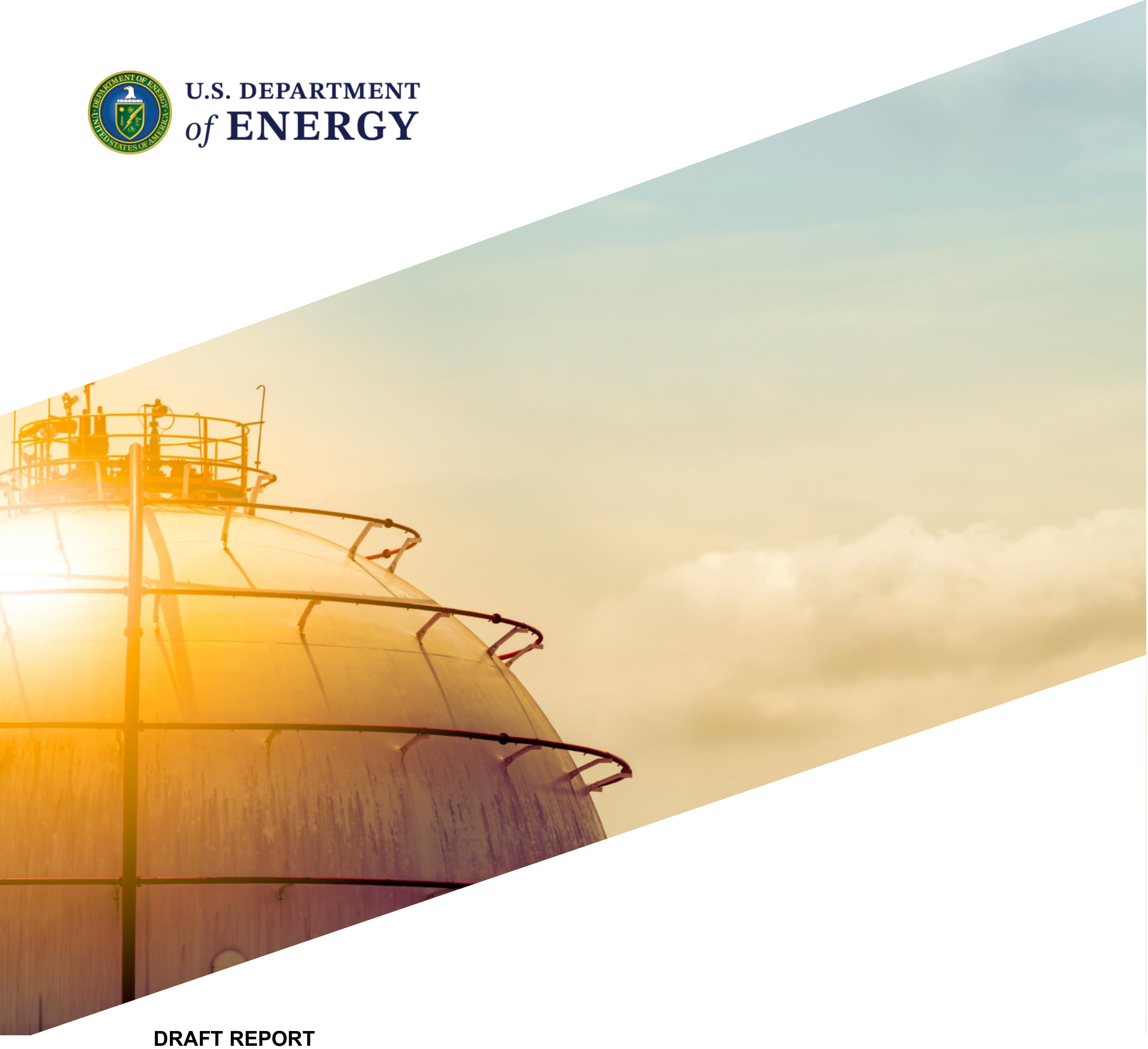
U.S. DEPARTMENT
of ENERGY



DRAFT REPORT

Microgrids R&D Strategic Plans

Topic 5 – Advanced Microgrid Control and Protection

March 2026

Disclaimer

Original Authors

The authors of the original 2021 document that formed the basis for this iteration are:

Ben Ollis, Oak Ridge National Laboratory (ORNL)

Max Ferrari, ORNL

Travis Smith, ORNL

Matthew Reno, Sandia National Laboratories (SNL)

Mike Ropp, SNL

Lee Rashkin, SNL

Wei Du, Pacific Northwest National Laboratory (PNNL)

Frank Tuffner, PNNL

Ravindra Singh, Argonne National Laboratory (ANL)

Art Barnes, Los Alamos National Laboratory (LANL)

Yashen Lin, National Laboratory of the Rockies (NLR)

Kumaraguru Prabakar, NLR

Vaibhav Donde, Lawrence Livermore National Laboratory (LLNL)

Ciaran Roberts, Lawrence Berkeley National Laboratory (LBNL)

Original Acknowledgments

With special thanks to the 2021 industrial advisory board who provided valuable reviews of the contents herein:

Wade Malcolm (Open Energy Solutions), Scott Manson (Schweitzer Engineering Laboratories), Jim Reilly (Reilly Associates) and Aleksander Vukojevic (ComEd).

