International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 22s, 2025
https://theaspd.com/index.php

Protection Systems for Modern Converter-Dominated Power Networks: A Comprehensive Analysis of Challenges and Solutions

Ajinkya V. Golande[1], Dr. Pooja V. Paratwar[2]
[1]Research Scholar, Department of Electrical Engineering, Mansarovar Global University, Bhopal (M. P), India (ORCID ID:0009-0009-9013-1904)
[2]Research Guide and Associate Professor, Department of Electrical Engineering, Mansarovar Global University, Bhopal (M. P), India (ORCID ID: 0000-0001-7761-0286)
[*]**Corresponding Author Email:** ajinkyagolande1@gmail.com

Abstract
The present power system landscape is transitioning towards a dramatic shift due to the unprecedented penetration of renewable energy sources, complementary Energy Storage (ES) systems, and Power Electronic Converters. This shift has profoundly affected contemporary power networks' operational behavior and security needs, where the conventional synchronous generator-based systems are moving towards converter-dominated infrastructures. Traditional protection methods, which were carefully engineered and tuned to serve networks controlled by synchronous machines, now have many operational difficulties in environments with pervasive use of converters. Such difficulties mainly arise from the inherently distinct fault response behavior of power electronic converters; they have much lower fault current contributions, time-varying dynamic impedances, and their control-induced dynamics lack predictability as opposed to traditional mechanical rotating machines. In this work, a thorough review is performed to systematically investigate the varied protection issues faced by conventional power networks penetrated with converters. It comprehensively evaluates the state-of-the-art technological solutions being developed to deal with these challenges. Analyses include adaptive protection schemes that adjust to dynamic system conditions, wide-area protection systems using synchronized measurements over several network locations, and advanced communication-assisted approaches supporting coherent protection actions. This effort provides comprehensive state-of-the-art analyses of present trends in research, along with the key technical gaps that need to be closed to enable practical, affordable, and reliable protection solutions for the fast-growing 21st-century power grid infrastructure.
Keywords: *Converter-dominated networks, power system protection, renewable energy integration, microgrids, fault detection, adaptive protection*

1. INTRODUCTION

The world of energy from every nook and corner is changing like never before, with the nations around the globe stepping up their decarbonization ambitions and achieving sustainable energy aspirations. A prominent lump in the stepwise transition towards this MF is due to the heavy penetration of Renewable Energy Sources (RES), such as wind farms, solar photovoltaic plants, and different types of energy storage systems interfaced to the grid via complex power electronic converters [1]. This change leads to so-called converter-dominated power networks, where an increasingly large proportion of both generation and load is connected to the power grid via power electronic interface, opposed to traditional synchronous machines, which traditionally formed the backbone constituents of electrical ANC (Active Network Components) [1]. The evolution towards a power system dominated by converters is more than mere technological change; it represents a paradigm shift that questions many of the basic suppositions on which traditional power systems have operated and been protected. This transformation provides several concrete benefits, such as increased power flow controllability and system efficiency, reduced greenhouse gas emissions, and new flexibility in grid operations. Still, at the same time, it has brought along an assorted set of technical challenges that must be addressed carefully to ensure the continued reliability and security of the system [3]. Because synchronous generators and motors were historically the only generation sources, traditional power system protection schemes evolved based on well-established principles involving the predictable behavior of these machines. Those conventional approaches made extensive use of the assumptions that fault conditions would cause fault currents with large magnitude,

limited impedance, and clear directions [4]. Protection philosophy was devised based on the idea that faults would lead to changes in current magnitude, regularly many times that of normal operating urrents, such that a faulted network segment could be detected and subsequently isolated with high repeatability. Despite this, converter-dominant networks behave differently in both normal and fault states. For power electronic converters, the fault current contributions are limited to about 1.1–1.5 per-unit of their rated current capacity due to the physical constraints of the semiconductor devices [5]. As well it should, because should anything more be allowed through, this opens challenges for some protective systems whose detection and response were designed based on fault levels many times higher. Moreover, the time-varying impedance characteristics and nonlinearity in the dynamic behavior of converter control systems make fault detection and location problems difficult because multiple converter units interact. The diversity of network configurations that underpin modern power systems also increases the complexity of these challenges. The different case studies considered involve high voltage transmission networks with significant renewable generation, distribution networks with multiple distributed energy resources (DERs), and microgrids that may be operated in grid-connected or islanded modes, comprising highly converter-interfaced generation sources. These configurations bring liability and present protection challenges requiring specific measures fitting the operational profile and necessities. The main objective of this comprehensive review is to thoroughly investigate protection issues and their countermeasures in converter-centric power networks. This analysis includes the full scope of networks, ranging from large transmission systems to small microgrids, while providing theoretical bases with regular practical implementation of protection technology in today's power system operations.

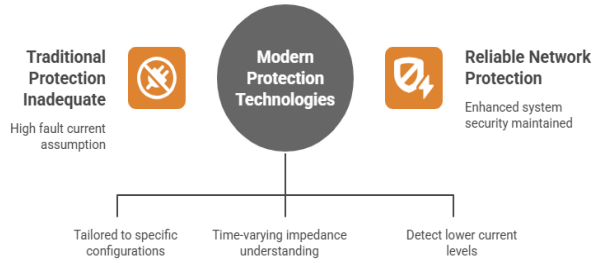

Figure 1. Protecting Converter-Dominated Power Network.

2. CHARACTERISTICS OF CONVERTER-DOMINATED POWER NETWORKS

2.1 Network Architecture Evolution

The architectural change in modern power networks is one of the most critical events in the electrical power industry since AC systems were introduced. Like traditional grid power networks, the Abilene generation facility did, by and large, belong to a handful of centralised utilities producing the power (from some thermal or hydro-electric facilities or nuclear). Still, the consumption was hierarchical and belonged to different levels, from consumers having green time at their disposal within grids due to a distributed production source [8]. Generation — transmission—electricity distribution, and the final user) The network topology was similar for all utilities in that region, with a one-way communication model between the power generators and customers. The traditional architecture has fundamentally changed by integrating renewable energy sources and distributed energy resources. The power networks are now transitioning into more distributed and interconnected systems, where the power generation sources are located ubiquitously throughout the network on different voltage levels [6]. Wind farms might be connected at transmission voltage levels; on the other hand, rooftop solar installations frequently connect at the level of low-voltage distribution. Battery energy storage systems are also locationally flexible and can be deployed throughout the network, ranging from utility-scale installations at transmission substations to residential units behind customer meters. Because of this architecture, the power flow division pattern, network topology management, andection event coordination, are very compIn contrast to the traditional systems when power flowed from large generators to loads along predictable roots, contemporary networks have to be able to withstand a dynamic bidirectional power flow (Grubb and Newberry, 2008), which dynamically changes depending on the availability of renewable resources, consumer load patterns and cycles of charging/ discharging energy storages [20]. It is a dynamic and ever-changing network environment that ends many static assumptions that telcos have long considered the cornerstone of their traditional protection schemes. Converter-interfaced resources have created additional layers of system

complexity by putting multiple control systems in play. Integrated into the system, each converter has advanced control algorithms engineered to maximize performance, ensure grid compliance, and protect surrounding equipment. When hundreds or thousands of these units work together in a network, their behavior can lead to emergent phenomena that are hard to predict and model analytically.

2.2 Fault Current Characteristics

Changing fault current characteristics is probably the most challenging technical problem in a converter-dominated network. For conventional synchronous generators, faults for two similar cases have been studied. The abnormal fault current behaviour with an initial subtransient period of significant magnitude (initially still) transits to a transient afterwards, and for a week during the steady-state fault current level. The initial fault current generated by a synchronous generator can reach 8 -12 times the rated current level during faults, which offers a generously strong signal for protection [8]. This is the case because power electronic converters behave differently under fault conditions. In models of modern devices, such as IGBTs and MOSFETs used in converters, the semiconductor devices are highly restricted by current or thermal limitations due to potential failure risk. Therefore, the control of converter systems is realized using borderline overcurrent limiting algorithms so that the fault current is limited to a range that would be acceptable for semiconductor devices (e.g., 1.1-1.5 x rated current) [8].

2.2.1 Current Limiting Control Strategies

Several current-limiting control strategies are used in modern grid-connected converters to protect the semiconductor devices during fault conditions while providing some grid support capability [9]. As the name implies, the Instantaneous Current Limiting technique is based on a quick cut-off of the current output whenever fault conditions are detected. The converter control system monitors current values at any time and applies immediate control actions to avoid even transient overcurrent conditions. While this approach provides exceptional device protection, fault current contributions may be too low for use in a conventional protection system. While the Peak Current Limiting approach can be better than instantaneous limiting for fault current contribution, it remained much lower than that from synchronous generators. Peaked current limiting strategies: Some converters implement a peak current limiting strategy, which allows for short-term enjoyment of increased peak I_{out} but ensures that maximum values do not go outside the safe device limits. Thermal-based current limiting during regular operation provides a higher current contribution for short durations. Still, it ensures that the device thermal limits are not exceeded during more extended periods. More advanced control systems may also employ thermal-based current limiting that accounts for the various thermal time constants of the semiconductor devices.

