内部资料
注意保存

附件 7:

电力监控系统安全防护评估规范

1 范围

本规范规定了电力监控系统安全防护评估的总体要求、工作形式、评估内容、评估方法、实施流程和评价标准等，适用于各电力企业电力监控系统的安全防护评估工作。

2 引用标准与规范

下列文件中的条款通过在本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，鼓励根据规范达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本规范。

- 《电力监控系统安全防护规定》（国家发展改革委 2014 年第 14 号令）
- 《电力监控系统安全防护总体方案》
- 《省级以上调度中心监控系统安全防护方案》
- 《地县级调度中心监控系统安全防护方案》
- 《发电厂监控系统安全防护方案》
- 《变电站监控系统安全防护方案》
- 《配电监控系统安全防护方案》
- 《GB/T 22239-2008 信息安全技术 信息系统安全等级

保护基本要求》

- 《信息安全等级保护管理办法》（公通字[2007]43号）
- 《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》
- 《GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南》
- 《GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南》
- 《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》
- 《GB/T 28448-2012 信息系统安全等级保护测评要求》
- 《GB/T 28449-2012 信息系统安全等级保护测评过程指南》
- 《关于开展电力行业信息系统安全等级保护定级工作的通知》（电监信息[2007]34号）
- 《电力行业信息系统等级保护定级工作指导意见》（电监信息[2007]44号）
- 《电力行业信息系统安全等级保护基本要求》（电监信息[2012]62号）

3 术语和定义

电力监控系统

电力监控系统，是指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，以及做为基础支撑的通信及数据网络等。

组织

由作用不同的个体为实施共同的业务目标而建立机构。一个单位是一个组织，某个业务部门也可以是一个组织。

资产

指在电力监控系统建设和运行过程中积累起来的具有价值的信息或资源，是安全策略的保护对象。

资产价值

指资产对电力监控系统的重要程度，以及对电力监控系统完成相关电力生产工作的重要程度。资产价值是资产的属性，也是进行资产识别的主要内容。

威胁

电力监控系统资产可能受到的来自内部和外部的安全侵害。

脆弱性

电力监控系统资产及其防护措施在安全方面的不足，通常也称为漏洞。脆弱性可能被威胁利用，并对电力监控系统资产造成损害。

安全事件

人为或自然的威胁利用电力监控系统及其管理体系中存在的脆弱性导致的不安全状况。

信息安全风险

安全事件发生的可能性及其潜在的影响。

残余风险

采取了安全防护措施，提高了防护能力后，仍然可能存在的风险。

安全措施

保护资产，抵御威胁，减少脆弱性，降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

型式安全评估

电力监控系统设计、开发完成后，系统供应商自行组织或委托评估机构对系统进行的安全评估。

上线安全评估

电力监控系统投运前及发生重大变更时，运行单位自行组织或委托评估机构对系统进行的安全评估。

自评估

运行单位对本单位电力监控系统组织实施的安全评估，以及调度机构在调度管辖范围内（以下简称“调管范围内”）各运行单位自评估结果基础上，对调管范围内电力监控系统组织实施的安全评估。

检查评估

由国家能源局及其派出机构（以下简称“能源监管机构”）组织或委托安全评估机构对电力行业监控系统进行的

具有强制性的安全评估。

4 安全评估管理

4.1. 总体要求

电力监控系统安全防护评估工作应当常态化、定期进行。电力监控系统的规划、设计阶段要进行安全评审，建设改造、运行维护和废弃阶段均要进行安全评估，确保系统全生命周期安全性。

4.2. 评估工作形式

电力监控系统安全防护评估有四种工作形式：自评估、检查评估、上线安全评估和型式安全评估。各种形式评估均应当遵循《电力监控系统安全防护总体方案》及国家等级保护相关要求等规范性文件，在不影响电力监控系统生产业务的基础上实施。

部署了安全保护等级为4级和3级业务系统的安全区，应当由运行单位结合等级保护工作委托评估机构定期开展安全评估工作，评估周期最长不超过三年。在此期间，运行单位应当定期组织开展自评估工作，以确保不因系统调整而造成系统安全性降低的情况发生，评估周期原则上不超过一年。自评估以脆弱性评估为主，评估的项目、要点见附录B。

仅部署安全保护等级为2级业务系统的安全区，应当由运行单位定期组织开展自评估工作，评估周期最长不超过两

年，也可以根据情况委托评估机构开展自评估工作。

调度机构应当在定期收集、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。

能源监管机构可以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。

安全保护等级为 4 级和 3 级的电力监控系统在设计、开发完成后，应当委托评估机构进行型式安全评估，安全保护等级为 2 级的应当自行组织开展型式安全评估。各单位安全保护等级为“4 级和 3 级”的电力监控系统投运前或发生重大变更时，应当委托评估机构进行上线安全评估，安全保护等级为 2 级应当自行组织开展上线安全评估。

检查评估、型式安全评估、上线安全评估主要包括资产识别、威胁分析、脆弱性分析、风险分析和安全建议等，其中脆弱性分析项目、要点包括但不限于附录 B，评估方法应符合国家、行业标准规范，评估报告模板见附录 E。评估工作角色和职责

4.3. 评估工作角色和职责

电力监控系统安全防护评估工作涉及能源监管机构、上

级主管部门、运行单位、调度机构、供应商、评估机构等角色。各角色在评估中承担不同的职责，如表 4-1 所示。其中受委托开展电力监控系统安全防护评估工作的评估机构，其评估人员应当经过能源监管机构培训合格，同时还应当具备国家等级保护测评资质。

表 4-1　电力监控系统安全防护和等级保护评估角色职责

安全评估相关角色	职责
能源监管机构	对评估机构的资质进行审核 发起检查评估工作 监管电力企业的评估开展情况 检查或督导评估整改方案落实情况
上级主管部门	发起下属单位的自评估工作 监督下属单位安全评估实施过程 检查下属单位安全评估整改方案落实情况
运行单位	发起本单位的自评估工作 参加评估方案等文档的评审工作 按照评估规范实施自评估 配合检查评估实施工作 根据安全评估结果落实整改方案 系统投运前及发生重大变更时实施上线安全评估，运行单位总体负责相关工作，可委托评估机构进行评估
调度机构	发起调管范围内的自评估工作 收集、汇总调度管辖范围内各运行单位的自评估结果 参加评估方案等文档的评审工作 按照评估规范组织实施调管范围内电力监控系统的自评估 配合开展调管范围内的检查评估工作 根据安全评估结果督促、落实整改方案
系统供应商	系统设计、开发完成后实施型式安全评估 配合完成系统上线的安全评估 在运行维护阶段支持、配合安全评估工作 配合执行安全评估整改工作
评估机构	编制安全评估实施方案 自行组织评审评估实施方案 实施安全评估 出具安全评估报告，提出整改建议 自行组织评审评估结果

4.4. 保密管理

应当加强对评估资料和评估结果的管理，按照国家及被评估单位的相关要求做好保密工作，确保评估机构和人员可靠、稳定和可控，确保评估过程中产生、接触的所有记录、数据与评估结果安全、保密、可控。评估工作采取以下控制措施：

（1）签署保密协议

项目实施前，评估机构应当与被评估单位签订保密协议，明确双方的保密责任。

（2）最小接触原则

项目实施工作中，项目组必须接触、使用被评估单位敏感信息时，评估机构应当遵循最小接触原则。仅授权必不可少的人员可接触到相关信息。

（3）职业道德

评估机构应当保证评估项目参与人员具有良好的职业道德，相关人员无违法犯罪记录，未发生过违反职业道德的情况。

（4）人员保密管理

应当确保参与评估项目的人员均与评估机构签署保密协议。项目人员对工作过程中接触、产生的数据以及评估结果应当严格保密，未经授权不得泄露给任何第三方。项目人员不得利用项目过程中接触、产生的数据进行任何侵害被评

估单位网络信息系统的行为。

（5）设备保密管理

评估机构项目组应当根据被评估单位的需要，使用专用的办公设备进行工作，禁止将被评估单位的任何设备带出允许的办公场地，项目完成以后，立即归还。

（6）文档保密管理

评估项目组应当采取加密的方式进行项目组内、项目组与被评估单位间的数据交换。依据被评估单位的要求，评估机构应当对项目有关文档、数据、资料设置保密期，在保密期结束后，应当使用可信的方式彻底销毁有关数据与文件资料。评估机构应当保证不在任何第三方场合与第三方文档中发布或引用被测系统信息。

