ICS 35.240.50
F 07

中华人民共和国国家标准

GB/T 37138—2018

电力信息系统安全等级保护实施指南

Implementation guide for cyber security classified protection of electric power information system

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家能源局提出。

本标准由全国电力监管标准化技术委员会(SAC/TC 296)归口。

本标准起草单位:国家能源局信息中心、中国南方电网公司、国家电力投资集团公司、中国长江三峡集团公司、全球能源互联网研究院有限公司、北京卓识网安技术股份有限公司、中国电力科学研究院有限公司、国网电力科学研究院有限公司、国电南京自动化股份有限公司、南方电网科学研究院有限责任公司、中国软件评测中心。

本标准主要起草人:梁建勇、胡红升、王保喜、陈雪鸿、阴玉清、李焕、叶世超、陶文伟、王静、李旸照、张鋆、毛澍、房磊、赵婷、焦安春、高艳坤、于学军、李凌、刘育辰、吴国华、秦学嘉、丁晓玉、刘寅、张敏、郁宝坤、张五一、许爱东、陈华军、蒙家晓、周锋、郝鑫。

引　言

为规范电力信息系统安全等级保护实施的流程、内容和方法，加强电力信息系统的安全管理，防范网络攻击对电力信息系统造成的侵害，保障电力系统的安全稳定运行，依据国家和行业有关政策，制定本标准。

在对电力信息系统实施网络安全等级保护的过程中，除使用本标准外，在不同的阶段，还应参照其他有关网络安全等级保护的标准开展工作。

电力信息系统安全等级保护实施指南

1 范围

本标准规定了电力信息系统安全等级保护实施的基本原则、角色和职责，以及定级与备案、测评与评估、安全整改、退运等基本活动。

本标准适用于指导电力信息系统安全等级保护的实施。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 25058 信息安全技术 信息系统安全等级保护实施指南

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069 和 GB/T 25058 界定的以及下列术语和定义适用于本文件。

3.1

电力信息系统 electric power information system

与电力企业的生产控制、管理运营相关的信息系统。

注：根据信息系统的责任单位、业务类型和业务重要性及物理位置差异等各种因素，可分为管理信息系统和电力监控系统。

3.2

管理信息系统 management information system

支持电力企业管理经营的信息系统。

注：包括门户网站系统、财务管理系统、人力资源管理系统等。

3.3

电力监控系统 electric power supervision and control system

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智能设备，以及作为基础支撑的通信及数据网络等。

注：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、电能量计量系统、实时电力市场的辅助控制系统、电力调度数据网络等。

3.4

生产控制大区 production control zone

由具有数据采集与控制功能、纵向联接使用专用网络或专用通道的电力监控系统构成的安全区域。

注：一般包括控制区和非控制区。

3.5

管理信息大区　management information zone

生产控制大区之外的，主要由企业管理、办公自动化系统及信息网络构成的安全区域。

4　等级保护实施概述

4.1　基本原则

电力信息系统安全等级保护的核心是对电力信息系统分等级、按标准进行规划、建设、使用。电力信息系统安全等级保护实施过程应满足 GB/T 25058 中对等级保护实施的基本原则，电力监控系统除此之外还应遵循以下特定原则。

4.1.1　结构优先原则

电力监控系统安全防护应坚持“安全分区、网络专用、横向隔离、纵向认证”的总体原则。以结构安全为防护重点，通过优化结构，强化边界防护，实施纵深防御。

4.1.2　联合防护原则

根据电力监控系统在厂网两端的特点和安全保护等级需求，应采用统一分类定级，同步完善厂网两端电力信息系统的安全防护，通过划分统一的安全区，实现厂网两端边界之间的隔离、认证及统一监视。

4.1.3　安全可控原则

关键装置（如：电力专用横向单向隔离装置、电力专用纵向加密认证装置）应经国家有关机构安全检测认证。电力监控系统在设备选型及配置时，不应选用经国家相关管理部门检测认定并经电力行业主管（监管）部门通报存在漏洞和风险的系统及设备，生产控制大区除安全接入区外不应选用具有无线通信功能的设备，电力监控系统在新建、改建、扩建时宜进行安全性测试。

4.1.4　立体防御原则

电力监控系统网络安全防护应逐步建立包括基础设施安全、体系结构安全、系统本体安全、可信安全免疫、安全应急措施、全面安全管理等措施形成的多维栅格状立体防护体系。

4.2　角色和职责

4.2.1　电力信息系统运行单位

电力信息系统运行单位负责依照国家及电力行业网络安全等级保护的管理规范和技术标准，确定电力信息系统的安全保护等级，并在规定的时间内向当地设区的市级以上公安机关备案。

按照国家及电力行业网络安全等级保护管理规范和技术标准，进行电力信息系统安全保护的规划设计；使用符合国家及电力行业有关规定，满足电力信息系统安全保护等级需求的信息技术产品和网络安全产品，开展电力信息系统安全建设或者整改工作。

制定、落实各项安全管理制度，定期对电力信息系统的安全状况、安全保护制度及相应措施的落实情况进行自查，选择符合国家及电力行业相关规定的等级测评机构，定期进行等级测评和安全防护评估。

制定不同等级信息安全事件的响应、处置预案，对电力信息系统的信息安全事件分等级进行应急处置，并定期开展应急演练；按照网络与信息安全通报制度的规定，建立健全本单位信息通报机制，开展信息安全通报预警工作，及时向电力行业主管（监管）部门、属地监管机构报告有关情况。

加强信息安全从业人员考核和管理，从业人员定期接受相应的政策规范和专业技能培训，并经培训合格后上岗。

4.2.2 电力调度机构

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、发电厂涉网部分的电力监控系统安全防护的技术监督。

电力调度机构、发电厂、变电站等运行单位的电力监控系统安全防护实施方案应在经本企业的上级专业管理部门和信息安全管理部门审阅后报相应电力调度机构的审核，方案实施完成后应由上述机构验收。

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应经直接负责的电力调度机构同意。

建立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。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。

4.2.3 电力信息系统安全服务机构

根据电力信息系统运行单位的委托，依照国家及电力信息系统安全等级保护的管理规范和技术标准，协助电力信息系统运行单位完成等级保护建设及整改工作，包括电力信息系统的安全保护等级确定、安全需求分析、安全总体规划、安全建设和安全改造实施、服务支撑平台提供等。

