

电力监控自动化系统中信息安全防护的应用

梁 超

中广核风电有限公司 北京 100070

DOI:10.12238/etd.v3i8.6218

【摘要】: 在目前我国社会发展的这一阶段, 科学技术的进步使社会各个行业的发展速度不断提升, 越来越多高科技技术融入到行业内部, 为行业的发展起到了有力的推动性作用。电力系统的发展关系到人们的生产、工作和生活, 所以本文的研究也是结合电力行业中, 监控自动化这一系统的信息安全防护工作展开分析, 希望能够在有效的自动化技术发展阶段, 实现电力工程信息的有效共享, 在保证其安全性的同时, 推动电力行业的发展和进步, 从而为我国社会整体的发展水平提升奠定坚实的基础。

【关键词】: 电力监控; 自动化系统; 信息安全防护

中图分类号: TM734 文献标识码: A

Application of Information Security Protection in Electric Power Monitoring Automation System

Chao Liang

CGN Wind Power Co., Ltd., Beijing 100070

Abstract: At this stage of China's social development, the progress of science and technology makes the development speed of various industries in the society constantly improve, more and more high-tech technology into the industry, for the development of the industry has played a strong role in promoting. The development of electric power system is related to people's production, work and life, so the research of this paper is combined with the electric power industry, monitoring automation system information security protection work analysis, hope in effective automation technology development stage, realize the effective sharing of power engineering information, ensure the security at the same time, promote the development and progress of electric power industry, to the development of social overall level lay a solid foundation.

Keywords: Electric power monitoring; Automation system; Information security protection

引言

随着科学技术迅速的发展, 其相关行业的整体水平也得到了提升。国内外电力企业还有技术的标准相关组织, 统一的提出了对电力监控的自动化系统进行筹划的相关要求。特别是在自动化系统中, 信息安全的防护更是受到了人们的关注。所以在进入到一个全新发展态势的过程之中, 电力系统既需要跟随时代发展的脚步, 走上以科技制胜的道路。也需要拥有强有力的后方保障, 从而确保电力监控系统的信息安全和稳定建设。因此这也能够看出, 在我国逐渐发展阶段, 电力系统中监控的自动化应用, 需要拥有较强的安全性, 这样才能够日趋成熟的网络技术环境下, 实现电力系统的发展, 也能够真正地为监控的自动化应用起到有力的保障。

1 电力监控自动化系统概述

在电力事业发展和进步的过程中, 其监测自动化这个系统所包含的主要就是电力、电气的相关软件, 其中涉及的有历史数据库中的 XPMS 通信的网关, 以及网络的服务器等相

关的内容。其中计算机还有数据的通信是主要的核心, 也是对各种数据进行收集和存储的关键方法。通过这个模式的应用, 能够对电力系统运行的情况进行有效的监督, 所以也可以看出, 这一自动化系统被各个企业和工厂应用到信息管理的过程之中。

电力的监测中其自动化的系统所包含的有数据通信的相关软件, 而这个软件在使用的阶段, 也呈现出了多种用途。根据主要运用的方法, 可以分为: 生产信息的有效控制、企业的经营和管理, 还有市场的营销等相关的工作。对于电力生产的系统来说, 能够起到的作用是相对更大的。因为其中所包含的有生产制造的相关制度, 变电站的自动化系统, 还有质量的安全保障等一系列的内容。所以这也能够使网络在生产、调度等相关工作应用过程中, 实现信息的有效传送。总体来看, 供电的系统其业务在开展的过程中, 所呈现主要的特点就是独立封闭, 所以必定需要利用物理隔离的方法, 来使监测自动化这一技术最大程度地提高自身的可靠性。在生产管控的相关阶段, 也需要运用有效的方法来避免各方面因素所造成的干扰, 只有这样才能够使监控的自动化系统中

的信息得到有效的防护和保障。

2 电力监控自动化系统中信息安全防护的基本要求

电力的监控系统所包含的主要就是三个子系统,具体的内容就是:生产控制信息、生产管理信息,还有网络通信这三个系统。所以在实际的信息安全防护阶段,还需要满足其中所涉及的基本要求,才能够实现相关工作开展效果的最大化。

第一方面是遵循国家所颁布的规定,按照规章制度和管理方法的要求执行相关的工作,这也是信息安全防护工作实施过程中的主要标准。特别是在我国确立了网络信息的法律地位之后,电力监控系统的安全防护,更是要在法律保障的前提下实施和运行。

