企业电力监控系统安全风险及防护策略

李林鹤
内蒙古龙源新能源发展有限公司

摘　要：在电力系统中，电力监控系统是对发电、供电等各个方面进行监控的一个关键的组成部分。比如，电能监控与监控与数据获取、能源管理、变电所监控、广域相位计量、继电保护设备与监控设备、电网调度网络等。在电力系统的发展过程中，由于电力系统的自动化程度日益提升，使得电力系统的安全性得到了极大的改善。要确保电力系统的安全、可靠地工作，就需要在管理与技术两个层面上进行努力。为此，本论文拟从企业电力监控系统中所面临的各种安全风险入手，研究相应的安全防护策略。

关键词：企业；电力监控系统；安全风险；安全防护；策略
【DOI】10.12252/j.issn.2096-627X.2022.09.220

在电力行业中，电力监控系统通常被称作“电力二次系统”，是指“以计算机和网络技术为基础的，用于对电力生产和供应过程进行监测与控制的业务系统和智能设备，以及以此为基础的通信和数据网络等”。电力监控系统是整个电网的神经网络与控制中枢，是保证电网安全、稳定、可靠供电的关键。进入二十一世纪之交，我国各大电力公司相继发生了“二滩电厂停机事件”、“时间逻辑炸弹”等与电力监控系统有关的信息安全事件，造成事故或形成安全隐患。这些事件表明，电力监控系统面临着越来越多的信息安全风险，这直接威胁着电力系统的安全、稳定、可靠的供电。对此，电力行业高度重视，先后出台《电力二次系统安全防护规定》和《电力监控系统安全防护规定》等配套措施，制定了符合国家信息安全等级保护要求的电力行业标准，积极推进电力监控系统安全防护体系的建设，取得了很好的效果。

一、电力监控系统安全防护的特点

（一）系统性

电力监控系统内部有分层划分，各个子系统之间有着密切的联系，需要利用防火墙将调度自动化主站和厂站控制区与非控制区之间的信息交互，同时，在生产控制区与管理信息区之间，还需要利用正反向隔离装置实现信息交互，同时，在厂站站控层系统、间隔层系统和过程层系统之间也存在着信息交互，各个子系统内部存在的漏洞和缺陷，都会对整个系统的安全性造成一定的影响，但是，整个系统的安全性最终还是由系统中最薄弱的部分来决定，所以在系统的建设和运行过程中，一定要对最容易受到攻击的环节和漏洞给予重视。

（二）动态性

随着我国网络科技的迅猛发展，网络病毒、黑客攻击等问题日益突出。因此，对电力系统进行主动、动态和实时的安全保护显得尤为重要。

（三）电子化

目前，电力监控系统的安全防护与传统的电力监控系统最大的不同之处在于，电力系统的电子特性十分明显，传统的电力系统安全防护工作主要依赖于手工操作，它的安全防护和监控工作不能保证及时性，也不能做到全方位，而工作人员的素质和业务能力则在很大程度上影响着他们的安全防护工作的执行程度和效果。而现在，在电力行业与电子信息技术不断发展的情况下，将二者有效地融合在一起，使电力监控系统的安全工作呈现出电子化的特征，只有顺应时代的潮流与潮流，才能充分利用这一特点，做好安全防护等相关工作。

二、企业电力监控系统中存在的安全风险

（一）工作人员安全意识不足

当前，负责电力监控系统的一些工作人员在安全意识方面还不够强，对这部分工作人员的安全培训力度不够，导致在电力监控系统运行时，不能采取切实有效的安全保护措施。同时，有些工作人员对进入电力监控系统的密码保护不够，例如使用简单的默认密码，或者长时间使用相同的密码，都有可能造成监控系统中的密码泄漏，如果密码被不法分子获得，将会给整个电力监控系统带来安全隐患。

（二）网络木马及病毒的威胁

近几年来，随着信息技术的飞速发展，电力系统中大量的新兴技术被充分利用起来，一些网络系统和网络平台给电力行业带来了很大的方便，可以更方便地进行管理。但在这一过程中，也有可能出现网络木马病毒，使电力监控系统存在被恶意入侵的风险，从而威胁到整个电网的安全。近几年国内外新闻报道中，网络木马病毒入侵电力系统的情况也比较常见，所以网络木马病毒对电力监控系统构成了很大的威胁。

（三）安全系统方面存在不足

目前，我国电力监控系统运行中存在着安全体系方

面的问题。首先，新兴技术的应用使网络面临着某种程度的威胁，但目前尚无一种科学、合理的防范和控制手段。其次，风险预警和安全保护没有形成有效的联动。最后，目前的安全系统仅仅是将多种安全防护机制进行简单的叠加，而不能形成互补的防护策略，对整个网络风险的抵御能力较弱，不法分子可以利用该漏洞对电力监控系统进行攻击。