4.2.4 电力信息系统安全等级测评机构

电力信息系统安全等级测评机构根据电力信息系统运行单位的委托，协助电力企业按照国家及电力行业网络安全等级保护的管理规范和技术标准，对已经完成等级保护建设的电力信息系统进行等级测评及安全防护评估，按要求对测评报告进行评审和备案；对信息安全产品供应商提供的产品进行安全测评。

电力信息系统安全等级测评机构应履行相应的义务，包括遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；保守在测评活动中知悉的国家秘密、商业秘密、业务敏感数据和个人隐私，防范测评风险；对测评人员进行安全保密教育，与其签订安全保密责任书，规定应履行的安全保密义务和承担的法律责任，并负责检查落实。

电力信息系统安全等级测评机构可根据信息系统运行单位安全保障需求，提供信息安全咨询、应急保障、安全运维、安全监理等服务。

4.2.5 电力信息系统安全产品供应商

电力信息系统安全产品供应商负责按照国家及电力信息系统安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的网络安全产品，接受安全测评；按照国家有关要求销售网络安全产品并提供相关服务。

电力信息系统专用产品供应商除应做好上述工作外，还应以合同条款或者保密协议的方式保证其所提供的设备及系统符合政策法规的要求，在设备及系统的全生命周期内对其负责；并按照国家有关要求做好保密工作，防范关键技术和设备的扩散。

4.2.6 电力信息系统供应商

电力信息系统供应商应按照电力信息系统安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的电力信息系统，不得设置恶意程序，并按照等级保护相关要求对所开发的电力信息系统进行部署，并提供相关服务。一旦发现其产品和服务存在安全缺陷、漏洞等风险时，应立即采取补救措施

按照规定及时告知用户并向有关主管部门报告。

电力信息系统供应商应为其产品、服务持续提供安全维护；在规定的期限内，不得终止提供安全维护。

电力信息系统供应商提供的产品、服务具有数据采集功能的，应将所采集的数据类型和需求向运行单位说明，并取得同意后方可实施。

在设备选型及配置时，不应选用经国家相关管理部门检测认定并经电力行业主管（监管）部门通报存在漏洞和风险的系统及设备；对于已投入运行的系统及设备，应按照电力行业主管（监管）部门的要求及时配合运行单位进行整改。

4.2.7 电力信息系统设计单位

电力信息系统设计单位规划设计管理信息系统、电力监控系统、智能设备、通信及数据网络时，应明确系统的安全保护需求，设计合理的安全总体方案，制定安全实施计划，负责安全建设工程的技术支撑。在设计过程中，应充分考虑系统整体结构方面与电力信息系统安全防护原则的一致性，与 GB/T 22239 及行业基本要求在技术类各安全层面、控制点、要求项的一致性。

4.2.8 主管部门

参见 GB/T 25058。

4.3 实施的基本活动

电力信息系统安全等级保护实施基本流程见 GB/T 25058。根据电力信息系统监管实际，电力信息系统实施等级保护的基本活动见图 1。

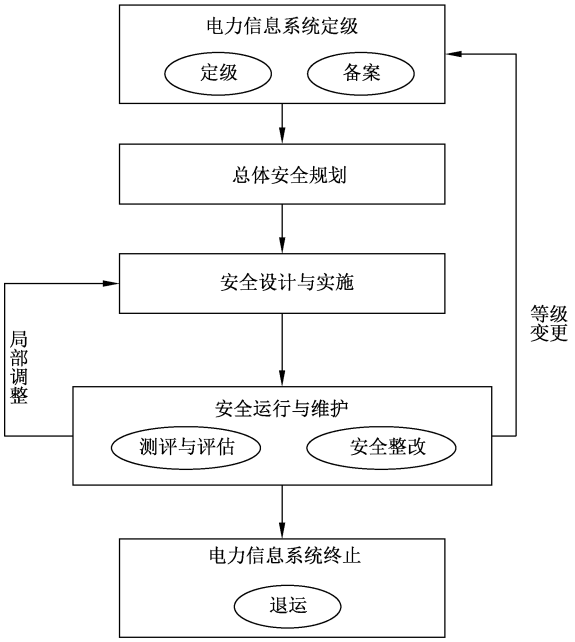

图 1 电力信息系统安全等级保护实施基本活动

在安全运行与维护阶段，电力信息系统因需求变化等原因导致局部调整，而其安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全措施，确保满足等级保护的要求；当电力信息系统发生重大变更导致安全保护等级变化时，应从安全运行与维护阶段进入等级保护对象定级与备案阶段，重新开始一轮网络安全等级保护的实施过程。

5 定级与备案

5.1 定级与备案阶段的流程

电力信息系统运行单位应按照国家和行业有关标准和管理规范，确定所管辖电力信息系统的安全保护等级，组织专家评审，经本企业的上级信息安全管理部门或组织审核、批准后，报公安机关备案，获取《信息系统安全等级保护备案证明》，主管部门有备案要求的，应将定级备案结果报送其备案。

