代电网调度控制系统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下文所述。

5.1 能量管理系统安全防护

能量管理功能实现对实时运行的电力系统进行数据采

集、监视、控制和安全分析的功能，是调度中心的核心系统；其中电网和设备监控、AGC、AVC 和安全分析等功能模块置于控制区。

根据能量管理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。

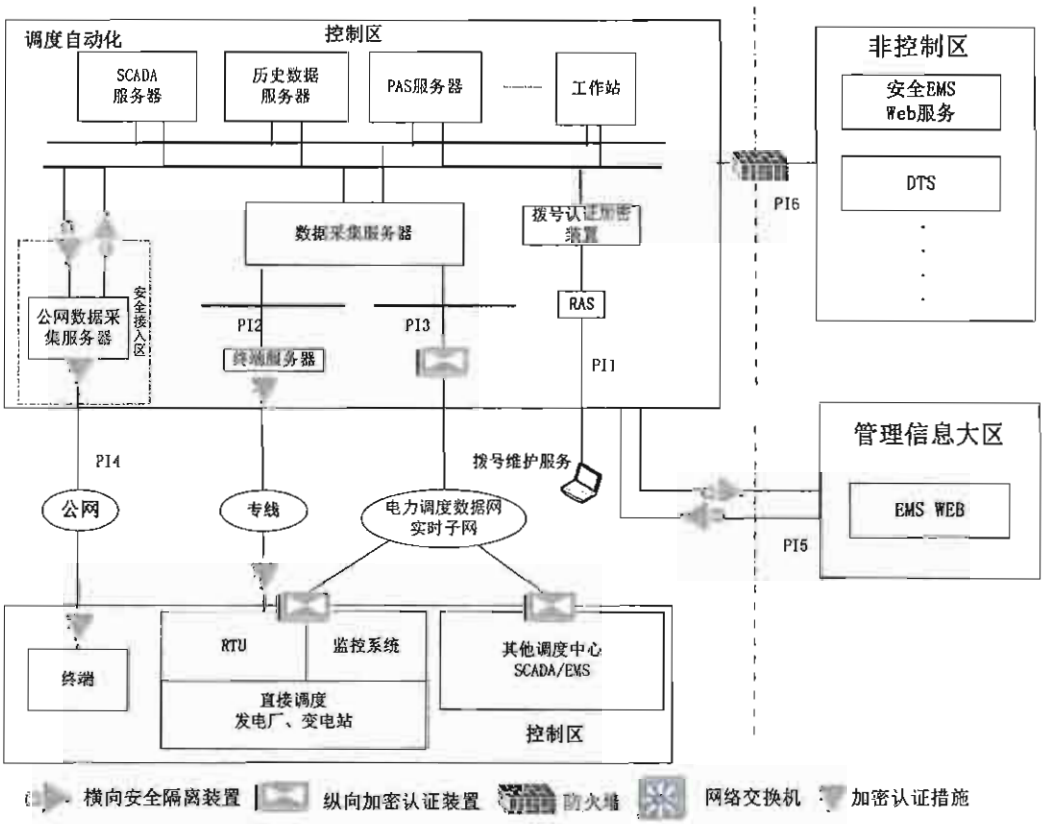

图 5　能量管理系统的物理边界及安全部署示意图

能量管理系统的物理边界为：拨号网络边界（PI1）、传统专用远动通道（PI2）、纵向网络边界（PI3）、横向网络边界（PI4,PI5,PI6），这六个边界的安全防护措施按照总体方案实施。

5.2 电力市场运营系统安全防护

电力市场运营系统（PMOS）是电力调度（交易）中心的

核心业务系统之一，主要包括市场交易、报价处理、合同管理、交易结算等功能模块，是电力市场技术支持系统的重要组成部分。该系统横跨三个安全区域，其主体部分位于非控制区，实时电力市场中的在线控制功能应当位于控制区，对社会发布市场信息的功能模块应当位于管理信息大区。根据电力市场运营系统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。

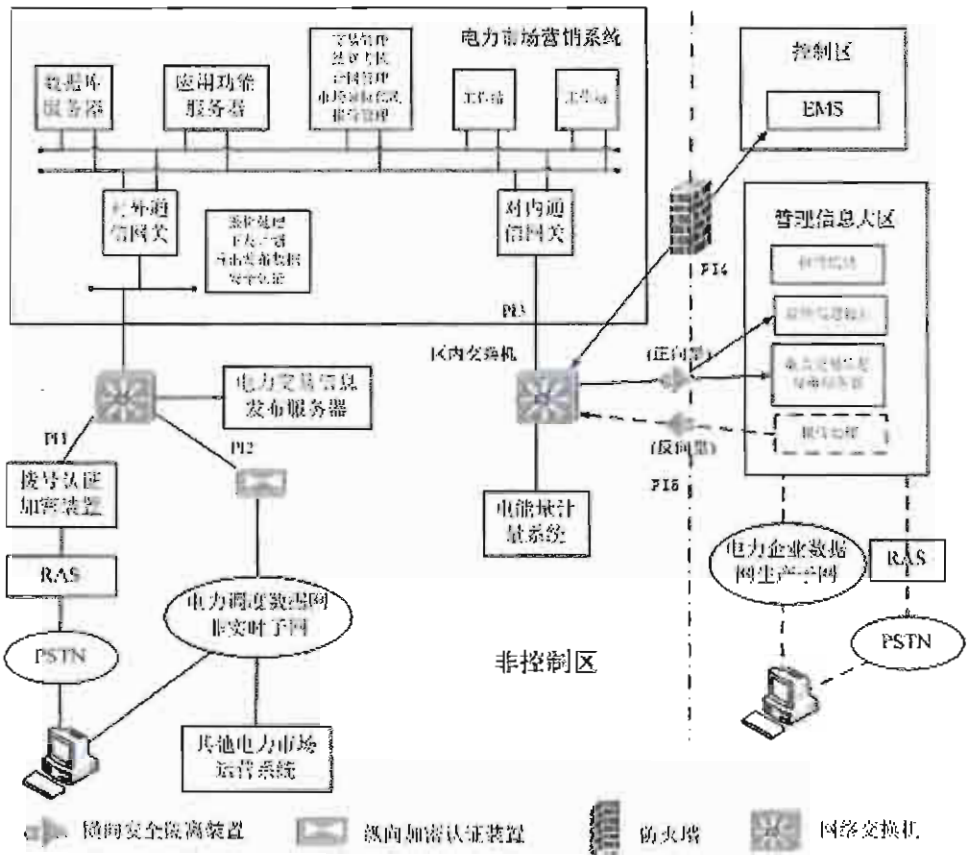

图 6　电力市场运营系统的物理边界及安全部署示意图

电力市场运营系统的物理边界为拨号网络边界（PI1）、纵向网络边界（PI2，PI3）和横向网络边界（PI4，PI5）。这五个边界的安全防护措施按照总体方案实施。

电力市场运营系统应当以网络通信方式为主，拨号方式

可以作为备用，拨号访问安全风险较大，应当限制使用，禁止无安全措施的拨号访问。

电力市场运营系统应当支持加密认证机制，实现与远方市场交易成员的基于电力调度数字证书的身份认证与加密通信。

电力市场运营系统的市场信息发布功能模块部署在非控制区和管理信息大区，分别面向市场交易成员和社会公众。

根据《电力监管条例》的要求，将电力市场监管信息经过加密认证等安全措施，直接向电力监管机构报送。

5.3 电能量计量系统安全防护

电能量计量系统（TMR）通过电能量采集装置采集电能量数据，作为计量和结算的依据，禁止修改原始数据。根据电能量计量系统的特点和《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 7。

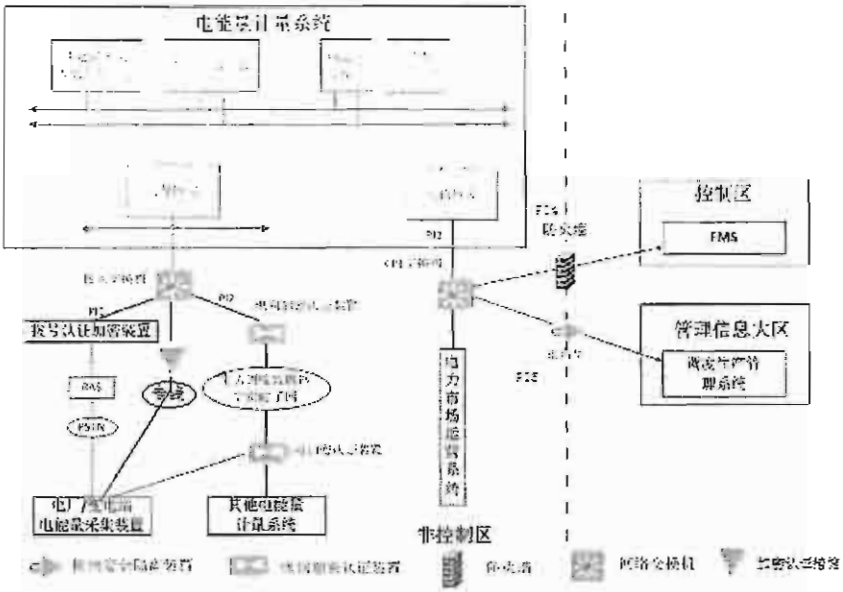

图 7　电能量计量系统的物理边界及安全部署示意图

电能量计量系统的物理边界为：拨号网络边界（PI1）、纵向网络边界（PI2，PI3）和横向网络边界（PI4，PI5）。这五个边界的安全防护措施按照总体方案实施。

推荐采用网络方式采集电能量数据，采用单向拨号通信方式时应当满足相应安全防护措施。省级以上调度中心的电能量计量系统中原则上不采用 GPRS 或 CDMA 等公用移动数据通信方式，确实需要者，可以将主站通信网关机置于安全接入区，电能量数据通过专用横向单向安全隔离装置（反向型）导入。

5.4 水库调度自动化系统安全防护

水库调度自动化系统功能采集水情、水文、气象信息，进行水情预报和水库调度。其主体在非控制区，气象信息采集模块、与外部机构（如防洪指挥部、流域委员会）通信的模块在管理信息大区。根据水库调度自动化功能系统的特点

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 8。

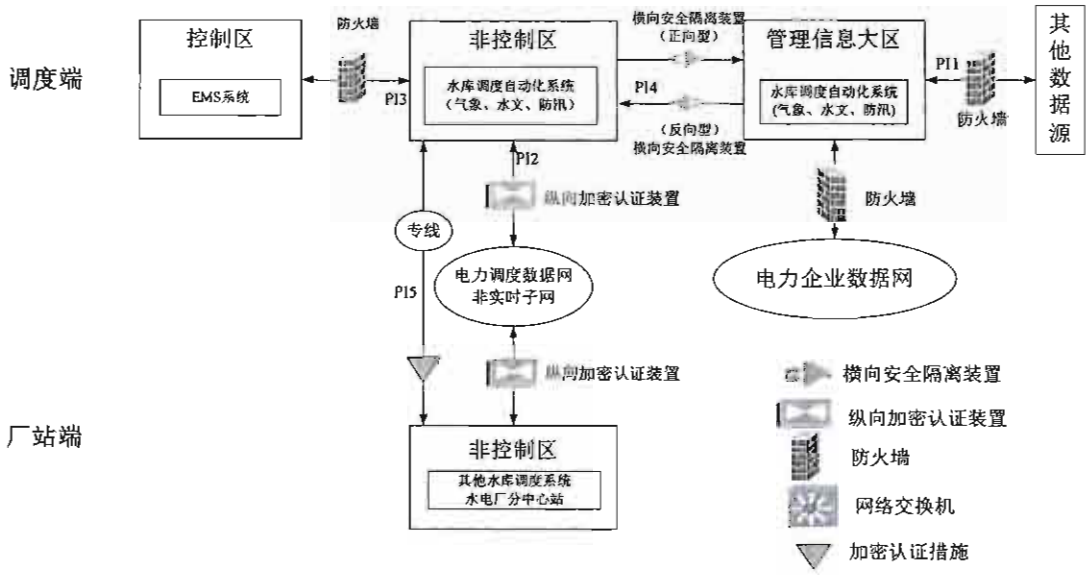

图 8 水库调度自动化功能系统物理边界及安全部署示意图

水库调度自动化功能系统的物理边界为外部网络边界（PI1）、纵向网络边界（PI2，PI5，PI6）和横向网络边界（PI3、PI4）。这六个边界的安全防护措施按照总体方案实施。

5.5 继电保护、故障信息管理系统安全防护

继电保护、故障信息管理系统采集继电保护装置的相关信息和故障录波的故障信息，监视继电保护运行状态，为电网故障判断和分析提供技术手段。继电保护功能模块应当置于控制区，故障信息管理模块应当置于非控制区。根据继电保护、故障信息管理系统的特点和电力监控系统安全防护总体方案的要求，其物理边界和安全部署如图 9。

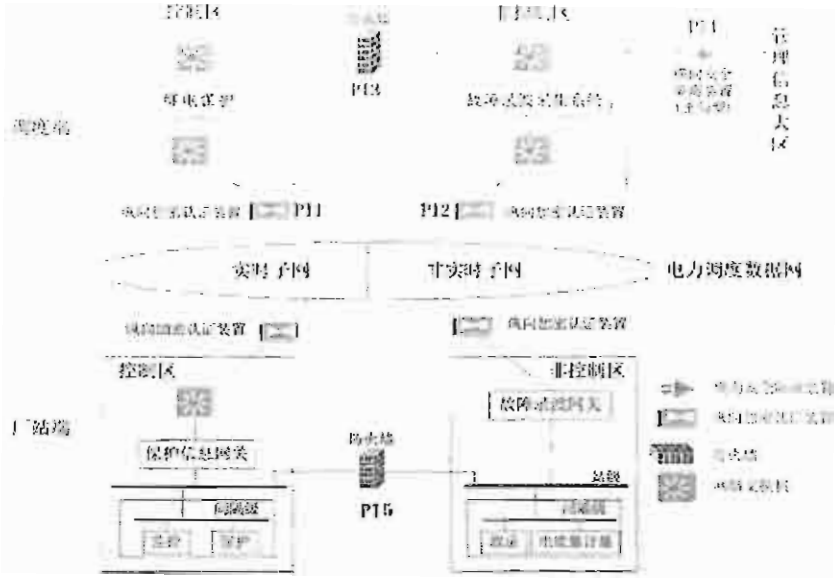

图9 继电保护、故障信息管理系统安全部署示意图

继电保护、故障信息管理系统的物理边界为纵向网络边界（PI1，PI2）和横向网络边界（PI3、PI4、PI5）。这四个边界的安全防护措施按照总体方案实施。

进行保护远方定值修改和投退操作的人员必须使用电力调度数字证书进行身份认证，设置工作站和厂站端也须进行双向身份认证。

5.6 调度生产管理系统安全防护

调度生产管理主要包括调度生产数据服务、调度报表管理、调度检修信息、水文气象信息、雷电监测等多种业务，系统主体位于管理信息大区。

调度生产管理系统使用电网企业数据网的生产子网进行广域网通信，并采用硬件防火墙实现安全隔离。调度生产管理系统属于电网企业管理信息大区中的一个重要业务系统，与发电企业管理信息大区没有直接联系。

调度生产管理系统与生产控制大区之间的数据通信必须经过电力专用横向单向安全隔离装置。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。

调度生产管理系统的安全防护部署如图 10。

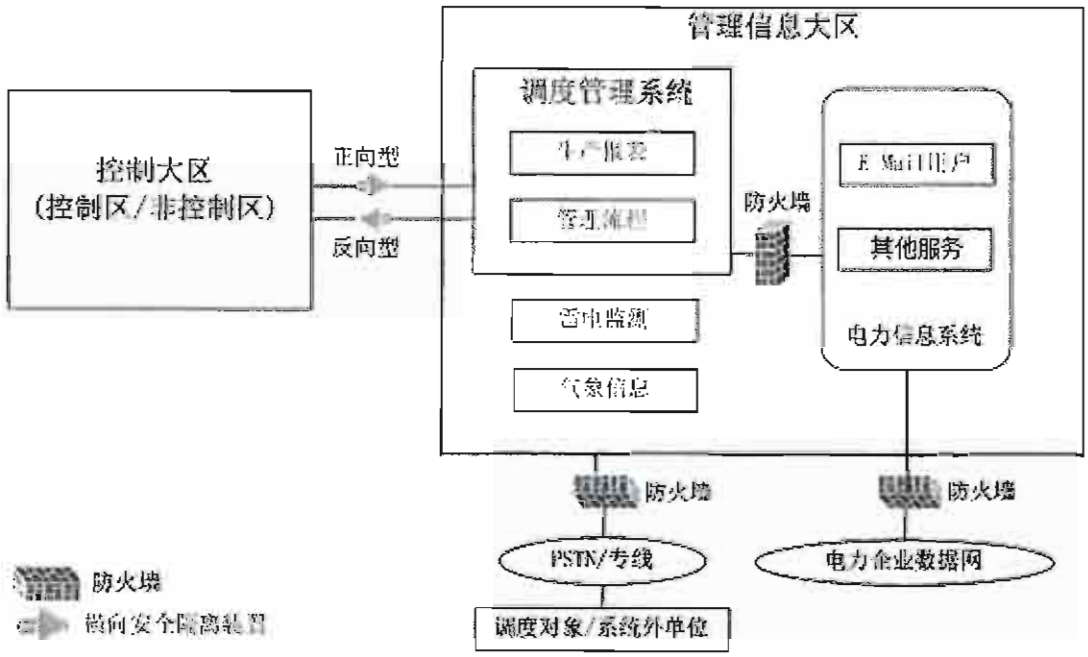

图 10　调度生产管理系统安全部署示意图

5.7 大屏幕投影系统安全防护

生产控制大区中各业务系统可以采用网络方式接入大屏幕投影系统，同时采用硬件防火墙等进行隔离。管理信息大区中的各业务系统可以采用非网络方式接入该大屏幕投影系统。生产控制大区和管理信息大区中的各业务系统不能同时以网络方式接入大屏幕投影系统。

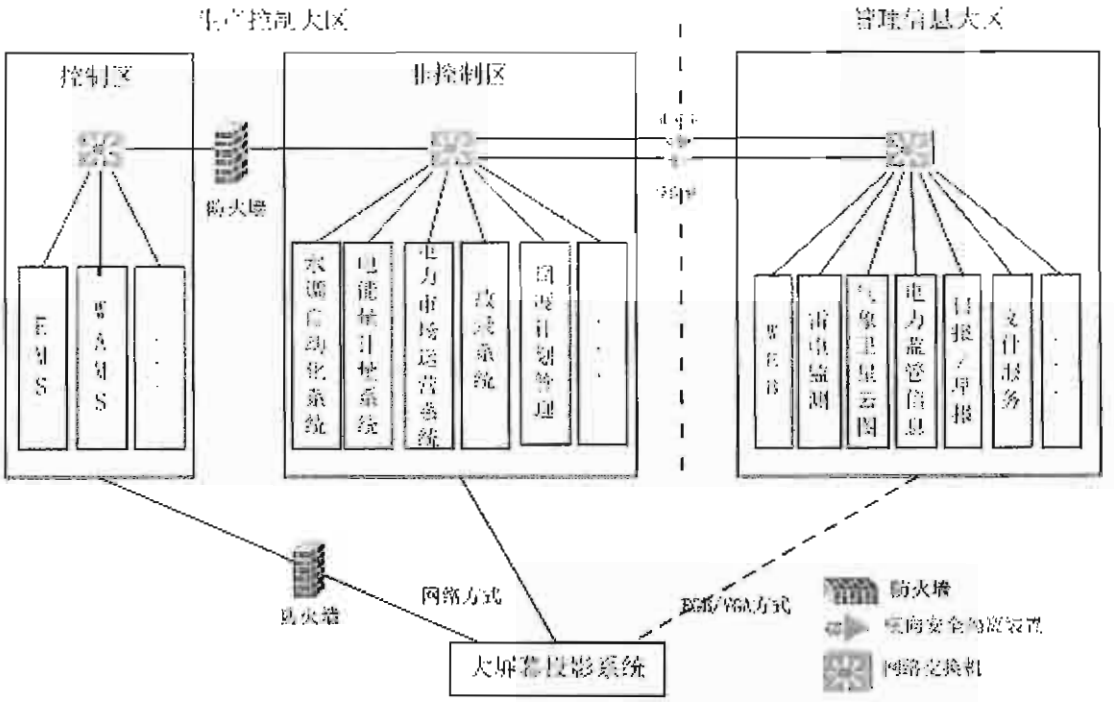

图 11 大屏幕系统安全防护结构示意图

附录　主要术语中英文对照

AGC（Automatic Generation Control）：自动发电控制
AVC（Automatic Voltage Control）：自动电压控制
DTS（Dispatcher Training Simulator）：调度员培训模拟系统
EMS （Energy Management System）：能量管理系统
MIS（Management Information System）：管理信息系统
OA （Office Automation）：办公自动化系统
PMOS（Power Market Operation System）： 电力市场运营系统
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
TCP/IP（Transaction Control Protocol/Internet Protocol）：互联网传输协议
TMR（Tele-Meter Reading）：电能量计量系统