（四）网络建设与风险相脱节

在建立电力监控系统的网络安全保护机制时，要符合国家和电力部门的有关规定，设置防火墙、网关等防护设施。然而，尽管在入口设置了保护机制，但在信息管理方面依然存在着被攻击的危险，这是由于电力监控系统中，网络建设和安全管理两个部分没有结合起来，无法保证随着电力监控系统的改变而发生变化。这将使得电力监控系统的安全保护变得薄弱，这对整个系统的安全构成了一定的威胁，必须提高对这一问题的重视程度，并加以适当的解决。

三、企业电力监控系统安全防护措施

（一）建立健全电力监控系统的安全防护计划

为保证各类保护设施在电力监控系统中发挥各自的作用，需要建立科学的安全防护方案，推动系统正常运行，通过不同类型的方案和防护措施的实施，保证防护计划的持续完善，定期更新完善相关的防护工作，保证系统内相应的技术措施能够有效地运行。在此基础上，不断地改进方案，最终形成了一个较为完整的系统安全体系。为了确保安全防护策略的有效实施，需要建立切实可行、精确的地基模型，并结合具体的计算结果，确定系统的外部影响及维修周期。据此，制定有针对性的保护方案，落实相关工作，并定期对监测系统进行保护。系统检查应严格按计划执行，确保各项安全防护措施能有效实施。需要对系统运行过程中存在的潜在风险进行定期统计，全面收集网络安全相关数据，为优化保护方案与方案提供依据，最终明确并迅速地将风险类型及应对策略公布并实施。

（二）有效落实安全管理措施

一般而言，电力监控系统所面临的安全威胁主要来自企业内部，因此，必须采取有针对性的安全管理措施，以确保发电厂运行的规范性与安全性，及时发现企业的安全漏洞。此外，还应不断增强相关人员的责任心，保证各项管理措施的有效执行，并严格按照相关法律法规进行。与此同时，充分利用现代信息技术在安全保护上的优势，对电力监控系统与保护措施进行持续更新，对防病毒系统与防火墙进行强化，对日志进行分析与修复，保证对外部威胁的及时发现与排除，从内部防止各种供给漏洞和信息泄漏隐患。

四、电力监控系统网络安全技术的应用策略

（一）应用数据传输加密技术，加强电力系统网络安全性

从目前的情况来看，要确保电力系统内各种信息、数据或有关数据不发生泄漏，对其进行加密处理是一种行之有效的方法。数据传输加密是指利用加密钥匙和加密算法等加密技术来保护电力系统的信息，将重要信息转化为无关紧要或无法理解的符号，从而保护电力监控系统的安全。加密包括明文，密文和密钥三部分。事实上，数据加密技术的应用意味着，在电力监控系统的运行过程中，传输信息的一方需要使用密钥来发送密文，而获取密钥的工作人员则需要对密文进行解密。密匙又被分成私用密匙和公共密匙。相关技术要求各有不同，但均适用于电力监控系统的网络安全保护工作。具体来说，国产电力监控系统必须选择纵向加密认证设备。纵向加密认证设备是通过调整数据网络系统来增强网络的安全性，采用独特的密文技术，提高数据的安全、可靠和完整性，而不影响用户的网络设置。一般来说，数据网安全区域都是采用垂直加密的方式，通过相应的设备将明文转化为密文，以保证数据传输的安全性。垂直加密技术包括多种技术，目前国内外使用最多的是 RSA算法。目前，国内电力监控系统必须采用国产加密算法。对电力监控系统中的每一个环节都采用了加密措施，保证了信息不会被不法分子窃取，即使被盗取了，也无法得知内容。采用的具体方法就是先将设备还原为初始化状态，然后在初始化设置过程中设置密钥。图1示出了工作的基本步骤：无论在哪个层次上进行资源调度，都必须使用垂直保密技术，以最大限度地避免信息泄漏。

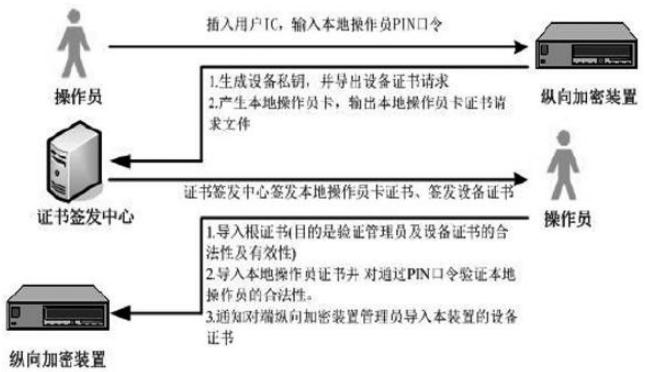

图1 基本的工作步骤

（二）构建防火墙强化网络认证

防火墙及时地保护了网络上的信息，它不但可以防止潜在的危险，防止内部信息泄漏、病毒入侵，而且还能对网络安全进行检查检测，对侵犯网络安全的违法行

为进行制止。防火墙分为三种类型，每一种都有自己的优点和缺点。为了提高电力监控系统的安全性能，必须根据实际情况建立一道防火墙，对重要的逻辑数据进行保护。另外，许多人之所以会在网上为所欲为，完全是因为网上找不到他们任何真实的信息，所以，为了阻止更多的人违法犯罪，就需要加强网络实名认证。保证每个人的真实身份，保证每个人的身份信息都不会泄漏出去。

