电气二次设备继电保护与网络安全融合研究

翟艳坤

湖北能源集团襄阳宜城发电有限公司，湖北襄阳，441400；

摘要：电气二次设备是保障电力系统稳定运行的核心支撑要素，其运行状态直接关系电力系统的整体可靠性。继电保护作为电气二次设备的核心功能，其响应效率直接决定电力系统故障发生后的处置效果，能够快速隔离故障元件，有效避免事故范围进一步扩大。本文系统梳理电气二次设备继电保护与网络安全融合的核心需求，深入分析二者实现深度融合的关键技术方向，进而针对融合过程中的重点与难点，提出具有针对性的融合应用优化策略。通过上述研究工作，助力提升电气二次设备运行的稳定性与安全性，为电力系统的可靠供电提供坚实保障。

关键词：电气二次设备；继电保护；网络安全；技术融合

DOI：10.64216/3080-1508.26.02.048

引言

电力系统在社会能源体系中占据核心地位，承担着能源传输与电能供给的关键职能。其运行的稳定性与连续性，不仅关乎工业生产活动的正常开展，更与民生用电需求的满足密切相关。电气二次设备作为电力系统的“神经中枢”，在系统运行中发挥着监测与控制的核心作用，主要负责对电气一次设备的运行状态进行实时监测，并根据监测结果执行相应的控制操作。当前，电气二次设备的继电保护设计，多将重点聚焦于故障响应的速度与效率，以实现故障的快速隔离；而网络安全防护则多以风险隔离为核心目标，侧重阻断外部恶意攻击与内部异常访问。二者在设计理念与实施路径上缺乏统一的协同规划，难以形成防护合力，无法有效应对当前复杂多变的运行环境与安全风险。如何推动电气二次设备的继电保护与网络安全实现深度融合，构建“故障防护”与“网络防护”协同联动的安全体系，已成为保障电气二次设备可靠运行、维护电力系统整体安全的重要研究方向与实践课题。

1 电气二次设备继电保护与网络安全融合的核心需求

电气二次设备继电保护与网络安全的融合，并非简单的功能叠加，而是需始终围绕“保障继电保护功能可靠实现、有效抵御网络安全风险”两大核心目标展开。结合电气二次设备的运行特性、工作原理，以及电力系统对安全稳定的整体需求，可明确二者融合的三大核心需求，为后续融合技术的选择与应用提供清晰方向。

1.1 保障继电保护功能不中断

继电保护功能的核心目标，是在电力系统故障发生时实现快速响应与精准动作，因此，在与网络安全融合的过程中，需将保障继电保护功能不中断作为首要需求。一方面，所采取的各类网络安全防护措施，均不得对继电保护相关数据的实时传输造成负面影响。继电保护数据涵盖故障发生时的特征信息、设备控制指令等，此类数据对传输延迟具有严格要求，必须将延迟控制在预设的安全阈值范围内，否则将影响保护动作的及时性；另一方面，防火墙、入侵检测装置等网络安全设备，需具备“故障旁路”的核心能力。当网络安全设备自身出现故障或异常时，能够自动切换至旁路模式，不阻断继电保护信号的传输通道。

1.2 实现网络风险与故障的协同识别

在电气二次设备的实际运行过程中，存在一种关键问题：网络攻击行为（如恶意伪造故障指令、篡改监测数据）与电气设备实际故障，可能产生相似的数据特征。这种特征相似性极易导致运维人员或自动化系统产生误判，要么将网络攻击误判为设备故障，引发继电保护误动；要么将设备故障误判为网络攻击，导致继电保护拒动，二者均会对电力系统安全造成威胁。基于此，继电保护与网络安全融合的核心需求之一，便是实现网络风险与设备故障的协同识别。具体而言，需通过建立数据关联分析机制，整合继电保护与网络安全的监测数据，从数据特征、产生时序、关联设备等维度，区分“真实故障数据”与“恶意攻击数据”的本质差异；同时，需构建二者的联动预警机制，当继电保护装置监测到异常数据时，可实时向网络安全系统推送预警信息，网络安

全系统接收到预警后，立即启动风险排查流程，将排查结果（如是否存在攻击痕迹、攻击类型）反馈至继电保护装置，辅助继电保护装置精准判断是否启动保护动作，从而有效避免保护误动或拒动问题[1]。