2.2.2 Grid Code Compliance and Fault Ride-Through Requirements

To accommodate converter-interfaced generation sources, grid codes worldwide have evolved to include fault ride-through (FRT) requirements. Some of these requirements include renewable energy installations having to stay connected and support the grid during certain fault conditions instead of instantaneously tripping offline, which was typical in earlier installations [10]. The requirements of the FRT have some substantive impacts on behaviour from the fault current of the converter and the protection system architecture. Low Voltage Ride-Through (LVRT) requirements mandate that the inverter remain connected during voltage dips due to network faults, and be able to provide reactive current support for voltage recovery at the grid site. Converters generally lower their active power outputs and use increasing reactive current injections when LVRT operation occurs, in which the fault current contributions are dominantly reactive. Similar to LVRT requirements, high voltage ride-through (HVRT) requires the connection operation even during voltage rises, which could happen in fault conditions or load rejection incidents. Actual current injection requirements during HVRT events can differ widely across various grid codes and geographies.

2.2.3 Control Mode Variations and Their Impact

Different control modes of converter-interfaced sources have different fault response characteristics [11]. Converters in Grid-Following Mode track the voltage and frequency of the larger power system. In a faulted network, grid-following converters typically operate as current-controlled sources, and their contribution to the fault current is dictated mainly by their current-limitation clock cycles and grid codes. Grid-Forming Mode converters actively set voltage and frequency in their local network area and can operate islanded. Grid-forming converters imitate synchronous generators in fault conditions to provide higher fault current contributions. Their response is, however, fundamentally a result of constraints with

semiconductor devices and control system design. Current behavior changes due to the control mode used, which, in turn, affects the protection system design and operation. Networks with an abundance of grid-following (Type III) converters may provide very low fault current levels, and networks with some contribution from grid-forming converters might give slightly higher fault current contributions, but still limited.

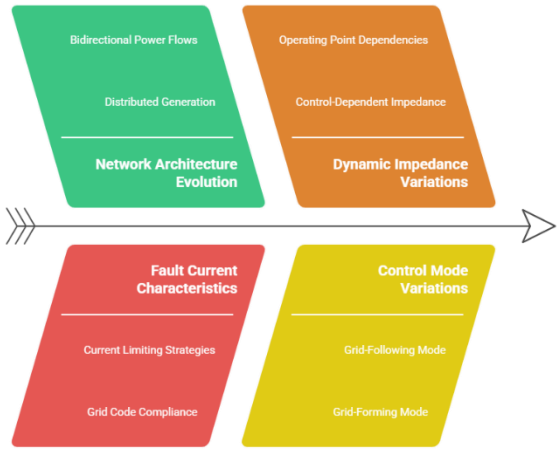

Figure 2. Challenges in Convertor-Dominated Power Networks.

2.3 Dynamic Impedance Variations

From the protection point of view, converter-based networks' most complex issue is that converter-interfaced resources' impedance characteristics are dynamic over time. Compared to synchronous generators, which typically have a constant impedance profile and can be well-characterized using traditional parameters, converters have an evolving impedance characteristic primarily due to the control algorithms, operating conditions, and fault locations [12].

2.3.1 Control-Dependent Impedance Variations

The impedance presented by a converter to the grid is not a fixed physical property but an effect of how the control system in the converter operates. Notably, this should not be the case: two equivalent hardware sets could produce significantly different impedance properties if controlled by different control algorithms. The impedance seen by the network takes into account how the control system responds to disturbances on the cabled link, to reference signals, and interacts with other system components. The current control loops embedded in converter control systems with finite bandwidth and response times determine the impedance characteristics of the converter itself. A fast current regulator would exhibit a low-impedance nature at a transient; meanwhile, the slower controller indicates a high-impedance value. The voltage control loops interact with the current control loops to shape the converter's behavior for grid-forming applications. These interactions can create complex impedance changes that are hard to model and forecast. Converters manipulate output to follow power reference signals. In turn, the newer direction is called power control modes. During a change in power references, say those issued by the automatic generation control signals, the market dispatch instructions, or the local optimization algorithms, there are associated changes in the converter power reference that, consequently, also reflect variations of impedance characteristics.

2.3.2 Operating Point Dependencies

Converter-interfaced sources have variable-impedance characteristics that depend strongly on their operating point, including power output level, voltage conditions, and frequency variations. However, a converter operating at its full rated power cannot exhibit the same impedance characteristics as when operated at lower output power levels. The relationship between active and reactive power output influences converter impedance characteristics. Large loads can cause a much different impedance than small loads, especially when current limiting is in effect. Network deviations in voltage will impact the behavior of the converter control system, and thus also the impedance characteristics [50]. All overvoltage and under voltage states can activate different control responses, modifying the impedance of the converter representation to the network. Converter operation and impedance magnitudes can be heavily affected by changes in the network frequency, especially for islanded microgrid applications. Frequency

control functions determine changes in the impedance, load-frequency droop characteristics, and frequency-dependent load shedding algorithms.

2.3.3 Implications for Distance Protection

The fault distance in traditional distance protection schemes is measured by measuring the voltage and current magnitudes. It is converted into apparent impedance that is then compared against some preset impedance zones to locate and trip relevant protection for a particular fault. Distance protection is based on the assumption that there lies a relatively constant impedance between the relay location and the fault point, allowing for ideal indication of fault location. Away from the low-impedance liaisons, the impedance seen in converters changes dynamically, and converter sources are particularly destabilizing on distance protection. This will cause the measured impedance to change, mimicking a network topology or fault condition change, which could miscommunicate on protection decisions. Any dynamic changes in impedance will result in the swelling or shrinking of the distance protection zones, causing overreach or underreach requirements. This can cause finding fault location inappropriately, resulting in wrong protection actions. Relays in distance protection schemes require precise fault direction identification, which depends on phasor relationships between voltage and current. These relationships can be impacted by dynamic impedance variations, which may lead to errors in determining direction. More advanced distance protection schemes compare impedance trajectories in different planes and at different times to determine whether multiple types of faults are present or other conditions. The dynamic impedance variance in converter-dominant networks may lead to complicated impedance trajectories, which are difficult to detect with conventional analysis methods.

3. PROTECTION CHALLENGES IN CONVERTER-DOMINATED NETWORKS

3.1 Reduced Fault Current Levels

For power system protection, the single most significant long-term challenge posed by declining fault current levels in converter-rich networks is difficult to overstate. This issue impacts nearly all facets of protection system design, from the simple task of fault detection to more elaborate protection coordination schemes that safely allow only a selective operation during fault scenarios.

3.1.1 Sensitivity Issues in Fault Detection

The traditional overcurrent protection system functions based on the realization that fault current is often at levels many times greater than the normal operating current, thus a definitive indication of an abnormal state (Denholm 2006) [13]. Because the fault current contributed by converter sources is limited, this can lead to fault currents that are only slightly higher than normal load currents in converter-dominated networks, making the fault detection sensitivity more challenging. The minimum pickup current settings of overcurrent relays are designed to be coordinated with nondisturbance normal load currents in normal system conditions. For high-impedance faults or faults limited to parts of the network with less converter penetration, fault currents may not be enough to trip these devices above their pickup thresholds in networks dominated by converters. The converters can provide limited fault current contributions, making fault currents comparable to load currents. Hence, it resembles load encroachment problems where protection systems can't separate faulting and heavy loading conditions, so that they will either fail to identify faults or, in case of normal heavy loading, result in improper action. Even in traditional networks, high impedance faults (such as conductors falling onto high resistance surfaces) are typically characterised by very low fault currents. Add to that the negligible fault current contribution in converter-dominated networks, and the existing low fault current contributions will even disappear for high-impedance faults, making them virtually impossible to detect with traditional overcurrent-based techniques.

3.1.2 Protection Coordination Disruption

Time-current characteristic curves have to be correctly designed to allow protection devices to operate in the proper sequence during fault conditions, which is essential for effective protection coordination in power systems [14]. The nearest fault protection device will execute first. In contrast, the backup protection devices will operate as delays depending on the expiration time if the primary does not respond to clear the fault. This coordination scheme relies on the fault currents to be very high and hence easily discriminable among inequitable protection zones. Lower fault currents may invalidate existing time-current coordination concepts in networks with converters. The protection devices may not see the designed time frames of protection settings due to low values of current, thus prevailing coordination

violations where either backup operation and then primary operation or simultaneous operations on several property sections are found. As fault currents may not be adequately strong to ensure clear discrimination between protection zones, this impinges on the ability of the system to be selectively protected, i.e., isolate only the faulty portion of a network without affecting service in other areas. This may lead to overbroad service disruptions (wider than necessary) and greater system vulnerability. If fault currents are so low that reliable operation is complex, backup protection schemes (those meant to operate if primary protection fails) may no longer be effective. Ultimately, this results in single points of protection failure and decreases the total reliability of a system.

3.1.3 Directional Protection Element Challenges

Numerous protection schemes require directional protection elements, especially in networked systems where fault currents flow in different directions [15]. These features establish the direction of fault current flow to ensure that protection devices operate only for faults inside their designated protection zones. Directional elements need a minimum amount of current to operate with the desired accuracy and determine direction correctly. The absence of traditional unsynchronized operating characteristics within fault currents below these sensitivity thresholds in converter-dominated networks can make Directional elements unable to operate correctly or result in no operation. Certain directional elements use polarizing amounts, such as zero-sequence voltage, for ground fault direction determination, which the presence of converter sources can influence. Converter contribution to fault current is limited, and converters infer potential filtering effects on polarizing quantities, affecting their reliability. The Initial angle offsets introduced in fault currents by the control systems of converter sources, which could mislead the directional elements, have a direct correlation. The distortions thus caused can make the directional determinations wrong, and hence, result in improper operation of protection systems.