4.5. 风险控制

安全评估工作本身也会引入安全风险，必须加强安全评估实施过程中的风险控制。电力监控系统安全防护评估工作实施前，应当根据确定的评估范围，对评估过程中可能引入的风险进行分析，并制定应对措施。评估实施过程的风险控制手段主要包括：

（1）操作的申请和监护

在实施过程中，评估操作必须遵守电力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。

（2）操作时间控制

对直接涉及电力生产的电力监控系统的评估工作，尽可能避开电力生产敏感时期。

（3）制定应急预案

根据评估范围界定的电力监控系统情况，在被评估单位的配合下，由评估机构在评估实施前制定应急预案。

（4）运行系统模拟环境

在对电力关键业务系统评估时，电力企业能够提供备用设备搭建临时模拟测试环境的，应优先考虑模拟真实系统的结构、配置、数据、业务流程，以保证评估的真实性和运行系统的安全、稳定。

（5）关键业务系统风险控制

对位于生产控制大区内的电力监控系统在无法搭建模拟环境的情况下，原则上不采用评估工具进行评估，采用人工评估的方式进行。

（6）其他

评估实施中，为防止发生影响系统运行的安全事件，应当根据评估对象的不同采取相应的风险控制手段。

5 安全评估基本内容

本章主要描述自评估、检查评估、上线安全评估和型式安全评估共有的基本内容和流程。评估的内容、方法和流程见附录C。

5.1. 评估原则

针对电力监控系统安全防护的特点，设置如下必须满足的基本要求：

（1）安全分区。发电企业、电网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（又称安全区Ⅰ）和非控制区（又称安全区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，但是应避免形成不同安全区的纵向交叉联接。

（2）网络专用。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数据网的安全隔离。

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。

（3）横向隔离。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。

安全接入区与生产控制大区中的联接处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。

（4）纵向认证。在生产控制大区与广域网的纵向联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。

上述任何一项要求未满足即为不合格。

在上述基本要求都满足情况下，参照附录B开展电力监控系统安全防护评估。

5.2. 风险分析

风险分析主要包括数据整理、风险计算和风险决策三个步骤。

数据整理是将资产调查、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，进行分析和整理的过程。

风险计算是在完成资产评估、威胁评估和脆弱性评估后，根据资产赋值、资产面临的威胁和存在的脆弱性赋值情况对资产面临的风险进行分析和计算。

计算风险值公式为：

$$风险值 = R(A, T, V)$$

其中：R表示安全风险计算函数；A表示资产；T表示威胁；V表示脆弱性。评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。

风险决策是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、计算消除或降低风险所需要的成本，决定对风险采取接受、消除或转移等处理方式的过程。风险决策是提出安全建议的基础，科学、合理的风险决策是提高安全建议质量、防止过度防护和防护不足的保障。

6 系统生命周期各阶段的安全评估

电力监控系统生命周期包含五个基本阶段：规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。安全评估工作应当贯穿于电力监控系统整个生命周期，其中规划阶段、设计阶段应当结合规划审查及设计审查进行安全评审，实施阶段、运行维护阶段和废弃阶段需结合本阶段的实际情况开展安全评估。

6.1. 规划阶段

规划阶段安全评审工作应当根据电力监控系统的业务使命、功能，确定系统建设应达到的安全目标。

本阶段评审主要是对根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行威胁分析；重点分析系统应该达到的安全目标。

规划阶段的评审结果应当包含在电力监控系统整体规划中。

6.2. 设计阶段

设计阶段的安全评审需要根据规划阶段所明确的系统

安全目标，对系统设计方案的安全功能设计进行判断，以确保设计方案满足系统安全目标，并作为采购过程风险控制的依据。

设计阶段的评审结果最终应当体现在系统设计方案中。

6.3. 实施阶段

实施阶段安全评估的目的是根据系统安全需求和运行环境对系统开发实施过程进行安全风险识别，并对系统建成后的安全功能进行验证。根据设计阶段分析的威胁和建立的安全控制措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施以及评估开发过程中对上述要求的保障，实施阶段应当对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定上述安全措施能否抵御现有威胁、脆弱性的影响，并对源代码进行安全测评，提高代码安全性。在系统投运前，运行单位应当自行组织或委托评估机构对系统进行上线安全评估。实施阶段安全评估主要对系统的开发与技术或产品获取、系统交付实施两个过程进行评估。

6.4. 运行维护阶段

运行维护阶段安全评估的目的是掌握和控制电力监控系统运行过程中的安全风险，包括在线运行电力监控系统资产、威胁、脆弱性等各方面评估，是一种较为全面的安全评估。

运行维护阶段的安全评估应当常态化开展。电力监控系统业务流程、系统状况发生重大变更时，也需要及时进行安全评估。重大变更包括：

（1）增加新的应用或应用发生较大变更；

（2）网络结构和连接状况发生较大变更，例如，系统升级改造、新机房投入使用或局域网、广域网结构发生较大变化时；

（3）技术平台大规模的更新；

（4）系统扩容或改造；

（5）发生重大安全事件后，或存在发生重大安全事件的隐患；

（6）系统运行维护管理机构或人员发生较大规模调整。

6.5. 废弃阶段

电力监控系统的废弃阶段可以分为部分废弃和全部废弃，废弃阶段安全评估包括：

（1）系统软、硬件等资产及残留信息的废弃处置；

（2）废弃部分与其他系统（或部分）的物理或逻辑连接情况；

（3）在系统变更时发生废弃，还应当对变更的部分进行评估。

本阶段应当重点分析废弃资产对组织的影响，对由于系统废弃可能带来的新的威胁进行分析。

附录A 电力监控系统安全防护定级表

类别	定级对象	系统级别	
		省级以上	地级及以下
电力监控系统	能量管理系统（具有SCADA、AGC、AVC等控制功能）	4	3
	变电站自动化系统(含开关站、换流站、集控站）	220千伏及以上变电站为3级，以下为2级	
	火电厂监控（含燃气电厂）系统DCS（含辅机控制系统）	单机容量300MW及以上为3级，以下为2级	
	水电厂监控系统	总装机1000MW及以上为3级，以下为2级	
	水电厂梯级调度监控系统	3	
	核电站监控系统DCS（含辅机控制系统）	3	
	风电场监控系统	风电场总装机容量200MW及以上为3级，以下为2级	
	光伏电站监控系统	光伏电站总装机容量200MW及以上为3级，以下为2级	
	电能量计量系统	3	2
	广域相量测量系统（WAMS）	3	无
	电网动态预警系统	3	无
	调度交易计划系统	3	无
	水调自动化系统	2	
	调度管理系统	2	
	雷电监测系统	2	
	电力调度数据网络	3	2
	通信设备网管系统	3	2
	通信资源管理系统	3	2
	综合数据通信网络	2	
	故障录波信息管理系统	3	
	配电监控系统	3	
	负荷控制管理系统	3	
	新一代电网调度控制系统的实时监控与预警功能模块	4	3
	新一代电网调度控制系统的调度计划功能模块	3	2
	新一代电网调度控制系统的安全校核功能模块	3	2
	新一代电网调度控制系统的调度管理功能模块	2	

注：

1. 备用调度中心相关系统与主调系统同级别。

附录B 电力监控系统安全防护脆弱性评估表（主要指标）

B1 技术要求

B1.1 物理安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况[1]	备注
				3级、2级	4级		
1	物理位置的选择(G)	机房和办公场地的物理位置选择在防震、防风和防雨的建筑内	✓	✓	✓		
		机房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	—	✓	✓		
2	物理访问控制(G)	对机房划分区域进行管理，区域和区域之间设置物理隔离设施，在重要区域前设置交付或安装等过渡区域，将设备区域与维护操作区域分离	—	✓	✓		
		机房门禁系统具备人员授权分级管理、日志管理（含人员进出、时间、身份类型等信息）功能	✓	✓	✓		
		四级系统部署两道电子门禁系统	—	—	✓		
		进出机房建立相应的申请和审批流程	✓	✓	✓		
3	防盗窃和防破坏(G)	机房部署视频监控系统，覆盖所有关键区域（厂站仅要求在厂站内部署视频监控系统，不要求覆盖所有关键区域）	✓	✓	✓		
		重要设备机柜上锁处理	✓	✓	✓		
4	防雷击(G)	机房建筑设置避雷装置、防雷保安器和交流电源地线（厂站不要求部署防雷保安器）	✓	✓	✓		
5	防火(G)	机房在自动灭火、耐火材料、物理区域隔离等方面进行防护（厂站不要求自动灭火）	✓	✓	✓		
6	防水和防潮	机房设置措施防止外部雨水渗漏、水蒸汽结露和地下积水	✓	✓	✓		