1.3 兼顾数据共享与安全隔离

数字化背景下，电气二次设备需通过电力专用网络共享各类运行数据，这些数据包括设备实时运行状态、关键监测参数、故障历史记录等，其共享效果直接为电力系统的运维检修、调度决策提供数据支撑，是提升系统运行效率的重要基础。因此，继电保护与网络安全的融合，需兼顾数据共享效率与安全隔离效果，二者不可偏废。一方面，需构建专属的安全数据传输通道，针对继电保护相关数据的传输特点，采用专用的安全防护手段，确保数据在传输过程中不被篡改、不被窃取，保障数据的完整性与保密性；另一方面，需按照“分域防护”的原则，划分电气二次设备的安全区域，将承担继电保护核心功能的设备（如保护装置、测控装置）与非核心设备（如辅助监测终端）划分至不同安全区域，通过设置访问控制策略，限制无关网络与非授权设备的访问权限，既满足电力系统对数据共享的实际需求，又从空间隔离层面降低网络安全风险。

2 电气二次设备继电保护与网络安全融合的关键技术方向

基于上述继电保护与网络安全融合的核心需求，需依托电力行业专用的技术手段，实现二者的深度协同与功能融合。技术应用需重点聚焦数据传输、风险识别、设备防护三大核心环节，形成相互支撑、相互联动的技术体系，确保融合需求能够有效落地，保障融合效果。

2.1 安全化数据传输技术

安全化数据传输技术是实现继电保护与网络安全融合的基础技术，其核心目标是同时保障继电保护数据传输的实时性与安全性，解决“安全防护与传输效率”的协同问题。在具体技术应用中，一方面，需采用电力行业专用的加密协议，该协议需适配继电保护数据的传输速率与格式要求，对继电保护的故障指令、实时监测数据等核心数据，实施端到端的加密处理，从数据源头到接收终端全程加密，防止数据在传输链路中被恶意篡改或非法窃取，保障数据安全；另一方面，需在数据传输网络中引入优先级传输机制，明确各类数据的传输优先级，将继电保护相关数据设定为最高传输优先级。当网络出现拥堵、数据传输压力增大时，网络系统可优先保障继电保护数据的传输通道畅通，优先分配传输带宽，避免因网络拥堵导致继电保护数据传输延迟，影响保护动作效率，最终实现“安全加密”与“实时传输”的协同统一。

2.2 故障与风险协同识别技术

故障与风险协同识别技术是解决“故障与攻击误判”问题的核心技术，其核心是建立一套融合继电保护与网络安全数据的联动识别模型，实现异常原因的精准判断。技术实施路径主要分为两步：第一步是嵌入协同识别算法，在继电保护装置与网络安全设备（如入侵防御系统、安全审计设备）中，均嵌入统一的协同识别算法，确保二者能够实现数据的互通与分析逻辑的统一；第二步是整合数据并关联分析，通过算法整合两类设备的监测数据——继电保护装置提供设备故障相关的特征数据，如电流异常波动、电压骤降骤升等；网络安全设备提供网络风险相关的特征数据，如异常 IP 访问、指令格式异常、数据篡改痕迹等；协同识别算法对两类数据进行关联分析，结合预设的判断规则，精准识别异常原因是电气设备实际故障还是网络恶意攻击，随后将识别结果（如故障类型、攻击来源）推送至电力系统运维管理平台，为运维人员后续的故障处置或风险阻断提供精准依据，避免因误判导致的保护误动或安全漏防[2]。

2.3 嵌入式安全防护技术

嵌入式安全防护技术聚焦于电气二次设备自身，实现“继电保护功能”与“安全防护功能”的硬件级融合，从设备本体层面提升安全防护能力，避免安全防护功能与保护功能的相互干扰。技术核心实施方式为：在继电保护装置的硬件设计阶段，便在装置内部嵌入专用的安全芯片，该芯片需具备独立的运算能力与存储能力，集成入侵检测、病毒防护、异常行为拦截等核心安全防护功能；安全芯片可实时监测继电保护装置的运行状态，包括程序运行完整性、数据读写合法性、外部指令接入安全性等，当发现恶意代码注入、非法操作、异常指令写入等风险行为时，可立即启动本地防护机制，快速阻断攻击行为，同时确保该过程不影响继电保护核心功能的正常运行

