火电厂电力监控系统安全防御体系构建路径研究

刘 敏，郑宝俊

华能兰州范坪热电有限公司 甘肃兰州

【摘要】电力监控以通信和数据网络为支撑，针对火电厂的电力生产以及供应过程进行监视和控制。近年来，火电厂自动化、数字化和智能化程度越来越高，其电力监控系统信息交互也越来越复杂。火电厂电力监控系统涵盖全厂日常生产以及管理等多项业务，通过对不同区域的专项管控，从而保障火电厂日常发电工作正常运转。在工控安全形势下，火电厂企业应当通过构建完善的安全防御体系，从而有效保障电力监控系统能够安全稳定运行。对此，本文阐述火电厂电力监控系统安全防护范围及其防护特点，针对其所存在的安全风险隐患进行分析，提出相应的安全防御体系构建路径。

【关键词】火电厂；电力监控系统；安全防御体系

【收稿日期】2022 年 12 月 26 日 【出刊日期】2023 年 1 月 21 日 【DOI】10.12208/j.aics.20230004

Research on construction path of safety defense system of power monitoring system in thermal power plant

Min Liu, Baojun Zheng

Huaneng Lanzhou Fanping Thermoelectric Co., LTD. Lanzhou, Gansu

【**Abstract**】Power monitoring is supported by communication and data networks for the monitoring and control of power production and supply processes in thermal power plants. In recent years, thermal power plants have become increasingly automated, digital and intelligent, and their power monitoring systems have become increasingly complex in terms of information interaction. The thermal power plant power monitoring system covers a number of operations such as daily production and management of the whole site, and through special control of different areas, thus ensuring the normal operation of the thermal power plant's daily power generation work. In the form of industrial control security, Thermal power plant enterprises should build a perfect security defence system so as to effectively guarantee that the power monitoring system can operate safely and stably. In this regard, this paper explains the scope of safety protection and its protection characteristics of the power monitoring system in thermal power plants, analyses the safety risks and hazards that exist in it, and proposes a corresponding path for the construction of a safety defence system.

【**Keywords**】Thermal power plant; Power monitoring system; Security defense system

引言

电力系统作为我国基础设施之一，其安全稳定运行关系着国家的经济发展，同时也维系着国家的安全。在市场化转型工程中，越来越多的新兴技术被应用于电力行业日常生产运行中，不仅加大管理技术人员日常工作难度，其工作量同时也在与日俱增。近年来，网络安全事故频发，网络安全问题也越来越突出，电力监控系统安全防御体系构建成为全球研究热点。对此，笔者将从安全防御区域划分、安全审计平台建设以及主机设备安全管理这三个方面着手分析，不断增强火电厂电力监控系统安全防御能力，从而保障火电厂安全生产运行。

1 火电厂电力监控系统安全防御范围及其防护特点

1.1 防御范围

火电厂电力监控系统安全防御范围主要包括主

作者简介：刘敏（1985-）女，汉族，硕士，工程师，华能兰州范坪热电有限公司；郑宝俊（1988-）男，汉族，工程师，单华能兰州热电有限公司

控系统、电力生产辅控系统、独立检测控制系统、涉网侧系统及设备等。根据火电厂的安全防御划分范围，其电力监控系统主要将电力生产以及业务管理这两个系统划分为生产控制以及管理信息这两个区域。

1.2 防御特点

火电厂所涉及的工艺流程十分复杂。在发电过程中，大型分散控制系统控制燃烧、汽水以及电气三大系统的运转。生产环节不同，三大系统内部的工作系统又被分为输煤、锅炉燃烧以及除尘等系统，不同的生产环节其控制系统也是不同的。在电力生产过程中，各项系统的运行还需要借助管理信息系统以及厂级监控信息系统等协同完成，从而优化火电厂电力实施生产过程[1]。

在上述控制系统中，大型分散控制系统、管理信息系统以及厂级监控信息系统所用协议、面向的对象以及侧重点皆不相同。因而在数字化进程中，不同系统的更新与优化在给火电厂电力生产带来更多便捷的同时，也会让系统整体变得更加复杂，火电厂的管理同时也会产生许多问题。

