Volume 1 (Issue 3: July- October, 2025): Pages 14-25 | https://www.swamivivekanandauniversity.ac.in/jrtee/
Published on November 16, 2025

ISSN: 3049-382X (Online)
Journal of Recent Trends of Electrical Engineering
contents available at: https://www.swamivivekanandauniversity.ac.in/jrtee/

Integration of AI in Modern Protection Schemes: Challenges, Limitations, and Prospects

Suvraujjal Dutta , MAKAUT, Haringhata, Nadia, India

Abstract

The transformation of power systems—driven by renewable integration, deregulated markets, digital substations, and distributed energy resources (DERs)—has challenged traditional protection mechanisms. Fixed threshold-based relays often fail to address dynamic grid conditions, uncertain fault currents, bi-directional power flows, and evolving grid topologies. Artificial Intelligence (AI) has emerged as a promising solution due to its ability to learn nonlinear relationships, process real-time data, and enable adaptive decision-making. This paper presents a comprehensive analysis of AI integration in modern power system protection before 2021, discussing key techniques, capabilities, challenges, and implementation barriers. The limitations relating to data requirements, interpretability, cybersecurity, compatibility with legacy infrastructure, generalization, and regulatory issues are critically examined. A set of research directions is proposed based on hybrid AI–physical models, explainable AI (XAI), PMU-driven dynamic protection, and AI-enabled Digital Twin technologies. This review aims to bridge the gap between theoretical advancements and practical deployment of AI-based protection systems.

Keywords

Artificial Intelligence (AI), Power System Protection, Fault Detection, Adaptive Relaying, Smart Grid, Machine Learning, PMU-Based Protection, XAI, Digital Twin.

1. Introduction

Power systems are evolving from static, centrally controlled networks to dynamic cyber-physical energy ecosystems. The increasing presence of renewable energy sources, inverter-based generators, microgrids, and active distribution networks introduces complexity into fault behaviour and protection coordination. Traditional protection schemes rely on predefined settings, impedance calculations, and deterministic logic. Such approaches are insufficient under modern grid conditions, particularly during non-classical faults, uncertain fault currents, and frequent topology changes. Furthermore, the transition towards decentralized generation and bidirectional power flows has significantly challenged conventional relay coordination strategies. Fault signatures in inverter-dominated networks often lack characteristic current magnitudes, making threshold-based protection increasingly unreliable. Additionally, fluctuations in power availability, rapid changes in load demand, and integration of intermittent renewable sources produce dynamic operating states where static relay settings become inadequate. These issues highlight the need for intelligent and adaptive protection frameworks capable of learning from data, responding autonomously to disturbances, and evolving with system conditions. The emergence of advanced metering infrastructure (AMI), Phasor Measurement Units (PMUs), and Intelligent Electronic Devices (IEDs) has enabled high-resolution data collection from substations and transmission networks. These devices generate synchronized and time-stamped data that capture the transient behaviour of power systems with greater fidelity. AI and Machine Learning (ML) methods can utilize this data for real-time fault identification, high-impedance fault detection, predictive decision-making, and adaptive relay settings. Signal processing techniques such as Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA), when combined with ANN, SVM, or Deep Learning models, have demonstrated substantial potential in identifying fault patterns and improving diagnostic accuracy. However, practical adoption remains limited due to concerns involving reliability, interpretability, data scarcity, cybersecurity risks, and regulatory compliance. AI-based models often operate as “black boxes,” which restricts utility acceptance because protection systems must provide fully explainable and auditable decisions. Moreover, integrating AI with existing substation infrastructure requires compatibility across communication protocols, hardware platforms, latency constraints, and protection response times. Regulatory frameworks also demand extensive testing, validation, and certification before deployment, which further delays implementation. Research progress prior to 2021 was promising but largely confined to simulation environments and laboratory prototypes. Most publications demonstrated accuracy in fault diagnosis but lacked deployment strategies for real-world conditions were inconsistent measurements, incomplete datasets, and communication failures are common. Field data variability, PMU noise, and representativeness issues present significant challenges to building robust AI models that generalize well across operating scenarios.

