2025年电力二次系统安全防护处置方案模板(三)

一、总体要求

1.1. 安全防护目标

(1) 安全防护目标旨在确保电力二次系统的稳定运行，保障电力供应的安全可靠。具体而言，目标是实现电力二次系统的物理安全、网络安全、数据安全、设备安全和运行安全，防止因外部攻击、内部误操作或自然灾害等因素导致的系统故障和安全事故。

(2) 在物理安全方面，目标是确保电力二次系统的硬件设施不受物理破坏，包括对数据中心、通信设备、控制室等关键设施的物理保护，防止非法侵入、破坏和盗窃等行为。

(3) 在网络安全方面，目标是建立完善的网络安全防护体系，包括防火墙、入侵检测系统、安全审计等，以防止网络攻击、病毒入侵、恶意代码传播等网络安全威胁，保障电力二次系统的稳定运行和数据安全。同时，加强对网络流量和用户行为的监控，及时发现并处理异常情况，确保网络安全。

2.2. 安全防护原则

(1)

安全防护原则应遵循系统性、全面性、动态性和可操作性。系统性要求安全防护措施应覆盖电力二次系统的各个环节，全面性强调对物理、网络、数据、设备和运行等各个方面的安全进行综合防护。动态性原则要求安全防护策略应能适应新技术、新威胁和新环境的变化，保持其有效性。可操作性则要求安全防护措施必须具体可行,便于实施和管理。

(2) 在实施安全防护时，应坚持预防为主、防治结合的原则。预防为主意味着在系统设计和运行过程中，应充分考虑安全因素，从源头上减少安全风险。防治结合则要求在采取预防措施的同时，也要建立健全的检测、预警和应急响应机制，确保在安全事件发生时能够迅速、有效地进行处置。

(3) 安全防护工作应遵循法律法规，符合国家标准和行业标准。在制定和实施安全防护策略时，必须严格遵守国家有关电力安全、网络安全和信息安全的相关法律法规，确保安全防护工作的合法性和合规性。同时，要关注国内外安全防护的最新动态，及时跟踪和引进先进的安全技术和方法，提高电力二次系统的整体安全防护水平。

3.3. 安全防护范围

(1) 安全防护范围涵盖了电力二次系统的全部关键组成部分，包括但不限于电力生产、传输、分配和消费等各个环节。这包括发电厂的控制和保护系统、输电线路的监控和保护设备、变电站的自动化和监控装置、配电网络的调度和控制系统，以及用户端的电力计量和监控设备。

(2)

安全防护范围还涉及电力二次系统的网络基础设施，包括专用通信网络、互联网接入点、内部网络以及与外部系统互联的接口。此外，还包括所有与电力二次系统相关的软件应用、数据库、配置文件以及相关的物理设备，如服务器、工作站、交换机、路由器等。

(3) 安全防护范围还扩展到对电力二次系统数据的保护，包括实时数据、历史数据、配置数据和管理数据等。这要求对数据传输、存储和处理的各个环节进行安全控制，防止数据泄露、篡改和非法访问，确保电力二次系统的运行数据安全可靠。同时，还包括对系统操作日志、审计日志等安全日志的保护，以便于安全事件的追踪和调查。

二、组织管理与职责

1.1. 组织机构设置

(1) 组织机构设置应以保障电力二次系统安全防护为核心，设立专门的电力二次系统安全防护领导小组，由公司领导担任组长，各部门负责人为成员，负责统筹协调全公司的安全防护工作。领导小组下设办公室，负责日常管理工作，包括制定安全防护策略、组织安全培训、监督安全措施的执行等。

(2) 在公司内部，设立安全防护管理部门，负责具体实施电力二次系统的安全防护措施。管理部门下设多个职能小组，如网络安全小组、设备安全小组、数据安全小组等，分别负责相应领域的安全防护工作。此外，还设立应急响应小

组，负责处理突发事件和安全威胁。

(3) 各基层单位也应设立相应的安全防护组织，明确安全防护责任人和职责，负责本单位的电力二次系统安全防护工作。基层单位的安全防护组织应定期向上级管理部门汇报工作进展，接受指导和监督，确保安全防护措施得到有效实施。同时，加强与其他单位的协作与沟通，形成联动机制，共同应对安全挑战。

2.2. 职责分工

(1) 电力二次系统安全防护领导小组负责制定安全防护战略规划，审批重大安全防护措施，协调解决安全防护工作中的重大问题。领导小组组长负责总体协调，副组长协助组长工作，成员根据各自职责分工，负责相应的安全防护领域。