Revision Authors

The authors of the 2025 revision to the strategy document are:

Maximiliano Ferrari, ORNL

Matthew Reno, SNL

Jhi-Young Joo, LLNL

Jake Gentle, Idaho National Laboratory (INL)

List of Acronyms

ADMS	Advanced Distribution Management System
AI	Artificial Intelligence
CERTS	Consortium for Electric Reliability Technology Solutions
CHP	Combined Heat and Power
CIP	(NERC) Critical Infrastructure Protection
DERMS	Distributed Energy Resource Management System
DMS	Distribution Management System
DOE	U.S. Department of Energy
EDS	Electric Delivery System
EMS	Energy Management System
GO	Generator Owner
GOP	Generator Operator
IED	Intelligent Electronic Device
IEEE	Institute for Electrical and Electronics Engineers
HIL	Hardware In the Loop
INL	Idaho National Laboratory
IoT	Internet of Things
LEL	Large Electric Loads
LLNL	Lawrence Livermore National Laboratory
MCS	Microgrid Control System
ML	Machine Learning
NERC	North American Electric Reliability Corporation
OE	(U.S. DOE) Office of Electricity
ORNL	Oak Ridge National Laboratory

PCC	Point of Common Coupling
PMU	Phasor Measurement Unit
RD&D	Research, Development, and Deployment
SCADA	Supervisory Control and Data Acquisition
SNL	Sandia National Laboratories
SMR	Small Modular (Nuclear) Reactor
T&D	Transmission and Distribution
TA	Technical Assistance

Executive Summary

The growing number and variety of microgrids being deployed today introduces challenges and complexities in control and protection design for microgrids. No longer are microgrids only used in remote applications with a dependence on traditional generation; many existing microgrids provide grid services and support, operate with a mix of different generation sources, and can seamlessly go from grid-connected to islanded for enhanced reliability. Additionally, increasing attention is being given to multi-microgrid systems and interactions between their controls and utility control systems. If microgrids are to become ubiquitous, it will require advanced methods of control and protection ranging from low-level inverter generator controls that can respond to faults to high-level multi-microgrid coordination using AI/ML to operate and protect the system.

Microgrids are inherently dynamic systems due to their ability to operate grid-connected or islanded, with different system requirements in each operational mode. Our vision for the future of microgrids includes the ability to adapt and operate efficiently to perpetually changing grid conditions through controls while simultaneously protecting the system and its customers. Achieving this vision will require developing innovative technologies, control algorithms, sensors, and protection schemes. These developments will advance microgrid protection systems and maximize system resilience, reliability, efficiency and minimize grid modernization cost. In that context, the Microgrid R&D program seeks to accomplish these three goals:

> Goal 1: Promote microgrids as a core solution for enhancing **resilience** of the electricity delivery system while supporting faster recovery of critical infrastructure during and after black sky events
>
> Goal 2: Ensure that microgrids serve as a driver to maintain a **reliable and secure** electricity delivery system by allowing important infrastructure to have consistently available alternative sources of power that can support the operations through both natural and man-made events.
>
> Goal 3: Use microgrids to enhance **energy abundance** by providing additional capacity through distributed energy supply and demand assets, as well as by providing necessary services and capabilities back to the bulk power system to help maintain consistent operations.

These goals additionally have cross-cutting topics of focus on designing dependable electric supply infrastructure and reducing economic inefficiencies using microgrid-integrated distributed energy supply and demand resources in both R&D and partnered demonstrations. This strategy document is one of nine prepared for the DOE Microgrid R&D program as part of the strategy development. The nine strategy documents focus on the following areas:

1. Program vision, objectives, and R&D targets in 5 years
2. T&D co-simulation of microgrid impacts and benefits
3. Building blocks for microgrids
4. Microgrids as a building block for the future grid
5. **Advanced microgrid control and protection**
6. Integrated models and tools for microgrid planning, designs, and operations
7. Small Nuclear Reactors in Future Microgrids
8. Artificial Intelligence and Machine Learning for Microgrid Applications
9. Enabling regulatory and business models for broad microgrid deployment

This strategy document identifies research and development (R&D) areas targeting advancement of microgrid protection and control in an increasingly complex future of microgrids. To identify these areas, we considered microgrids with multiple points of interconnections, combinations of hybrid AC/DC microgrids, networked microgrids, microgrids within microgrids, and microgrids inside secondary networks.

Table of Contents

1 Introduction

For years, microgrids have been considered for providing resilience to critical infrastructure, remote areas, and during emergencies. This is partially due to a microgrid's ability to flexibly serve loads using a variety of generation sources, and partially to provide nearly uninterruptible power for applications that demand high power quality such as data centers. As microgrid technology has matured, it has become clear that microgrids can play a part in normal distribution system operations instead of as only a sophisticated backup system. This will require inspection of device level controls, individual microgrids, and systems of multiple microgrids. This strategy document will lay out methods for controlling and protecting microgrid systems to enable a resilient and cost effective grid of the future.

Microgrid controls and protection will be critical in a future where a significant increase in power electronic load and generation is expected (30-50% of total generation capacity in the next decade). Specifically, control and protection will be leveraged to achieve:

1) A future electric delivery system (EDS) where microgrids act as a core solution to **increase the resilience and reliability** of critical infrastructure and alleviate grid stress and outages.
2) A future with **energy abundance** where microgrids utilize advanced controls and protection methods to integrate all types of generation with fewer restrictions.
3) A **reduction in microgrid capital costs** by 15%, as well as a **reduction in project development, construction, and commissioning** by 20% by 2031.