In this context, this paper presents a comprehensive review of AI-based protection methodologies developed before 2021, outlining their capabilities, limitations, and applicability to practical systems. Emphasis is placed on fault classification, high-impedance fault detection, adaptive relaying, PMU-based dynamic protection, and hybrid AI–physics-driven models. A structured analysis of challenges and prospects is provided, with emphasis on strategies to enable practical implementation—such as explainable AI, Digital Twin

validation environments, interoperability frameworks, and standardized testing protocols. By bridging the gap between theoretical advancements and operational deployment, AI-driven protection can support the development of future **s**elf-healing, resilient, and adaptive power systems capable of addressing the challenges of a decentralized and data-driven energy landscape.

2. Evolution of Protection Systems

2.1 Conventional and Numerical Protection

Traditional power-system protection schemes primarily rely on overcurrent, distance, differential, and directional relays, each designed to detect specific fault signatures based on well-established analytical criteria. These electromechanical and static relays operate using fixed pickup values, time–current characteristics, and zone settings, which require periodic manual tuning to match evolving grid conditions. While they are robust and widely deployed, their inability to dynamically respond to system disturbances—such as rapid load fluctuations, increased penetration of renewable sources, or changes in network topology—poses limitations in modern grids. The introduction of numerical relays marked a major technological shift by incorporating microprocessors, digital signal processing (DSP), and advanced filtering algorithms. Numerical relays significantly improved selectivity, computation speed, self-diagnostics, and event recording capabilities. Their ability to process sampled values, perform real-time phasor estimation, and integrate multiple protection functions within a single device enhanced both efficiency and reliability. Nevertheless, numerical relays still operate fundamentally on predetermined thresholds and logic structures. Even though setting groups and adaptive elements exist, they cannot fully adjust to sudden and unpredictable grid changes without manual intervention or predefined rules. This makes them less effective in highly dynamic systems with distributed energy resources (DERs), inverter-based power plants, and bidirectional power flows, where fault signatures are often non-traditional and variable.

As power systems migrate toward increased decentralization and variability, the limitations of both conventional and numerical protection methods become more apparent. These challenges are driving interest in adaptive, communication-assisted, and data-driven protection philosophies that can autonomously modify settings, learn fault patterns, and respond to evolving operating conditions in real time.

2.2 Smart Grid and Advanced Protection

The transition toward smart grids have fundamentally changed the requirements of protection systems, necessitating solutions that are adaptive, communication-enabled, and data-driven. Modern power networks are increasingly characterized by high penetration of distributed energy resources (DERs), inverter-based generation, electric vehicles (EVs), and other non-linear, power-electronic-dominated loads. These elements introduce variability in fault currents, alter system inertia, and often produce fault signatures that differ significantly from those encountered in conventional synchronous-generator-based systems. As a result, traditional deterministic protection strategies, designed around predictable current magnitudes and symmetrical fault conditions, often struggle to maintain sensitivity and selectivity.

Advanced protection frameworks in smart grids leverage wide-area measurement systems (WAMS), phasor measurement units (PMUs), and high-speed communication channels to achieve coordinated decision-making across multiple protection zones. This allows relays to access real-time system information, enabling dynamic adjustment of settings, self-adaptation to network reconfigurations, and improved situational awareness under stressed operating conditions. Artificial intelligence (AI) and machine learning (ML) have emerged as key enablers of next-generation protection. AI-based protection schemes utilize data-driven models capable of learning complex patterns in system disturbances and differentiating between normal, transient, and fault conditions. Techniques such as artificial neural networks (ANNs), support vector machines (SVMs), decision trees, random forests, and deep learning models have been applied for fault classification, fault location, and event prediction. These approaches can process high-dimensional data, handle non-linear relationships, and adapt to evolving operating conditions without requiring manual recalibration. Importantly, they offer potential resilience against the variability and uncertainty introduced by DERs.

