天融信
TOPSEC
002212.SZ

政策解读
《电力监控系统安全防护规定》

国家发展改革委2024年第27号令

天融信科技集团

2024年12月

第一章 总则

第一条

原文：

为了强化电力监控系统安全防护，保障电力系统安全稳定运行，根据《中华人民共和国网络安全法》《电力监管条例》《关键信息基础设施安全保护条例》等法律法规和国家有关规定，结合电力监控系统的实际情况，制定本规定。

解读：

此条目对《电力监控系统安全防护规定》（2024 年第 27 号令）（以下简称《规定》）编制的目的和主要政策依据进行了说明。

第二条

原文：

本规定适用于中华人民共和国境内的电力监控系统运营者以及与其相关的规划设计、研究开发、产品制造、施工建设、安装调试等单位。

解读：

此条目明确了本《规定》的适用范围，不仅包括中华人民共和国境内的电力监控系统运营者，还包括其他所有与电力监控系统相关的主体单位。

- **电力监控系统运营者**

这是本规定的核心适用对象。电力监控系统运营者指的是负责电力监控系统日常运行、维护和管理的实体，包括但不限于电网公司、发电企业、供电公司等。他们直接管理着电力监控系统的运行状态，确保其安全、稳定、可靠地运行，是电力监控系统安全防护的第一责任人。

- **电力监控系统规划设计单位**

电力监控系统规划设计单位主要负责电力监控系统的整体规划和设计，包括系统架构、网络布局、安全防护策略等。因此，规划设计单位必须遵循本规定的相关要求，确保所设计的电力监控系统符合安全标准和防护要求。

- **电力监控系统研究开发单位**

电力监控系统规划研究开发单位是电力监控系统技术创新和升级的重要力量。他们负责新技术、新产品的研究和开发工作，为电力监控系统的升级换代提供技术支持。由于研究开发活动直接关系到电力监控系统的安全性和稳定性，因此研究开发单位也必须遵守本规定，确保其研究开发工作符合安全防护的要求。

- **电力监控系统产品制造单位**

电力监控系统规划产品制造单位是电力监控系统设备和软件的直接生产者。他们负责生产符合安全标准和防护要求的电力监控系统设备和软件，为电力监控系统的建设和运行提供物质基础。产品制造单位必须严格遵守本规定的相关要求，确保所生产的设备和软件在设计和制造过程中就具备足够的安全防护能力。

- **电力监控系统施工建设单位**

电力监控系统规划施工建设单位是电力监控系统建设过程中的重要参与者。他们负责按照规划设计方案进行电力监控系统的施工建设，包括设备安装、网络布线、系统调试等工作。施工建设单位必须遵循本规定的相关要求，确保施工建设过程符合安全防护标准，避免在建设过程中引入安全隐患。

- **电力监控系统安装调试单位**

电力监控系统规划安装调试单位是电力监控系统建设完成后的关键一环。他们负责电力监控系统的安装调试工作，确保系统能够正常运行并满足安全防护要求。安装调试单位必须严格按照本规定和相关技术标准进行操作，确保安装调试过程中不出现任何安全问题。

第三条

原文：

电力监控系统安全防护应当落实国家网络安全等级保护制度和关键信息基础设施安全保护等制度，坚持“安全分区、网络专用、横向隔离、纵向认证”结构安全原则，强化安全免疫、态势感知、动态评估和备用应急措施，构建持续发展完善的防护体系。

解读：

电力监控系统作为国家关键信息基础设施，其安全防护体系建设需要遵循国家网络安全等级保护制度、关键信息基础设施安全保护制度等政策法规要求，同时坚持“安全分区、网络专用、横向隔离、纵向认证”的结构安全原则，在安全免疫、态势感知、动态评估和备用应急措施等方面重点开展安全能力建设工作，强化整体安全能力，以适应新形势下的网络安全建设需求。

第二章 安全技术

第四条

原文：

电力监控系统应当实施分区防护，防护区域按照安全等级从高到低划分为生产控制区（可以分为安全Ⅰ区和安全Ⅱ区）、管理信息区（可以分为安全Ⅲ区和安全Ⅳ区）。不同电力监控系统的生产控制区、管理信息区可以分别独立设置。

解读：

为了确保电力监控系统的安全稳定运行，防止外部攻击和内部误操作对系统造成损害，电力生产运营企业应根据电力监控系统中不同业务系统的安全等级进行安全区域划分，从高到低划分为生产控制区、管理信息区，并实施分区防护策略。

- **生产控制区**

生产控制区是电力监控系统中安全等级最高的区域，它直接关系到电力系统的实时控制和监控。该区域可以进一步细分为安全Ⅰ区和安全Ⅱ区：

a） 安全Ⅰ区

该区域包含与电力调度生产直接相关的业务系统，如调度自动化系统、安全自动控制系统等。这些系统需要高度的安全性和实时性，以确保电力系统的稳定运行。

b） 安全Ⅱ区

安全Ⅱ区虽然不直接参与控制，但与安全Ⅰ区的业务系统联系紧密，对电力生产和供应有较大影响。如电量计量系统、故障录波信息管理系统等。

- **管理信息区**

管理信息区是电力监控系统中用于运行指挥、分析决策等业务的区域。该区域可以进一步细分为安全Ⅲ区和安全Ⅳ区。管理信息区的安全等级低于生产控制区，但仍然需要采取必要的安全防护措施，以防止外部攻击和内部误操作对系统造成影响。

此外，不同电力监控系统的生产控制区可以分别独立设置，以适应不同电力系统的实际情况和需求。

第五条

原文：

电力监控系统各业务模块应当根据功能和安全等级要求部署。对电力一次系统（设备）进行实时监控的业务模块应当按照安全Ⅰ区防护要求部署；与安全Ⅰ区的业务模块交互紧密，对电力生产和供应影响较大但不直接实施控制的业务模块应当按照不低于安全Ⅱ区防护要求部署；与电力生产和供应相关，实现运行指挥、分析决策的业务模块应当按照不低于安全Ⅲ区防护要求部署；其他业务模块应当按照不低于安全Ⅳ区防护要求部署。

基于计算机及网络技术的业务系统及设备的分区，不得降低电力监控系统安全防护强度。

解读：

本条目明确了电力监控系统各业务模块的部署原则，即根据功能和安全等级要求分别部署业务模块，这一点与第五条中的安全区域划分原则保持一致，反映了对电力监控系统进行分区防护的必要性。

本条目进一步细化了各业务模块在电力监控系统中的部署要求。具体说明如下：

- **安全Ⅰ区防护要求部署**

实时监控业务模块：这些模块直接对电力一次系统（设备）进行实时监控，如 SCADA（监控和数据采集）系统、自动发电控制（AGC）和自动电压控制（AVC）系统等。由于它们直接控制电力系统的运行，对安全性的要求最高，因此必须按照安全Ⅰ区的防护要求进行部署。这包括使用专用的实时 VPN 子网、严格的访问控制、加密通信等安全措施。

- **不低于安全Ⅱ区防护要求部署**

与安全Ⅰ区交互紧密的业务模块：这些模块虽然不直接实施控制，但与安全Ⅰ区的业务模块交互紧密，对电力生产和供应有较大影响。例如电量计量系统、故障录波信息管理系统等。它们需要按照不低于安全Ⅱ区的防护要求进行部署，以确保数据传输的安全性和实时性，同时防止外部攻击和内部误操作。

- **不低于安全Ⅲ区防护要求部署**

运行指挥、分析决策业务模块：这些模块与电力生产和供应相关，主要用于运行指挥、分析决策等。它们虽然不直接控制设备，但对电力系统的稳定运行和优化调度具有重要意义。因此，这些模块需要按照不低于安全Ⅲ区的防护要求进行部署，包括合理的网络隔离、访问控制、数据备份等安全措施。

- **不低于安全Ⅳ区防护要求部署**

其他业务模块需要按照不低于安全Ⅳ区防护要求进行部署。

- **基于计算机及网络技术的业务系统及设备的分区**

不降低安全防护强度：电力监控系统中可能还包含其他基于计算机及网络技术的业务系统及设备。这些系统的分区不应降低电力监控系统整体的安全防护强度。即使它们不属于直接控制或监控电力系统的部分，也应当采取相应的安全措施，如网络隔离、访问控制、数据加密等，以防止外部攻击和内部数据泄露。