3.2 False Tripping and Sympathetic Tripping Phenomena

Protection system misoperations are problematic in converter-dominated networks and can lead to false and misleading tripping events. This affects system reliability and customer satisfaction with unnecessary service interruptions due to climatic disturbances.

3.2.1 Transient Response-Induced False Tripping

Due to their nature, power electronic converters are based on high-frequency switching operations, and they are operated with intelligent control techniques that may lead to short-term currents and voltages while the inverter is operating [16]. These transients are often mistaken for fault conditions by protection systems, which results in them tripping erroneously. Converters switch at frequencies from several kilohertz to tens of kilohertz, and in doing so can cause transient currents above the base power frequency. Although such transitory changes are a regular phenomenon arising during the operation of converters, with correlated protection responses, they fail to discriminate between switching-related and fault-based transients. The complexity in the transient patterns that occur when multiple converter control systems interact, especially during system disturbances or topology changes, may trigger traditional protection algorithms to detect it as a fault condition. The potential problem is especially intuitive in the case of networks with many converters of decreasing diversity, operating with control schemes using similar principles. The starting and stopping operations of a planned or forced converter controlled by the control systems can produce large transient currents that may exceed protection system limits. That can be not easy in renewable energy systems where converters might operate intermittently due to the availability of resources.

3.2.2 Harmonic Distortion Effects

Power electronic converters are harmonic sources due to their nonlinear switching characteristics (So and Wu 2008). Although modern converters employ sophisticated filtering and control techniques to reduce harmonic injection, some Degree of harmonic distortion is inevitable, influencing the behavior of protection systems. In a fault condition, the harmonic content of currents from the converter sources may differ significantly from that of the current from synchronous generators. The differences between VTB and CB could lead to misoperations of the protection algorithms that use harmonic analysis for fault detection and classification. The converter installations' filtering systems can wreak havoc on protection system algorithms. Passive filters can resonate between inductive and capacitive components, potentially amplifying specific harmonic frequencies, while active filters may introduce extra harmonic interference that impacts the function of the protection system. In some protection schemes, total harmonic distortion (THD) levels are monitored as they can indicate abnormal conditions within the

system. The regular operation of a converter may also increase the background THD levels in converter-dominated networks, reducing the detection sensitivity of THD-based protection methods and masking actual fault conditions.

3.2.3 Voltage Fluctuation-Induced Misoperations

Fast voltage variations caused by converter switching operations, load changes, and the system dynamic response can have undesired effects on the operation of voltage-based protection elements [18]. These voltage fluctuations are often still within the rated limits; however, rates are too rapid for traditional protection algorithms to identify, assess, and act upon. Operating as voltage-controlled current converters, these devices may quickly change the bus voltage magnitude in response to system conditions or commands from controllers. Such changes can cause acceleration of similarly tripped Over-voltage or Under-voltage protection elements, if protection settings are not adequately coordinated with the slew rates determined by the converter controls. Specific operating modes or fault conditions can lead to temporary voltage unbalance, which could be caused by three-phase converters. Protection measures implemented to detect excessive voltage imbalance can recognize these transients as system malfunctions, resulting in unnecessary system trips. A Degree of frequency fluctuations can also be introduced on account of the control systems within the converters themselves, which, if severe enough, can trip other protection elements (frequency-based). The dynamic behavior of frequency control systems in converter-dominated networks may lead to frequency excursions within the permissible operating region but exceed the grid protection system thresholds.

3.3 Loss of Protection System Robustness

Power system protection is very robust due to the application of different and redundant principles of protection, where several relays operate independently through separate channels to sense and detect faults over a wide range of system conditions. However, maintaining robustness in the face of complexity is also more challenging on converter-dominated networks.

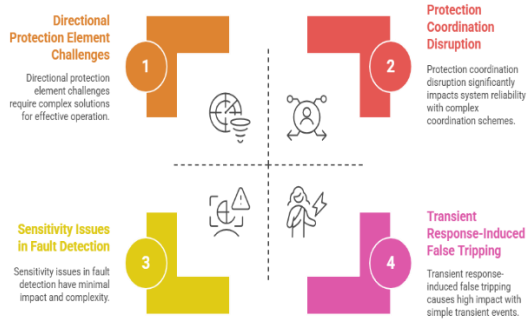

Figure 3. Challenges in Converter-Dominated Networks.

3.3.1 Reduced Protection Diversity

The resilience in the traditional power system protection is obtained using different protection principles, such as overcurrent protection, distance protection, differential protection, and directional protection [19]. Those principles use the physical phenomena, and our measured quantities of them, differently and redundantly enough that at least one of them usually fails safe with multiple failures. However, the similar response characteristics of converter sources in converter-dominated networks can limit their efficacy. Specific fault response characteristics can be described because identical control algorithms, current limiting strategies, and Grid Code compliance requirements are used for multiple sources in a network. This reduces the variety of fault signatures in critical conditions and consequently leads to the concurrent failure of several protection principles. It is suitable for interoperability and integration to the grid, but it undermines the robustness of protection systems since both converters behave more uniformly and predictably. The standardization may also remove the organic diversity in networks with multiple generations. Similar design practices about power electronic components and control hardware among several converter installations can lead to safe failure modes and similar responses on a protection system. In more traditional systems, a mix of generator types and ages naturally provided this diversity; however, modern converter installations are often very similar.

3.3.2 Common Mode Failure Risks

Most of these elements and systems are based on similar or the same converter technologies and control systems, which makes it easier for a common mode failure to affect multiple protection elements simultaneously [20]. It can happen because of software bugs, control algorithm limitations, or external problems affecting multiple converters similarly. Software algorithms are used to a significant extent by modern control systems in converters for regular operation and fault response. One major issue is that a fault in software or an algorithm limiting (causing over-reaching / under-reaching) may impact multiple installations of similar converters throughout the network, creating large-scale cybersecurity grid defense issues. Communication networks play a greater role in the ability of more advanced converter control systems to perform coordination and optimization functions. Fast-acting converter protection systems installed at specific converter locations can be activated because of communication system failures or even malicious cyber-attacks. If this occurs in multiple converters simultaneously, it could lead to a collapse of the entire system. Since the hardware being used and control algorithms are similar in various converter installations, they may be subjected to common external factors (environmental conditions, EMF, or disturbances in a grid), influencing them all simultaneously.

3.4 Microgrid Protection Challenges

Modes of these familiar environmental effects result in nationwide response actions and compromise the protection system's effectiveness! Background and Problem Definition Inverter-dominated systems are a subset of converter-dominant networks, and microgrids form an example of this class with some specific protection challenges brought by their ability to operate in split mode (grid-connected or islanded) and by their size and the traditions of having a high percentage of inverter-interfaced resources.

3.4.1 Islanding Detection and Management

Fast and accurate detection, identification, and operation for managing islanding conditions is fundamental in microgrid systems with high penetration of generation units [21]. Islanding detection: must differentiate between intentional islanding operations, which are part of typical microgrid functionality, and unintentional islanding events, which create safety hazards that necessitate protective action. Microgrids are intentionally designed to island during disturbances on the utility system to continue providing service to critical loads. Yet they might inadvertently island through protection system operations or equipment failures. Systems protection has to be able to differentiate reliably between the two and address them accordingly. All distributed generation interconnection standards require anti-islanding, as unintentional islanding can result in safety hazards. However, microgrids need the capability of intentionally islanding for resiliency. This presents a fundamental conflict requiring an advanced control and protection system design.

3.4.2 Bidirectional Power Flow Management

Switching between grid-connected and islanded operation results in considerable power quality disturbances, which may lead to incorrect operation of protection systems. Voltage and frequency excursions during islanding transitions must be controlled within the limits to prevent unwanted protection operations while maintaining power system stability. The load and generation balance must be met for a microgrid to island successfully. Protection system coordination with load shedding and generation control systems for protection reliability during islanded operation has to be considered. The traditional distribution system protection schemes have been designed using unidirectional power flow from utility sources to loads [6–8]. Distributed generation means power is flowing both ways on microgrids, and as a result, protection system designs and coordination have to change radically. A microgrid's protection system must support this bidirectional power and be capable of operating in both grid-connected and islanded modes. Coordinating directional protection elements becomes more complex, and care must be taken to ensure proper operation for all possible faults in forward and reverse flow directions. In other words, DC removal from the grid will alter fault current distribution patterns, which can become very complex and highly dependent on system operating conditions. To address this issue, protection coordination studies must account for every power flow state to detect and isolate faults accurately. This requires the automatic reclosing operations, common in distribution systems, to become much more complex, particularly for circuit breakers where generation can exist on both sides of the switching devices. Reclosers must be deactivated with distributed generation protection deactivated to protect against dangerous conditions and equipment damage.

3.4.3 Variable Network Configuration Challenges

The presence of distributed resources that go on and offline, loads being connected or disconnected, and network topology changes due to operational or maintenance practices make microgrids typically present a variable network configuration [23]. Topological changes, in turn, raise considerable issues for protection system coordination and maintenance. The solution? Modern protection systems are based on scenario settings and network transactions. In microgrids with a diverse topology, these hardcoded values may become unsuitable as network conditions change and eventually cause miscoordination or the collapse of the protection system. The defense systems need to be able to identify changes and respond accordingly. That calls for fancy monitoring and controlling features, which are not necessarily in all microgrid installations. Several protection systems can handle network configurations that can vary by using multiple setting groups, which can be selected based on system conditions. However, protecting systems over multiple setting groups complicates the protection system's design and operation. For instances where the microgrid configuration can switch, we need an overlaid protection coordination exercise that allows us to apply new values based on operating network conditions continuously. On the other hand, using such features necessitates a high level of communication, computation, and cooperation, which is still not state-of-the-art.

