内部资料
注意保存

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。

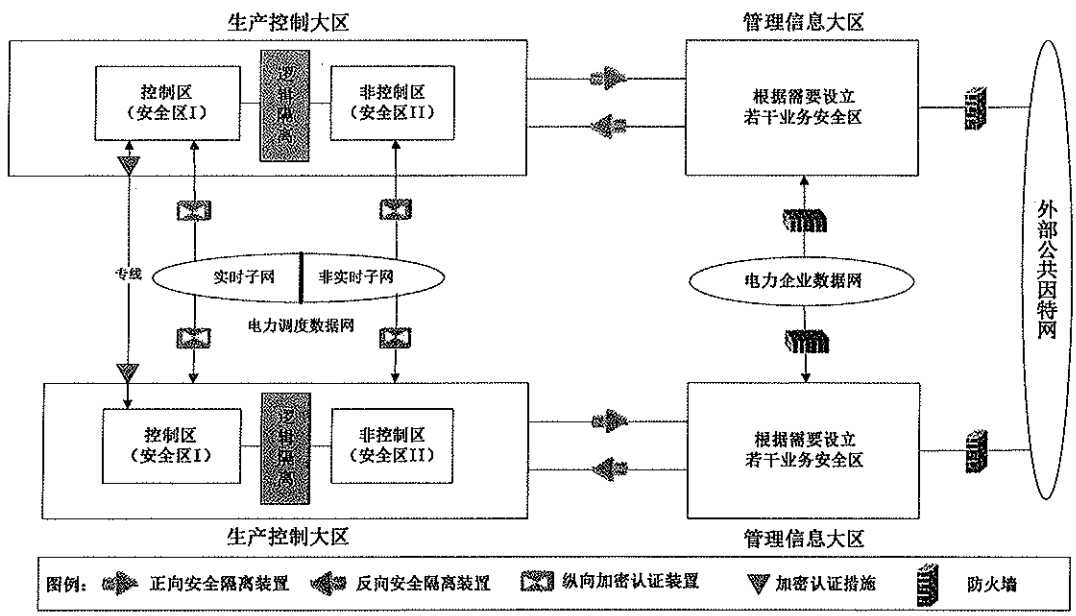

图 1　电力监控系统安全防护总体框架结构示意图

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。

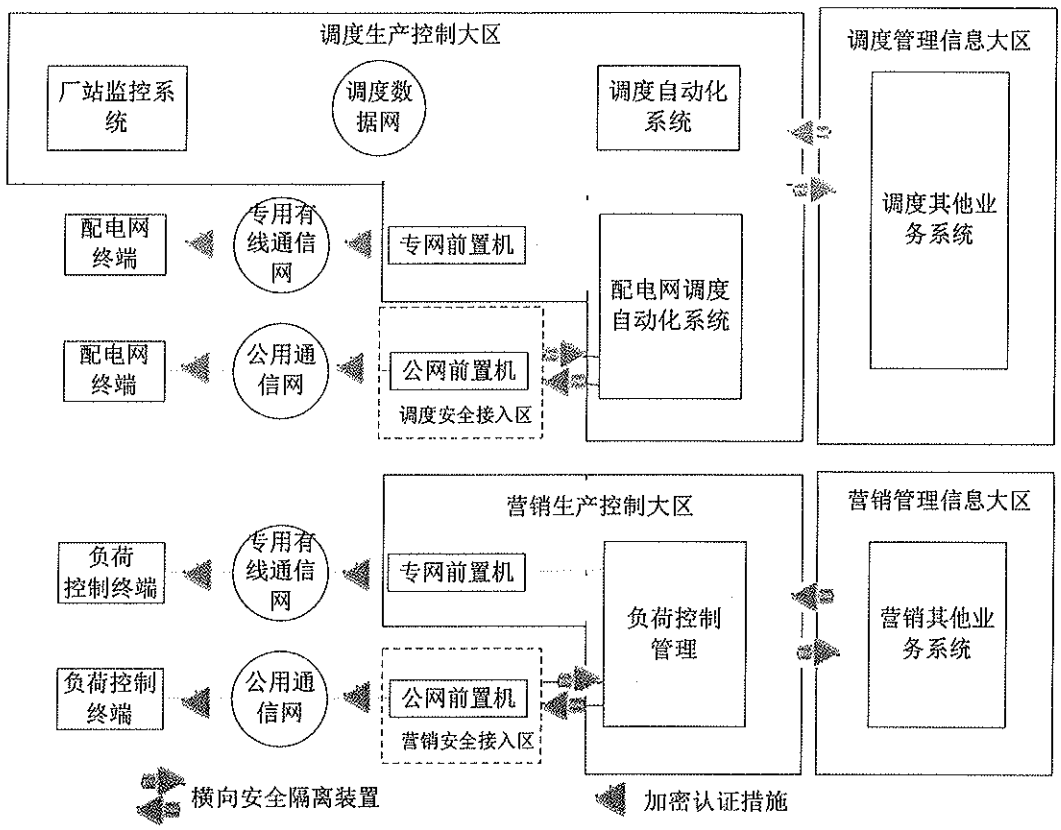

图 2　安全接入区的典型安全防护框架结构示意图

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。

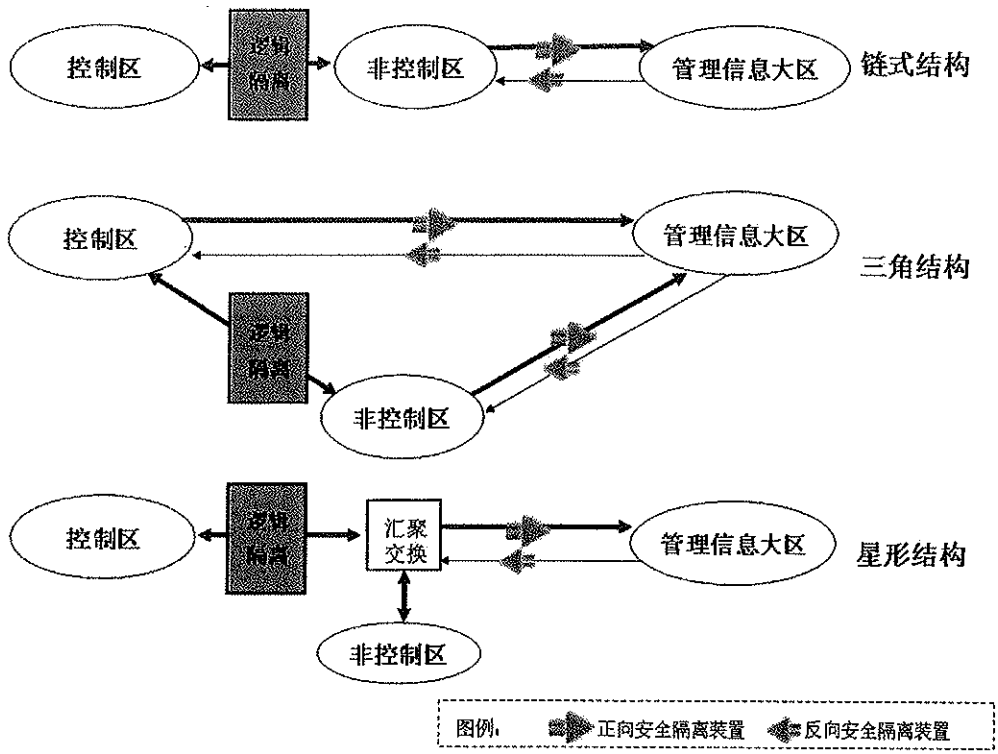

图 3 电力监控系统安全区连接拓扑结构

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