Adaptive Protection of Microgrids Using Machine Learning: A Review of Fault Detection, Classification and Dynamic Relay Setting

Rakhi[1], Nishant Patnayak[2]
1,2Department of Electrical Engineering, RSR Rungta College of Engineering and Technology, Bhilai, India.
1rakhisrit@gmail.com, 2nishanthpatnaik_eee@cbit.ac.in

Abstract—

Microgrids are increasingly promoted as a route to resilient, low-carbon electricity, yet their protection remains the weakest link in the chain. A relay set for the strong, utility-fed fault current of grid-connected operation turns blind the moment the microgrid islands and its inverter-based sources can deliver only a modest current. This review examines why fixed relay settings are structurally unsuited to microgrids and how adaptive protection, coupled with machine learning, is being used to close that gap. Drawing on forty peer-reviewed studies spanning 1995 to 2025, the paper follows the arc from classical overcurrent relaying, through setting-group adaptation, to contemporary data-driven schemes in which a classifier watches voltage and current features and prompts a relay to revise its settings in real time. We compare the signal-processing tools and learning algorithms that recur across the literature, record the performance that has been reported and the conditions under which those numbers were obtained, and argue that the field's central unresolved problems are less algorithmic than evidential: scarce and unbalanced data, weak generalisation across topologies, limited explainability, unaddressed cyber risk and a shortage of field validation. The paper closes with a research agenda intended to move learning-based adaptive protection from simulation toward deployment.

Keywords—microgrid protection; adaptive protection; fault detection and classification; machine learning; support vector machine; neural networks; inverter-based resources; relay coordination

I. INTRODUCTION

The electricity system is being rebuilt from both ends at once. At the transmission level, large synchronous plants are giving way to variable renewables; at the distribution level, generation that once sat far away is now appearing behind the meter, on rooftops and in small industrial parks. Microgrids sit at the meeting point of these two movements. A microgrid groups local sources, storage and loads under a single controller so that the whole assembly can either lean on the utility network or stand alone when that network fails [2], [6]. The promise is attractive: higher reliability, cheaper energy, and the ability to ride through the kind of outage that has become more frequent with extreme weather.

That promise is constrained by protection. A distribution feeder is protected assuming fault current comes from one direction, from a single strong source, and that its magnitude is large enough to distinguish it from load. A microgrid violates every part of that assumption. Power can flow either way; the sources may be inverters that cannot deliver much fault current at all; and the network's topology and short-circuit capacity change as units are switched in and out [3], [9], [11]. The consequence is well documented: relays that protect the grid-connected microgrid correctly can miss faults entirely once it islands, or trip spuriously on ordinary load changes when they are made sensitive enough to catch those faults [1], [5], [17], [18].

Adaptive protection is the field's long-standing answer to this mismatch. Rather than freezing relay settings at commissioning, an adaptive scheme observes the microgrid's state and revises the settings to match it [1], [10], [12]. For most of its history, that meant choosing between a handful of pre-computed setting groups. More recently, machine learning has entered the picture. If a classifier can infer the operating mode and the presence, type and severity of a fault from local voltage and current measurements, then the relay no longer has to choose from a fixed menu of settings; it can be steered continuously and in real time [12], [27], [29].

This review brings together the strands of that development. Our aims are fourfold. First, to state precisely why static protection fails in microgrids, in terms that connect the physics of fault current to the behaviour of relays. Second, to survey the adaptive architectures that have been proposed and the extent to which they depend on communication. Third, to compare the signal-processing techniques and learning algorithms that dominate the literature, and to be candid about the evidence behind their reported accuracy. Fourth, to identify the obstacles that stand between a working simulation and a relay in a substation, and to propose how they might be addressed.

The remainder of the paper is organised as follows. Section II describes microgrid architecture and the protection problem in detail. Section III reviews conventional, static protection and its limits. Section IV covers adaptive protection architectures. Section V treats signal processing and feature extraction. Section VI surveys machine learning for fault detection and classification. Section VII discusses AI-enabled adaptive protection and the coupling of a classifier to relay settings. Section VIII offers a comparative synthesis. Section IX sets out challenges and open problems, Section X a research agenda, and Section XI concludes.

II. Microgrid Architecture and the Protection Problem

A. What a microgrid is

A microgrid is a cluster of distributed energy resources (DERs), energy storage and controllable loads that operates as a single, coordinated entity with respect to the wider grid [2], [6]. It connects to the utility through a point of common coupling (PCC), often through a transformer and a static switch, and it is managed by a controller that decides when to import, export or island. The sources inside it are heterogeneous. Some, such as small diesel gensets or micro-turbines, are synchronous machines and behave in the familiar way under fault, delivering several times their rated current. Others, photovoltaic arrays and battery systems in particular, are coupled through power-electronic converters and behave very differently [22], [25].

