基于自动化的电气工程安全防护技术研究

杨　博
葫芦岛市中心医院　辽宁葫芦岛　125000

摘　要：本文针对传统电气安全防护在实时性与智能化方面的不足，探讨自动化技术赋能下的解决方案。研究系统梳理了电气安全防护的基础理论与标准体系，分析了自动化技术的核心作用与关键技术，进而构建了基于分层分布式架构的自动化防护系统设计框架，并提出了相应的评估方法与优化策略。通过典型工程案例验证，本研究表明，深度融合感知、分析与控制功能的自动化体系，能有效实现从被动响应到主动预警与自适应防护的范式转变，显著提升电气系统的安全性与可靠性。

关键词：自动化技术；电气工程；安全防护；主动防御体系

引言

随着电气系统规模与复杂度不断提升，传统安全防护手段已难以满足实时性、精准性要求。自动化技术通过智能监控、故障诊断与快速隔离，为电气工程安全防护提供了新的解决方案。本文在梳理电气安全防护标准与技术体系的基础上，重点研究自动化技术在电气安全防护中的关键作用，设计集成监测、分析与控制的自动化防护系统，并通过评估方法与案例验证其有效性，以提升电气系统的安全防护水平与智能化程度。

1 电气工程安全防护基础理论

1.1 电气安全防护概述 [1]

电气安全防护的核心目标在于通过技术与管理的综合措施，保障人员、设备及电力系统的安全。传统防护主要依赖物理隔离与继电保护等静态手段。随着电力系统数字化、网络化程度的加深，安全威胁已从单纯的物理设备故障，演变为信息层与物理层相互交织的复杂风险，防护范围需扩展至信息物理系统的协同防护。这要求防护体系必须具备更强的实时性、自适应性及预测能力，从而为后续引入自动化、智能化的主动防护技术奠定了需求基础。

1.2 电气工程安全防护标准

电气工程安全防护标准是构建系统化安全屏障、指导技术实施的法定依据与规范框架。国际上，IEC（国际电工委员会）制定的系列标准（如 IEC 60204 机械电气安全标准）与 IEEE 相关标准构成了技术基准。国内体系则以国家强制性标准（如 GB 系列）为核心，例如《GB/T 13955–2017 剩余电流动作保护装置安装和运行》明确了漏电保护的具体要求，行业标准作为补充。这些标准共同规定了设备安全、操作规范、系统设计与测试方法，确保了防护技术的合规性与互操作性，也为自动化安全系统的功能设计、性能评估提供了必须遵循的准则和量化指标。

1.3 电气工程安全防护技术分类

根据防护原理与作用阶段，电气工程安全防护技术可分为三大类。其一为故障前预防性防护，包括绝缘、间距、安全电压、电气隔离等基础措施，旨在消除或减少危险源。其二为故障时保护性防护，如接地与接零保护、过电流与漏电保护（通过断路器、熔断器、RCD 实现），核心是快速检测并切断故障回路。其三为综合性与主动性防护，涉及联锁、安全标志、监测预警系统等，强调多技术协同与事前预警。随着自动化与智能化发展，防护技术正从传统的被动、静态隔离，向集成实时监测、智能诊断与自动控制的主动、自适应防护体系演进，为后续章节讨论自动化技术深度应用奠定基础。

1.4 自动化技术在电气安全防护中的应用

自动化技术是实现电气工程主动性综合防护的关键。其应用体现在三个层面：在系统级控制上，集成的电力管理系统（PMS）可实现毫秒级的快速负荷投切、自动恢复供电等操作，极大提升了系统应对突发事件的稳定性与可靠性 [2]；在设备状态监测上，多传感器融合技术（如压力、位移传感器）能对保护压板等关键设备进行智能监测，显著提高了操作准确性与可靠性；在故障智能识别上，基于红外成像与机

器学习的算法能自动诊断过电压保护设备故障，而融合多元数据的模型则能高精度、低延时地识别微电网开关误操作。这些技术共同推动了安全防护从事后被动响应向事前预测与实时自适应拦截的深刻转变。

2 基于自动化的电气工程安全防护技术

2.1 自动化技术概述 [2]

自动化技术是一门综合性技术，其核心在于使机器、设备或生产管理过程在无需或仅需较少人工干预的情况下，能自动执行检测、信息处理、分析判断与操纵控制，以达成预定目标。该技术深度整合了控制理论、计算机技术、传感技术与通信技术，其发展经历了从经典控制理论、现代控制理论到当前融合人工智能与大系统理论的智能化阶段。在电气工程领域，自动化构成了从底层设备感知、过程控制到上层系统调度管理的完整技术体系。它通过构建“感知 – 决策 – 执行”的闭环，将传统静态、被动的安全防护范式，转变为具备实时监测、智能诊断与自主响应能力的动态主动防御体系，为提升电力系统的安全性、可靠性与运行效率奠定了根本性的技术基石。

