电力行业等级保护基本要求

目 课程内容目录

中国南方电网
CHINA SOUTHERN POWER GRID

中国南方电网有限责任公司

安全等级保护管理作业规范

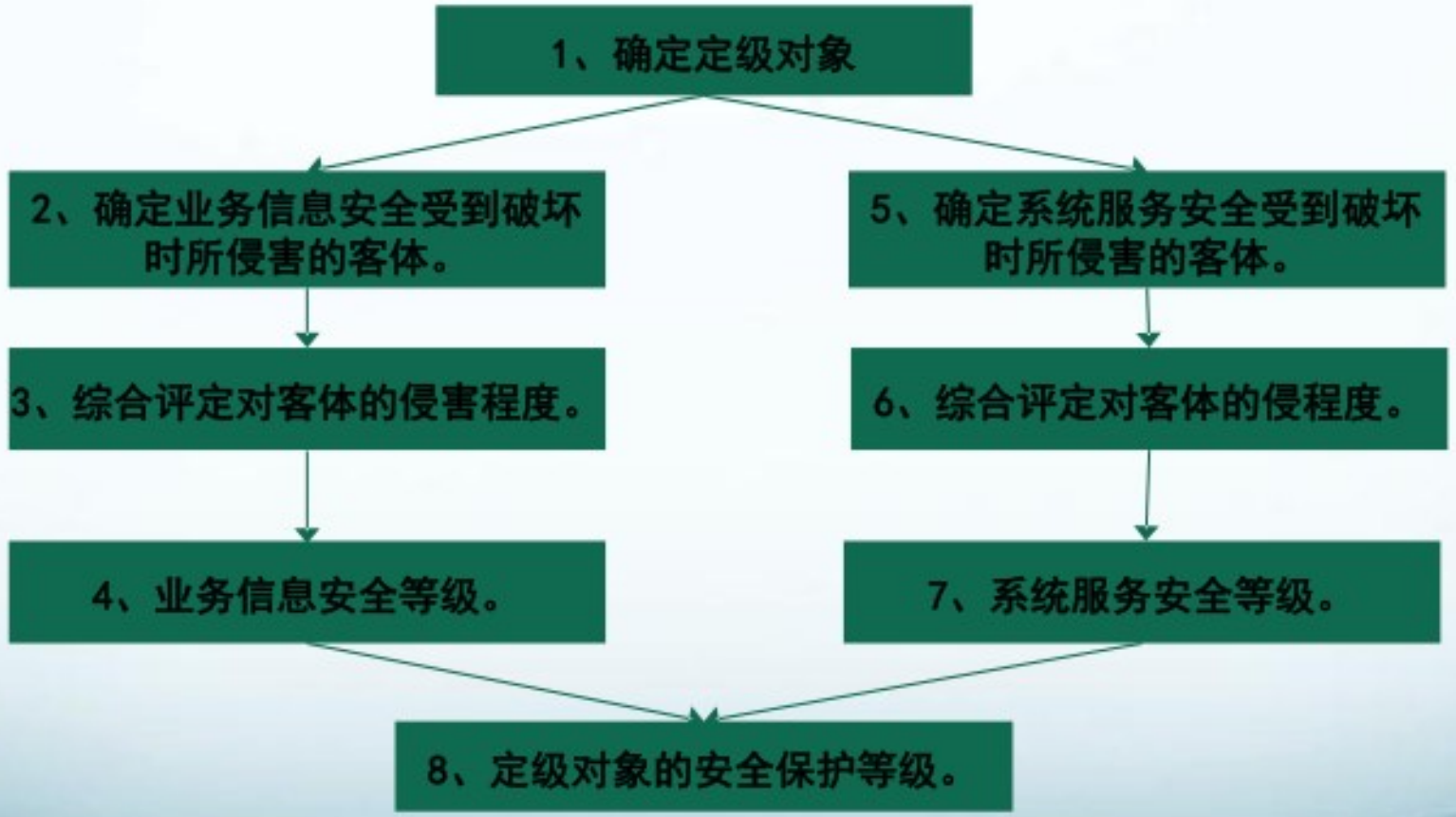
1　南网等级保护定级、备案相关规范

1.1 定级流程

1.2 定级方法

1.3 定级备案作业规范

定级流程


1、确定定级对象
2、确定业务信息安全受到破坏时所侵害的客体。
3、综合评定对客体的侵害程度。
4、业务信息安全等级。
5、确定系统服务安全受到破坏时所侵害的客体。
6、综合评定对客体的侵程度。
7、系统服务安全等级。
8、定级对象的安全保护等级。