The distinction matters enormously for protection. A converter is a controlled current source with a thermal limit. Its semiconductor switches cannot tolerate the large currents that a fault invites, so its controller deliberately restricts output during a fault, typically to somewhere between one and two times the rated current, and in some designs to even less [21], [22]. Where a synchronous machine might deliver five or ten times rated current into a short circuit, an inverter delivers something close to normal load current. The relay, whose entire job is to tell a fault from a heavy load, is thereby handed a much harder problem [3], [7].

B. Two operating modes, two fault-current regimes

The defining feature of a microgrid, for protection purposes, is that it can run in two modes. In grid-connected mode, the utility network is the dominant source and the fault current is large; several authors note that it can be an order of magnitude or more above nominal, since the utility impedance is low [18], [21]. In islanded mode, that source is gone, and the fault current is set by the local DERs alone. In an inverter-dominated island, it collapses to roughly the 1.2 to 2 per unit band noted above [21], [22].

A protection scheme has to work in both. A single overcurrent setting cannot do so. If it is chosen to be dependable in grid-connected mode, with a pickup well above the highest load current, it will not operate at all in the islanded mode, where the fault current never reaches that level. This is the failure mode known as protection blinding. If, instead, the setting is lowered to catch islanded faults, the relay becomes sensitive to load, and the inrush of a motor or the switching of a capacitor bank can push it over the threshold and cause a spurious trip [18], [21]. Between these two failures lies the reason adaptive protection exists.

C. The catalogue of protection challenges

Beyond the mode-dependent fault level, a microgrid accumulates a set of related difficulties, catalogued at length in the review literature [3], [4], [7], [9]. Bidirectional power flow means that a relay can no longer assume which end of a line feeds a fault, so coordination between primary and backup devices, worked out for a radial network, may no longer hold. Blinding and sympathetic tripping both follow: a relay may fail to see a fault because a downstream source back-feeds it, or it may trip for a fault that is not in its zone because a neighbouring source contributes current through it [9]. Variable and uncertain generation, especially from photovoltaics and wind, means the short-circuit level drifts with the weather even within a single mode [7], [9]. High-impedance faults, whose small currents and nonlinear arcs resemble switching events, are hard for any threshold method and harder still in a converter-rich network [6], [34]. Finally, the presence of converters introduces harmonics and fast transients that conventional phasor-based relays were never designed to interpret [6], [7].

TABLE I. Protection challenges in microgrids and their effect on static protection.

Challenge	Why it arises	Consequence for static protection
Mode-dependent fault level	Fault current falls sharply on islanding as the utility source is lost	One setting cannot be both dependable (grid-connected) and sensitive (islanded)
Protection blinding	A source between relay and fault reduces the current the relay sees	Relay fails to operate for a genuine fault
Sympathetic tripping	Contribution from a neighbouring source flows through a healthy relay	Relay trips for a fault outside its zone
Loss of coordination	Bidirectional flow and changing topology alter relay pair margins	Backup relay may operate before, or instead of, the primary
Low fault current from inverters	Converter controllers limit current to protect semiconductors	Fault current approaches load current; discrimination fails
High-impedance faults	Small, nonlinear arc currents resemble switching events	Threshold methods miss them or confuse them with transients
Variability of renewables	Short-circuit level drifts with solar and wind output	Settings valid at one moment are wrong at the next

III. Conventional Protection and the Limits of Static Settings

The protective devices inherited from distribution practice are, in rough order of prevalence, overcurrent relays, fuses, reclosers, directional overcurrent elements, distance relays and differential schemes [4], [9]. Each is built on a fixed relationship between a measured quantity and a decision. An overcurrent relay trips when current exceeds a pickup; a distance relay trips when measured impedance falls inside a zone; a differential relay trips when the currents entering and leaving a protected zone disagree. All of them encode assumptions about the network that a microgrid breaks [3], [9].

Fuses and reclosers are the most exposed. Their inverse time-current characteristics are chosen so that they coordinate with the relay above and the load below, and that coordination is calibrated to a fault-current level. When the fault current falls, as it does on islanding, a fuse may never reach its melting point while a downstream fault burns, and the recloser may reclose onto a fault it cannot clear [18], [21]. Directional elements recover some of the lost selectivity, since they can at least tell which way a fault lies, but they still rely on a current magnitude that the islanded microgrid may not supply [3], [9]. Differential protection is comparatively robust because it compares currents rather than judging their absolute size, and it is therefore attractive for microgrids; its difficulty is cost and the need for communication between line ends [3], [6].

The conventional response to the mode problem is the setting group: a relay stores several pre-computed settings and switches between them as the microgrid changes state [1], [4]. This is genuinely useful and is the most common non-conventional scheme found in operating microgrids [4]. Its weakness is granularity. Commercial relays hold only a small number of groups, and the number of distinct operating states a microgrid can present, one for every combination of connected sources, open lines and load levels, is far larger [7], [9]. A handful of settings cannot span that space, and the gaps are exactly where coordination fails. This limitation is the hinge on which the move to continuous, learning-based adaptation turns.