However, the adoption of AI-based protection also introduces new challenges. These include the need for large and high-quality training datasets, robustness against cyber threats, explain ability of decision-making processes, and the reliability of ML models under unseen or abnormal scenarios. Despite these concerns, AI-driven protection systems represent a promising direction toward achieving fully adaptive, autonomous, and resilient smart-grid protection strategies.

2.3 Motivation for AI Integration

The deployment of artificial intelligence within modern protection systems is driven by several critical needs associated with increasingly complex and dynamic power networks:

Real-time decision-making:

As modern grids operate closer to their stability limits, protection systems must process large volumes of data and react almost instantaneously to disturbances. AI algorithms—particularly those optimized for streaming data and edge computation—enable faster detection, classification, and response compared to rule-based or threshold-driven methods. This is especially important in systems with rapid changes caused by inverter-based resources, where fault characteristics evolve within milliseconds.

Enhanced fault detection accuracy:

Traditional protective relays rely on fixed pickup currents and predefined logic, which can lead to disoperation in networks experiencing distorted waveforms, harmonics, or low fault currents. AI-based models can analyse complex patterns in voltage and current signals, improving the accuracy of fault classification, distinguishing between internal and external faults, and detecting high-impedance or evolving faults that conventional relays often miss.

Adaptation to grid dynamics:

With increasing integration of DERs, micro grids, and flexible loads, grid characteristics such as fault levels, power flow directions, and inertia become highly variable. AI models can adapt to these changes in near real time by learning from operational data, enabling self-tuning protection schemes that remain reliable even under fluctuating or uncertain conditions.

Reduced reliance on manual relay coordination:

Traditional coordination of protection settings requires extensive offline studies, periodic adjustments, and manual intervention to accommodate network modifications. AI-driven tools

can automate coordination studies, continuously optimize settings, and predict future operational scenarios. This reduces human error, speeds up engineering processes, and supports scalable protection strategies for large, decentralized power systems.
Improved resilience during cyber-physical disturbances:
As smart grids become more interconnected, they face heightened risks from cyberattacks, data corruption, and coordinated attacks that target both physical and communication infrastructure. AI techniques—such as anomaly detection models, graph-based cyber monitoring, and data-driven intrusion detection—can identify abnormal patterns, recognize stealthy cyber threats, and support resilient protection actions. This dual-layer defines enhances overall system stability and reliability.

3. AI Techniques Used in Protection Schemes

AI Technique	Application in Protection
ANN	Fault classification, high-impedance fault detection
SVM	Multi-class fault classification
Decision Trees	Relay coordination, fault location
Fuzzy Logic	Adaptive relaying under uncertainties
Deep Learning	Pattern recognition using raw waveforms
Hybrid AI–Signal Processing	Improved fault diagnosis using DWT + ANN
Reinforcement Learning	Adaptive settings in changing networks

Table 1: AI Techniques Used in Protection Schemes

Among these, ANN and SVM emerged as the most widely used methods prior to 2021. Deep learning was in its early research phase, with limited real-time field implementations due to computational demands.

4. Applications of AI in Power System Protection

4.1 Fault Detection and Classification

AI-based classifiers significantly enhance the capability of protection systems to accurately identify fault types, faulted phases, and fault inception times by analysing current, voltage, or traveling-wave signals. Machine learning models such as Artificial Neural Networks (ANNs), Support Vector Machines (SVMs), Random Forests, and Convolutional Neural Networks (CNNs) have demonstrated high accuracy in controlled simulation environments. They excel at capturing nonlinear features and subtle waveform distortions that traditional relays overlook. However, these models often exhibit limitations in data generalization when confronted with real-world disturbances, noise, or previously unseen grid operating conditions. Ongoing

research focuses on domain adaptation, transfer learning, and synthetic data generation to address these generalization challenges.