业务信息安全保护等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

系统服务安全保护等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级

南方电网管理信息系统安全保护的定级对象及等级建议

一、南方电网管理信息系统安全保护的定级对象

企业级应用系统类

企业级应用系统类包括但不限于资产管理系统、财务管理系统、人力资源管理系统、营销管理系统、协同办公系统、综合管理系统。

南方电网管理信息系统安全保护的定级对象及等级建议

一、南方电网管理信息系统安全保护的定级对象

企业分析决策应用类

企业分析决策应用类系统包括但不限于决策支持系统、知识管理系统等。

专业系统类

专业系统类包括但不限于对外网站、邮件系统、电网规划系统、综合计划与统计节能管理系统、电子商务系统、应急指挥中心系统、网络招聘系统、网络培训和评价系统、数字档案馆系统、企业架构管理系统、ITM信息化管理系统等。

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

1. 资产管理系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
投资计划管理子系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级
项目管理子系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级
物资管理子系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级
安全生产管理子系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级
固定资产管理子系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

2. 财务管理类系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
财务管理系统	公司总部	第二级	第三级	第三级
	分子公司	第二级	第三级	第三级
	分子公司下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

3. 人力资源管理系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
人力资源管理系统	公司总部	第二级	第二级	第二级
	分子公司及其下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

4. 营销管理系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
营销管理系统	公司总部	第三级	第三级	第三级
	分子公司及其下属单位	第三级	第三级	第三级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

5. 协同办公系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
协同办公系统	公司总部	第二级	第三级	第三级
	分子公司及其下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

6. 综合管理系统的安全保护等级

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
综合管理系统	公司总部	第二级	第二级	第二级
	分子公司及下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

企业分析决策应用类系统的安全保护等级表

名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
知识管理系统	公司总部	第一级	第一级	第一级
	分子公司及下属单位	第一级	第一级	第一级
决策支持系统	公司总部	第二级	第二级	第二级
	分子公司及下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

专业系统类的安全保护等级表

序号	名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
1	对外网站	公司总部	第二级	第三级	第三级
		分子公司及下属单位	第一级	第二级	第二级
2	PKI/CA数字证书管理系统/4A系统	公司总部	第三级	第三级	第三级
		分子公司及下属单位	第二级	第三级	第三级
3	邮件系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级
4	电网规划系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

专业系统类的安全保护等级表

序号	名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
5	综合计划与统计节能管理系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级
6	电子商务系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第一级	第一级	第一级
7	电网运行管理系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级
8	网络招聘系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第一级	第一级	第一级

二、南方电网管理信息系统安全保护等级建议

企业级应用系统类 | 企业分析决策应用类 | 专业系统类

专业系统类的安全保护等级表

序号	名称	运营使用单位	系统服务安全保护等级	业务信息安全保护等级	信息系统安全保护等级
9	网络培训和评价系统	公司总部	第一级	第一级	第一级
		分子公司及下属单位	第一级	第一级	第一级
10	数字档案馆系统	公司总部	第一级	第一级	第一级
		分子公司及下属单位	第一级	第一级	第一级
11	企业架构管理系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级
12	ITM信息化管理系统	公司总部	第二级	第二级	第二级
		分子公司及下属单位	第二级	第二级	第二级