IV. Adaptive Protection: Architectures and Mechanisms

Adaptive protection is best defined as an online process that adjusts protective responses in step with changes in the system's condition or requirements [1], [12]. In the microgrid context, its purpose is to keep the relay matched to the microgrid's present mode and topology, so that sensitivity in the islanded mode and selectivity in the grid-connected mode are not in conflict. The literature divides the implementations into three families.

A. Centralised, decentralised and hybrid schemes

A centralised scheme gathers measurements and status information at a central controller, which computes the appropriate settings for every relay and distributes them [18], [24]. It can, in principle, solve the coordination problem globally, which is its great advantage, but it depends on a communication network that is a single point of failure and, in an adversarial setting, a single point of attack [18]. A decentralised scheme does the opposite: each relay infers the microgrid's state from local measurements alone, typically from voltage and frequency, and adapts without reference to a central authority [18]. This removes the communication dependency at the cost of a narrower view; a relay acting alone cannot easily know what its neighbours are doing. Hybrid schemes split the difference, using a central unit for slow, network-wide changes and local logic for fast events such as loss of a generator [18], [24]. The combination of centralised and decentralised communication has been shown to improve both speed and reliability of adaptation [24].

Multi-agent designs generalise the hybrid idea, giving each protection device a degree of autonomy and a means of negotiating with its peers. They scale well to microgrids with many converters and frequent mode transitions, but they inherit the communication and cyber-security concerns of any distributed system [7], [18].

B. Setting groups, online models and optimisation

Within these architectures, several mechanisms recur. The simplest is setting-group selection, in which a supervisory layer detects the mode and loads the matching group [1], [4]. A more ambitious mechanism runs an online model of the microgrid: the controller continuously computes the available short-circuit current from the present topology and derives the relay settings from it, so that no finite set of pre-stored groups is needed [16]. A third mechanism formulates coordination as an optimisation problem and solves it for the current configuration, minimising total operating time subject to coordination constraints. Genetic algorithms, particle swarm optimisation and related metaheuristics are widely used for this, and dual-setting directional overcurrent relays, which carry separate forward and reverse characteristics, are a popular vehicle for it [21], [23].

The published schemes differ in how much they assume about the future. Hailuoto Island, an early and well-known field example, combined adaptive protection with microgrid control and demonstrated the approach on a real network [15]. Other work has targeted distribution systems that can operate in either mode [13], microgrids with electronically coupled generation [14], systems with several points of common coupling [20], and designs that switch adaptively between grid-connected and islanded algorithms [19]. A recurring theme is that the more the scheme adapts, the more it leans on information beyond the local measurement, and therefore on communication [18], [20].

Adaptive protection so far is a mature idea with an incomplete reach. It solves the mode-selection problem neatly, but most implementations still reduce a rich, continuous state space to a small number of discrete settings. It is at that point that machine learning becomes attractive, because a trained classifier can, in effect, provide an arbitrarily fine partition of the operating space [12], [29].

V. Signal Processing and Feature Extraction

No classifier can be better than the features it is given, and a large share of the literature's effort has gone into deciding what to measure. The measurements themselves are usually the three-phase currents and voltages at the relay, sampled at rates from a few kilohertz to tens of kilohertz. The question is how to turn those waveforms into a compact description that separates a fault from normal operation, and one fault type from another.

A. Phasors, RMS values and symmetrical components

The classical tools remain the most common. A discrete Fourier transform over a sliding window yields the fundamental phasor of each phase, from which RMS magnitudes and phase angles follow; symmetrical-component transformation then decomposes the three phases into positive, negative and zero-sequence quantities [27], [29]. This decomposition is particularly valuable for protection because it makes fault type legible: an unbalanced fault produces negative-sequence current, a ground fault produces zero-sequence current, and a balanced three-phase fault leaves both small. Several schemes therefore train their classifiers on the RMS values of sequence components rather than on raw

samples, which keeps the feature vector small and the computation light enough for an embedded device [27], [29], [32]. Barkhi and co-workers, for instance, base a combined detection and classification method on the RMS values of symmetrical components and report that local information alone is sufficient [29], while Srivastava and Parida use one-cycle RMS voltage and current measurements as the input to a support vector machine for fault identification [32].

B. Time-frequency methods: wavelet and its relatives

Faults are transient events, and a purely frequency-domain view discards the timing that matters for fast detection. Wavelet analysis addresses this by localising a signal in both time and frequency. The discrete wavelet transform and its variants, including the maximal overlap discrete wavelet transform and the empirical wavelet transform, appear repeatedly [30], [31], [33], [34]. The usual recipe decomposes a short window of the post-fault signal into detail and approximation coefficients and then summarises them statistically, using means, standard deviations, energies, entropies and higher moments as the features fed to the classifier [30], [33]. Bukhari and colleagues use a convolutional network on wavelet features for an intelligent protection strategy [33], and a related scheme applies the empirical wavelet transform to the same end [34]. Other transforms, including the Hilbert-Huang transform, the S-transform and the short-time Fourier transform, play similar roles and recur in the wider fault-diagnosis literature [36], [38].