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:

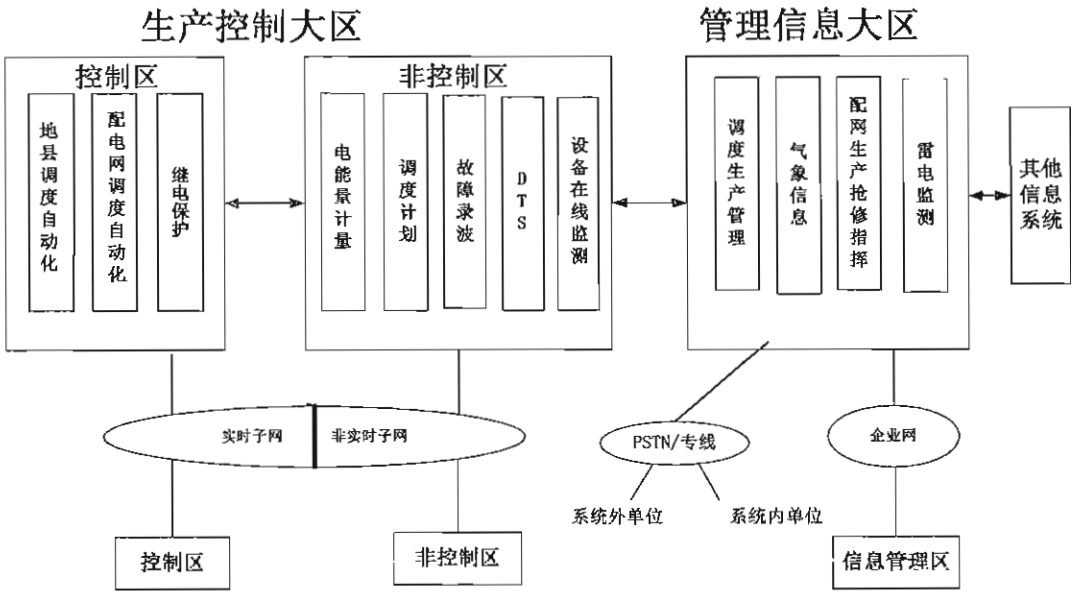

图 1 地（县）级调度中心监控系统典型结构示意图

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

过程中，上述所列系统大多都集成为一个整体，并统称新一代电网调度控制系统。典型的新一代电网调度控制系统，通常包含一个基础平台和实时监控、调度计划和调度管理三类应用构成。典型逻辑结构见图 2。

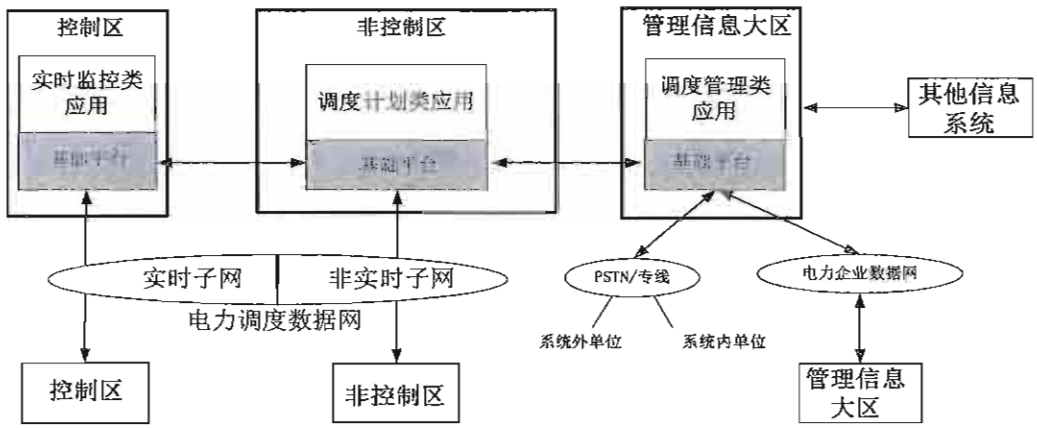

图 2 新一代地（县）级调度中心调度控制系统典型结构示意图

其中配电网调度自动化、负荷管理等采用公网通信和无线网络通信方式进行数据采集控制的业务的安全防护可以参照《配电监控系统安全防护方案》执行。

小型县调的安全防护措施可以根据具体情况进行简化，对生产控制大区可以不再细分，重点保护监控系统，相当于只有控制区，与厂站端数据通信的纵向边界可以采用简单有效的数据加密等安全防护措施。

3 安全分区

3.1 控制区

传统电网调度自动化系统的控制区主要包括：电网实时监控、自动电压控制（AVC）、电力系统高级应用软件（PAS）、

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。

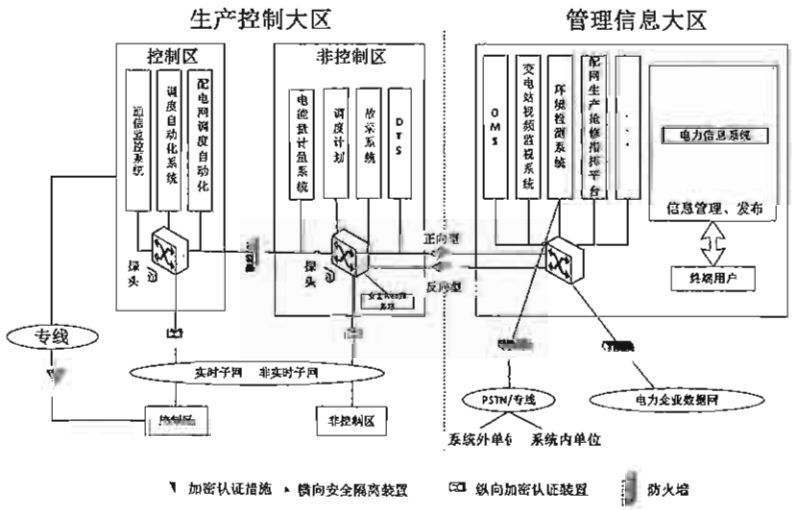

图 3 传统地（县）级调度中心调度自动化系统安全防护总体部署示意图

新建调度控制系统安全防护总体逻辑结构如下图所示。

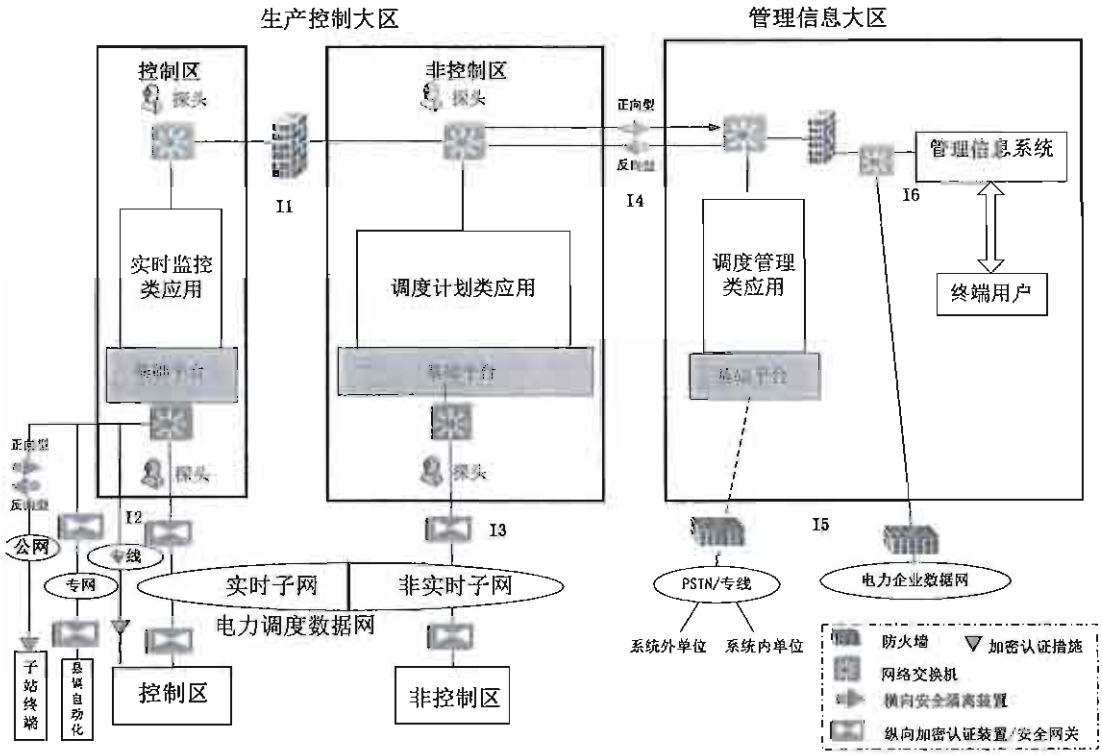

图 4 新一代地（县）级调度中心调度控制系统安全防护总体部署示意图

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 TCP/IP
I2	控制区纵向边界	1. 遥信、遥测及计算数据； 2. 电网模型数据等	电力调度数据网 TCP/IP
I3	非控制区纵向边界	1. 负荷需求数据 2. 发电计划数据 3. 联络线数据 4. DTS 相关数据 5. 市场交易安全校核等相关数据	电力调度数据网 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 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 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 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。

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。

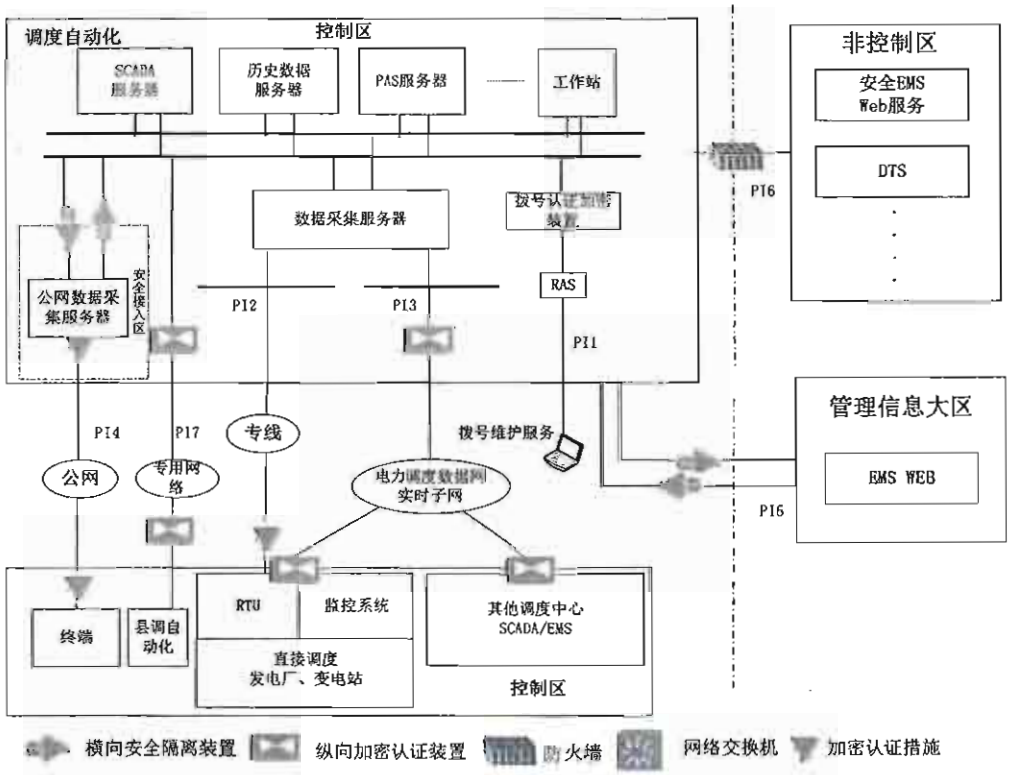

图 5 调度自动化系统的物理边界及安全部署示意图

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。

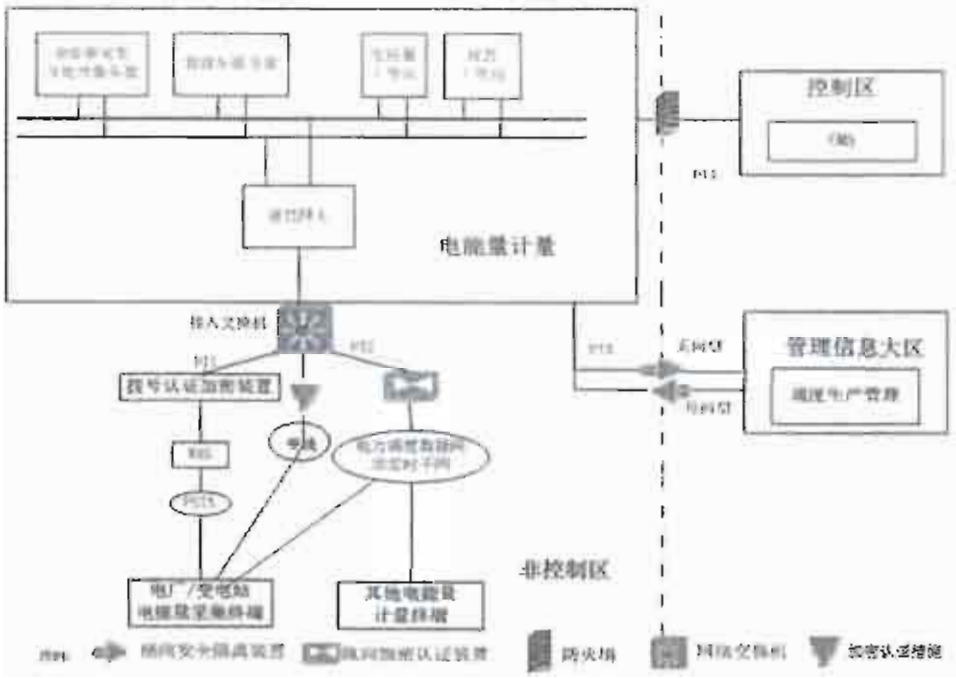

图 6 电能量计量功能的物理边界及安全部署示意图

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。

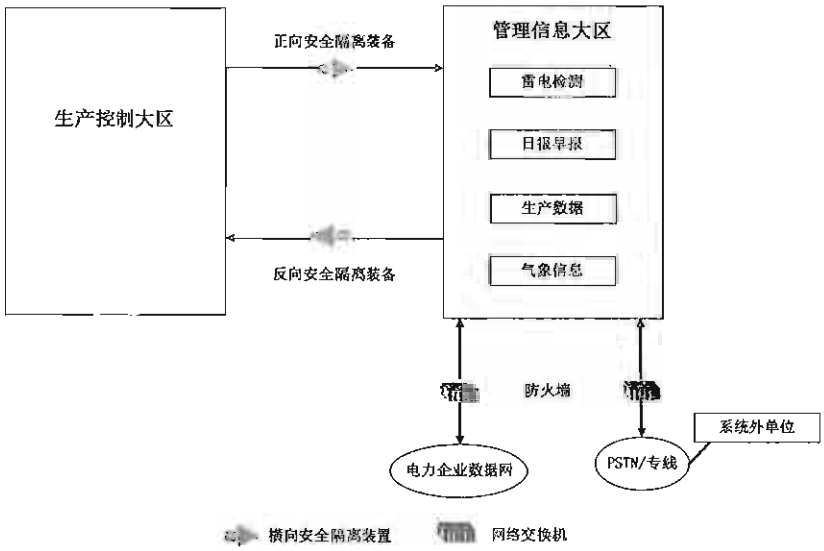

图 7 调度生产管理功能安全部署示意图

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

附件 4:

发电厂监控系统安全防护方案

1 总则

1.1 为了加强发电厂电力监控系统安全防护，抵御黑客及恶意代码等对发电厂监控系统发起的恶意破坏和攻击，以及其它非法操作，防止发电厂电力监控系统瘫痪和失控，和由此导致的发电厂一次系统事故和其他事故，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》、《地（县）级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》、《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 本方案适用于火电厂、水电厂、核电站、风电场、光伏电站、燃机电厂等各种类型发电厂。

2 基本原则

2.1 安全分区

按照《电力监控系统安全防护规定》，原则上将发电厂基于计算机及网络技术的业务系统划分为生产控制大区和管理信息大区，并根据业务系统的重要性和对一次系统的影响程度将生产控制大区划分为控制区（安全区 I）及非控制区（安全区 II），重点保护生产控制以及直接影响电力生产

(机组运行)的系统。

2.2 网络专用

电力调度数据网是与生产控制大区相连接的专用网络，承载电力实时控制、在线生产交易等业务。发电厂端的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电力企业其它数据网及外部公共信息网的安全隔离。发电厂端的电力调度数据网应当划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。

2.3 横向隔离

横向隔离是电力监控系统安全防护体系的横向防线。应当采用不同强度的安全设备隔离各安全区，在生产控制大区与管理信息大区之间必须部署经国家指定部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。生产控制大区内部的安全区之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设施，实现逻辑隔离。防火墙的功能、性能、电磁兼容性必须经过国家相关部门的认证和测试。

2.4 纵向认证

纵向加密认证是电力监控系统安全防护体系的纵向防线。发电厂生产控制大区与调度数据网的纵向连接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置，实现双向身份认证、数据加密和访问控制。

2.5 综合防护

综合防护是结合国家信息安全等级保护工作的相关要求对电力监控系统从主机、网络设备、恶意代码防范、应用安全控制、审计、备份及容灾等多个层面进行信息安全防护的过程。

3 安全区的划分

3.1 控制区（安全区Ⅰ）

火电厂和水电厂的控制区主要包括以下业务系统和功能模块：火电机组分散控制系统（DCS）、火电机组辅机控制系统、自动发电控制系统（AGC）、自动电压控制系统（AVC）、火电厂厂级信息监控系统的监控功能、水电厂集中监控系统、梯级调度监控系统、网控系统、相量测量装置（PMU）、继电保护、各种控制装置(调速系统、励磁系统、快关汽门装置等)、五防系统等。

核电站的控制区主要包括以下业务系统和功能模块：核电站厂级分散控制系统（DCS）、自动电压控制系统（AVC）、厂级信息监控系统的监控功能、网控系统、继电保护、辅机控制系统、相量测量装置（PMU）和自动控制装置（安控、电力系统稳定器等），其中辅机控制系统包括三废处理系统、循环水处理系统、凝结水精处理系统和除盐水系统等。

风电场的控制区主要包括以下业务系统和功能模块：风电场监控系统、无功电压控制、发电功率控制、升压站监控

系统、继电保护和相量测量装置（PMU）等。

光伏电站的控制区主要包括以下业务系统和功能模块：光伏电站运行监控系统、无功电压控制、发电功率控制、升压站监控系统、继电保护等。

燃机电厂的控制区主要包括以下业务系统和功能模块：燃机电厂厂级分散控制系统（DCS）、燃气轮机控制系统（TCS）、厂级信息监控系统的监控功能、自动发电控制系统（AGC）、自动电压控制系统（AVC）、相量测量装置（PMU）、火警探测系统、升压站监控系统、继电保护等。