Achieving this future will require research in three categories: (1) technology development, (2) analysis and tools for planning, and (3) institutional frameworks. This paper will focus mostly on research in category 1, technology development for microgrids, specifically addressing microgrid control and protection technologies.

The paper will present the many technical areas of microgrids which play a part in how they are controlled and protected, from device-level to system-of-systems level. We expand on the current state of the art by first laying out our vision for how microgrids should be controlled and protected in the next five years. This vision will be used to identify the gaps between today's technology and where research can accelerate progress in the areas of microgrid control, protection, and communications. Ongoing projects in these areas will be identified and will feed into a multi-year research plan to accomplish the vision statement. Lastly, we provide a brief justification on why DOE should drive research in this area.

2 Vision for the future

Microgrids are expected to increase both in the number of installations, but also the size and spatial extent of microgrid installations. Additionally, collections of networked microgrids both customer- and utility-owned are expected to be able to connect on distribution networks to increase efficiency and reliability by taking advantage of additional load diversity, larger numbers of generators and multiple paths between generation and loads. New sensing technologies, protection schemes and generator controls enable the operation of such networked microgrids in terms of providing black start capability and protection coordination.

2.1 Controls for a Distributed grid

2.1.1 Normal Operations

Grid-tied operation of microgrids is considered "normal operations". Most non-remote microgrids will operate grid-tied by default and will be able to influence the operations of the local grid and customers. Microgrids today are often subject to interconnection agreements with the local utility (unless utility-owned), and often those contracts will specify the microgrids' allowable operating ranges and expected behavior, including export restrictions, voltage support, and connect/disconnect criteria. This contract structure works for pre-planned microgrids with known interconnection points to the main grid which can be monitored easily. However, in a future where microgrids could be even more present, multi-owner, and uncertain boundaries, the interconnection agreements can quickly become burdensome to utilities, and can even limit the efficacy of the microgrids and its distributed generators to support the bulk grid.

Additionally, the intersection between multiple domains of energy consumption will become more significant and must be addressed. Controllers will need to be aware of building-level controls, data center load profiles, and integrate with weather stations, forecasting, district heating, and fueling infrastructure, to name few.

In a future grid, we would expect to see controllers dynamically respond to grid conditions, self-optimizing and reconfiguring to best serve its customers without putting undue strain on the electric system. Multi-objective optimizations will allow microgrids to balance operating costs, resiliency, and uncertainty. A wide range of control schemes can be utilized to achieve these goals. To support this, distributed generators and microgrid controllers should be flexible enough and have access to enough information to enable different control strategies. Standardizing the type and data format can streamline integration and significantly reduce commissioning times for microgrids.

2.1.2 Grid-Independent Operations

One of the key characteristics of microgrids is that they can operate in an islanded mode, disconnected from bulk power systems. After a transmission outage caused by extreme weather or natural disasters, using local distributed generators to operate a distribution feeder, or portions of it as microgrids can minimize the impacts of outages on customers. In addition, the grid-independent operation capability of microgrids can also benefit remote areas such as rural villages that are far from the bulk power grids;

this feature significantly improves the reliability and resiliency of power grids. However, the islanded operation of microgrids also brings new technical challenges, such as the low system inertia, low-short circuit current, and the uncertainties with local distributed generators. These challenges should be addressed at the different levels of hierarchical control levels. At the primary control layer, new control strategies for power electronic-based generators such as grid-forming with droop control should be studied to ensure system stability in the context of multiple parallel distributed generators. Controls and hardware of grid-forming controls of power-electronic based resources should consider their impact in the protection system and be designed to provide the required sequence components to allow protection coordination. At higher-control layers, the microgrid controller should be designed to operate and dispatch the distributed generators by overcoming the uncertainties caused by local distributed generators. Meanwhile, the power system must operate without interruption should loads trip, transmission interconnections open, generation trips, and/or communication failures of any kind occur. In addition, a smooth transition between the grid-connected mode and islanded mode should be guaranteed with or without the microgrid controllers in service. Degraded frequency and voltage performance should be allowed in these multiple contingency outage scenarios, but the flow of energy to society must not stop.

Finally, research is needed with regards to emergency response to unanticipated grid loss. Within the context of microgrids, effective ways to maintain power to specific subsets of the grid without even momentary interruption during grid loss will massively benefit industrial processes, data centers, medical facilities, and critical service providers. Fail-over to diesel generators does not prevent the momentary outages that could result in millions of dollars in lost industrial processes, expensive medical equipment restarts (e.g., MRI), and emergency service interruption.

2.1.3 Blackstart Capabilities

In an ideal world, a microgrid is always able to isolate and operate in grid-independent mode for as long as necessary before closing back into the main grid. In reality, unforeseen outages, internal faults, insufficient generation controller instabilities, and/or a number of other scenarios can cause microgrid failure. In the future, certain microgrids should be designed in such a way to enable blackstart for critical loads. While blackstart generators have been used in practice for many years, more research should be given to power electronic-based generators as blackstart devices. Because power electronic-based generators have strict current limiting behavior, they can exhibit severe cold load pickup and magnetic inrush limitations compared with traditional synchronous generators.

