Universe Scientific Publishing

Building Developments 建筑发展

第 1 卷 ♦ 第 3 期 ♦ 版本 1.0 ♦ 2017 年 3 月

文章类型：论文 | 刊号 (ISSN): 2425-0082

电力调度自动化系统运行的二次安全防护策略及其意义

熊熠

国网九江供电公司

DOI: 1.18686/bd.v1i3.164

出版日期：2017 年 3 月 1 日

摘要：电力二次系统是由电力监控系统、电力通信及数据网络等组成的复杂系统，因此必须加强电力二次系统的安全防护，保障电力监控系统和电力调度数据网络的安全。随着科技信息技术的快速发展，使得网络系统越来越不安全，为了保障电力调度自动化系统的安全运行，需要加强对其进行二次安全防护，从而保障电力系统的安全运行。本文阐述了电力调度自动化系统运行的二次安全区划分及其影响因素，对电力调度自动化系统运行的二次安全防护策略及其意义进行了论述分析。

关键词：电力调度；自动化系统运行；二次安全；影响因素；安全防护；策略；意义

电力调度自动化系统运行的安全性直接关系到电力企业的供电的安全性以及可靠性，为了确保企业、个人的正常用电需求，应加强电力调度自动化系统的二次安全防护。电力调度自动化系统二次安全防护需要确立“安全分区、网络专用以及横向隔离”的策略，全面落实以及实现生产控制区域与管理信息区域的有效隔离。同时需要加强安全防护设备的安装及其防护，从而确保电力调度自动化系统的可靠运行以及网络数据的安全性。

1 电力调度自动化系统运行的二次安全区划分及其影响因素

1.1 电力调度自动化系统运的二次安全区划分

通常将电力调度自动化系统运行的二次安全区划分为：实时控制区（Ⅰ区）、非控制生产区（Ⅱ区）、生产管理区（Ⅲ区）以及管理信息区（Ⅳ区）。(1）实时控制区。其是电力系统最为重要的实时在线运行，并且是调度数据网络一级专用通道，对于实时要求的性能较高。(2）非控制生产区。其实现功能是电力系统运行的必要环节，非控制生产区不具备控制功能，只是使用调度数据网络，实现在线运行，与实时控制区中的功能模块有着紧密联系。该区域包括自动化系统、电力交易系统以及 DTS 系统等。(3）生产管理区。该区只是实现电力生产的管理功能，也不具备控制功能，不存在在线运行，与管理信息区自动化系统有着较为密切的关系。其主要包括气象信息、DMIS 系统以及雷电监测系统等。(4）管理信息区。其主要是实现电力信息管理以及办公自动化功能，业务系统的访问界面主要为桌面终端，该区域则主要包括 OA 系统、客户服务以及管理信息系统等，并且该区域的外部通信边界则为互联网，各个区域之间是横向联系的，可实现信息共享。

1.2 影响因素

笔者认为各个区域的影响因素主要：(1）设备因素。主要表现在原有的二次安全防护设备相对较为落后，缺乏先进的硬件设备；加上在安全防护策略的制定上也比较宽松，没有严格的要求，使得每一个区域之间的联系较少。(2）人为因素。电力调度自动化系统工作人员态度较为松散，没缺乏科学合理的管理理念，加上业务素质不高，影响了二次安全防护。

2 电力调度自动化系统运行的二次安全防护策略

2.1 建立健全电力调度自动化系统二次安全防护的相关管理规定

通常电力调度系统运行的主要安全隐患并不是系统自身，而是与其相连的其他网络，因此需要建立一个科学、合理的管理模式，从而有效抵御黑客以及病毒的攻击破坏，最终保护电力实时闭环监控系统，阻止有网络病毒攻击所带来的系统崩溃现象，保障电力系统的安全稳定运行。首先需要建立完善的安全分级负责制，坚持“谁主管，谁负责”的原则，建立完善的二次系统安全防护制度，根据要求设置电力监控系统，同时明确各个相关人员的职责。同时需要加强日常维护以及管理，定期对安全防护系统进行巡查，一旦发现有问题，立即采取相关解决措施。若不在自己管辖范围之内，应将安全隐患向上一级相关部门反映，同时做好详细的记录。

