

# 电力系统配网自动化通信的网络安全管理问题

魏云

国能中卫热电有限公司

**摘要:**在当前新的历史发展时期,科学技术的全面发展,为电力系统配网的自动化和智能化发展起到了积极的作用,大量的新型科学技术以及先进设备的运用,为配电系统综合性能的提升创造了良好的条件。通信网络属于配电系统中的一个重要部分,其主要作用就是对各项实践工作进行良好的协调。当下,尽管信息通信能够为电力系统配电提供更多的便利,但是就其实践运用情况来说还存在诸多的问题,诸如:网络通信安全问题较为严重,大部分电力企业通信网络的使用中都会遇到黑客的袭击、信息的泄漏等诸多问题,对于电力企业的发展造成了诸多的阻碍。对于上述问题要想进行有效解决,还需要利用各种有效的方法来增强网络安全性,专业工作人员也需要适当的增强通信系统安全管理工作力度。

**关键词:**电力系统;配网自动化通信;网络安全管理

【DOI】10.12252/j.issn.2096-6261.2022.08.227

## 引言

就电力系统实际情况来说,电力通信系统的创建效果往往都与整个系统的综合性能存在密切的关联。近些年,我国电力市场的信息化发展取得了显著的成绩,电力通信系统的自动化以及智能化水平也随之不断提高。但是因为电力系统在运行的过程中表现出了较强的开放性,并且远程接入实际操作也相对十分简单,这样就导致配网自动化通信网络运行存在诸多的隐形风险。为了切实地规避各类危险问题的发生,还需要我们积极的落实管理工作,制定完善的管理方案。

## 一、电力系统配网自动化技术简述

通常来说,在电力系统之中,配网管理系统所具有的主要作用就是可以对配电网络的运行进行全面管理。当前,就配网自动化网络体系实际情况来看,其不但与先进的通信技术进行了融合,并且也与自动化技术以及网络技术完成了切实地整合。从而使得配电网的整个系统结构以及在线数据的合理性和完整性得到了良好的保障,并且也形成了较为完善的电力配网自动化系统。在电力系统运行的过程中,切实地将所涉及的各方面信息数据进行统一的收集和分析,结合所掌握的信息来完成电网资源的合理分配,可以有效的对网络负荷进行调控,对网络环境加以完善,对于整个电网的运行安全和运行效率也能够加以根本保障。

## 二、配电网自动化技术及通信系统的建设要求

### (一)通信系统的可靠性要求

配电网控制中心与用户在整个配电网自动化通信系统管理中具有十分重要的作用。当代配网自动化系统要想加以有效的运行还需要利用到多种专业技术和设备,要想保证将各类设备的实践作用充分发挥出来,还需要创建满足实际需要的通信系统。

### (二)通信系统的经济性要求

要想有效的提升民众的生活水平,那么还需要对配

网系统的大范围推广和运用给予更多的关注。在进行通信系统建设工作的过程中,如果需要投入大量的资金,那么必然会对系统的推广造成一定的限制。所以在对通信系统实施投资的时候,还需要从整体的角度入手,切实地实施经济控制,逐步提升资金利用效率。

### (三)通信系统的可拓展性要求

科学发展使得各个行业都随之快速发展壮大,以往老旧的通信网络系统已经无法再满足电力配电网系统运行的实际需要了,所以为了进一步的推动社会的发展,我们还需要对整个系统实施全面的研究和创新,尤其是配电网自动化系统需要给予更多的关注。在实施设计工作的过程中,需要结合通信系统的各方面实际情况,从多个不同的角度入手来对其进行优化升级,这样才可以将其实践作用充分的发挥出来。

### (四)廉价的运行维护成本

就当下实际情况来看,数据在传输的过程中,配电网信息系统所运用到的载体主要是光纤和电磁波,所选方式方法的不同在实践中因为遭到技术因素的影响,使得通信技术的使用效果也会遭到诸多的限制,并且使用时间也相对较短。为了从根本上将通信技术的适用性加以提升,还需要对各项技术的运行效果给予根本保障,尽可能的控制运行维护成本。

## 三、电力系统网络安全管理的重要性

配电网自动化系统属于信息管理系统的一种,其具有较强的综合性特征,其也牵涉到多方面的内容,诸如:现代设备、计算机技术、数据传输技术、控制系统等等。配电网自动化系统的运用能够对整个电网的运行情况进行全面的监督,并且可以依据规定要求来完成对其他系统的信息数据的交互。配电网自动化通信系统的主要作用就是完成数据的传递,其实质是借助遥感、遥测技术来进行各项数据的收集和整理工作,随后将各项数据信息依据设计的程序输送给各个分支系统,利用遥控命令

