国家电网公司信息安全等级保护安全建设整改工作经验介绍

国家电网公司信息化工作部　王继业

国家电网公司作为全球最大的公用事业企业，运转着世界上用户规模最大的信息系统，按照公司实现数字化电网和信息化企业的目标，已基本建成了覆盖全国的生产控制系统和管理信息系统。信息安全作为信息化深入推进的重要保障，对电网安全有着重大影响。国家电网公司将自身信息安全建设和国家等级保护制度要求有机结合，按照公安部和国家电监会的要求，加强自主知识产权安全措施的研发与部署，在信息系统定级备案工作的基础上，依据等级保护相关标准，全面开展信息安全等级保护安全建设整改工作。目前，全国12个网省公司已完成建设任务，18个网省公司计划年底完成，21个直属单位已全面开展相关工作。

一、主要工作方法

1. 全局规划，典型设计

国家电网公司结合电网安全需求，依照等级保护相关标准要求，对电网信息安全工作进行整体规划，实施“双网双机、分区分域、等级防护、多层防御”的信息安全防护总体策略。其核心内容是将管理信息网划分为信息内网和信息外网，信息内外网分别使用物理独立的服务器和桌面计算机，并采用逻辑强隔离策略进行隔离。同时在信息内网，按照“统筹资源、重点保护、适度安全”的原则，依据信息系统安全等级定级结果，采用“二级系统统一成域，三级系统独立分域”的方法划分安全域。在信息外网，按照不同应用，划分为外网应用系统域和外网桌面终端域。国家电网公司针对各安全域防护特点，按照等级保护要求，从边界、网络、主机、应用四个层次进行安全防护典型设计。在边界方面应用国产防火墙和具有自主知识产权的逻辑强隔离装置、正反向隔离装置等措施，使边界的内部不受来自外部的攻击，也防止内部人员跨越边界对外实施攻击，或外部人员通过开放接口、隐通道进入内部网络；在网络方面采用国产网络设备和安全设备，并对经由网络传输的业务信息流进行安全防护；在主机方面开展主机安全加固，采用信息保障技术确保业务数据在进入、离开或驻留服务器与桌面主机时保持可用性、完整性和保密性；在应用方面，依照国家和公司标准，从用户身份认证、访问控制、安全审计、通信数据保护、容错能力等多方面进行应用系统安全改造和建设。同时，在数据保护上，使用安全移动存储介质进行内外网数据交换，启动北京、上海、西安三个集中式信息系统容灾中心建设，确保不因人为或自然的原因，造成数据信息丢失和信息系统支持的业务功能停止或服务中断。

2. 深化标准，强化测评

国家电网公司结合电网信息安全防护的特殊性，以国家信息系统等级保护基本要求和电力行业信息安全要求为基础，对电网等级保护标准指标进行深化、扩充，将国家等级保护二级系统技术指标项由79个扩充至134个，三级系统技术指标项由136个扩充至184个，并在试点单位

实施验证。在明确电网等级保护标准指标的基础上，国家电网公司组织内部测评队伍，在等级保护安全建设整改之前，从技术和管理两个方面对信息系统进行现状评估，寻找信息系统在物理安全、网络安全、主机安全、应用安全、数据安全以及管理要求上与相应安全等级标准的差距，并进行差距汇总和分析，有针对性地提出改进措施，制定整改方案，逐项进行落实。在等级保护安全建设整改之后，电网公司结合安全建设整改工程验收工作，组织内部测评队伍进行效果测评。内部测评结束后，再聘请国家信息安全等级保护工作协调小组备案的测评机构进行等级测评，验证与国家等级保护要求的符合性。通过公司内部和专业测评机构的两级测评，有效推进了国家、行业、电网信息安全标准在电网企业的落实完善。