The choice between phasor-based and time-frequency features is a trade-off between simplicity and speed. Phasor features are cheap and interpretable but need most of a cycle to settle, which sets a floor on detection time. Wavelet and other transient features can flag a fault within a fraction of a cycle, at the cost of more computation and a need to tune the mother wavelet and decomposition level to the application [30], [33], [38].

VI. Machine Learning for Fault Detection and Classification

Once features are chosen, the learning problem is usually framed as classification. Two questions are asked most often: is there a fault or not, and if so, what type and where. Some schemes answer them separately, and some, following the argument that detection and classification are best done together, use a single multi-class model [29].

A. Classical supervised learning

The support vector machine (SVM), introduced by Cortes and Vapnik [26], is the most conspicuous algorithm in the microgrid protection literature. Its appeal is that it performs well on modest, well-chosen feature sets and offers a principled margin, which suits problems where data are scarce and the cost of a wrong decision is high. Manohar and Koley train an SVM on wavelet coefficients to detect, classify and locate shunt faults in grid-connected and islanding modes [28]; Hooshyar and co-workers address fault-type classification in microgrids that include photovoltaic DGs [27]; Dash and colleagues apply an SVM to fault classification on a series-compensated line, an early demonstration of the protection method [40]; and Ahmadipour et al. combine wavelet-derived entropy features with an SVM for fast fault identification in a grid-connected photovoltaic system [35]. The SVM's reliance on a kernel also means that its performance depends on tuning two hyper-parameters, the penalty and the kernel width, which several authors handle with metaheuristic search [31], [38].

Decision trees, k-nearest neighbours, naive Bayes and random forests form the rest of the classical family. They are lighter to train, easier to interpret and, in the ensemble form, often competitive. Gradient-boosted trees on wavelet features have been used for fault detection and classification in a smart microgrid [31], and comparative studies find that tree-based ensembles can match or exceed SVM accuracy on high-impedance fault problems while being less sensitive to feature scaling [38]. The lesson from these comparisons is that no single algorithm dominates; the feature representation and the quality of the dataset usually matter more than the choice of classifier [38], [39].

B. Neural networks and deep learning

Neural networks entered the field early, in the form of shallow multilayer perceptrons applied to fault classification, and more recently as deep architectures [36], [37]. Convolutional networks are attractive because they can learn features directly from waveform or time-frequency images, reducing the burden of hand-crafting inputs; Bukhari et al. build a convolutional protection strategy for microgrids on this principle [33], and the broader deep-learning literature reports strong results for fault detection, classification and location across transmission and distribution networks [36]. Recurrent architectures, particularly long short-term memory networks, are used where the temporal evolution of the signal carries information, as in high-impedance faults [38]. The trade-off is familiar from machine learning generally: deeper models can be more accurate, but they need more data, demand more computation at inference time, and are harder to explain, which sits awkwardly with a domain that prizes auditable decisions [7], [36].

C. Hybrid pipelines

Most effective schemes are hybrids, in which a signal-processing stage produces features and a learning stage classifies them. The combination of wavelet or empirical-mode decomposition with an SVM or a neural network is the archetype, and it recurs across the reviews [7], [30], [38]. A second kind of hybrid couples machine learning to a physical model, using the model to generate training data or to constrain the learner. This is the more promising direction, because it directly attacks the data problem described in Section IX.

ISSN: **3107-6513**

TABLE II. REPRESENTATIVE MACHINE-LEARNING METHODS FOR MICROGRID FAULT DETECTION AND CLASSIFICATION.

Method family	Typical features	Task	Representative works
Support vector machine	Sequence-component RMS; wavelet coefficients; entropy	Detection, classification, mode identification	[27], [28], [32], [35], [40]
Decision tree / random forest / boosting	Wavelet energy; statistical moments	Detection, classification, high-impedance faults	[31], [38]
k-nearest neighbours / naive Bayes	RMS; wavelet features	Detection and classification (baselines)	[28], [38]
Shallow neural networks (MLP)	RMS; phasor magnitudes	Classification, fault location	[36], [37]
Deep networks (CNN, LSTM)	Waveform or time-frequency images; raw sequences	Detection, classification, location	[33], [36], [38]
Hybrid signal-processing + learning	Wavelet / empirical-mode decomposition + classifier	Detection, classification, section identification	[30], [31], [33], [34]

VII. AI-ENABLED ADAPTIVE PROTECTION: COUPLING LEARNING TO RELAY SETTINGS

The step that distinguishes AI-enabled adaptive protection from the wider fault-diagnosis literature is the coupling of a learned decision to an actual change in relay behaviour. The classifier does not merely announce a fault; it identifies the operating mode and the fault condition, and that output selects or computes the relay settings that will be used [12], [29].

