2021 年 3 卷 1 期 ISSN: 2661-3476(Print); 2661-3484(Online)

火电机组网络信息安全隔离技术研究与应用

郭瀚清

安徽淮南平圩发电有限责任公司 通信工程 安徽 淮南 232000

【摘要】火电机组承担着国家电力供应重要任务，在电力企业蓬勃发展的今天，必须对网络信息安全产生重视，一旦出现数据丢失的问题，会对电力企业产生无法想象的负面影响。因此，本文就针对火电机组网络信息安全隔离技术进行深层次的研究，明确安全隔离技术的作用，让其能够在火电机组网络中得到真正应用，并且结合实际案例，进一步分析判断火电机组网络信息实际效果，确保信息的安全性，让网络信息安全得到真正的保障。

【关键词】火电机组；网络信息；安全隔离；技术研究

引言

在计算机技术飞速发展的今天，国际互联网安全态势逐渐严峻，一些攻击手段、攻击技术甚至成为了不正当的竞争手段，攻击国家网络和对手企业，信息安全存在着极大的威胁。对于火电厂而言，其承担着至关重要的供电任务，在强化自身运营能力的同时，也要保证信息安全性，抵御互联网威胁。借助信息安全隔离技术，编制相应的信息技术方案，可以更好地完成网络安全隔离建设，确保火电机组的正常运行。

1 火电机组网络信息发展现状问题

在一个电厂中涵盖的区域较多，区域之间利用广域网、互联网进行沟通交流，为了保证信息数据的安全性，在广域网和互联网便捷都设置了防火墙，以此保证安全。但在实际调查过程中发现，很多区域之间的安全防护程度较低，在非重点区域中，仅针对交换机进行了 VLAN 隔离，而且作为核心服务器的前端区域并没有防火墙隔离，也没有对访问进行严格的控制，给核心区域带来了安全威胁。终端安全和终端防病毒上也存在极大的问题，一些软件已经过期，无法完全发挥作用。在入侵检测和统一监测上，基本维持在低于攻击、防范入侵基本效果上，面对核心应用、内部访问等行为缺少必要、有效的安全检测。整个网络缺少整体、精细的监控设备，无法纳入整体的审计监测平台中。在很多发电厂中信息系统的脆弱性相对较强，WEB 网站、OA 等应用系统都面临着安全风险，需要及时地发现安全漏洞、消除隐患。另外 IT 系统运维管理层面上也存在一些问题，导致安全运维管理无法维持电力企业的正常运行。火电机组作为电力企业内部的重点区域，上述问题自然存在，必须得到系统的处理。

2 火电机组网络信息安全重要性

对于任何一个电力机组而言，信息的安全性都非常重要，如果信息出现问题，那么会对整个企业产生负面影响。安全隔离技术是保证信息安全的重要性措施，必须得到有关人员的重视，尤其是在网络技术飞速发展的今天，电力企业也进入了全新的发展阶段，但需要面对的问题也在逐渐增加。火电机组作为电力企业中最为关键的组成部分，想要对其进行信息安全保护面临着极大的风险，具体表现在以下几点：第一，信息数据量较大，结构复杂，而且火电机组承担着企业的主力业务，一旦信息安全出现问题，不仅会对供电产生影响，还会威胁到社会的安全。第二，缺少必要的综合性防护系统，当前黑客数量较多，一旦入侵就会威胁到信息安全，还会对电力调度产生影。第三，网络问题动态化发展，信息安全技术也要随之变化，但电力企业有关人员的认识度较低，导致信息安全技术落后。第四，电力企业缺少对信息安全保护的重视程度，一般情况下，业务机组信息技术局都会被存储在数据库中，但并非绝对安全，需要采取不同强度的安全保护措施，以此有效避免漏洞、隐患。

虽然很多电力企业已经采取了相应的防护措施，但网络安全信息技术依然没有形成完整的体系，很多薄弱的环节一旦受到冲击就会出现问题，导致各方面出现威胁。另外还要考虑到运行成本和运行性能等方面的问题，因此数据安全性必须得到保证。

3 火电机组网络信息安全隔离技术总体方案

以某发电厂为例，针对该发电厂内的胡电机组展开了系统的网络安全隔离技术方案，具体的技术方案如下：

第一，在内、外网展开安全区域划分，尤其是外联区、DMZ 区域以及数据交换区等安全防护等级较高的区域设置防火墙，严格控制访问等级，阻止非授权访问。第二，

在内部网络中不止网络入侵检测设备，借助 IDS 动态检测功能，对访问、通信、应用等内容进行深度检测，全面识别内部网络用户和外部攻击者，防止出现非授权的攻击行为和滥用行为。第三，在外部网络部署 IPS，同时在服务区前布置 WEB 来抵御互联网的攻击行为、保护重要应用系统。另外，借助上网行为管理设备对网络行为进行分析，及时发现敏感和违规行为。第四，借助 VPN 设备进行远程接入，并且在内网增加堡垒机，以此实现远程协助，更加有效地控制内部网络系统运行维护。