One solution is to specify power-electronic based resources to source the inrush currents of transformers and large motor loads, while recovering the voltage and providing a strong frequency reference for other distributed generators and loads. Another solution that is used today but needs more research is to incrementally add transformers and loads back thereby not overloading inverters.

Going beyond the traditional boundaries of a microgrid, more work must be done in exploring how a microgrid can support the blackstart of feeder sections, entire feeders, substations, and even support the local transmission system. This would require an increase in the level of device coordination on the distribution system as well as additional planning models for multi-microgrid systems and significant retraining of the utility workforce to ensure safe operation and restoration.

2.1.4 Multi-microgrid Control

The future distribution systems are expected to have a high penetration of microgrids deployed by different vendors and owned by different owners. Interconnecting geographically close microgrids as networked microgrids can further enhance the reliability and resilience of power systems. Currently there are only a few deployments of networked microgrid in the real world. Therefore, a significant amount of research efforts is needed to develop appropriate control and coordination strategies to support the operation of the multi-vendor and multi-owner networked microgrids. Both centralized and decentralized approaches should be investigated to understand their applicability to the networked microgrids.

2.2 Protecting a distributed grid

2.2.1 Future Protection Methods

Although commercial microgrid deployments are proliferating, the spatial extent of such microgrids is limited by the capabilities of the state-of-the-art in microgrid protection. An unfortunate fact is that microgrid protection largely focuses on shutting down the local generation and the entire system to clear the fault, rather than minimizing the outage area. New protection methods are needed that can operate between grid-connected and islanded modes while providing protection coordination. This will enable the reliable operation of large and networked microgrids even during disaster events, where causes such as severe weather can cause faults on an operating microgrid.

2.2.2 The Role of Device Controls

The varying behavior of microgrid generation, controls, and power electronics under short-circuit conditions is a gap in existing microgrid standards. This creates difficulties for both the protection engineer who wishes to simulate a microgrid under short-circuit conditions to design and test a protection system, and inherent difficulties for the protective relaying itself in some conditions.

2.3 Communications and Cyber Security

2.3.1 Communications

Novel control and protection of generation sources and critical loads within microgrids are often reliant on some form of communication. Devices are expected to report measurements and be configurable for controllers. Controllers are expected to communicate setpoints and data to Supervisory Control and Data Acquisition (SCADA) systems. Feeder management systems may be expected to provide weather and pricing forecasts to microgrid controllers to influence control actions.

For future operations, microgrid controllers will need to interact with large numbers of generation assets and intelligent loads spread across wide areas. To further complicate the situation, microgrids will undoubtedly include multi-owner and multi-vendor assets, which have more complicated communication topologies. Microgrid controllers will also be expected to interact with other microgrid and feeder controllers, as well as SCADA and Advanced Distribution System Management Systems (ADMS). To enable this highly complex interaction at scale, research is required on microgrid communication and control schemas which will detail the types of measurements collected, controller setpoints, and other behavioral characteristics, and capabilities.

Thus, an opportunity exists to standardize behavior of Intelligent Electronic Devices (IEDs) when given standardized commands such as activate and deactivate, new setpoints, and measurement requests. This is a marked difference from adoption of a new data schema in that it would not require adoption of any particular structure, but would instead be a standardized behavioral response when the IED is presented with the command. Research in this area would lead to heightened interoperability between IEDs, microgrid controllers, historians, and SCADA systems in general.

An additional emerging research area is one focused on the effectiveness, security, and feasibility of inter-device communication. Traditional communication structure utilizes a spoke-and-wheel approach where direct communication between devices is generally denied. While this decreases the number of communication pathways an attacker could attempt to compromise, it limits the speed at which decisions can made between multiple devices at the edge. Such edge-based communication and control activities include real-time load and generation smoothing algorithms, co-sharing of V/f regulation for redundancy and stability, and rapid response to operational changes in geographically near devices. Moreover, by enforcing communication through a centralized area like a command room at a distribution center, there is generally a single point of failure for the communications exiting the substation or generation facility, thereby preventing the kind of inter-device communication that would be needed for effective autonomous operation until communications were re-established.

Additional attention needs to be paid to microgrid operations when communication between devices faulters or outright fails. Minimal and backup communication functionality (such as heartbeat signals and beaconing) needs to be further explored and standardized to better *Strengthen Grid Reliability and Security.*

2.3.2 Cyber Security

Microgrids are effective in ensuring energy availability to critical infrastructure nodes of a network during prolonged outages due to successful cyberattacks, thereby enhancing the overall resilience. With increasing rates of data acquisition and no vendor agnostic cybersecurity posture, distribution systems pose unique challenges that transmission systems do not. Coupled with a broadening attack surface, these make microgrids lucrative targets for coordinated attacks. A microgrid control system (MCS) coordinates among individual resources and abstracts the microgrid as a single entity when communicating with the main grid. A poor cybersecurity posture could, therefore, render MCS a single point of failure for the entire microgrid. A key point is that if a load is important enough to warrant having a microgrid, then it's also important enough to apply cybersecurity protections to the entire system - which would be practically roughly equivalent to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Medium Impact levels. But, most microgrids are not going to be subject to anything NERC CIP, except for some that may have the resources to qualify as a Generator Owner/Generator Operator (GO/GOP) Category 2 (if they're greater than 20 MVA in aggregate AND connected at 60 kV or higher). Those will need to meet NERC CIP Low Impact requirements, which IMHO are insufficient for the level of security that a load important enough to warrant being supported by a microgrid implies.