(2) 安全防护管理部门负责具体执行领导小组的决策，制定详细的安全防护方案和操作规程，组织实施安全防护措施，对安全防护工作进行日常管理。网络安全小组负责网络设备的配置与维护，监测网络安全状况，处理网络攻击事件；设备安全小组负责设备的定期检查、维护和更新，确保设备安全可靠运行；数据安全小组负责数据的安全存储、传输和备份，防止数据泄露和篡改。

(3)

各基层单位的安全防护责任人负责本单位的电力二次系统安全防护工作，包括组织安全培训、制定安全操作规程、监督安全措施的执行等。他们需定期向上级管理部门汇报工作情况，接受指导和监督。同时，基层单位的安全防护责任人应与上级管理部门保持密切沟通，确保安全防护工作的一致性和有效性。在发生安全事件时，基层单位责任人应立即启动应急预案，采取应急措施，并及时向上级汇报。

3.3. 安全防护培训

(1) 安全防护培训是提高员工安全意识和技能的重要手段。公司应定期组织安全防护培训，确保所有员工都能了解电力二次系统安全防护的基本知识和操作规程。培训内容应包括安全防护的基本原则、网络安全、设备安全、数据安全等方面的知识，以及应对突发事件和应急响应的技能。

(2) 安全防护培训应针对不同岗位和职责的员工制定差异化的培训计划。对于关键岗位的员工，如网络安全管理员、设备维护人员、数据管理人员等，应进行专业化的深度培训，提高他们在各自领域的安全防护能力。同时，对于一般员工，应普及基本的安全防护知识，增强他们的安全意识。

(3) 安全防护培训应采用多种形式，如课堂讲授、实操演练、在线学习、案例分析等，以提高培训效果。公司可邀请外部专家进行专题讲座,分享最新的安全防护技术和经验。此外，通过组织内部竞赛和交流活动，激发员工学习安全防护知识的积极性，形成良好的安全文化氛围。培训结束后，

应对员工进行考核，确保培训目标的实现。

三、安全防护技术措施

1.1. 网络安全防护

(1)

网络安全防护是电力二次系统安全防护的重要组成部分。应建立多层次、全方位的网络安全防护体系，包括物理安全、网络安全、应用安全、数据安全等多个层面。物理安全方面，确保网络设备、服务器等关键设备的安全存放和物理访问控制。网络安全方面，通过部署防火墙、入侵检测系统等，对网络流量进行监控和控制，防止恶意攻击和非法访问。

(2) 应用安全方面，应定期对系统软件进行更新和补丁管理，以修复已知的安全漏洞。同时，对关键应用进行安全加固，如采用强认证机制、访问控制策略等，确保应用层的安全性。数据安全方面，对敏感数据进行加密存储和传输，防止数据泄露和篡改。此外，建立数据备份和恢复机制，确保在数据丢失或损坏时能够迅速恢复。

(3) 网络安全防护还应包括安全事件监测、预警和应急响应。通过建立安全事件监测系统，实时监控网络流量和系统状态，及时发现异常行为和安全威胁。预警机制能够对潜在的安全风险进行预警，提醒相关人员进行干预。在发生网络安全事件时，应迅速启动应急响应计划，采取有效措施进行处置，减少损失，并防止事态扩大。

2.2. 设备安全防护

(1)

设备安全防护是电力二次系统安全的关键环节，涉及到对各类电气设备、自动化装置、控制系统的维护与管理。首先，应确保设备选型符合安全标准，具有良好的抗干扰能力和稳定性能。对于关键设备，应实施双重或三重冗余设计，以防止单点故障导致系统瘫痪。

(2) 设备安全防护措施包括日常维护保养、定期检查和及时更换老旧设备。日常维护保养要严格执行操作规程，定期对设备进行清洁、润滑和调整，确保设备处于最佳工作状态。定期检查应覆盖设备的所有关键部件，包括电气、机械、传感器等，及时发现并修复潜在的安全隐患。

(3) 对于设备安全防护,还需建立完善的事故应急预案。一旦发生设备故障或安全事故，应能迅速启动应急预案，采取有效措施进行隔离、修复和恢复。同时，对事故原因进行深入分析，制定预防措施，避免类似事件再次发生。此外，定期组织应急演练，提高员工应对突发事件的能力，确保设备安全防护工作落到实处。