在上述安全隔离技术的保护下，账户、信息的安全性都得到了极大的保证。在总体隔离技术的基础上，还需要对一些细节进行进一步明确，以此确保安全性得到进一步提高，并且落实相应的应用不符。

4 火电机组网络信息安全隔离技术具体规划

4.1 内网建设

以内网信息安全隔离技术为例，将内网分成核心区、服务器区、终端区、广域网接入区、运维管理区等，进而按照相应的网络策略进行隔离防护。首先利用内网服务器汇聚交换机，将信息内网服务器单独成区，针对重点保护地区服务器去和核心交换机之间布置两台防火墙设备，以此实现双机双链路备份，保证业务系统得到稳定运行。另外，信息内网部署 IDS 设备，监控网络、系统运行情况，及时发现可能存在的攻击企图、攻击行为以及攻击结果，尽可能确保网络系统资源的机密性、完整性、可用性。在此基础上，根据火电机组内部实际运行需要，购置交换机，配合虚拟化技术，打造出良性接入方案。为了保证原有电网终端可以全部放置在内网中使用，从利旧原则、利旧方法出发，完成具体的安全防护建设。

4.2 信息外网建设

在外部网络建设上利用防火墙设备保证便捷安全，将服务器放置在 DMZ 区域，并且联入 Internet，针对不同的服务器采用不同的防火墙进行保护，如，WEB 服务器采用 WAF 防火墙。在此基础上，结合具体的移动接入需求，选择具体网关，同样利用利旧方式部署原有设备。一般情况下，火电机组有自己的互联网出口，但很少会布置管理设备，在此基础上，对其进行改造，增加网络行为管理设备，以此为后续的审计管理工作提供参考。在无线建设方案下，成本得到进一步降低，来 AC 控制器可以在核心交换机旁边，以此降低成本。将传统三层架构结构转变为两层架构，在核心层中利用高可靠性框式交换机，以此有效简化管理、增强网络，在横向虚拟化技术的辅助下，实现了统一管理。信息外网相对而言，安全性较低，采用 PC 机可以有效避免问题。

5 火电机组网络信息安全隔离技术具体落实

在完整整体和分别建设后，还需要对应用系统进行部署，确保信息内网安全，火电机组网络信息安全隔离技术需要对整个区域进行划分，然后按照相应的管理规范进行管理。从实际效果来看，改造前该电厂安全管理水平较弱，改造后这一问题得到了根本上的解决，采用 C/S 架构，能够更好地对信息进行管理。在完成相应的设备采购后，实现了相应的安全接入、身份认证、防内网外联、桌面管理等工作。考虑前者的网络安全问题，需要对病毒库进行更新，并且扩大病毒系统覆盖范围。在此基础上，打造出了统一的监测、审计平台，让内网信息系统运行使用得到监控，所有访问的行为和内容都会进行全面审计，以此在发现问题的第一时间进行有效溯源，从根本上保证信息安全。除了上述几个方面之外，想要保证火电机组网络信息运行的安全可靠性，还要对网络运行过程中存在的安全风险威胁提高重视。消除火电机组网络信息运行过程中存在的安全威胁，解决其应用问题，能够让通信网络中的重要因素得到有效管理。常见的对策包括：加强对线路、设备的维护保养工作以及针对特殊风险进行预防等，在此基础上，配合其他运行安全保证对策，可以有效解决通信网络运行中存在的问题，最大程度避免通信网络崩溃。以雷击隐患的规避为例，可以在火电机组网络信息中加入防雷接地设备，将雷击隐患降到最低。在这个过程中，还可以在一些固定位置设置屏蔽层，避免模块运行过程中出现相互打扰的情况。与此同时，要保证这些设备、设置本身的功能和绝缘性不会出现退化，定期对设备、线路进行维护保养，如此可以进一步降低火电机组网络信息出现故障的概率，网络运行的安全性就会得到提高。

6 总结

综上所述，火电机组网络信息安全隔离技术在实际应用过程中效果较优，可以极大程度地保证明暗信息安全性，而且经济性、实用性、先进性较强，也不会对信息化办公效率产生负面影响，让网络安全得到了保证。不仅如此，还可以建设形成统一的平台，具备远程检测、实时监测的效果功能，有效保证了电场网络隔离效果。在电力信息系统建设过程中网络安全至关重要，必须得到良好的技术进行保护，安全隔离技术是最为彻底、安全的防范技术，可以有效降低信息交换中的安全隐患，值得大范围推广使用。

【参考文献】

[1] 胡传力 , 李卓群 . 基于信息安全的网络隔离技术研究与应用 [J]. 网络安全技术与应用 ,2019,219(03):82-83.
[2] 王强 . 关于信息安全的网络隔离技术研究及其应用 [J]. 电子测试 ,2019(16):66-67.
[3] 孙一帆 , 范洵 , 符凌翔等 . 电力信息网络安全技术研究 [J]. 数字化用户 ,2019,025(028):41.