第六条

原文：

部署在生产控制区的业务模块与终端联接使用非电力监控专用网络（如公用有线通信网络、无线通信网络、运营者其他数据网等）通信或终端不具备物理访问控制条件的，应当设立安全接入区。

解读：

在电力监控系统中，可能存在生产控制区的业务模块需要与终端通过非电力监控专用网络进行通信，或者业务模块需要与不具备设置电子门禁、安全门锁、视频监控系统等物理访问控制措施条件的终端进行通信的情况。针对这些情况，非电力监控专用网络及终端应按照GB/T 36572-2018《电力监控系统网络安全防护导则》中的相关要求，设立安全接入区并且采取相应的安全措施，以确保电力监控系统整体的安全性。

- **业务模块与终端通过非电力监控专用网络通信**

当生产控制区的业务模块需要与终端通过非电力监控专用网络（如公用有线通信网络、无线通信网络、运营商其他数据网等）进行通信时，应设立安全接入区，在网络边界设置严格的安全防护措施，如防火墙、入侵检测/防御系统（IDS/IPS）、加密设备等，以确保数据在传输过程中的机密性、完整性和可用性。

- **业务模块与不具备物理访问控制条件的终端通信**

当生产控制区的业务模块需要与不具备物理访问控制条件的终端通信时，应设立安全接入区，加强终端的身份认证、访问控制和数据加密等措施，以确保只有授权用户才能访问终端数据，并且数据在传输和存储过程中得到有效保护。此外，还可以考虑采用远程监控和管理技术，对终端进行实时监控和维护，以进一步提高系统的安全性。

第七条

原文：

根据实际情况，在满足总体安全要求的前提下，可以简化安全区的设置，低安全等级业务模块可就高放置于高安全等级区域，但是应当避免形成不同安全区的纵向交叉联接。

解读：

在电力监控系统的实际应用中，可能存在灵活调整安全区设置的需求，以适应不同的业务场景和安全要求。此时可在满足总体安全要求的前提下简化电力监控系统安全区的设置，并且允许低安全等级业务模块就高放置于高安全等级区域。

具体实施时需要遵循以下原则：

- **总体安全原则**

无论如何简化或调整安全区的设置，都必须确保系统的总体安全原则不被破坏，确保对关键业务模块和数据的严格保护，防止外部攻击和内部误操作对系统造成损害。

- **避免纵向交叉联接原则**

在简化安全区设置的过程中，应当特别注意避免形成不同安全区的纵向交叉联接。纵向交叉联接可能会引入潜在的安全风险，因为低安全等级区域的安全措施可能不足以保障高安全等级区域的数据和业务安全。因此，在部署时应确保各安全区之间的边界清晰、隔离有效，防止数据泄露和非法访问。

第八条

原文：

生产控制区应当使用电力监控专用网络。电力监控专用网络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运营者其他数据网及外部公用数据网的安全隔离。

电力监控专用网络划分为逻辑隔离的实时子网和非实时子网，分别连接安全Ⅰ区和安全Ⅱ区。

解读：

- **生产控制区网络专用**

在电力监控系统的设计和应用中，确保生产控制区的稳定性和安全性是至关重要的。通过在

生产控制区使用电力监控专用网络，应用独立的网络设备组网，能够实现在物理层面上的安全隔离和防护。这种隔离方式能够有效阻止运营者其他数据网及外部公用数据网等外部网络对电力监控系统的潜在威胁，如黑客攻击、恶意软件传播等。同时，专用通道和设备的使用还保证了数据传输的稳定性和可靠性，降低了因网络拥堵或故障导致的系统风险。

- **电力监控专用网络逻辑隔离**

在电力监控专用网络内部，进一步划分为逻辑隔离的实时子网和非实时子网，以满足不同安全等级和业务需求。这种划分方式不仅提高了系统的安全性和灵活性，还优化了网络资源的利用。

实时子网：实时子网直接连接安全Ⅰ区，负责承载对电力一次系统（设备）进行实时监控的业务模块。这些业务模块对实时性和可靠性要求极高，需要低延迟、高带宽的网络支持。实时子网通过严格的安全策略和控制措施，确保数据传输的机密性、完整性和可用性。

非实时子网：非实时子网连接安全Ⅱ区，主要用于承载与安全Ⅰ区交互紧密但不直接实施控制的业务模块。这些业务模块对实时性要求相对较低，但同样需要安全可靠的网络环境。非实时子网在逻辑上与实时子网隔离，防止了潜在的安全风险扩散。

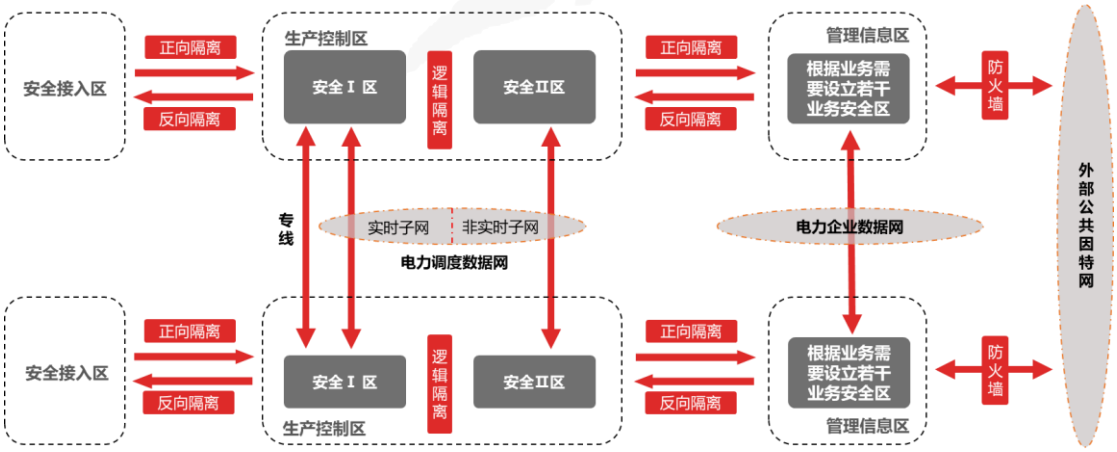
通过物理和逻辑上的双重隔离，电力监控专用网络为电力监控系统提供了强大的安全保障。同时还可以配合其他安全措施，如防火墙、入侵检测/防御系统（IDS/IPS）、数据加密等，以确保数据在传输和存储过程中的安全性。

第九条

原文：

生产控制区与管理信息区、安全接入区之间的联接处应当设置电力专用横向单向安全隔离装置。

解读：



- **横向单向安全隔离**

在电力监控系统的安全防护架构中，为确保生产控制区与管理信息区、安全接入区之间的数据传输既满足业务需求，又符合安全隔离的原则，应在区域之间联接处设置电力专用横向单向安全隔离装置，防止某一安全区潜在的安全威胁扩散到其它区域。

a） 生产控制区与管理信息区之间横向单向安全隔离

在生产控制区（如安全Ⅰ区和安全Ⅱ区）与管理信息区（安全Ⅲ区）之间的联接处，需要设置电力专用横向单向安全隔离装置。确保生产控制区的核心业务数据在传输到管理信息区进行管理和分析时，不会受到来自管理信息区的潜在威胁。

b） 生产控制区与安全接入区之间横向单向安全隔离

在生产控制区与安全接入区之间的联接处，需要设置电力专用横向单向安全隔离装置。安全接入区通常用于与外部网络（如公用有线通信网络、无线通信网络等）进行连接，通过单向隔离装置可以确保外部数据在进入生产控制区前经过严格的安全检查和控制。

- **电力专用横向单向安全隔离装置设备选择与应用**

电力专用横向单向安全隔离装置是一种特殊的安全设备，仅允许数据从低安全等级区域向高安全等级区域单向传输，同时阻止任何反向的数据流和未经授权的访问。这种装置通过物理隔离和逻辑控制相结合的方式，实现了不同安全区域之间的安全隔离，有效降低了外部攻击和内部误操作的风险。