4.2 High-Impedance Fault (HIF) Detection

Traditional overcurrent and distance relays often fail to detect high-impedance faults due to low, fluctuating, or distorted fault currents that resemble normal load variations. AI techniques improve detection by extracting weak features through time–frequency analysis tools such as the Wavelet Transform, Hilbert–Huang Transform, and Empirical Mode Decomposition. Once meaningful features are extracted, classifiers such as ANNs, SVMs, fuzzy logic systems, or deep learning architectures identify anomalous patterns indicative of HIFs. Recent studies also explore graph-based neural networks and ensemble learning to improve robustness against noise and measurement uncertainty.

4.3 Adaptive Relaying

AI enables adaptive protection schemes where relay settings dynamically adjust in response to real-time changes in load levels, DER outputs, or network reconfigurations. Reinforcement Learning (RL) approaches, including Q-learning and Deep Reinforcement Learning (DRL), have shown promise in autonomously determining optimal protection settings by learning from system behaviour over time. These methods can theoretically reduce disoperation during abnormal or rapidly changing grid conditions. However, the lack of large-scale field validation, challenges in ensuring stable training, and cybersecurity concerns limit current deployment. Hybrid approaches integrating rule-based logic with AI-driven adaptation are gaining attention as more practical solutions.

4.4 Fault Location Estimation

AI enhances the accuracy of fault location, especially in complex transmission and distribution networks with distributed generators. Hybrid techniques combining Discrete Wavelet Transform (DWT) with machine learning models such as ANNs, SVMs, or Long Short-Term Memory (LSTM) networks improve the precision of locating the faulted section by capturing transient behaviour and extracting multiresolution features. These models can effectively handle faults occurring under varying load conditions, different fault resistances, and communication delays in wide-area measurement systems. Recent developments also explore PMU-based data fusion and physics-informed neural networks (PINNs) for more reliable fault location under low-inertia grid conditions.

5. Challenges and Limitations

5.1 Data Scarcity and Quality Issues

AI models require large volumes of labelled, diverse, and high-resolution fault data to achieve reliable performance. In real power systems, faults occur infrequently, making it difficult to gather representative datasets under varied operating conditions. Simulated data, although useful, cannot fully capture real-world noise, equipment aging effects, evolving load patterns,

inverter-based distortions, or communication delays. Additionally, PMU and IED measurements may suffer from synchronization errors, missing samples, and harmonic interference, which degrade the quality of training datasets. Ensuring standardized, high-quality data pipelines remains a major challenge.

5.2 Black-Box Nature and Lack of Trust

Many AI models—particularly deep learning, LSTMs, CNNs, and ensemble methods—operate as "black boxes," offering limited insight into how decisions are made. This poses a barrier in protection engineering, where deterministic and transparent logic is mandatory to ensure system safety, comply with regulatory standards, and enable post-event analysis. The lack of interpretability limits engineer confidence, complicates certification processes, and creates concerns about unknown failure modes. Research into explainable AI (XAI) for protection is emerging but still not mature enough for widespread deployment.

5.3 Generalization and Overfitting

AI models often exhibit strong accuracy on training datasets but struggle to generalize to unseen or rare operating conditions, such as unusual DER configurations, evolving fault resistances, or atypical transient events. Overfitting remains a persistent challenge, especially when training datasets are limited or biased. Continuous retraining and periodic validation are required to maintain performance, increasing operational complexity. Moreover, rapid changes in grid characteristics due to DER integration can quickly render pre-trained models obsolete.

5.4 Cybersecurity Concerns

AI-based protection frameworks rely heavily on communication networks, cloud platforms, edge computation, and remote data exchange. This dependency introduces new attack surfaces. Potential cyber threats include spoofing of sensor measurements, false data injection attacks (FDIAs), adversarial machine learning attacks, data poisoning during training, and denial-of-service (DOS) attacks targeting communication links. Since protection decisions must be made rapidly and reliably, even minor data integrity compromises can lead to relay disoperation or system instability. Ensuring secure, authenticated, and tamper-proof data pathways is therefore essential.