2 火电厂电力监控系统安全风险分析

2.1 边界防护薄弱

火电厂在电力生产过程中，通常是需要借助管理系统完成各项工作流程的协调与控制，这也使火电厂电力生产系统网络与管理信息系统网络相互掺杂。控制生产的大型分散控制系统受到外部信息网络干扰，对其安全运行造成威胁，导致火电厂控制系统内部被入侵。2015 年，黑客通过恶意软件向电力系统内网进行渗透，利用系统漏洞获取电力监控系统控制权限并在远程操作下对其发送相关跳闸操作命令，导致乌克兰至少三个区域以内的电力系统遭受攻击，部分变电站的控制系统以及发电设备产生故障，造成当地大面积的停电。对此，火电厂必须重视电力生产系统网络边界的划分，保证电力系统安全稳定运行[2]。

2.2 网络监控能力不高

云计算、大数据以及物联网等新兴技术在电力监控系统中得到广泛应用的同时，也面临着新的网络安全风险。火电厂电力监控系统简单，在相关机组投入到生产运营当中后，相关人员很少对其进行更新并及时修补系统漏洞，火电厂电力监控系统识别网络入侵、病毒等异常现象的技术手段十分薄弱，一旦发现问题，很难对这些问题进行溯源和处理。大多数大面积停电事件，大多是因为外力或者是电力设备故障所造成的，火电厂相关技术管理人员必须重视电力监控系统的更新与升级，加强电力监控系统的网络监控能力，不断提升电力监控系统安全防御等级。

2.3 终端存在安全风险

火电厂电力监控系统专业性非常强，通常需要由设备厂商的专业维修人员进行运维检修，对于运维检修工作这点，大多数火电厂并未有合适的监管手段，如若外部设备厂家以此控制系统运维人员的电脑中，那么电力监控系统工作主机容易出现被入侵或者是病毒感染等情况。此外，以外火电厂运用的电力控制系统，大多是西门子、ABB 或者是艾默生这类紧扣控制系统，这些系统是否存在后门或者是漏洞这一点尚不明晰；传统工业控制系统终端安全防御能力较为薄弱，部分控制系统终端本身就存在漏洞，这些漏洞一旦被外界利用，容易产生巨大的生产安全事故[3]。

3 火电厂电力监控系统安全防御体系构建路径

3.1 合理划分电力监控系统安全防御区域

火电厂电力生产控制区域可以被分为控制区与非控制区，控制区是火电厂电力生产的主要环节，能够实现对电力生产的实时监控，这是电力监控系统安全防御的核心部分。另外，使用电力调度数据的专用通道进行数据传输的业务系统也属于控制区域内；非控制区作为火电厂电力生产的必要环节，并不具备控制功能，与控制区域内的业务系统相联系。因此，电力调度数据网的非实时子网进行数据传输的业务系统，则是需要按照电网要求将其划分至独立的非控制区域内。在不影响电力生产控制区域安全的前提下，管理信息区域则可以根据不同单位的具体工作情况来划分安全区域，其中就包括企业内网、互联网等需要利用网络运行所使用的信息系统。

电力生产控制大区内的控制区与非控制区之间应当采用电力专用正向隔离装置，这种装置基本只允许纯数据类的信息进行单向安全传递。在生产以及业务大区之间部署单向安全隔离装置。虽然这种装置从形式上来看更为接近于物理隔离，但是这种

装置能够对这两个区域数据传输产生有效的管控。此外，生产控制大区内的业务系统应当采用 VLAN 以及访问控制等安全防御措施，以此来限制各个系统直接产生信息互通。除此之外，电力监控系统在控制电力生产大区内的业务系统时，还应向当地的环保部门以及网络安全部门进行数据传输时，应当遵守按照安全防护规定执行[4]。

火电厂电力监控系统机房应当设有防水、火、静电以及雷击等措施，同时配置电子门禁等物理访问权限，同时还要开启电磁屏蔽仪从而避免机房内的各类设备受到影响。核心生产领域还应装有 24h 的连续监控系统，便于监控管理人员对监控内容的查阅。