信息对故障问题进行定位和隔离，并且也可以对系统的运行状态加以切实地控制。数据表现出了上行链路高、下行链路低的特征，并且主站终端通常都被设置在地级以上城市地区。电力公司在进行电力系统建设工作的过程中，对于信息传递的效果和安全务必要加以侧重关注。因为电力系统运行过程中往往会遭到外界多方面因素的影响，所以网络安全问题得到了人们的广泛关注。要想从根本上对电力行业的发展给予保障，推动电力行业的稳步健康发展，还需要我们增强对电力系统网络安全运行的根本保障力度。在当前信息化的时代中，电力信息系统得到了全面的优化和完善，很多的信息都会对电力系统造成一定的影响，这个时候最为关键的一项工作就是加强对电力信息网络安全保障，从多个不同的角度入手完成对安全技术以及防护技术的升级。电力系统不但需要切实地对各类软硬件设备实施更新和升级，并且也可以聘任一些高水平的专业技术人员对整个系统的数据安全加以保障。电力网络信息安全系统可以发挥出预防黑客入侵、规避病毒破坏的作用，电力企业应当在提升配电网系统通信安全防护整体水平方面投入更多的支持。从而对电力系统运行的高效性和稳定性给予根本保障，确保为所有用户提供稳定的电力能源。

#### 四、电力系统配网自动化通信的网络安全管理问题分析

##### （一）对控制性能的威胁

就整个智能电网系统实际情况来说，在使用的过程中表现出了较强的实时通讯的特征，并且也能够对电网的运行情况加以全面把控。最为常见的智能电网控制系统的运用，网络响应时间往往可以对控制系统的性能加以调控。一般来说，如果局域网遭到了病毒的侵害，那么必然会导致整个网络运行稳定性的下降，最终就会造成网络响应时间的增加，无法对系统的控制性能加以根本保障，甚至会导致系统出现无法正常运行的情况。对于一些网络病毒软件来说，其也会遭到一定的破坏，使得病毒文件进入到系统之中，导致难控制软件会遭到病毒的损害，无法确保系统能够始终维持稳定运行的状态。另外，就病毒方面来说，其也可以利用系统漏洞嵌入到系统之中，对于整个系统的正常运行势必会造成诸多的阻碍。

##### （二）对传感装置网络的威胁

在电网自动化系统实际运行的过程中，将传感器装置进行有效的安设，能够对通信系统的运行给予良好的辅助，促使其可以与主体系统进行良好的连接，并且形成一个完整的整体，这样就能够将整个电网运行过程中所产生的各项数据进行统一的收集。一般来说，因为传感器的运行安全性较差，所以在实践工作的开展中，极易出现危险事故的情况。诸如：外部人员缺少对各项信息的合理运用，传感器在获取信息的过程中，信息的读

取效果无法加以根本保障。另外，很多工作人员会随意的对传感信息进行修改，这样对于电力数据的准确性和真实性必然会造成一定的损害，也会出现弄虚作假的情况。对于整个电力系统的稳定运行势必会造成一定的威胁。一般来说，外部人员也会利用传感器之中所存在的漏洞对网络层实施一定的干扰，这样就会对电网自动化系统的运行带来诸多的隐形风险。

#### 五、电力系统配网自动化通信的网络安全管理中的风险因素

##### （一）病毒风险因素

在将配网网络安全管理系统加以实践运用的时候，网络技术人员能够通过专业的技术来明确网络系统中所存在的漏洞，并且能够及时的进行处理。那些无法得到修复的网络系统运行漏洞通常都被称之为病毒，病毒其实质始终都存在于电力系统的配电自动化系统之中，这些网络病毒通常都会对整个网络的运行造成一定的攻击，极易导致网络运行过程中出现信息丢失的情况。对于整个电力系统的持续、安全运行会造成诸多的阻碍。在我国电力系统自动化和智能化水平逐步提升的过程中，网络环境发生了诸多的变化，电力系统运行过程中经常会遭到病毒的攻击，特别是在将自动化技术运用到对配电网系统的调节和管理工作中之中的时候，如果遭到病毒的攻击那么必然会对整个局域网的正常运行造成一定的损害，不能保证电力系统的持续稳定运行。

##### （二）操作风险因素

要想将电力系统的自动化技术在系统电力调节以及资源优化配置方面所具有的实践作用充分的发挥出来，专业技术人员务必要对整个系统实施合理的操控，确保自动化技术能够加以良好的运用。与之前老旧模式的电力系统相对比来说，配电电力系统中自动化技术的实用性相对较强，但是自动化技术并不能彻底的取代人工管理技术，还需要利用人工操作给予适当的辅助，这样可以保证配电网电力系统得以稳定持续运行。但是，人工操作通常也会受到工作人员专业能力以及工作态度的影响，经常会出现操作失误的情况，对于用户的用电安全是无法加以根本保障的。

##### （三）信息失真因素

在整个电力系统之中，合理的将自动化技术进行实践运用，尽管从根本上促进了电力系统运维管理工作效率和效果的提升，但是自动化技术与当代互联网技术进行良好的整合，能够对网络环境的整体水平加以良好的保障。当代信息技术以及自动技术在我国电网系统中的起步时间较晚，所以导致我国专业人员对于电力系统中网络技术的运用技巧的掌握整体效果较差，还需要进一步的进行优化。所以在将自动化技术引用到电力系统之中的时候，往往会出现因为接口或者是格式不匹配的情况而导致一些电力信息存留在网络系统之中，这样就为