[1] 按“符合”、“部分符合”、“不符合”填写。

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况[1]	备注
				3级、2级	4级		
	(G)	机房部署防水报警装置，具备漏水检测和报警能力（厂站不要求漏水检测和报警能力）	✓	✓	✓		
		水管安装，不得穿过机房屋顶和活动地板下	✓	✓	✓		
7	防静电(G)	机房具备设备接地、防静电地板（厂站不要求防静电地板）	✓	✓	✓		
		配备静电消除器（防静电手环）措施	—	—	✓		
8	温湿度控制(G)	机房设置温湿度自动调节设施（厂站具备温湿度检测调节设施）	✓	✓	✓		
9	电力供应(A)	机房设置专用冗余UPS电源，UPS电源为双路供电	✓	✓	✓		
10	电磁防护(S)	采用接地方式防止外界电磁干扰和设备寄生耦合干扰	✓	✓	✓		
		动力电缆和信号电缆必须隔离铺设	✓	✓	✓		
		重要设备（SCADA服务器、前置机、通信机）放置于电磁屏蔽机柜内	—	—	✓		
合计			75	85	100		

B1.2 网络安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	结构安全(G)	业务准确分区，调度数据网网络承载安全区I、安全区II的业务	✓	✓	✓		必须实现项
		根据电力监控系统安全等级保护定级结果在生产控制大区划分不同的网络安全域，并进行区域之间的安全访问控制	✓	✓	✓		必须实现项
		横向部署专用隔离装置，仅允许非TCP直连方式的数据通信	✓	✓	✓		必须实现项

序号	评估项目	评估要点	厂站端系统(3级、2级)	调度端系统		符合情况	备注
				3级、2级	4级		
		调度数据网纵向部署专用加密认证装置，仅允许专用的通信服务，严格设置访问控制策略	✓	✓	✓		必须实现项
		局域网核心交换设备、广域网核心路由设备应采取设备冗余或准备了备用设备，同时路由链路也应该施行冗余方式，核心网络不存在明显的单点故障隐患	✓	✓	✓		
		绘制与当前运行情况相符的网络拓扑结构图	✓	✓	✓		
2	访问控制(G)	根据业务系统划分不同 VLAN，VLAN 间配置严格的访问控制策略	✓	✓	✓		
		生产控制大区内禁止 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务	✓	✓	✓		
		远程拨号访问采用专用拨号认证服务器	✓	✓	✓		
3	安全审计(G)	具有内网安全监视功能，对设备日志进行集中采集和统计分析	-	✓	✓		
4	边界完整性检查(S)	对电力调度数据网络的网络设备进行安全配置，防止非授权访问，禁止 III 区系统与办公系统对生产控制大区的非授权访问	✓	✓	✓		
5	入侵防范(G)	生产控制大区和管理信息大区分别部署入侵检测/防御系统，采用离线方式及时升级系统特征库	-	✓	✓		
6	网络设备防护(G)	口令长度不低于 8 位，为数字、字母组合，且定期更换	✓	✓	✓		
		网络设备远程管理采用加密方式，并对管理地址进行限制	✓	✓	✓		
		网络设备具有登录失败处理功能，可采取结束会话、限制非法登录次数、登录超时自动退出等措施	✓	✓	✓		
合计			90	100	100		

B1.3　主机安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	身份鉴别(S)	口令长度不低于8位，为数字、字母组合，且定期更换	✓	✓	✓		
		设置合理的口令策略（包括设置口令长度、复杂性、口令存留期等）	✓	✓	✓		
		设置用户安全策略(包括设置帐户锁定登录失败锁定次数、锁定时间、超时自动锁定时间等）	✓	✓	✓		
		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	✓	✓	✓		
2	安全标记(S)	采用安全操作系统和安全数据库，对所有主体和客体设置敏感标记	-	-	✓		
3	访问控制(S)	依据所有主体和客体设置的敏感标记控制主体对客体的访问	-	-	✓		
		配置操作系统、数据库系统重要文件的访问权限，只授予必要的用户必需的访问权限	✓	✓	✓		
		及时删除多余的、过期的帐户，避免共享帐户的存在	✓	✓	✓		
		修改默认帐号/口令	✓	✓	✓		
		删除默认共享目录	✓	✓	✓		
4	可信路径(S)	采用安全操作系统，在系统对用户进行身份鉴别和访问时，系统与用户之间能够建立一条安全的信息传输路径	-	-	✓		
5	安全审计(G)	审计范围覆盖到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	✓	✓	✓		
		开启主机日志审计功能或采用内网安全监视系统，对主机安全类日志和运行类日志进行集中采集和统计分析	✓	✓	✓		
		对审计数据分配合理的存储空间和存储时间，避免审计记录受到未预期的删除、修改或覆盖	✓	✓	✓		
6	剩余信息保护	确保系统内的用户鉴别信息、文件、目录和数据库记录等资源所在的	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
	(S)	存储空间，被释放或重新分配给其他用户前得到完全清除					
7	入侵防范(G)	生产控制大区和信息管理大区分别部署入侵检测/防御系统，采用离线方式及时升级系统特征库	✓	✓	✓		
		在系统上线或发生重大变更时测试并安装系统安全补丁，在不影响业务系统正常运行情况下，对发现的系统漏洞在确保安全的情况下进行修补，停止或禁用与承载业务无关的服务或端口	✓	✓	✓		
8	恶意代码防范(G)	生产控制大区和信息管理大区分别部署独立的防恶意代码管理系统，采用离线方式及时升级经测试验证过的系统特征库	✓	✓	✓		
9	资源控制(A)	通过设定终端接入方式、网络地址范围等条件限制终端登录	✓	✓	✓		
		具备对服务器CPU、硬盘、内存、网络等资源使用情况进行监视和报警的功能	✓	✓	✓		
10	安全免疫(G)	以可信计算技术为核心，构建可信计算基础设施，为高安全等级生产控制系统建立主动防御机制（可选）	✓	✓	✓		
合计			85	85	100		

B1.4 应用安全

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	身份鉴别(S)	口令长度不低于8位，为数字、字母组合，设置口令过期时间、口令不能重复的次数、锁定口令错误输入次数、锁定时间，且定期更换	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
		在应用软件的各组成部分中都不能存储明文的口令数据	✓	✓	✓		
		启用登录失败处理功能，采取结束会话、限制非法登录次数和自动退出等措施	✓	✓	✓		
2	安全标记(S)	对所有主体和客体设置敏感标记（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全调用）	-	-	✓		
3	访问控制(S)	依据所有主体和客体设置的敏感标记控制主体对客体的访问（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全访问控制）	-	-	✓		
		提供系统管理员用户一个产生和修改用户授权的管理模块，新建帐户时，帐户初始权限应为空，不应内置匿名账户，也不允许匿名用户的登录	✓	✓	✓		
		及时删除多余的、过期的帐户，修改默认帐号/口令，避免共享帐户的存在	✓	✓	✓		
4	可信路径(S)	在系统对用户进行身份鉴别和访问时，系统与用户之间能够建立一条安全的信息传输路径（智能电网调度控制系统的数字证书和安全标签技术实现了远程服务的安全访问控制）	-	-	✓		
5	安全审计(G)	启用应用系统日志审计功能，或采用安全审计设备记录业务系统发生的历史安全事件，对安全事件发生的规律和频率进行统计和分析	✓	✓	✓		
		安全审计记录只有授权的管理人员可访问，且仅为只读权限，无修改和删除权限	✓	✓	✓		
		安全审计信息需进行备份	✓	✓	✓		
6	剩余信息保护(S)	确保系统内的用户鉴别信息所在的存储空间，被释放或重新分配给其他用户前得到完全清除	✓	✓	✓		
7	通信完整性(S)	采用纵向加密认证装置，基于电力调度数字证书，通过加密认证、HTTPS 等技术措施，实现远程通信的完整性保护	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
8	通信保密性(S)	采用纵向加密认证装置，基于电力调度数字证书，通过加密认证、HTTPS等技术措施，实现远程通信的保密性保护	✓	✓	✓		
9	抗抵赖(G)	具有应用系统安全审计功能，对用户登录、操作等行为进行记录，实现发送、接收数据的抗抵赖	✓	✓	✓		
10	软件容错(A)	对用户输入的数据进行合法性检验，并执行强制的非法数据过滤功能，禁止提交可能产生危害的数据	✓	✓	✓		
		能够允许多用户同时对同一个系统资源进行不相冲突的访问操作，并且设定保护措施，防止相互可能造成的冲突，禁止多个客户端用户同时执行互斥的操作	✓	✓	✓		
		在故障发生时，应用系统能够继续提供一部分功能，确保对部分严重故障进行自动处理，采取可能使系统恢复正常状态的措施或保护现存数据的措施	✓	✓	✓		
11	资源控制(A)	当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方能够自动结束会话	✓	✓	✓		
		对系统的最大并发会话连接数和单个帐户的多重并发会话进行限制	✓	✓	✓		
合计			85	85	100		

