电力监控系统主动防御技术架构剖析

杨伟 张磊 张庆

新疆华电苇湖梁新能源有限公司，新疆省乌鲁木齐市，830000；

摘要：电力监控系统的主动防御技术正逐渐成为确保电力安全的关键要素。在如今电力行业面临日益复杂的威胁与风险之际，这些技术不仅能提供基础的防御机制，更能以智能化、自动化的方式，实现对潜在风险的主动识别和应对。这种技术的应用远远超出了传统的防护手段，它要求系统具备自适应、自恢复的能力，以面对从网络攻击到设备故障等各类威胁。深入剖析这些技术的架构、协同作用和提升措施，能够揭示出其在电力监控系统中所扮演的重要角色。通过这一技术，电力企业能够不仅应对突发事件，还能实现持续稳定的运营保障。电力监控系统的主动防御技术，正是未来电力安全的关键。

关键词：电力监控；主动防御；技术架构；安全保障；系统协同

DOI：10.64216/3080-1508.25.02.021

引言

在电力系统日益复杂的环境中，如何保障电力系统的稳定、安全运行，不仅是技术问题，更是社会责任。电力监控系统作为电力企业的“神经中枢”，其安全性直接决定了国家基础设施的可靠性。然而，随着技术的进步，电力监控系统面临的安全威胁愈加多元。传统的被动防御手段已经无法应对日益严峻的挑战。因此，主动防御技术的提出与应用，为电力行业提供了新的解决路径。主动防御不仅是对现有安全防护体系的补充，更是对电力系统未来发展的积极回应。通过技术创新和深度集成，电力监控系统的安全防护将进入一个全新的阶段。

1 电力监控系统主动防御技术背景

1.1 电力监控系统的核心功能、结构概述

电力监控系统是整个电力企业工作的心脏，保障着每一个电力生产传输或者分配过程安全与稳定。整个电力系统监控的作用包括采集数据、报警故障、控制调度、实时监察等，可以为整个电力行业的工作提供准确及时的数据信息，使得电力流动畅通安全。电力监控系统主要包括现场采集层、数据传输层以及电力调度控制层三部分，电力各个层次在互相配合作用过程中，从现场设备向调度控制中的一系列工作能够快速及时准确地进行调度反馈，高度一体化的结构以及准确的信息流动使得电力系统能够很好地应对复杂的电力行业运行环境，保障电力供应安全性、稳定。

1.2 主动防御技术在电力监控中的应用前景、需求

电力系统智能化、数字化不断演进过程中，恶意攻击与技术故障的风险提升了很多，电力监控系统不仅只是一个数据采集平台了，它还要承担起主动防御一切挑战的需求，这也是主动防御技术不断应运而生的原因。主动防御技术与以前的被动防御技术不同，前者能够提前察觉异常情况的存在，实时监控和智能化分析就可以预警到可能存在的隐患问题，除了可被用在防御网络攻击方面，可以辅助电力监控系统提前预判，预测出设备可能发生的故障并作出高效响应，实现智能化防御电力监控系统自身的修复、隔离威胁和及时恢复，有效提高了电力系统安全保障水平[1]。这也说明了电力未来安全的思维与态度，同时也标志着智能化时代的来临。

2 电力监控系统面临的挑战、技术难点

2.1 电力系统中的安全风险、防御需求

电力系统关系到国民经济的命脉和社会的正常运行，因此，它的好坏是十分重要的。电力监控系统的安全威胁越来越多，影响系统安全的风险因素很多，其中网络攻击、设备操作、自然灾害等可能造成电力系统运行中断或者造成对供电系统严重的损害，同时，随着信息化进程的快速发展，电力系统与外部网络的接轨也增加了系统所面对的风险。这种传统防御方式已经不能满足当前需求，因此，需要采用主动防御技术主动寻找、抵抗外部入侵和对内部设备的运行检测，及时发现系统内部潜在问题等来实现电力系统的主动防御。

2.2 防御技术实施过程中的实际困境

虽然主动防御技术给电力监控系统安全带来了新的解决办法，但是落实到工程中也存在许多困难。由于技术复杂度高，使得系统实施部署和后期运维难度增加；电力监控系统存在多个层次的硬件或软件子系统、不同技术应用于同一个系统中的适配、系统架

构设计、应用防御技术等等，都需要付出许多资源成本；防御技术响应和控制要求很高，系统延迟程度稍高就有可能导致严重威胁的发生；特别需要提到的是，在设备数量庞大、地理分布广泛，安全隐患种类繁多的电力系统中实现防御控制要求及时，这对技术人员的素质和安全意识的要求非常高。

