监管委员会令

第 5 号

《电力二次系统安全防护规定》已经国家电力监管委员会主席办公会议通过，现予公布，自2005年2月1日起施行。

主　席　柴松岳

二〇〇四年十二月二十日

电力二次系统安全防护规定

总　则

第一条　为了防范黑客及恶意代码等对电力二次系统的攻击侵害及由此引发电力系统事故，建立电力二次系统安全防护体系，保障电力系统的安全稳定运行，根据《中华人民共和国计算机信息系统安全保护条例》和国家有关规定，制定本规定。

第二条　电力二次系统安全防护工作应当坚持安全分区、网络专用、横向隔离、纵向认证的原则，保障电力监控系统和电力调度数据网络的安全。

第三条　电力二次系统的规划设计、项目审查、工程实施、系统改造、运行管理等应当符合本规定的要求。

技术措施

第四条 发电企业、电网企业、供电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(安全区Ⅰ)和非控制区(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，但是应当避免通过广域网形成不同安全区的纵向交叉连接。

第五条 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。

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。

第六条 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。

第七条 在生产控制大区与广域网的纵向交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。

第八条 安全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大区和管理信息大区之间边界的通用网络服务。

生产控制大区中的业务系统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。

第九条 依照电力调度管理体制建立基于公钥技术的分布式电力调度数字证书系统，生产控制大区中的重要业务系统应当采用认证加密机制。

安全管理

第十条 国家电力监管委员会负责电力二次系统安全防护的监管，制定电力二次系统安全防护技术规范并监督实施。

电力企业应当按照“谁主管谁负责，谁运营谁负责”，的原则，建立健全电力二次系统安全管理制度，将电力二次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。

电力调度机构负责直接调度范围内的下一级电力调度机构、变电站、发电厂输变电部分的二次系统安全防护的技术监督，发电厂内其他二次系统可由其上级主管单位实施技术监督。

第十一条 建立电力二次系统安全评估制度，采取以自评估为主、联合评估为辅的方式，将电力二次系统安全评估纳入电力系统安全评价体系。

对生产控制大区安全评估的所有记录、数据、结果等，应按国家有关要求做好保密工作。

第十二条 建立健全电力二次系统安全的联合防护和应急机制，制定应急预案。电力调度机构负责统一指挥调度范围内的电力二次系统安全应急处理。

当电力生产控制大区出现安全事件，尤其是遭受黑客或恶意代码的攻击时，应当立即向其上级电力调度机构报告，并联合采取紧急防护措施，防止事件扩大，同时注意保护现场，以便进行调查取证。

第十三条 电力二次系统相关设备及系统的开发单位、供应商应以合同条款或保密协议的方式保证其所提供的设备及系统符合本规定的要求，并在设备及系统的生命周期内对此负责。

电力二次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，禁止关键技术和设备的扩散。

第十四条 电力调度机构、发电厂、变电站等运行单位的电力二次系统安全防护实施方案须经过上级信息安全主管部门和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。

接入电力调度数据网络的设备和应用系统，其接入技术方案和安全防护措施须经直接负责的电力调度机构核准。

第十五条 电力企业和相关单位必须严格遵守本规定。

对于不符合本规定要求的，应当在规定的期限内整改；逾期未整改的，由国家电力监管委员会根据有关规定予以行政处罚。

对于因违反本规定，造成电力二次系统故障的，由其上级单位按相关规程规定进行处理；发生电力二次系统设备事故或者造成电力事故的，按国家有关电力事故调查规定进行处理。

附　则

第十六条　本规定下列用语的含义：

（一）电力二次系统，包括电力监控系统、电力通信及数据网络等。

（二）电力监控系统，是指用于监视和控制电网及电厂生产运行过程的、基于计算机及网络技术的业务处理系统及智能设备等。包括电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量计费系统、实时电力市场的辅助控制系统等。

（三）电力调度数据网络，是指各级电力调度专用广域数据网络、电力生产专用拨号网络等。

（四）控制区，是指由具有实时监控功能、纵向联接使用电力调度数据网的实时子网或专用通道的各业务系统构成的安全区域。

（五）非控制区，是指在生产控制范围内由在线运行但不直接参与控制、是电力生产过程的必要环节、纵向联接使用电力调度数据网的非实时子网的各业务系统构成的安全区域。

第十七条 本规定未作规定的事项，适用原国家经济贸易委员会2002年5月8日发布的《电网和电厂计算机监控系统及调度数据网络安全防护规定》。

第十八条 本规定自2005年2月1日起施行。