2.2 自动化技术在电气工程安全防护中的作用

自动化技术在电气工程安全防护中扮演着核心赋能角色，其作用主要体现在三个层面。在感知与预警层面，它通过集成各类传感器与在线监测装置，实现了对电气参数、设备状态与环境信息的7x24小时不间断实时采集与异常捕捉，将防护关口从事后处置大幅前移至事前预警。在诊断与决策层面，借助嵌入式系统与边缘计算，能够对采集的海量数据进行就地快速分析与智能诊断，精准定位绝缘劣化、接触不良等早期隐患或瞬时故障，替代传统依赖人工经验的判断。在执行与控制层面，最终通过联动继电保护装置、智能断路器及电源控制系统，实现故障区域的毫秒级自动隔离、负荷的快速转供或运行方式的自适应调整，从而构成一个“实时感知、智能研判、精准控制”的闭环主动防护体系，全面提升系统可靠性。

2.3 自动化技术的关键技术 [2]

构建基于自动化的电气安全防护体系，依赖几项贯穿“感知 – 传输 – 分析 – 控制”闭环的关键技术。在感知层，多传感器融合技术是基础，它通过集成压力、位移等多种传感器，实现对设备状态的全方位精准监测。在通信与数据层，确保海量监测数据实时、安全传输的网络技术至关重要。在核心分析决策层，人工智能算法（如用于特征提取与模式识别的机器学习模型）发挥着大脑作用，能对复杂故障进行智能诊断。最终在执行控制层，可靠的可编程逻辑控制器（PLC）与智能继电保护装置负责准确执行分析结果，完成故障隔离或参数调整。这些技术共同构成了实现实时预警、智能研判与精准控制的主动防护体系的技术基石。

3 电气工程安全防护自动化系统的设计

3.1 自动化系统设计原则 [3]

基于自动化的电气工程安全防护系统设计，遵循一套以保障系统整体安全与效能为核心的原则。首先，安全可靠性是设计的首要原则，要求系统在任何工况下都能确保人身与设备安全，这通常通过冗余设计（如硬件、通信冗余）和故障安全模式来实现。其次，设计需遵循功能性、实时性与可扩展性的平衡。系统必须具备明确的输入 / 输出功能和满足故障快速隔离的实时响应能力，同时采用模块化架构以适应未来功能的扩展需求。此外，人机协同与规范性也至关重要，设计应考虑人机交互的清晰性，并严格遵循国家和行业相关安全标准与设计规范，确保系统设计的合规性与工程实践的规范性。

3.2 自动化系统架构

典型的基于自动化的电气安全防护系统通常采用分层分布式架构。该架构自下而上可分为现场设备层、控制层与系统管理层。现场设备层由各类传感器（如电流、温度传感器）、智能断路器和保护装置构成，负责实时数据采集与最终控制命令执行。控制层以 PLC、智能保护单元或专用控制器为核心，承载着系统的“大脑”功能，负责运行保护算法、进行逻辑判断并发出控制指令。系统管理层则提供集中监控、数据分析、报警管理和人机交互界面。各层级之间通过工业以太网、现场总线等可靠网络进行数据交互，确保指令与状态信息的实时、准确传输，从而实现从精准感知到快速执行的闭环安全防护。

3.3 关键组件与技术选择

在构建自动化安全防护系统时，关键组件的选型与技术路径的确定直接决定了系统效能。在硬件层面，核心包括：高精度、高可靠性的感知组件（如非接触式电流传感器、温度传感器及局部放电检测装置），用于精确采集关键状态量；高性能、高可靠性的控制与执行组件（如具备高速逻辑处理能力的 PLC、集成保护功能的智能继电器及快速真空断

路器），负责算法执行与故障快速隔离；以及高实时性、高抗干扰的通信网络组件（如工业以太网、PROFINET 或 IEC 61850 标准协议设备），确保信息实时可靠传输。在软件与平台层面，则需要选择或开发集成实时数据库、智能分析算法（如故障诊断模型）及可视化监控平台的软件系统。技术选择必须严格遵循可靠性、实时性、开放性与经济性相平衡的原则，并确保所有组件符合相关电气安全标准，以实现整个防护体系的最优配置与稳定运行。