Lin and colleagues gives one of the clearest formulations of this idea, combining adaptive protection with machine learning so that the protection responds to the microgrid's state rather than to a fixed rule [12]. A natural division of labour follows. A slow, mode-identification model, updated as sources connect and disconnect, chooses the base setting; a fast, fault-detection model watches for the event and trips. The two can share features but run at different rates. Several works treat mode detection as a classification task in its own right, because the mode is the variable that most strongly conditions every subsequent decision [28], [29].

Where the scheme computes settings from an online model rather than selecting from a list, the learning component can supply the quantities the model needs, such as the estimated fault resistance or the contribution of each source [16]. This is the point at which learning and physical modelling most usefully meet, and it is where the more recent proposals are concentrated [7], [16].

Deployment realities shape the design. A classifier that runs in a substation intelligent electronic device has a budget of milliseconds and a modest processor, so compact models and sequence-component features are favoured over deep networks and raw samples [27], [29], [32]. Edge computing, in which the inference is done close to the measurement rather than centrally, is a recurring theme, since it removes the round trip to a control centre and so removes communication latency from the critical path [7]. Confidence handling matters as much as raw accuracy: a detector that trips on a marginal probability will generate nuisance trips, which are as damaging to a microgrid's credibility as a missed fault, so thresholds and decision logic are tuned with the false-positive rate in view [18], [29].

VIII. COMPARATIVE SYNTHESIS

Read together, the literature suggests a clear trajectory. Static protection is simple, communication-free and adequate for a network whose fault current does not move. Setting-group adaptation recovers most of that adequacy for a microgrid that toggles between two well-defined states, at the cost of a supervisory layer and a finite, and therefore incomplete, set of settings. Continuous adaptive protection, especially when driven by a learning model, removes the granularity limit and can respond to states that were never enumerated in advance, but it introduces a dependence on data and on whatever communication the scheme requires [7], [12], [18]. The comparison is summarised in Table III

.

TABLE III. STATIC, SETTING-GROUP AND LEARNING-BASED ADAPTIVE PROTECTION COMPARED.

Scheme	Basis of decision	Strengths	Limitations
Static protection	Fixed pickup and time-current settings	Simple, fast, communication-free, well understood	Fails when fault level changes with mode; blinding or nuisance tripping
Setting-group adaptation	Pre-computed groups selected by supervisory logic	Handles two well-defined modes; proven in service	Limited number of groups cannot span all configurations; needs supervision
Learning-based adaptive protection	Classifier output steering settings in real time	Fine-grained response to unseen states; strongest in islanded mode	Depends on data and communication; generalisation, explainability and cyber risk

Two conclusions follow. The first is that the advantages of learning-based adaptation are real but conditional: they appear most clearly in the islanded, inverter-dominated regime, where the fault current is small, and the static relay's margin is thinnest [21], [22]. In the grid-connected regime, where the fault current is large and unambiguous, a well-set conventional relay is fast and hard to beat, and a learning scheme's contribution is largely in selectivity, distinguishing

a fault from the load transients that would fool a sensitive relay [18]. The second is that the field's headline accuracy figures should be read with care. Reported classification accuracies above ninety-five per cent are common, but they are obtained on simulated datasets, frequently from a single test system, and the reviews are unanimous that this makes them hard to compare and harder to trust [7], [36], [38], [39].

IX. Challenges and Open Problems

A. Data: scarcity, imbalance and the simulation gap

The deepest problem is data. Faults are rare by design, so real recordings are scarce and skewed heavily toward normal operation, and most published schemes are therefore trained on simulated data from a digital model of one test network [7], [38]. A model trained this way learns the idiosyncrasies of its simulator as much as the physics of a fault, and it can fail when transferred to a network with different impedances, different converters or different grounding [7], [39]. Class imbalance compounds the difficulty, since a detector that simply never declares a fault will score well on accuracy and be useless in practice; the field is moving, belatedly, toward metrics such as the Matthews correlation coefficient and the area under the receiver operating curve that expose this [38]. Physics-informed generation of training data, in which a model is used to create the scenarios a field recording cannot supply, is the most credible route out of the corner [16], [39].

B. Generalisation, robustness and explainability

A protection scheme must work on networks it was not trained on, under conditions it did not see. Transferability across topologies, load levels and fault resistances is inconsistently reported, and where it is tested, it is often fragile [36], [39]. Explainability is a related and more pointed concern. A relay decision has consequences, and an operator or a regulator will want to know why the model acted. Opaque deep models are at odds with that expectation, and the reviews single out explainable AI as a prerequisite for acceptance rather than a luxury [7], [36]. The tension is not irreducible, since compact models on physical features can be both accurate and interpretable, but it does argue for restraint in the choice of model complexity [27], [29].

C. Cyber-security and communication dependence

Adaptive protection that communicates inherits the vulnerabilities of the network it communicates over. A scheme that trusts a central controller's settings is only as safe as that controller, and the links to it, and the failure of either can turn a protection system into a liability [18]. Communication failure specifically, and its mitigation through local fallback logic or energy storage as a contingency, has been studied directly [18], and multi-agent schemes are exposed to the same class of risk [7]. Any credible proposal must say how it behaves when the link is lost or corrupted, and the honest answer for many centralised designs is that it must fall back to something local and conservative.

