试论电力自动化控制系统网络信息安全管理设计

李倩
国网山东禹城市供电公司

摘要：电力自动化控制系统是保障电力可靠供应的重要条件，为了更好优化电力自动化控制系统运行效果，切实做好网络信息安全管理工作极为必要，力求针对各类风险问题进行全面防护。本文就重点围绕着电力自动化控制系统网络信息安全管理设计工作进行了分析论述。

关键词：电力自动化控制系统；网络信息安全；管理

引言

随着当前我国电力系统的不断发展，不仅仅电力输送以及供电要求越来越高，需要体现出更强的功能价值，往往还需要重点关注于技术层面的创新，同时考虑到系统安全性保障。对于电力自动化控制技术在现阶段电力系统中的应用来看，为了更好优化作用效果，注重做好网络信息安全管理工作极为必要，需要围绕着当前常见风险问题进行重点研究，以便采取更为适宜合理的策略，优化网络信息安全保障效果。

一、电力自动化控制系统常见网络信息安全风险分析

在当前我国电力系统发展中，电力自动化控制系统的应用越来越普遍，该系统的应用确实表现出了明显优势，在适应当前越来越复杂电力系统的前提下，能够更好优化电力系统运行效率，在信息处理和传输方面同样也具备积极作用。基于此，针对电力自动化控制系统的应用进行高度关注极为必要。但是在现阶段电力自动化控制系统运行中，同样也存在着一些不容忽视的风险问题，应该作为安全防护的重要目标。

现阶段电力自动化控制系统在运行中主要面临的网络信息安全风险问题主要有以下几类：一是旁路控制风险，主要就是指在电力自动化控制系统运行过程中，受到外来破坏者的影响，导致其能够对于电力系统下发一些非法命令，进而也就容易给电力系统的稳定运行带来影响，甚至出现系统崩溃风险；二是工作人员方面的风险，因为相应电力自动化控制系统管理人员不注重网络信息安全防护，在工作中存在较为明显的疏忽大意，或者是明显违规行为，致使系统密码或者是关键信息外泄，同样也会带来严重风险；三是拦截或者篡改风险，主要就是指外界因素针对电力自动化控制系统中的一些关键参数或者是控制程序进行非法篡改，或者是拦截一些重要信息供自己非法使用；四是欺骗风险，主要就是指电力自动化控制系统网络信息结构在IP或者是Web欺骗中遇到的不良影响和损失；五是黑客，主要就是非法个体通过技术手段实现相应系统的入侵，进而对于电力自动化控制系统的运行产生不良影响，可能导致系统无法正常执行命令，或者是出现严重崩溃问题。

二、电力自动化控制系统网络信息安全管理设计要点

（一）明确设计目标

针对电力自动化控制系统网络信息安全管理工作的开展进行分析，为了更好提升安全保障效果，首先应该具体明确设计目标，把握好电力自动化控制系统网络信息安全防护的各项要求，细化具体安全管理任务。比如分区防护就是比较关键的一个具体目标，安全管理设计人员需要重点围绕着整个电力自动化控制系统进行详细分析，结合其运行特点以及强弱水平进行合理划分，进而最终保障整个系统都可以形成理想防护效果，后续具体安全防护也能够具备理想针对性。此外，针对电力自动化系统进行总体安全防护设计，做好横向隔离、网络隔离以及纵向防护处理，也需要引起管理设计人员的高度重视，将其作为重要目标和任务。

（二）优化网络设计

在电力自动化控制系统网络信息安全管理中，为了更好优化系统运行效果，切实优化网络设计极为必要，这也是降低一些不必要风险侵入威胁的重要手段。比如在外网接入设计中，需要充分考虑到发电厂调度数据网接入需求，进而按照标准化要求进行合理布置，确保外网的接入可以发挥出应有的作用效果，保障网络设备技术得到可靠运用；针对内网访问以及控制同样也需要进行科学设计，促使内部网络的运行更为安全合理，尤其是在横向访问以及纵向访问上，更是需要予以详细管控；针对路由也需要进行合理设计，促使中调发出的相关指令能够得到较好获取，进而保障电力自动化控制系统的稳定运行，在相关路由设备选择以及网络配置方面都需要引起高度重视，保障整个线路运行更为可靠；针对业务交换机以及CE交换机也需要进行安全设计，利用加密网关或者是防火墙进行优化。

（三）中调汇聚接入设计

在电力自动化控制网络信息系统的运行中，为了确保控制和非控制区的安全接入冗余问题可以得到较好解决，必然需要关注于中调汇聚接入优化设计，促使相应环节运行更为安全可靠。在该方面设计处理中，应该重点关注数据信息传输的逻辑隔离，借助于恰当的路由器以及纵向数据传输等手段，通过逻辑隔离形成数据信息的安全保护，尽量避免在该方面形成较为严重的数据信息混乱问题，保障数据安全。

（四）合理运用隔离手段

为了较好保障电力自动化控制网络信息系统的安全运行，借助于恰当合理的隔离手段同样极为必要。对于控制区和非控制区，就可以借助于横向隔离手段，促使两者间形成较为理想的运行效果，避免因为相互干扰，影响到整个系统的安全运行效果，比如防火墙NAT的应用就可以在该方面发挥积极作用，有效规避因为非控制区到控制区的主动连接带来不良安全隐患；借助于Eudemon 100E纵向互联硬件防火墙还能够有效保障控制区到非控制区的安全访问，避免影响功能发挥。从调度数据网和管理信息网的运行中来看，借助于恰当的隔离手段进行处理同样也能够发挥出较强安全防护效果，比如正向和反向的隔离装置就需要予以恰当安装，促使安全等级不同的区域能够形成有效管控，避免了信息数据的随意传输带来的严重安全风险威胁。

三、结束语

综上所述，电力自动化控制系统在当前我国电力行业发展中比较常用，为了更好提升该系统的运行效果，借助于网络信息安全管理工作极为必要，这也就需要围绕着各个风险问题进行有效防护，构建较为完善全面的信息安全防护体系，保障电力自动化控制系统网络信息安全。

参考文献

[1]王博翰,李欣欣.电力系统网络信息安全风险防范措施研究[J].居舍，2019（10）:191.

[2]赵妍,刘娜.电力系统计算机网络信息安全的防护探究[J].数字通信世界，2019（01）:124.

[3]刘鸣.电力系统计算机网络信息安全防护问题分析[J].中国新通信，2018，20（21）:167.

[4]姜晓涛.基于电力系统的网络信息安全的分析[J].信息技术，2017（12）:82-84+89.