3 电气二次设备继电保护与网络安全融合的优化策略

为推动上述关键技术在实际场景中落地应用，进一步提升继电保护与网络安全的融合效能，解决融合过程中可能出现的体系断层、运维脱节、技术滞后等问题，

需从体系设计、运维管理、技术升级三个维度，制定针对性的优化策略，保障二者融合后的系统能够长期可靠运行[3]。

3.1 构建协同化融合体系

构建协同化融合体系的核心，是打破继电保护与网络安全“各自独立设计、各自分散实施”的传统模式，实现二者从规划到落地的全流程协同。在电气二次设备的前期规划阶段，需将继电保护功能设计与网络安全防护设计纳入统一的规划方案中，同步开展需求分析、方案论证与细节设计，避免后续出现功能冲突或接口不兼容问题；同时，需在方案中明确继电保护装置与网络安全设备的协同接口标准与联动响应机制，确保二者能够实现数据无缝互通与指令快速交互；此外，需统一两类设备的数据采集标准、数据格式标准与数据传输协议，消除因数据标准不统一导致的融合断层问题，最终实现“设计阶段协同”与“运行阶段数据协同”的双重目标，构建完整的协同化融合体系。

3.2 完善常态化运维机制

常态化运维机制是保障继电保护与网络安全融合效果的关键，需打破“继电保护运维与网络安全运维各自为战”的局面，建立“继电保护+网络安全”一体化协同运维机制。首先，需提升运维人员的综合能力，要求运维人员不仅熟练掌握继电保护的工作原理、调试方法与故障处置流程，还需具备网络安全风险识别、漏洞排查、攻击处置等专业知识，能够应对融合后的复杂运维场景；其次，需制定统一的定期巡检制度，运维人员开展巡检工作时，需同时检查两方面内容：一是继电保护功能的可靠性，包括保护定值准确性、动作逻辑正确性、信号传输及时性等；二是网络安全风险，包括安全设备运行状态、防护策略有效性、数据传输安全性等，确保隐患能够早发现、早处置；最后，需制定协同处置预案，针对可能出现的“故障叠加攻击”“保护误动关联安全风险”等复杂场景，明确运维人员的处置流程、职责分工与联动方式，当故障或攻击发生时，运维人员可同步开展继电保护动作核查与网络安全风险阻断，大幅提升处置效率，避免因各自为战导致的处置延迟或处置遗漏。

3.3 推动技术动态升级

随着电力系统数字化程度不断提升，网络运行环境呈现出动态变化特征，新型网络攻击手段（如定向攻击、APT 攻击）也不断涌现，继电保护与网络安全融合所依赖的技术，若长期保持不变，极易出现技术滞后问题，无法应对新的风险挑战。因此，需建立技术动态升级机制，推动融合相关技术持续适配新需求、新风险。一方面，需定期对融合系统中的核心技术组件进行更新升级，包括电力专用加密协议、故障与风险协同识别算法、嵌入式安全芯片的防护功能等，确保这些技术能够适配新型网络攻击手段与电气二次设备的升级需求；另一方面，需建立行业技术标准跟踪机制，实时关注电力行业关于继电保护、网络安全的最新技术标准与规范要求，及时根据标准更新调整融合方案中的技术选型与实施细节，确保融合技术与行业规范保持同步，避免因技术不符合规范要求导致的安全隐患，或因技术滞后导致的保护效能下降问题。

4 结语

电气二次设备继电保护与网络安全的深度融合，是电力系统顺应数字化转型趋势的必然要求，也是提升电力系统整体安全防护能力的核心路径。二者通过协同联动，可实现“电力故障快速防护”与“网络安全风险抵御”的双重保障，弥补单一防护的不足。通过明确“保障保护功能不中断、实现风险与故障协同识别、兼顾数据共享与安全隔离”三大核心融合需求，依托安全化数据传输、故障与风险协同识别、嵌入式安全防护等关键技术，再辅以协同化融合体系构建、常态化运维机制完善、技术动态升级推进等优化策略，可构建起完善、可靠的继电保护与网络安全融合体系。该融合体系能够有效提升电气二次设备运行的稳定性与安全性，从根本上避免因继电保护功能失效或网络安全攻击引发的电力系统事故，为电力系统的可靠供电、持续运行与能源安全提供坚实且有力的支撑。

参考文献

[1]黄永杰,林金燕.电气自动化技术在电气工程中的应用研究[J].工业建筑,2022,52(6):234.

[2]钟自强,武亮,张天恒,等.平面二维时栅位移传感器电气系统设计[J].重庆理工大学学报(自然科学),2022,36(5):128-136.

[3]何光树.大理地区电网二次回路与系统状态检修研究[D].昆明:昆明理工大学,2021.