对于新建电力信息系统，第二级及以上电力信息系统，按照国家及行业有关要求（原则上在系统投入运行后 30 日内），电力信息系统运行单位到公安机关办理备案手续。

对于在运电力信息系统，按照国家及行业有关要求（原则上在安全保护等级确定后 30 日内），第二级及以上电力信息系统运行单位到公安机关办理备案手续。

电力信息系统定级与备案阶段的工作流程见图 2。

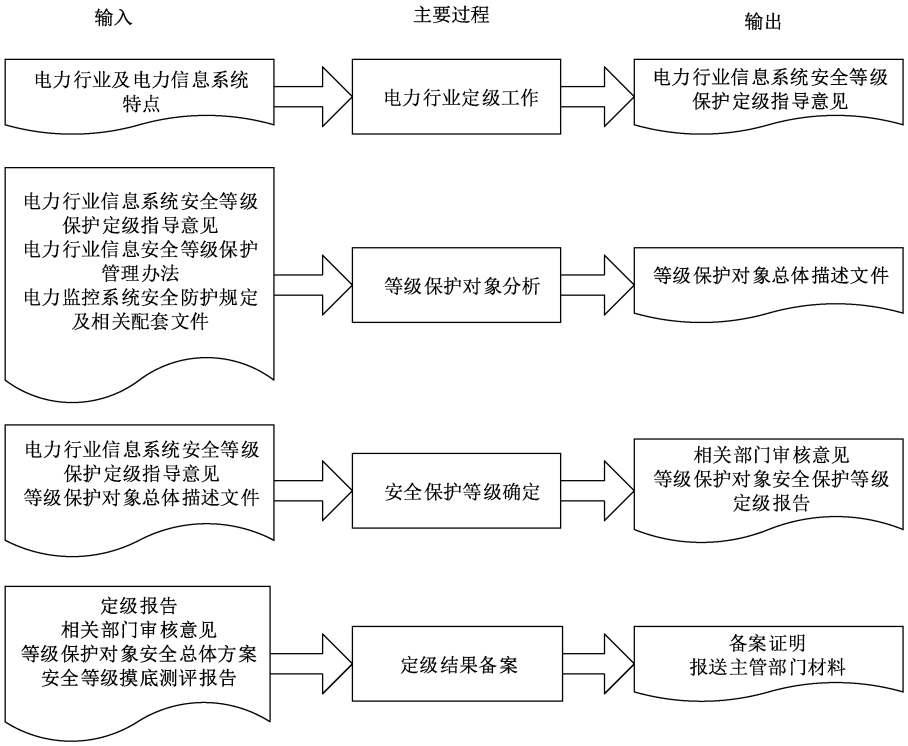

图 2 电力信息系统定级与备案阶段流程

5.2 定级对象分析

5.2.1 电力信息系统分析

本活动的目标是通过收集了解有关电力信息系统的信息，并对信息进行综合分析和整理，分析运行单位的主要社会功能/职能及作用，确定履行主要社会功能/职能所依赖的电力信息系统，整理电力信息系统处理的业务及服务范围，最后依据分析和整理的内容，依据电力行业定级指导意见，形成单位内电力信息系统的总体描述性文档。

参与角色为运行单位，电力信息系统安全服务机构。

活动输入为单位情况说明文档，电力信息系统的立项、建设和管理文档，电力行业定级指导意见。

本活动主要包括以下子活动内容：

a） 识别单位的基本信息

调查了解电力信息系统所属单位的业务范围和类型、所在电力供应环节、单机容量、总装机容量、供热机组容量和服务范围、电压等级、涉网范围、所占电网负荷比例、地理位置、生产产值、上级主管部门等信息，明确单位在保障国家安全、经济发展、社会秩序、公共服务等方面发挥的重要作用。

b） 识别单位的电力信息系统基本信息

了解电力信息系统业务功能、控制对象、业务流程、业务连续性要求、生产厂商以及其他基本情况；分析电力信息系统类别，属于管理信息系统还是电力监控系统。

c） 识别电力信息系统的管理框架

了解电力信息系统的组织管理结构、管理策略、责任部门、部门设置和部门在业务运行中的作用、岗位职责等，明确等级保护对象的安全责任主体。

d） 识别电力信息系统的网络及设备部署

了解电力信息系统的物理环境、网络拓扑结构和硬件设备的部署和设备公用情况，明确电力信息系统的边界。

e） 识别电力信息系统处理的信息资产

了解电力信息系统处理的信息资产的类型，这些信息资产在机密性、完整性和可用性等方面的重要性程度。

f） 电力信息系统描述

对收集的信息进行整理、分析，形成对电力信息系统的总体描述文件。

活动输出为电力信息系统总体描述文件。

5.2.2 定级对象确定

本活动的目标是依据电力信息系统总体描述文件，在综合分析的基础上将电力信息系统进行合理分解，确定所含的定级对象及套数。

参与角色为电力信息系统运行单位，电力信息系统安全服务机构。

活动输入为行业定级指导意见，行业/单位定级工作部署文件，电力信息系统总体描述文件。

本活动主要包括以下子活动内容：

a） 划分方法的选择

以管理机构、业务类型、物理位置、所属安全区域等因素，确定电力信息系统的对象分解原则。

b） 识别等级保护实施安全责任主体

当电力信息系统运行单位和业主单位隶属单位统一且具有唯一运行单位时，可以电力信息系统运行单位作为定级实施主体，如发电机组运行班组，电网调度自动化处室等。当电力信息系统业主单位委托隶属于不同垂直管理关系的运行单位代管运行时，可以电力信息系统业主单位作为定级实施主体，运行单位协助开展定级工作。当两个及以上由不同运行单位运行但属于同一上级业务管理部门时，可以上级业务管理部门作为安全责任主体。

c） 识别定级备案系统的基本特征

作为定级对象的电力信息系统应是由计算机软硬件、计算机网络、处理的信息、提供的服务以及相关的人员等构成的一个人机系统。单个装置或设施不具备定级备案系统特征。

d） 识别电力信息系统承载的业务应用

作为定级对象的电力信息系统应该承载比较“单一的”的业务应用，或者承载“相对独立的”的业务应用。“单一”的业务应用是指该业务应用的业务流程独立，不依赖于其他业务应用，同时与其他业务应用没有数据交换，并且独享各种信息处理设备；“相对独立”的业务应用是指该业务应用的业务流程相对

独立，不依赖于其他业务应用就能完成主要业务流程，同时与其他业务应用只有少量数据交换，相对独享某些信息处理设备。对于承担“单一”业务应用的系统，可以直接确定为定级对象；对于承担多个业务应用的系统，应通过判定各类业务应用是否“相对独立”，将整个电力信息系统划分为“相对独立”的多个部分，每个部分作为一个定级对象。应避免将业务应用中的功能模块认为是一个业务应用。对于多个业务系统其流程存在大量交叉，业务数据存在大量交换或者业务应用共享大量设备等情况，也应避免将业务系统强行“相对独立”，可以将两个或多个业务系统涉及的组件作为一个集合，确定为一个定级对象。原则上电网企业不同管理机构（本部、网、省、地、县）管理控制下相对独立的电力信息系统应分开作为不同的定级对象。

e） 识别电力信息系统安全保护定级对象安全区域

应遵从安全分区原则，尽量避免将不同安全区的系统作为同一个定级对象，运行单位应根据电力行业管理方式、业务特点、部署方式等要素在各安全区内自主定级。

f） 识别需整合的定级备案系统

具有相同安全防护属性的同一安全区域业务子系统，可以整合为一个整体定级对象。

g） 定级对象详细描述

参见 GB/T 25058。

活动输出为电力信息系统定级对象详细描述文件。

5.3 安全保护等级确定

5.3.1 定级、审核和批准

参见 GB/T 25058。原则上管理信息系统业务信息安全（S）等级不低于系统服务安全（A）等级；电力监控系统服务安全（A）等级不低于业务信息安全（S）等级；云计算和大数据平台定级可在信息系统定级结果上递增一级。