5.5 Legacy Infrastructure and Integration Issues

A significant portion of global substations still employ electromechanical or early-generation numerical relays. Integrating AI-enabled protection systems into these legacy infrastructures requires extensive retrofitting, hardware upgrades, and interoperability assessments. Communication protocols may not support high-frequency data streams, and many old systems lack the computational capacity to process AI-based algorithms. These constraints create economic and logistical barriers for utilities, especially in developing regions where modernization budgets are limited.

5.6 Computational Burden

Real-time protection requires decision-making within millisecond-scale windows. Highly complex AI and deep learning models—such as transformer-based networks or deep CNNs—often require significant computational power, making them difficult to deploy without specialized hardware like FPGAs, GPUs, or edge accelerators. Even when hardware is available, model latency, memory requirements, and energy consumption may pose operational challenges. Ensuring deterministic timing behaviour is also difficult, as many AI models have variable execution times under different input loads.

5.7 Standardization and Regulatory Barriers

Protection systems operate under stringent industry standards (IEC, IEEE, NERC). AI-based methods lack established testing frameworks, certification procedures, and standardized performance metrics. Utilities and regulators face uncertainty regarding how to validate AI algorithms under all possible fault scenarios. The absence of well-defined benchmarks slows deployment and discourages risk-averse stakeholders.

5.8 Model Drift and Long-Term Maintenance

As grid conditions evolve over months and years, AI models may experience "concept drift," where their performance degrades due to changes in load patterns, DER penetration, equipment aging, or network reconfiguration. Maintaining long-term accuracy requires periodic retraining, model updating, and continuous monitoring. This increases operational workload and necessitates skilled labour, adding new maintenance responsibilities not present in traditional protection systems.

6. Prospects & Future Research Directions

6.1 Hybrid Physics–AI Models

Future protection schemes are expected to integrate machine learning with physics-based models to combine the strengths of both domains. Hybrid frameworks that merge ANN/ML techniques with state estimation, Kalman Filters, Unscented Kalman Filters (UKF), or model-based residual analysis can significantly enhance robustness. Such systems maintain the interpretability and stability of physics-based models while benefiting from the adaptability and pattern-recognition capabilities of AI. Research is also progressing toward *physics-informed neural networks (PINNs)*, which embed grid equations directly into the training process, ensuring physically consistent outputs even with limited datasets.

6.2 Explainable AI

Explain ability will be crucial for future deployment of AI-based protection. Techniques such as SHAP, LIME, attention-based visualization, and rule-extraction frameworks will enable engineers to understand the reasoning behind AI relay decisions. This transparency is vital for post-event analysis, regulatory auditing, and system operator trust. Future research aims to design inherently interpretable models tailored specifically for protection logic rather than retrofitting generic XAI tools.

6.3 PMU-Based Dynamic Protection

High-resolution, time-synchronized data from Phasor Measurement Units will play a central role in next-generation protection. PMU-enhanced systems can support dynamic state estimation, real-time situational awareness, transient stability detection, and predictive tripping schemes. As PMU deployment expands into distribution networks and micro grids, research will shift toward distributed protection architectures that coordinate multiple PMUs using AI-based decision agents and decentralized optimization.

6.4 Digital Twin Integration

Digital Twins of substations, feeders, and DER clusters will revolutionize how protection systems are designed and validated. AI-enabled Digital Twins can simulate a wide range of realistic fault scenarios, DER behaviours, and cyber–physical interactions. They allow safe offline testing of relay logic, algorithm training, and verification of coordination strategies. Future research will explore real-time co-simulation platforms where AI relays continuously learn from both physical and virtual environments.