3 Technology Developments

In a future grid where microgrids become a ubiquitous solution to integrating distributed energy supply and demand resources and maintaining system reliability, many new technologies and methods will be required. These include:

3.1 Control

3.1.1 Hierarchical, distributed, and hybrid control strategies for devices, microgrids, and networked microgrids

Microgrid control is typically organized into multiple levels, known as hierarchical control. Primary control operates at the generation source level, using fast controllers to regulate voltage and frequency of the system. Secondary control allows distributed parallel operation of multiple generation sources. Tertiary control incorporates intelligent controllers, optimization algorithms and forecasting tools to manage microgrid assets via communication systems (Fazel Mohammadi). Extending this level, quaternary control allows coordination of a fleet of interconnected microgrids considering aspects such as ownership models and data privacy (A. Sundararajan).

The upper layers of control can be implemented in centralized, decentralized, or hybrid architectures. Centralized control is a common approach; however, it can be limited in scalability and data privacy. As the complexity microgrids and of interconnected microgrids increases, distributed and hybrid approaches offer greater scalability, enhanced data privacy, and improved interoperability across different microgrid types and ownership models.

Multiple control strategies can be applied across these layers, each one with unique strengths and weaknesses that merit further research. There is no single prescriptive method for microgrid control; instead, control architectures should be designed support a variety of strategies tailored to the microgrid’s mission, whether focused on resiliency, economic performance, or other objectives.

One way to enabling adaptable controllers is to pursue modularity, interoperability and standardization. This approach can allow for rapid changes in optimization, data storage, communications, and others without having to change the underlying framework, similar to apps running on an operating system.

3.1.2 Identification of critical device information for control and modelling, including power-electronics based resources transient response characteristics and operational capabilities / limits

Microgrids incorporate diverse assets and distributed generation sources, including both traditional and power electronics-based units. Power electronics-based generators characterized by input resource intermittency, smaller unit capacities, and low or synthetic inertia (Xiaorong Xie) . As a result, high-fidelity models are required to understand stability challenges, which differ fundamentally from those encountered in traditional power systems. Developing such models necessitates critical device information to create realistic models that replicate microgrid behavior under normal and abnormal conditions across various operation modes (grid-tied, islanded, or as part of a microgrid network). High-fidelity models enable assess in systems dynamics in diverse scenarios, support control validation and allow companies and researchers to design controllers with realistic conditions and limitations, resulting in accelerate deployment of advanced systems.

Identification and format of critical information will be needed for controllers to perform their core function. Often, microgrid controls operate on assumptions of device behavioral characteristics, but this is far from an optimal control method. If devices can report their unique operational data and characteristics, that information can be built into the controllers and used to create a more stable microgrid.

3.1.3 Characterizing the dynamic response of power electronic connected loads to system disturbances to ensure no adverse control loop interactions across both generation and load resources

Loads such as data centers and electric vehicles may contain high-frequency harmonics and contain fast and large spikes that are difficult to predict. In a microgrid with power electronic-based generation, these characteristics can interact with generation control causing challenges for stability or for maintaining a stable voltage and frequency regulation, particularly during disturbances or rapid load changes.

Power electronic-based generation interacts with the bulk grid when the microgrid is grid-tied. These interactions are complex and difficult to model, especially during transient events. These interactions can influence both local and system-wide stability. Developing methods to characterize the dynamic, work can be done on methods for characterizing dynamic behavior of sources and loads in a microgrid is necessary to create more accurate transient model, required to predict and mitigate adverse effects during such events (Guocheng 2020).

3.1.4 Dynamic stability region calculation and state estimation for robust off-grid controls, including imbalanced system controls

Maintaining microgrid stability is critical for a reliable operation. Unlike the bulk power system, many energy sources in microgrids are connected to the system via power electronic devices. These resources are often distributed and have a wide range of size and control strategies which may introduce challenges to analyze and ensure microgrid stability. In large microgrids and networked microgrids, the interaction of the power electronics control and large, rapid load changes may compromise system stability. Small-signal stability and transient stability are a necessary requirement for analyzing systems oscillations, abrupt disturbances grid transients, required for maintaining a secure and resilient microgrid operation. (Schneider, et al. 2020).

3.1.5 Bulk system interactions and grid service provisioning

While grid services provided by microgrids has been fairly well studied for individual microgrids, there is still considerable work needed determining how large numbers of microgrids can co-dispatch to provide coordinated grid services. Networked microgrids operated under a higher level microgrid orchestrator framework could unlock capabilities that are challenging or limited for single microgrids to achieve. For instance, a coordinated group of microgrids could potentially provide blackstart services by sequentially energizing segments of the grid and supporting each other's start-up sequences with the ultimate objective of assist restoring larger sections of the bulk grid more rapidly. Similarly, coordinated microgrids could be collectively deliver frequency regulation and voltage regulation services to the main grid. Beyond these, reactive support, congestion relief, peak demand management and synthetic inertia, increasing bulk system resiliency. Achieving these capabilities require advances in interoperability standards and control architectures capable of managing interactions among heterogenous microgrids considering operational constrains and ownership models.