3.2 基于工控协议部署工控安全审计平台

基于工控协议部署工控安全审计平台，一旦监控系统自身出现故障，那么管理技术人员可以通过工控安全审计平台及时了解到系统故障信息以及明确位置等，确保在尽快时间内完成对电力监控系统故障的修复，避免电力监控系统造成其内部数据丢失或者是损毁，以此保障火电厂电力监控系统网络安全问题。针对主机以及网络层面，管理技术人员还应通过合理的安全审计，使每日的网络异常活动情况能够得到记录，这样在电力监控系统出现故障时，管理技术人员能够及时对故障情况进行追溯，从而最大限度的缩短系统故障修复时间。针对设备访问权限，管理技术人员应严格制定相应的审查管理制度，设置合理的应用流程，从而有效保障电力监控系统主机设备安全。在必要条件下，通过第三方接入的网络以及设备需要通过严格审计，这样才能让整体系统拥有良好的网络运行环境，这也让电力监控系统在火电厂的日常生产运行中得以充分发挥其优势。

火电厂电力监控的生产控制大区与管理信息大区边界处应当部署一套网络入侵检测机制，分析火电厂潜在威胁并对其加以安全审计。在控制区以及非控制区边界及各个子系统之间也应当基于工控协议部署安全防火墙，在针对特有私有协议时应当进行深度解析，从而不断完善火电厂电力监控安全防御策略，针对跨越边界的流量进行严格管控，将威胁火电厂电力监控系统安全的因素遏制在小范围内，从而有效避免不良因素产生跨区域的传播。针对生产控制大区内的各类关键生产系统，技术管理人员应当部署一套工业网络审计设备，这样能够及时发现隐藏在系统网络流量中所存在的异常数据。此外，针对流量入侵检测措施，火电厂电力监控技术管理人员可以在控制区域内的关键节点处部署工控安全审计平台，对通讯流量语义级别进行深度解析，从而实现对区域内合法流量的异常行为进行检测[5]。

3.3 加强电力监控系统主机设备安全管理

火电厂电力监控系统管理人员针对 USB 接口、设备滥用以及系统漏洞等主机设备安全管理问题时，应当采取主机安全加固手段。对电力监控系统主机及服务器中固化可信的进程、网络以及外设等多类对象，这样能够防止主机内文件被篡改。针对相应操作系统安全进行加固，从而提高整体安全防护水平。对此，针对电力监控系统主机设备安全防御，管理技术人员应当做到以下几点。

首先，加强计算机主机设备的安全管理。电力监控系统主机设备应当被禁止采用双网卡的方式去实现跨区域联系，USB 等物理端口以及物象装置等网络接口也应当是禁止使用的，这样能够有效保证主机安全；其次，针对计算机操作系统方面的安全防御工作。管理技术人员一方面要加强操作系统登录管理，限制连续失败登录次数，定期对登录密码进行修改，对默认账户能够访问的权限进行限制，管理技术人员自身在设置登录账号时也应当尽量避免使用弱口令等；另一方面，针对使用人员进行严格管理，在外来人员使用电力监控系统时，必须经过书面申请并得以审批后才能够使用，履行监控系统审查或者是密码管理人员在调离岗位后，新的密码则需要由新接手工作的人员立即更改，抑或者是对原用户名进行删除；最后，对于第三方设备的管理。管理技术人员在使用移动存储设备时，必须要对内部所存在的病毒进行检查，对主机内的各项数据文件等进行备份并妥善保管备份存储的数据，定期对数据文件备份情况进行检查，以此确保数据文件的有效性。

4 结语

近年来，我国在信息安全以及网络安全方面给予极大的重视，针对国内外发电厂电力监控系统事故，我们也应进一步提高对新形势的认识，把握工

作关键方法，努力开创电力网络安全信息化工作新局面。

参考文献

[1] 马铭宏，王子豪，刘悦. 火电厂电力监控系统安全防护应用[J]. 东北电力技术, 2022(003):043.

[2] 郭宾，陈超，文昱博,等. 浅谈电力监控系统安全风险及其安全防护措施[J]. 工业信息安全, 2022(006):000.

[3] 贾爱静. 基于 CAN 通信技术的火电厂电气监控系统设计与研究[J]. 通信电源技术, 2022, 39(6):3.

[4] 田嘉. 火电厂电力监控系统安全防护体系的建设与研究[J]. 网络安全技术与应用, 2021(3):2.

[5] 刘健. 电力设备火力发电厂电力监控系统安全防护运营管控实践[J]. 轻松学电脑, 2021, 000(005):P.1-2.