4 基于自动化的电气工程安全防护技术评估与优化

4.1 安全防护技术评估方法

对基于自动化的电气安全防护技术进行评估，需建立一套系统化、多维度的综合评估体系。该体系首先需涵盖功能性、可靠性与经济性三大核心维度。具体评估通常采用定量与定性相结合的方法，包括：基于性能指标的定量评估，如通过故障识别准确率、保护动作速度（毫秒级）、系统可用性（如 MTBF）等硬性指标衡量其技术效能；仿真与模拟测试，在接近真实的数字孪生或 RTDS 仿真环境中验证系统在各类预设故障与极端工况下的响应性能；以及现场试点与对比分析，通过在实际工程中与传统防护方案的对比，综合评价其提升安全性、可靠性及经济性的实际效果。这一评估过程为后续的性能优化与技术迭代提供了科学的决策依据。

4.2 自动化安全防护技术的性能评估

自动化安全防护技术的性能评估，聚焦于量化其在实际运行中的效能、可靠性及边界。其核心在于通过关键性能指标（KPIs）进行精确度量，主要包括：①保护效能指标，如故障识别准确率、动作正确率；②时效性指标，如从故障发生到发出指令的全过程响应时间（通常要求毫秒级）；③可靠性指标，如系统 / 设备的平均无故障时间（MTBF）以及在干扰下的误动率与拒动率。评估方法结合实验室测试（验证基础功能）、数字仿真（模拟复杂故障场景）与现场试点运行（考核长期稳定性），综合分析其在常态与极端工况下的表现，为技术优化与选型提供核心数据支撑。

4.3 安全防护技术优化策略

安全防护技术的优化是一个基于性能评估结果的闭环迭代与深度协同过程。优化策略主要沿三个方向展开：首先是参数与算法的精准调优，依据评估中发现的误动、拒动或响应延迟等问题，对保护定值、故障识别算法的阈值与模型参数进行修正，并引入更先进的机器学习算法以提升诊断精度。其次是系统架构与可靠性的增强，通过在关键路径部署硬件冗余、改进通信协议与抗干扰设计来提升系统整体可用性。再者是人机交互与运维策略的优化，完善预警信息的清晰度与分级，并基于设备状态监测数据推动定期检修向预测性维护转变。最终，这些策略旨在使防护系统具备持续的自适应与自学习能力，实现动态最优防护。

4.4 案例分析：自动化技术在特定电气工程中的应用与优化 [4]

本节以超高压变电站保护压板状态监测与高比例分布式光伏接入的主动配电网为典型案例，分析自动化技术的具体应用与优化路径。在变电站场景中，针对传统人工投退保护压板存在的效率与误操作风险，基于多传感器（压力、位移、微动开关）融合与模糊逻辑推理的智能监测系统被设计与应用，实现了压板状态的实时、准确监测，将相关操作的准确性与可靠性提高了 50% 以上。在主动配电网场景中，为应对海量分布式资源带来的模型不准、控制实时性差等挑战，建立了基于机器学习的“集群自律 – 电网协同”分层调控体系。该体系通过数据驱动的在线反馈优化、升维动态建模以及安全强化学习等方法，实现了在弱模型依赖下的分布式资源集群自律运行、动态主动支撑及配电网风险量化概率调度，显著提升了系统应对随机波动的安全性与经济性。上述案例表明，自动化技术的深度应用正推动电气安全防护从单点、被动响应向系统化、主动预测与自适应协同控制演进。

5 结论与展望

本研究系统构建了基于自动化的电气工程安全防护技术体系。研究成果主要体现在三个方面：一是深化了自动化技术与传统电气安全理论的融合，明确了其在构建主动防御体系中的核心作用；二是系统梳理并集成了从智能感知、数据分析到精准控制的关键技术，提出了分层分布式系统架构及设计原则；三是建立了结合定量性能指标与案例的评估优化方法。然而，研究仍存在局限，如部分前沿技术（如数字孪生、高级人工智能算法）的工程化应用成熟度有待验证，跨系统协同防护的标准化不足。未来展望集中于推动防护体系向全状态感知、智能预测与自适应协同控制的更高阶段发展，并加强信息物理深度融合背景下的跨域安全标准建设。

参考文献：

[1] 杨杰，郭逸豪，郭创新，等 . 考虑模型与数据双重

驱动的电力信息物理系统动态安全防护研究综述 [J]. 电力系统保护与控制，2022, 50(7): 176–187.

[2] 杨浩，孙鑫，陈晨 . 多传感器融合的保护压板投退智能监测系统设计 [J]. 电气工程与自动化，2025, 52(897): 4–8.

[3] 徐青 . 控制系统工程设计中的方法论研究 [J]. 自动化仪表，2010, 31(10): 5–8.

[4] 吴文传，蔺晨晖，孙宏斌，等 . 基于机器学习的主动配电网能量管理与运行控制 [J]. 电力系统自动化，2024, 48(20): 2–11.

作者简介：杨博（1992.04—），女，汉族，辽宁省葫芦岛市，本科，中级工程师，研究方向：电气工程及其自动化。