

强化电力监控安全防护体系，支撑新型电力系统建设——《电力监控系统安全防护规定》专家解读

发布时间：2024-12-12 来源：国家发展改革委

近日，国家发展改革委在深入调查研究、广泛听取意见的基础上修订出台了《电力监控系统安全防护规定》（国家发展和改革委员会令 2024 年第 27 号，取代原 2014 年 14 号令，以下简称《规定》），《规定》以习近平新时代中国特色社会主义思想为指导，深入落实“四个革命、一个合作”能源安全新战略，适应新型能源体系和新型电力系统建设的要求，为我国新型电力系统建设提供了有力支撑。

一、《规定》的修订具有重要意义

（一）体现了国家主管部门对网络安全高度重视。

自 2000 年二滩水电站遭受网络攻击之后，国家电力行业主管部门高度重视，已相继颁布了三个相关法令，指导电力行业逐步建立了比较完善的电力监控系统安全防护体系，并形成了两个国家标准。2002 年，国家经济和贸易委员会颁布第 30 号令，明确电力控制系统必须采用专用通信网络和计算机系统；2005 年，国家电力监管委员会颁布第 5 号令，提出了“安全分区、网络专用、横向隔离、纵向认证”的十六字方针；2014 年，国家发展改革委颁布第 14 号令，提出建立电力监控系统安全防护体系，核心内容形成了国家标准 GB/T 36572-2018《电力监控系统网络安全防护导则》，防护体系由三维空间和一维时间构成：安全防护技术作为 X 轴（包括基础安全、结构安全、本体安全、可信免疫），应急备用措施作为 Y 轴（包括拟态冗余备用、横向三道防线、纵向三道防线）、全面安全管理作为 Z 轴（包括全部设备管理、全体人员管理、全生命周期管理）、体系的不断发展完善作为 t 轴（时间轴，已经发的三个法令代表三大阶段，现在进入第四阶段）。该标准于 2022 年泛化为 GB/Z 41288-2022《信息安全技术 重要工业控制系统网络安全防护导则》，指导其他重要工控领域建立本领域的网络安全防护体系。本次新颁布的《规定》是二十多年来国家电力行业主管部门相继颁布的第四个法令，体现了国家对电力监控系统安全的持续高度关注。

（二）贯彻党中央网络安全强国战略部署的重要举措。

习近平总书记多次强调，没有网络安全就没有国家安全，没有信息化就没有现代化。近年来，随着《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《中华人民共和国数据安全法》等法律法规陆续颁布，我国正从网络大国向网络强国转变，网络安全已上升到国家战略，事关国家安全和经济发展、事关广大人民群众工作生活。《规定》的颁布既秉承国家新的战略要求，又适应日益严峻的网络安全形势，对加强电力行业网络安全管理，规范系统运行提供了具体指引。

（三）顺应新型电力系统发展建设的客观要求。

2022 年国家关于建设电力市场体系、“十四五”能源体系规划中，明确了构

建新型电力系统是国家能源战略的重要发展方向。在新型电力系统建设背景下，新业务形态和运行模式不断涌现，原《规定》在指导网络安全工作实践过程中需要不断发展完善。如新型电力系统接入主体更多样、边端分布更广泛、交互方式更丰富等特征增加了网络安全防护的难度、降低了防护体系的强度。《规定》分析了新型电力系统环境下电源结构、电网形态、业务模式、技术基础等方面的变化带来的安全风险，从技术、应急、管理三个层面明确了防护标准，细化了防护措施，为电力系统安全发展保驾护航。

二、《规定》完善了电力监控系统安全防护要求

（一）明确电力监控系统范围。《规定》对电力监控系统的定义进行了更全面的描述，以系统功能描述的形式，对电力监控系统的具体定义范围进行解释，涵盖了从发电、输电、变电、配电到用电的全链条新型业务形态。在适用范围上，《规定》不仅适用于传统公用的各级电网、各类变电站（换流站、开关站等）和各类发电厂，也适用于与主网并网运行的地方电网或专用电网、以及各类自备发电厂和变电站，还将与电力监控系统相关的产品制造、安装调试等单位纳入监管范围，强调供应商须承诺所提供的设备和系统不存在恶意安全隐患，并终身负责，凸显了对全系统安全和供应链安全的重视，增强了安全防护措施的适用性。

（二）深化防护原则与策略。随着电力系统源网荷储互动频繁，网络空间边界不再局限于封闭的环境，安全威胁的源头和形式更加多样。《规定》明确提出了“安全免疫”和“态势感知”的防护要求，通过引入主动免疫、智能监测、实时溯源、多功能预警等前沿技术手段，提升防护体系的层次感和动态感，确保实时感知潜在威胁，提高系统的主动应急响应能力，帮助应对多样复杂的网络攻击场景。

（三）完善违规事项和罚则。《规定》根据《网络安全法》《关键信息基础设施安全保护条例》等上位法律法规及相关网络安全管理制度要求，首次规定了运营者的违规事项及对应的处罚标准，罚则包括责令改正、警告、罚款三种，不仅提升了《规定》的教育引导作用，强调了运营者的安全主体责任和义务，又强化了《规定》的严肃性和权威性，确保各级机构的监管穿透和下沉，保障各项措施高效落地执行。

三、《规定》有助于解决安全防护面临的突出问题

（一）深化生产控制系统本体内生安全。经过多年的持续发展建设，早期投运的电力生产控制系统及网络设施已陆续进入更新换代阶段。《规定》要求充分利用技改大修和更新换代的机会，采用更先进实用的技术和更安全的产品，逐步构建更安全的电力监控系统，不断完善电力监控安全防护体系。

（二）强化安全接入区防护措施。安全接入区是生产控制区与采用非电力监控专用网络的终端之间的一个过渡区域，《规定》明确了安全接入区的功能定位和防护要求。安全接入区内应简化功能配置，主要实现代理和转发功能，控制指令需要进行端到端的身份认证，防止数据在传输过程中被窃取或篡改。同时，应使用可信验证措施加强通信代理模块的保护，提升安全接入区的安全。相关措施有效强化了负荷控制与管理、配电自动化、用电采集、分布式能源监控等低压电力监控系统中涉控功能模块的网络安全防护。

（三）强化电力监控系统专用安全产品管理。电力监控系统专用安全产品，

是落实“安全分区，网络专用，横向隔离，纵向认证”结构安全原则，构建网络安全防护体系的核心设备。《规定》明确由国家电力调度控制中心牵头组建电力监控系统专用安全产品管理委员会，保障电力监控系统专用安全产品安全可控，对推动专用安全产品技术更新换代和全生命周期安全管理具有积极意义。

（四）优化技术监督管理。《规定》明确不同主体的技术监督职责和范围，运营者应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，电力调度机构应按照《规定》要求开展涉网部分电力监控系统技术监督工作。《规定》还增加技术监督过程中风险管控措施，明确存在重大安全风险情况时，可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。

此次修订印发的《规定》全面贯彻党的二十大精神，深入落实党中央、国务院决策部署，对安全技术、安全管理、应急措施、监督管理等方面进行了系统的修订。我们要在工作中认真学习领会《规定》修订精神，确保相关要求和措施落地，切实提高电力监控系统安全防护水平，保障电力生产及供应可靠，更好的支撑新型电力系统建设。（作者：辛耀中 工业控制系统产业联盟理事长、原国家电网公司国家电力调度控制中心副主任）