3. 完善体系，加强管理

按照等级保护管理工作要求，国家电网公司完善了信息安全管理体系。公司各级单位成立了信息化工作领导小组，落实了信息安全各级责任；建立了完善的信息安全管理、信息系统运行、信息内容保密等规章制度和操作规程；建立了与公司信息化发展相适应的信息安全运行管理机制、技术督查机制、事件通报机制、责任追究机制、应急响应机制和风险管理机制。同时运用技术手段加强日常管理，将等级保护融入日常安全运行与管理中。建设了一体化信息安全运行监管平台，实现对电网信息网络设备、安全设备、网络边界、应用系统、桌面终端的日常实时安全监测，提高重要信息系统日常安全监测、预警、应急响应与防御能力；建设了信息安全综合工作平台，利用现代化、信息化手段，以信息安全等级保护工作为核心，涵盖信息安全管理、风险评估、事件应急处置、资源管理、实时监测、统计分析、政策标准库等信息安全工作主要内容。平台整合了国家电网公司的信息安全日常管理、运行与督查工作需求，将国家信息安全等级保护工作要求细化为可量化、可操作的技术和管理指标，按照总部、网省公司、地市公司的国网信息安全管理模式，实现信息安全日常工作情况的上报、监管、核查等，能够在线查询、统计信息系统定级、备案、安全建设整改、等级测评和安全检查等主要工作情况，使国网各级单位的信息安全工作特别是等级保护工作常态化。

二、主要工作经验

1. 领导高度重视，经费和人员保障有力

长期以来，国家电网公司党组高度重视信息安全，始终坚持一手抓信息化建设，一手抓信息安全工作。公司坚决贯彻信息安全等级保护制度要求，在体制和机制上确保各项工作任务落到实处。公司不断加大信息安全资金投入，强化信息安全队伍建设，完善了公司和网省两级运行服务队伍建设；建立了中国电科院和国网电科院两个信息安全实验室；建立了380人的两级信息安全技术督查队伍，负责监督、督促、指导各单位信息安全工作落实；组建了信息安全专家组，组织对重大信息安全决策、事件会商研判。

2. 吃透政策标准，先行试点示范

为确保等级保护实施工作取得实效，国家电网公司通过国家发改委立项审批，开展了“电网信息安全等级保护纵深防御示范工程”建设，选择了浙江省电力公司、陕西省电力公司、中国电力财务有限公司进行试点示范，三个试点单位除进行边界、网络、主机、应用数据的等级保护纵深防御建设外，其等级保护建设全部采用国产产品，核心安全防护设备采用自主研发的逻辑强隔离装置和安全移动存储介质系统，核心信息系统和基础类、通用类以及专业类应用系统采用全国产服务器、操作系统、数据库和中间件，并开展了大量细致的国产化测评与验证工作。对实施等级保护的系统，强化信息系统全生命周期过程管控，实施了标准化建设、安全测评、风险测试、知识产权管理等系列措施。通过示范工程建设，进一步熟悉掌握了国家信息安全等级保护工作相关政策，在实践中进一步验证了等级保护的相关标准，并在实践中与电网特色有机结合，取得了良好的试点、示范效果，提升了电网信息安全综合防御能力，摸索出在电网公司开展等级保护工作的经验，为等级保护在电网的全部推广应用奠定了基础。

3. 统筹组织安排，确保各项措施落到实处

为加快等级保护在国网范围的推广应用，国家电网公司制定了《信息安全等级保护建设的实施指导意见》，按照“统筹组织、统一规范、全面覆盖”的实施原则，规范了包括信息系统定级、符合性评估、建设方案设计、实施建设、等级测评的信息安全等级保护实施流程，在信息安全等级保护定级备案工作的基础上，统一组织了机房物理环境整改、安全域划分与实现、边界网络防护、安全配置加固、应用及数据安全防护、信息安全管理完善、建设信息安全综合工作平台等七方面工作，逐步构建国网上下一致的以信息安全等级保护为核心内容的安全防护体系。