2.3 技术适配、系统协同问题

电力监控系统包含大量不同厂商、不同技术提供商的设备和软件，因此，技术适配、系统协同是有效防御的关键。电力监控系统内的各种子系统，尽管有着在不同场景下不同的功能需求，但却必须协调配合以实现系统的防御目标。由于各种设备/系统的技术标准不同，这些设备/系统之间的互操作能力和数据共享是一个很大的挑战。此外，系统内部多防御机制/模块的协同作用也需要发挥，以实现快速和高效的防御应对[2]。例如，入侵检测系统和异常行为分析系统之间需要共享实时数据信息并共同分析威胁，从而提供精确的防护响应。

3 电力监控系统主动防御技术架构剖析

3.1 电力监控系统的架构设计、功能分配

电力监控系统既然是由多种技术的集合体，并且是基于电力企业运行和社会经济发展的“血液”，如何设计电力监控系统的架构不但关系到系统的功能实现，同样也关系到电力企业在面对突发事件时如何灵活地做出反应和应对。完善的电力监控系统的架构，应该具有一定的柔性，使其能够根据突发情况随机应变。通常来说，电力监控系统的架构基本分为数据采集层、数据传输层、控制决策层和管理层 4 个部分。数据采集层，通过电力系统中装置和传感器的连续数据采样和监测，能够检测到实时的电压、电流、频率等主要数据。该层是电力系统和实际社会的桥梁，可以看作为最底层的感知。数据传输层是对数据和信息从现场端传输到控制决策层，同时也要保证信息数据的完整性、实时性，其稳定性的高低决定系统整体的时效。控制决策层就是所谓的电力系统大脑，通过采集来的数据做出有效的分析和处理，进而做出调度与控制决策。管理层，对于这些综合的数据，企业决策层可以利用其进行综合分析，为企业做长期的分析与制定，对企业系统进行综合性的维护与完善，在长期运行中保证电力系统的安全与高效。在这样一个具有多层的架构中，无论是哪一层的功能和作用都要明确，同时也必须要有各个层级的协调和配合。主动防御技术正好是嵌在这个架构上实现的，每一层要具备防御机制，不管是什么样的网络攻击在数据传送层、故障自动响应在控制层都要体现出来，实现主动防御的无缝对接[3]。

3.2 主动防御技术的核心组件、实现模式

主动防御技术的融入为电力监控系统提供了不同于以往被动防御的主动化应对能力，从而推动电力系统不仅仅再扮演单一的被动防御者的角色，而是具有一定主动性、可以对抗与攻击、应对与防范的能力和机制。而主动防御系统中的核心部件则是这一套系统的核心，它们将数据流、异常行为等信息从海量的数据中提取出来，给予电力监控系统向一个预先计划好的方案中规避的建议与措施，从而最大限度将电力控制系统遭受威胁情况的扩大与升级控制。在这套核心部件中，威胁检测系统无疑是其中的核心部件，系统借助一定的算法不断进行数据的分析、行为的监视、流量的解析从而提升电力系统运行中针对非正常行为异常的识别效率与即时性。因此，威胁检测系统是在事前警觉还未显现之前就借助数据等提前进行相应的警报。响应部分是主动防御系统的第二个重要构成。它包含系统在获得威胁的检测后如何将威胁进行即时与有效、智能化的处理[4]。例如在攻击过程中，系统会自动将遭到破坏的系统进行隔离，并启用备份路径，将遭受攻击事件与范围控制在最小的程度；或者当遭遇故障而产生重大损害时，系统将立刻调整负荷，重新分配其任务，保证其运行中的电力保障不受影响。但同时，在响应上，这种响应过程与能力一定要达到极其高程度的自动化、智能化的程度与能力，同时能够对于风险的严重性、能否使用到何种针对性的措施快速做出判断。

3.3 系统内各技术模块的协同防御作用

不同技术模块在电力监控系统中并非独立存在，它们之间的协调作用是电力监控系统主动防御能力形成的基础。技术模块不仅需要在其责任范围内起作用，更为重要的是其与其他模块进行协调才能形成更为高效的防护防御体系，两个技术模块之间协调工作，进而形成一个协调的、信息共享的防御系统。入侵检测系统与异常行为分析系统之间的协调，可以看作是防御工作中的重中之重。入侵检测系统对网络流量进行检测，从中捕获异常情况；而异常行为分析系统则是根据其保存的历史数据、异常行为规律、攻击模式等对发现的异常情况与正常情况分别进行判断。通过两者的协作，使得判断更为准确，能够规避单一防御技术在防御工作过程中出现的误报或是漏报现象。数

据安全防护模块是数据本身进行防护，其中数据加密技术以及备份恢复系统进行协作，从而在发现数据被控制或者失陷时能够尽快的进行备份恢复操作，防止重要信息被篡改或者丢失[5]。不同技术模块相互独立相互联系，利用不同层次不同组件进行数据加密、数据传输监督、数据备份恢复，从而完成各个技术模块的综合防护体系。