B1.5 数据安全及备份恢复

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	数据完整性(S)	基于电力调度数字证书和安全标签技术，通过加密认证、HTTPS等安全技术措施，实现远程通信的完整性保护	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
2	数据保密性(S)	基于电力调度数字证书和安全标签技术，通过加密认证、HTTPS等安全技术措施，实现远程通信的保密性保护	✓	✓	✓		
3	备份和恢复(A)	实现主备调互备机制	-	✓	✓		
		采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障	✓	✓	✓		
		提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性	✓	✓	✓		
		提供本地数据备份与恢复功能，备份介质场外存放	✓	✓	✓		
		定期对关键业务的数据与系统进行备份	✓	✓	✓		
合计			90	100	100		

B2 管理要求

B2.1 安全管理制度

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	管理制度(G)	制定电力监控系统安全防护的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等	✓	✓	✓		
		按照“谁主管谁负责，谁运营谁负责”的原则，建立电力监控系统安全管理制度	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
		针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序；按照审批程序执行审批过程，对重要活动建立逐级审批制度，记录审批过程并保存审批文档	✓	✓	✓		
		制定并严格执行操作票、工作票制度	✓	✓	✓		
4	沟通和合作(G)	加强各类管理人员之间、组织内部机构之间以及信息职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息问题	–	✓	✓		
		加强与兄弟单位、公安机关、专业机构、上级主管部门的合作与沟通	–	✓	✓		
5	审核和检查(G)	制定安全审核和安全检查制度规范；定期按照程序进行安全审核和安全检查活动	–	✓	✓		
合计			25	40	40		

B2.3 人员安全管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	人员录用(G)	相关人员签署保密协议	✓	✓	✓		
2	人员离岗(G)	及时收回离岗人员的相关证件，限制其系统访问权限，并通告相关单位	✓	✓	✓		
3	人员考核(G)	对各个岗位的人员进行安全技能及安全认知的考核，考核结果进行记录并保存，并纳入绩效考核	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统(3级、2级)	调度端系统		符合情况	备注
				3级、2级	4级		
		对要求管理人员或操作人员执行的日常管理操作建立操作规程:包括门禁、人员管理、访问控制、设备、恶意代码的防护、审计、数据及系统的备份、帐号、培训等管理制度	✓	✓	✓		
		将电力监控系统安全防护及其信息报送纳入日常安全生产管理体系	✓	✓	✓		
2	制定和发布(G)	安全管理制度具有统一的格式，并进行版本控制	✓	✓	✓		
		安全管理制度通过正式、有效的方式发布	✓	✓	✓		
		安全管理制度注明发布范围，并对收发文进行登记	✓	✓	✓		
3	评审和修订(G)	组织相关人员对管理制度进行审定	✓	✓	✓		
合计			40	40	40		

B2.2 安全管理机构

序号	评估项目	评估要点	厂站端系统(3级、2级)	调度端系统		符合情况	备注
				3级、2级	4级		
1	岗位设置(G)	明确本单位所辖电力监控系统的安全防护的领导责任人，设置监控系统安全防护岗位	✓	✓	✓		
2	人员配备(G)	指定专人负责本单位电力监控系统的安全防护，明确各业务系统专责人的安全管理责任	✓	✓	✓		
3	授权和审批(G)	根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
4	意识教育和培训(G)	对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训	✓	✓	✓		
		对教育和培训的情况和结果进行记录并归档保存	✓	✓	✓		
5	外部人员访问管理(G)	外部人员访问需提出书面申请或由主管人员批准后由专人全程陪同或监督，并登记备案	✓	✓	✓		
		对外部人员允许访问的区域、系统、设备、信息等内容进行书面的规定，并按照规定执行	✓	✓	✓		
		关键区域不允许外部人员访问	✓	✓	✓		
合计			40	40	40		

B2.4 系统建设管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	系统定级和备案(G)	明确现有系统安全保护等级，系统等级及相关材料报行业主管部门及公安机关备案	✓	✓	✓		
2	安全方案设计(G)	依据监控系统安全防护方案进行详细方案设计	✓	✓	✓		
3	产品采购和使用(G)	电力监控系统安全产品的采购和使用符合国家的有关规定	✓	✓	✓		
4	软件开发(G)	自行开发或外包开发的软件产品投运前应进行安全评估	✓	✓	✓		
5	工程实施和安全服务商选择	选择具备国家和行业主管部门要求的资质的施工单位和安全服务商，与选定的安全服务商签订与相关的协议，明确约定相关责任，	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
	(G)	并签署保密协议					
6	测试验收(G)	测试验收在已有工程验收和现场验收的基础上，增加第三方安全机构的参与（二级系统不要求第三方安全机构参与）；组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认	✓	✓	✓		
7	系统交付(G)	指定或授权专门的部门负责系统交付的管理工作，制定详细的系统交付清单，根据交付清单对所交接的设备、软件和文档等进行清点；对负责系统运行维护的技术人员进行相应的技能培训	✓	✓	✓		
8	等级评估(G)	按行业主管部门要求进行安全防护评估和等级保护测评，两项工作一起完成	✓	✓	✓		
合计			40	40	40		

B2.5 系统运维管理

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
1	环境管理(G)	建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境等方面的管理作出规定；指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理	-	✓	✓		
2	设备、介质和资产管理(G)	建立设备安全管理制度、介质安全管理制度和资产安全管理制度，对设备和介质的存放环境、使用、维护和销毁等方面作出规定；加强对移动存储设备、重要文档的安全管理；对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理	✓	✓	✓		

序号	评估项目	评估要点	厂站端系统（3级、2级）	调度端系统		符合情况	备注
				3级、2级	4级		
3	监控管理和安全管理中心(G)	建立安全审计管理制度，指定专人对安全审计工作进行管理	✓	✓	✓		
4	网络和系统安全管理(G)	建立网络、系统安全管理制度，指定专人对网络设施、主机系统进行管理；定期检查违反规定拨号上网或其他违反网络策略的行为；依据操作手册对系统进行维护，详细记录操作日志，严禁进行未经授权的操作；指定专人对网络和主机进行恶意代码检测并保存检测记录	✓	✓	✓		
5	密码管理(G)	建立密码使用管理制度	✓	✓	✓		
6	变更管理(G)	建立变更管理制度，实现流程化管理	✓	✓	✓		
7	备份与恢复管理(G)	建立备份与恢复管理相关的安全管理制度；建立控制数据备份和恢复过程的程序	✓	✓	✓		
8	安全事件处置和应急预案管理(G)	制定安全事件报告和处置管理制度；制定安全事件报告和响应处理程序；制定应急处理预案；定期对应急预案进行演练，定期审查应急预案和根据实际情况更新的内容	✓	✓	✓		
合计			35	40	40		

附录C 电力监控系统安全防护评估

C1 评估内容

电力监控系统安全防护评估的主要内容包括：资产评估、威胁评估、脆弱性评估、总体评价。

C1.1 资产评估

电力监控系统资产评估是指依据《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。各单位资产评估对象必须包括附录A电力监控系统安全防护定级表所列内容。

（1） 资产识别

资产识别是对电力监控系统设备、数据和人员等系统构成元素进行分类、标记的过程。在确定评估范围后，对其中资产价值进行分析。资产识别是为了明确资产用途、使命和作用，进而确定资产价值的准备工作。

