工程与管理科学
Engineering and Management Science
第 6 卷◆第 12 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

电力调度自动化二次系统安全防护初探

刘爽
国网冀北围场供电分公司　河北承德　068450
DOI：10.12238/ems.v6i12.10890

［摘　要］作为地区用电的中心，电网二次电网的安全保护对于保障全国电网的稳定运行具有十分重要的意义。文章总结配电网络中二次保护的关键技术，并对其在配电网络中的运用进行探讨，以期对配电网络的安全保护工作起到一定的指导作用，从而推动整个区域的经济发展。
［关键词］电力调度；自动化；二次系统；安全防护

Preliminary Study on Safety Protection of Power Dispatching Automation Secondary System

Liu Shuang
State Grid Jibei Weichang Power Supply Branch, Chengde, Hebei　068450

[Abstract] As the center of regional electricity consumption, the safety protection of the secondary power grid is of great significance for ensuring the stable operation of the national power grid. The article summarizes the key technologies of secondary protection in distribution networks and explores their application in distribution networks, in order to provide guidance for the safety protection of distribution networks and promote the economic development of the entire region.
[Keywords] power dispatching; Automation; Secondary system; safety protection

引言

近几年来，随着人们的生活水平越来越高，对电力调度自动化控制的品质和系统服务水平的要求也越来越高。特别是在安全方面，对二次设备的安全提出更高的要求。这样的要求使得电力调度控制系统需要对技术进行持续的改进和创新，提升它的技术水平、质量和安全，所以，在追求不同的自动化二次系统的控制方式的同时，也要提升设备的操作水平。必须强化二次自动控制系统的技术监管，持续优化工艺运用，全面提升工艺质量，强化安全保护手段；使系统运行最大化。

1.二次系统安全防护技术概述

电网二次设备的安全性保护，是指以计算机为基础，以计算机为基础的、以计算机为基础的、以计算机为基础的自动化设备。电力系统的安全保护主要针对电力系统中的各种病毒、黑客、恶意代码等的入侵和损害，防止电力系统发生大规模停电事故和电力系统事故。二次配电装置等为用电资源的监视和控制，对发电厂中的各种自动、智能化装置进行实时的监视和控制。在此基础上，提出“网络专用”“安全分区”“横向隔离”和“纵向认证”四种安全保护策略，其主要功能是保护，反应，探测，恢复。二次电源是继电保护与控制一次电网电源回路,其作用是对电网中有关电器进行保护，如变压器，电机，发电机，母线等。如果主电路出现过电流，短路，过热；当出现过电压，雷击等故障时，将立刻进行二次保护动作。

2.电力调度自动化二次系统安全防护要点

在电力调度自动化的次级系统中，安全防护工作至关重要，其核心在于对信息流通过程、存储环节以及数据处理阶段的严密监控。通过实施一系列高效的技术策略，确保病毒及其他风险因素被有效隔绝。次级系统的安全防护旨在确保数据在监控和应用系统间的交换过程中，能够得到充分的安全保障。针对跨远程区域的数据传输，必须采取加密等手段，确保数据在传输过程中不被截获或篡改。对于非法入侵者，限制其访问权限是主要的防护策略。此外，数据备份作为一种保障数据完整性和真实性的措施，对于应对数据传输中可能出现的问题至关重要，即便在数据传递后期出现问题，原始数据依然可以得到保留。

作为电力调度系统的关键组成部分，自动化次级系统的稳定运行对于提升供电系统的安全性、可靠性和经济性至关重要。在夏季，我国电力需求达到顶峰，用电量的剧增为电力调度带来严峻挑战，配电网络也承受着巨大压力。由于系统问题导致的电力故障频繁,这些故障不仅会导致供电中断，还会给居民生活和社会发展带来诸多不便。因此，确保自动化次级系统的顺畅运作，对于提升电力调度系统的供电质量和效率具有积极作用，进而推动整个电力调度系统的稳定运