D. Validation and standards

The gap between simulation and the field is bridged, in the best work, by hardware-in-the-loop testing on real-time simulators, and by field trials. Several schemes have been validated on real-time platforms [21], [32], and a small number on operating networks [15], but these remain the exception [7]. Standards matter here too: compatibility with IEEE 1547 for interconnection and with IEC 61850 for substation communication shapes what can actually be deployed, and schemes that ignore those interfaces risk being correct on paper and unimplementable in a substation [7], [9].

X. Future Research Directions

The agenda that emerges from these gaps is less about inventing new classifiers than about making existing ones trustworthy. Five directions stand out.

Initially, consider physics-informed and hybrid modeling. By integrating a learned component with a defined network model, each can offset the other's limitations: the model provides data and physical constraints, while the learner offers pattern recognition capabilities that the model lacks [16], [39]. This approach also facilitates the development of features that retain significance even when the topology alters. Next, focus on transfer learning and domain adaptation, enabling a model trained on one microgrid to be adapted to another with minimal new data, avoiding the need for complete retraining [36], [39]. This method effectively tackles the generalization issue and reduces data collection expenses. Lastly, emphasize explainability and calibrated uncertainty. Protection decisions should be accompanied by justifiable reasons and genuine confidence levels. The field would gain from integrating explainable AI tools rather than considering them as secondary [7], [36]. Fourth, incorporate security from the outset. Adaptive systems must be designed with the expectation that communication might be disrupted or tampered with, and they should be capable of smoothly transitioning to a local, conservative mode. The cyber-physical attack surface should be prioritized as a fundamental design consideration [7], [18]. Fifth, establish shared benchmarks and resilience metrics. The difficulty in comparing results within the literature arises from the absence of standardized test systems, data, and metrics. Implementing standardized datasets and reporting, which include reliability and recovery measures in addition to accuracy, would enhance the field's credibility more than the introduction of any single new algorithm [7], [36], [38].

XI. Conclusion

Microgrids run into protection trouble because of the very thing that makes them work. Distributed, converter-based generation gives a microgrid its flexibility, but it also keeps fault currents small and changeable, so they look a lot like normal load. Relay settings borrowed from conventional distribution systems are fixed, and they simply can’t adjust to that. Adaptive protection tackles the problem of changing operating modes. Machine learning goes a step further, since it lets the response follow the microgrid’s actual state instead of switching between a few preset configurations.

What the reviewed studies show is mixed. In simulation, learning-based schemes detect and classify faults with high accuracy, and they gain the most in the islanded, inverter-dominated case, where static protection struggles hardest. But the same studies make it plain that these methods aren’t ready for wide use. The data are limited and largely simulated. Performance doesn’t carry over reliably from one system to another. Explanations of decisions are shallow, cyber risk is frequently ignored, and very few schemes have been validated in the field.

So the field needs better evidence more than it needs new algorithms. That means physics-informed datasets, models that transfer between systems, decisions that can be interpreted, secure architectures and benchmarks that everyone shares. If adaptive protection is built on that base, a microgrid will be able to island without going dark and reconnect without going blind.

REFERENCES

[1] S. M. Brahma and A. A. Girgis, "Development of adaptive protection scheme for distribution systems with high penetration of distributed generation," IEEE Transactions on Power Delivery, vol. 19, no. 1, pp. 56–63, 2004, doi: 10.1109/TPWRD.2003.820204.

[2] A. Dagar, P. Gupta, and V. Niranjan, "Microgrid protection: A comprehensive review," Renewable and Sustainable Energy Reviews, vol. 149, p. 111401, 2021, doi: 10.1016/j.rser.2021.111401.

[3] B. Patnaik, M. Mishra, R. C. Bansal, and R. K. Jena, "AC microgrid protection – A review: Current and future prospective," Applied Energy, vol. 271, p. 115210, 2020, doi: 10.1016/j.apenergy.2020.115210.

[4] B. J. Brearley and R. R. Prabu, "A review on issues and approaches for microgrid protection," Renewable and Sustainable Energy Reviews, vol. 67, pp. 988–997, 2016, doi: 10.1016/j.rser.2016.09.047.

[5] S. A. Hosseini, H. A. Abyaneh, S. H. H. Sadeghi, F. Razavi, and A. Nasiri, "An overview of microgrid protection methods and the factors involved," Renewable and Sustainable Energy Reviews, vol. 64, pp. 174–186, 2016, doi: 10.1016/j.rser.2016.05.089.

[6] N. H. Hussain, M. Nasir, J. C. Vásquez, and J. M. Guerrero, "Recent developments and challenges on AC microgrids fault detection and protection systems – A review," Energies, vol. 13, no. 9, p. 2149, 2020, doi: 10.3390/en13092149.