3.4 防御能力提升的技术措施、方法

电力监控系统防御能力提升，是要多方面层层递进的提高防御技术、构建防御体系，来应对不断出现的网络攻防攻击和故障隐患。提高电力监控系统防御能力的重点，是要靠电力监控系统的自我处理能力和动态快速响应能力来完成，而这一目标的实现也不是靠某个技术的提升实现，而是需要多种新技术的有机融合。其中最重要的技术手段之一就是人工智能和深度学习，通过对系统历史数据的分析找出可以预示系统的攻击行动的模型并提前进行预警，这样的智能防御方式，不仅要能够发现已知攻击方式带来的系统安全风险，还可以通过自我学习发现未知的风险隐患，而自我发现能力是防御能力中“主动预防”的体现，就比传统的被动防御方式更精确有效；动态风险评估系统的建立，对电力监控系统中的各个环节从外部、内部、历史安全事件及预警信息等多方面进行实时动态风险评估，对可能存在的风险点进行预测，这样在攻击行动之前就及时发现潜在隐患，及时主动防御。

3.5 电力监控系统的安全维护、运行保障

长久的电力监控系统安全与稳定，并不是侥幸，而是依赖于一系列细化、全面的安全维护与保障系统。高效安全防护工作，既要应付日常使用中的突发问题，也应对一旦发生的重大事故灾难。因此电力监控系统的安全保护工作，并不是静止的，而是持续性的，在每一个环节形成监控机制和保障机制。其中的持续监控机制需要完成对电力监控系统日常运行中监控每一个终端、每一个数据。依靠精良的监控系统，实现对系统运行状态的持续监控，一旦发生异常，可以及时报告并发出警戒，对系统进行自动修复。而这种持续性监控工作，并非安全防护的前置条件和准备，却是提高系统工作效率、有效性的重要保证。而另外一方面，防护系统并不能够放松对系统中潜在问题的防范，除了及时修复漏洞外，还需要定期排查系统漏洞，及时更新和修补系统漏洞，无法及时修复和补丁漏洞可能会让系统崩溃。因此，电力监控系统必须具备数据备份、灾备恢复等防护能力。数据是电力系统经营工作的“命脉”，一旦数据遭到破坏，甚至是丢失，整个电力系统可能会陷入瘫痪的状态，所以，系统需要有多重备份措施，定期将系统中的数据备份至独立存放数据的设备当中，在任何情况下，系统可以迅速恢复业务[6]。此外，灾难恢复系统快速启动机制能保证系统在运行过程中出现严重故障时，电力系统能以最快的速度重新运作起来，保障供电连续性。此外，安全培训与人员管理同样为电力监控系统长期安全运行中至关重要的环节。技术人员培训不仅要重视最新技术的掌握，还应重点强化对安全意识的培养。只有让每一个操作人员都提高自己的安全责任意识，才能进一步降低人为操作失误给系统安全带来的隐患。电力监控系统的安全管理并不仅仅是一项技术性工作，而是一项系统性工程，它不仅涉及设备更换等内容，还涉及人员管理，保证系统长期高效和稳定运行。

4 结束语

电力监控系统的主动防御技术架构为电力行业注入了新的生命力。面对日益复杂的安全挑战，主动防御不仅改变了传统的安全观念，还推动了电力系统向智能化、自动化的方向发展。通过系统内各个模块的协同作用与技术的不断迭代，电力监控系统将能够更高效地识别、应对潜在威胁，确保电力行业的稳定运行。然而，尽管我们在防御技术上取得了诸多进展，未来仍然需要在技术适配、系统协同等方面不断深化研究与探索。电力监控系统的主动防御不仅是技术的突破，更是对于电力安全的深度承诺。

参考文献

[1]李建明,张涛.电力监控系统安全防护技术研究[J].电力系统保护与控制,2020,48(23):102-109.

[2]王旭东,陈莉.电力监控系统中的网络安全问题与防御措施[J].电力自动化设备,2021,41(5):40-45.

[3]刘伟,赵明.基于主动防御的电力监控系统架构分析[J].电力工程技术,2019,38(4):56-61.

[4]孙亮,王国栋.电力监控系统信息安全防护策略的探讨[J].电力安全与环保,2020,36(2):44-47.

[5]陈鹏,李霞.电力监控系统中主动防御技术的应用研究[J].电力系统及其自动化学报,2021,33(10):124-130.

[6]周琳,李志宏.电力监控系统主动防御策略的技术框架探析[J].电力建设,2018,39(12):55-60.

作者简介：杨伟（1984-09），男，汉族，研究方向：电力。