行。此外，自动化次级系统的应用还在一定程度上减少电能损耗，体现自动化技术的环保价值。

2.1 电气设计

将二次控制技术引入到电网运行中，具有比常规电网更加稳定的特点。要对电路设计的科学和合理给予足够的关注，在选用系统的电路设计的方案时要慎重考虑，使用高质量的材料如 ZnO 避雷器和 PVC 电缆，来建造整个系统的配电网络。这种材料制成的配电装置具有很好的气密性，可以确保二次装置的工作效率和整个自动化系统的品质。在二次自动控制中，电气设计的重点是：①在电力系统中，合理地确定和选取合适的参数，以确保变压器在电网中的稳定性，提升其供电效率和供电品质。②在二次自动控制中，应将低电压电容器的补偿装置进行并联，以实现对变压器的供电进行补偿，从而提高设备的工作年限，节省电网的费用；取得一些经济效益。③针对电网的各种需要和规范，电网的电气设计要适应电网的现实需要，针对电网的工作特点，持续改进电网的设计，减少电网建设的困难。

2.2 网络接线模式设计

在二次系统的应用设计中，网络布线方式是最为关键的一环。科学、合理的网络布线方式能够推动自动化二次系统的建造和建造工作的平稳进行，从而提升自动化技术的使用效果。如果不能与电网协调运行，不仅会导致输电速度下降，而且还会浪费巨大的电能，从而导致较高的经济价值。为此，为确保电力系统安全可靠地进行二次设备的运营与使用，必须建立起一套科学合理的配网方式。在实际的建设中，对电力系统中的各种导线进行合理的连接，选用适当的材质，使之成为一种可靠、可靠的电网结构；确保电网配网方式与电网整体运行协调一致。

2.3 开闭所接线模式设计

对开关柜的电气连接方式进行研究，并提出相应的解决方案。通常，开关的布线方式是一项非常繁琐的工作，它对设计者有着非常高的技术素质。传统的配电线路方式存在着开关所配线不稳、供电品质较低等问题。电能的传送速度也减少。所以，对开关柜二次设备进行合理的布线方式是进行自动二次设备的设计。要正确地选用开关所配线方式，使其负载等级保持平稳，并改善其内部装置的工作品质，同时还要注重在设计时对装置的安装孔进行预留；从而确保电网的平稳运行。

2.4 安全防护原则

在二次自动控制中，对其进行安全保护时，要注意科学原理。二次系统的安全保护是一个更加科学和严格的工作，对其进行的安全性评估也要将其科学需求加以重视，所以在整个工作中要注意科学性。安全保护工作的科学性主要表现在工作方法和工作目标上。在对自动控制系统进行安全性保护时，要注意其完整性。当前，由于对安全保护问题的研究还不充分，仅从表层上对安全保护程度进行评判，使得整个过程太过“片面性”，很难对其进行有效的激励。在对自动控制系统进行安全性保护时，要注意弹性原理。对自动控制的研究是一件非常繁琐和困难的工作，若采用的方式和方式太死板，没有弹性，就会造成建设工期和工期的延误；会对整体的申请工作造成负面的影响。在安保工作的过程中，要增强安保手段和手段的操作性，把柔性的原理融合到实际问题当中，才能保证安保工作的顺利进行；为电网的开发注入生机。

3. 电力调度自动化二次系统安全防护策略分析

3.1 二次系统安全防护体系

图 1 是二次配电装置的安全性保护的一般构架示意图。电网的安全保护应满足以下几个基本原理：电网的安全性水平愈高，对外部环境的影响就愈小。电源监测系统具有较高的安全性，表明其本身具有较高的安全性。对电能监测系统的保护水平还有待提高，在进行分级连接时应特别小心，不要将其与下级的联网联系起来。在安全区中，通过配置各种程度的安全装置，来确保每一个安全区域都有独立的作用，从而使整个系统受到足够的防护。