5.3.2 形成定级报告

参见 GB/T 25058。

5.4 定级结果备案

参见 GB/T 25058。

6 测评与评估

6.1 测评与评估的流程

本活动的目标是通过电力信息系统安全等级测评机构以及安全评估机构对已经完成等级保护建设的电力信息系统进行等级测评和安全评估，确保等级保护对象的安全保护措施符合相应等级的安全要求以及国家和行业对电力信息系统安全防护的相关要求。管理信息系统安全评估参见 GB/T 20984，电力监控系统安全评估参见电力监控系统安全防护评估规范；电力监控系统信息安全等级测评应与电力监控系统安全防护第三方评估工作同步进行，一次测评分别出具等级保护测评报告及电力监控系统安全防护评估报告。

等级测评包括测评机构选择、测评准备、方案编制、现场测评、分析及报告编制等主要过程。安全评估包括评估工作形式选择、评估机构选择、评估准备、现场评估、分析与报告编制等主要过程。等级测评与安全评估阶段的流程见图 3 和图 4。

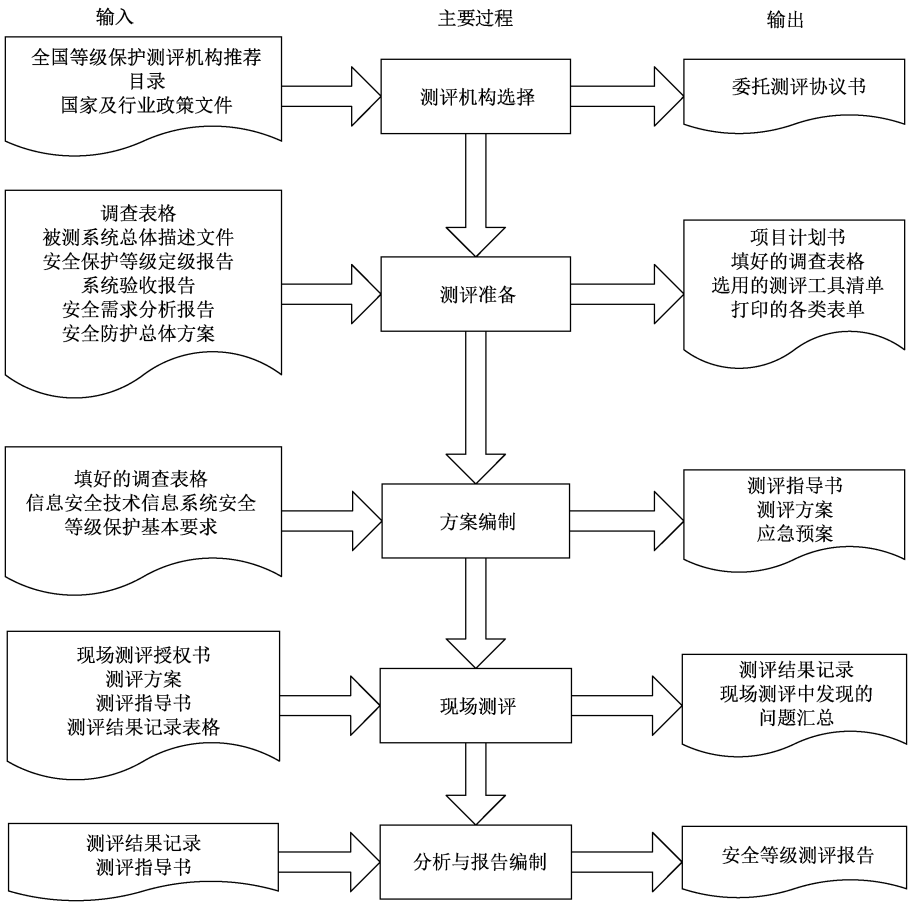

图 3　电力信息系统测评流程

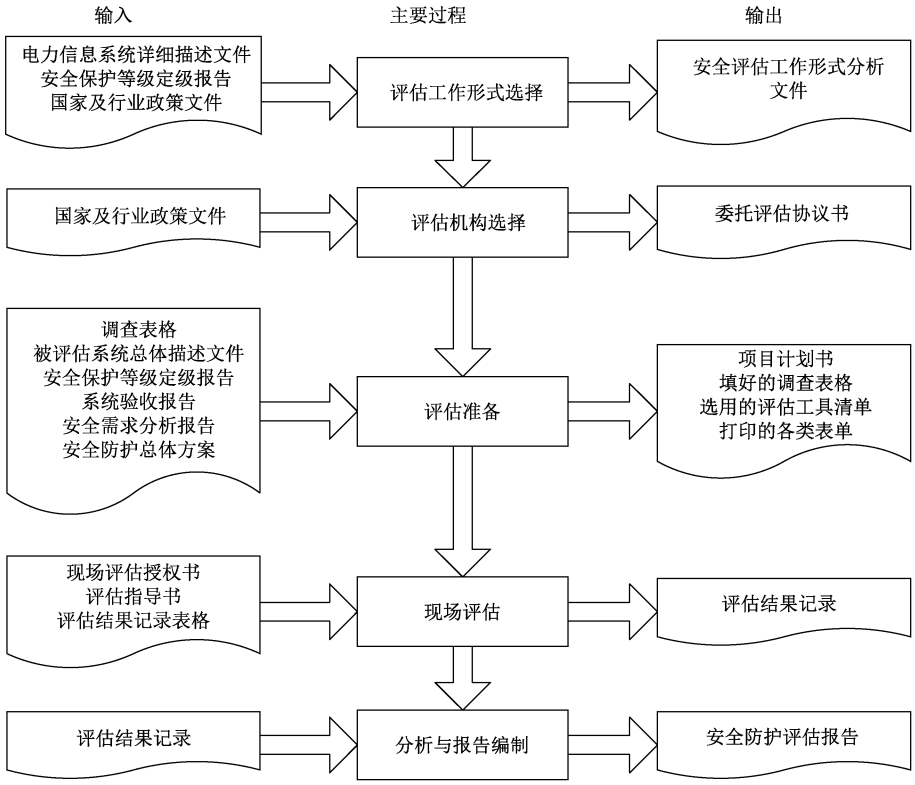

图 4　电力监控系统安全防护评估流程

6.2 等级测评

6.2.1 测评机构选择

本活动的目标是选择合适的电力信息系统安全等级测评机构。

参与角色为电力信息系统运行单位，等级测评机构。

活动输入为全国等级保护测评机构推荐目录，国家及行业政策文件，测评机构相关资质证书。

具体活动描述如下：

a） 行业要求分析

由于电力信息系统的特殊性，在选择测评机构时应优先考虑具备行业等级测评经验，符合行业政策要求的测评机构。

b） 服务能力分析

从影响电力信息系统、业务安全性等关键要素层面分析测评机构服务能力，根据国家及行业相关要求，选择最佳测评机构，这些要素可能包括：测评机构的基本情况、企业资质和人员资质、信誉、技术力量和行业经验、内部控制和管理能力、持续经营状况、服务水平及人员配备情况等。