6.5 Standardization and Testing Frameworks

For AI-based protection to become viable in operational grids, standardized certification frameworks are essential. This includes establishing benchmark datasets, simulation protocols, hardware-in-the-loop (HIL) testing environments, and performance evaluation metrics. International bodies such as IEEE, IEC, and CIGRÉ are expected to play key roles in formalizing these standards. Development of shared open-source datasets will also accelerate research and ensure fairness in model comparison.

6.6 Edge Computing and AI Acceleration Hardware

Advances in embedded AI processors, FPGAs, and edge-computing modules will support real-time deployment of complex AI models in substations. Edge-based AI processing reduces communication delays and improves reliability by making decisions locally, even during network outages. Research is ongoing into low-latency model compression, pruning, quantization, and lightweight neural architectures specifically optimized for protection devices.

6.7 Federated Learning and Collaborative Model Training

Federated learning offers a promising approach for utilities to collaboratively train AI models without sharing raw operational data. Multiple substations or utilities can train a global model while keeping data locally stored, enhancing privacy and cybersecurity. This approach also increases dataset diversity, improving generalization. Future work will focus on the resiliency, synchronization, and robustness of federated frameworks under heterogeneous grid conditions.

6.8 Cyber–Physical Resilience Enhancements

AI-driven protection will increasingly incorporate mechanisms to detect and withstand cyberattacks, including adversarial ML defences, anomaly detection systems, and secure multi-

agent coordination. Research will emphasize making models robust to manipulation, ensuring data authenticity, and developing self-healing protection schemes capable of isolating compromised components and maintaining operational continuity.

6.9 Integration with Wide-Area Protection (WAP)

Future protection architectures will likely employ multi-agent AI systems capable of utilizing wide-area data for coordinated relay actions across large geographical regions. These systems may use graph neural networks (GNNs) to model network topology, multi-agent reinforcement learning for coordination, and distributed decision-making to prevent cascading failures.

7. Conclusion

AI-based protection schemes hold significant promise to enhance fault detection, improve system resilience, and enable adaptive protection in dynamic modern grids. The integration of data-driven decision-making and intelligent fault analysis represents a major step toward autonomous and self-correcting power systems. However, prior to 2021, full-scale deployment of such AI-driven protection strategies remained largely experimental and confined to simulation environments or pilot projects. The limitations were strongly linked to insufficient real-time datasets, lack of standardization across utilities, heterogeneity of network infrastructure, dependence on communication systems, and regulatory requirements demanding complete transparency in protection decision-making. The reliability of AI algorithms under unseen operating conditions remains a critical issue, especially when considering rare faults, evolving grid configurations, and inverter-based disturbances. The “black-box” nature of many ML and deep learning models further restricts utility acceptance, as protection systems must be auditable and physically explainable. Moreover, cybersecurity threats—such as data poisoning, spoofing, and false data injection—pose new challenges to intelligent protection frameworks deployed in cyber-physical energy systems. To enable practical deployment, future research should prioritize hybrid physics-informed AI methods, where machine learning is supported by established protection principles and state estimation frameworks. Explainable AI (XAI) must be adopted to improve transparency, enabling operators to trace and justify every decision taken by the protection scheme. PMU-enabled real-time protection and Digital Twin environments offer promising platforms for model training, system validation, and experimental fault-injection studies without risking operational reliability. Additionally, regulatory bodies and utilities must collaborate to create benchmark datasets, validation protocols, and interoperability standards to evaluate AI-based protection tools under realistic conditions.

Bridging the gap between theoretical potential and field implementation is essential for achieving safe, dependable, and intelligent AI-driven protection systems. As the grid evolves toward decentralization, renewable integration, and active distribution networks, the role of AI will gradually transition from a supplementary diagnostic tool to a core component of modern protection architecture. With continued advances in sensing technologies, communication infrastructure, and grid digitalization, AI-based protection systems can become an operational reality—contributing to a future of self-adaptive, self-healing, and resilient power networks.