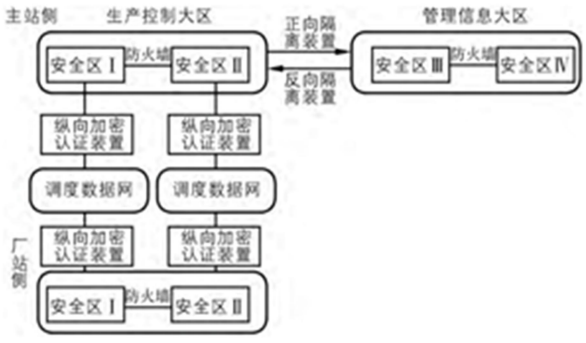

图 1　二次系统安全防护框架图

3.2 电力二次系统安全防护体系策略分析

3.2.1 安全分区

电网二次安全保护系统包括：安全区 I 是 SCADA（实时闭环控制）系统，安全区 II 是 DTS（调度员训练仿真）系统，安全区 III 是 OMS（调度管理）系统：各个安全区域要按照自己设置的准则执行。

3.2.2 横向隔离

安全区一和二安全区二是无法跨越等级连接到三号安全区的，所以要从安全区一号和二号传送消息到安全区三号，都要经过前向安全隔离设备，不能用电子邮件穿过隔离设备，在传送资料的时候，会清除掉一切恶意代码。为实现安全距离内各安全区域间的信息传递，必须使用安全隔离设备来实现信息的分离。

3.2.3 纵向加密

当前，国内许多地区都建立纵向加密设备、纵向加密设备管理系统、电力调度凭证系统和安全监测平台，其中纵向加密设备中的加密算法有对称加密算法、不对称加密算法、随机数产生算法等。该纵向密码设备的管理系统不但可以对整个网络的密码验证网关进行设定和查询，还可以对网络中的所有密码设备进行管理和初始化，还可以查询并设定整个网络的密码验证网关的工作方式、状态等，并且可以对整个网络中的每一个密码设备进行有效的监测和管理。

3.2.4 入侵检测

为确保电脑系统中的资料的安全，必须建立一套专用的电脑侵入侦测装置，使其可以及时侦测到电脑内之异常，并做出相应的处理。另外，它也能对电脑网络中的装置进行安全性检验，侦测到电脑网络中违背安全政策的装置，将电脑网络与 IDS 控制线及交换机连接起来，及时地侦测到侵入信号，并作出回应。

3.2.5 防火墙

电力核心区域 I 依托于 SCADA 技术，扮演着电力生产的核心角色，它能够对基础电力系统进行实时监控；而区域 II 则配备 DTS 技术。这两个安全区域若需交换数据，必须借助防火墙来确保信息安全。若黑客企图对计算机系统发起攻击，就必须突破防火墙的严密防线才能够使其破坏。

3.2.6 安全监测

为确保电力网路的稳固与安全，电力企业部署专门的监控体系，其中安全区域一内的监控体系与安全区域一级三相连，旨在监控能源管理系统的安全状态，而安全区域二的监控体系则与安全区域二及三相接，负责对电力计量系统的安全性能进行监控。

3.2.7 安全管理

安全管理工作对于确保网络安全至关重要，建立一套完整的安全管理体系，对电力行业的相关法律法规进行普及教育，有助于增强员工的防护意识。在遭受网络侵袭的情况下，除依赖尖端的网络技术外，还可以借助健全的网络安全规章来应对。因此，将安全管理融入电力系统的每一个安全环节，有助于提升系统的整体安全水平，确保信息资料的保密性。在电力企业的安全管理中，应着重强化对数据中心、员工队伍、硬件设施等方面的安全规章建设，遵循技术治理的方向，对网络安全技术进行持续的研究与分析，并与行业专家保持沟通，形成符合电力企业特点的安全管理方案，进而明确安全管理的具体界限。