4. EMERGING PROTECTION SOLUTIONS

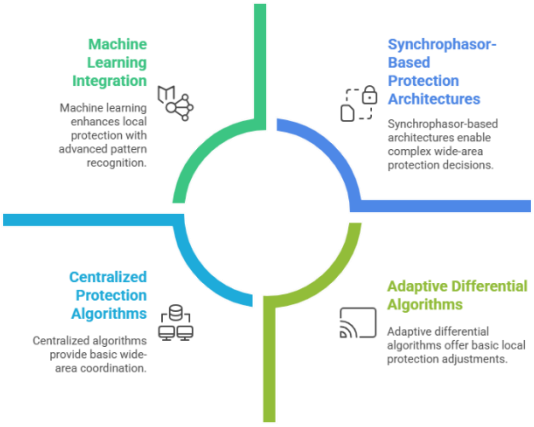

Figure 4. Emerging Protection Solutions in Convertor-Dominated Networks.

4.1 Adaptive Protection Schemes

Adaptive protection means a paradigm shift from traditional fixed-protection settings to innovative functions, which can dynamically adapt the function's characteristics and settings by analyzing real-time data. The method is adapted, in particular, for converter-dominated networks with strongly time-dependent system parameters and operation conditions.

4.1.1 Real-Time Setting Adjustment Mechanisms

An essential part is basic adaptive protection, ensuring optimal performance is maintained in various interruption scenarios. This principle is based on monitoring runtime conditions and adjusting settings in real time to deal with different operating conditions [24]. This provides the means to address many challenges seen in converter-dominated networks, such as maintaining the effectiveness of protection systems and fault ride-through capability under various network topologies, generation dispatch, or load conditions. Adaptive protection systems use intelligent surveillance know-how that constantly monitors system conditions, including voltage levels, current flows, impedance features, and power flow patterns. Advanced measurement systems, such as Phasor Measurement Units (PMUs) and Intelligent Electronic Devices (IEDs), deliver high-rate sampling data of the power grid to enable more accurate, real-time evaluation of the system's status. Current adaptive modern protection systems can calculate the best settings automatically to add to the productivity of an algorithm. A discrimination coordination algorithm considers fault current levels, impedance characteristics, coordination requirements, and sensitivity to derive suitable settings for each protection element. Adaptive systems could then implement these settings automatically without manual intervention. This automated approach helps facilitate fast responses in protection system operations as conditions change, and reliability is always optimal. Some more sophisticated adaptive-protection systems have validation and verification mechanisms that ensure the calculated settings are appropriate and safe before application. The mechanism may include simulation-

based validation, constraint checking, and coordination verification to prevent reservations from setting changes that inadvertently reduce the system's security.

4.1.2 Multi-Agent System Implementations

Multi-agent systems are a more sophisticated way of Adaptive Protection, which takes advantage of dividing intelligence among the protection system instead of relying on central decision-makers [25]. This becomes even more powerful in converter-dominated networks, where local conditions may vary significantly over the system. Multi-agent protection systems have numerous intelligent agents, each a protective decision maker over one area or equipment. While operating independently, these agents will communicate and coordinate with each other to achieve the best protection across the system. Functional multi-agent systems require reliable communication that can inform agents' decision-making, coordination, and overall situational awareness of the system. The problem is that such protocols should be designed to work even if the underlying communication system suffers a failure or a denial of service attack. Every agent in a many-agent system contains local control to the Degree that it could respond within its level to adjust to the dynamic situation, without looking forward to suggestions at a central control point. This is a more distributed way of spreading the load, faster reads, and has more sustainable systems. Emergent behaviours: Behaviour(s) of the multi-agent system that result from interactions between multiple agents in a population. Though these emergent behaviors could deliver superior system performance, they have to be controlled so that they do not interfere with the security or stability of the system.

4.1.3 Machine Learning Integration

Among the potentials of an adaptive protection system, deploying machine learning methods within the protection systems could be the most attractive [26]. Machine Learning: Identify patterns in system behavior, learn from historical data, and predict future system conditions for early protection actions. Machine learning algorithms are excellent at detecting sophisticated patterns from massive datasets, patterns that other analytical methods may not be able to find. For protection purposes, these algorithms may recognize fault signatures, differentiate between several system disturbances, and discover abnormal conditions that are precursors to any developing problem. Machine learning systems can mine this historical data at high speed and generate valuable information about trends, patterns, and relationships, which can be used in protecting. This analysis may provide subtle signs of system issues that would otherwise go unnoticed with standard protective means. More advanced machine learning systems can predict the future state of a system based on present measurements and past behaviour. These predictions provide more proactive protection, so that problems can be thwarted before they arise, or at least manage their consequences with minimal disruption to the system. These systems do not remain static. The more data and experience fed into them, the more they learn and slowly increase their performance over time. This strength is especially valuable in converter-dominated networks, where system characteristics can change as new technologies are switched on and operation changes.

4.2 Wide-Area Protection Systems

Wide-area protection (WAP) systems comprise a foundational shift in the design and architecture of protection systems, moving out of the historical local-based protection into an era that experiences coordinated protection actions at multiple locations across the network. This scheme can be valuable, especially in converter-dominated networks where the local measurements might not provide a precise line on the system's state.

4.2.1 Synchrophasor-Based Protection Architectures

The synchrophasor technology is achieved using phasor measurement units (PMUs), which yield synchronized and high-resolution voltage and current phasors at different locations in the power system [27]. That framework in Tang builds the highest-level wide-area protection systems that can take a globally coordinated action in system-global information. Synchronized measurements provided by PMU networks can report data in 30 to 120 samples per second, enabling real-time monitoring of system dynamics. GPS-synchronized time stamping allows measurements from different locations to be correlated and compared accurately. Synchrophasors make it possible to provide system-wide awareness that was unimaginable even a decade ago. This visibility allows for global system conditions, not purely local measurements, to be the basis of protection decisions. It provides a method for online monitoring and assessing system dynamic behavior, oscillations, stability margins, and transient responses using synchrophasor measurements. These can then be utilised to improve protection system performance and

prevent cascade failures. The wide-area protection systems incorporate synchrophasor data and combine it with traditional SCADA-based measurements to offer overall system monitoring facilities. This integration allows protection systems to use high-resolution dynamic measurements and traditional steady-state monitoring data.

4.2.2 Centralized Protection Algorithms

Coordinated protection decisions over the central data of multiple sources are realized by one centralized protection algorithm, which can be employed to exploit system-wide performance optimisation [28]. These algorithms can jointly consider global system conditions, coordination requirements, and optimization objectives. Centralized algorithms fuse data from various sources, such as PMUs, digital protective relays, SCADA systems, and other monitoring devices. These advanced data fusion techniques ensure that information is appropriately weighted and integrated for accurate system assessment across multiple sources. Global optimization algorithms, which can take a system-wide perspective, including customer-level (planning for service restoration to be as quick and efficient as possible), to minimize customer interruptions, maintain system stability, and optimize restoration from the operation, are managed from a centralized protection system. Without revealing the micro architectural states to software, those algorithms can make protection decisions that result in better system-wide performance than if local protection systems were working independently. Centralised algorithms can operate over several constraints, such as equipment thermal limits, voltage stability margins, system security requirements, and operational policies. This holistic constraint awareness enables safety-conscious protection decisions that preserve system security yet optimize functionality. More sophisticated centralized systems can choose which protection algorithms to employ as a function of the system's state at that moment. For instance, performance and precision, such as sensitivity and speed, can be considered when the system is in a nominal condition, while in downbeat intended states, safety and security can be chosen using stability and coming behavior features based on the model.

4.2.3 Communication Infrastructure Requirements

For wide-area protection systems, the essential elements in terms of functionality are not only primary/backup handover and critical time-response but also fast communication that can easily support a large amount of data across broad areas [29]. Communication demands for these systems are much higher than traditional protection systems. For wide-area protection applications, the communication latencies required are usually 2-4 milliseconds for critical protection functions. Ensuring this requirement may require dedicated communication channels or high-priority network services capable of delivering data with low latency. This involves a lot of communication bandwidth for continuous streaming synchrophasor data and other monitoring information. The PMU data streams are usually 64-128 kbps per PMU, and systems with hundreds of individual PMUs may need tens of megabits per second aggregate bandwidth. Reliability: For Wide-Area protection applications, the reliability of the communication system is paramount. Continuous operation in the face of communication system failures requires redundant communication paths and automatic failover capability using robust network architectures. Cybersecurity schemes should be developed and integrated appropriately with wide-area protection communication systems to prevent cyberattacks from exposing PAS functionality. For instance, encrypting data, using authentication between devices, detecting intrusions, and accessing safe network protocols.

4.3 Advanced Signal Processing Techniques

Converter-based networks are considered complex operational environments and therefore require advanced signal processing algorithms capable of extracting relevant information from noisy, distorted, and time-varying signals. Advanced signal processing techniques enhance the capability of protection systems to differentiate actual fault conditions from system transients, thus making the power system more secure and reliable.