2.2 进行逻辑横向隔离及安全纵向认证

(1）实时控制区是电力系统安全防护的重点，其可直接实现对一次系统运行的监控，非控制生产区有调度员模拟以及仿真 DTS 系统。为此，实时控制区域非控制生产区系统之间则采用防火墙，具有较好的防护功能。若入侵者想进入到目标计算机，则必须穿越防火墙。该防火墙性能符合实时控制区、非控制生产区之间的性能。实时控制区、非控制生产区与管

理信息区不得直接联系，同时实时控制区、非控制生产区域生产管理区应采用经过有关部门认定以及审核的专用安全隔离装置，分为正向型以及反向型。另外从实时控制区、非控制生产区向安全隔离装置单向传输信息。对于非控制生产区的电量采集计量系统以及生产管理区采用实时隔离网关，同时隔离网管必须符合相关规定要求。（2）加强安全纵向认证。电力调度自动化系统二次安全防护体系中的电力调度数据网是其基础，承载着电力实时控制已经在线生产交易的重要任务。调度数据网的主要目的是实现调度中心之间以及调度中心与厂站之间的调度。采用 SDH/PDH 的相关技术，在物理层面上实现与电力企业其他数据网与公共信息网络之间的隔离。

2.3 强化检测系统的安全

在加强电力调度自动化系统二次安全防护过程中，为了保障计算机系统的安全，需要选择先进的入侵检测系统，该检测系统的设计及其配置需要及时发现并报告系统中异常现象，同时也能够检测计算机网络中违反安全策略的行为，如果发现用户的违规行为或者非法用户的违规行为，则立即进行拦截。此外，该检测系统应用 IDS 系统，与非控制生产区相连接。其功能应用有提供记录流的信息源，分析引擎的检测结果等，进而采取有效防治措施，保障电力系统的安全运行。

2.4 其他安全防护措施。

在电力调度自动化系统的二次安全防护工作完成之后，通常都能够有效防治病毒或者黑客侵入，此外还需要做好其他相应控制。（1）需要严格加强生产控制区的 PC 机的网络安全管理，并且在接入之前应做好防病毒的相关措施，需要将其列入到日常运行管理中，同时做好相关记录。（2）电力调度自动化系统在二次安全防护过程中，生产控制区需要禁止其与对外互联网相联。

3 电力调度自动化系统运行安全防护的意义

电力调度自动化系统在整个电力系统中，能提供电网运行的数据和实现网络监控，得到监控数据并进行处理，帮助电力企业工作人员了解电力系统的运行情况，是电力系统安全运行的重要内容。当前应用先进的信息技术和网络技术不断改善电力调度系统，但是在安全方面依然存在诸多。随着电网不断扩大发展，其在管理技术和要求上需要不断更新，需要提高电力系统的安全防护。需要要强化调度中心和监控中心，提高电力中心工作人员的安全意识，工作人员提高自身素质，熟悉专业技能，提升安全防范意识。同时在管理方面要科学合理满足时代发展的需求，保证电网系统的安全运行。并且电力系统和人们的利益密不可分，如果没有较好的维护好电力系统的安全性，那么就很难确保人们在用电过程中的安全性。当前电力系统主要有 EMS、DTS、PAS、AGC、AVC 等，电力系统的二次防护就是对这些系统进行有效的把控。

4 结束语

随着经济的发展及工业化程度的提高，使得工业及民用的电量需求日益增加，同时对电力系统的安全要求更高。并且电力企业作为国民经济的组成部分，使得电力系统业务也不断增加，如 AVG 系统，PAS 系统，电力调度数据网等对电力调度系统的安全提出了更高的要求。因此必须加强电网调度系统的二次安全防护。

参考文献

[1] 李延瑾等．电网调度系统二次安全防护的策略分析 [J] 现代企业教育，2012(11).
[2] 周瑾．论电网调度自动化二次系统的安全防护 [J]. 北京电力高等专科学校学报，2011(11).
[3] 李文静．电力调度自动化二次系统安全防护探析 [J]. 中国科技博览，2015(21).