电力专用横向单向安全隔离装置应选用经过国家指定部门检测认证的产品，确保其满足电力行业的安全标准和要求。

第十条

原文：

安全Ⅰ区与安全Ⅱ区之间、安全Ⅲ区与安全Ⅳ区之间、安全接入区与终端之间应当设置具有访问控制功能的设备、防火墙或者相当功能的逻辑隔离设施。

解读：

在电力监控系统的安全防护中，为了确保不同安全区域之间的有效隔离和数据传输的安全性，应在按照第十一条安全要求设置电力专用横向单向安全隔离装置的基础上，进一步强化安全区域间的边界安全防护能力，在联接处设置具有访问控制功能的设备、防火墙或者相当功能的逻辑隔离设施，构建可靠的安全屏障。

- **安全Ⅰ区与安全Ⅱ区之间隔离**

在生产控制区内部的安全Ⅰ区和安全Ⅱ区边界处，应部署具有访问控制功能的专业防护设备，如工业防火墙，以实现两区域之间的逻辑隔离，落实严格的访问控制策略。

- **安全Ⅲ区与安全Ⅳ区之间隔离**

在安全Ⅲ区与安全Ⅳ区之间的联接处，需要设置具有访问控制功能的设备、防火墙或相当功能的逻辑隔离设施，这些设施应能够严格控制管理信息区内部不同区域之间的数据访问，确保只有经过授权和验证的请求才能通过。

- **安全接入区与终端之间隔离**

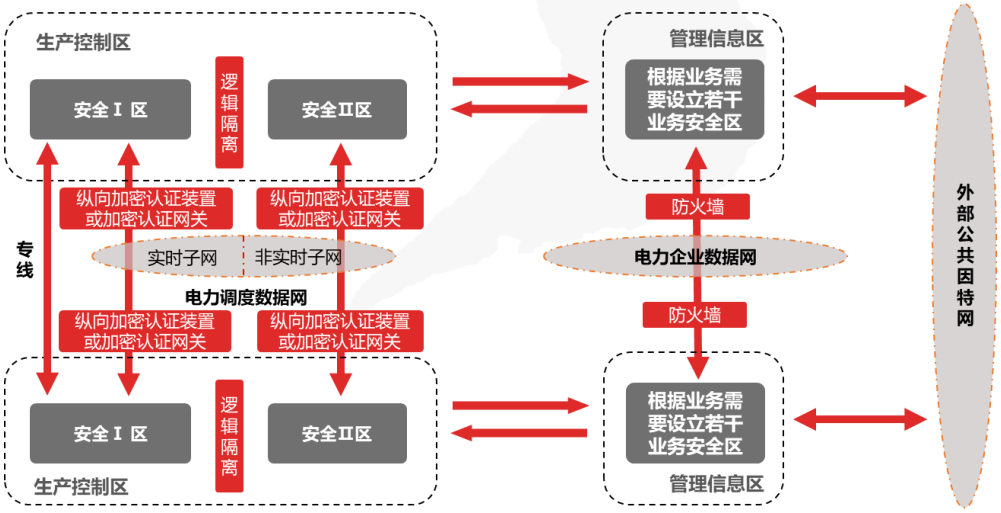
安全接入区作为电力监控系统与终端的接口，其与终端之间的联接处需设置防火墙或具有相当功能的逻辑隔离设施。实现对外部网络的通信内容过滤和检查，确保只有符合安全策略的数据才能传输到安全接入区，并进一步传输到生产控制区。

第十一条

原文：

生产控制区与电力监控专用网络的广域网之间的联接处应当设置电力专用纵向加密认证装置或者加密认证网关。

解读：



生产控制区与电力监控专用网络的广域网进行通信时，可能面临来自广域网的网络攻击、病毒入侵等安全风险，可能造成电力生产控制系统瘫痪、生产数据泄露等后果。为了保障生产控制区与广域网之间传输数据的完整性和安全性，防止非授权设备接入电力监控系统，需要在生产控

制区与广域网的联接处设置电力专用纵向加密认证装置或者加密认证网关，实现网络层的加密认证，增强电力监控系统抵御安全威胁的防护能力。

- **电力专用纵向加密认证装置**

电力专用纵向加密认证装置采用认证、加密、访问控制等技术措施，确保电力监控系统数据的远方安全传输以及纵向边界的安全防护。该装置经过国家指定部门的检测认证，具有较高的安全性和可靠性。

- **加密认证网关**

除了电力专用纵向加密认证装置外，加密认证网关也是实现网络层加密认证的重要设备之一。加密认证网关能够在数据传输过程中对数据进行加密处理，并通过认证机制确保数据接收方的身份合法性，从而有效防止数据泄露和非法访问。

第十二条

原文：

电力调度机构应当依照电力调度管理体制建立基于数字证书等技术的分布式电力调度认证机制。生产控制区处理重要业务过程中应当采用应用层端到端加密认证机制，其中与电力调度机构交互业务数据应当纳入电力调度认证机制，保障数据传输的完整性和真实性。

解读：

- **生产控制区应用层端到端加密认证**

在生产控制区处理重要业务过程中，应当采用应用层端到端加密认证机制。这种机制在数据传输的起点和终点都进行加密和解密操作，确保了数据在传输过程中的安全性。同时，通过认证机制验证数据传输的完整性和真实性，防止数据被篡改或伪造。

- **生产控制区与电力调度机构的交互**

生产控制区与电力调度机构交互的业务数据应当纳入电力调度认证机制。这意味着这些数据在传输过程中将受到严格的加密和认证保护，确保数据的真实性和完整性。此外，电力调度机构还可以通过对这些数据的监控和分析，及时发现潜在的安全威胁并采取相应措施。

第十三条

原文：

生产控制区应当具有高安全性和高可靠性，禁止采用安全风险高的通用网络服务功能，禁止选用具有无线通信功能的产品，应当对外设接入行为进行管控。

生产控制区重要业务应当优先采用可信验证措施实现安全免疫。

解读：

在电力监控系统中，生产控制区作为核心区域，承担着对电力一次系统进行实时监控和控制的重要任务，因此必须具备高安全性和高可靠性。

此条目为了确保生产控制区的安全稳定运行，明确了生产控制区安全防护需要遵循的一系列严格的安全规定和原则。这些措施的实施将有效提升电力监控系统的安全防护水平，保障电力生产的安全稳定运行。

- **禁止采用高风险通用网络服务功能**

生产控制区应当避免使用安全风险高的通用网络服务功能，如未经安全加固的 Web 服务、FTP 服务、Telnet 服务等。这些服务可能存在已知的安全漏洞和弱点，容易被黑客利用进行攻击和渗透。因此，在生产控制区内应仅部署必要的、经过严格安全加固的业务系统和服务。

- **禁止选用具有无线通信功能的产品**

无线通信虽然带来了便利，但也增加了安全风险。无线通信信号容易被截获和干扰，可能导致数据泄露或系统失控。因此，在生产控制区内应禁止使用具有无线通信功能的产品，包括无线鼠标、无线键盘、无线网卡等。如果确实需要使用无线设备，必须采取严格的安全措施进行防护。

- **对外设接入行为进行管控**

生产控制区应当加强对外部存储设备、网络设备等的接入管控，包括终端设备接口管控，禁止在生产控制区内使用个人移动存储介质（如 U 盘、移动硬盘等）进行数据传输等。这些措施可以有效防止外部恶意代码和攻击通过外部设备渗透到生产控制区内。

- **优先采用可信验证措施**

为了进一步提升生产控制区的安全性，重要业务应当优先采用可信验证措施实现安全免疫。可信验证措施包括数字签名、身份认证、加密通信等多种技术手段，可以确保数据的真实性、完整性和保密性。通过可信验证措施的应用，可以大大降低外部攻击和内部误操作的风险，保障电力监控系统的稳定运行。