4.3.1 Wavelet Transform Applications

Wavelet transform techniques assist in multi-resolution analysis; hence, the wavelet transform has been an essential tool for analyzing transient phenomena occurring in power systems [30]. Unlike the usual study of waves, where one looks at a single frequency band at a time, wavelets allow us to look all over the spectrum and maintain some resolution. Wavelet analysis is a method used to decompose signals into different frequency bands with variable time resolutions (Arya et al., 1999). Hence, it provides information on both high-frequency transients and low-frequency system dynamics. These findings are

significant in analyzing quick converter switching transients and separation from fault-related transients. Based on wavelets, these algorithms can identify transition events and group them according to their time-frequency characteristics. This feature allows the protection system to differentiate between various types of transients, e.g., converter switching events, fault inception, and load switching operations. Wavelet analysis techniques can dampen noise and interference, which might be included in measuring a protection system. Enhanced signal quality and improved protection system decision-accuracy require advanced wavelet denoising algorithms. Wavelet transforms are particularly suited to extracting only the most crucial information from complex signals that indicate certain system conditions or events. They can be used as input to pattern recognition algorithms or machine-learning systems for improved fault detection and classification.

4.3.2 Advanced Fourier Analysis Methods

Classical Fourier analysis has limitations in the case of time-varying systems; however, other advanced time-honored Fourier-based techniques can provide useful frequency domain information for protection applications [31]. We will apply these methods to study converter-enriched networks' underlying harmonic composition and frequency domain specifics. The STFT allows frequency domain analysis with a much better time resolution than traditional Fourier analysis. This method can monitor harmonic changes of a process and identify the frequency content feature related to multiple classes of system events in the time domain. Recursive DFT algorithms with high computation throughput are well-suited to perform real-time frequency domain analysis for protection system applications. They can recalculate frequency domain information as new samples come in. Harmonic content is free from noise or other interference and can be measured accurately using advanced Fourier techniques. This is a critical feature for protection systems operating in converter-dominant networks, as disturbance harmonics are common. Frequency detection functions in real time will change analysis parameters to adapt to the new system frequency using adaptive Fourier analysis techniques. This is essential, especially for islanded microgrids, where the frequency could deviate significantly from the nominal value due to non-dispatchable distributed generation. Hence, pattern recognition methods with machine learning provide an effective tool for the fault detection and classification in challenging converter continental European networks [32]. These approaches can even detect patterns in measurement data that could be too weak for standard analytical techniques.

4.3.3 Pattern Recognition and Machine Learning Integration

Pattern recognition in this sense relies on well-defined feature spaces that capture subtle differences between system states - a task, most commonly referred to as feature engineering. These may comprise statistical statistics, frequency domain traits, time-domain parameters, and derived quantities that discriminate among different occasions. Training machine learning models requires a lot of data to perform well. This data can be related to past incidents, simulation studies, or even controlled testing procedures in protection applications. The performance of algorithms greatly depends upon the quality and representativeness of training data. Different machine learning algorithms may suit each type of protection application. It is essential to protect the system from Homeomorphic Attacks. Still, not all machine learning models are equally good at this task, depending on weights and feature extraction method, support vector machines, neural networks, decision trees, ensemble methods ...Different Machine Learning algorithms have strengths and weaknesses that must be accounted for in protection system design. This required the implementation of pattern recognition algorithms that could operate in real-time enforcement applications. This could range from algorithm optimization, parallel processing, hardware-specific deployments, etc., to a level you can afford to achieve the desired performance.

4.4 Differential Protection Enhancements

Therefore, differential principles are still applied in converter-dominated networks, and the classical implementations need considerable modifications to cope with the peculiarities of converter sources. These improvements relate to the adaptation of differential algorithms for converter-specific phenomena. Still, at the same time, they make sure that they do not compromise the inherent security and reliability benefits attributed to differential protection.

4.4.1 Adaptive Differential Algorithms

Flexible differential protection strategies can vary their tripping characteristic depending on the converter operating modes and conditions of the system [6]. This implementation enhances the effectiveness of differential protection in converter-dominated networks under various operating conditions

encountered. Before it can begin to establish a per-unit model of the converter sources in the protected zone, an adaptive differential system needs to detect their operating mode. Regardless of the operation mode, i.e., grid-following vs. grid-forming operation, different parameters must be set for optimal performance. The fixed operating thresholds of traditional differential protection may not be appropriate for converter sources with limited fault current capability. These thresholds are adjusted by adaptive systems, depending on the actual characteristics of the converter and its state of operation. For the application to converters, adjusting slope characteristics of differential protection (differential curve concerning restraint and operating quantities) might also be necessary. Converter control mode and system conditions can change these characteristics, and adaptive systems can adjust. The results have indicated the potential for current transformer saturation to impact differentiation protection performance, especially under high-current fault conditions. Thus, the CT saturation effect can be avoided with the help of adaptive algorithms, such that they continue to detect and provide accurate protection even under challenging conditions.

4.4.2 Harmonic Restraint Modifications

Sources of converters inject harmonic quantities that might hinder the differential protection performance. Post-contingency harmonic restraint signals are being studied for their feasibility of online fault detection related to the converter operation [34]. Each type of converter produces characteristic harmonics that can be used to determine if it is operating correctly. These patterns can be learned via adaptive harmonic restraint algorithms, which tailor restraint characteristics to the particular pattern. Dynamic harmonic filtering, an advanced type used on more sophisticated differential systems, responds to the change in harmonic conditions. Such a filter can cancel the harmonics due to the converter, but does not affect the harmonics due to the fault. Modern systems can identify various system conditions by analysing several harmonic frequencies, rather than using the classical second and fifth harmonic restraint. The converter operation can cause harmonic cross-coupling between phases in three-phase differential systems. Improved algorithms must consider these cross-coupling effects to ensure continued protection precision.

4.4.3 Communication-Based Differential Protection

Modern examples of this are represented by communication-based differential protection schemes in which measurements from remote locations via high-speed communication channels enable differential protection over large areas [35]. Such schemes are beneficial in converter-dominated networks, where traditional current transformer-based approaches may be inadequate. Standardized digital communication protocols such as IEC 61850 GOOSE messages or in-house high-speed protocols are used in modern communication-denominated differential systems. They are equipped with your bio-readings protocols that send current measurements and control signals. The time synchronization in this process is essential for the proper differential protection. It is possible to compare present images recorded at different locations with the help of GPS-based synchronization systems or high-precision network timing protocols. Systems with communication may also monitor data quality reports at intervals to catch communication errors, timing issues, or failed measurements. Sophisticated data quality monitoring algorithms can help differentiate actual differential conditions from communication issues. Strong communication-based differential systems have fallback operating modes where bearing protection can be provided while the primary communication means have failed. These fallback modes can use local measurements or simplified protection algorithms.

5. COMMUNICATION-BASED PROTECTION SYSTEMS

In converter-dominant networks, the evolution towards more advanced protection systems has led to an ever-growing reliance on both communication technologies. Because these approaches are based primarily on communication, they can prevent coordination between many protection devices, require central decision-making authority, and support advanced protection algorithms that need data from various sources.

Figure 5. Communication-Based Protection Systems.

5.1 IEC 61850 Standard Integration

The IEC 61850 standard has become the mainstream communication standard in substation automation and protection systems. It provides a complete protocol for manufacturing intelligent electronic devices (IEDs) and Detailed Editorial Correction Values.

5.1.1 Standardized Data Models and Object-Oriented Approach

The IEC 61850 defines the standardized data models necessary for protection devices of different vendors to interact with each other [36]. Standardization is especially needed when it comes to converter-dominated networks that not only have many types of equipment but also have the mentioned devices delivered by different vendors (to ensure better pan-vendor compatibility). IEC 61850 LNs: Functionality is organized into dedicated logical nodes (LNs), corresponding to specific protection or control functions. Data objects represent measurements, settings, and control points for each logical node. This hierarchical structure allows protection system functionality to be coded consistently across implementations, devices, and standards. It defines common data classes (CDCs) that describe the layout and operation of different data object categories. These standardized classes consistently represent similar types of information across different devices and applications. IEC 61850 allows detailed device modeling, so it is possible to describe the whole protection system functionality in a structured, standardized way. This forms a model that contains all a device's non-measurement and control data (device capabilities, configuration information, diagnostic data, etc.). IEC 61850-enabled devices can automatically provide rich self-description information that helps discover and configure the system components. This is especially true in large, intricate protection systems where configuring manually would be time-consuming and error-prone.

5.1.2 High-Speed Communication Services

Several communication services are defined within IEC 61850 that have been tailored for different protection system needs [37], primarily focusing on high-speed applications that demand deterministic communication performance. GOOSE (Generic Object Oriented Substation Event) messages are suitable for high-speed and multicast communication of time-critical protection applications. The GOOSE messages are transmitted within 4 milliseconds in response to a specific trigger. Consequently, they are used for protection without considering the problems related to latencies that occur in peer-to-peer communication. It has two purposes: high-speed transmission of digitized current and voltage waveforms from instrument transformers to protection devices over the Sampled Values (SV) service. This service replaces traditional analog current and voltage circuits, which allows flexibility in protection system design with more accurate elements. MMS is suitable for applications that are not time-critical and require client-server communication, such as parameter setting, data retrieval, and system configuration. Although slower than GOOSE, MMS offers a connection-oriented communication path for deterministic and real-time applications. IEC 61850 provides detailed support for accurate time synchronization via protocols like Simple Network Time Protocol (SNTP) or Precision Time Protocol (PTP). Your protection actions and event analysis may be time-coordinated, so it is essential to have real-time, accurate, synchronized time.