那些不法分子提供了可乘之机，他们可以借助网络信息传递漏洞以及现有电力信息来获取一己私利，对于国家电力系统的发展势必会造成一定的阻碍。另外，这些私人行为也会上升到国家的层面上，诸如：电力系统如果出现信息漏洞，那么就可能会导致网络会遭到黑客的攻击而导致信息数据出现泄漏或者是丢失的情况，对于我国电网的运行以及未来发展都是非常不利的。

## 六、电力系统配网自动化通信的网络安全管理的优化策略

### （一）提高密码技术水平

要想对通信和信息安全加以根本保障，可以采用设置密码的方法。电力自动化网络中密码技术涉及多种类型。对称密钥算法其实质就是利用统一的密码来完成信息的加密工作，并且也可以使用密码进行解密操作，通信双方都知道密码，就可以进行直接通信。不对称算法其实质就是知道加密密码，但是只有拥有权限的人才可以进行解密。

### （二）提高防病毒技术

如果遭到计算机病毒的入侵，那么对于整个系统的运行安全必然会造成一定的损害。在电力系统网络化发展的过程中，网络病毒所形成的危害越发的严重，还需要相关工作人员加以重点关注。切实地对网络运行中计算机实施综合检查，并且逐步增强维护工作的力度，保证系统运行安全性。结合病毒传播的特征，避免使用其他U盘进行接入。另外，对于外来传输文件需要给予更多的重视，尽可能的运用正规的杀毒软件进行杀毒，如果有必要还需要定期对软件进行更新，这样才可以对电力系统的运行安全加以根本保障。

### （三）提高防火墙技术

在整个系统之中，防火墙的主要作用就是完成对局域网的保护工作，预防病毒的侵害。详细的来说，防火墙技术的运用其实质就是借助安设了防火墙软件的计算机系统来实施网络的全面管理，对整个方案实施全面的检验，保证路由器与网络系统能够形成完整的整体。另外，防火墙技术的运用也可以对整个网络运行情况进行全面的观察和监督，从根本上保证电力系统能够持续稳定的运行。

### （四）应用入侵监测技术

入侵检测主要是对各项操作行为实施审核以及全面检测工作。入侵检测技术的运用能够确保对各项信息进行统一的收集和整理，并且完成综合分析工作。监测系统的主要职责就是将电力系统运行中各项信息进行收集，借助处理系统与模型完成匹配，从而对侵入行为加以判断，借助有效的方法进行处理。

### （五）减少人为因素影响

对于电力系统，实际工作中，必须采取统一的操作。根据不同的需要，管理者需要授予具有差异性的操

作权限，从而为通信系统的安全性提供保证。

### （六）网管系统的管理

网管系统可以对网络进行全面的监控和科学、有效的管理，使管理能力逐渐提高。运用网络系统进行巡视的过程中，可以及时发现问题，并进行针对性的处理。同时，还需要不断加大预防力度，借助图像等多种辅助手段进行综合性的管理，使网络运行环境更加安全、稳定，使配电网具有更多的安全保障。

### （七）运维人员的管理

对网络管理加大巡视力度，同时采取专业的方式进行运行管理，使终端通信接入网的安全得到更多的支撑，使网络后期管理水平不断提升。加大人员培训力度，使所有的管理人员都具有较高的整体素质，可以与网络安全管理水平保持一致。强化管理人员的安全意识，及时对重要文件进行备份，以便紧急故障发生时能够从容处理。及时更新基础资料，并将责任落实到个人。

## 结语

综上所述，电力系统的自动化发展以及智能化发展虽然有效地提升了电力系统运行过程中资源的分配效率和质量，但同时让电力系统的运行面临着更加复杂的外部网络环境。因此，电力系统应该通过不断加强密码技术，提升电力网络运维人员专业素质，提高防病毒技术等方式，确保电力系统配网自动化通信工作的安全性。

## 参考文献

- [1] 刘啸, 蒋斌. 电力系统配网自动化通信的网络安全管理问题探讨[J]. 信息与电脑(理论版), 2022, 34(08): 212-214.
- [2] 余文斌, 王彬. 配网自动化建设对供电可靠性的影响分析[J]. 光源与照明, 2022, (03): 231-233.
- [3] 张媛. 电力配电网自动化系统中网络安全防护有效性探究[J]. 山西电力, 2020, (05): 31-33.
- [4] 蔡田田, 索思亮, 简淦杨等. 基于集成双向加密认证FTU的配网自动化安全防护方案研究与应用[J]. 电力信息与通信技术, 2020, 18(07): 64-70.
- [5] 倪伟东, 武利会, 王俊丰. 基于自主安全芯片的配网自动化系统网络安全防护及硬件加速[J]. 电力科学与技术学报, 2020, 35(03): 166-172.
- [6] 叶剑. 关于电力系统配网自动化通信的网络安全管理问题探究[J]. 科学技术创新, 2019, (36): 99-100.
- [7] 蒿峰. 基于灰关联投影的配电自动化通信网络安全性能评判研究[J]. 电子测量技术, 2019, 42(20): 143-147.
- [8] 薛磊. 电力系统配网自动化通信网络安全管理[J]. 山东工业技术, 2019, (08): 179.