对于没有分散控制系统（DCS）的小型发电厂的监控系统，其生产控制大区可以不再细分，可将各业务系统和装置均置于控制区，其中在控制区中的故障录波装置和电能量采集装置可以通过调度数据网或拨号方式与相应的调度中心通信。

3.2 非控制区（安全区Ⅱ）

火电厂和水电厂的非控制区主要包括以下业务系统和功能模块：火电厂厂级信息监控系统的优化功能、梯级水库调度自动化系统、水情自动测报系统、水电厂水库调度自动化系统、电能量采集装置、电力市场报价终端、故障录波信息管理终端等。

核电站的非控制区主要包括以下业务系统和功能模块：厂级信息监控系统的优化功能、电能量采集装置和故障录波

装置等。

风电场的非控制区主要包括以下业务系统和功能模块：风功率预测系统、状态监测系统、电能量采集装置和故障录波装置等。

光伏电站的非控制区主要包括以下业务系统和功能模块：光伏功率预测系统、电能量采集装置和故障录波装置等。

燃机电厂的非控制区主要包括以下业务系统和功能模块：厂级信息监控系统的优化功能、电能量采集装置和故障录波装置等。

对于将电能量采集装置置于发电厂控制区内的情况，可以只将计量通信网关置于非控制区。

3.3 管理信息大区

火电厂和水电厂的管理信息大区主要包括以下业务系统和功能模块：火电厂厂级信息监控系统的管理功能、雷电监测系统、气象信息系统、大坝自动监测系统、防汛信息系统、报价辅助决策系统、检修管理系统和管理信息系统（MIS）等。

核电站的管理信息大区主要包括以下业务系统和功能模块：厂级信息监控系统的管理功能、检修管理系统和管理信息系统（MIS）。

风电场的管理信息大区主要包括以下业务系统和功能模块：天气预报系统、检修管理系统、测风塔系统和管理信

息系统（MIS）等。

光伏电站的管理信息大区主要包括以下业务系统和功能模块：天气预报系统、检修管理系统和管理信息系统（MIS）等。

燃机电厂的管理信息大区主要包括以下业务系统和功能模块：厂级信息监控系统的管理功能和管理信息系统（MIS）等。

发电厂管理信息大区的业务主要运行在发电企业数据网或公共数据网，各发电企业可以遵照安全防护规定的原则，根据各自实际情况，自行决定其安全防护策略和措施。

此外，核电站的辐射监测系统、地震监测系统、环境监测系统、实物保护系统、应急分析与指挥系统等信息系统，与电力生产没有直接关系，不属于电力监控系统，不在本规定的防护范围内。建议核电站应尽可能将上述系统划分在管理信息大区，并按照相关主管部门的要求进行安全防护。

4 边界安全防护

4.1 横向边界防护

4.1.1 生产控制大区与管理信息大区边界安全防护

发电厂生产控制大区与管理信息大区之间通信应当部署电力专用横向单向安全隔离装置。

4.1.2 控制区（安全区Ⅰ）与非控制区（安全区Ⅱ）边界安全防护

安全区Ⅰ与安全区Ⅱ之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的设备，实现逻辑隔离、报文过滤、访问控制等功能。所选设备的功能、性能、电磁兼容性必须经过国家相关部门的认证和测试。

发电厂（DCS）系统部署在安全区Ⅰ，与运行在安全区Ⅱ的发电厂厂级监控系统（SIS）优化功能进行信息交换应当采用逻辑隔离的安全防护措施。

4.1.3 系统间安全防护

发电厂内同属于安全区Ⅰ的各机组监控系统之间、机组监控系统与控制系统之间、同一机组的不同功能的监控系统之间，尤其是机组监控系统与输变电部分控制系统之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂内同属于安全区Ⅱ的各系统之间、各不同位置的厂站网络之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂内同属于管理信息大区的各系统之间、各不同位置的厂站网络之间，根据需要可以采取一定强度的逻辑访问控制措施，如防火墙、VLAN 等。

发电厂电力市场报价终端部署在非控制区，与运行在管理信息大区的报价辅助决策系统信息交换应当采用电力专用横向单向安全隔离装置。发电企业的市场报价终端与同安全区内其它业务系统进行数据交换时，应当采取必要的安全措施，以保证敏感数据的安全。

4.2 纵向边界防护

发电厂生产控制大区系统与调度端系统通过电力调度数据网进行远程通信时，应当采用认证、加密、访问控制等技术措施实现数据的远方安全传输以及纵向边界的安全防护。发电厂的纵向连接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施，与调度端实现双向身份认证、数据加密和访问控制。

参与系统 AGC、AVC 调节的发电厂应当在电力调度数据网边界配置纵向加密认证装置或纵向加密认证网关进行安全防护。对于没有 DCS 系统，或不参与 AGC、AVC 调节的发电厂，其电力调度数据网边界配置的安全防护措施可以根据具体情况进行简化。

对于不具备建立调度数据网的小型发电厂可以通过拨号、无线等方式接入相应调度机构的安全接入区，其他发电厂禁止使用远程拨号方式与调度端进行数据通信。

4.3 第三方边界安全防护

如果发电厂生产控制大区中的业务系统与环保、安全等

政府部门进行数据传输，其边界防护应当采用生产控制大区与管理信息大区之间的安全防护措施。

管理信息大区与外部网络之间应采取防火墙、VPN 和租用专线等方式，保证边界与数据传输的安全。

禁止设备生产厂商或其它外部企业（单位）远程连接发电厂生产控制大区中的业务系统及设备。

5 综合安全防护

5.1 入侵检测

生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计。

5.2 主机与网络设备加固

发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机、Web 服务器等，应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。

非控制区的网络设备与安全设备应当进行身份鉴别、访问权限控制、会话控制等安全配置加固。可以应用电力调度数字证书，在网络设备和安全设备实现支持 HTTPS 的纵向安全 Web 服务，能够对浏览器客户端访问进行身份认证及加密传输。

应当对外部存储器、打印机等外设的使用进行严格管理。

生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备；管理信息大区业务系统使用无线网络传输业务信息时，应当具备接入认证、加密等安全机制。

5.3 应用安全控制

发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录应用系统、访问系统资源等操作进行身份认证，提供登录失败处理功能，根据身份与权限进行访问控制，并且对操作行为进行安全审计。

对于发电厂内部远程访问业务系统的情况，应当进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。

5.4 安全审计

生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。

可以采用安全审计功能，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集中收集、自动分析。

5.5 专用安全产品的管理

安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙、入侵检测系统等专用安全产品的，应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散。

5.6 备用与容灾

应当定期对关键业务的数据进行备份，并实现历史归档数据的异地保存。关键主机设备、网络设备或关键部件应当进行相应的冗余配置。控制区的业务系统（应用）应当采用冗余方式。

5.7 恶意代码防范

应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。

5.8 设备选型及漏洞整改

发电厂电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞和风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统及设备的运行管理和安全防护。生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备。

附录1　各类型电厂安全分区表

表1 火电厂、水电厂监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	火电机组分散控制系统 DCS	DCS			A2
2	火电机组辅机控制系统	辅机 PLC/DCS			A2
3	火电厂厂级信息监控系统	监控功能	优化功能	管理功能	A2
4	调速系统和自动发电控制功能 AGC	调速、自动发电控制			A1
5	励磁系统和自动电压控制功能 AVC	励磁、自动电压控制			A1
6	水电厂监控系统	水电厂监控			A1
7	梯级调度监控系统	梯级调度监控			A1
8	网控系统	网控系统			A1
9	相量测量装置 PMU	PMU			B
10	自动控制装置	PSS、汽门快关等			B、A1
11	五防系统	五防系统			A2
12	继电保护	继电保护装置及管理终端			B
13	故障录波		故障录波装置		B
14	梯级水库调度自动化系统		梯级水库调度自动化		A1
15	水情自动测报系统		水情自动测报		A1
16	水电厂水库调度自动化系统		水电厂水库调度自动化		A1
17	电能量采集装置		电能量采集		B、A1
18	电力市场报价终端		电力市场报价		B
19	管理信息系统 MIS			MIS	A2
20	雷电监测系统			雷电监测	A2
21	气象信息系统			气象信息	A2
22	大坝自动监测系统			大坝自动监测	A2
23	防汛信息系统			防汛信息	A2
24	报价辅助决策系统			报价辅助决策	A2
25	检修管理系统			检修管理	A2
26	火灾报警系统	火灾报警			A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

与调度中心无关的电力监控系统不接入调度数据网。

表 2 核电站监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	核电站厂级分散控制系统 DCS	DCS			A2
2	自动电压控制 AVC	自动电压控制功能			A1
3	厂级信息监控系统	监控功能	优化功能	管理功能	A2
4	相量测量装置 PMU	PMU			B
5	网控系统	网控系统			A1
6	火警探测系统	火警探测系统			A2
7	辅机控制系统	辅机控制系统（三废处理系统、循环水处理系统、凝结水精处理系统、除盐水系统）			A2
8	继电保护	继电保护装置及管理终端			B
9	自动控制装置	安控、电力系统稳定器 PSS 等			A1、B
10	故障录波		故障录波装置		B
11	电能量采集装置		电能量采集装置		A1、B
12	管理信息系统 MIS			管理信息系统	A2
13	检修管理系统			检修管理系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

与调度中心无关的电力监控系统不接入调度数据网。

表 3 风电场监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	风电场监控系统	风机监控 风电场监控			A2
2	无功电压控制	无功电压控制功能			A1
3	发电功率控制	发电功率控制功能			A1
4	升压站监控系统	升压站监控功能			A1

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
5	相量测量装置 PMU	PMU			B
6	继电保护	继电保护装置及管理终端			B
7	故障录波		故障录波装置		B
8	电能量采集装置		电能量采集装置		A1、B
9	风功率预测系统		风功率预测		A1、A2
10	状态监测系统		风机状态监测		A2
11	测风塔系统			测风塔	A2
12	天气预报系统			数字天气预报	A2
13	管理信息系统 MIS			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

表 4 光伏电站监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	光伏电站运行监控系统	电站运行监控			A2
2	无功电压控制	无功电压控制功能			A1
3	发电功率控制	发电功率控制功能			A1
4	升压站监控系统	升压站监控功能			A1
5	相量测量装置 PMU	PMU			B
6	继电保护	继电保护装置及管理终端			B
7	故障录波		故障录波装置		B
8	电能量采集装置		电能量采集装置		A1、B
9	光伏功率预测系统		光伏功率预测		A1
10	天气预报系统			数字天气预报	A2
11	管理信息系统			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

表 5 燃机电厂监控系统安全分区表

序号	业务系统及设备	控制区	非控制区	管理信息大区	备注
1	燃机电厂厂级分散控制系统 DCS	机组单元控制、自动发电控制、机组保护、辅机控制、公共系统等			A2
2	燃气轮机控制系统 TCS	燃气轮机控制功能			A2
3	自动电压控制 AVC	自动电压控制功能			A1
4	厂级信息监控系统	监控功能	优化功能	管理功能	A2
5	升压站监控系统	升压站监控功能			A1
6	相量测量装置 PMU	相量测量功能			B
7	自动发电控制 AGC	自动发电控制功能			A1
8	火警探测系统	火警探测系统			A2
9	变电站综合自动化系统	变电站监控、继保、故障录波 RTU			A1
10	继电保护	继电保护装置及管理终端			B
11	故障录波		故障录波装置		B
12	电能量采集装置		电能量采集装置		A1、B
13	管理信息系统			管理信息系统	A2