5.1.3 Configuration Management and Engineering Tools

Modern protection systems' complexity demands advanced configuration management tools that accurately grasp the intricate interactions between numerous devices and communication services. According to 38, IEC 61850 provides a standardized XML-based language for protection system configuration description. SCL files contain complete descriptions of system architecture, device capability, communication services, and parameter values. Standardized configuration languages facilitate

the integration of engineering tools from various vendors. Therefore, protection engineers can employ best-of-breed configuration tools while ensuring system-wide consistency and compatibility. Advanced configuration management tools offer version control functions, tracking configuration changes over time. This is crucial for protecting system integrity and ensuring the reversibility of any transformation if the implemented configuration leads to unpredictable behavior. Configuration management systems provide automated validation and verification of protection system configurations to identify errors, inconsistencies, or potential coordination issues before installation.

5.2 Cybersecurity Considerations

The dependence of protection systems on communication technologies generates multiple cybersecurity risks that should be dealt with accordingly to secure the system performance. Cybersecurity in communication-based protection systems relies on three lines of defense: technical, procedural, and organizational measures. **5.2.1 Authentication and Access Control Mechanisms**

Robust authentication and access control systems are required to prevent brute-force access to the protection systems. It needs to be balanced with the necessity to respond rapidly in emergencies. Multi-factor authentication is available in advanced protection systems, where multiple credentials are required for identification. Role-based access control is also applied to secure the system against unauthorized internal access. Public key infrastructure is used for certificate-based user identification. Certificate management systems are responsible for certificate generation, distribution, renewal, and revocation during the system lifecycle. Nothing detrimental to Date() Session management is implemented to establish, monitor, and terminate user sessions. The session may be limited by timeouts and concurrent sessions, and may be encrypted to prevent unauthorized access through any compromised session.

5.2.2 Encryption and Data Protection

Data in transit and at rest must be well protected against eavesdropping, tampering, and unauthorized information disclosure [40]. The connection between protection systems' devices must be secured just like how all App Store communication is securely done over HTTPS, and even more so, all the traffic transiting along these channels must be strongly encrypted with a cipher suite using something like an Advanced Encryption Standard (AES). However, this encryption must not interfere with the real-time throughput metrics protection applications require. Integrated key management mechanisms should support encryption/decryption keys generation, distribution, storage, and rotation. Automate key management wherever possible and in compliance with security policies. Using digital signatures and message authentication codes (MACs) to detect tampering verifies that the messages received have been unmodified and in transit. This protection is critical, especially for control messages that the protection system uses to activate devices. Records and configuration files of the protection system need to be kept secure with proper access control and in an encrypted form. All backup and archival systems provide the same assurance as primary storage systems.

5.2.3 Intrusion Detection and Response

Comprehensive Intrusion Detection Systems (IDS) monitor protection system networks for indications of unauthorized access or malicious activity [41]. Such systems also have to recognize familiar attack patterns and unusual behavior (that might indicate a new or previously unknown/understood nature of threat). An analysis of network flows can be used to determine communications anomalies that could be cyber-offensive. The machine learning standards can recognize what regular network traffic looks like to realize when a departure warrants further examination. On the other hand, host-based intrusion detection systems have sensors placed on every host, which means watching out for potential intrusions by monitoring files and processes running on a local host. Intrusion detection systems can be programmed to recognize or anticipate what a suspicious user or system may do next. The ARS can identify insider threats, along with slow-and-low attacks, that signature-based detection methods may be unable to detect. Incident response is responding to cybersecurity incidents once identified, and a set of procedures should be defined to help protectors respond effectively. These processes must challenge the constraints of reacting quickly and ensuring system operation even in an emergency.

6. FUTURE RESEARCH DIRECTIONS

The protection of converter-dominated networks is a rapidly developing area, and new technologies are emerging in the market. In some regions, penetration levels have increased to almost 100% of power

delivery systems. We mentioned some of the ways these research directions seem promising in providing more support against defeating some of them with more proactive mitigation options.

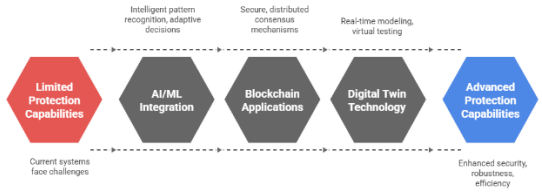

Figure 6. Enhancing Protection Systems with New Technologies.

6.1 Artificial Intelligence and Machine Learning Integration

Artificial Intelligence (AI) and Machine Learning (ML) are some of the most interesting fields for future development in protection systems. These technologies provide an opportunity to converge deterministic and analytical methods for pattern discovery, predictive analytics, and adaptive decision-making, which could potentially ease most of the complexities posed by converter-dominated networks.

6.1.1 Deep Learning Applications

In recent years, deep learning methods, particularly using multi-layer neural networks, have demonstrated unprecedented promise for analyzing complex patterns in data from power systems [9]. Such techniques can pick up on nuanced signs of an underlying problem within a system that might not be made evident through any traditional analytical mechanism. Time-series data and waveform measurements can be analyzed using CNN architectures. They have the potential to detect fault signatures in converter-dominated networks by looking at time-domain features of current and voltage waveforms. RNN architectures like Long Short-Term Memory (LSTM) are designed to work with sequential data to mine temporal patterns for early signs of trouble or to identify changes in the system behavior. These are of particular interest in studying transient network dynamics in converter-dominated networks. Autoencoder neural networks can learn representations of 'normal' system behavior and can detect the occurrence of anomalies that deviate from learned patterns. This feature is handy for detecting atypical system situations that do not synergistically cover the existing fault buckets. The techniques around transfer learning allow neural networks trained on one machine or data set to be adapted for use on other machines with minimum additional training. Such capability could lead to a significant decrease in the data needed and time of training to deploy AI-based protection systems

6.1.2 Reinforcement Learning for Adaptive Protection

Reinforcement learning (RL) is an extraordinary strategy that offers the potential to create adaptive protection systems that can learn optimal strategies using their interaction with the power system environment [49]. Q-learning algorithms can learn the optimal protection actions of various system states by trying all possible action alternatives and learning from their consequences. The implication is that the protection system will be able to commit more intelligent actions in tackling conditions that are many-fold system effects. Several policy gradient reinforcement learning methods have been proposed to solve the problem of protection policies (i.e., protecting devices under attacks or failures) that directly optimize performance objectives such as a minimum number of customer interruptions, maximum system security level, or minimum restoration time. It's like Multi-agent RL, where all the protection agents in your system learn and act together. This is important if a distributed system implements the protection, and local agents must reason about their actions to contribute efficiently to global outcomes. Traditional reinforcement learning algorithms may take actions that could harm the system's security during the learning process. This includes techniques from the area of safe reinforcement learning, which ensure that learning algorithms do not violate safety constraints and keep within bounds at each step in order not to cause harm to the power system.

6.2 Blockchain Technology Applications

Blockchain technology offers unique capabilities for enhancing protection system security, enabling distributed consensus mechanisms, and providing tamper-proof records of protection system operations [50].

6.2.1 Distributed Consensus for Protection Decisions

Such blockchain-based consensus mechanisms enable loosely connected protection systems to coordinate autonomously without a central control system. A blockchain consensus algorithm must be fault-tolerant or not worthy of the name. A network agreement system only has meaning if it functions as intended despite arbitrary participant actions. Finally, operating against the background significantly increases the resilience of protection systems, even in cases where some protection equipment is unusable. Protect ONLINE – could be implemented via proof-of-authority consensus mechanisms, where certified protective devices vote on protection decisions according to their local measurements and analysis. Decentralizing protection logic—this could be implemented as smart contracts in a distributed, tamper-proof way. It might be that protection rules and coordination schemes are encoded as smart contracts that automatically execute based on systemic conditions. Blockchain technology can further help decentralized protection coordination, where many protection devices meet consensus on the correct action without a central coordination authority.

6.2.2 Tamper-Proof Logging and Audit Trails

Blockchain can also provide unchangeable proof of action that helps in post-event analysis and compliance [51]; Relay operations, setting changes, and communication events could all be recorded in a blockchain, which would allow for an end-to-end audit of all the actions taken as part of the protection system to be maintained on that blockchain—event Records for Forensic Analysis. Because event records are used to verify system events and compare these to known responses by the network protection system, they can be enhanced using blockchain. Immutable event records would greatly aid in achieving regulatory compliance, offering irrefutable documentation that the system performed as designed and operated in complete compliance with prescribed procedures. It can allow utilities to securely share information about their protection system with other utilities and maintain an end-to-end integrity within the data, such that they are not tampered with, testifying to some guarantee against attacks.

6.3 Digital Twin Technology

Digital twin concepts represent a revolutionary design, testing, and operation approach that could transform how protection systems are developed and maintained [52].

6.3.1 Real-Time System Modeling

The digital twins generate models of power systems that resemble real physical system behavior as accurately as possible, simultaneously becoming a real-time updated version. By collecting real-time measurements from the live plant, digital twin models are updated continuously, accurately depicting the system's current state. Digital twins can operate faster than real time, providing the ability to predict system conditions or issues of tomorrow. This predictive capability would allow protective actions to be taken before problems happen. Being digital, the twins widely facilitate fast analysis of what-if scenarios regarding the impact/consequences of various forms of protection or system reengineering. Digital twins offer an environment for the steady-state verification of security system models and attributes by verifying estimated conduct with true-device performance.