安全等级保护管理作业规范

2　电力行业等级保护基本要求

2.1 总体要求

2.2 技术要求

2.3 管理要求

总体要求（新增）

总体技术要求

a） 管理信息大区网络与生产控制大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置；

b） 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间有信息通信交换时防护强度应强于逻辑隔离；

c） 具有层次网络结构的单位可统一提供互联网出口；

d） 二级系统统一成域，三级系统可独立成域；

e） 三级系统域可由独立子网承载，每个域有唯一网络出口，可在网络出口处部署能使系统整体达到三级等级保护要求的安全设备。

总体管理要求

a） 如果本单位管理信息大区仅有一级信息系统时，通用管理要求等同采用一级基本要求；

b） 如果本单位管理信息大区含有二级及以下等级信息系统时，通用管理要求等同采用二级基本要求；

c） 如果本单位管理信息大区含有三级及以下等级信息系统时，通用管理要求等同采用三级基本要求。

技术要求

1	物理安全	b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁,如果不可避免，应采取有效防水措施。（落实） c） 机房各出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；（增强） c) 应对机房划分区域进行管理，区域和区域之间应用物理方式隔断，在重要区域前设置交付或安装等过渡区域；（增强） a） 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房,与主机房相关的给排水管道必须有可靠的防渗漏措施；（落实） c) 设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方式；（增强）
2	网络安全	
3	主机安全	
4	应用安全	
5	数据安全及备份恢复	

技术要求

1	物理安全
2	网络安全
3	主机安全
4	应用安全
5	数据安全及备份恢复

a) 管理信息大区网络与生产控制大区网络应物理隔离;两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置;（新增）

b) 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间的防护强度应强于逻辑隔离；（新增）

c) 电力（集团）公司应逐步统一互联网出口；（新增）

d) 单个系统可单独划分安全域，系统可由独立子网承载，每个域的网络出口应唯一；（新增）

h) 应绘制与当前运行情况相符的网络拓扑结构图，主要包括设备名称、型号、IP地址等信息，并提供网段划分、路由、安全策略等配置信息；（增强）

技术要求

1	物理安全
2	网络安全
3	主机安全
4	应用安全
5	数据安全及备份恢复

l)在进行内外网隔离的情况下，应将应用系统部署在内网，如有外网交互功能的应用系统，可将前端部署在外网，数据库部分可部署在内网。（新增）

j)在业务高峰时段，现有宽带不能满足要求时，应按照对业务服务的重要次序来制定带宽分配优先级，优先保障重要业务服务的带宽；（落实）

k)采用冗余技术设计网络拓扑结构，提供主要网络设备、通信线路的硬件冗余，避免关键节点存在单点故障；（增强）

g) 在互联网出口和核心网络接口处应限制网络最大流量数及网络连接数；（细化）

d) 应限制具有拨号、VPN等访问权限的用户数量；（增强）

c） 应能够根据记录数据进行分析，并生成审计报表，网络设备不支持的应采用第三方工具生成审计报表；（落实）

技术要求

1	物理安全	b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；（落实） c) 应逐步采用网络准入、终端控制、身份认证、可信计算等技术手段，维护网络边界完整性；(新增） c) 网络设备标识应唯一，同一网络设备的用户标识应唯一，禁止多人共用一个账号；（增强） d） 身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换；应修改默认用户和口令，不得使用缺省口令；口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令不得等同；禁止明文存储口令；（增强） h） 应实现设备特权用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作；（细化）
2	网络安全	
3	主机安全	
4	应用安全	
5	数据安全及备份恢复	

技术要求

1	物理安全
2	网络安全
3	主机安全
4	应用安全
5	数据安全及备份恢复

i）应关闭不需要的网络端口，关闭不需要的网络服务。如需使用SNMP服务，应采用安全性增强版本；并应设定复杂的Community控制字段，禁止使用Public、Private等默认字段。（新增）

技术要求

1	物理安全	**c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施应限制同一用户连续失败登录次数；（增强）** **f）应对重要信息资源设置敏感标记，主机不支持敏感标记的，应在系统级生成敏感标记，使系统整体支持强制访问控制机制；（落实）** a）审计范围应覆盖服务器和重要客户端上的每个操作系统用户和数据库用户，系统不支持该要求的，应采用第三方安全审计产品实现审计要求：（落实） b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统重要安全相关事件，至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；（细化）
2	网络安全	
3	**主机安全**	
4	应用安全	
5	数据安全及备份恢复	

技术要求

1	物理安全	**e）应能够通过操作系统自身功能或第三方工具根据记录数据进行分析，并生成审计报表；（细化）** b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用 户前得到完全清除。 c)应能够对重要程序的完整性进行检测，并具有完整性恢复的能力。（增强) a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本 和琴意代码库；（细化） c) 应根据需要限制单个用户对系统资源的最大或最小使用限度：（细化）
2	网络安全	
3	主机安全	
4	应用安全	
5	数据安全及备份恢复	