c） 安全风险分析

在选择测评机构时，需要识别其测评可能产生的风险，防止测评次生风险，测评次生风险包括但不限于以下几点：

——测评机构可能的泄密行为。

——测评机构服务能力及行业系统特性了解不够导致误操作等。

——物理和系统访问越权、信息资料丢失等。

——测评机构企业资质不全、人员资质管理不善，口碑、业绩不良等引发测评质量问题。

——测评机构以往服务项目案例未覆盖本类系统测评导致的经验不足等。

d） 服务内容互斥分析

在选择服务商时，需要识别测评机构提供的服务与之前或后续提供的服务之间没有互斥性。承担等级测评服务的机构不应同时提供安全建设、安全整改等服务。

活动输出为含保密条款的委托测评协议书或合同（保密条款也可以保密协议形式单独签署）。

6.2.2 测评准备

本活动的目标是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

参与角色为电力信息系统运行单位，电力信息系统安全等级测评机构。

活动输入为调查表格，被测系统总体描述文件，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全防护总体方案。

本活动主要包括以下子活动内容：

a） 项目启动

测评机构组建等级测评项目组，测评人员签署保密承诺书，获取运行单位及被测系统的基本情况，从基本资料、人员、计划安排等方面为整个等级测评项目的实施做基本准备。

b） 信息收集和分析

测评机构通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，为编写测评方案和开展现场测评工作奠定基础。

c） 工具和表单准备

测评项目组成员在进行现场测评之前，应熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。

活动输出为项目计划书，填好的调查表格，选用的测评工具清单，打印的各类表单。

6.2.3 方案编制

本活动的目标是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

参与角色为电力信息系统运行单位，电力信息系统安全等级测评机构。

活动输入为填好的调查表格，GB/T 22239 中相应等级的基本要求，行业相关规范文件。

本活动主要包括以下子活动内容：

a） 测评指标确定

根据已经了解到的被测系统定级结果，确定本次测评的测评指标。

b） 测评对象确定

根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，按照相关国家标准根据测评指标选取测评对象。

c） 测评工具接入点确定

根据已经确定的测评对象分析确定需要进行工具测试的测评对象，选择测试路径，确定测试工具的接入点。

d） 测评内容确定

把各层面上的测评指标结合到具体测评对象上，并说明具体的测评方法，确定现场测评的具体实施内容，即单项测评内容。

e） 测评指导书开发

根据单项测评内容确定测评活动，包括测评指标、测评方法、测评实施和结果判定等四部分，编制测评指导书。

f） 测评方案编制

根据委托测评协议书和填好的调研表格，提取项目来源、测评委托单位整体信息化建设情况及被测系统与单位其他系统之间的连接情况等，将测评活动所依据的标准进行罗列，估算现场测评工作量，编制工作安排情况和具体测评计划，汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿。

g） 应急预案编制

根据测评范围界定的电力信息系统，测评机构在运行单位的配合下编制测评风险应急预案。

活动输出为测评指导书，测评方案，应急预案。

6.2.4 现场测评

本活动的目标是按照测评方案的总体要求，严格执行测评指导书，分步实施所有测评项目，包括单项测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

参与角色为电力信息系统运行单位，电力信息系统安全等级测评机构。

活动输入为现场测评授权书，测评方案，测评指导书，测评结果记录表格。

本活动主要包括以下子活动内容：

a） 现场测评准备

运行单位签署现场测评授权书，召开测评现场首次会。测评机构介绍测评工作，交流测评信息，进一步明确测评计划和方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排等。测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评条件等，确认被测系统已备份过系统及数据。

b） 现场测评和结果记录

测评人员与被测系统有关人员(个人/群体)进行交流、讨论等活动,获取相关证据,了解有关信息,形成完整过程文档记录并妥善保管。

检查 GB/T 22239 中规定的应具有的制度、策略、操作规程等文档是否齐备。检查是否有完整的制度执行情况记录,如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等。

根据测评结果记录表格内容,利用上机验证的方式检查应用系统、主机系统、数据库系统以及网络设备的配置是否正确,是否与文档、相关设备和部件保持一致,对文档审核的内容进行核实(包括日志审计等)。

根据测评指导书,利用技术工具对系统进行测试,包括基于网络探测和基于主机审计的漏洞扫描、渗透性测试、性能测试、入侵检测和协议分析等,备份测试结果。

根据被测系统的实际情况,测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况,测评其是否达到了相应等级的安全要求。

在对电力信息系统进行测评时,运行单位能够提供备用设备搭建临时模拟测试环境的,优先考虑模拟真实系统的结构、配置、数据、业务流程,以保证测评最大程度接近真实情况。

对位于生产控制大区内的电力监控系统在无法搭建模拟测试环境的情况下,原则上不采用工具进行测评,而是采用人工进行测评。

现场测评人员应遵守电力信息系统的相关操作章程,以防止敏感信息泄漏和确保及时处理意外事件。

对直接涉及电力生产的电力信息系统的测评工作,应避开电力生产敏感时期。

测评实施中,为防止发生影响电力信息系统运行的安全事件,应根据测评对象的不同采取相应的风险控制手段。

c) 结果确认和资料归还

运行单位召开测评现场结束会,测评双方对测评过程中发现的问题进行现场确认。测评机构归还测评过程中借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认。

活动输出为测评结果记录,现场测评中发现的问题汇总。

6.2.5 分析与报告编制

本活动的目标是根据现场测评结果和 GB/T 22239 的有关要求,通过单项测评结果判定、整体测评和风险分析等方法,找出整个系统的安全保护现状与相应等级的保护要求之间的差距,并分析这些差距导致被测系统面临的风险,从而给出等级测评结论,形成测评报告文本。