6.3.2 Virtual Testing and Validation

This means the digital twin system test will change the traditional protection system test, emulating physical behavior in a virtual environment to realize unified testing [53]. Digital twins can be interfaced with physical protection equipment so the latter can do hardware-in-the-loop testing where the behavior of complete virtual power systems is simulated exactly like real-world systems. The project has already produced a first-of-its-kind dynamic-security virtual testbed that tests protection systems in a domain that would be impractical or unsafe to do with actual physical systems. Digital twins that can run at higher speeds can be used to conduct experiments over extended durations in seconds. Virtual Testing environments enable protection systems to be thoroughly tested under extreme or hazardous conditions without risk to physical equipment or personnel.

7. CHALLENGES AND LIMITATIONS

Despite the significant progress in developing protection solutions for converter-dominated networks, several challenges and limitations impede the widespread implementation of advanced protection technologies.

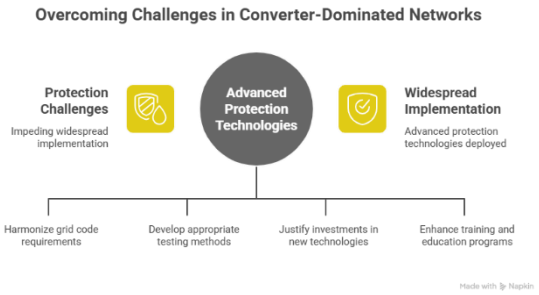

Figure 7. Overcoming Challenges in Converter-Dominated Networks.

7.1 Standardization Issues

The lack of comprehensive standards for protection systems in converter-dominated networks presents significant challenges for equipment manufacturers, system operators, and consulting engineers.

7.1.1 Grid Code Harmonization Challenges

Finding 53 B Grid Code Requirements Differ by Jurisdiction for Converter-Interfaced Generation, Making Equipment Manufacturer and System Operator Compliance Difficult. Grid codes in some regions may have different fault ride-through demand, power quality standards, and protection function requirements. This thrust asymmetry makes it challenging to design equipment that works across product platforms and requires manufacturers to customize equipment for different markets. There are instances where the needs of standards or regulations from counterpart authorities collide and become so adversarial with others that it is impossible to meet all the relevant requirements at once. Experience gains with converter-dominated Networks entail continuous evolution of Grid codes—such differences and variations challenge equipment designed to satisfy older standards revisions, necessitating retrofitting or replacement. Differing country standards can restrict international trade in protective equipment and hinder the worldwide spread of comprehensive protection concepts.

7.1.2 Testing and Certification Standards

The implementation to validate the performance of protection systems in converter-dominant networks still does not provide standards with comparable performances [55]. The performance assessment methods used in conventional protection system testing may not be suitable for converter-dominated networks. There is a substantial requirement for new testing approaches that faithfully reflect the behaviour of converter sources and network regimes. Additionally, the certification process of protection equipment has to be adapted for these specific situations observed in a converter-dominated network. This also allows for the certification of communication-based protective schemes, adaptive protection algorithms, and other AI-based protection methods. As communication-based protection schemes are increasingly used, there is a growing requirement for wide-ranging interoperability testing to ensure equipment from different vendors can interoperate successfully. For instance, in converter-dominated networks, new metrics for performance evaluation could be necessary to assess the effectiveness of a protection system. However, new metrics, such as speed and selectivity, will need to be introduced alongside traditional ones to evaluate security, adaptability, and robustness.

7.2 Economic Considerations

Implementing advanced protection systems for converter-dominated networks involves significant economic considerations that must be carefully evaluated.

7.2.1 Capital Investment Requirements

Advanced protection technologies typically require higher initial capital investments than traditional protection systems [56]. Advanced protection equipment, including PMUs as mentioned in Section 6.2.1, advanced protection technologies generally require a higher upfront investment than conventional protection systems [56]. Advanced protection equipment, such as the PMUs, communication systems, and intelligent electronic devices, is usually more expensive than traditional protection equipment. There is a potential for relatively higher costs to hamper uptake, particularly by smaller utilities or in developing countries. More generally, such advanced protection systems may need new communication infrastructure, computing facilities, and training programs that can amount to significant added-value investments over and beyond the cost of the protection equipment. The enhancement of protection systems with advanced techniques often causes a substantial increase in coordination within the current

utility infrastructure, especially considering that a transitional coexistence period must be made together with the old traditional systems. Advanced protective environments can be designed to cost more up front, and sometimes also cost more across the life of an ecosystem due to software updates, cybersecurity measures, and advanced maintenance needs., communication systems, and intelligent electronic devices typically cost more than traditional protection equipment. These higher costs can hinder implementation, particularly for smaller utilities or developing countries. Advanced protection systems may require new communication infrastructure, computing facilities, and training programs that represent significant investments beyond the protection equipment. Integrating advanced protection systems with existing utility infrastructure can be complex and expensive, particularly when legacy systems must be maintained during transition periods. While advanced protection systems may have higher initial costs, they may also have higher lifecycle costs due to software updates, cybersecurity measures, and specialized maintenance requirements.

7.2.2 Benefit-Cost Analysis Challenges A potential drawback of enabling conditions with this advanced protection is the difficulty in quantifying durable correct operation that requires confidence in capital investments for new technologies [57]. The reliability impacts of sophisticated protection systems—the decreased outage frequency and duration—can be hard to pinpoint. Much of the value of more sophisticated protection systems results from cost savings due to avoided damage, shorter restoration times, and better customer satisfaction. It can be hard to identify these avoided costs, and they are likely not included in the standard cost-benefit analysis. The regulatory frameworks in place to govern the activities of the utilities may fail to recognize or create a financial reward for establishing new advanced protection systems. The concern is that traditional rate-making might not supply the fairest cost recovery model for protecting system investments. However, the benefits of advanced protection systems typically result in improved performance upon the rare, high-consequence event occurrences. Estimating these benefits requires a complex risk assessment methodology for low-probability, high-consequence events.

7.3 Skills and Training Requirements

The complexity of modern protection systems requires enhanced training and education programs for protection engineers and system operators.

7.3.1 Educational Program Development

To address the need to secure converter-dominated networks, educational institutions should develop new curricula and training programs to prepare engineers to face these challenges [58]. Conventional power system protection courses must be enhanced to cover the technological advances associated with converters, sophisticated signal processing algorithms, communication-based large-power system protection systems, and cybersecurity aspects. Making these updates calls for a significant commitment to faculty development and courseware. Protection engineers in converter-dominated networks must have expertise in protection fundamentals and power electronics, control systems, communication networks, and cybersecurity. The interdisciplinary nature of this requirement will force educators to break down traditional educational silos and develop a new pedagogy for engineering education. This requires students to also touch the modern protection systems in action, and see how converter-dominated networks work. Colleges must invest in the costly upkeep of modern laboratory equipment and simulation tools. The paper recommended more continuing education opportunities for practicing engineers to help them transition their skills in a world of converter-dominated networks. Action should be taken to create and sustain professional development programs that cater to his needs until the end of his career.

7.3.2 Simulation and Training Tools

Protection Engineer Training and Testing: Protection System Simulation. The new challenges in protection design are due to changes introduced by technology or design methodologies, which require advanced tools/simulation for training protection engineers [59]. With real-time simulation platforms, training new engineers on protection systems can be easily accomplished without the expense and danger of testing on a live power system. To provide good training experiences, these platforms must model converter behavior and network dynamics. Workshops in which engineers can train on operating and maintaining the protection system could be provided using immersive training experiences, such as virtual reality (i.e., Virtual Reality or VR) and augmented reality (AR). Some gamification techniques, such as scoring, competition, and progressive skill development, can be implemented to turn protection system

training into a game. Online collaboration platforms could also support protection engineers across multiple entities to share practices, co-create ideas, and provide joint training.

8. CONCLUSION

Converter-dominated power networks represent a significant change in how the system operates compared to the classical grid composed of synchronous generators, and traditional protection has not been easily adapted to these changes. Converters inject little fault current (converting system type), have source impedance that varies with mode, and operate in such a way as to defeat conventional overcurrent or distance protection. However, new solutions are on the horizon, such as adaptive protection schemes that can adapt to different fault conditions, multi-terminal wide-area protection systems based on synchrophasor technology, and artificial intelligence algorithms for pattern recognition by the protective relay. However, wind farms, solar installations, and microgrids are proving the concept in practical examples, but there are still problems with standardization, economic rationality, and workforce training. Achieving that will demand a multi-pronged strategy that weaves together technological advances, regulatory collaboration, and educational outreach to guarantee dependable safeguards as power systems march toward deeper converter integration spurred by decarbonization targets.