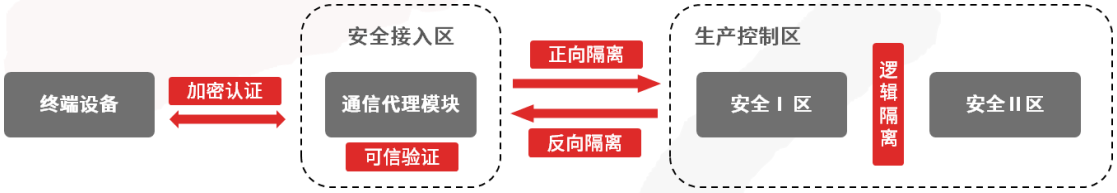
第十四条

原文：

安全接入区应当设置负责转发采集与控制报文的通信代理模块，通信代理模块与终端之间的通信应当采用加密认证措施。业务模块经安全接入区与终端之间传输控制指令等重要的数据时，应当与终端进行端到端的身份认证。

安全接入区内应当简化功能配置，禁止存储重要数据，并使用可信验证措施加强通信代理模块保护。

解读：



安全接入区作为生产控制区与外部网络之间连接的桥梁，在电力监控系统中承担数据通信与转发、安全隔离等重要功能。本条目明确了安全接入区需要遵循一系列安全防护规定，以确保电力监控系统的安全稳定运行。

- **通信代理模块的设置与加密认证**

安全接入区应当设置专门的通信代理模块，通过该模块转发来自生产控制区的采集与控制报文至终端，同时也将终端的响应数据回传给生产控制区。

通信代理模块与终端之间的通信应采用加密技术，确保数据传输过程中的机密性和完整性。

通信代理模块与终端之间应进行双向身份认证，确保通信双方的身份真实可靠。身份认证可以通过数字证书、用户名密码等方式实现。

- **端到端的身份认证**

当业务模块经安全接入区与终端之间传输控制指令等重要数据时，应采用端到端的身份认证机制，身份认证应覆盖通信传输过程中的每一个环节，确保数据在传输过程中不会被未经授权的第三方篡改或窃取。

- **安全接入区的功能配置与数据保护**

安全接入区应当简化功能配置，仅保留必要的转发和认证功能，避免引入不必要的复杂性和潜在的安全风险。

应禁止在安全接入区内存储重要数据，防止重要数据被泄露和非法访问。所有重要数据应存储在安全的生产控制区内，并通过加密技术进行保护。

安全接入区应使用可信验证措施加强对通信代理模块的保护，包括对通信代理模块进行数字签名验证、安全加固、定期更新安全补丁、实施严格的访问控制策略等，确保其软件完整性和来源可靠性。

第十五条

原文：

电力监控系统各分区边界应当采取必要的安全防护措施，禁止任何穿越生产控制区与管理信息区、安全接入区之间边界的通用网络服务。

解读：

本条目与 GB/T 36572-2018《电力监控系统网络安全防护导则》中的相关要求保持一致：“各区域安全边界应采取必要的安全防护措施，禁止任何穿越生产控制大区和管理信息大区之间边界的通用网络服务（如 FTP、HTTP、TELNET、MAIL、RRLOGIN，SNMP 等）。

电力监控系统通常被划分为不同的安全区域，以隔离不同等级的数据和业务系统，各区域之间的边界是安全防护的关键点，应采取禁止穿越边界的通用网络服务等措施，防止外部攻击者通过通用网络服务渗透到生产控制区，有效提升电力监控系统的安全防护水平，防范通用网络服务带来的安全威胁，保障电力生产的安全稳定。

第十六条

原文：

电力监控系统优先选用安全可信的产品和服务。不得选用存在已知安全缺陷、漏洞等风险但未采取有效补救措施的产品和服务。

电力监控系统投运前应当进行安全加固，对于已经投入运行且存在漏洞或风险的系统及设备，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。

解读：

- **安全产品和服务选择**

电力监控系统作为国家关键基础设施的重要组成部分，其稳定性和安全性直接关系到电力

系统的平稳运行和国家能源安全。因此，在电力监控系统设计和建设过程中，对安全产品和服务的选择应遵循以下规定：

a） 优先选用经过国家相关管理部门严格检测和认证、安全可信的产品和服务，确保其安全可信；

b） 不得选用存在已知安全缺陷、漏洞等风险但未采取有效补救措施的产品和服务；

c） 定期对已选用的产品和服务进行安全评估，确保其持续满足安全要求。

- **电力监控系统投运前的安全加固**

a） 全面测试

在电力监控系统投运前，应进行全面的安全测试和加固工作，包括漏洞扫描、渗透测试、安全配置审核等，确保系统无安全漏洞。

b） 合规性检查

开展电力监控系统合规性检查工作，确保系统符合国家和电力行业的相关安全标准、规范要求。

- **已运行系统的整改与管理**

a） 及时整改

对于已经投入运行且存在漏洞或风险的系统及设备，应按照国家能源局及其派出机构的要求及时进行整改，消除安全隐患。

b） 加强运维

加强电力监控系统及设备的运行管理和安全防护，包括定期巡检、安全审计、备份恢复等，确保系统稳定运行。

c） 应急响应

建立完善的电力监控系统应急响应机制，制定应急预案并定期进行演练，以应对电力监控系统可能发生的安全事件和突发事件。

- **持续提升安全防护能力**

a） 技术培训

加强对电力监控系统运维人员的安全培训和技术培训，提高其安全意识和技能水平。

b） 技术创新

鼓励和支持技术创新，引入新的安全防护技术和手段，提升电力监控系统的安全防护能力。

c） 合作共享

加强与相关单位和机构的合作与交流，共享安全信息和经验，共同提升电力监控系统的安全防护水平。

第十七条

原文：

运营者应当建立网络安全监测预警机制，建设基于内置探针等的网络安全监测手段，实时监视分析电力监控系统网络安全运行状态及可疑行为告警。与调度数据网相连的电力监控系统，其网络安全运行状态及可疑行为告警信息应当同步传送至相应电力调度机构。监视过程中应当尽量避免对原始安全数据的重复采集。

解读：

本条目与《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）中相关安全要求保持一致：“电力企业应当建立健全本单位网络安全监测预警和信息通报机制，及时掌握本单位网络安全运行状况、安全态势，及时处置网络安全威胁与隐患，定期向行业部门报告有关情况。电力行业关键信息基础设施运营者应当建立 7×24 小时值班值守制度，建设网络安全态势感知平台，并与行业部门、公安机关等有关平台对接。”

电力监控系统态势感知涉及到对电力监控系统网络安全状态、异常行为的全面实时监测、分析、预警和维护，能够有效提升电力监控系统的安全监测能力，实现网络安全事件的及时响应处置。因此为了确保电力监控系统的网络安全，运营者应当建立完善的网络安全监测预警机制，并采取以下具体措施：

- **建立网络安全监测预警机制**

制定详细的网络安全监测和预警流程，明确各环节的责任人和操作规范。设立专门的网络安全监测团队，负责日常的网络安全监视、分析和预警工作。建设基于内置探针的网络安全监测手段，实时捕获和分析电力监控系统网络流量、系统日志等关键数据，对电力监控系统的网络安全运行状态进行实时监视，及时发现异常行为和潜在的安全威胁。

- **同步传送网络安全运行状态信息**

对于与调度数据网相连的电力监控系统，应通过安全可靠的通信渠道，将关键的安全状态和

事件信息实时同步传递至相应的电力调度机构。

- **避免对原始安全数据的重复采集**

在监视过程中，应合理规划数据采集点，通过数据聚合、清洗等技术手段，提高数据处理的效率和准确性，避免对原始安全数据的重复采集，减少冗余数据。

第三章 安全管理

第十八条

原文：

电力监控系统安全防护是电力安全生产管理体系的有机组成部分。运营者是电力监控系统安全防护的责任主体，其主要负责人对电力监控系统安全防护负总责。运营者应当按照“谁主管谁负责，谁运营谁负责”的原则，建立健全电力监控系统安全防护管理制度，将电力监控系统安全防护工作及其信息报送纳入日常安全生产管理体系，落实分级负责的责任制。

解读：

电力监控系统的安全防护是电力安全生产的重要组成部分，本条明确了电力监控系统安全防护的管理机制，强调了运营者是电力监控系统安全防护的责任主体，应当建立健全电力监控系统安全防护管理制度，确保安全防护工作的有效实施和持续改进，并纳入日常安全生产管理体系。

