电力监控系统安全防护规定

第一章 总则

第一条 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。

第二条 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。

第三条 电力监控系统安全防护应当落实国家网络安全等级保护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。

第二章 安全技术

第四条 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）和管理信息区（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。

第五条 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。

第六条 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。

第七条 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以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。

第八条 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。

第九条 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。

第十条 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。

第十一条 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。

第十二条 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。

第十三条 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。

第十四条 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，禁止存储重要的数据，并使用可信验证措施加强通信代理模块保护。

第十五条 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。

第十六条 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。

第十七条 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。

第三章 安全管理

第十八条 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。

第十九条 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。

第二十条 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，可以按业务、地域分别设立安全接入区。

第二十一条 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。

第二十二条 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。

第二十三条 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。

第二十四条 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。

第二十五条 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日前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。

第二十六条 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。

第二十七条 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。

第四章 应急措施

第二十八条 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。

第二十九条 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。

第五章 监督管理

第三十条 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。

第三十一条 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。

第三十二条 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；拒不改正或情节严重的，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。

第三十三条 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。

第三十四条 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。

第三十五条 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。

第六章 附　则

第三十六条 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。

第三十七条 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。