REFERENCES

[1] B. Kroposki et al., "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," IEEE Power Energy Mag., vol. 15, no. 2, pp. 61-73, Mar./Apr. 2017.
[2] J. Rocabert et al., "Control of power converters in AC microgrids," IEEE Trans. Power Electron., vol. 27, no. 11, pp. 4734-4749, Nov. 2012.
[3] P. Denholm et al., "Grid flexibility and storage required to achieve very high penetration of variable renewable electricity," Energy Policy, vol. 39, no. 3, pp. 1817-1830, Mar. 2011.
[4] A. G. Phadke and J. S. Thorp, Computer Relaying for Power Systems, 2nd ed. Hoboken, NJ: Wiley, 2009.
[5] J. Driesen and K. Visscher, "Virtual synchronous generators," in Proc. IEEE Power Energy Soc. General Meeting, Pittsburgh, PA, USA, Jul. 2008, pp. 1-3.
[6] T. Ackermann et al., "Distributed generation: A definition," Electric Power Syst. Res., vol. 57, no. 3, pp. 195-204, Apr. 2001.
[7] N. Hatziargyriou et al., "Microgrids," IEEE Power Energy Mag., vol. 5, no. 4, pp. 78-94, Jul./Aug. 2007.
[8] J. Bialek et al., "Benchmarking and validation of cascading failure analysis tools," IEEE Trans. Power Syst., vol. 31, no. 6, pp. 4887-4900, Nov. 2016.
[9] M. Liserre et al., "Grid converters for photovoltaic and wind power systems," Hoboken, NJ: Wiley-IEEE Press, 2011.
[10] E. Troester, "New German grid codes for connecting PV systems to the medium voltage power grid," in Proc. 2nd Int. Workshop Concentrating Photovoltaic Power Plants, Darmstadt, Germany, Mar. 2009, pp. 1-4.
[11] Q. C. Zhong and G. Weiss, "Synchronverters: Inverters that mimic synchronous generators," IEEE Trans. Ind. Electron., vol. 58, no. 4, pp. 1259-1267, Apr. 2011.
[12] L. Harnefors et al., "Dynamic analysis of grid-connected voltage source converters," IEEE Trans. Power Electron., vol. 22, no. 6, pp. 2526-2537, Nov. 2007.
[13] S. M. Brahma and A. A. Girgis, "Development of adaptive protection scheme for distribution systems with high penetration of distributed generation," IEEE Trans. Power Del., vol. 19, no. 1, pp. 56-63, Jan. 2004.
[14] H. H. Zeineldin et al., "Impact of distributed generation on the coordination of protection systems in distribution networks," in Proc. IEEE Power Energy Soc. General Meeting, Detroit, MI, USA, Jul. 2011, pp. 1-8.
[15] N. Kagan et al., "Directional overcurrent protection in distribution systems with distributed generation," in Proc. IEEE Power Energy Soc. General Meeting, San Diego, CA, USA, Jul. 2012, pp. 1-7.
[16] M. Baran and I. El-Markaby, "Fault analysis on distribution feeders with distributed generators," IEEE Trans. Power Syst., vol. 20, no. 4, pp. 1757-1764, Nov. 2005.
[17] J. H. R. Enslin and P. J. M. Heskes, "Harmonic interaction between a large number of distributed power inverters and the distribution network," IEEE Trans. Power Electron., vol. 19, no. 6, pp. 1586-1593, Nov. 2004.
[18] T. Loix et al., "Protection of microgrids with a high penetration of inverter-coupled energy sources," in Proc. CIGRE/IEEE PES Joint Symp. Integration Wide-Scale Renewable Resources Power Del. Transmission Networks, Calgary, AB, Canada, Jul. 2009, pp. 1-6.
[19] H. J. Altuve Ferrer and E. O. Schweitzer III, Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems. Pullman, WA: SEL, 2010.
[20] P. Mahat et al., "A simple adaptive overcurrent protection of distribution systems with distributed generation," IEEE Trans. Smart Grid, vol. 2, no. 3, pp. 428-437, Sep. 2011.
[21] Z. Ye et al., "Evaluation of anti-islanding schemes based on nondetection zone concept," IEEE Trans. Power Electron., vol. 19, no. 5, pp. 1171-1176, Sep. 2004.
[22] S. Chaitusaney and A. Yokoyama, "Prevention of reliability degradation from recloser-fuse miscoordination due to distributed generation," IEEE Trans. Power Del., vol. 23, no. 4, pp. 2545-2554, Oct. 2008.
[23] A. Zamani et al., "A communication-assisted protection strategy for inverter-based medium-voltage microgrids," IEEE Trans. Smart Grid, vol. 3, no. 4, pp. 2088-2099, Dec. 2012.
[24] S. H. Horowitz and A. G. Phadke, "Adaptive relaying," IEEE Comput. Appl. Power, vol. 3, no. 3, pp. 47-51, Jul. 1990.

[25] G. Joos et al., "The potential of distributed generation to provide ancillary services," in Proc. IEEE Power Energy Soc. General Meeting, San Francisco, CA, USA, Jun. 2000, pp. 1762-1767.
[26] Y. Zhang et al., "Machine learning-based protection scheme for low-voltage DC microgrids," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5230-5240, Sep. 2019.
[27] A. G. Phadke, "Synchronized phasor measurements in power systems," IEEE Comput. Appl. Power, vol. 6, no. 2, pp. 10-15, Apr. 1993.
[28] V. Terzija et al., "Wide-area monitoring, protection, and control of future electric power networks," Proc. IEEE, vol. 99, no. 1, pp. 80-93, Jan. 2011.
[29] M. Kezunovic et al., "Smart fault location for smart grids," IEEE Trans. Smart Grid, vol. 2, no. 1, pp. 11-22, Mar. 2011.
[30] S. Santoso et al., "Power quality assessment via wavelet transform analysis," IEEE Trans. Power Del., vol. 11, no. 2, pp. 924-930, Apr. 1996.
[31] A. A. Girgis and F. M. Ham, "A quantitative study of pitfalls in the FFT," IEEE Trans. Aerosp. Electron. Syst., vol. AES-16, no. 4, pp. 434-439, Jul. 1980.
[32] F. V. Lopes et al., "A traveling-wave detection method based on Park's transformation for fault locating in transmission lines," IEEE Trans. Power Del., vol. 28, no. 3, pp. 1626-1633, Jul. 2013.
[33] E. O. Schweitzer III and D. Hou, "Filtering for protective relays," in Proc. IEEE WESCANEX 93 Communications, Computers Control Power Ind., Saskatoon, SK, Canada, May 1993, pp. 15-23.
[34] J. Lewis Blackburn and T. J. Domin, Protective Relaying: Principles and Applications, 3rd ed. Boca Raton, FL: CRC Press, 2006.
[35] K. Zimmerman and D. Costello, "Impedance-based fault location experience," in Proc. 58th Annu. Conf. Protective Relay Engineers, College Station, TX, USA, Apr. 2005, pp. 211-226.
[36] "Communication protocols for smart substations," IEC 61850 Standard, International Electrotechnical Commission, Geneva, Switzerland, 2003.
[37] T. S. Sidhu et al., "IEC 61850-based communication in a centralized protection and control scheme for electrical power systems," in Proc. IEEE Power Energy Soc. General Meeting, Tampa, FL, USA, Jun. 2007, pp. 1-8.
[38] U. D. Annakkage et al., "Current status of IEC 61850 applications in protection and control," in Proc. IEEE Power Energy Soc. General Meeting, Calgary, AB, Canada, Jul. 2009, pp. 1-7.
[39] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," in Proc. IEEE Power Energy Soc. General Meeting, Detroit, MI, USA, Jul. 2011, pp. 1-5.
[40] Y. Wang et al., "Cyber security for the smart grid," USENIX Login, vol. 36, no. 5, pp. 40-45, Oct. 2011.
[41] S. Sridhar et al., "Cyber-physical system security for the electric power grid," Proc. IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012.
[42] J. Morren and S. W. H. de Haan, "Protection of distributed generation connected through an electronic interface," in Proc. 8th IEE Int. Conf. Developments Power System Protection, Amsterdam, The Netherlands, Apr. 2004, pp. 98-101.
[43] M. Tsili and S. Papathanassiou, "A review of grid code technical requirements for wind farms," IET Renew. Power Gen., vol. 3, no. 3, pp. 308-332, Sep. 2009.
[44] J. Johnson et al., "Photovoltaic DC arc fault detector testing at Sandia National Laboratories," in Proc. 37th IEEE Photovoltaic Specialists Conf., Seattle, WA, USA, Jun. 2011, pp. 3614-3619.
[45] B. Kroposki et al., "Making microgrids work," IEEE Power Energy Mag., vol. 6, no. 3, pp. 40-53, May/Jun. 2008.
[46] R. H. Lasseter, "MicroGrids," in Proc. IEEE Power Eng. Soc. Winter Meeting, New York, NY, USA, Jan. 2002, pp. 305-308.
[47] T. Funabashi et al., "Digital frequency relay for load shedding," IEEE Trans. Power Del., vol. 1, no. 4, pp. 87-95, Oct. 1986.
[48] Y. LeCun et al., "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, May 2015.
[49] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed. Cambridge, MA: MIT Press, 2018.
[50] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[51] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, 2015.
[52] F. Tao et al., "Digital twin-driven product design framework," Int. J. Prod. Res., vol. 57, no. 12, pp. 3935-3953, 2019.
[53] M. Grieves, "Digital twin: Manufacturing excellence through virtual factory replication," Digital Manuf., vol. 1, no. 1, pp. 1-7, 2015.
[54] International Energy Agency, "Grid integration of variable renewables," Tech. Rep., Paris, France, 2017.
[55] IEEE Standards Association, "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," IEEE Std 1547-2018, Jul. 2018.
[56] Electric Power Research Institute, "Smart grid demonstration and deployment program: Investment grant summary report," Tech. Rep. 3002002001, Palo Alto, CA, USA, 2013.
[57] U.S. Department of Energy, "Smart grid investment grant program: Progress report," Tech. Rep., Washington, DC, USA, 2012.
[58] National Academy of Engineering, "The engineer of 2020: Visions of engineering in the new century," Washington, DC: National Academies Press, 2004.
[59] P. Kundur et al., "Definition and classification of power system stability," IEEE Trans. Power Syst., vol. 19, no. 3, pp. 1387-1401, Aug. 2004.