- **运营者的主体责任**

总体负责：运营者的主要负责人需对电力监控系统安全防护负总责，这意味着他们要对整个安全防护体系的建立、运行和维护进行全面管理和监督。

制度建设：按照“谁主管谁负责，谁运营谁负责”的原则，运营者必须建立健全电力监控系统安全防护管理制度。这些制度应涵盖安全防护的各个方面，如物理安全、网络安全、系统安全、数据安全、应急响应等，并明确各级人员的职责和权限。

融入日常管理体系：运营者应将电力监控系统安全防护工作及其信息报送纳入日常安全生产管理体系中。这意味着安全防护工作不再是独立于日常运营之外的额外任务，而是与电力生产、调度、运维等各个环节紧密相连、相辅相成的。

分级负责：落实分级负责的责任制是确保安全防护工作有效执行的关键。运营者应根据系统的重要性和复杂性，将安全防护工作划分为不同的层级，并明确各层级的责任人和具体任务。通过层层压实责任，确保安全防护工作的每一个环节都有人负责、有人监督。

- **具体措施**

加强人员培训：定期对相关人员进行安全防护知识和技能的培训，提高他们的安全意识和应对能力。

完善技术手段：采用先进的安全防护技术和设备，如防火墙、入侵检测系统、加密技术等，提高系统的防护能力。

强化信息报送：建立快速、准确的信息报送机制，确保一旦发生安全事件或异常情况，能够迅速将相关信息报告给相关部门和人员。

定期评估与改进：定期对电力监控系统安全防护工作进行评估和检查，及时发现和整改存在的问题和隐患。同时，根据新的安全威胁和技术发展趋势，不断优化和完善安全防护体系。

第十九条

原文：

运营者在电力监控系统规划设计、建设运营过程中，应当保证网络安全技术措施同步规划、同步建设、同步使用。

解读：

运营者在电力监控系统规划设计、建设、改造、升级等环节，应依据《关键信息基础设施安全保护条例》《信息安全技术 关键信息基础设施安全保护要求》等政策标准要求，确保网络安全技术措施同步规划、同步建设、同步使用，从源头上构建安全可靠的电力监控系统，保障电力系统的稳定运行和数据安全。

以下是具体的要求和措施：

- **同步规划**

明确安全需求：在电力监控系统的规划设计阶段，运营者需明确系统的安全保护需求，包括网络安全、系统安全、数据安全等方面的要求。

制定安全方案：基于安全需求，制定详细的网络安全技术方案，包括网络架构、安全设备选型、安全策略配置等。该方案应经过专业技术人员评审，确保其科学性和可行性。

融入整体规划：将网络安全技术措施纳入电力监控系统的整体规划之中，确保其与系统建设的其他环节相互协调、相互促进。

- **同步建设**

安全设备部署：在电力监控系统的建设过程中，按照既定的安全方案部署相应的安全设备，如防火墙、入侵检测系统、加密设备等。

安全策略实施：配置并启用安全设备的策略，确保其能够有效地防御网络攻击和数据泄露等安全威胁。

安全测试与验证：在系统建设过程中，进行定期的安全测试和验证，确保各项安全措施得到有效执行，并及时发现和修复潜在的安全漏洞。

- **同步使用**

安全培训：在系统投入使用前，对运维人员进行全面的安全培训，使其了解系统的安全架构、安全设备的使用方法和安全策略的具体要求。

安全运维：在系统运行过程中，实施严格的安全运维管理，包括定期的安全巡检、安全审计和应急响应等。

持续优化：根据系统运行情况和安全威胁的变化，持续优化网络安全技术措施，确保系统的安全防护能力始终保持在较高水平。

第二十条

原文：

运营者在电力监控系统规划设计阶段，应当制定电力监控系统安全防护方案并通过本单位电力监控系统网络安全管理部门以及相应电力调度机构审核，系统投运前应当完成方案实施并通过本单位电力监控系统网络安全管理部门验收。

接入调度数据网的系统及设备，其接入技术方案和安全防护措施必须经相应电力调度机构审核同意。

需要设立安全接入区的电力监控系统，应当在安全防护方案中对接入对象规模进行评估，避免单个安全接入区接入规模过大，可按业务、地域分别设立安全接入区。

解读：

- **安全防护方案制定和验收**

在电力监控系统的规划设计阶段，运营者需要高度重视安全防护工作，严格按照相关要求制定安全防护方案，并在经过相关单位审核后正式实施方案，确保安全防护方案符合行业规范和电

力系统的整体安全要求。

对于需要设立安全接入区的电力监控系统，运营者应在安全防护方案中对接入对象规模进行评估。为避免单个安全接入区接入规模过大带来的安全风险，可按业务、地域等因素分别设立多个安全接入区。这样可以更好地实现安全隔离和风险控制。

安全防护方案实施完成后应由本单位电力监控系统网络安全管理部门进行验收，确保各项安全防护措施得到有效落实，并能够满足预期的安全防护效果。

- **接入调度数据网的要求**

对于需要接入调度数据网的系统及设备，为了确保接入过程不会对调度数据网的安全性和稳定性造成影响，接入技术方案和安全防护措施必须经相应电力调度机构审核同意后方可实施。

第二十一条

原文：

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，将电力监控系统安全防护评估纳入电力系统安全评价体系。

省级及以上电力调度机构应当定期将调管范围内电力监控系统安全防护评估和整改情况报国家能源局及其派出机构。

解读：

电力系统安全评价体系是电力安全管理体系的重要组成单元，通过评价安全管理体系运转情况、发现管理体系存在的缺陷和不足，有助于及时调整和优化安全管理措施，实现电力安全水平持续提升。

- **健全电力监控系统安全防护评估制度**

电力监控系统安全防护评估制度旨在通过科学的方法和手段，系统地分析电力监控系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，并指出有针对性的抵御威胁的防护策略和整改措施。这一制度的建立，有助于全面提升电力监控系统的安全防护水平，为电力系统的安全稳定运行提供有力保障。

电力监控系统安全防护评估应以自评估方式为主。运营单位应对本单位电力监控系统定期组织自评估工作，通过内部专业人员或委托第三方评估机构，对系统的安全性、稳定性进行全面检查和分析。

在自评估的基础上，国家能源局及其派出机构或相关监管部门可组织对电力监控系统进行

检查评估，发现自评估中可能遗漏的问题，并对系统的安全防护水平进行更全面的评价。

- **省级及以上电力调度机构报告机制**

省级及以上电力调度机构作为电力系统的重要管理机构，应定期将调管范围内电力监控系统安全防护评估和整改情况报告给国家能源局及其派出机构。报告内容应包括评估工作的基本情况、发现的主要问题、采取的整改措施以及下一步工作计划等。

通过这一报告机制，国家能源局及其派出机构可以及时了解电力监控系统的安全防护状况，并对存在的问题进行指导和监督。

第二十二条

原文：

运营者应当以合同条款的方式要求电力监控系统供应商保证：提供的产品和服务未设置恶意程序、不存在已知安全缺陷和漏洞，并在产品和服务的全生命周期内负责；当产品和服务存在安全缺陷、漏洞等风险时，立即采取补救措施，并及时告知运营者；当存在重大漏洞隐患时，及时向国家能源局及其派出机构报告。

解读：

此条目体现了电力监控系统对于产品和服务安全性的高度重视，以及明确供应商安全责任的管理思路。电力监控系统作为关键基础设施的一部分，其安全性和稳定性直接关系到电力系统的整体运行安全和社会经济的平稳运行。因此，从合同条款的角度对供应商提出明确的安全保证和服务要求，是保障电力监控系统安全的重要措施。

- **明确合同条款**

运营者应当在与电力监控系统供应商签订的合同中，要求供应商保证其提供的产品和服务中未设置任何恶意程序，包括但不限于病毒、木马、后门等可能危害系统安全的程序。

供应商应确保提供的产品和服务不存在已知的、未修复的安全缺陷和漏洞。这要求供应商在交付前进行充分的安全测试和漏洞扫描。

供应商应对其提供的产品和服务在全生命周期内负责，包括设计、开发、测试、部署、运维及退役等各个阶段。这意味着供应商需持续关注产品安全，并在必要时提供更新、补丁或技术支持。