第二方面是系统信息安全的防护和相关工作开展方案,需要具有一定的预测和预防性特点。在具体方案应用的过程中,需要遵循网络专用、安全分区、横向隔离、纵向认证等一系列的原则,这样才能够形成一个安全防护的体系。也能够有效地把外部的网络进行隔离,快速的对现阶段网络所呈现出的异常进行诊断,从而利用安全防护系统、预警系统等,避免信息泄露的情况出现。

第三方面是系统信息在安全的防护工作开展和实施的过程中,需要利用等级保护的等级,来提高安全防护的整体能力。等级的保护应该在电力监控的系统不同的层面着手,通过有效的安全管理工作,最大程度的完善及工作开展的效果。包括的有:网络、主机、数据等各个层面。针对不同层面安全等级的制定,也需要有不同的内容和要求,根据相应的防护方案,确定其保护的等级,这样才能够使系统自身就拥有着防范恶意攻击行为的能力,也能够实时地对网络异常的现状进行有效的感知。

第四方面是需要对电力监控系统的安全防护功能进行有效的细化,使防护功能满足系统的边界,还有网络在传输过程中的边界等相关防护的要求,从而设计出不同的安全防线,提高安全防护的效果和整体的质量。

3 电力监控自动化系统中信息安全防护的具体应用策略

3.1 数据加密技术

在电力事业发展阶段,对于其监控的自动化这一系统的实际应用情况进行深入的分析能够看出,数据的加密这个技术能够有效地对网络传输过程中可能存在的信息篡改、窃取等情况进行有效的防范和控制,也能够避免网络中受到非法的入侵等各种情况的威胁。其中主要使用到的就有 RSA、DES 等加密的技术,这也是对信息进行有效防护和安全保障

的关键技术。在实际应用的过程中就能够了解到, RSA、DES 这两种算法其自身的优缺点能够达到互补的效果。其中对称密钥在加密的过程中,整个系统无法完全被替代,也很难实现公开密钥的加密。所以在电力监控的过程中,就需要把两种算法的优势进行有效的结合,这样才能够真正的实现最大防护的效果。

例如:可以结合使用对称加密这个技术,对电力系统中所涉及的文件内容进行加密,然后再利用公开密钥这个技术,对上述已经加密的文件再一次进行加密。通过混合加密这种方法,提高整体运行的速度,强化密钥在分配过程中管理工作开展的整体效果。在具体应用的范围角度来看,对称加密这个技术比较适用于大量数据之间的有效加密和合理处理,公开加密这个技术适合使用在加密的机密性和关键性数据基础上再一次进行加密。所以在对电力监控的系统进行应用的过程中,还需要根据级别进行前期加密和后期加密,这也能够最大限度地使加密的范围得以扩大,更能够保证数据系统的安全性。

3.2 防火墙技术

对于数据来说防火墙属于一道阻隔不良信息侵扰,以及对现有消息进行保密的屏障。在设置的过程中,其能够通过对被保护的网路与外部网路之间的有效隔离墙,建立起对破坏性侵入行为防范的最佳效果和目标。防火墙这个技术可以对跨越防火墙的数据,进行深入的检测,不良的数据能够有效地被限制,这也能够看出防火墙就可以最大程度地把外部信息合理地进行屏蔽,也能够避免外部非法信息入侵到网络之中。

专业化发展的角度上来看,电力系统在应用的过程中,使用防火墙技术能够真正地达到逻辑隔离的最佳效果,也能够从根本上保障社会系统中信息的安全性。电力监控系统在设置防火墙时,也需要对相关的参数进行考量,从而确保信息安全,防护正义功能最大程度的得以实现。其中具体的功能主要包括的有:

第一方面是数据包的有效过滤。在网络层进行设计时,需要把过滤及进行有效的边界,根据过滤及选择合理的数据包,保证每个数据包中协议的状态目的地地址,还有原地址等都能够接受逐一性的检查。最后再进行组合性的检查,了解其中所存在的问题,进而确定数据包是否能够通过网络层,实现数据的过滤。

第二方面是应用级的网关把协议过滤之后,需要通过转发功能有效地进行建立。通过应用层中数据协议的过滤,以及对逻辑数据包的有效整合,重新进行分析登记。也需要把数据进行有效的统计,了解数据应用的具体情况,生成数据

包的过滤报告之后,才能够进行下一步的相关工作。

第三方面是代理服务等内容。对跨越防火墙中网络信息的链接进行有效的划分,就需要有两个终止代理服务器的链接,对防火墙内外的计算机系统进行有效的考量和合理的链接,这样才能够使外部的网络系统能够受到代理的相关服务工作。与此同时,计算机在代理服务的支持下,也能够对登记过的数据包进行准确的分析,从而形成过滤报告,一旦在代理的服务工作开展和实施的过程中,发现了被攻击的情况,就需要及时地发出警报,并且把攻击的痕迹进行保留,从而使这些问题不会再一次的发生。