资产的形式和内容各不相同，主要包括信息、软件、硬件、人员和系统五个表现形式。电力监控系统的各构成元素可按照表C-1的定义进行归并和分类：

表C-1 电力监控系统资产分类表

类别	解释
信息	以物理或电子的方式记录的数据，或者用于完成组织任务的知识产权。电力监控系统资产本质上是无形的，与系统资产紧密联系。系统存储、处理和传输驱动组织的关键信息。因此，当组织建立策略和计划以保护系统资产时，同时也保护了组织的关键信息，及其软硬件资产。
软件	软件应用程序和服务、如操作系统、数据库应用程序、网络软件、业务应用程序等，用于处理、存储和传输信息。
硬件	信息技术的物理设备，例如路由器、交换机、工作站、服务器等。通常强调单独考虑这些物理设备的替代价值。
人员	指组织中拥有独特技能、知识和经验的，他人难以替代的人。当人被标识为资产时，要确定是否还有更适于标识的相关资产。例如，标识他们使用、维护、管理的关键系统，或者他们为其他使用者提供的信息。
系统	处理和存储信息的信息系统，代表一组信息、软件和硬件资产。系统是一个整体，其任一组件都无法代表其整体，因此，对系统的评估需要完整的考虑系统的各个部分，并进行综合考虑。

（2） 资产赋值

资产赋值是根据电力监控系统安全保护等级对系统重要性进行赋值的过程。

各企业可根据《电力监控系统安全防护总体方案》和《电力行业信息系统安全等级保护定级工作指导意见》对资产进行赋值。

依据电力监控系统安全保护等级情况进行资产赋值，对应关系如表 C-2 所示。

表 C-2 资产赋值与安全等级对应表

资产赋值	标识	备注
5	很高	非常重要，生产控制大区内安全等级属于 4 级，具有控制功能的且其安全属性破坏后可能对组织造成非常严重的损失。
4	高	重要，生产控制大区内安全等级属于 3 级，不具有控制功能的且其安全属性破坏后可能对组织造成比较严重的损失。
3	中等	比较重要，生产控制大区内安全等级属于 2 级，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	不太重要，生产控制大区内安全等级属于 2 级，其安全属性破坏后可能对组织造成较低的损失。
1	很低	不重要，其安全属性破坏后对监控系统不会造成损害的。

C1.2 威胁评估

威胁是信息资产可能受到的来自内部和来自外部的安全侵害。

威胁评估是通过技术手段、统计数据和经验判断来确定电力监控系统面临威胁的过程。威胁评估主要包括两个方面，一是根据电力监控系统的运行环境确定面临的威胁来源，二是确定威胁的严重程度和发生的频率。

资产所处的环境不同，面临的威胁也不尽相同。应根据资产分类结果，对电力监控系统进行独立或整体的威胁评估。实际评估工作中，可按照安全分区和资产类别划分进行统一的威胁判断。

（1） 威胁识别

电力监控系统防护面临的主要威胁包括黑客、病毒、恶意代码、集团式攻击。此外，还应根据物理、网络和人员环境，对资产进行威胁判定。

（2） 威胁赋值

应根据威胁出现的频率判断得出威胁赋值。评估中，可以根据威胁发生的可能性进行分析、赋值。赋值越高，说明资产面临的威胁越大。

威胁赋值的过程是一个交流、观察与调查的过程，评估者应根据经验和（或）有关的统计数据进行判断，电力监控系统的运行维护及管理人员对系统自身运行

状况的了解程度是准确进行威胁赋值的关键。表 C-3 根据威胁发生的可能性，定义了年发生频率和威胁赋值。

表 C-3 威胁年发生频率和威胁赋值表

标识	赋值	定义	年发生频率
很高	5	威胁发生的可能性很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过。	年发生频率＞50
高	4	威胁发生的可能性较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过。	12＜年发生频率≤50
中	3	威胁发生的可能性中等（或＞ 1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。	2＜年发生频率≤12
低	2	威胁发生的可能性较小；或一般不太可能发生；或没有被证实发生过。	0.1＜年发生频率≤2
很低	1	威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生。	年发生频率≤0.1

表 C-4 列出了电力监控系统面临的常见威胁表现形式。

表 C-4 常见威胁表现形式

威胁分类	威胁名称	说明	年发生频率	威胁赋值
非人为威胁	系统软件故障	由于电力监控系统软件故障所产生的问题		
	应用软件故障	由于电力监控系统应用软件故障所产生的问题		
	软件缺陷	软件缺陷导致的安全问题		
	硬件故障	系统由于硬件设备老旧、损坏等造成的无法使用问题		
	通信故障	由于通信故障所产生的问题		
	火山爆发	由火山爆发引起的故障		
	台风	由于台风引起的系统故障		
	地震	由地震引起的系统故障		
	地质灾害	因泥石流等地质灾害引起的系统故障		
	雷电	由雷电引起的系统故障		
	火灾	由火灾引起的系统故障，包括在火灾发生后进行消防工作中引起的设备不可用问题		
	水灾	由水灾引起的系统故障，包括在水灾发生后进行消防工作中引起的设备不可用问题		
	雪崩	由于雪崩引起的问题		
	人员丧失	由于各种原因，如疾病、道路故障、		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
		暴动等原因导致人员无法正常工作引起的系统无法使用故障		
	电力故障	由于电力中断、用电波动、供电设备损坏导致电力监控系统停止运行等导致的系统故障		
	温度异常	由温度超标引起的故障		
	湿度异常	由湿度超标引起的故障		
	灰尘、尘土	由灰尘超标引起的故障		
	强磁场干扰	由磁暴以及其他强磁场源等干扰引起的故障		
人为威胁	离开时未锁门	由于离开时未锁门造成系统的安全问题		
	离开时屏保未锁定	由于离开时屏保未锁定造成的安全问题		
	恶意破坏系统设施	对系统设备、存储介质等资产进行恶意破坏		
	设备或软件被控制或破坏	恶意的控制或破坏设备，以取得机密信息		
	由于误操作传输错误的或不应传送的数据	个人失误导致的安全问题		
	不恰当的使用设备、系统与软件	不当的使用设备造成的安全威胁		
	不恰当的配置和操作	不恰当的管理系统、数据库、无意的数据操作，导致安全问题		
	拒绝服务攻击	攻击者以一种或者多种损害信息资源访问或使用能力的方式消耗信息系统资源		
	关键员工的离职	由于关键员工的离职造成系统的安全问题		
	在不恰当的人员中讨论敏感文档	由于在不恰当的人员中讨论敏感文档造成的安全问题		
	由于设备（如笔记本）丢失	导致泄密等安全问题		
	过时的规定	由于采用过时的规定所造成的安全问题		
	不遵守安全策略	可能导致各种可能的安全威胁		
	滥用	由于某授权的用户（有意或无意的）执行了授权他人要执行的举动、可能		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
		会发生检测不到的电力监控系统资产损害		
	远程维护端口被非授权的使用	恶意的使用远程维护端口，控制主机		
	数据传输或电话被监听	恶意截获传输数据		
	办公地点被非授权的控制	恶意监控办公地点、重要地带，获取重要信息		
	侦察	通过系统开放的服务进行信息收集，获取系统的相关信息，包括系统的软件、硬件和用户情况等信息		
	口令的暴力攻击	恶意的暴力尝试口令		
	各类软件后门或后门软件	软件预留的后门或其他专门的后门软件带来的信息泄露威胁		
	偷窃移动设备	带有机密信息的移动设备被窃取		
	恶意软件	计算机病毒、蠕虫带来的安全问题		
	伪装	标识的仿冒等信息安全问题		
	分析信息流	分析信息流带来的信息安全问题		
	非法阅读机密信息	非授权的从办公环境中取得可获得的机密信息或复制数据		
	社会工程学攻击	通过邮件、即时聊天软件、电话、交谈等欺骗或其他方式取得内部人员的信任，进而取得机密信息		
	未经授权将设备连接到网络	未经授权对外开放内部网络或设备		
	密码猜测攻击	对系统账号和口令进行猜测，导致系统中的敏感信息泄漏		
	伪造证书	恶意的伪造证书，进而取得机密信息		
	远程溢出攻击	攻击者利用系统调用中不合理的内存分配执行了非法的系统操作，从而获取了某些系统特权，进而威胁到系统完整性		
	权限提升	通过非法手段获得系统更高的权限，进而威胁到系统完整性		
	远程文件访问	对服务器上的数据进行远程文件访问，导致敏感数据泄漏		
	法律纠纷	由企业或信息系统行为导致的法律纠纷造成信誉和资产损失		
	不能或错误地响应和恢复	系统无法或错误地响应和恢复导致故障和损失		