- **风险应对机制**

当产品和服务存在安全缺陷、漏洞等风险时，合同应明确供应商应立即采取提供修复程序或

补丁、协助运营者进行紧急安全加固等补救措施，以消除这些风险。

同时，供应商还应在发现风险后立即告知运营者，以便运营者能够及时了解并采取相应措施。

- **重大漏洞隐患上报**

合同应明确规定当发现存在重大漏洞隐患时，供应商应及时向国家能源局及其派出机构报告。

第二十三条

原文：

电力监控系统专用安全产品应当采用统一的技术路线。

国家电力调度控制中心牵头，中国南方电网电力调度控制中心和主要电力企业等参与，组建电力监控系统专用安全产品管理委员会，负责电力监控系统专用安全产品管理，统筹解决重大问题，保障电力监控系统专用安全产品安全可控。

解读：

此条目明确了电力监控系统专用安全产品的统一技术路线，通过组建电力监控系统专用安全产品管理委员会，对专用安全产品的认证、检测、选择等环节进行安全管理，保障电力监控系统专用安全产品安全可控。

- **组建电力监控系统专用安全产品管理委员会**

电力监控系统专用安全产品管理委员会将负责全面管理电力监控系统专用安全产品的相关工作，包括但不限于技术规范制定、产品选型与测试、安全评估与认证、市场准入与监管等。

通过管理委员会的建立，可以更有效地统筹解决电力监控系统专用安全产品领域内的重大问题，如技术标准的统一、产品质量的提升、安全漏洞的及时修复等。同时，这一机制还有助于促进各参与方之间的信息共享与经验交流，推动技术创新与产业升级，共同提升电力监控系统的安全防护水平。

- **保障电力监控系统专用安全产品的安全可控性**

在电力系统中，安全可控是确保系统稳定运行和防范外部攻击的基本要求。通过统一技术路线和电力监控系统专用安全产品管理委员会的严格管理，可以确保电力监控系统专用安全产品在研发、生产、部署和使用过程中始终符合安全可控的要求，为电力系统的安全稳定运行提供有力保障。

第二十四条

原文：

管理委员会严格落实有关政策法规要求，制定工作章程，动态维护电力监控系统专用安全产品目录及技术规范，组织并推动安全认证和安全检测，督促运营者及相关单位落实供应链安全管控措施，组织开展电力监控系统专用安全产品风险评估，对存在安全风险的电力监控系统专用安全产品进行通报。

解读：

在电力监控系统专用安全产品管理机制建立和完善过程中，管理委员会应以有关政策法规为依据，落实对电力专用安全产品的一系列安全管理措施。

- **严格落实政策法规要求**

管理委员会的首要任务是确保所有活动都严格遵守国家及行业相关的政策法规要求。这包括但不限于网络安全法、电力安全生产法等法律法规，以及电力监控系统安全防护相关的标准、规范和指导意见。

- **制定工作章程**

为了明确管理委员会的组织架构、职责分工、工作流程和决策机制，需要制定详细的工作章程。工作章程应确保各参与方能够高效协作，共同推进电力监控系统专用安全产品的管理工作。

- **动态维护产品目录及技术规范**

随着技术的不断发展和安全威胁的日益复杂，电力监控系统专用安全产品的目录及技术规范需要不断更新和完善。管理委员会应负责定期评估现有产品和技术规范的有效性，并根据需要进行修订和补充，以确保其适应最新的安全需求和技术趋势。

- **组织并推动安全认证和安全检测**

安全认证和安全检测是确保电力监控系统专用安全产品质量和安全性的重要手段。管理委员会应组织相关机构对产品进行严格的测试和评估，确保其符合安全标准和规范要求。同时，还应推动建立安全认证体系，为合格产品颁发认证证书，提高市场的信任度和产品的竞争力。

- **督促落实供应链安全管控措施**

供应链安全是电力监控系统安全防护的重要环节。管理委员会应督促运营者及相关单位建立健全供应链安全管理制度，加强管理和审核，确保所采购的产品和服务来源可靠、质量过关。同时，还应加强对供应链中关键环节的风险评估和监控，及时发现并处置潜在的安全威胁。

- **组织开展风险评估**

为了全面了解电力监控系统专用安全产品的安全状况和风险水平，管理委员会应定期组织开展风险评估工作。通过收集和分析相关数据和信息，评估产品的安全性、稳定性和可靠性等方面的问题，并提出相应的改进建议和措施。对于存在安全风险的产品，应及时进行通报和处置，防止安全事件的发生和扩散。

- **通报存在安全风险的安全产品**

对于在风险评估或安全检测中发现存在安全风险的电力监控系统专用安全产品，管理委员会应及时进行通报。通报内容应包括产品的名称、型号、生产厂家、安全风险类型及等级等信息，以便相关单位及时采取措施进行处置和防范。同时，还应加强对通报产品的跟踪和监管，确保其得到妥善处理和解决。

第二十五条

原文：

管理委员会建立议事机制，国家能源局和政府有关部门可以派员参加管理委员会有关会议。管理委员会应当于每年 11 月 1 日向国家能源局报告工作开展情况，包括但不限于：工作章程制修订情况，电力监控系统专用安全产品目录及技术规范制修订情况，安全认证和安全检测工作开展情况，运营者专用安全产品管理情况，风险评估及通报情况等。管理委员会运作出现重大问题时应当提请国家能源局组织协调解决。

解读：

对电力监控系统实施全面而深入的监督管理是国家能源局的主体职责之一。管理委员会应依据电力监控系统专用安全产品管理要求，建立议事机制，国家能源局和政府有关部门可以派员参加管理委员会有关会议。管理委员会应每年 11 月 1 日向国家能源局提交相关工作报告，详细阐述具体工作的开展情况。

第二十六条

原文：

运营者应当选用经管理委员会组织检测认证合格的电力监控系统专用安全产品，不得选用经管理委员会通报存在供应链安全风险的产品。运营者对专用安全产品的采购、运行、退役等全过程安全管理负责。

解读：

此条目明确了运营者对电力监控系统专用安全产品的安全管理职责，包括专用安全产品的采购、运行、退役等环节的安全管理。

- **选用合格产品**

运营者应当优先选用经管理委员会组织检测认证合格的电力监控系统专用安全产品。这些产品已经通过了严格的安全测试和评估，能够满足电力监控系统对安全性的要求。通过选用合格产品，运营者可以有效降低系统遭受安全攻击的风险。

- **避免选用风险产品**

运营者应当坚决避免选用经管理委员会通报存在供应链安全风险的产品。这些产品可能存在未知的安全漏洞或缺陷，一旦被恶意利用，将可能对电力监控系统造成严重的安全威胁。因此，运营者在采购过程中应仔细核对产品清单和通报信息，确保不选用风险产品。

- **全过程安全管理**

运营者应对电力监控系统专用安全产品的采购、运行、退役等全过程进行安全管理。在采购阶段，运营者应制定严格的采购标准和流程，确保所采购的产品符合安全要求；在运行阶段，运营者应建立健全的运行管理制度和应急预案，及时发现并处理潜在的安全问题；在退役阶段，运营者应妥善处理废旧产品，防止其成为安全隐患。

第二十七条

原文：

电力监控系统安全防护方案、安全测试评估报告和漏洞隐患细节等有关资料应当按国家有关要求做好保密工作。管理委员会和运营者等应当按国家有关要求做好保密工作，禁止关键技术和产品的扩散。

解读：

此条目与发改委[2014]14 号令《电力监控系统安全防护规定》中保密管理安全要求保持一致，在资料保密、工作机制、运营者等方面提出了具体要求。

- **资料保密**

电力监控系统安全防护方案及相关资料可能涉及国家安全战略和关键技术，一旦泄露，可能对国家安全和稳定造成重大威胁。应采取措施限制敏感资料的接触范围，实行分级管理，确保只有经过授权的人员才能接触和使用相关资料；对存放敏感资料的场所实施物理防护，如安装门禁