参与角色为电力信息系统运行单位,电力信息系统安全等级测评机构。

活动输入为测评结果记录,测评指导书。

本活动主要包括以下子活动内容:

a) 单项测评结果判定

针对测评指标中的单个测评项,结合具体测评对象,客观、准确地分析测评证据,形成初步单项测评结果。

b) 整体测评

针对单项测评结果的不符合项,采取逐条判定的方法,从安全控制点、安全控制点间和层面间出发考虑,给出整体测评的具体结果。

c) 风险分析

测评人员依据等级保护的相关规范和标准,采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

d) 等级测评结论形成

测评人员在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。经测评，电力信息系统存在违反结构优先原则的，测评机构在测评报告中的等级测评结论应为不符合。

e） 测评报告编制

测评人员整理前面几项任务的输出/产品，编制测评报告相应部分。测评报告应包括但不局限于以下内容：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单项测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

活动输出为安全等级测评报告。

6.3 电力监控系统安全防护评估

6.3.1 评估形式选择

本活动的目标是根据电力监控系统运行单位管辖范围内电力监控系统级别选择合适的安全防护评估形式。

参与角色为电力监控系统运行单位，电力信息系统安全供应商，电力调度机构，电力监控系统安全防护评估机构，主管部门。

活动输入为电力监控系统详细描述文件，安全保护等级定级报告，国家及行业政策文件。

具体活动描述如下：

电力监控系统运行单位、电力调度机构、主管部门根据国家及行业政策文件、管辖范围内电力监控系统所在的生命周期、安全保护级别等要素分析评估周期和评估形式。

电力监控系统运行单位对本单位安全保护等级为第三级或第四级的电力监控系统定期组织开展自评估工作，评估周期原则上不超过一年；对安全保护等级为第二级的电力监控系统定期组织开展自评估工作，评估周期原则上不超过两年。

电力监控系统运行单位在安全保护等级为第三级或第四级的电力监控系统投运前或发生重大变更时，委托电力监控系统评估机构进行上线安全评估；安全保护等级为第二级的电力监控系统可自行组织开展上线安全评估。

电力信息系统安全供应商在安全保护等级为第三级或第四级的电力监控系统设计、开发完成后，委托电力监控系统评估机构进行型式安全评估；对安全保护等级为第二级的电力监控系统自行组织开展型式安全评估。

电力调度机构在定期收集、汇总调管范围内各运行单位自评估结果的基础上，自行组织或委托评估机构开展调管范围内电力监控系统的自评估工作，省级以上调度机构的自评估周期最长不超过三年，地级及以下调度机构自评估周期最长不超过两年。

主管部门根据实际情况对各运行单位的电力监控系统或调度机构调管范围内的电力监控系统组织开展检查评估。

活动输出为安全评估形式分析文件。

6.3.2 评估准备

本活动的目标是掌握被评估系统的详细情况，准备评估工具，为现场评估做好准备。

参与角色为电力监控系统运行单位、评估机构。

活动输入为调查表格，被评估系统总体描述文件，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全防护总体方案。

本活动主要包括以下子活动内容：

a） 成立评估工作组

组建安全评估项目组，获取运行单位及被评估系统的基本情况，从基本资料、人员、计划安排等方面为整个安全评估项目的实施做基本准备。

b） 确定评估范围

召开评估组工作会议确定评估范围，评估范围包括代表被评估系统的所有关键资产。评估范围确定后，运行单位管理人员根据选定的内容进行资料的准备工作。

c） 评估工具准备

评估项目组根据收到的评估资料，进行评估工具的准备。

d） 准备应急措施

评估项目组在运行单位的配合下制定应急预案，确保在发生紧急事件时不对电力监控系统正常运行产生大的影响。

活动输出为项目计划书，填好的调查表格，选用的评估工具清单，打印的各类表单。

6.3.3 现场评估

本活动的目标是对被评估系统的资产、威胁、脆弱性和已有安全措施进行识别和赋值。

参与角色为电力监控系统运行单位、评估机构。

活动输入为现场评估授权书，评估指导书，评估结果记录表格。

本活动主要包括以下子活动内容：

a） 资产评估

评估人员依据电力监控系统安全防护总体方案和国家等级保护相关要求对电力监控系统的评估对象进行资产识别和赋值，确定其在电力生产过程中的重要性。

b） 威胁评估

根据电力监控系统的运行环境确定面临的威胁来源，通过技术手段、统计数据和经验判断来确定威胁的严重程度和发生的频率，对威胁进行识别和赋值。

c） 脆弱性评估

识别资产本身的漏洞，分析发现管理方面的缺陷，综合评价该资产或资产组（系统）的脆弱性，对脆弱性进行识别和赋值。

d） 安全防护措施确认

对已有安全防护措施进行识别，确定防护措施是否发挥了应有的作用。

活动输出为评估结果记录。

6.3.4 分析与报告编制

本活动的目标是对安全事件发生的可能性和造成的损失进行风险分析，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题，从而给出安全评估结论，形成评估报告文本。

参与角色为电力监控系统运行单位、评估机构。

活动输入为评估结果记录。

本活动主要包括以下子活动内容：

a） 数据整理

将资产调查、威胁分析、脆弱性分析中采集到的数据按照风险计算的要求，进行分析和整理。

b） 风险计算

采用矩阵法或相乘法，根据资产价值、资产面临的威胁和存在的脆弱性赋值等情况对资产面临的风险进行分析和计算。

c） 风险决策

在风险排序的基础上，分析各种风险要素、评估系统的实际情况和计算消除或降低风险所需的成

本，并在此基础上决定对风险采取接受、消除或转移等处理方式。

d） 安全建议

根据风险决策提出的风险处理计划，结合资产面临的威胁和存在的脆弱性，经过统计归纳形成安全解决方案建议。

e） 评估报告编制

评估人员整理前面几项任务的输出/产品，编制评估报告相应部分。评估报告应包括但不局限于以下内容：概述、评估对象描述、资产识别与赋值、威胁分析、脆弱性分析、安全措施有效性分析、风险计算和分析、安全风险整改建议等。