威胁分类	威胁名称	说明	年发生频率	威胁赋值
	流量过载	由于网络中通信流量过大导致的网络无法访问		

根据威胁的发生可能性对威胁年发生频率进行赋值，并由此得出威胁赋值。

C1.3 脆弱性评估

脆弱性是信息资产及其防护措施在安全方面的不足，通常也称为漏洞。脆弱性可能被威胁利用，并对信息资产造成损害。

脆弱性评估包括脆弱性识别和赋值两个步骤，是发现与分析电力监控系统中存在的可被威胁利用的缺陷的过程。

（1） 脆弱性识别

脆弱性识别应围绕资产展开，即首先识别资产本身的漏洞，然后分析发现管理方面的缺陷，最后综合评价该资产或资产组（系统）的脆弱性。

脆弱性识别可从技术和管理两方面进行综合分析，技术方面的脆弱性识别主要采用工具审计和人工审计结合的方式进行，管理方面的脆弱性主要通过访谈和调查问卷来识别。对以往安全事件的统计和分析是确定脆弱性的重要方法。

脆弱性识别的结果应根据评估策略和目的进行调整，可参照相应的技术或管理标准，以及评估发起方的要求实施。

（2） 脆弱性赋值

脆弱性赋值包含严重程度和对系统安全属性的影响两部分内容，即确定脆弱性对电力监控系统资产的暴露程度（包括被威胁利用的可能性和难易程度）和脆弱性对安全属性的哪方面产生了破坏。

附录 B 列出了电力监控系统安全技术和管理两方面要求，不符合要求为缺陷或漏洞。根据附录 B 各分表的符合率确定脆弱性赋值，对应关系如表 C-65:

表 C-5 脆弱性赋值表

标识	赋值	定义
很高	5	如果脆弱性被威胁利用，将对资产造成完全损害
高	4	如果被威胁利用，将对资产造成重大损害
中	3	如果被威胁利用，将对资产造成一般损害
低	2	如果被威胁利用，将对资产造成较小损害
很低	1	如果被威胁利用，将对资产造成的损害可以忽略

（3） 脆弱性总体评价

根据脆弱性识别和脆弱性赋值结果，对系统脆弱性进行总体评价，找到被评估系统与电力监控系统安全防护要求的差距。

脆弱性总体评价标准见 5.1。

C1.4 安全防护措施确认

识别脆弱性的同时，评估人员应对现有安全措施的有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生后对组织或系统造成的影响，如业务持续性计划。

已有安全措施确认与脆弱性识别存在一定的联系，安全措施的使用将减少系统技术或管理上的脆弱性，但安全措施确认并不需要和脆弱性识别过程那样具体到每个资产、组件的弱点，而是一类具体措施的集合，安全措施只为风险处理计划的制定提供依据和参考。

C1.5 风险分析

风险分析中主要涉及资产、威胁、脆弱性三个基本要素，每个要素有各自的属性，资产的属性是资产价值威胁的属性可以是威胁主体、影响对象、出现频率、动机等，脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

1) 对资产进行识别，并对资产的价值进行赋值，即资产赋值；

2) 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值，即威胁赋值；

3) 对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值，即脆弱性赋值；

4) 根据威胁赋值及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

5) 根据脆弱性的严重程度及安全事件所作用的资产的赋值计算安全事件造

成的损失;

6) 根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

风险分析模型如图 C-1 所示:

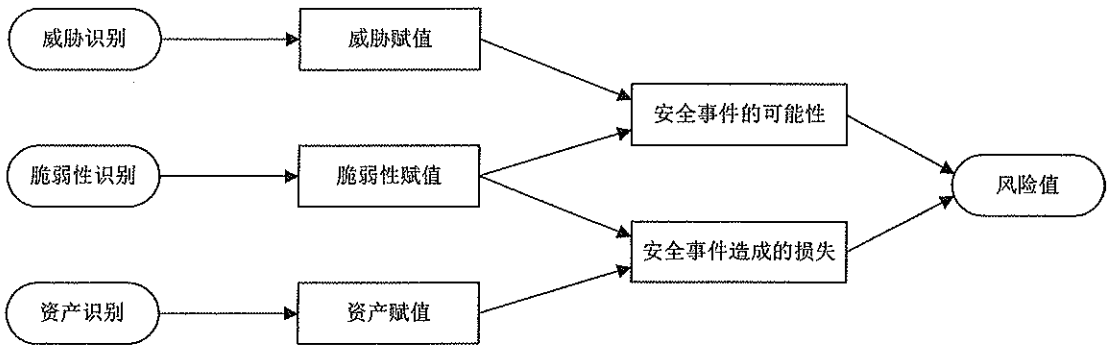

图 C-1　风险分析模型

C2 评估实施流程

电力监控系统安全防护评估实施流程分为四个阶段: 启动准备阶段、现场实施阶段、安全分析阶段和安全建议阶段。在评估实施完毕后，需要根据评估结论进行安全整改。实施流程如图 C-2 所示:

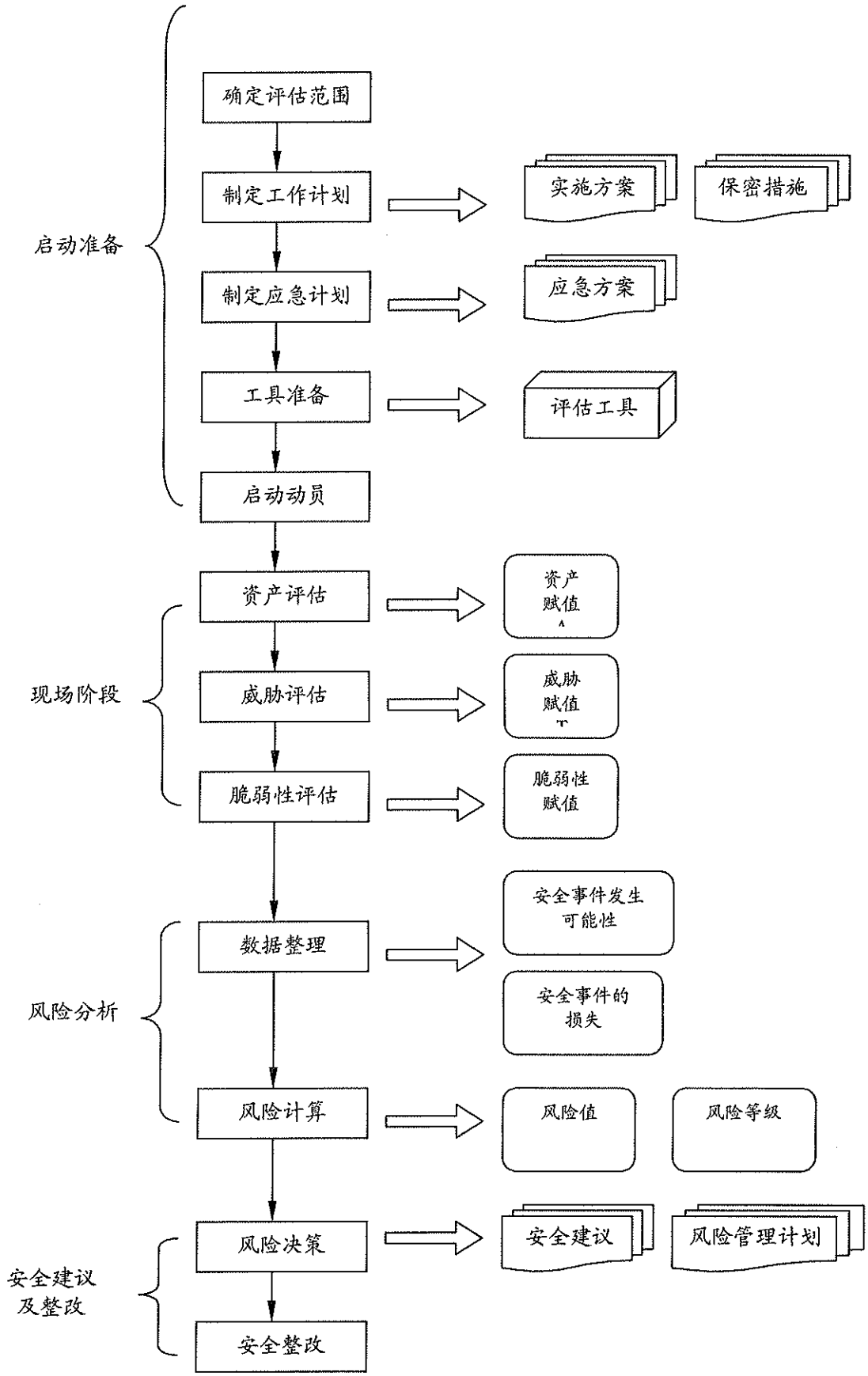

图 C-2　电力监控系统安全防护评估实施流程

C2.1 评估准备

第 1 步：成立评估工作组

评估工作下达后，应成立评估工作组，组织人员实施评估工作。评估工作组通常包括如下两方面的人员：

评估人员：由专业评估机构或内部人员组成的评估队伍。

系统管理人员：待评系统的运行维护、管理人员。

第 2 步：确定评估范围

评估范围可通过评估组的工作会议进行确定。

确定的评估范围应能代表待评估系统的所有关键资产，包括：网络范围、主机范围、应用系统范围、制度与管理范围。

评估范围确定后，待评系统管理人员需要根据选定的内容进行资料的准备工作，包括：网络拓扑结构图、电力监控系统资产清单、应用系统的说明文档、组织机构设置说明等内容。

第 3 步：评估工具准备

评估工作组根据收到的评估资料，进行评估工具的准备，包括威胁列表、网络评估工具、主机评估工具、资产识别工具、安全管理访谈表等内容。

评估工具中大部份内容需要根据评估范围和评估的主要目的进行定制，例如：威胁列表需要根据实际的物理、网络环境来进行定制；安全管理访谈表需要根据待评估系统的管理结构、管理方式进行定制。

在评估工具中，网络、主机脆弱性评估的通用性较强，目前可找到的商用和免费工具较多。下表是一些通用的脆弱性评估工具列表，但不得对生产控制大区在线运行系统进行自动化工具评估。

表 C-6　脆弱性评估工具

工具类型		用途说明
漏洞扫描工具	集成漏洞扫描工具	主机安全漏洞扫描、网络设备安全漏洞扫描
	数据库漏洞扫描工具	发现 Oracle、SQL 等主流数据库上存在的安全漏洞
	Web 漏洞扫描工具	发现 Web 服务中存在的安全漏洞
端口分析		Windows 系统主机端口分析工具
协议分析工具		网络协议分析

人工审计工具	用来进行远程主机登录，可方便存取人工审计数据
网络拓扑发现	可用于网络拓扑发现、网络设备配置下载

第 4 步：准备应急措施

电力监控系统安全防护评估中，为应对评估实施工作可能对系统带来的不利影响，评估工作组应在被评估方的配合下制定应急预案，确保在发生紧急事件时不对业务系统正常运行产生大的影响。如果需要对在线运行系统进行扫描，必须按照管理制度履行相关操作手续进行登记和向主管领导汇报。

C2.2 现场评估

根据现场评估阶段工作流程，规范工作步骤如下：

第 1 步：电力监控系统资产评估

电力监控系统资产评估包括了资产识别和资产赋值两部分内容，其中资产赋值需要在对业务系统进行充分了解和分析的基础上进行。资产评估中采用以业务系统为主线的方法，将每一项电力监控系统资产按照所属业务系统进行归类，在业务系统划分的基础上评估系统的安全性。

表 C-7　资产识别

输入	输出
电力监控系统资产识别表、网络拓扑和说明、业务系统说明、信息系统描述与系统分析报告	电力监控系统资产清单列表

第 2 步：电力监控系统威胁评估

电力监控系统威胁评估是利用电力系统安全威胁列表，通过访谈以及现场访谈和观察的方式，对当前电力监控系统所面临的主要安全威胁进行判定的过程。威胁评估主要包含以下三项内容：

（1）威胁统计

威胁统计是对电力监控系统面临的威胁的确认过程，威胁数据来源的方式较为多样，评估中可根据情况先进性威胁列表的维护，再根据实际环境进行判断和分析。

表 C-8　威胁统计

输入	输出
威胁列表、信息系统日志、系统环境说明	系统威胁统计表

（2）威胁赋值与计算

表 C-9　威胁赋值与计算

输入	输出
系统威胁统计表	资产威胁赋值表

第 3 步：安全分区合理性评估

参照总体方案的分区要求，对电力监控系统安全区的划分是否合理性进行检查。此外，安全分区合理性评估还包括对各安全区中业务系统网络构架合理性的评估。

表 C-10 安全分区合理性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统分区情况记录

第 4 步：边界完整性评估

边界完整性是对安全区 I、II 和 III 之间的边界连接情况进行的审核，确定在规定的边界点外没有短路情况。

表 C-11　边界完整性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统分区边界完整性审计记录

第 5 步：节点通信关系分析

通过对电力监控系统的业务数据流和业务网络结构的审核，对电力监控系统节点间通信关系进行分析，以确定某一安全区中的那些业务系统功能模块需要同其他安全区进行通信，以及这些通信间的安全要求。

表 C-12　节点通信关系分析

输入	输出
网络拓扑说明、业务系统功能说明	电力监控系统通信关系表

第 6 步：边界安全性评估

边界安全性评估是对安全区边界点的防护强度、访问控制力度和粒度的审核，以确定安全区边界的防护是否符合总体方案的要求。

表 C-13 边界安全性评估

输入	输出
《电力监控系统安全防护总体方案》、电力监控系统现状说明	电力监控系统边界点审计记录

第 7 步：主机安全评估

主机安全性评估是对业务系统范围内的主机进行安全漏洞的发现的过程，包括如下内容：

（1）设备安全漏洞扫描

设备安全漏洞扫描是采用漏洞扫描工具对系统技术漏洞的发现过程，在漏洞扫描的过程中可能会对业务系统的运行产生影响，因此需要得到操作许可，并准备应急预案以避免由安全评估产生的风险。

表 C-14 设备安全漏洞扫描

输入	输出
电力监控系统资产清单	设备漏洞扫描结果

（2）设备审计

设备审计是采用人工登录主机或网络设备的方式对设备的安全配置情况进行的审计，由于设备配置数据是信息系统的敏感数据，因此在审计前需要得到操作许可。

表 C-15 设备审计

输入	输出
电力监控系统资产清单，主机或网络审计检查列表	设备审计结果

第 8 步：网络系统评估

网络系统评估包括对调度数据网、本地局域网的网络结构、网络设备的安全性、网络管理情况、网络配置评估等评估内容。

表 C-16 网络系统评估

输入	输出
网络拓扑结构说明、关键网络设备配置	网络安全评估记录

第 9 步：安全管理评估

安全管理评估包括策略访谈和管理制度文档审计两项内容。评估参照《GB/T 22080-2008 信息安全管理体系要求》和《电力监控系统安全防护总体方案》中对电力监控系统的信息安全管理要求进行。

（1）安全管理制度文档分析

文档分析主要是对电力监控系统管理中已制定和采用的安全管理制度文档以及制度的执行情况进行分析，通过分析发现现有制度中的缺陷。本部分的工作可以先期展开。

表 C-17 安全管理制度文档分析

输入	输出
安全管理规章、制度，管理制度评估工具	安全制度文档分析报告

（2）业务系统管理分析

对业务系统管理的分析从对具体业务系统的管理制度、岗位职责定义文档出发，并通过实际的观察和访谈确认系统管理的情况。

表 C-18 业务系统管理分析

输入	输出
业务系统管理制度，系统岗位分配文档	业务系统管理审计结果记录

第 10 步：业务系统安全评估

对业务系统软件提供的安全功能和自身的安全配置进行审核，以确定这些业务系统软件安全缺陷。

表 C-19 业务系统安全评估

输入	输出
电力监控系统资产清单(含业务系统)	业务系统软件安全评估记录

第 11 步：现有安全技术措施评估

对现有安全技术措施，如安全分区情况、安全隔离装置、防火墙和防病毒系

统等部署情况、管理与运维情况等进行审核，确定防护措施是否发挥了应有作用。

表 C-20 现有安全措施审计

输入	输出
电力监控系统资产清单、（现有安全措施部署方案）	现有安全措施审计记录

C2.3 风险分析

风险分析过程包括数据整理、风险计算和风险决策三个步骤。

（1） 数据整理

数据整理是将资产调查、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，进行分析和整理的过程，整理内容如下：