注：

A1：与调度中心有关的电厂监控系统

A2：电厂内部监控系统

B：调度中心监控系统的厂站侧设备

附录 2　各类型电厂监控系统安全防护示意图

火电厂监控系统安全分区及边界防护如图 1 所示。

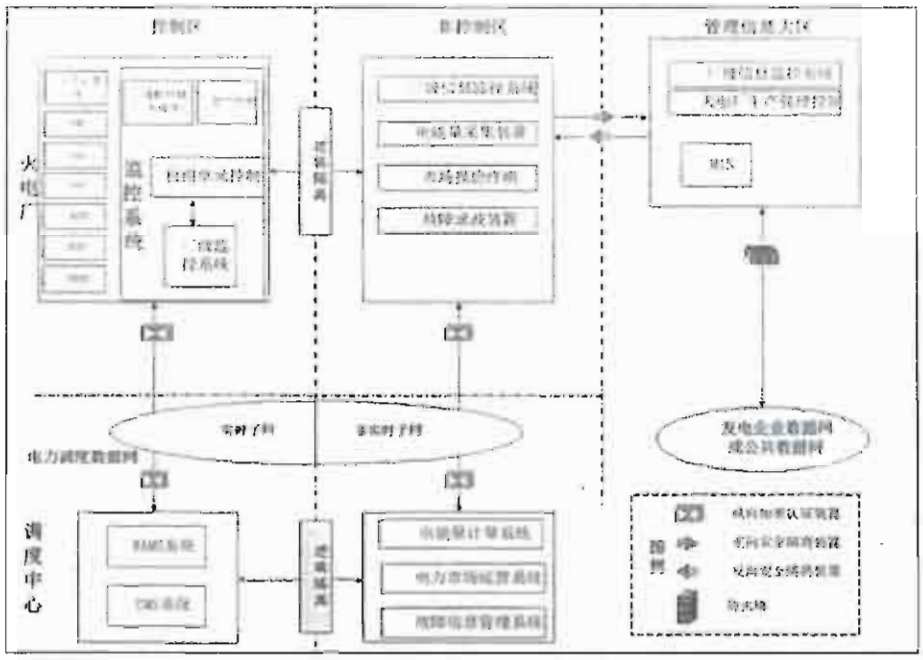

图 1 火电厂监控系统安全部署示意图

水电厂监控系统安全分区及边界防护如图 2 所示。

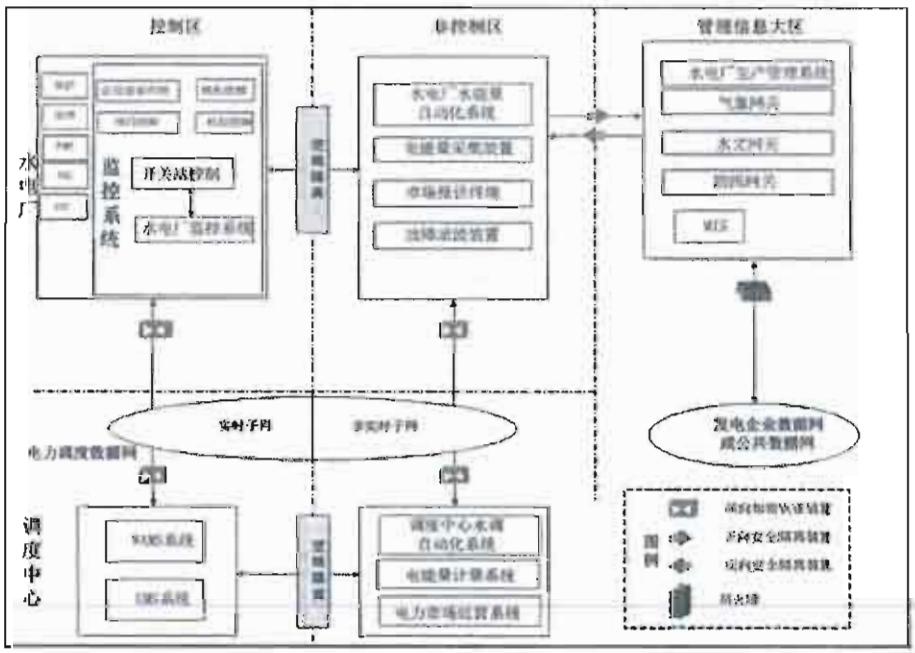

图 2 水电厂监控系统安全部署示意图

当水电厂监控系统与监控中心或梯级调度中心之间通过广域网络连接时，应当采取纵向加密认证措施进行安全防

护。梯级水电厂的安全防护部署如图 3 所示。

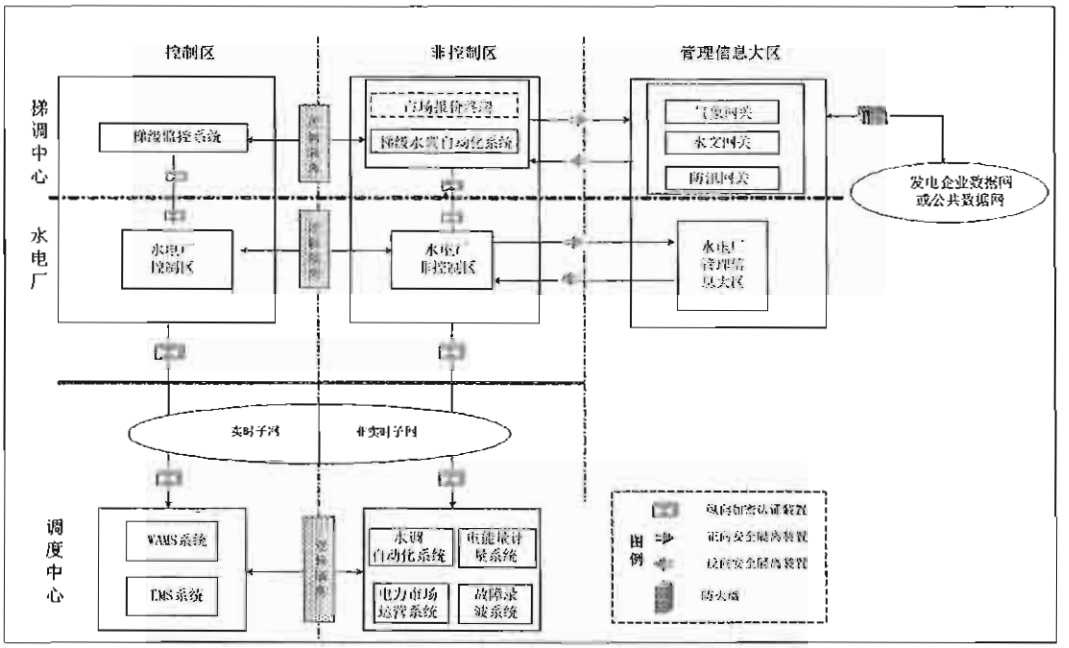

图 3 梯级水电厂监控系统安全部署示意图

核电站监控系统安全分区及边界防护如图 4 所示。

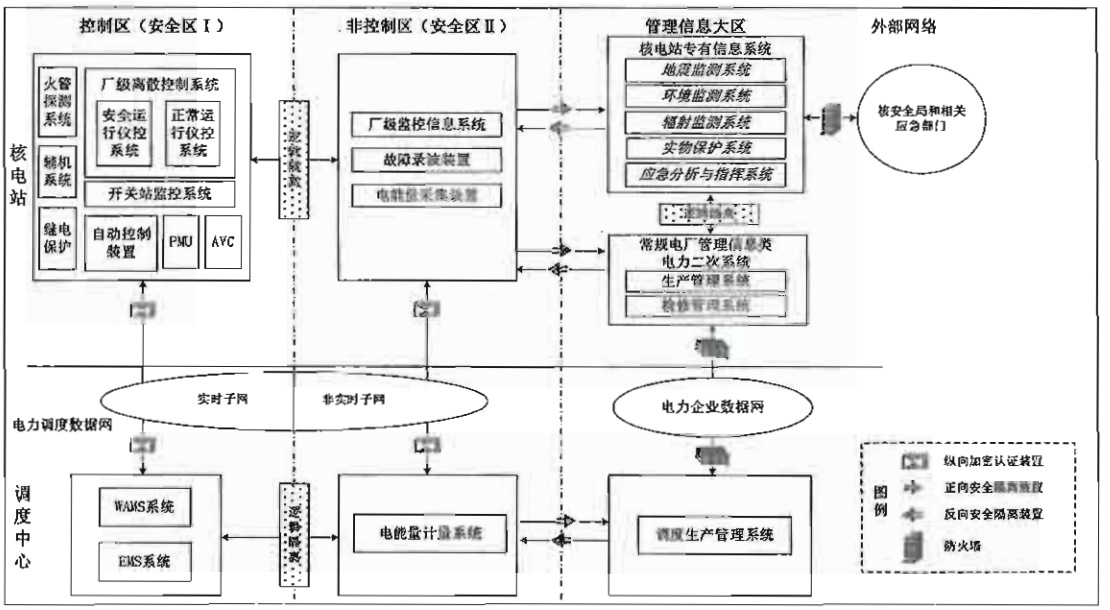

图 4 核电站监控系统安全部署示意图

风电场监控系统安全分区及边界防护如图 5 所示。

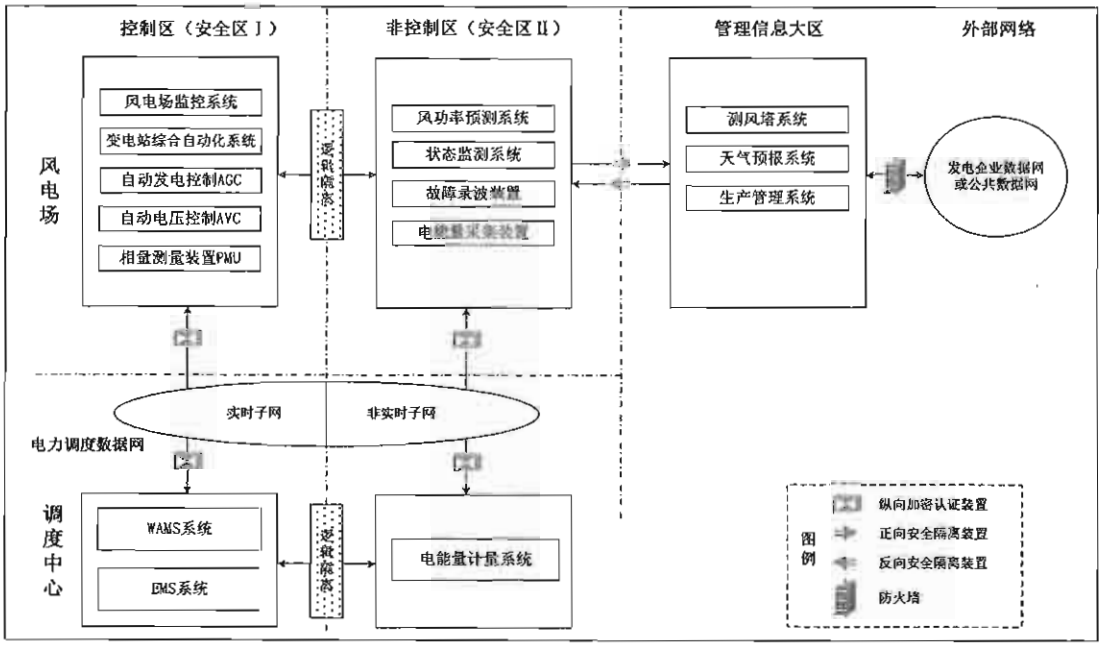

图 5 风电场监控系统安全部署示意图

光伏电站监控系统安全分区及边界防护如图 6 所示。

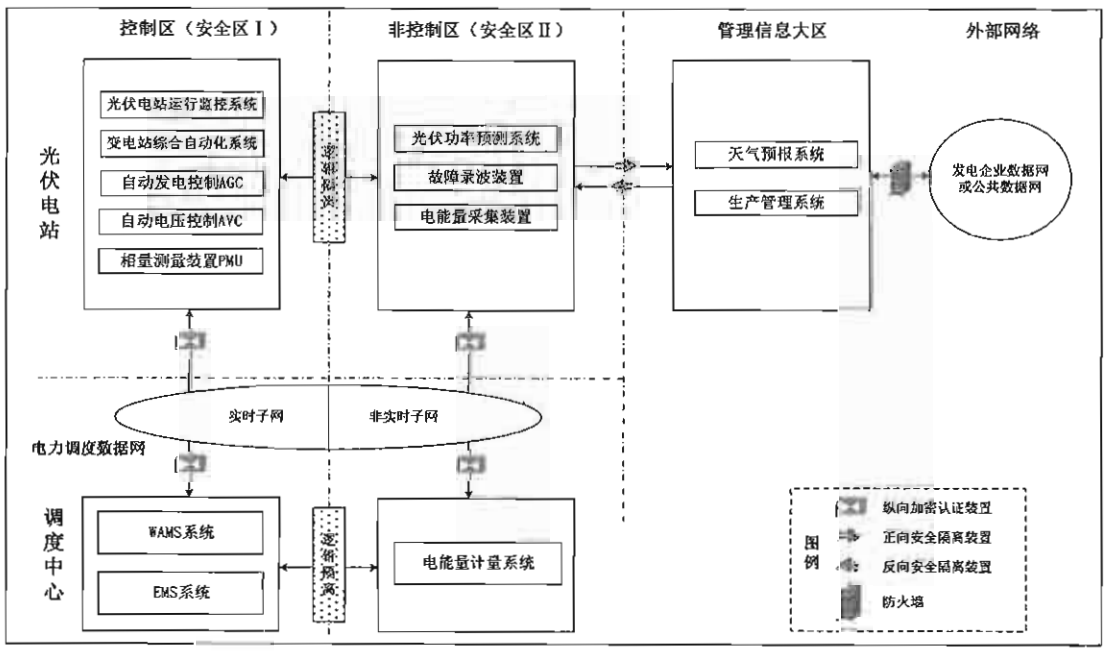

图 6 光伏电站监控系统安全部署示意图

燃机电厂监控系统安全分区及边界防护如图 7 所示。

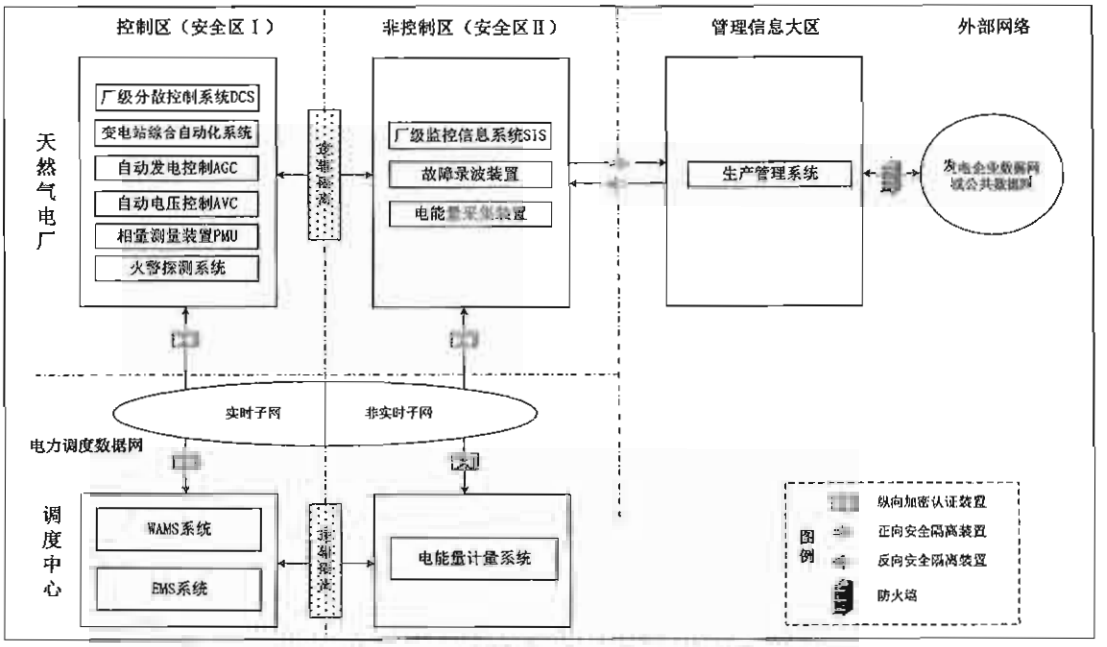

图 7 燃机电厂监控系统安全部署示意图

附录 3　用语的含义

安全接入区：如果生产控制大区内个别业务系统或其功能模块（或子系统）需使用公用通信网络、无线通信网络以及处于非可控状态下的网络设备与终端等进行通信，其安全防护水平低于生产控制大区内其他系统时，应设立安全接入区。安全接入区不是独立分区，与生产控制大区相连时，应当采用电力专用横向单向安全隔离装置进行集中互联。

附录 4　主要术语中英文对照

DCS (Distributed Control System)：分散控制系统

AGC (Automatic Generation Control)：自动发电控制

AVC (Automatic Voltage Control)：自动电压控制

PMU (Phasor Measurement Unit)：相量测量装置

PSS (Power System Stabilizer)：电力系统稳定器

TCS (Turbine Control System)：燃气轮机控制系统

SIS (Supervisory Information System)：厂级信息监控系统

OA (Office Automation)：办公自动化系统

MIS (Management Information System)：管理信息系统

VLAN (Virtual Local Area Network)：虚拟局域网

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)：超文本传输安全协议

PLC (Programmable Logic Controller)：可编程逻辑控制器

RTU (Remote Terminal Unit)：远方终端装置

附件 5:

变电站监控系统安全防护方案

1 总则

1.1 为了加强变电站监控系统安全防护，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》、《信息安全等级保护管理办法》及国家有关规定，制定本方案。

1.2 本方案是与《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》、《地（县）级调度中心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 变电站监控系统的防护目标是抵御黑客、病毒、恶意代码等通过各种形式对变电站监控系统发起的恶意破坏和攻击，以及其它非法操作，防止变电站监控系统瘫痪和失控，并由此导致的变电站一次系统事故。

1.4 变电站监控系统安全防护的重点是强化变电站边界防护，加强物理、人员等内部安全措施，保障变电站安全稳定运行。

1.5 本方案适用于变电站、换流站、开关站监控系统安全防护，包括发电厂的升压站或开关站；集控中心或集控站的

集中监控系统的安全防护可以参照《地（县）级调度中心监控系统安全防护方案》执行。

2 典型结构

变电站监控系统主要包括：监控系统、广域相量测量装置（PMU）、五防系统、继电保护、安全自动装置、故障录波装置、辅助设备监控、电能量采集装置和一次设备在线监测等；换流站还包括阀控系统及站间协调控制系统等，有人值班变电站还有生产管理系统终端等；集控站还包括对受控变电站的监控系统等。变电站监控系统逻辑结构如图 1。

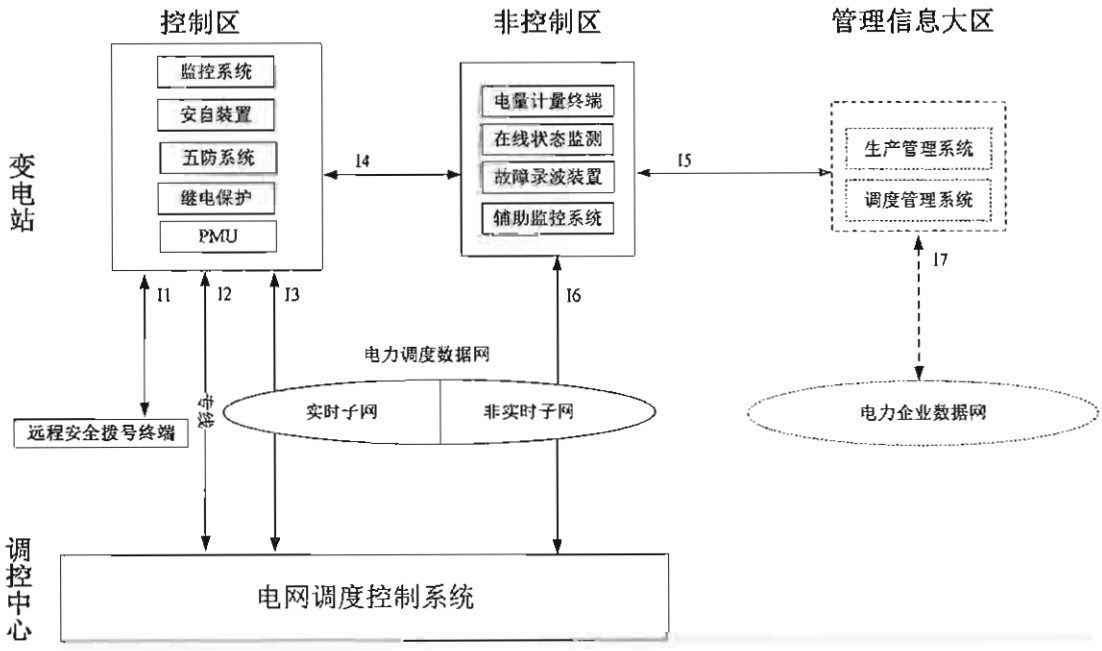

图 1 变电站监控系统典型逻辑结构示意图

根据所用技术和设备的不同，数字化变电站与常规变电站在监控系统结构上存在差异。

数字化变电站监控系统在网络结构上由站控层、间隔层、过程层三个层次组成，全站网络采用高速以太网。站控层网络负责实现站控层设备之间以及与间隔层之间的通信；间隔层网络负责实现间隔层设备之间、间隔层与站控层之间的通信；过程层网络负责实现过程层设备之间、过程层与间隔层之间的通信。数字化变电站内涉及远方控制功能的装置及设备应采用加密及身份认证等安全防护措施。数字化变电站监控系统安全部署结构如图 2 所示。

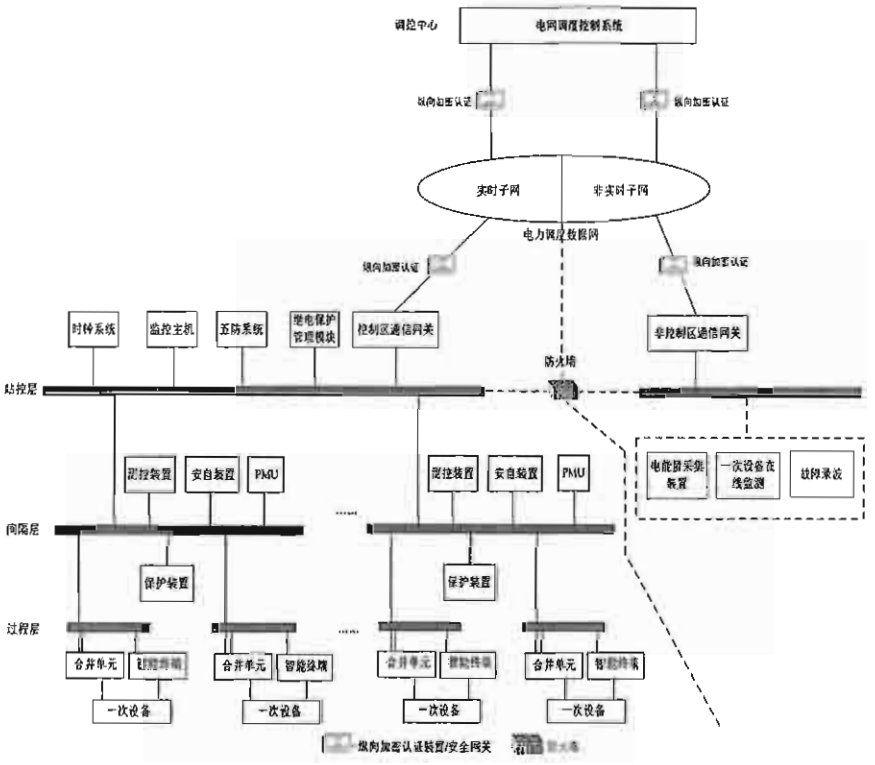

图 2　数字化变电站监控系统安全部署结构示意图

3　安全分区

按变电站的电压等级、规模、重要程度的不同以及变电

站运行模式（有人值班模式、无人值班少人值守模式、无人值守模式等）差别，变电站监控系统的安全区划分应该根据实际情况确定。220 千伏及以上变电站监控系统的生产控制大区应当设置控制区和非控制区；对于 110 千伏及以下变电站，其监控系统生产控制大区可以不再进行细分，相当于只设置控制区。

变电站监控系统安全分区详见表 1。

表 1 变电站电力监控系统安全分区表

序号	业务应用或设备	控制区	非控制区	管理信息大区
1	变电站监控系统	变电站监控系统		
2	五防系统	五防系统		
3	广域相量测量装置	广域相量测量装置		
4	继电保护	继电保护装置及管理模块		
5	安全自动控制	安自装置及管理模块		
6	火灾报警	火灾报警		
7	电能量采集装置		电能量采集装置	
8	故障录波		故障录波装置	
9	一次设备在线监测		一次设备在线监测	
10	辅助设备监控		辅助设备监控	
11	生产管理			生产管理终端

4 安全部署

根据《电力监控系统安全防护总体方案》的原则对变电

站监控系统进行逻辑边界分析，安全分区及安全部署如图 3 所示。

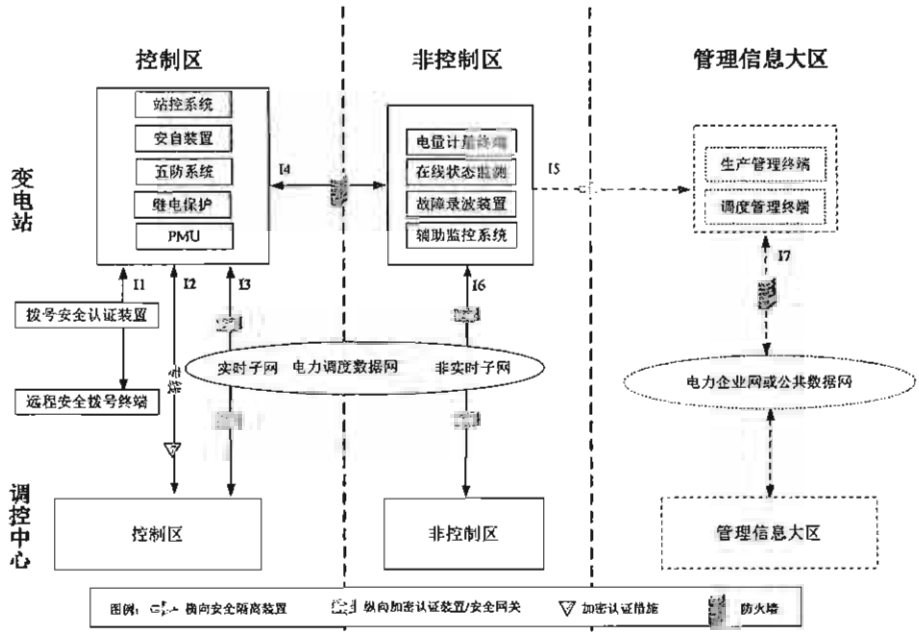

图 3　变电站监控系统安全部署示意图

图 3 中所列出的逻辑接口（I1-I7）的描述见表 2。

表 2　变电站监控系统的逻辑接口

序号	名称	数据类型	通信方式和规约
I1	厂商的远程维护接口	厂商通过拨号方式远程维护变电站监控系统，数据类型不定。	电话拨号 TCP/IP
I2	通过专线通道连接变电站自动化系统的接口	1．实时监控数据：遥信、遥测、遥控和遥调等数据 2．继电保护数据：继电保护的远方投退和远方设置命令、继电保护装置信息	专线 专用协议
I3	通过网络连接变电站自动化系统的接口	1．实时监控数据：遥信、遥测、遥控和遥调等数据 2．广域测量数据：带时标的 PMU 数据	电力调度数据网 TCP/IP IEC60870-5-101、104 TASE.2

		3．继电保护数据：继电保护的远方投退和远方设置命令、继电保护装置信息	DL476-92 IEC61850 等专用协议
I4	控制区与非控制区间的通信接口	控制区与非控制区之间数据交互	本站局域网 TCP 或 UDP IEC61850
I5	生产控制大区与管理信息大区间的通信接口	生产控制大区与管理信息大区之间数据交互	本站局域网 TCP 或 UDP IEC61850
I6	非控制区的纵向通信接口	1．一次设备在线监测信息 2．故障录波信息 3．辅助设施监控信息 4．电能量计量数据	电力调度数据网 TCP 或 UDP IEC61850 IEC60870-5-102、103 COMSTRAT 等专用协议
I7	站内管理信息大区与电力企业相应管理系统间的接口	1．生产管理系统信息 2．调度管理系统信息	电力企业数据网 TCP/IP