3.1.6 Grid-forming control and off-grid behavioral characteristics

Grid-forming control of power-electronics based resources will play an important role in the reliable, stable and resilient microgrid operation. Different from the traditional grid-following control, grid-forming controls can regulate their terminal voltage and frequency, which enables distributed energy supply sources in the microgrids to help maintain the system voltage and frequency. While early deployment of grid-forming capable power-electronic based resources have demonstrated their effectiveness in small-scale systems, there are still many open research questions that need to be addressed for large-scale adoption. Key technical challenges include frequency control, voltage control during unbalanced and abnormal conditions mixed controls and control-modes coordination, control adjustability, grid behavior anomaly detection and associated control response, system protection, fault ride-through and system recovery and stability in networks with multiple grid-forming resources. Advances are needed in modelling and simulation approaches that can capture accurately grid-forming dynamics and account for interactions with other power-converter based generators and traditional generators on diverse configurations such as networked microgrids and grid-tied large-scale simulations. (Lin, et al. 2020).

3.1.7 Seamless online transition from grid-forming mode of operation to grid-following mode of operation

Many existing grid-forming devices require a shutdown to transition from grid-forming mode to grid-following mode. There are benefits to having seamless transitions of devices, but it is often difficult to achieve in practice. Research is needed on quantifying the benefits and demonstrating the ability for devices to behave in this manner.

3.1.8 Black-start capabilities of microgrids – local and bulk

Traditionally, black-start capability for the bulk grid has almost exclusively been provided by synchronous generators. However, the generation and energy storage assents of microgrids can also be leveraged to provide black-start support. This may include forming the voltage and frequency references during restoration process, or using intelligent load control to incrementally re-energize segments and restore loads in a coordinated manner. Early work has demonstrated the potential of black-starting via distributed generation. However, many challenges remain, including how to address the stochastic natural of local generation in the restoration process and how to properly and adaptively protect the network with sources limited short-circuit capabilities. Other challenges include controlling heterogeneous microgrids with diverse ownership models during the restoration process.

3.1.9 Network reconfiguration of microgrids and networked-microgrid systems

The environment in a network of microgrids is inherently heterogeneous, involving a diverse mix of power-electronic-based and conventional generation, different microgrid controllers from various vendors, and multiple ownership models (e.g., utility, commercial, industrial), each with distinct data privacy requirements. Designing controls for such systems requires approaches that minimize information exchange to preserve privacy, coordinate grid-forming and grid-following distributed generators, and determine appropriate interconnection methods, whether direct AC coupling or power-electronic-based interlink configurations (C. -C. Liu)(M.Ferrari) . Reconfiguration of distribution systems is a popular academic area of study; however, many projects make assumptions about controls, communications, and modelling that are critical to building a functional multi-microgrid system in the field. Leveraging microgrids and network microgrids for restoration with grid forming controllers requires addressing questions regarding impacts such as transformer inrush, seamless synchronization between interconnected microgrids and the bulk grid, effects of faults during the restoration process, many of these questions remain to be addressed at large-scale system levels.

3.1.10 Integration of legacy devices

The electrical grid is an evolving infrastructure that contains a large array of legacy equipment over decades of operation. This equipment ranges from protective relays, transformers, communication protocols, metering and control systems. New technologies should consider in their design their compatibility with existing legacy equipment enabling a gradual modernization. I Considering this compatibility minimizes the need of complete retrofits while allowing incremental upgrades.

3.1.11 DC Microgrids

DC microgrids provide an efficient alternative to AC microgrids by reducing conversion losses and directly accommodating DC-native loads such as data centers. Data centers, in particular, may benefit from DC microgrids because AC–DC conversions stages are minimized, improving efficiency, reducing costs. DC architectures also allow direct integration with DC-native generation and energy storage systems, which can further reduce power-electronic conversion stages. AC and DC microgrids can be interconnected via power electronics to leverage the strengths of both domains. Via power-electronics interlinks and coordinated control, hybrid AC/DC microgrids can enable bi-directional power flow to improve operational flexibility. However, large-scale adoption remains constrained by gaps in DC microgrid protection, as well as interoperability challenges. Future research should address adaptive and privacy-preserving control architectures, high-fidelity modeling, interlinks for hybrid systems, as well as large-scale testbed for validating hybrid AC/DC microgrids, and protection schemes tailored for both DC and hybrid configurations (Z. Ali).

3.2 Protection

3.2.1 Fault modelling and estimation techniques

An ongoing issue in protection of microgrids is how to model them under short-circuit conditions. While there is ongoing research that shows promise for the ability to protect microgrids, it is necessary to be able to validate such methods on microgrids of practical size, particularly for power electronics based microgrids such as data centers and when considering networked microgrid operation. While it is possible to accomplish this with transient simulation software, models are typically limited to around 10^4 electrical nodes, while practical distribution systems can exceed 10^5 nodes. Additionally, the number of parameters required for modeling power producing assets can be prohibitive. An alternate approach is to model the short-circuit behavior in the phasor domain after the initial dc offset of the short-circuit current has died out. This presents a challenge on account of the nonlinear behavior of power electronics and the range of potential distributed generation sources from batteries up to Small Modular Reactors (SMRs). For example, grid-following generators typical of residential grid-connected systems and grid-forming generators that are typical of microgrids will respond to faults differently. Additionally, even within these two broad categories there is variation on account of the type of control used (a rotating reference frame or stationary reference frame, incorporating multiple control loops to regulate harmonics, how power sharing is implemented) and how fault current limiting is implemented (whether a simple threshold or hysteresis is used, how the current reference for current-limiting operation is produced). There is ongoing work to produce both transient and phasor-based short-circuit models and to validate them against experimental results.