（三）探索技术路线，以实现安全可控

安全可控主要指的是自主可控，没有自主可控，就不可能有网络安全。目前，中国的科技发展遭到了外部封杀，电力行业等能源行业面临着严峻的网络安全问题，加强自主可控的网络安全防护能力迫在眉睫。“自主可控”是国家电网构建主动安全防护能力的根本要求。国调中心成立多个工作组，开展多项研究与评估工作，促进电力生产关键环节（如电网调度、变电站等）的保护监测、网络安全等核心技术的自主控制与替代。在核心技术领域，包括 CPU处理器、存储器、网络控制、FPGA等关键基础芯片，以及操作系统、数据库等基础软件部件的技术攻关和科学规划，构建基础技术研究、产业研发、工程应用的迭代生态，保证电力产业链、供应链的自主安全和可靠性，建立安全可控的电网生产控制信息技术体系。

（四）强化化工控制系统的安全防护意识

在电力系统信息通信网络安全保护方面，工作者可考虑在工业控制系统的构建中应用人工智能技术和大数据技术，提高信息通信网络安全保护的主动性，降低恶意攻击等网络安全问题给电力系统造成的危害。在这一过程中，工人可利用人工智能技术赋予工业控制系统学习能力，让工业控制系统根据系统运行数据，判断是否存在安全隐患，并依据大数据分析结果对安全隐患进行追溯，以避免因恶意攻击及其他网络安全问题而造成的损失，从而实现对电网通信安全的预警与保护。此外，工作者也可直接运用人工智能技术，为工业控制系统搭建态势感知平台，以数据为驱动，对信息通信网络流量、工业控制系统威胁情报数据、网络安全行为、持续高威胁因子等进行持续监控，进而对工业控制系统进行自动审计、感知、预警和运维，全面掌握和掌握工业控制系统的安全状况，保证电力系统信息通信的可靠性。

结语

总而言之，在当前的时代背景下，加强电力监控系统的安全性与稳定性是极为必要的，人们应该加强对电力监控系统的重视程度，针对其中存在的安全风险进行深入地探索分析，并提出切实有效的解决策略，切实降低安全风险概率，让电力行业在未来的发展中更加稳定更加高效，为国家电力行业的运行提供安全保障，这对于今后的社会经济发展都会产生极大的促进作用。由此可见，为电力监控系统运行中存在的安全风险制定安全防护策略是极为必要的。

参考文献

[1]郭宾，陈超，文昱博，徐芳.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，2021（06）：73-82.

[2]潘峰.电厂电力监控系统安全防护策略浅析[J].中国新通信，2020（9）：32-35.

[3]邓志平.电厂电力监控系统的安全防护措施研究[J].大众标准化，2020（5）：88-91.

[4]刘中坚.电厂电力监控系统安全防护策略研究[J].电子制作，2020（3）：145-147.

[5]蒋涛，董贵山，杨乐怡，黄妮娜.新形势下电力监控系统网络安全风险分析与防护对策[J].信息安全与通信保密，2021（04）：79-84.

[6]张庆.浅谈电力监控系统安全防护重点要求[C]//.2021年电力行业技术监督优秀论文集，2021：153-157.

[7]苏生平，赵金朝.青海电网电力监控系统安全防护全过程管理体系构建与实践[J].青海电力，2021，40（03）：44-47.

[8]欧阳宇宏，康文倩，车向北.电力监控系统信息通信网络安全及防护问题研究[J].信息系统工程，2020（12）：60-61.

[9]高昆仑，辛耀中，李钊，等，智能电网调度控制系统安全防护技术及发展[J]，电力系统自动化，2015（1）：48-52，

[10]胡若琳，王昆，肖添，姚远，刘渺，刘建国.电力监控系统安全防护管理方法探讨[J].通讯世界，2019，26（06）：228-229.

[11]陈明亮，余侃胜，钟文慧，吴颖，张瑛.电网电力监控系统安全防护管理提升研究[J].电力，2018，42（10）：22-24+32.

[12]张亮，屈刚，李慧星，等.智能电网电力监控系统网络安全态势感知平台关键技术研究及应用[J].上海交通大学学报，2021，

[13]孟庆东，李满坡，安天瑜，等.电力监控系统网络安全管理平台设计与实现[J].实验技术与管理，2020，37（7）：53-57