References :

[1] Benitez and Teodoro (2020) provided a focused evaluation of both technical challenges and practical opportunities, establishing a strong conceptual foundation for AI integration in protection systems.
[2] The IEEE PES Report (2019) offered industry-level insights into emerging protection trends and highlighted gaps between research prototypes and field implementation.
[3] Girgis & Makram (2009) were among the earliest researchers to explore AI applications in protection systems, making this paper foundational for later developments.
[4] Dash (2016) presented ML and signal-processing-based fault diagnosis methods, demonstrating how AI improves accuracy over deterministic algorithms.
[5] Kezunovic (2018) pioneered data-driven relay coordination using real-time datasets, providing direction for adaptive and intelligent protection solutions.
[6] Wang et al. (2019) investigated PMU-aided protection, emphasizing how high-speed synchronized measurements enhance fault detection and classification.
[7] Jamali (2017) introduced adaptive relaying strategies based on AI, highlighting the need for dynamic protection settings in active distribution networks.
[8] Dey et al. (2020) raised awareness of cybersecurity threats in AI-enabled protection and discussed vulnerabilities to data manipulation and cyber-attacks.
[9] Aziz (2019) demonstrated the potential of deep learning for fault location, showcasing improved performance over classic pattern recognition approaches.
[10] Maduranga & Elangovan (2015) presented SVM-based classifiers for identifying fault types and phases, proving ML viability in practical protection scenarios.
[11] Esmaili (2013) employed fuzzy logic for enhancing protection coordination in distribution networks with uncertain and fluctuating operating states.
[12] Phadke & Thorp (2011) reviewed wide-area PMU-based protection and demonstrated how synchronized data forms the backbone of future smart protection schemes.
[13] Li & Xia (2014) addressed the difficult problem of high-impedance fault detection using ANN models, providing strong motivation for AI-based solutions.
[14] Taylor (2020) investigated ML deployment in digital substations, highlighting real-time applicability and practical integration challenges.
[15] Horowitz (2018) critiqued conventional protection methods in the context of distributed energy integration, justifying the transition towards AI-based methods.
[16] Singh & Murthy (2016) implemented decision tree-based fault classification, proving that lightweight AI models can operate under real-time constraints.
[17] Chatterjee et al. (2017) proposed hybrid DWT–ANN models that combine signal processing with AI to improve transient fault identification.
[18] Kamel (2019) explored reinforcement learning for fast adaptive protection, introducing real-time learning-based relay setting updates.
[19] Mirzaei (2020) introduced Digital Twin–based simulation platforms to train and validate AI-driven protection strategies safely.
[20] The IEEE Working Group (2018) provided structured guidelines for AI integration, classification of technical challenges, and possible standardization pathways.
[21] Sarkar & Bhattacharya (2015) applied PMU-based data analytics for continuous online monitoring of faults and power quality disturbances.

[22] Liu et al. (2016) validated SVM models on real-time datasets for fault classification, demonstrating strong accuracy and computational efficiency.
[23] Zhou & Luo (2020) studied reliability and risk assessment of AI-based relays, emphasizing utility concerns about misoperation and explainability.
[24] Jain (2018) explored big data analytics for grid protection, laying groundwork for large-scale training of AI protection models.
[25] Mehta (2020) focused on Explainable AI (XAI), addressing the trust and transparency issues that hinder AI adoption in protection systems.
[26] Nguyen (2019) analyzed cyber–physical threats targeting AI-based protection relays and recommended a protective defense framework.
[27] Zhang & Kang (2017) studied ML applications specifically for microgrid protection, where fault signatures are highly nonlinear and unpredictable.
[28] Haque (2019) proposed an AI-based substation protection framework and discussed integration with IEC 61850-based automation systems.
[29] Pillai & George (2020) combined AI with state estimation techniques to improve robustness and reduce dependency on pure data-driven models.
[30] Salahuddin et al. (2019) provided a comprehensive review of AI in fault detection and location, identifying major limitations and future research directions.