3.2.2 Improved and standardized fault controls for improving protection coordination

The previous section on fault modeling highlighted the difficulty of modeling different types of generation on account of the current lack of standardization. To facilitate design of microgrid protection systems, it is highly recommended to extend existing standards on microgrid protection to include standard behavior for distributed generators under fault currents. In addition to adding complexity to the modeler or protection designer, some current-limiting methods can cause difficulty for protection. As an example, a simple current threshold will result in voltage and current clipping, causing significant harmonics which will interfere with calculations that are based on phasor quantities.

3.2.3 Protection schemes with low fault currents

Existing protection schemes have documented limitations in microgrids, particularly power-electronics-interfaced microgrids on account of the lack of fault current. This is the case for standard time-overcurrent protection which will at best have prohibitively long operating times. It is necessary to investigate non-traditional protection methods for distribution, both methods that have been adapted from transmission systems (that normally operate in meshed configuration) and novel protection methods, with a theme being that most methods are some variation of differential protection. It is important to study the applicability of transmission protection methods to microgrids. For example, there is currently a lack of consensus in terms of the usefulness of admittance relaying, where there is evidence suggesting that the line admittances on practical microgrids are too low to reliably discriminate between in- and out-of-zone faults [3, 4, 5]. Novel methods include the family of setting-less/dynamic state estimation protection methods, which overcome issues of current mismatch at the terminals of a protected zone by incorporating a detailed model of the physics of the protected device [6, 7, 8, 9]. An alternate approach that exploits new relaying hardware with high sample rates is traveling-wave protection which makes use of the property that distribution lines can be modeled as distributed-parameter lines at high frequencies [10, 5]. This allows traveling-wave protection to locate faults based on the timing on current pulses given either knowledge of the line propagation constant or the ability to take multiple measurements on either side of a fault. A last approach takes an integrated view of fault location on a microgrid by deploying micro-PMUs such that the microgrid is observable [5].

3.2.4 Re-coordination of devices in a dynamic environment

A second issue with protection of microgrids is varying levels of fault current caused by changing generation dispatch, and switching configurations, which can include the transition between grid-connected and islanded modes [5]. This exposes a second limitation of conventional protection outside of its requirement for fault current as an operating quantity. Typical protective relaying systems for both distribution and transmission are inflexible or used in inflexible manners and are designed to use pre-set protection zones. This can result in misoperation or lack of operation under different microgrid operating configurations. When assessing protection technologies, this needs to be considered [5]. While time-overcurrent protection is certainly affected by microgrid reconfiguration, newer technologies such as setting-less protection and even older ones such as differential protection are immune to change in fault current magnitude and direction.

3.2.5 Microgrid grounding

Grounding of microgrids is one of the most challenging topics for microgrid protection. In grid-connected mode, the system grounding is generally provided by the substation transformer. If the microgrid or energy producing assets in the microgrid are grounded during grid-connected operation, it can result in bi-directional ground current flows, desensitization of ground current protection settings, and sympathetic tripping. Once the microgrid is islanded from the rest of the system, the connection to the substation transformer is lost. Without grounding in the microgrid, it is very challenging to detect single-line-to-ground faults (especially for systems that are already fault current limited), there are additional safety risks, and faults can cause extreme temporary overvoltages. For this reason, it is common that the microgrid grounding will be switching in and out during mode transitions, either using a grounding bank or grounding switch on a wye-delta-wye transformer. Controlling this grounding switch, transition timing, handling transformer inrush, and other additional aspects make this a challenging problem. It is also important to size the microgrid grounding appropriately, which can be challenging for power electronics systems where traditional coefficient-of-grounding rules do not apply.

3.2.6 DC microgrid protection and fault extinguishing devices

While this has been an area of long-term interest, many practical issues present barriers to progress. With recent progress on standardizing DC metering, it is anticipated renewed interest and effort will be placed on protection and fault extinguishing.

Recently, DC microgrids are gaining more popularity as both more generation is DC with power-electronic converters and more energy consumption of lighting and computers shift towards DC. Data centers are an example that investigating future systems being entirely a DC microgrid. Because DC microgrid are converter-based systems, the entire system has very fast dynamics and can potentially be very sensitive to disturbances and faults. For this reason, fast fault detection schemes need to be developed to minimize the fault clearing time. Analysis of DC microgrid protection schemes is challenging because 1) as discussed in previous sections each converter controls and operation is unique, and 2) there are limited software available for simulating DC systems. Without appropriate standards and guidelines, it is difficult to address the DC microgrid system restoration strategies. There should be more research on this topic to develop proper guidelines for the closing sequence of primary and backup protection devices based on the fault characteristics and system components.

3.3 Communication

3.3.1 Reliable, high-speed communication is key for many microgrid protection methods including differential, setting-less and double-ended traveling wave

Demonstrations of communications-driven protection schemes for microgrids are needed to demonstrate their ability to respond to constantly-shifting microgrid conditions.