1) 评估资产列表：针对评估范围中的资产，对资产根据业务、类型进行分类，形成具体的资产或资产组；根据资产或资产组承载的业务和数据、所处的位置进行资产赋值的调整，确定出可计算的资产价值；
2) 威胁分析表：针对具体的资产或资产组，根据现场识别和赋值的威胁列表判断资产面临的威胁情况，并对现场所赋的威胁可能性和威胁影响值进行调整；
3) 脆弱性列表：针对具体的资产或资产组，整理脆弱性列表，并进行管理、运维和技术的分析，分析其产生原因和被利用的后果；
4) 安全事件的损失：根据资产值和脆弱性严重程度，采用矩阵法或者相乘法计算安全事件的损失；
5) 安全事件发生的可能性：根据威胁出现的频率等级和脆弱性严重程度，采用矩阵法或者相乘法计算安全事件发生的可能性。

（2） 风险计算

在完成资产评估、威胁评估和脆弱性评估后，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。

风险计算可采用矩阵法或者相乘法，在符合国标要求下不限定计算方法。通过安全事件损失值和安全事件发生可能性计算相应的风险值，并根据风险值确定风险等级。风险计算的原理方法参见 5.2 和附录 C1.5。

（3） 风险决策

风险决策是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的过程。风险决策步骤如下：

（1）根据风险计算结果，按照给资产造成的损失大小对风险进行排序，并计算消除或降低风险所需的成本，在此基础上决定对风险采取的处理方法；

（2）对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中应明确采取的弥补脆弱性的安全措施、预期效果、实施条件、进度安排、责任部门等；

（3）对不可接受的风险进行安全整改后的残余风险要进行评估，确保其在可接受的范围内。

风险决策是提出安全建议的基础，科学、合理的风险决策是提高安全建议质量、防止过度防护和防护不足的保障。

C2.4 安全建议

安全建议是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，经过合理的统计归纳，形成安全解决方案建议报告的过程。安全建议报告应包含安全建议阶段的所有工作内容，具体如下：

（1）需求分析：需求分析根据风险分析的结论将电力监控系统的防护需求进行归纳和总结，并根据评估结果进行了现状分析、可行性分析和紧迫性分析；

（2）安全建议：根据需求分析的结论针对不同评估节点提出安全防护措施；

（3）实施计划：根据可行性分析和紧迫性分析结论提出安全建议的实施计划。

评估工作组必须对安全建议方案着重讨论，确保安全建议的合理性、可行性。

C2.5 安全整改

被评估单位应根据安全建议方案制定整改计划、落实整改措施，不断提高电力监控系统安全防护能力。

附录D电力监控系统安全防护与等级保护基本要求对照表

安全类别		等保要求	电力监控系统安全防护要求	关键点
技术	物理安全	位置选择、访问控制、防盗防破坏、防雷击、防火、防水防潮、防静电、温湿度控制、电力供应、电磁防护	按照安全分区的原则，将不同重要程度的设备置于各安全区域内，对重要设备采取电磁屏蔽措施。其防护强度等同于等级保护要求。	① 四级系统采取电磁屏蔽措施； ② 按照设备、操作间进行机房物理区域划分，按安全分区摆放机柜； ③ 四级系统要采用两道门禁。
	网络安全	结构安全、访问控制、安全审计、边界完整性、入侵防范、恶意代码防护、网络设备防护	电力监控系统遵循“安全分区、网络专用、横向隔离、纵向认证”的防护原则，将电力监控系统分置于生产控制大区和管理信息大区，在两个大区之间部署横向单向隔离装置，在生产控制大区专用的调度数据专用网络边界部署纵向加密认证装置，形成栅格状安全防护体系架构，其防护强度等同于等级保护要求。	① 专网专用； ② 安全分区； ③ 横向边界部署返回1比特的新型横向隔离装置； ④ 纵向边界部署纵向加密认证装置，配置IP+限定端口的控制策略，对端有装置的应启用密通功能。
	主机安全	身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制	对原有系统按照《电力监控系统安全加固规范》进行安全加固，并通过加强运维管理保障主机及操作系统安全。 新一代调度控制系统采用国产设备，国产安全操作系统提高了安全防护水平，同时满足等级保护要求。其防护强度等同于等级保护要求。	① 对原有系统进行安全加固； ② 各个层面的口令均应杜绝7位以内弱口令。 ③ 新系统采用国产设备、国产安全操作系统、国产安全数据库；
	应用安全	身份鉴别、安全标记、访问控制、可信路径、	原有系统在安全加固的基础上，加强访问控制措施和对内	① 加强对原有系统及人员的日常管理；

安全类别		等保要求	电力监控系统安全防护要求	关键点
		安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、 资源控制	部人员的管理措施，以提升其安全防护水平。使防护强度基本等同于等级保护四级要求。新一代系统采用基于调度数字证书及安全标签的一体化基础平台，实现安全访问控制可信可控。其防护强度等同于等级保护要求。	② 各个层面的口令均应杜绝 7 位以内弱口令; ③ 新系统采用基于调度数字证书及标签的安全认证。
	数据安全及备份恢复	数据完整性 数据保密性 备份和恢复	电力监控系统从数据层面、系统层面和调度业务层面三个层面均要求实现备用，以此为基础建立备用调度体系，实现全面的电力监控系统安全备用机制，其防护强度等同于等级保护要求	① 实现数据级备用; ② 实现自动化系统及功能备用; ③ 实现调度业务及人员备用。
管理	安全管理制度	管理制度、制定和发布、评审和管理	建立了电力监控系统安全防护相关管理制度，依照“谁主管谁负责，谁运营谁负责”的原则，与调度安全性评价相结合，常态化开展管理工作。	① 制定电力监控系统安全防护管理制度。
	安全管理机构	岗位设置、人员配备、授权和审批、沟通和合作、审核和检查	成立了电力监控系统安全防护领导小组，建立安全工作协调机制，明确职责分工。调度部门的安全管理人员专人专岗。	① 建立电力监控系统安全管理机构。
	人员安全管理	人员录用、人员离岗、人员考核、安全意识教育和培训、外来人员访问管理	要求对电力监控系统安全防护专职人员定期进行培训和考核。同时建立保密制度，加强保密教育，提高安全防护意识，并与相关人员签署保密协议。加强对外来人员的管控，强化出入管理核查。	① 定期培训; ② 签署保密协议; ③ 外来人员管控。
	系统建设	系统定级、安全方案设	制定了针对电力监控系统专用	① 加强安全产品和业务

安全类别		等保要求	电力监控系统安全防护要求	关键点
	管理	计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择	安全产品和业务系统的开发单位及供应商的管控措施，对自主开发的软件进行严格管理防止关键技术扩散。	系统的开发单位及供应商的管控措施； ② 与开发单位及供应商签署保密协议。
	系统运维管理	环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码管理、密码管理、变更管理、备份与恢复、安全事件处置、应急预案管理	制定电力监控系统日常安全管理制度，制定了监控系统的应急处理预案。	① 制定安全运维管理制度； ② 制定监控系统的应急预案。

附录E 电力监控系统安全防护评估报告大纲

报告编号：----------

电力监控系统安全防护评估报告

被评单位：_____

委托单位：_____

评估单位：_____

报告时间：_____

电力监控系统安全防护评估基本信息表

<table>
<tr><td colspan="6">委托单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td>评估对象</td><td colspan="5"></td></tr>
<tr><td rowspan="2">联系人</td><td rowspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>邮箱</td><td colspan="3"></td></tr>
<tr><td colspan="6">评估单位信息</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="3"></td><td>邮编</td><td></td></tr>
<tr><td rowspan="2">联系人</td><td rowspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>邮箱</td><td colspan="3"></td></tr>
<tr><td>评估日期</td><td colspan="5"></td></tr>
<tr><td rowspan="3">评估小组</td><td>组长</td><td colspan="4"></td></tr>
<tr><td>组员</td><td colspan="4"></td></tr>
<tr><td>监督员</td><td colspan="4"></td></tr>
<tr><td>编制人</td><td></td><td>编制日期</td><td colspan="3"></td></tr>
<tr><td>审核人</td><td></td><td>审核日期</td><td colspan="3"></td></tr>
<tr><td>批准人</td><td></td><td>批准日期</td><td colspan="3"></td></tr>
</table>

1. 概述

1.1 项目背景

1.2 项目目的

1.3 项目依据

1.4 评估范围

1.5 工作方法

1.6 评估过程

1.7 报告分发范围

2. 评估对象描述

2.1 业务系统描述

3. 资产识别与赋值

3.1 资产类别

3.2 资产识别

3.3 资产赋值

4. 威胁分析

4.1 威胁类别

4.2 威胁识别

4.3 威胁赋值

5. 脆弱性分析

以下无正文