3.3. 数据安全防护

(1) 数据安全防护是电力二次系统安全防护的核心内容，涉及对系统内所有数据的保护，包括实时数据、历史数据、配置数据和管理数据等。数据安全防护的首要任务是确保数据的机密性、完整性和可用性。机密性要求对敏感数据进行加密存储和传输，防止未授权访问；完整性要求确保数据在存储、传输和处理过程中不被篡改；可用性要求在数据

遭到破坏或丢失时能够迅速恢复。

(2)

数据安全防护措施包括但不限于数据加密、访问控制、审计跟踪和数据备份。数据加密技术用于保护数据在存储和传输过程中的安全，访问控制机制确保只有授权用户才能访问特定数据，审计跟踪记录所有数据访问和操作，以便于事后调查和责任追究。数据备份则是为了在数据丢失或损坏时能够及时恢复，通常采用定期备份和灾难恢复计划。

(3) 数据安全防护还需要建立数据安全管理制度，明确数据安全责任，制定数据安全政策和操作规程。这包括对数据分类、数据生命周期管理、数据安全事件处理等方面的规定。同时，应定期对数据安全防护措施进行评估和审计，确保防护措施的有效性和适应性，以应对不断变化的安全威胁和挑战。通过持续改进，不断提升数据安全防护水平，保障电力二次系统的稳定运行和数据安全。

四、安全监测与预警

1.1. 安全监测系统

(1) 安全监测系统是电力二次系统安全防护的关键组成部分，其主要功能是对系统内的安全状态进行实时监控，及时发现潜在的安全威胁和异常情况。系统应具备全面性、实时性和准确性，能够覆盖电力二次系统的各个层面，包括网络安全、设备安全、数据安全等。

(2) 安全监测系统应具备数据采集、分析和报警等功能。数据采集部分负责从各种监测点收集实时数据，如网络流量、设备状态、系统日志等；分析部分对采集到的数据进行处理

和分析，识别异常模式和潜在的安全威胁；报警功能则是在检测到异常时及时向相关人员发出警报。

(3)

安全监测系统还应具备联动功能，能够在检测到安全事件时，自动触发相应的应急响应措施。这包括隔离受威胁的设备、切断数据传输通道、启动备份系统等。此外，系统应支持历史数据的存储和查询，便于事后分析和审计。通过持续优化和升级安全监测系统，可以不断提高电力二次系统的安全防护能力。

2.2. 预警机制

(1) 预警机制是电力二次系统安全防护体系的重要组成部分，旨在通过实时监测和数据分析，提前发现并报告潜在的安全风险和威胁。预警机制的设计应考虑系统的整体安全目标，确保能够及时响应各种安全事件，降低安全风险对电力系统的影响。

(2) 预警机制通常包括以下几个关键要素：一是预警信息收集，通过部署各种传感器、监控系统等，实时收集系统运行数据和安全事件信息；二是预警信息分析，利用先进的数据分析技术，对收集到的信息进行深度分析，识别异常模式和潜在威胁；三是预警信息发布，通过短信、邮件、系统弹窗等方式，将预警信息及时传递给相关人员。

(3) 预警机制的运行需要与应急响应系统紧密配合。一旦预警信息被确认，应立即启动应急响应流程，采取相应的措施进行干预。这包括安全事件的隔离、恢复受损系统、修复漏洞、加强监测等。同时，预警机制还应具备自我学习和自我调整的能力，根据历史数据和实时反馈不断优化预警模

型，提高预警的准确性和有效性。

3.3. 应急响应

(1) 应急响应是电力二次系统安全防护体系中的关键环节，旨在确保在发生安全事件时，能够迅速、有效地采取行动，减少损失，恢复正常运行。应急响应计划应包括明确的组织结构、职责分工、响应流程和资源调配。

(2) 应急响应组织结构通常包括应急指挥中心、应急小组和专业技术人员。应急指挥中心负责统一协调和指挥应急响应行动，应急小组负责执行具体任务，如现场处理、技术支持、信息沟通等。专业技术人员提供技术支持和专家意见，确保应急响应措施的合理性和有效性。

(3) 应急响应流程包括以下几个步骤：首先，监测系统发现安全事件后，立即向应急指挥中心报告；其次，应急指挥中心评估事件严重程度，决定是否启动应急响应；接着，应急小组按照预案进行行动，采取隔离、修复、恢复等措施；最后，事件得到控制后，进行事件总结和后续改进，以提高未来应急响应的效率和效果。此外，定期的应急演练和培训是确保应急响应能力的关键。

五、安全防护管理制度

1.1. 安全管理制度

(1)

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。

如要下载或阅读全文，请访问：

https://d.book118.com/147201032161010046