活动输出为电力监控系统安全防护评估报告。

7 安全整改

7.1 安全整改的流程

电力信息系统安全整改是等级保护的重要环节。本活动主要针对等级测评、安全评估、安全自查、监督检查工作中发现的安全问题进行有计划的建设整改，确保电力信息系统安全保护能力满足相应等级的安全要求。

安全整改阶段的工作流程见图 5。

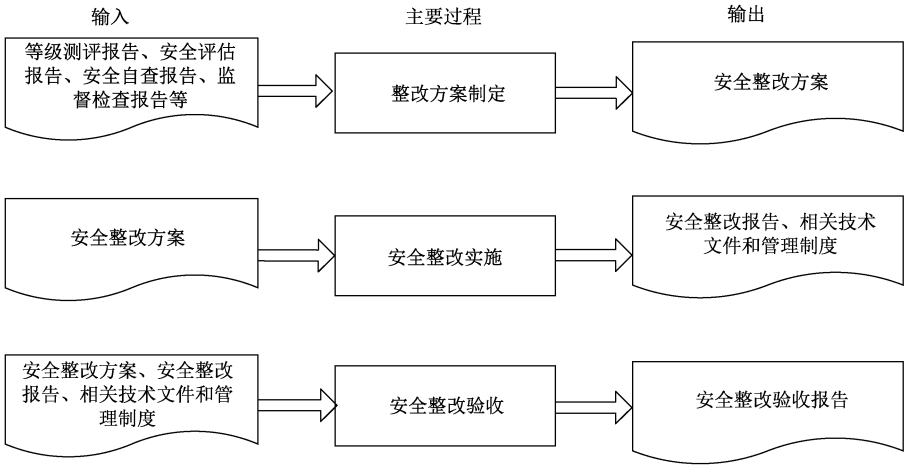

图 5 电力信息系统安全整改流程

7.2 整改方案制定

本活动的主要目标是依据等级测评、安全评估、安全自查、监督检查的结果，开展安全整改方案设计，为后续的安全整改实施提供基础。

参与角色为电力信息系统运行单位、电力信息系统安全服务机构、电力信息系统安全供应商、电力信息系统安全产品供应商、电力信息系统设计单位、电力信息系统开发单位。

活动输入为等级测评报告、安全评估报告、安全自查报告、监督检查报告。

本活动主要包括以下子活动内容：

a） 安全整改立项

根据等级测评、安全评估、安全自查以及监督检查的结果确定安全整改策略：如果涉及安全保护等级的变化，则应进入安全保护等级保护实施的一个新的循环过程；如果安全保护等级不变，但是调整内容较多、涉及范围较大，则应对安全整改项目进行立项，重新开始安全实施/实现过程，见 GB/T 25058；

如果调整内容较小，则可以直接进行安全整改。

根据安全问题类型确定整改优先级：首先整改因不满足“安全分区、网络专用、横向隔离、纵向认证”原则导致的安全问题，强化边界防护；配置等较易整改的技术问题，尽快整改；整改周期长、难度大的安全问题，制定长期整改计划，按照整体设计、逐步实施的原则进行。对于行业普遍存在的、整改难度较大的系列安全问题，可在行业主管部门的指导下，联合行业内其他单位共同选出典型单位，进行试点实施，形成经典案例，确认无误后实施整改。管理类安全问题应尽快整改，完善管理制度体系。

明确整改配合单位：技术类安全问题，应联合设计单位、开发单位、供应商以及其他运行单位共同进行，并在上级主管部门的指导下进行。系统运营单位在针对评估或测评所发现的问题进行安全整改时，从开发单位、设备供应商获得技术支持有难度的，应上报集团公司、上级主管部门或行业主管部门统一规划部署，以合适的方式督促系统和设备原厂提供商支持、配合系统单位的安全加固整改，有效落实网络安全整改措施。

b） 制定安全整改方案

确定安全整改的工作方法、工作内容、人员分工、时间计划等，制定安全整改方案。小范围内的安全改进，如安全加固、配置加强、系统补丁、管理措施落实等也需制定安全整改方案控制整改次生风险，大范围的改进，如系统安全重新设计等需纳入技术改造项目。整改时间计划应综合考虑业务运行周期及特点，所有整改工作应以不影响生产运行为前提条件。应对整改措施的有效性和可行性进行评估。

c） 安全整改方案审核

依据行业相关要求，电力调度机构、发电厂、变电站等运行单位的电力信息系统安全整改方案经本企业的上级专业管理部门和信息安全管理部门以及相应电力调度机构审核通过后再实施。

活动输出为安全整改方案。

7.3 安全整改实施

本活动的目标是保证按照安全整改方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。

参与角色为电力信息系统运行单位、电力信息系统安全服务机构、电力信息系统供应商、网络安全产品供应商、电力信息系统设计单位、电力信息系统开发单位。

活动输入为安全整改方案。

本活动主要包括以下子活动内容：

a） 安全整改实施控制

在安全整改方案实施过程中，应对实施质量、风险服务、变更、进度和文档等方面的工作进行监督控制和科学管理，保证系统整改处于等级保护制度所要求的框架内，具体内容见 GB/T 25058。另外，整改实施过程中应做好保密措施。

b） 技术措施整改实施

主要工作内容是依据整改方案落实技术整改，如安全加固、配置加强、系统补丁等。技术措施整改实施首先在测试环境中测试和验证通过后，再部署到实际生产环境中，并尽量选择大小修期间、停机状态进行，避免对生产过程造成影响。

c） 配套技术文件和管理制度的修订

安全整改技术实施完成之后，应调整和修订各类相关的技术文件和管理制度，保证原有电力信息系统安全防护体系的完整性和一致性。

d） 管理措施整改实施

管理类安全问题的整改可与技术类安全问题的整改同步进行，确保尽快完善管理制度体系，并实现技术措施和管理措施相互促进、相互弥补。

活动输出为安全整改报告、相关技术文件和管理制度。

7.4 安全整改验收

本活动的目标是检验安全整改实施是否严格按照安全整改方案进行，是否实现了预计的功能、性能和安全性，是否确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作，保证电力信息系统的正常运行。