除了图 3 及表 2 中所描述的逻辑接口以外，还有发电厂升压站或开关站的监控系统与发电厂监控系统之间的逻辑接口，集控站的集控功能部分与被控制的变电站监控系统之间的逻辑接口。

对于 220 千伏以上的变电站监控系统，应该在变电站层面构造控制区和非控制区，继电保护管理模块及安自装置管理模块应当置于控制区，故障录波装置、电能量采集装置和在线状态监测置于非控制区。

对于110千伏及以下变电站的监控系统，其生产控制大区可以不再细分，可以将各业务系统和装置均置于控制区，其中在控制区中的故障录波装置和电能量采集装置可以通过调度数据网将录波数据及计量数据传输到上级调控中心。

在与调控中心数据通信的生产控制大区纵向边界处，110千伏及以上变电站均应当部署纵向加密认证装置，110千伏以下变电站应当采用符合国家安全要求的认证技术实现身份认证，可以采用微型纵向加密认证器的方式实现。

具有远方遥控功能的业务（如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。

当采用专用通道和专用协议进行非网络方式的数据传输时，可以采取加密认证等安全防护措施。

加强变电站，尤其是无人值班变电站的物理安全保护和现场设备的运行管理，防止无关人员接近自动化、继电保护和电力通信相关设备。

隶属于电网公司的变电站监控系统等级保护工作纳入所属电网调度机构统一开展，作为调度自动化系统子站部分统一定级备案，不作为独立系统定级备案，并保持防护标准不变，220千伏及以上变电站自动化系统仍按等级保护3级要求防护；其它产权的变电站监控系统等级保护工作由产权方负责。

变电站监控系统在设备选型及配置时，应当禁止选用经

国家相关管理部门检测认定并经国家能源局通报存在漏洞和风险的系统及设备；对于已经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统及设备的运行管理和安全防护。生产控制大区中除安全接入区外，应当禁止选用具有无线通信功能的设备。

附录　主要术语中英文对照

IEC 61850：变电站数据通信协议体系
DL476-92：电力系统实时数据通信应用层协议
IEC 60870-5：远动设备及系统第 5 部分传输规约
TASE.2：远动应用服务元素
TCP/IP（Transaction Control Protocol/Internet Protocol）：互联网传输协议

附件 6:

配电监控系统安全防护方案

1 总则

1.1 为了加强配电监控系统安全防护，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 本方案是与《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》、《地（县）级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》和《电力监控系统安全防护评估规范》。

1.3 配电监控系统的防护目标是抵御黑客、恶意代码等通过各种形式对配电监控系统发起的恶意破坏和攻击，以及其它非法操作，防止配电监控系统瘫痪和失控，并由此导致的配电网一次系统事故。

1.4 本方案重点描述配电网调度自动化、负荷控制管理等具有控制功能的业务系统的安全防护，保证配电监控系统的安全，提高供电可靠性。

1.5 本方案适用于配电监控系统安全防护。

2 典型结构

配电监控系统主要包括：配电网调度自动化系统、电力负荷控制管理系统、调度地理信息系统及其他业务系统功能（如配网生产抢修指挥、电网地理信息、电力营销管理、生产管理、客户服务、用电信息采集等），以及相连的局域网和广域网。配电网调度自动化系统和电力负荷控制管理系统具有控制功能，有实时性要求，而其它系统不具备控制功能，无实时性要求。其中，电力负荷控制管理系统属于营销系统，与生产控制大区相关调度业务系统无网络联系，独立存在。

配电监控系统典型应用系统结构如图 1 所示：

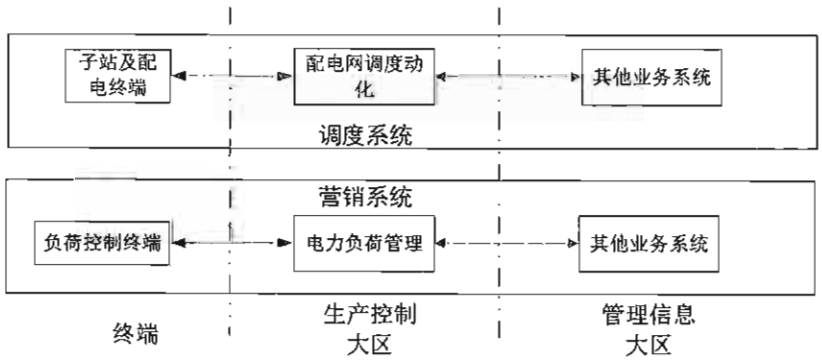

图 1 配电监控系统典型应用系统结构示意图

3 安全分区

鉴于配电监控系统涉及面广，地区差异较大，为减少防护成本，降低实施风险，应当简化安全区设置，重点防护具有直接控制功能的系统。将各业务系统分别置于生产控制大区和管理信息大区。

生产控制大区主要包括具有控制功能的配电网调度自动化系统、电力负荷控制管理系统、低频低压减负荷装置、电能量采集装置等，对于配电网调度自动化系统、电力负荷控制管理系统中采用公网作为数据采集控制方式的前置机及终端应当置于安全接入区。

当用电采集系统实现对用户电表等设施实施远方控制时，应当采取必要的安全认证措施，尽量实行局部控制。

管理信息大区主要包括配网生产抢修指挥、管理地理信息、生产管理、电力营销管理、客户服务、用电信息采集等功能，管理信息大区统一实施安全防护。安全分区如表1所示。

表1配电监控系统及其配套管理信息系统安全分区表

序号	业务功能	控制区	非控制区	管理信息大区
1	配电网调度自动化	SCADA、高级应用		
2	配电生产抢修指挥			配网生产抢修
3	电力负荷控制管理	负荷采集及控制		
4	电能量采集	电能量采集		
5	低频低压减负荷	低频低压减负荷		
6	电网地理信息	调度地理信息		管理地理信息
7	电力营销管理			营销管理
8	客户服务			客户服务管理
9	用电信息采集			用电信息采集
10	生产管理			生产管理

4 安全部署

本章仅对典型配电监控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。根据电力监控系统安全防护总体方案的原则，对配电网调度自动化系统和电力负荷控制管理系统进行逻辑边界分析及安全防护部署，如图 2 所示：

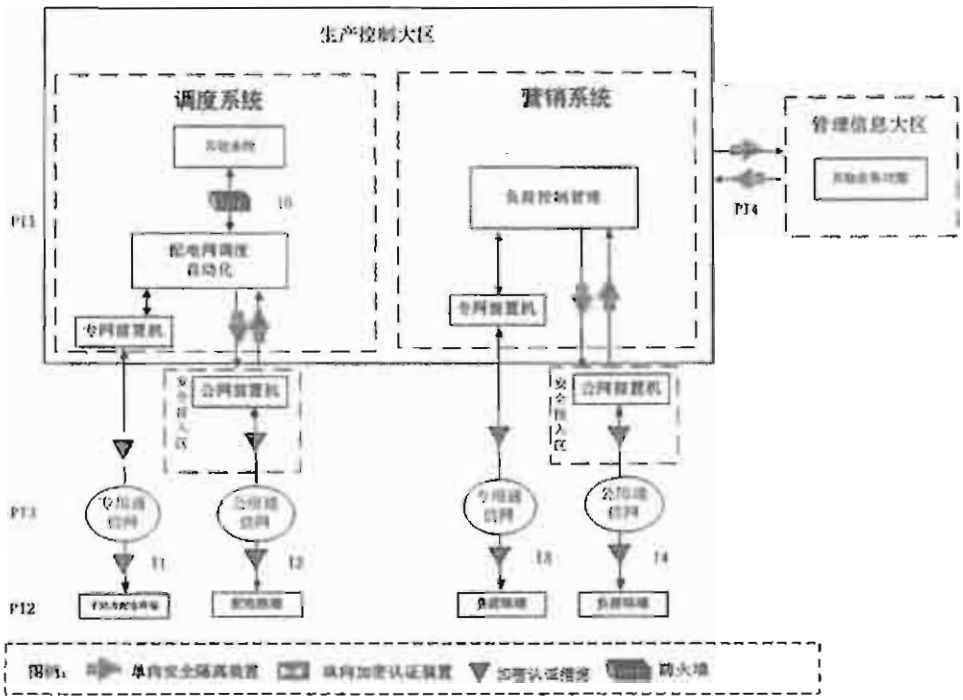

图 2 配电监控系统安全部署示意图

安全部署图中所指的逻辑接口（I0-I5）的描述见表 2。

表 2 配电监控系统逻辑接口描述表

序号	名称	数据类型	通信方式及协议
I0	与其他系统接口	实时信息（遥测、遥信）、地理信息	本地局域网 TCP/IP
I1	专用网络连接子站及配电终端	实时数据：遥信、遥测、遥控等信息	专用数据网 专用协议
I2	通过公网通道连接的	实时遥测、遥信、遥控等信	公用数据网

	配电终端	息	专用协议
I3	通过专用网络连接负荷终端的接口	实时数据： 1、终端的遥信、遥测 2、负荷的计算数据等信息	专用数据网 专用协议
I4	通过公网连接负荷终端	实时数据： 1、终端的遥信、遥测 2、负荷的计算数据等信息	公用数据网 专用协议
I5	与管理信息大区接口	1、用户信息（实时信息和设备信息） 2、地理信息 3、计算数据等 4、抄表信息、工作管理信息等	本地局域网 TCP/IP

按照配电网调度自动化系统典型的结构，安全防护分为以下四个部分，负荷控制管理等系统参照执行。

（1）主站的安全防护（PI1）；

（2）子站终端的安全防护（PI2）；

（3）纵向通信的安全防护（PI3）；

（4）横向边界的安全防护（PI4）。

4.1 主站的安全防护（PI1）

配电网调度自动化系统与本级调度自动化或其他系统通信时应当采用逻辑隔离防护措施，保障调度自动化系统安全。

无论采用何种通信方式，自动化系统主站至少前置机应当采用经国家指定部门认证的安全加固的操作系统，并采取

严格的访问控制措施。

在前置机应当配置安全模块，对控制命令和参数设置指令进行签名操作，实现子站对主站的身份鉴别与报文完整性保护；对重要子站及终端的通信可以采用双向认证加密，实现主站和子站间的双向身份鉴别，确保报文机密性和完整性。对于采用公网作为通信信道的前置机，公网前置机属于安全接入区，必须采用电力专用的正反向隔离装置与自动化系统进行隔离。

4.2 子站终端的安全防护（PI2）

在子站终端设备上配置安全模块，对来源于主站系统的控制命令和参数设置指令采取安全鉴别和数据完整性验证措施，以防范冒充主站对终端进行攻击，恶意操作电气设备。为增加安全性，对重要子站及终端可以配置具有双向认证加密能力的安全模块，实现主站和子站终端间的双向身份鉴别和数据加密。

对于能被手持设备控制或配置的配电终端，应当采用严格的访问控制措施；终端与手持设备应当采用安全的通讯措施并采用符合国家要求的非对称加密算法的身份认证措施；对用户登录的口令强度进行严格要求。

子站终端设备应当具有防窃、防火、防破坏等物理安全防护措施。

4.3 纵向通信的安全防护（PI3）

配电网调度自动化系统主站与子站及终端的通信方式原则上以电力光纤通信为主，主站与主干配电网开闭所的通信应当采用电力光纤，在各种通讯方式中应当优先采用EPON接入方式的光纤技术。对于不具备电力光纤通信条件的末梢配电终端，采用无线通信方式。

无论采用何种通信方式，应当对控制指令与参数设置指令使用基于非对称加密算法的认证加密技术进行安全防护，实现配网终端对主站的身份鉴别与报文完整性保护。对重要子站及终端的通信可以采用双向认证加密技术，实现配网终端和主站之间的双向身份鉴别，确保报文的机密性、完整性保护。

当采用 EPON、GPON 或光以太网络等技术时应当使用独立纤芯或波长。

当采用 GPRS/CDMA 等公共无线网络时，应当启用公网自身提供的安全措施，包括:

1）采用 APN+VPN 或 VPDN 技术实现无线虚拟专有通道;

2）通过认证服务器对接入终端进行身份认证和地址分配;

3）在主站系统和公共网络采用有线专线+GRE 等手段。

当采用 230MHz 等电力无线专网时，可以采用相应安全防护措施。

4.4 横向边界的安全防护（PI4）

根据《电力监控系统安全防护总体方案》要求，在生产控制大区与管理信息大区之间必须部署经国家指定部门监测认证的电力专用单向横向隔离装置，隔离强度应当接近或达到物理隔离。生产控制大区内部安全区之间应当采用具有访问控制功能的网络设备、防火墙或者相当功能的设施，实现逻辑隔离。

附录主要术语中英文对照

SCADA(Supervisory Control And Data Acquisition)：监控和数据采集
EPON(Ethernet Passive Optical Network) 以太无源光网络
GPON(Gigabit-Capable Passive Optical Network) 千兆比特无源光网络
GPRS（General Packet Radio Service) 通用分组无线服务技术
CDMA(code-division multiple access) 码分多址
APN(Access Point Name) 接入点
VPN（Virtual Private Network) 虚拟专用网络
VPDN(Virtual Private Dial－up Networks) 虚拟专用拨号网
GRE(generic route encapsulation) 通用路由封装
TCP/IP（Transaction Control Protocol/Internet Protocol）互联网传输协议

附件 7:

电力监控系统安全防护评估规范

1 范围

本规范规定了电力监控系统安全防护评估的总体要求、工作形式、评估内容、评估方法、实施流程和评价标准等，适用于各电力企业电力监控系统的安全防护评估工作。

2 引用标准与规范

下列文件中的条款通过在本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，鼓励根据规范达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本规范。

- 《电力监控系统安全防护规定》（国家发展改革委 2014 年第 14 号令）
- 《电力监控系统安全防护总体方案》
- 《省级以上调度中心监控系统安全防护方案》
- 《地县级调度中心监控系统安全防护方案》
- 《发电厂监控系统安全防护方案》
- 《变电站监控系统安全防护方案》
- 《配电监控系统安全防护方案》
- 《GB/T 22239-2008 信息安全技术 信息系统安全等级

保护基本要求》

- 《信息安全等级保护管理办法》（公通字[2007]43号）
- 《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》
- 《GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南》
- 《GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南》
- 《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》
- 《GB/T 28448-2012 信息系统安全等级保护测评要求》
- 《GB/T 28449-2012 信息系统安全等级保护测评过程指南》
- 《关于开展电力行业信息系统安全等级保护定级工作的通知》（电监信息[2007]34号）
- 《电力行业信息系统等级保护定级工作指导意见》（电监信息[2007]44号）
- 《电力行业信息系统安全等级保护基本要求》（电监信息[2012]62号）

3 术语和定义

电力监控系统

电力监控系统，是指用于监视和控制电力生产及供应过

程的、基于计算机及网络技术的业务系统及智能设备，以及做为基础支撑的通信及数据网络等。

组织

由作用不同的个体为实施共同的业务目标而建立机构。一个单位是一个组织，某个业务部门也可以是一个组织。

资产

指在电力监控系统建设和运行过程中积累起来的具有价值的信息或资源，是安全策略的保护对象。

资产价值

指资产对电力监控系统的重要程度，以及对电力监控系统完成相关电力生产工作的重要程度。资产价值是资产的属性，也是进行资产识别的主要内容。

威胁

电力监控系统资产可能受到的来自内部和外部的安全侵害。

脆弱性

电力监控系统资产及其防护措施在安全方面的不足，通常也称为漏洞。脆弱性可能被威胁利用，并对电力监控系统资产造成损害。

安全事件

人为或自然的威胁利用电力监控系统及其管理体系中存在的脆弱性导致的不安全状况。

信息安全风险

安全事件发生的可能性及其潜在的影响。

残余风险

采取了安全防护措施，提高了防护能力后，仍然可能存在的风险。

安全措施

保护资产，抵御威胁，减少脆弱性，降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

型式安全评估

电力监控系统设计、开发完成后，系统供应商自行组织或委托评估机构对系统进行的安全评估。

上线安全评估

电力监控系统投运前及发生重大变更时，运行单位自行组织或委托评估机构对系统进行的安全评估。

自评估

运行单位对本单位电力监控系统组织实施的安全评估，以及调度机构在调度管辖范围内（以下简称“调管范围内”）各运行单位自评估结果基础上，对调管范围内电力监控系统组织实施的安全评估。

检查评估

由国家能源局及其派出机构（以下简称“能源监管机构”）组织或委托安全评估机构对电力行业监控系统进行的

具有强制性的安全评估。

4 安全评估管理

4.1. 总体要求

电力监控系统安全防护评估工作应当常态化、定期进行。电力监控系统的规划、设计阶段要进行安全评审，建设改造、运行维护和废弃阶段均要进行安全评估，确保系统全生命周期安全性。

4.2. 评估工作形式

电力监控系统安全防护评估有四种工作形式：自评估、检查评估、上线安全评估和型式安全评估。各种形式评估均应当遵循《电力监控系统安全防护总体方案》及国家等级保护相关要求等规范性文件，在不影响电力监控系统生产业务的基础上实施。

部署了安全保护等级为4级和3级业务系统的安全区，应当由运行单位结合等级保护工作委托评估机构定期开展安全评估工作，评估周期最长不超过三年。在此期间，运行单位应当定期组织开展自评估工作，以确保不因系统调整而造成系统安全性降低的情况发生，评估周期原则上不超过一年。自评估以脆弱性评估为主，评估的项目、要点见附录B。

仅部署安全保护等级为2级业务系统的安全区，应当由运行单位定期组织开展自评估工作，评估周期最长不超过两

年，也可以根据情况委托评估机构开展自评估工作。

调度机构应当在定期收集、汇总调管范围内各运行单位自评估结果的基础上，自行组织或委托评估机构开展调管范围内电力监控系统的自评估工作。省级以上调度机构的自评估周期最长不超过三年；地级及以下调度机构自评估周期最长不超过两年。

能源监管机构可以根据实际情况对各运行单位的电力监控系统或调度机构调管范围内的电力监控系统组织开展检查评估。

安全保护等级为 4 级和 3 级的电力监控系统在设计、开发完成后，应当委托评估机构进行型式安全评估，安全保护等级为 2 级的应当自行组织开展型式安全评估。各单位安全保护等级为“4 级和 3 级”的电力监控系统投运前或发生重大变更时，应当委托评估机构进行上线安全评估，安全保护等级为 2 级应当自行组织开展上线安全评估。

检查评估、型式安全评估、上线安全评估主要包括资产识别、威胁分析、脆弱性分析、风险分析和安全建议等，其中脆弱性分析项目、要点包括但不限于附录 B，评估方法应符合国家、行业标准规范，评估报告模板见附录 E。评估工作角色和职责

4.3. 评估工作角色和职责

电力监控系统安全防护评估工作涉及能源监管机构、上

级主管部门、运行单位、调度机构、供应商、评估机构等角色。各角色在评估中承担不同的职责，如表 4-1 所示。其中受委托开展电力监控系统安全防护评估工作的评估机构，其评估人员应当经过能源监管机构培训合格，同时还应当具备国家等级保护测评资质。

表 4-1　电力监控系统安全防护和等级保护评估角色职责

安全评估相关角色	职责
能源监管机构	对评估机构的资质进行审核 发起检查评估工作 监管电力企业的评估开展情况 检查或督导评估整改方案落实情况
上级主管部门	发起下属单位的自评估工作 监督下属单位安全评估实施过程 检查下属单位安全评估整改方案落实情况
运行单位	发起本单位的自评估工作 参加评估方案等文档的评审工作 按照评估规范实施自评估 配合检查评估实施工作 根据安全评估结果落实整改方案 系统投运前及发生重大变更时实施上线安全评估，运行单位总体负责相关工作，可委托评估机构进行评估
调度机构	发起调管范围内的自评估工作 收集、汇总调度管辖范围内各运行单位的自评估结果 参加评估方案等文档的评审工作 按照评估规范组织实施调管范围内电力监控系统的自评估 配合开展调管范围内的检查评估工作 根据安全评估结果督促、落实整改方案
系统供应商	系统设计、开发完成后实施型式安全评估 配合完成系统上线的安全评估 在运行维护阶段支持、配合安全评估工作 配合执行安全评估整改工作
评估机构	编制安全评估实施方案 自行组织评审评估实施方案 实施安全评估 出具安全评估报告，提出整改建议 自行组织评审评估结果