技术要求

1	物理安全	e）应对重要信息资源设置敏感标记，应用不支持敏感标记的，应在系统级生成敏感标记，使系统整体支持强制访问控制机制：（落实）
2	网络安全	a) 应提供覆盖每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（细化）
3	主机安全	b) 应保证无法删除、修改或覆盖审计记录，维护审计活动的完整性；（增强）
4	应用安全	b) 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令不得等同；禁止应用软件明文存储口令：（增强）
5	数据安全及备份恢复	

技术要求

1	物理安全	a）应提供数据本地备份与恢复功能，对重要信息进行备份，数据备份至少每天一次，已有数据备份可完全恢复至备份执行时状态，备份介质场外存放；（增强）
2	网络安全	
3	主机安全	
4	应用安全	
5	数据安全及备份恢复	

管理要求

1	安全管理制度	无
2	安全管理机构	
3	人员安全管理	
4	系统建设管理	
5	系统运维管理	

管理要求

1	安全管理制度
2	安全管理机构
3	人员安全管理
4	系统建设管理
5	系统运维管理

c）应成立指导和管理信息安全工作的委员会或领导小组，电力企业主要负责人是本单位信息安全的第一责任人，对本单位的网络与信息安全负全面责任；（增强）

b）每个电力企业应配备专职安全管理员，不可兼任；（落实）

a)应保障信息系统安全建设、运维、检查、等级保护测评及其它信息安全资金。（新增）

d）应针对关键活动建立审批流程，并由批准人签字确认，存档备查。（落实）

b）应加强与电力监管机构、公安机关及相关单位和部门的合作与沟通；（增强）

管理要求

1	安全管理制度
2	安全管理机构
3	**人员安全管理**
4	系统建设管理
5	系统运维管理

c）应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议。（细化）

a） 应严格规范人员离岗过程，依次收回离岗员工的所有访问权限；（细化）

c）只有在收回其访问权限并各种证件、设备之后方可办理调离手续，关键岗位人员离须承诺调离后的保密义务后方可离开。（细化）

b)应对安全管理员、系统管理员、网络管理员、信息安全主管或专责等关键岗位的人员进行全面、严格的安全审查和技能考核；（细化）

c）应按照行业要求，对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进p的培训应至少每年举办一次：（增强）

管理要求

1	安全管理制度
2	安全管理机构
3	人员安全管理
4	系统建设管理
5	系统运维管理

c）信息系统定级结果应通过电力监管机构的审批；（细化）

d）对于跨电力（集团）公司联网运行的信息系统，由行业信息安全监管部门统一确定安全保护等级。对于属同一电力（集团）公司，但省联网运行的信息系统，由（集团）公司责任部门统一确定安全保护等级。（细化）

d）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，重大项目应报行业信息安全监管部门进行信息安全专项审查批准；（落实）

e）电力系统重要设备及专用信息安全产品应通过国家及行业监管部门推荐的专业机构的安全性检测后方可购使用。（新增）

a）应委托国家或电力行业认可的测评机构对系统进行安全性测试验收;(细化）

管理要求

1	安全管理制度	b）应对负责系统运行维护的技术人员每年进行相应的技能培训，对安全教育和培训的情况和结果进行记录并归档保存；（细化） b）电力（集团）公司应统一汇总所属单位定级结果，报电力监管机构审批备案：（细化） c）应将经电力监管机构审批的系统等级及其他要求的备案材料报相应公安机关备案。（细化） c）系统运营使用单位应选择具有行业监管部门推荐的具有电力行业信息安全等级测评资格的机构承担本单位信息系统的测评工作；（增强） **b）应与选定的安全服务商签订安全协议，明确安全责任；（细化）** c）应与服务商签订安全服务合同，明确技术支持和服务承诺。（增强）
2	安全管理机构	
3	人员安全管理	
4	**系统建设管理**	
5	系统运维管理	

管理要求

1	安全管理制度
2	安全管理机构
3	人员安全管理
5	系统建设管理
4	系统运维管理

b）应建立移动存储介质安全管理制度，落实移动存储介质管控措施；（新增）

a）应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；