[7] M. Uzair, L. Li, M. Eskandari, M. J. Hossain, and J. Zhu, "Challenges, advances and future trends in AC microgrid protection: With a focus on intelligent learning methods," Renewable and Sustainable Energy Reviews, vol. 178, p. 113228, 2023, doi: 10.1016/j.rser.2023.113228.

[8] J. I. Cisneros-Saldana, S. Samal, M. M. Begovic, and S. R. Samantaray, "On protection schemes for AC microgrids: Challenges and opportunities," IEEE Transactions on Industry Applications, vol. 60, no. 3, pp. 4843–4854, 2024, doi: 10.1109/TIA.2024.3353721.

[9] A. N. Sheta, G. M. Abdulsalam, B. E. Sedhom, and A. A. Eladl, "Comparative framework for AC-microgrid protection schemes: Challenges, solutions, real applications, and future trends," Protection and Control of Modern Power Systems, vol. 8, no. 1, p. 24, 2023, doi: 10.1186/s41601-023-00296-9.

[10] S. Mirsaeidi, X. Dong, S. Shi, and D. Tzelepis, "Challenges, advances and future directions in protection of hybrid AC/DC microgrids," IET Renewable Power Generation, vol. 11, no. 12, pp. 1495–1502, 2017, doi: 10.1049/iet-rpg.2017.0079.

[11] S. Sarangi, B. K. Sahu, and P. K. Rout, "Distributed generation hybrid AC/DC microgrid protection: A critical review on issues, strategies, and future directions," International Journal of Energy Research, vol. 44, no. 5, pp. 3347–3364, 2020, doi: 10.1002/er.5128.

[12] H. Lin, K. Sun, Z.-H. Tan, C. Liu, J. M. Guerrero, and J. C. Vásquez, "Adaptive protection combined with machine learning for microgrids," IET Generation, Transmission & Distribution, vol. 13, no. 6, pp. 770–779, 2019, doi: 10.1049/iet-gtd.2018.6230.

[13] Y. Ateş, A. R. Boynueğri, M. Uzunoglu, A. Nadar, R. Yumurtacı, O. Erdinç, et al., "Adaptive protection scheme for a distribution system considering grid-connected and islanded modes of operation," Energies, vol. 9, no. 5, p. 378, 2016, doi: 10.3390/en9050378.

[14] R. Sitharthan, M. Geethanjali, and T. K. S. Pandy, "Adaptive protection scheme for smart microgrid with electronically coupled distributed generations," Alexandria Engineering Journal, vol. 55, no. 3, pp. 2539–2550, 2016, doi: 10.1016/j.aej.2016.06.025.

[15] H. Laaksonen, D. Ishchenko, and A. Oudalov, "Adaptive protection and microgrid control design for Hailuoto Island," IEEE Transactions on Smart Grid, vol. 5, no. 3, pp. 1486–1493, 2014, doi: 10.1109/TSG.2013.2287672.

[16] L. V. Strezoski, I. Stefani, and D. D. Bekut, "Novel method for adaptive relay protection in distribution systems with electronically-coupled DERs," International Journal of Electrical Power & Energy Systems, vol. 116, p. 105551, 2020, doi: 10.1016/j.ijepes.2019.105551.

[17] M. N. Alam, "Adaptive protection coordination scheme using numerical directional overcurrent relays," IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 64–73, 2019, doi: 10.1109/TII.2018.2834474.

[18] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency," IEEE Transactions on Industry Applications, vol. 54, no. 2, pp. 1194–1207, 2018, doi: 10.1109/TIA.2017.2776858.

[19] F. C. Sampaio, F. L. Tofoli, L. S. Melo, G. C. Barroso, R. F. Sampaio, and R. P. S. Leão, "Smart protection system for microgrids with grid-connected and islanded capabilities based on an adaptive algorithm," Energies, vol. 16, no. 5, p. 2273, 2023, doi: 10.3390/en16052273.

[20] P. Naveen and P. Jena, "Adaptive protection scheme for microgrid with multiple point of common couplings," IEEE Systems Journal, vol. 15, no. 4, pp. 5618–5629, 2021, doi: 10.1109/JSYST.2020.3039881.

[21] T. E. Sati and M. A. Azzouz, "Optimal protection coordination for inverter-dominated islanded microgrids considering N-1 contingency," IEEE Transactions on Power Delivery, vol. 37, no. 3, pp. 2256–2267, 2022, doi: 10.1109/TPWRD.2021.3108760.

[22] W. T. El-Sayed, M. A. Azzouz, H. H. Zeineldin, and E. F. El-Saadany, "A harmonic time-current-voltage directional relay for optimal protection coordination of inverter-based islanded microgrids," IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 1904–1917, 2021, doi: 10.1109/TSG.2020.3044350.

[23] T. E. Sati, M. A. Azzouz, and M. F. Shaaban, "Harmonics dual-setting directional overcurrent protection for inverter-based islanded microgrids," IEEE Access, vol. 11, pp. 34630–34642, 2023, doi: 10.1109/ACCESS.2023.3264842.