系统、监控摄像头等；对电子文档进行加密存储和传输，防止数据泄露。

- **工作机制层面**

制定保密制度：工作机制应制定详细的保密制度，明确保密范围、保密责任、保密措施和保密纪律等内容，确保保密工作有章可循。

加强人员管理：对参与电力监控系统安全防护方案制定、安全测试评估及漏洞隐患排查的人员进行严格的保密审查，签订保密协议，并进行定期的保密教育和培训。

- **管理委员会和运营者层面**

建立健全保密管理体系：管理委员会和运营者应建立健全的保密管理体系，明确保密工作责任部门和责任人，制定并实施保密计划和措施。

加强供应链管理：在采购电力监控系统专用安全产品时，应要求供应商遵守保密协议，确保关键技术和产品在供应链中的安全可控。

定期进行保密检查：管理委员会和运营者应定期对自身的保密工作进行检查和评估，及时发现并纠正存在的问题和隐患。

加强应急响应：建立完善的应急响应机制，一旦发生保密事件或泄密风险，能够迅速启动应急预案，采取有效措施减少损失和影响。

- **禁止关键技术和产品的扩散**

为了防止关键技术和产品的扩散，应采取以下措施：

限制技术输出：对于涉及国家安全的核心技术和产品，应严格控制其出口和转让，避免技术泄露和扩散。

加强技术保护：对关键技术进行专利申请和知识产权保护，加强技术壁垒，防止他人非法获取和使用。

签订保密协议：在与合作伙伴、供应商等外部单位合作时，应签订保密协议，明确保密责任和保密要求，防止技术泄露。

加强宣传教育：加强对员工的保密宣传教育，提高员工的保密意识和责任心，确保他们了解并遵守保密规定。

第四章 应急措施

第二十八条

原文：

重要电力监控系统应当建立系统备用和恢复机制，对重要设备冗余配置，对重要的数据定期备份，并定期进行恢复性测试，支撑系统故障的快速处理和恢复，保障电力监控系统业务连续性。

解读：

电力监控系统的稳定运行对于电力系统的安全至关重要，重要电力监控系统应建立系统备用和恢复机制，对重要设备冗余配置，对重要数据定期备份，并定期进行恢复性测试，确保电力供应稳定性和业务连续性。

- **系统备用机制**

a） 备用系统建设

重要电力监控系统应建立独立的备用系统，该系统在主系统出现故障时能够迅速接管业务，确保监控工作的连续进行。

备用系统应与主系统保持同步更新，确保在切换时能够无缝衔接，避免数据丢失或业务中断。

b） 冗余配置

对重要设备进行冗余配置，如关键服务器、网络设备、存储设备等，采用双机热备、集群等技术手段，提高系统的可靠性和可用性。

冗余设备应定期进行切换测试，确保在需要时能够正常接管业务。

- **数据备份与恢复机制**

a） 定期备份

对重要数据进行定期备份，包括配置文件、业务数据、日志信息等。备份频率应根据数据的重要性和更新速度来确定，一般建议每日或每周进行全量备份，并根据需要进行增量备份。

备份数据应存储在安全可靠的位置，如异地灾备中心，以防止本地灾难导致的数据丢失。

b） 恢复性测试

定期对备份数据进行恢复性测试，验证备份数据的完整性和可恢复性。测试应包括数据恢复

速度、恢复后系统的稳定性等方面。

通过恢复性测试，可以及时发现备份策略中的问题和不足，并进行相应的调整和优化。

- **快速故障处理和恢复**

a） 故障检测与定位

建立智能化的故障检测系统，通过实时监测和数据分析，及时发现电力监控系统中的异常和故障。

利用故障定位技术，快速准确地确定故障位置和原因，为后续的故障处理提供有力支持。

b） 快速响应与恢复

制定详细的故障处理流程和应急预案，明确各环节的职责和操作步骤。

在发现故障后，立即启动应急预案，组织相关人员进行快速响应和处理。利用备用系统和恢复机制，尽快恢复系统的正常运行，减少故障对电力供应的影响。

- **其它安全保障措施**

a） 加强人员培训

定期对运维人员进行培训和演练，提高员工对电力监控系统备用和恢复机制的理解和操作能力。

加强与其他相关部门和单位的沟通协调，形成合力共同应对电力系统中的突发事件。

b） 完善管理制度

制定和完善电力监控系统备用和恢复机制的管理制度，明确各项工作的标准和要求。

加强对制度执行情况的监督检查和考核评估，确保各项措施得到有效落实。

第二十九条

原文：

健全电力监控系统安全的联合防护和应急机制，制定应急预案并定期开展演练。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置，定期组织联合演练。

当遭受网络攻击，电力监控系统出现异常或者故障时，运营者应当立即启动应急预案，向相应电力调度机构以及当地国家能源局派出机构报告，并联合采取紧急防护措施，防止事态扩大，同时注意保护现场，以便进行调查和溯源取证。

解读：

“以信息共享为基础的协同联防”是国家关键信息基础设施开展安全保护工作应遵循的三大基本原则之一。

国家关键信息基础设施的电力监控系统应依据国家及电力行业在应急预案、网络安全事件处置等方面的安全要求，健全电力监控系统安全的联合防护和应急机制。

- **联合防护机制**

跨部门协作：建立由电力调度机构、网络安全监管部门、电力运营者等多方参与的联合防护机制。各部门明确职责分工，加强信息共享和协同作战能力，共同维护电力监控系统的安全。

技术防护体系：构建多层次、全方位的技术防护体系，包括防火墙、入侵检测/防御系统（IDS/IPS）、安全审计系统、加密通信技术等，对电力监控系统实施全面保护。

安全监测与预警：建立安全监测平台，对电力监控系统进行实时监控和数据分析，及时发现潜在的安全威胁和攻击行为。同时，建立预警机制，对发现的异常情况进行快速响应和处理。

安全培训与意识提升：加强对电力监控系统运维人员的安全培训和意识提升工作，提高他们对网络安全风险的识别、防范和应对能力。

- **应急机制**

制定应急预案：根据电力监控系统的实际情况和安全风险特点，制定详细的应急预案。预案应明确应急处置流程、应急指挥体系、应急资源调配等内容，确保在突发事件发生时能够迅速、有序地开展应急处置工作。

定期演练：定期组织电力调度机构、电力运营者等相关部门开展联合演练。通过模拟真实的网络攻击和系统故障场景，检验应急预案的可行性和有效性，提高应急处置的实战能力。

快速响应与报告：当电力监控系统遭受网络攻击或生产控制区出现异常、故障时，运营者应立即启动应急预案，迅速采取措施进行紧急防护和故障排查。同时，向相应电力调度机构以及当地国家能源局派出机构报告事件情况，请求支援和指导。

现场保护与调查取证：在应急处置过程中，注意保护现场设备和数据，避免破坏和篡改。同时，配合相关部门开展调查取证工作，追踪攻击来源和攻击手段，为后续的安全防护和打击犯罪提供有力支持。

- **电力调度机构的职责**

统一指挥调度：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置工作。在突发事件发生时，根据应急预案的要求和实际情况，迅速作出决策和指挥调度。

组织联合演练：电力调度机构应定期组织相关部门开展联合演练工作。通过演练提高各部门的协同作战能力和应急处置水平，确保在突发事件发生时能够迅速、有效地开展应急处置工作。

信息共享与协调：电力调度机构应加强与相关部门的信息共享和协调工作。在应急处置过程中及时收集、整理和分析相关信息数据为决策提供有力支持；同时协调各部门之间的资源和力量共同应对突发事件的发生。

第五章 监督管理

第三十条

原文：

国家能源局负责制定电力监控系统安全防护相关管理和技术规范，国家能源局及其派出机构依法对电力监控系统安全防护工作进行监督管理，电力调度机构负责技术支持。

运营者应当建立本单位电力监控系统安全防护技术监督体系，全方位开展技术监督工作。电力调度机构对直接调度范围内的下一级电力调度机构、变电站（换流站）、发电厂（站）等涉网部分的电力监控系统安全防护进行技术监督。电力监控系统网络安全技术监督管理办法由国家能源局制定。

解读：

本条明确了国家能源局及其派出机构对电力监控系统的监督管理主体职责，运营者、电力调度机构分别应承担的监督职责，以及具体的监督管理机制。

- **国家能源局的职责**

国家能源局不仅负责制定电力监控系统相关管理和技术规范，还依法对安全防护工作进行严格的监督管理。这种双管齐下的管理方式确保了电力监控系统的安全性和稳定性。

制定规范：国家能源局负责制定电力监控系统安全防护的相关管理和技术规范，包括制定电力监控系统网络安全技术监督管理办法，为整个行业提供统一的指导和标准。这些规范涵盖了安全防护的各个方面，如系统架构设计、安全防护措施、应急响应机制等。