4.电力调度自动化二次系统整改措施

4.1 整改方案

4.1.1 准备工作

审查各设备与板块的工作状态是否良好：核实相应连接链路；按照纵向加密设备的指示连接网络线缆：对设备进行资料备份；激活特定端口：创建请求数据文件：进行数字证书的颁发：载入文档：进行审核流程；完成颁发操作。

4.1.2 安装机器

利用纵向加密设备对内部网络的安全监控系统实施监管，将该设备部署在 I 区域的交换机处，随后安装管理软件，扩充设备节点，并对设备进行隧道配置。

4.1.3 安装加密装置

首先对加密设备进行设置，接着导入证书，并搭建隧道以及进行策略配置，在配置过程中需新增设备节点，并为其设定隧道的相关参数。依据数据传输业务的具体需求来构建隧道。证书的安装与导入需遵循调度证书服务系统的根证书以及本设备的证书规范。

4.2 纵向加密管理与纵向加密配置

在核心站点一侧装备线性加密模块系统，同时部署平面控制单元，执行网络设置、路径规划、证书引入和隧道搭建等操作，依托层级指挥系统在核心站点构建线性加密通道。线性加密模块的配置规范详见表 1 所列。

表 1　纵向加密装置隧道配置要求

加密设备	是否导入证书文件	是否建立装置隧道
220KV 省调接入网纵向加密设备	是	是
220KV 地调接入网纵向加密设备	是	是
110KV 省调接入网纵向加密设备	是	是

4.3 导入证书、建立隧道

在启动隧道搭建流程之前，需在核心站点控制单元上新增节点信息，并对该节点进行隧道相关参数的设定。依据数据传输业务的具体需求，为核心站点一侧的线性加密模块分别构建加密通道，并设定相应的策略。证书的引入必须恪守相关准则，本地基础信息的配置也应严格遵守规定，操作人员登录系统后应立即更改账户名和登录密码。

4.4 人员控制

网络空间的安全受到多方面的威胁，其中恶意侵袭构成严重的安全风险，犯罪分子能够在不干扰网络常规运作的前提下窃取关键数据。此外，操作人员的疏忽同样会对网络的稳定安全构成挑战，系统内的大量缺陷往往成为黑客锁定的攻击目标。维护网络安全需要严格的管理制度，公众的安全防范意识亟需提升，在处理繁杂的网络调度数据时尤其不能有丝毫懈怠。管理不善、密码使用不规范、账户随意借给他人、信息资源共享不当等问题，都可能埋下重大安全风险。鉴于此，强化对员工的监管刻不容缓。具体的改进措施包括：强化对内部员工的管控，严格管理进出机房的人员，以及加强日常运行和系统登录的管理工作。

结束语

面对电力调度系统运维日益繁杂的态势，自动化的二次系统在安全防护及维护方面发挥着至关重要的支撑作用。深入剖析并归纳自动化二次系统的关键要素，是提升电力调度供电效率、实现电能资源节约的关键环节。为进一步提升自动化二次系统的安全级别，增强技术专精特新，满足用户多元服务需求，我们必须强化对自动化二次系统的管控，并升级安全防护策略。

[参考文献]

[1]牛雪朋，李瑞山，包芳，李永照，闫文敬.电力二次系统中的网络安全隔离技术分析[J].电子技术，2023，52（11）：351-353.

[2]李伟.光伏电站电力二次系统网络安全风险及防护措施[J].电子元器件与信息技术，2021，5（12）：242-243.

[3]周鹏林.电力调度数据网二次安全防护系统新型运维[J].网络安全技术与应用，2021，（11）：122-123.

[4]丁立顺.电力调度自动化二次系统安全防护研究[J].技术与市场，2021，28（10）：115-116.

[5]郭锦煌.电力调度自动化二次系统安全防护分析[J].光源与照明，2021，（04）：127-128.