参与角色为主管部门，电力信息系统运行单位、安全服务机构、安全等级测评机构以及其他相关单位。

活动输入为安全整改方案、安全整改报告、相关技术文件和管理制度。

具体活动描述如下：

安全整改验收应先由等级测评机构出具测评、评估报告，作为验收技术依据，再邀请主管部门以及其他相关单位参与。根据验收结果，出具安全整改验收报告。

活动输出为安全整改验收报告。

8 退运

8.1 电力信息系统退运阶段的流程

电力信息系统退运阶段是等级保护实施过程中的最后环节。在电力信息系统生命周期中，有些系统并不是真正意义上的退运，而是改进技术或转变业务到新的电力信息系统，对于这些电力信息系统在退运处理过程中应确保信息转移、设备迁移和介质销毁等方面的安全。

本标准在电力信息系统退运阶段关注信息转移、暂存和清除，设备迁移或退运，存储介质的清除或销毁等活动。

电力信息系统退运阶段的工作流程见图 6。

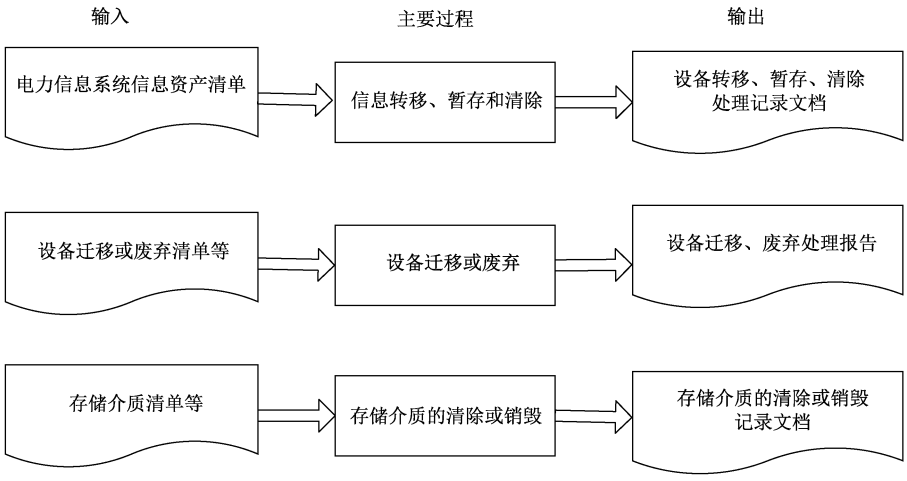

图 6 电力信息系统退运工作流程

8.2 信息转移、暂存和清除

本活动的目标是在电力信息系统退运处理过程中，对于可能会在另外的电力信息系统中使用的信息采取适当的方法将其安全地转移或暂存到可以恢复的介质中，确保将来可以继续使用，同时采用安全的方法清除要退运的电力信息系统中的信息。

参与角色为电力信息系统运行单位。

活动输入为电力信息系统信息资产清单。

本活动主要包括以下子活动内容：

a） 识别要转移、暂存和清除的信息资产

根据要退运的电力信息系统的信息资产清单，识别重要信息资产、所处的位置以及当前状态等，列出需转移、暂存和清除的信息资产的清单。

b） 信息资产转移、暂存和清除

根据信息资产的重要程度制定信息资产的转移、暂存、清除的方法和过程。如果是涉密信息，应该按照国家相关部门的规定进行转移、暂存和清除。

c） 处理过程记录

记录信息转移、暂存和清除的过程，包括参与的人员，转移、暂存和清除的方式以及目前信息所处的位置等。

活动输出为信息转移、暂存、清除处理记录文档。

8.3 设备迁移或退运

本活动的目标是确保电力信息系统退运后，迁移或退运的设备内不包括敏感信息，对设备的处理方式应符合国家和行业有关的要求。

参与角色为电力信息系统运行单位。

活动输入为设备迁移或退运清单等。

本活动主要包括以下子活动内容：

a） 软硬件设备识别

根据要退运的电力信息系统的设备清单，识别要被迁移或退运的硬件设备、所处的位置以及当前状态等，列出需迁移、退运的设备的清单。

b） 制定硬件设备处理方案

根据规定和实际情况制定设备处理方案，包括重用设备、退运设备、敏感信息的清除方法等。

c） 处理方案审批

包括重用设备、退运设备、敏感信息的清除方法等的设备处理方案应该经过主管领导审查和批准。

d） 设备处理和记录

根据设备处理方案对设备进行处理，如果是涉密信息的设备，其处理过程应符合国家相关部门的规定；记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出为设备迁移、退运处理报告。

8.4 存储介质的清除或销毁

本活动的目标是通过采用合理的方式对计算机介质（包括磁带、磁盘、打印结果和文档）进行信息清除或销毁处理，防止介质内的敏感信息泄露。

参与角色为电力信息系统运行单位。

活动输入为存储介质清单等。

本活动主要包括以下子活动内容：

a） 识别要清除或销毁的介质

根据要退运的电力信息系统的存储介质清单，识别载有重要信息的存储介质、所处的位置以及当前状态等，列出需清除或销毁的存储介质清单。

b） 确定存储介质处理方法和流程

根据存储介质所承载信息的敏感程度确定对存储介质的处理方式和处理流程。存储介质的处理包括数据清除和存储介质销毁等。对于存储涉密信息的介质应按照国家及行业有关规定进行处理。

c） 处理方案审批

包括存储介质的处理方式和处理流程等的处理方案应该经过审查和批准。

d） 存储介质处理和记录

根据存储介质处理方案对存储介质进行处理，记录处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出为存储介质的清除或销毁记录文档。

参 考 文 献

[1] GB 17859 计算机信息系统安全保护等级划分准则

[2] GB/Z 20986 信息安全事件分类分级指南

[3] GB/T 30976.1 工业控制系统信息安全 第1部分:评估规范

[4] GB/T 30976.2 工业控制系统信息安全 第2部分:验收规范

[5] 全国人民代表大会常务委员会.中华人民共和国网络安全法.2016年11月7日.

[6] 国务院.中华人民共和国计算机信息系统安全保护条例.2011年1月8日 国务院147号令.

[7] 公安部等四部委.信息安全等级保护管理办法.2007年6月22日 公通字[2007]43号.

[8] 国家电力监管委员会.电力行业信息系统等级保护定级工作指导意见.2007年11月16日 电监信息[2007]44号.

[9] 国家发展改革委.电力监控系统安全防护规定.2014年8月1日 国家发改委令2014年第14号.

[10] 国家能源局.电力行业网络与信息安全管理办法.2014年7月2日 国能安全[2014]317号.

[11] 国家能源局.电力行业信息安全等级保护管理办法.2014年9月22日 国能安全[2014]318号.