[24] A. H. El-Hamrawy, A. A. M. Ebrahiem, and A. I. Megahed, "Improved adaptive protection scheme based on combined centralized/decentralized communications for power systems equipped with distributed generation," IEEE Access, vol. 10, pp. 97061–97074, 2022, doi: 10.1109/ACCESS.2022.3205312.

[25] C. Chandraratne, T. Naayagi, T. Logenthiran, and G. Panda, "Adaptive protection for microgrid with distributed energy resources," Electronics, vol. 9, no. 11, p. 1959, 2020, doi: 10.3390/electronics9111959.

[26] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273–297, 1995, doi: 10.1007/BF00994018.

[27] A. Hooshyar, E. F. El-Saadany, and M. Sanaye-Pasand, "Fault type classification in microgrids including photovoltaic DGs," IEEE Transactions on Smart Grid, vol. 7, no. 5, pp. 2218–2229, 2016, doi: 10.1109/TSG.2015.2451675.

[28] M. Manohar and E. Koley, "SVM-based protection scheme for microgrid," in Proc. International Conference on Inventive Computing and Informatics Technologies (ICICICT), 2017, pp. 429–432, doi: 10.1109/ICICICT1.2017.8342601.

[29] S. Baloch and M. S. Muhammad, "An intelligent data mining-based fault detection and classification strategy for microgrid," IEEE Access, vol. 9, pp. 22470–22479, 2021, doi: 10.1109/ACCESS.2021.3056534.

[30] S. Baloch, S. S. Samsani, and M. S. Muhammad, "Fault protection in microgrid using wavelet multiresolution analysis and data mining," IEEE Access, vol. 9, pp. 86382–86391, 2021, doi: 10.1109/ACCESS.2021.3088900.

[31] B. Patnaik, M. Mishra, R. C. Bansal, and R. K. Jena, "MODWT-XGBoost based smart energy solution for fault detection and classification in a smart microgrid," Applied Energy, vol. 285, p. 116457, 2021, doi: 10.1016/j.apenergy.2021.116457.

[32] A. Srivastava and S. K. Parida, "A robust fault detection and location prediction module using support vector machine and Gaussian process regression for AC microgrid," IEEE Transactions on Industry Applications, vol. 58, no. 1, pp. 930–939, 2022, doi: 10.1109/TIA.2021.3129982.

[33] S. B. A. Bukhari, C.-H. Kim, K. K. Mehmood, R. Haider, and M. S. Uz Zaman, "Convolutional neural network-based intelligent protection strategy for microgrids," IET Generation, Transmission & Distribution, vol. 14, no. 7, pp. 1177–1185, 2020, doi: 10.1049/iet-gtd.2018.7049.

[34] S. B. A. Bukhari, A. Wadood, T. Khurshaid, K. K. Mehmood, S. B. Rhee, and K.-C. Kim, "Empirical wavelet transform-based intelligent protection scheme for microgrids," Energies, vol. 15, no. 21, p. 7995, 2022, doi: 10.3390/en15217995.

[35] M. Ahmadipour, H. Hizam, M. L. Othman, M. A. M. Radzi, and N. Chireh, "A fast fault identification in a grid-connected photovoltaic system using wavelet multi-resolution singular spectrum entropy and support vector machine," Energies, vol. 12, no. 13, p. 2508, 2019, doi: 10.3390/en12132508.

[36] M. Mishra and J. G. Singh, "A comprehensive review on deep learning techniques in power system protection: Trends, challenges, applications and future directions," Results in Engineering, vol. 25, p. 103884, 2025, doi: 10.1016/j.rineng.2024.103884.

[37] F. Aminifar, M. Abedini, T. Amraee, P. Jafarian, M. H. Samimi, and M. Shahidehpour, "A review of power system protection and asset management with machine learning techniques," Energy Systems, vol. 13, no. 4, pp. 855–892, 2022, doi: 10.1007/s12667-021-00448-6.

[38] F. M. Shakiba, S. M. Azizi, M. Zhou, and A. Abusorrah, "Application of machine learning methods in fault detection and classification of power transmission lines: A survey," Artificial Intelligence Review, vol. 56, no. 7, pp. 5799–5836, 2023, doi: 10.1007/s10462-022-10296-0.

[39] R. Vaish, U. D. Dwivedi, S. Tewari, and S. M. Tripathi, "Machine learning applications in power system fault diagnosis: Research advancements and perspectives," Engineering Applications of Artificial Intelligence, vol. 106, p. 104504, 2021, doi: 10.1016/j.engappai.2021.104504.

[40] P. K. Dash, S. R. Samantaray, and G. Panda, "Fault classification and section identification of an advanced series-compensated transmission line using support vector machine," IEEE Transactions on Power Delivery, vol. 22, no. 1, pp. 67–73, 2007, doi: 10.1109/TPWRD.2006.876695.