4.4. 保密管理

应当加强对评估资料和评估结果的管理，按照国家及被评估单位的相关要求做好保密工作，确保评估机构和人员可靠、稳定和可控，确保评估过程中产生、接触的所有记录、数据与评估结果安全、保密、可控。评估工作采取以下控制措施：

（1）签署保密协议

项目实施前，评估机构应当与被评估单位签订保密协议，明确双方的保密责任。

（2）最小接触原则

项目实施工作中，项目组必须接触、使用被评估单位敏感信息时，评估机构应当遵循最小接触原则。仅授权必不可少的人员可接触到相关信息。

（3）职业道德

评估机构应当保证评估项目参与人员具有良好的职业道德，相关人员无违法犯罪记录，未发生过违反职业道德的情况。

（4）人员保密管理

应当确保参与评估项目的人员均与评估机构签署保密协议。项目人员对工作过程中接触、产生的数据以及评估结果应当严格保密，未经授权不得泄露给任何第三方。项目人员不得利用项目过程中接触、产生的数据进行任何侵害被评

估单位网络信息系统的行为。

（5）设备保密管理

评估机构项目组应当根据被评估单位的需要，使用专用的办公设备进行工作，禁止将被评估单位的任何设备带出允许的办公场地，项目完成以后，立即归还。

（6）文档保密管理

评估项目组应当采取加密的方式进行项目组内、项目组与被评估单位间的数据交换。依据被评估单位的要求，评估机构应当对项目有关文档、数据、资料设置保密期，在保密期结束后，应当使用可信的方式彻底销毁有关数据与文件资料。评估机构应当保证不在任何第三方场合与第三方文档中发布或引用被测系统信息。

4.5. 风险控制

安全评估工作本身也会引入安全风险，必须加强安全评估实施过程中的风险控制。电力监控系统安全防护评估工作实施前，应当根据确定的评估范围，对评估过程中可能引入的风险进行分析，并制定应对措施。评估实施过程的风险控制手段主要包括：

（1）操作的申请和监护

在实施过程中，评估操作必须遵守电力系统的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

（2）操作时间控制

对直接涉及电力生产的电力监控系统的评估工作，尽可能避开电力生产敏感时期。

（3）制定应急预案

根据评估范围界定的电力监控系统情况，在被评估单位的配合下，由评估机构在评估实施前制定应急预案。

（4）运行系统模拟环境

在对电力关键业务系统评估时，电力企业能够提供备用设备搭建临时模拟测试环境的，应优先考虑模拟真实系统的结构、配置、数据、业务流程，以保证评估的真实性和运行系统的安全、稳定。

（5）关键业务系统风险控制

对位于生产控制大区内的电力监控系统在无法搭建模拟环境的情况下，原则上不采用评估工具进行评估，采用人工评估的方式进行。

（6）其他

评估实施中，为防止发生影响系统运行的安全事件，应当根据评估对象的不同采取相应的风险控制手段。

5 安全评估基本内容

本章主要描述自评估、检查评估、上线安全评估和型式安全评估共有的基本内容和流程。评估的内容、方法和流程见附录C。

5.1. 评估原则

针对电力监控系统安全防护的特点，设置如下必须满足的基本要求：

（1）安全分区。发电企业、电网企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区。生产控制大区可以分为控制区（又称安全区Ⅰ）和非控制区（又称安全区Ⅱ）；管理信息大区内部在不影响生产控制大区安全的前提下，可以根据各企业不同安全要求划分安全区。

根据应用系统实际情况，在满足总体安全要求的前提下，可以简化安全区的设置，但是应避免形成不同安全区的纵向交叉联接。

（2）网络专用。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电力企业其它数据网及外部公共数据网的安全隔离。

电力调度数据网划分为逻辑隔离的实时子网和非实时子网，分别连接控制区和非控制区。

（3）横向隔离。在生产控制大区与管理信息大区之间必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

生产控制大区内部的安全区之间应当采用具有访问控制功能的设备、防火墙或者相当功能的设施，实现逻辑隔离。

安全接入区与生产控制大区中的联接处必须设置经国家指定部门检测认证的电力专用横向单向安全隔离装置。

（4）纵向认证。在生产控制大区与广域网的纵向联接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施。

上述任何一项要求未满足即为不合格。

在上述基本要求都满足情况下，参照附录B开展电力监控系统安全防护评估。

5.2. 风险分析

风险分析主要包括数据整理、风险计算和风险决策三个步骤。

数据整理是将资产调查、威胁分析、脆弱性分析中采集到的数据按照风险计算的要求，进行分析和整理的过程。

风险计算是在完成资产评估、威胁评估和脆弱性评估后，根据资产赋值、资产面临的威胁和存在的脆弱性赋值情况对资产面临的风险进行分析和计算。

计算风险值公式为：

$$风险值 = R(A, T, V)$$

其中：R表示安全风险计算函数；A表示资产；T表示威胁；V表示脆弱性。评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。

风险决策是在风险排序的基础上，分析各种风险要素、

评估系统的实际情况、计算消除或降低风险所需要的成本，决定对风险采取接受、消除或转移等处理方式的过程。风险决策是提出安全建议的基础，科学、合理的风险决策是提高安全建议质量、防止过度防护和防护不足的保障。

6 系统生命周期各阶段的安全评估

电力监控系统生命周期包含五个基本阶段：规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。安全评估工作应当贯穿于电力监控系统整个生命周期，其中规划阶段、设计阶段应当结合规划审查及设计审查进行安全评审，实施阶段、运行维护阶段和废弃阶段需结合本阶段的实际情况开展安全评估。

6.1. 规划阶段

规划阶段安全评审工作应当根据电力监控系统的业务使命、功能，确定系统建设应达到的安全目标。

本阶段评审主要是对根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行威胁分析；重点分析系统应该达到的安全目标。

规划阶段的评审结果应当包含在电力监控系统整体规划中。

6.2. 设计阶段

设计阶段的安全评审需要根据规划阶段所明确的系统

安全目标，对系统设计方案的安全功能设计进行判断，以确保设计方案满足系统安全目标，并作为采购过程风险控制的依据。

设计阶段的评审结果最终应当体现在系统设计方案中。

6.3. 实施阶段

实施阶段安全评估的目的是根据系统安全需求和运行环境对系统开发实施过程进行安全风险识别，并对系统建成后的安全功能进行验证。根据设计阶段分析的威胁和建立的安全控制措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施以及评估开发过程中对上述要求的保障，实施阶段应当对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定上述安全措施能否抵御现有威胁、脆弱性的影响，并对源代码进行安全测评，提高代码安全性。在系统投运前，运行单位应当自行组织或委托评估机构对系统进行上线安全评估。实施阶段安全评估主要对系统的开发与技术或产品获取、系统交付实施两个过程进行评估。

6.4. 运行维护阶段

运行维护阶段安全评估的目的是掌握和控制电力监控系统运行过程中的安全风险，包括在线运行电力监控系统资产、威胁、脆弱性等各方面评估，是一种较为全面的安全评估。

运行维护阶段的安全评估应当常态化开展。电力监控系统业务流程、系统状况发生重大变更时，也需要及时进行安全评估。重大变更包括:

（1）增加新的应用或应用发生较大变更;

（2）网络结构和连接状况发生较大变更，例如，系统升级改造、新机房投入使用或局域网、广域网结构发生较大变化时;

（3）技术平台大规模的更新;

（4）系统扩容或改造;

（5）发生重大安全事件后，或存在发生重大安全事件的隐患;

（6）系统运行维护管理机构或人员发生较大规模调整。

6.5. 废弃阶段

电力监控系统的废弃阶段可以分为部分废弃和全部废弃，废弃阶段安全评估包括:

（1）系统软、硬件等资产及残留信息的废弃处置;

（2）废弃部分与其他系统（或部分）的物理或逻辑连接情况;

（3）在系统变更时发生废弃，还应当对变更的部分进行评估。

本阶段应当重点分析废弃资产对组织的影响，对由于系统废弃可能带来的新的威胁进行分析。

附录 A 电力监控系统安全防护定级表

类别	定级对象	系统级别	
		省级以上	地级及以下
电力监控系统	能量管理系统（具有 SCADA、AGC、AVC 等控制功能）	4	3
	变电站自动化系统（含开关站、换流站、集控站）	220 千伏及以上变电站为 3 级，以下为 2 级	
	火电厂监控（含燃气电厂）系统 DCS（含辅机控制系统）	单机容量 300MW 及以上为 3 级，以下为 2 级	
	水电厂监控系统	总装机 1000MW 及以上为 3 级，以下为 2 级	
	水电厂梯级调度监控系统	3	
	核电站监控系统 DCS（含辅机控制系统）	3	
	风电场监控系统	风电场总装机容量 200MW 及以上为 3 级，以下为 2 级	
	光伏电站监控系统	光伏电站总装机容量 200MW 及以上为 3 级，以下为 2 级	
	电能量计量系统	3	2
	广域相量测量系统（WAMS）	3	无
	电网动态预警系统	3	无
	调度交易计划系统	3	无
	水调自动化系统	2	
	调度管理系统	2	
	雷电监测系统	2	
	电力调度数据网络	3	2
	通信设备网管系统	3	2
	通信资源管理系统	3	2
	综合数据通信网络	2	
	故障录波信息管理系统	3	
	配电监控系统	3	
	负荷控制管理系统	3	
	新一代电网调度控制系统的实时监控与预警功能模块	4	3
	新一代电网调度控制系统的调度计划功能模块	3	2
	新一代电网调度控制系统的安全校核功能模块	3	2
	新一代电网调度控制系统的调度管理功能模块	2	

注：

1. 备用调度中心相关系统与主调系统同级别。

附录B 电力监控系统安全防护脆弱性评估表（主要指标）

B1 技术要求

B1.1 物理安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况[1]	备注
				3级、2级	4级		
1	物理位置的选择(G)	机房和办公场地的物理位置选择在防震、防风和防雨的建筑内	✓	✓	✓		
		机房避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁	—	✓	✓		
2	物理访问控制(G)	对机房划分区域进行管理，区域和区域之间设置物理隔离设施，在重要区域前设置交付或安装等过渡区域，将设备区域与维护操作区域分离	—	✓	✓		
		机房门禁系统具备人员授权分级管理、日志管理（含人员进出、时间、身份类型等信息）功能	✓	✓	✓		
		四级系统部署两道电子门禁系统	—	—	✓		
		进出机房建立相应的申请和审批流程	✓	✓	✓		
3	防盗窃和防破坏(G)	机房部署视频监控系统，覆盖所有关键区域（厂站仅要求在厂站内部署视频监控系统，不要求覆盖所有关键区域）	✓	✓	✓		
		重要设备机柜上锁处理	✓	✓	✓		
4	防雷击(G)	机房建筑设置避雷装置、防雷保安器和交流电源地线（厂站不要求部署防雷保安器）	✓	✓	✓		
5	防火(G)	机房在自动灭火、耐火材料、物理区域隔离等方面进行防护（厂站不要求自动灭火）	✓	✓	✓		
6	防水和防潮	机房设置措施防止外部雨水渗漏、水蒸汽结露和地下积水	✓	✓	✓		

[1] 按“符合”、“部分符合”、“不符合”填写。

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况[1]	备注
				3级、2级	4级		
	(G)	机房部署防水报警装置，具备漏水检测和报警能力（厂站不要求漏水检测和报警能力）	✓	✓	✓		
		水管安装，不得穿过机房屋顶和活动地板下	✓	✓	✓		
7	防静电(G)	机房具备设备接地、防静电地板（厂站不要求防静电地板）	✓	✓	✓		
		配备静电消除器（防静电手环）措施	—	—	✓		
8	温湿度控制(G)	机房设置温湿度自动调节设施（厂站具备温湿度检测调节设施）	✓	✓	✓		
9	电力供应(A)	机房设置专用冗余UPS电源，UPS电源为双路供电	✓	✓	✓		
10	电磁防护(S)	采用接地方式防止外界电磁干扰和设备寄生耦合干扰	✓	✓	✓		
		动力电缆和信号电缆必须隔离铺设	✓	✓	✓		
		重要设备（SCADA服务器、前置机、通信机）放置于电磁屏蔽机柜内	—	—	✓		
合计			75	85	100		

B1.2　网络安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	结构安全(G)	业务准确分区，调度数据网网络承载安全区I、安全区II的业务	✓	✓	✓		必须实现项
		根据电力监控系统安全等级保护定级结果在生产控制大区划分不同的网络安全域，并进行区域之间的安全访问控制	✓	✓	✓		必须实现项
		横向部署专用隔离装置，仅允许非TCP直连方式的数据通信	✓	✓	✓		必须实现项

序号	评估项目	评估要点	厂站端系统(3级、2级)	调度端系统		符合情况	备注
				3级、2级	4级		
		调度数据网纵向部署专用加密认证装置，仅允许专用的通信服务，严格设置访问控制策略	✓	✓	✓		必须实现项
		局域网核心交换设备、广域网核心路由设备应采取设备冗余或准备了备用设备，同时路由链路也应该施行冗余方式，核心网络不存在明显的单点故障隐患	✓	✓	✓		
		绘制与当前运行情况相符的网络拓扑结构图	✓	✓	✓		
2	访问控制(G)	根据业务系统划分不同 VLAN，VLAN 间配置严格的访问控制策略	✓	✓	✓		
		生产控制大区内禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务	✓	✓	✓		
		远程拨号访问采用专用拨号认证服务器	✓	✓	✓		
3	安全审计(G)	具有内网安全监视功能，对设备日志进行集中采集和统计分析	-	✓	✓		
4	边界完整性检查(S)	对电力调度数据网络的网络设备进行安全配置，防止非授权访问，禁止 III 区系统与办公系统对生产控制大区的非授权访问	✓	✓	✓		
5	入侵防范(G)	生产控制大区和管理信息大区分别部署入侵检测/防御系统，采用离线方式及时升级系统特征库	-	✓	✓		
6	网络设备防护(G)	口令长度不低于 8 位，为数字、字母组合，且定期更换	✓	✓	✓		
		网络设备远程管理采用加密方式，并对管理地址进行限制	✓	✓	✓		
		网络设备具有登录失败处理功能，可采取结束会话、限制非法登录次数、登录超时自动退出等措施	✓	✓	✓		
合计			90	100	100		

B1.3　主机安全

序号	评估项目	评估要点	厂站端系统(3级、2级)	调度端系统		符合情况	备注
				3级、2级	4级		
1	身份鉴别(S)	口令长度不低于8位，为数字、字母组合，且定期更换	✓	✓	✓		
		设置合理的口令策略（包括设置口令长度、复杂性、口令存留期等）	✓	✓	✓		
		设置用户安全策略(包括设置帐户锁定登录失败锁定次数、锁定时间、超时自动锁定时间等）	✓	✓	✓		
		启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施	✓	✓	✓		
2	安全标记(S)	采用安全操作系统和安全数据库，对所有主体和客体设置敏感标记	-	-	✓		
3	访问控制(S)	依据所有主体和客体设置的敏感标记控制主体对客体的访问	-	-	✓		
		配置操作系统、数据库系统重要文件的访问权限，只授予必要的用户必需的访问权限	✓	✓	✓		
		及时删除多余的、过期的帐户，避免共享帐户的存在	✓	✓	✓		
		修改默认帐号/口令	✓	✓	✓		
		删除默认共享目录	✓	✓	✓		
4	可信路径(S)	采用安全操作系统，在系统对用户进行身份鉴别和访问时，系统与用户之间能够建立一条安全的信息传输路径	-	-	✓		
5	安全审计(G)	审计范围覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户	✓	✓	✓		
		开启主机日志审计功能或采用内网安全监视系统，对主机安全类日志和运行类日志进行集中采集和统计分析	✓	✓	✓		
		对审计数据分配合理的存储空间和存储时间，避免审计记录受到未预期的删除、修改或覆盖	✓	✓	✓		
6	剩余信息保护	确保系统内的用户鉴别信息、文件、目录和数据库记录等资源所在的	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
	(S)	存储空间，被释放或重新分配给其他用户前得到完全清除					
7	入侵防范(G)	生产控制大区和信息管理大区分别部署入侵检测/防御系统，采用离线方式及时升级系统特征库	✓	✓	✓		
		在系统上线或发生重大变更时测试并安装系统安全补丁，在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补，停止或禁用与承载业务无关的服务或端口	✓	✓	✓		
8	恶意代码防范(G)	生产控制大区和信息管理大区分别部署独立的防恶意代码管理系统，采用离线方式及时升级经测试验证过的系统特征库	✓	✓	✓		
9	资源控制(A)	通过设定终端接入方式、网络地址范围等条件限制终端登录	✓	✓	✓		
		具备对服务器CPU、硬盘、内存、网络等资源使用情况进行监视和报警的功能	✓	✓	✓		
10	安全免疫(G)	以可信计算技术为核心，构建可信计算基础设施，为高安全等级生产控制系统建立主动防御机制（可选）	✓	✓	✓		
合计			85	85	100		

B1.4 应用安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	身份鉴别(S)	口令长度不低于8位，为数字、字母组合，设置口令过期时间、口令不能重复的次数、锁定口令错误输入次数、锁定时间，且定期更换	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
		在应用软件的各组成部分中都不能存储明文的口令数据	✓	✓	✓		
		启用登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施	✓	✓	✓		
2	安全标记(S)	对所有主体和客体设置敏感标记（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全调用）	-	-	✓		
3	访问控制(S)	依据所有主体和客体设置的敏感标记控制主体对客体的访问（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全访问控制）	-	-	✓		
		提供系统管理员用户一个产生和修改用户授权的管理模块，新建帐户时，帐户初始权限应为空，不应内置匿名账户，也不允许匿名用户的登录	✓	✓	✓		
		及时删除多余的、过期的帐户，修改默认帐号/口令，避免共享帐户的存在	✓	✓	✓		
4	可信路径(S)	在系统对用户进行身份鉴别和访问时，系统与用户之间能够建立一条安全的信息传输路径（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全访问控制）	-	-	✓		
5	安全审计(C)	启用应用系统日志审计功能，或采用安全审计设备记录业务系统发生的历史安全事件，对安全事件发生的规律和频率进行统计和分析	✓	✓	✓		
		安全审计记录只有授权的管理人员可访问，且仅为只读权限，无修改和删除权限	✓	✓	✓		
		安全审计信息需进行备份	✓	✓	✓		
6	剩余信息保护(S)	确保系统内的用户鉴别信息所在的存储空间，被释放或重新分配给其他用户前得到完全清除	✓	✓	✓		
7	通信完整性(S)	采用纵向加密认证装置，基于电力调度数字证书，通过加密认证、HTTPS 等技术措施，实现远程通信的完整性保护	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
8	通信保密性(S)	采用纵向加密认证装置，基于电力调度数字证书，通过加密认证、HTTPS等技术措施，实现远程通信的保密性保护	✓	✓	✓		
9	抗抵赖(G)	具有应用系统安全审计功能，对用户登录、操作等行为进行记录，实现发送、接收数据的抗抵赖	✓	✓	✓		
10	软件容错(A)	对用户输入的数据进行合法性检验，并执行强制的非法数据过滤功能，禁止提交可能产生危害的数据	✓	✓	✓		
		能够允许多用户同时对同一个系统资源进行不相冲突的访问操作，并且设定保护措施，防止相互可能造成的冲突，禁止多个客户端用户同时执行互斥的操作	✓	✓	✓		
		在故障发生时，应用系统能够继续提供一部分功能，确保对部分严重故障进行自动处理，采取可能使系统恢复正常状态的措施或保护现存数据的措施	✓	✓	✓		
11	资源控制(A)	当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方能够自动结束会话	✓	✓	✓		
		对系统的最大并发会话连接数和单个帐户的多重并发会话进行限制	✓	✓	✓		
合计			85	85	100		