监督管理：国家能源局及其派出机构依法对电力监控系统安全防护工作进行全面的监督管

理。这包括对运营者执行安全防护规范的情况进行检查，对发现的问题进行督促整改，以及对违规行为进行处罚等。

- **运营者的责任**

运营者作为电力监控系统的直接管理者和使用者，承担着建立本单位安全防护技术监督体系的重任。

建立技术监督体系：全方位开展技术监督工作，确保电力监控系统的各个环节都符合安全防护要求。

执行国家规范：严格遵守国家能源局制定的管理和技术规范，确保电力监控系统的安全防护工作有法可依、有章可循。

自我监督与提升：通过内部审查、演练等方式不断提升安全防护能力，及时发现并整改潜在的安全隐患。

- **电力调度机构的职责**

电力调度机构在电力监控系统安全防护中也扮演着重要角色。其主要职责包括：

直接调度范围内的技术监督：对直接调度范围内的下一级电力调度机构、变电站（换流站）、发电厂（站）涉网部分的电力监控系统安全防护进行技术监督，确保这些关键环节的安全可靠。

协助监督管理：国家能源局及其派出机构对电力监控系统安全防护工作进行监督管理时，提供技术支持和协助，共同维护电力监控系统的安全稳定。

第三十一条

原文：

运营者有下列情形之一的，由国家能源局及其派出机构责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款，涉及关键信息基础设施的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）未采取安全分区、边界防护等防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（二）未采取网络安全监测预警等技术措施监测、记录网络运行状态、网络安全事件。

在发生危害网络安全的事件时，未按规定及时报告的，由国家能源局及其派出机构责令改

正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款，涉及关键信息基础设施的重大事件，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

解读：

此条目明确了运营者在电力监控系统安全防护中的责任和义务，违反这些规定时以及在发生危害网络安全的事件时未按规定及时报告时所面临的法律后果。这是为了确保电力监控系统的网络安全，防止因技术疏忽或不当行为而导致的网络安全事件，从而保障电力监控系统的稳定运行和电力供应的连续性。

电力监控系统运营者一旦出现未采取安全分区、边界防护等必要的技术措施、未采取网络安全监测预警等技术措施、未及时报告网络安全事件等情形时，应及时改正。拒不改正或者导致危害网络安全等后果的，应按照以下规定进行处罚：

对于一般的违规行为，罚款金额为一万元以上十万元以下；对直接负责的主管人员处五千元以上五万元以下罚款。

如果涉及关键信息基础设施的违规行为，则罚款金额为十万元以上一百万元以下；对直接负责的主管人员处一万元以上十万元以下罚款。

第三十二条

原文：

运营者拒绝、阻碍国家能源局及其派出机构依法实施的监督检查或依照本规定委托电力调度机构组织开展的技术监督的，由国家能源局及其派出机构责令改正；拒不整改或情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款。

解读：

此条目进一步强调了运营者在电力监控系统安全防护中的合作与配合义务，以及对国家能源局及其派出机构或受其委托的电力调度机构进行监督检查和技术监督的积极响应要求。

首先，运营者必须配合国家能源局及其派出机构依法进行的监督检查工作，以及按照相关规定委托电力调度机构组织的技术监督工作。这种合作与配合是确保监督检查和技术监督有效性的基础。

其次，如果运营者拒绝或阻碍上述监督检查或技术监督工作的进行，将首先由国家能源局及其派出机构责令其改正。这意味着运营者有机会纠正其不当行为，以避免进一步的法律后果。

最后，如果运营者拒不整改或情节严重，将面临罚款的处罚。罚款金额根据违规情节的严重程度而定，但明确规定了最低五万元、最高五十万元的罚款范围。对于直接负责的主管人员和其他直接责任人员，也将处以一万元以上十万元以下的罚款。

第三十三条

原文：

电力调度机构在技术监督过程中发现被监督电力监控系统存在可能导致网络安全事件的重大安全风险时，可以采取断开其数据网络连接、断开其电力一次设备连接等措施管控安全风险。

解读：

电力调度机构在电力监控系统的技术监督中扮演着至关重要的角色。当发现被监督的电力监控系统存在可能导致网络安全事件的重大安全风险时，电力调度机构有权并应当及时采取安全措施来管控这些风险，例如断开其数据网络连接、断开其电力一次设备连接等，以确保电力系统的整体安全稳定运行。

第三十四条

原文：

对于其他不符合本规定要求的，由国家能源局及其派出机构责令改正；拒不改正或者导致危害网络安全等后果的，由国家能源局及其派出机构依法依规予以处罚。

解读：

此条目强调了国家能源局及其派出机构在电力监控系统安全防护领域的监管权威性和执行力。

对于运营者或其他相关方在电力监控系统安全防护工作中不符合《电力监控系统安全防护规定》要求的情况，国家能源局及其派出机构将采取一系列措施来确保规定的执行和电力监控系统的安全，包括责令相关方进行改正、实行处罚措施等。

第三十五条

原文：

对于因违反本规定，造成电力监控系统故障的，由其运营者按相关规程规定进行处理；导致电力设备事故或者造成电力安全事故（事件）的，按国家有关事故（事件）调查规定进行处理。

解读：

此条目明确了电力监控系统运营者因违规操作而引发系统故障或更严重后果时的处理原则，规定了相应的处理方式和责任追究程序。

- **引发系统故障的**

对于因违反本规定而造成电力监控系统故障的情况，由其运营者按照相关规程规定进行处理。这意味着，当电力监控系统运维人员因未遵守安全防护规定而导致系统故障时，其运营者将承担起监管和处理的职责。运营者将依据内部规章制度或行业规程，对违规行为进行调查、评估，并采取相应的纠正和处罚措施。

- **导致电力设备事故或者造成电力安全事故（事件）的**

如果违规行为导致了电力设备事故或者电力安全事故（事件）的发生，那么将按照国家有关事故（事件）调查规定进行处理。这种情况下，违规行为的后果更为严重，已经影响到了电力系统的安全稳定运行和电力供应的可靠性。因此，需要依据国家层面的法律法规和事故调查规定，例如《关键信息基础设施安全保护条例》《电力安全事故应急处置和调查处理条例》《电力安全事件监督管理规定》等，进行更为全面和深入的事故调查、责任认定和处罚工作。

第六章 附则

第三十六条

原文：

本规定下列用语的含义或范围：

（一）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设备，以及作为基础支撑的通信设施及数据网络等，包括但不限于实现继电保护和安全自动控制、调度监控、变电站(换流站)监控、发电厂监控、新能源发电监控、分布式电源监控、储能电站监控、虚拟电厂监控、配电自动化、变电站集控、发电集中监视、发电机励磁和调速、电力现货市场交易、直流控制保护、负荷监控、计费控制等功能的系统，以及支撑以上功能的通信设施、数据网络及配套网管系统。

（二）电力监控专用网络，是指承载电力监视和控制业务的专用广域数据网络、专用局域网络以及专用通信线路等，如调度数据网(各级电力调度专用广域数据网络)、发电企业集中监视中心与电厂之间的专用数据网络、调度自动化和厂站自动化的专用局域网继电保护和安全自动装置使用的专用通信通道等。

（三）物理访问控制，是指电力监控系统所处的物理环境出入口安排专人值守或配置电子门禁系统，鉴别和控制人员进出。

（四）电力监控系统专用安全产品，是指按照电力监控系统安全防护需求专门设计、研发、制造的网络安全防护产品，如电力专用横向单向安全隔离装置、电力专用纵向加密认证装置等。

解读：

此条目明确了本《规定》中主要名词用语的含义或范围。

第三十七条

原文：

本规定自 2025 年 1 月 1 日起施行。2014 年 8 月 1 日国家发展改革委公布的《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）同时废止。

解读：

此条目对本《规定》自何时起施行进行了说明，明确随着本《规定》的正式施行，《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）同时废止的要求。