3.3 身份认证技术

在电力系统的具体监控自动化工作开展和实施的过程中,对身份认证技术是能够保证网络信息安全的一个关键性技术内容,同时也是相关工作在实施过程中的核心内容所在,能够对用户的身份进行准确的确认和合理的辨别,也能够防止非法用户入侵到网络中的现象出现。因为网络通信所涉及的用户数量是相对比较多的,所以还需要把身份认证的技术引入其中,利用验证用户身份的方法,保证这项工作合理有效地得以开展。也需要确保与预留的用户信息达到一致性,根据预设所呈现出的权限,允许合法用户对网络进行有效的控制,以及合理的访问。为了能够保证网络信息自身所具有的安全性,就需要利用身份认证技术,为用户建设起准确良好的身份。根据不同的用户也需要结合特定网络的资源,设计出使用的权限,从而确保这一权限能够为网络的应用起到有效的隔离以及管理效果。

防范非法用户对网络资源进行应用的过程之中,还需要结合用户自身访问的权限,还有其他资源的实际的情况进行有效的认定。身份认证这一技术可以利用密钥、口令、智能卡、指纹等方法进行合理的认证,从而确保这项工作最大程度地得到有效的实施。在电力的监控系统中,也可以结合使用证书的授权这种方法展开认证的相关工作,由证书的授权中心进行分发以及有效的签署,从而确保客户的证书能够有效。其中也需要把公开密钥包含在内,使用户能够拥有独立的私密密钥,而密钥与证书之间更是需要相互对应,才能够实现最佳的使用效果。如果想要获取密钥中加密的相关信息内容,就需要使密钥能够解除加密,这样的方法就能够最大程度的保证信息的安全,这也是比较常用的公开密钥使用的模式。其中解除密钥的技术一般情况下都是数字签名,这也能够有效避免用户出现非法入侵网络的现象。

3.4 入侵检测技术

入侵检测这个技术通过实时的分析,就能够在连续或者积累的过程中拥有一系列的记录,从而快速地对其中所包含

的入侵行为进行有效的检测,也能够将检测信息传输到安全的管理部门之中,从而发出安全的入侵信号和相关的警告。这种技术针对的主要就是网络内部异常的活动进行有效的检测。其中具体的检测方法:

第一方面是通过定期的收集,还有统计分析等相关的数据内容,对所观察到的活动进行检验。判断活动在开展过程中的可靠性,如果活动的行为与合法用户的行为之间呈现出了符合性的特点,那么就被判为具有较高的可靠性和可信度。

第二方面是预先对其中的定义和规则进行设定。根据规则检测出入侵的行为,是否符合规则在电力的监控系统中入侵检测这个技术,是较为必要的安全防护技术。这种技术能够有效地检测和阻隔网络入侵的行为和现象,从而应对由于密码盗用,而出现的网络安全的问题。

4 结论

综上所述,在我国电力行业发展速度不断加快的阶段,监控自动化这一系统所应用的范围在逐渐变得广泛,而数据信息整体安全的风险和漏洞却随之而来,变得越来越多,这也在很大程度上为我国电力事业的发展造成了一定的影响。所以还需要找到正确有效的信息安全和防护工作开展模式,利用科学合理的手段,实现企业和相关行业的进步,才能够达到最佳的效果。所以本文就在上文的内容中,以监控自动化系统的概述为核心,分析了其信息安全防护技术在电力监控自动化中的具体应用措施,希望能够为我国行业的发展,以及数据安全的有效做出贡献。

参考文献:

- [1]史俊霞,洪成,王阳英夫等.电力监控自动化系统中信息安全防护设计分析[J].上海电力大学学报,2021,37(S1):41-43.
- [2]朱昊.电力监控系统信息安全管理系统的研究与分析[J].科技创新导报,2019,16(36):122+124.DOI:10.16660/j.cnki.1674-098X.2019.36.122.
- [3]乔林,周巧妮,吴赫等.基于等级保护的电力信息安全监控系统的设计[J].科技风,2019(10):91.DOI:10.19392/j.cnki.1671-7341.201910082.
- [4]覃炯聪.电力信息安全的监控与分析[J].中国新通信,2018,20(21):170.
- [5]郭仕杰,高鹏.电力监控自动化系统中信息安全防护与应用[J].电子技术与软件工程,2017(21):189.