B1.5 数据安全及备份恢复

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	数据完整性(S)	基于电力调度数字证书和安全标签技术，通过加密认证、HTTPS等安全技术措施，实现远程通信的完整性保护	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
2	数据保密性(S)	基于电力调度数字证书和安全标签技术，通过加密认证、HTTPS等安全技术措施，实现远程通信的保密性保护	✓	✓	✓		
3	备份和恢复(A)	实现主备调互备机制	-	✓	✓		
		采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障	✓	✓	✓		
		提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性	✓	✓	✓		
		提供本地数据备份与恢复功能，备份介质场外存放	✓	✓	✓		
		定期对关键业务的数据与系统进行备份	✓	✓	✓		
合计			90	100	100		

B2 管理要求

B2.1 安全管理制度

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	管理制度(G)	制定电力监控系统安全防护的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等	✓	✓	✓		
		按照“谁主管谁负责，谁运营谁负责”的原则，建立电力监控系统安全管理制度	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
		对要求管理人员或操作人员执行的日常管理操作建立操作规程：包括门禁、人员管理、访问控制、设备、恶意代码的防护、审计、数据及系统的备份、帐号、培训等管理制度	✓	✓	✓		
		将电力监控系统安全防护及其信息报送纳入日常安全生产管理体系	✓	✓	✓		
2	制定和发布(G)	安全管理制度具有统一的格式，并进行版本控制	✓	✓	✓		
		安全管理制度通过正式、有效的方式发布	✓	✓	✓		
		安全管理制度注明发布范围，并对收发文进行登记	✓	✓	✓		
3	评审和修订(G)	组织相关人员对管理制度进行审定	✓	✓	✓		
合计			40	40	40		

B2.2 安全管理机构

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	岗位设置(G)	明确本单位所辖电力监控系统的安全防护的领导责任人，设置监控系统安全防护岗位	✓	✓	✓		
2	人员配备(G)	指定专人负责本单位电力监控系统的安全防护，明确各业务系统专责人的安全管理责任	✓	✓	✓		
3	授权和审批(G)	根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
		针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序；按照审批程序执行审批过程，对重要活动建立逐级审批制度，记录审批过程并保存审批文档	✓	✓	✓		
		制定并严格执行操作票、工作票制度	✓	✓	✓		
4	沟通和合作(G)	加强各类管理人员之间、组织内部机构之间以及信息职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息问题	–	✓	✓		
		加强与兄弟单位、公安机关、专业机构、上级主管部门的合作与沟通	–	✓	✓		
5	审核和检查(G)	制定安全审核和安全检查制度规范；定期按照程序进行安全审核和安全检查活动	–	✓	✓		
合计			25	40	40		

B2.3 人员安全管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	人员录用(G)	相关人员签署保密协议	✓	✓	✓		
2	人员离岗(G)	及时收回离岗人员的相关证件，限制其系统访问权限，并通告相关单位	✓	✓	✓		
3	人员考核(G)	对各个岗位的人员进行安全技能及安全认知的考核，考核结果进行记录并保存，并纳入绩效考核	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
4	意识教育和培训(G)	对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训	✓	✓	✓		
		对教育和培训的情况和结果进行记录并归档保存	✓	✓	✓		
5	外部人员访问管理(G)	外部人员访问需提出书面申请或由主管人员批准后由专人全程陪同或监督，并登记备案	✓	✓	✓		
		对外部人员允许访问的区域、系统、设备、信息等内容进行书面的规定，并按照规定执行	✓	✓	✓		
		关键区域不允许外部人员访问	✓	✓	✓		
合计			40	40	40		

B2.4 系统建设管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	系统定级和备案(G)	明确现有系统安全保护等级，系统等级及相关材料报行业主管部门及公安机关备案	✓	✓	✓		
2	安全方案设计(G)	依据监控系统安全防护方案进行详细方案设计	✓	✓	✓		
3	产品采购和使用(G)	电力监控系统安全产品的采购和使用符合国家的有关规定	✓	✓	✓		
4	软件开发(G)	自行开发或外包开发的软件产品投运前应进行安全评估	✓	✓	✓		
5	工程实施和安全服务商选择	选择具备国家和行业主管部门要求的资质的施工单位和安全服务商，与选定的安全服务商签订与相关的协议，明确约定相关责任，	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
	(G)	并签署保密协议					
6	测试验收(G)	测试验收在已有工程验收和现场验收的基础上，增加第三方安全机构的参与（二级系统不要求第三方安全机构参与）；组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认	✓	✓	✓		
7	系统交付(G)	指定或授权专门的部门负责系统交付的管理工作，制定详细的系统交付清单，根据交付清单对所交接的设备、软件和文档等进行清点；对负责系统运行维护的技术人员进行相应的技能培训	✓	✓	✓		
8	等级评估(G)	按行业主管部门要求进行安全防护评估和等级保护测评，两项工作一起完成	✓	✓	✓		
合计			40	40	40		

B2.5 系统运维管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	环境管理(G)	建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境等方面的管理作出规定；指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理	-	✓	✓		
2	设备、介质和资产管理(G)	建立设备安全管理制度、介质安全管理制度和资产安全管理制度，对设备和介质的存放环境、使用、维护和销毁等方面作出规定；加强对移动存储设备、重要文档的安全管理；对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
3	监控管理和安全管理中心(G)	建立安全审计管理制度，指定专人对安全审计工作进行管理	✓	✓	✓		
4	网络和系统安全管理(G)	建立网络、系统安全管理制度，指定专人对网络设施、主机系统进行管理；定期检查违反规定拨号上网或其他违反网络策略的行为；依据操作手册对系统进行维护，详细记录操作日志，严禁进行未经授权的操作；指定专人对网络和主机进行恶意代码检测并保存检测记录	✓	✓	✓		
5	密码管理(G)	建立密码使用管理制度	✓	✓	✓		
6	变更管理(G)	建立变更管理制度，实现流程化管理	✓	✓	✓		
7	备份与恢复管理(G)	建立备份与恢复管理相关的安全管理制度；建立控制数据备份和恢复过程的程序	✓	✓	✓		
8	安全事件处置和应急预案管理(G)	制定安全事件报告和处置管理制度；制定安全事件报告和响应处理程序；制定应急处理预案；定期对应急预案进行演练，定期审查应急预案和根据实际情况更新的内容	✓	✓	✓		
合计			35	40	40		

附录 C 电力监控系统安全防护评估

C1 评估内容

电力监控系统安全防护评估的主要内容包括：资产评估、威胁评估、脆弱性评估、总体评价。

C1.1 资产评估

电力监控系统资产评估是指依据《电力监控系统安全防护总体方案》和国家等级保护相关要求对电力监控系统的评估对象进行资产识别和赋值，确定其在电力生产过程中的重要性。各单位资产评估对象必须包括附录 A 电力监控系统安全防护定级表所列内容。

（1） 资产识别

资产识别是对电力监控系统设备、数据和人员等系统构成元素进行分类、标记的过程。在确定评估范围后，对其中资产价值进行分析。资产识别是为了明确资产用途、使命和作用，进而确定资产价值的准备工作。

资产的形式和内容各不相同，主要包括信息、软件、硬件、人员和系统五个表现形式。电力监控系统的各构成元素可按照表 C-1 的定义进行归并和分类：

表 C-1 电力监控系统资产分类表

类别	解释
信息	以物理或电子的方式记录的数据，或者用于完成组织任务的知识产权。电力监控系统资产本质上是无形的，与系统资产紧密联系。系统存储、处理和传输驱动组织的关键信息。因此，当组织建立策略和计划以保护系统资产时，同时也保护了组织的关键信息，及其软硬件资产。
软件	软件应用程序和服务，如操作系统、数据库应用程序、网络软件、业务应用程序等，用于处理、存储和传输信息。
硬件	信息技术的物理设备，例如路由器、交换机、工作站、服务器等。通常强调单独考虑这些物理设备的替代价值。
人员	指组织中拥有独特技能、知识和经验的，他人难以替代的人。当人被标识为资产时，要确定是否还有更适于标识的相关资产。例如，标识他们使用、维护、管理的关键系统，或者他们为其他使用者提供的信息。
系统	处理和存储信息的信息系统，代表一组信息、软件和硬件资产。系统是一个整体，其任一组件都无法代表其整体，因此，对系统的评估需要完整的考虑系统的各个部分，并进行综合考虑。

（2） 资产赋值

资产赋值是根据电力监控系统安全保护等级对系统重要性进行赋值的过程。

各企业可根据《电力监控系统安全防护总体方案》和《电力行业信息系统安全等级保护定级工作指导意见》对资产进行赋值。

依据电力监控系统安全保护等级情况进行资产赋值，对应关系如表 C-2 所示。

表 C-2 资产赋值与安全等级对应表

资产赋值	标识	备注
5	很高	非常重要，生产控制大区内安全等级属于 4 级，具有控制功能的且其安全属性破坏后可能对组织造成非常严重的损失。
4	高	重要，生产控制大区内安全等级属于 3 级，不具有控制功能的且其安全属性破坏后可能对组织造成比较严重的损失。
3	中等	比较重要，生产控制大区内安全等级属于 2 级，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	不太重要，生产控制大区内安全等级属于 2 级，其安全属性破坏后可能对组织造成较低的损失。
1	很低	不重要，其安全属性破坏后对监控系统不会造成损害的。

C1.2 威胁评估

威胁是信息资产可能受到的来自内部和来自外部的安全侵害。

威胁评估是通过技术手段、统计数据和经验判断来确定电力监控系统面临威胁的过程。威胁评估主要包括两个方面，一是根据电力监控系统的运行环境确定面临的威胁来源，二是确定威胁的严重程度和发生的频率。

资产所处的环境不同，面临的威胁也不尽相同。应根据资产分类结果，对电力监控系统进行独立或整体的威胁评估。实际评估工作中，可按照安全分区和资产类别划分进行统一的威胁判断。

（1） 威胁识别

电力监控系统防护面临的主要威胁包括黑客、病毒、恶意代码、集团式攻击。此外，还应根据物理、网络和人员环境，对资产进行威胁判定。

（2） 威胁赋值

应根据威胁出现的频率判断得出威胁赋值。评估中，可以根据威胁发生的可能性进行分析、赋值。赋值越高，说明资产面临的威胁越大。

威胁赋值的过程是一个交流、观察与调查的过程，评估者应根据经验和（或）有关的统计数据进行判断，电力监控系统的运行维护及管理人员对系统自身运行

状况的了解程度是准确进行威胁赋值的关键。表 C-3 根据威胁发生的可能性，定义了年发生频率和威胁赋值。

表 C-3 威胁年发生频率和威胁赋值表

标识	赋值	定义	年发生频率
很高	5	威胁发生的可能性很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过。	年发生频率＞50
高	4	威胁发生的可能性较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过。	12＜年发生频率≤50
中	3	威胁发生的可能性中等（或＞ 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。	2＜年发生频率≤12
低	2	威胁发生的可能性较小；或一般不太可能发生；或没有被证实发生过。	0.1＜年发生频率≤2
很低	1	威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生。	年发生频率≤0.1

表 C-4 列出了电力监控系统面临的常见威胁表现形式。

表 C-4 常见威胁表现形式

威胁分类	威胁名称	说明	年发生频率	威胁赋值
非人为威胁	系统软件故障	由于电力监控系统软件故障所产生的问题		
	应用软件故障	由于电力监控系统应用软件故障所产生的问题		
	软件缺陷	软件缺陷导致的安全问题		
	硬件故障	系统由于硬件设备老旧、损坏等造成的无法使用问题		
	通信故障	由于通信故障所产生的问题		
	火山爆发	由火山爆发引起的故障		
	台风	由于台风引起的系统故障		
	地震	由地震引起的系统故障		
	地质灾害	因泥石流等地质灾害引起的系统故障		
	雷电	由雷电引起的系统故障		
	火灾	由火灾引起的系统故障，包括在火灾发生后进行消防工作中引起的设备不可用问题		
	水灾	由水灾引起的系统故障，包括在水灾发生后进行消防工作中引起的设备不可用问题		
	雪崩	由于雪崩引起的问题		
	人员丧失	由于各种原因，如疾病、道路故障、		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
		暴动等原因导致人员无法正常工作引起的系统无法使用故障		
	电力故障	由于电力中断、用电波动、供电设备损坏导致电力监控系统停止运行等导致的系统故障		
	温度异常	由温度超标引起的故障		
	湿度异常	由湿度超标引起的故障		
	灰尘、尘土	由灰尘超标引起的故障		
	强磁场干扰	由磁暴以及其他强磁场源等干扰引起的故障		
人为威胁	离开时未锁门	由于离开时未锁门造成系统的安全问题		
	离开时屏保未锁定	由于离开时屏保未锁定造成的安全问题		
	恶意破坏系统设施	对系统设备、存储介质等资产进行恶意破坏		
	设备或软件被控制或破坏	恶意的控制或破坏设备，以取得机密信息		
	由于误操作传输错误的或不应传送的数据	个人失误导致的安全问题		
	不恰当的使用设备、系统与软件	不当的使用设备造成的安全威胁		
	不恰当的配置和操作	不恰当的管理系统、数据库、无意的数据操作，导致安全问题		
	拒绝服务攻击	攻击者以一种或者多种损害信息资源访问或使用能力的方式消耗信息系统资源		
	关键员工的离职	由于关键员工的离职造成系统的安全问题		
	在不恰当的人员中讨论敏感文档	由于在不恰当的人员中讨论敏感文档造成的安全问题		
	由于设备（如笔记本）丢失	导致泄密等安全问题		
	过时的规定	由于采用过时的规定所造成的安全问题		
	不遵守安全策略	可能导致各种可能的安全威胁		
	滥用	由于某授权的用户（有意或无意的）执行了授权他人要执行的举动、可能		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
		会发生检测不到的电力监控系统资产损害		
	远程维护端口被非授权的使用	恶意的使用远程维护端口，控制主机		
	数据传输或电话被监听	恶意截获传输数据		
	办公地点被非授权的控制	恶意监控办公地点、重要地带，获取重要信息		
	侦察	通过系统开放的服务进行信息收集，获取系统的相关信息，包括系统的软件、硬件和用户情况等信息		
	口令的暴力攻击	恶意的暴力尝试口令		
	各类软件后门或后门软件	软件预留的后门或其他专门的后门软件带来的信息泄露威胁		
	偷窃移动设备	带有机密信息的移动设备被窃取		
	恶意软件	计算机病毒、蠕虫带来的安全问题		
	伪装	标识的仿冒等信息安全问题		
	分析信息流	分析信息流带来的信息安全问题		
	非法阅读机密信息	非授权的从办公环境中取得可获得的机密信息或复制数据		
	社会工程学攻击	通过邮件、即时聊天软件、电话、交谈等欺骗或其他方式取得内部人员的信任，进而取得机密信息		
	未经授权将设备连接到网络	未经授权对外开放内部网络或设备		
	密码猜测攻击	对系统账号和口令进行猜测，导致系统中的敏感信息泄漏		
	伪造证书	恶意的伪造证书，进而取得机密信息		
	远程溢出攻击	攻击者利用系统调用中不合理的内存分配执行了非法的系统操作，从而获取了某些系统特权，进而威胁到系统完整性		
	权限提升	通过非法手段获得系统更高的权限，进而威胁到系统完整性		
	远程文件访问	对服务器上的数据进行远程文件访问，导致敏感数据泄漏		
	法律纠纷	由企业或信息系统行为导致的法律纠纷造成信誉和资产损失		
	不能或错误地响应和恢复	系统无法或错误地响应和恢复导致故障和损失		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
	流量过载	由于网络中通信流量过大导致的网络无法访问		

根据威胁的发生可能性对威胁年发生频率进行赋值，并由此得出威胁赋值。

C1.3 脆弱性评估

脆弱性是信息资产及其防护措施在安全方面的不足，通常也称为漏洞。脆弱性可能被威胁利用，并对信息资产造成损害。

脆弱性评估包括脆弱性识别和赋值两个步骤，是发现与分析电力监控系统中存在的可被威胁利用的缺陷的过程。

（1） 脆弱性识别

脆弱性识别应围绕资产展开，即首先识别资产本身的漏洞，然后分析发现管理方面的缺陷，最后综合评价该资产或资产组（系统）的脆弱性。

脆弱性识别可从技术和管理两方面进行综合分析，技术方面的脆弱性识别主要采用工具审计和人工审计结合的方式进行，管理方面的脆弱性主要通过访谈和调查问卷来识别。对以往安全事件的统计和分析是确定脆弱性的重要方法。

脆弱性识别的结果应根据评估策略和目的进行调整，可参照相应的技术或管理标准，以及评估发起方的要求实施。

（2） 脆弱性赋值

脆弱性赋值包含严重程度和对系统安全属性的影响两部分内容，即确定脆弱性对电力监控系统资产的暴露程度（包括被威胁利用的可能性和难易程度）和脆弱性对安全属性的哪方面产生了破坏。

附录 B 列出了电力监控系统安全技术和管理两方面要求，不符合要求为缺陷或漏洞。根据附录 B 各分表的符合率确定脆弱性赋值，对应关系如表 C-65:

表 C-5 脆弱性赋值表

标识	赋值	定义
很高	5	如果脆弱性被威胁利用，将对资产造成完全损害
高	4	如果被威胁利用，将对资产造成重大损害
中	3	如果被威胁利用，将对资产造成一般损害
低	2	如果被威胁利用，将对资产造成较小损害
很低	1	如果被威胁利用，将对资产造成的损害可以忽略

（3） 脆弱性总体评价

根据脆弱性识别和脆弱性赋值结果，对系统脆弱性进行总体评价，找到被评估系统与电力监控系统安全防护要求的差距。

脆弱性总体评价标准见5.1。

C1.4 安全防护措施确认

识别脆弱性的同时，评估人员应对现有安全措施的有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生后对组织或系统造成的影响，如业务持续性计划。

已有安全措施确认与脆弱性识别存在一定的联系，安全措施的使用将减少系统技术或管理上的脆弱性，但安全措施确认并不需要和脆弱性识别过程那样具体到每个资产、组件的弱点，而是一类具体措施的集合，安全措施只为风险处理计划的制定提供依据和参考。

C1.5 风险分析

风险分析中主要涉及资产、威胁、脆弱性三个基本要素，每个要素有各自的属性，资产的属性是资产价值威胁的属性可以是威胁主体、影响对象、出现频率、动机等，脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

1）对资产进行识别，并对资产的价值进行赋值，即资产赋值；

2）对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值，即威胁赋值；

3）对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值，即脆弱性赋值；

4）根据威胁赋值及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

5）根据脆弱性的严重程度及安全事件所作用的资产的赋值计算安全事件造

成的损失;

6) 根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

风险分析模型如图 C-1 所示:

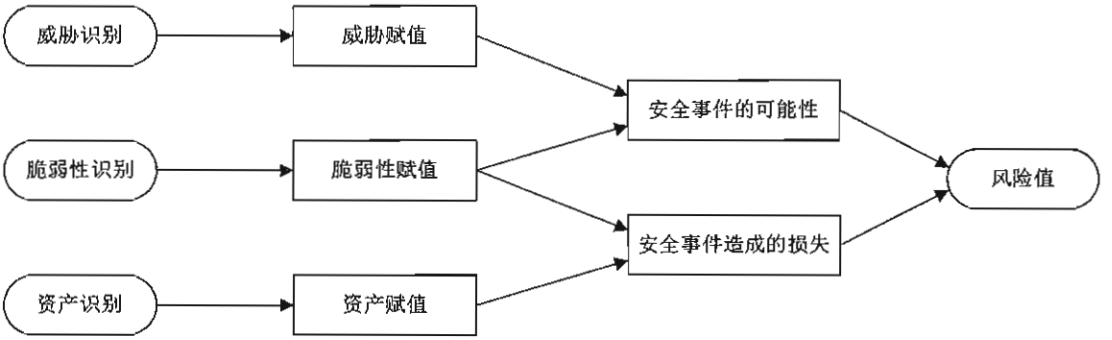

图 C-1　风险分析模型

C2 评估实施流程

电力监控系统安全防护评估实施流程分为四个阶段: 启动准备阶段、现场实施阶段、安全分析阶段和安全建议阶段。在评估实施完毕后，需要根据评估结论进行安全整改。实施流程如图 C-2 所示:

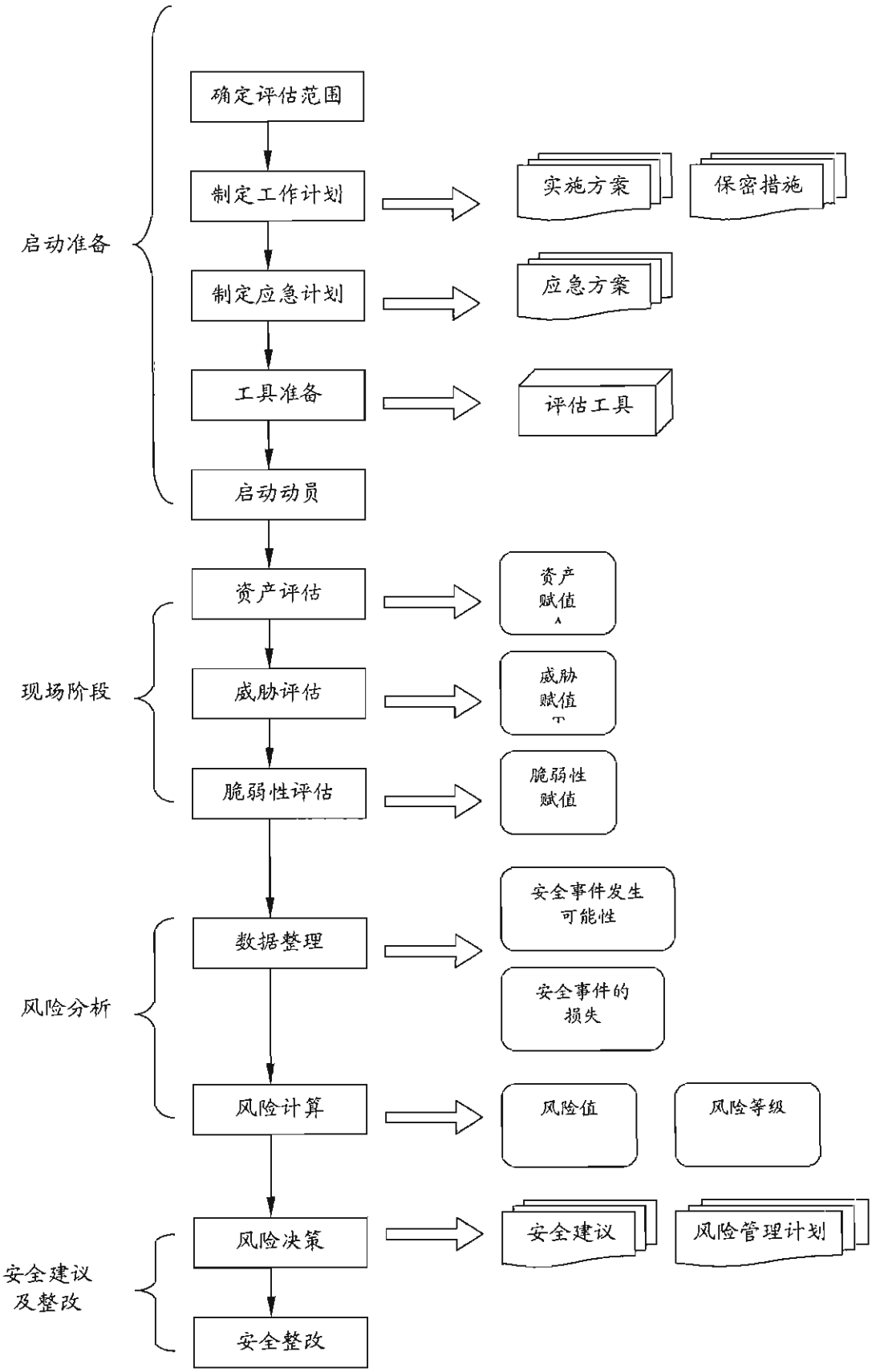

图 C-2　电力监控系统安全防护评估实施流程

C2.1 评估准备

第 1 步：成立评估工作组

评估工作下达后，应成立评估工作组，组织人员实施评估工作。评估工作组通常包括如下两方面的人员：

评估人员：由专业评估机构或内部人员组成的评估队伍。

系统管理人员：待评系统的运行维护、管理人员。

第 2 步：确定评估范围

评估范围可通过评估组的工作会议进行确定。

确定的评估范围应能代表待评估系统的所有关键资产，包括：网络范围、主机范围、应用系统范围、制度与管理范围。

评估范围确定后，待评系统管理人员需要根据选定的内容进行资料的准备工作，包括：网络拓扑结构图、电力监控系统资产清单、应用系统的说明文档、组织机构设置说明等内容。

第 3 步：评估工具准备

评估工作组根据收到的评估资料，进行评估工具的准备，包括威胁列表、网络评估工具、主机评估工具、资产识别工具、安全管理访谈表等内容。

评估工具中大部份内容需要根据评估范围和评估的主要目的进行定制，例如：威胁列表需要根据实际的物理、网络环境来进行定制；安全管理访谈表需要根据待评估系统的管理结构、管理方式进行定制。

在评估工具中，网络、主机脆弱性评估的通用性较强，目前可找到的商用和免费工具较多。下表是一些通用的脆弱性评估工具列表，但不得对生产控制大区在线运行系统进行自动化工具评估。

表 C-6 脆弱性评估工具

工具类型		用途说明
漏洞扫描工具	集成漏洞扫描工具	主机安全漏洞扫描、网络设备安全漏洞扫描
	数据库漏洞扫描工具	发现 Oracle、SQL 等主流数据库上存在的安全漏洞
	Web 漏洞扫描工具	发现 Web 服务中存在的安全漏洞
端口分析		Windows 系统主机端口分析工具
协议分析工具		网络协议分析

人工审计工具	用来进行远程主机登录，可方便存取人工审计数据
网络拓扑发现	可用于网络拓扑发现、网络设备配置下载

第 4 步：准备应急措施

电力监控系统安全防护评估中，为应对评估实施工作可能对系统带来的不利影响，评估工作组应在被评估方的配合下制定应急预案，确保在发生紧急事件时不对业务系统正常运行产生大的影响。如果需要对在线运行系统进行扫描，必须按照管理制度履行相关操作手续进行登记和向主管领导汇报。

C2.2 现场评估

根据现场评估阶段工作流程，规范工作步骤如下：

第 1 步：电力监控系统资产评估

电力监控系统资产评估包括了资产识别和资产赋值两部分内容，其中资产赋值需要在对业务系统进行充分了解和分析的基础上进行。资产评估中采用以业务系统为主线的方法，将每一项电力监控系统资产按照所属业务系统进行归类，在业务系统划分的基础上评估系统的安全性。

表 C-7 资产识别

输入	输出
电力监控系统资产识别表、网络拓扑和说明、业务系统说明、信息系统描述与系统分析报告	电力监控系统资产清单列表

第 2 步：电力监控系统威胁评估

电力监控系统威胁评估是利用电力系统安全威胁列表，通过访谈以及现场访谈和观察的方式，对当前电力监控系统所面临的主要安全威胁进行判定的过程。威胁评估主要包含以下三项内容：

（1）威胁统计

威胁统计是对电力监控系统面临的威胁的确认过程，威胁数据来源的方式较为多样，评估中可根据情况先进性威胁列表的维护，再根据实际环境进行判断和分析。

表 C-8 威胁统计

输入	输出
威胁列表、信息系统日志、系统环境说明	系统威胁统计表

（2）威胁赋值与计算

表 C-9　威胁赋值与计算

输入	输出
系统威胁统计表	资产威胁赋值表

第 3 步：安全分区合理性评估

参照总体方案的分区要求，对电力监控系统安全区的划分是否合理性进行检查。此外，安全分区合理性评估还包括对各安全区中业务系统网络构架合理性的评估。

表 C-10 安全分区合理性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统分区情况记录

第 4 步：边界完整性评估

边界完整性是对安全区 I、II 和 III 之间的边界连接情况进行的审核，确定在规定的边界点外没有短路情况。

表 C-11　边界完整性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统分区边界完整性审计记录

第 5 步：节点通信关系分析

通过对电力监控系统的业务数据流和业务网络结构的审核，对电力监控系统节点间通信关系进行分析，以确定某一安全区中的那些业务系统功能模块需要同其他安全区进行通信，以及这些通信间的安全要求。

表 C-12　节点通信关系分析

输入	输出
网络拓扑说明、业务系统功能说明	电力监控系统通信关系表

第 6 步：边界安全性评估

边界安全性评估是对安全区边界点的防护强度、访问控制力度和粒度的审核，以确定安全区边界的防护是否符合总体方案的要求。

表 C-13 边界安全性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统边界点审计记录

第 7 步：主机安全评估

主机安全性评估是对业务系统范围内的主机进行安全漏洞的发现的过程，包括如下内容:

（1）设备安全漏洞扫描

设备安全漏洞扫描是采用漏洞扫描工具对系统技术漏洞的发现过程，在漏洞扫描的过程中可能会对业务系统的运行产生影响，因此需要得到操作许可，并准备应急预案以避免由安全评估产生的风险。

表 C-14 设备安全漏洞扫描

输入	输出
电力监控系统资产清单	设备漏洞扫描结果

（2）设备审计

设备审计是采用人工登录主机或网络设备的方式对设备的安全配置情况进行的审计，由于设备配置数据是信息系统的敏感数据，因此在审计前需要得到操作许可。

表 C-15 设备审计

输入	输出
电力监控系统资产清单，主机或网络审计检查列表	设备审计结果

第 8 步：网络系统评估

网络系统评估包括对调度数据网、本地局域网的网络结构、网络设备的安全性、网络管理情况、网络配置评估等评估内容。

表 C-16 网络系统评估

输入	输出
网络拓扑结构说明、关键网络设备配置	网络安全评估记录

第 9 步：安全管理评估

安全管理评估包括策略访谈和管理制度文档审计两项内容。评估参照《GB/T 22080-2008 信息安全管理体系要求》和《电力监控系统安全防护总体方案》中对电力监控系统的信息安全管理要求进行。

（1）安全管理制度文档分析

文档分析主要是对电力监控系统管理中已制定和采用的安全管理制度文档以及制度的执行情况进行分析，通过分析发现现有制度中的缺陷。本部分的工作可以先期展开。

表 C-17 安全管理制度文档分析

输入	输出
安全管理规章、制度，管理制度评估工具	安全制度文档分析报告

（2）业务系统管理分析

对业务系统管理的分析从对具体业务系统的管理制度、岗位职责定义文档出发，并通过实际的观察和访谈确认系统管理的情况。

表 C-18 业务系统管理分析

输入	输出
业务系统管理制度，系统岗位分配文档	业务系统管理审计结果记录

第 10 步：业务系统安全评估

对业务系统软件提供的安全功能和自身的安全配置进行审核，以确定这些业务系统软件安全缺陷。

表 C-19 业务系统安全评估

输入	输出
电力监控系统资产清单(含业务系统)	业务系统软件安全评估记录

第 11 步：现有安全技术措施评估

对现有安全技术措施，如安全分区情况、安全隔离装置、防火墙和防病毒系

统等部署情况、管理与运维情况等进行审核，确定防护措施是否发挥了应有作用。

表 C-20 现有安全措施审计

输入	输出
电力监控系统资产清单、（现有安全措施部署方案）	现有安全措施审计记录

C2.3 风险分析

风险分析过程包括数据整理、风险计算和风险决策三个步骤。

（1） 数据整理

数据整理是将资产调查、威胁分析、脆弱性分析中采集到的数据按照风险计算的要求，进行分析和整理的过程，整理内容如下：

1) 评估资产列表：针对评估范围中的资产，对资产根据业务、类型进行分类，形成具体的资产或资产组；根据资产或资产组承载的业务和数据、所处的位置进行资产赋值的调整，确定出可计算的资产价值；
2) 威胁分析表：针对具体的资产或资产组，根据现场识别和赋值的威胁列表判断资产面临的威胁情况，并对现场所赋的威胁可能性和威胁影响值进行调整；
3) 脆弱性列表：针对具体的资产或资产组，整理脆弱性列表，并进行管理、运维和技术的分析，分析其产生原因和被利用的后果；
4) 安全事件的损失：根据资产值和脆弱性严重程度，采用矩阵法或者相乘法计算安全事件的损失；
5) 安全事件发生的可能性：根据威胁出现的频率等级和脆弱性严重程度，采用矩阵法或者相乘法计算安全事件发生的可能性。

（2） 风险计算

在完成资产评估、威胁评估和脆弱性评估后，根据资产价值、资产面临的威胁和存在的脆弱性赋值等情况对资产面临的风险进行分析和计算。

风险计算可采用矩阵法或者相乘法，在符合国标要求下不限定计算方法。通过安全事件损失值和安全事件发生可能性计算相应的风险值，并根据风险值确定风险等级。风险计算的原理方法参见 5.2 和附录 C1.5。

（3） 风险决策

风险决策是在风险排序的基础上，分析各种风险要素、评估系统的实际情况和计算消除或降低风险所需的成本，并在此基础上决定对风险采取接受、消除或转移等处理方式的过程。风险决策步骤如下：

（1）根据风险计算结果，按照给资产造成的损失大小对风险进行排序，并计算消除或降低风险所需的成本，在此基础上决定对风险采取的处理方法；

（2）对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中应明确采取的弥补脆弱性的安全措施、预期效果、实施条件、进度安排、责任部门等；

（3）对不可接受的风险进行安全整改后的残余风险要进行评估，确保其在可接受的范围内。

风险决策是提出安全建议的基础，科学、合理的风险决策是提高安全建议质量、防止过度防护和防护不足的保障。

C2.4 安全建议

安全建议是根据风险决策提出的风险处理计划，结合资产面临的威胁和存在的脆弱性，经过合理的统计归纳，形成安全解决方案建议报告的过程。安全建议报告应包含安全建议阶段的所有工作内容，具体如下：

（1）需求分析：需求分析根据风险分析的结论将电力监控系统的防护需求进行归纳和总结，并根据评估结果进行了现状分析、可行性分析和紧迫性分析；

（2）安全建议：根据需求分析的结论针对不同评估节点提出安全防护措施；

（3）实施计划：根据可行性分析和紧迫性分析结论提出安全建议的实施计划。

评估工作组必须对安全建议方案着重讨论，确保安全建议的合理性、可行性。

C2.5 安全整改

被评估单位应根据安全建议方案制定整改计划、落实整改措施，不断提高电力监控系统安全防护能力。

附录D电力监控系统安全防护与等级保护基本要求对照表

安全类别		等保要求	电力监控系统安全防护要求	关键点
技术	物理安全	位置选择、访问控制、防盗防破坏、防雷击、防火、防水防潮、防静电、温湿度控制、电力供应、电磁防护	按照安全分区的原则，将不同重要程度的设备置于各安全区域内，对重要设备采取电磁屏蔽措施。其防护强度等同于等级保护要求。	① 四级系统采取电磁屏蔽措施； ② 按照设备、操作间进行机房物理区域划分，按安全分区摆放机柜； ③ 四级系统要采用两道门禁。
	网络安全	结构安全、访问控制、安全审计、边界完整性、入侵防范、恶意代码防护、网络设备防护	电力监控系统遵循“安全分区、网络专用、横向隔离、纵向认证”的防护原则，将电力监控系统分置于生产控制大区和管理信息大区，在两个大区之间部署横向单向隔离装置，在生产控制大区专用的调度数据专用网络边界部署纵向加密认证装置，形成栅格状安全防护体系架构，其防护强度等同于等级保护要求。	① 专网专用； ② 安全分区； ③ 横向边界部署返回 1 比特的新型横向隔离装置； ④ 纵向边界部署纵向加密认证装置，配置 IP+限定端口的控制策略，对端有装置的应启用密通功能。
	主机安全	身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制	对原有系统按照《电力监控系统安全加固规范》进行安全加固，并通过加强运维管理保障主机及操作系统安全。 新一代调度控制系统采用国产设备，国产安全操作系统提高了安全防护水平，同时满足等级保护要求。其防护强度等同于等级保护要求。	① 对原有系统进行安全加固； ② 各个层面的口令均应杜绝 7 位以内弱口令。 ③ 新系统采用国产设备、国产安全操作系统、国产安全数据库；
	应用安全	身份鉴别、安全标记、访问控制、可信路径、	原有系统在安全加固的基础上，加强访问控制措施和对内	① 加强对原有系统及人员的日常管理；

安全类别		等保要求	电力监控系统安全防护要求	关键点
		安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、 资源控制	部人员的管理措施，以提升其安全防护水平。使防护强度基本等同于等级保护四级要求。新一代系统采用基于调度数字证书及安全标签的一体化基础平台，实现安全访问控制可信可控。其防护强度等同于等级保护要求。	② 各个层面的口令均应杜绝 7 位以内弱口令； ③ 新系统采用基于调度数字证书及标签的安全认证。
	数据安全及备份恢复	数据完整性 数据保密性 备份和恢复	电力监控系统从数据层面、系统层面和调度业务层面三个层面均要求实现备用，以此为基础建立备用调度体系，实现全面的电力监控系统安全备用机制，其防护强度等同于等级保护要求	① 实现数据级备用； ② 实现自动化系统及功能备用； ③ 实现调度业务及人员备用。
管理	安全管理制度	管理制度、制定和发布、评审和管理	建立了电力监控系统安全防护相关管理制度，依照“谁主管谁负责，谁运营谁负责”的原则，与调度安全性评价相结合，常态化开展管理工作。	① 制定电力监控系统安全防护管理制度。
	安全管理机构	岗位设置、人员配备、授权和审批、沟通和合作、审核和检查	成立了电力监控系统安全防护领导小组，建立安全工作协调机制，明确职责分工。调度部门的安全管理人员专人专岗。	① 建立电力监控系统安全管理机构。
	人员安全管理	人员录用、人员离岗、人员考核、安全意识教育和培训、外来人员访问管理	要求对电力监控系统安全防护专职人员定期进行培训和考核。同时建立保密制度，加强保密教育，提高安全防护意识，并与相关人员签署保密协议。加强对外来人员的管控，强化出入管理核查。	① 定期培训； ② 签署保密协议； ③ 外来人员管控。
	系统建设	系统定级、安全方案设	制定了针对电力监控系统专用	① 加强安全产品和业务

安全类别		等保要求	电力监控系统安全防护要求	关键点
	管理	计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择	安全产品和业务系统的开发单位及供应商的管控措施，对自主开发的软件进行严格管理防止关键技术扩散。	系统的开发单位及供应商的管控措施； ② 与开发单位及供应商签署保密协议。
	系统运维管理	环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码管理、密码管理、变更管理、备份与恢复、安全事件处置、应急预案管理	制定电力监控系统日常安全管理制度，制定了监控系统的应急处理预案。	① 制定安全运维管理制度； ② 制定监控系统的应急预案。

附录E 电力监控系统安全防护评估报告大纲

报告编号：----------

电力监控系统安全防护评估报告

被评单位：_____

委托单位：_____

评估单位：_____

报告时间：_____

电力监控系统安全防护评估基本信息表

<table>
<tr><td colspan="6">委托单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td>评估对象</td><td colspan="5"></td></tr>
<tr><td rowspan="2">联系人</td><td rowspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>邮箱</td><td colspan="3"></td></tr>
<tr><td colspan="6">评估单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td rowspan="2">联系人</td><td rowspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>邮箱</td><td colspan="3"></td></tr>
<tr><td>评估日期</td><td colspan="5"></td></tr>
<tr><td rowspan="3">评估小组</td><td>组长</td><td colspan="4"></td></tr>
<tr><td>组员</td><td colspan="4"></td></tr>
<tr><td>监督员</td><td colspan="4"></td></tr>
<tr><td>编制人</td><td></td><td>编制日期</td><td colspan="3"></td></tr>
<tr><td>审核人</td><td></td><td>审核日期</td><td colspan="3"></td></tr>
<tr><td>批准人</td><td></td><td>批准日期</td><td colspan="3"></td></tr>
</table>

以下无正文