3.3.2 Cyber security of hardware and communications to secure a large number of endpoints

Confidentiality, integrity, and availability are critical to information systems. Continuous energy delivery, on the other hand, is strongly tied to availability and integrity, which gain precedence over confidentiality. However, these two attributes need additional qualifiers to comprehensively represent the security requirements for a microgrid. These qualifiers can be adopted from the Parkerian Hexad into the control systems domain and include possession (continued access control over protected data), utility (usefulness of data in its protected form), and nonrepudiation (ensuring accountability and authorship of data provable via traceable means).

Defense-in-depth and layered defense technologies have been effective models in protecting systems with interdependent subsystems. However, they are limited in their flexibility to adapt to emerging paradigms of decentralized controls and edge or fog computing. Further, well-sponsored coordinated attacks, which have increasingly begun targeting the smart grid, can penetrate every layer of defense to compromise the system. Hence, it is imperative to augment such traditional security models with solutions that are dynamic, data-driven, distributed, and lightweight. Below, the emerging directions of research into microgrid cybersecurity are summarized.

3.3.3 Abstraction of behaviors to standardize controller/controlee interactions

Often microgrid controllers are designed as one-off systems based on the specific behaviors of the devices within the microgrid. However, if standardized command and control signals are developed, that greatly simplifies the controller's internal state machines and messaging structure, leading to shorter commissioning times and greater interoperability.

3.3.4 Data aggregation & filtering methods to extract only necessary data

Utilities today are running into big data problems, and most of that data is never utilized. This problem will only get worse as more endpoints on the system return information back to centralized utility systems like SCADA. A method of mitigating the vast amounts of generated data will be through aggregation and abstraction of certain data fields at the microgrid controller level. While the controller may have access to all information within its domain, only a portion of that data needs to flow upward to the feeder or the utility level.

3.3.5 Microgrid Data Privatization

The vast amount of data which is, and increasingly will be, collected within microgrids will have limited use if it cannot be more broadly shared. At present, utilities, vendors, aggregators, and customers are disinclined to share electric grid-related data due to privacy concerns. Differential privacy and other privacy-preserving mechanisms offer the potential to provide statistical guarantees of privacy for queries made over a given dataset. While this technology has been embraced by the entities in charge of large volumes of data, such as the U.S. Census Bureau (Census, 2024), it is only beginning to be explored in the microgrid community. Tailoring differential privacy techniques to microgrid functions offers the potential to alleviate significant legal and societal concerns related to data sharing. This, in turn, will further catalyze the development of new microgrid applications including, but not limited to, protection and control.

4 Use Case / Scenario Examples

For this section, we will bring forth some examples of areas where microgrid control and protection will need to expand to meet the vision laid out in this document.

4.1 Device – level

Device-level controls play a crucial role in how microgrids are controlled and protected. There is no guarantee that behavior of distributed generators will be common amongst device types or even amongst vendors. This complicates control philosophies and can lead to unintended and unmodelled instabilities in the microgrid. Furthermore, the parameters which dictate how the device responds to grid events are often not reported, and assumptions must be made in any transient simulation, leading to inaccuracies.

Ideally, distributed generators reporting to a microgrid controller would provide measurement, status, and behavioral data in a standard format that any microgrid controller could quickly model and implement into an optimization routine. This data should also be able to describe the fault characteristics of the device for inclusion in the protection system design, which will likely be partially controlled by the microgrid controller. While this will require significant changes from vendors, it will ultimately lead to more observable and controllable distribution system.

4.2 Single Microgrids

In the case of single microgrids, there are a multitude of different control paradigms which can be utilized to coordinate and dispatch the distributed generation and components under its jurisdiction. The goal of this paper is not to be prescriptive in which control methods are preferred, but instead to describe architecture for microgrids which can allow for multiple control schemes to be achievable.

For the purposes of this exercise, we are considering that a microgrid consists of at least one generator, one load, and at least one controller of some sort. The controllers can be centralized or distributed, and local or remote. The controller(s) will be expected to report information to existing utility systems, such as SCADA, and to coordinate the behavior of some subset of assets within the microgrid, including but not limited to: generation, load, protection, and voltage regulation.

A simple method of integration of a microgrid controller into utility operations would be through abstraction. High-level use cases are presented to the operator (ex., voltage regulation, power factor control, island mode), but most actual control is handled by the remote controller and not the power system operator. This keeps an operator from needing to individually seek out generator setpoints, and instead automates the control and dispatch of the assets. Similarly, protection setting groups can change based on dynamic fault current availability calculations to ensure the grid stays in a “protectable” range. This is a significant shift from how power systems are operated today, but could provide substantial benefits to customers and utilities.

4.3 Large Area Microgrids

It is becoming common to have very large microgrids that can span wide areas and produce large amounts of power. For example, data centers are continuing to grow and can have the ability to island into microgrids up to 500 MW in size. This generation can come from local sources such as batteries, SMR, and diesel or natural gas generators, but it often includes some other onsite generation from solar that can expand miles around the data center. Large communities on islands or remote areas can be similar in size geographically and in electrical size. For these large microgrids, much of the architecture described in the previous section remains the same for voltage regulation, generator dispatch, and other controls. On the other hand, the spatial distance between generators and controls can create some additional communication challenges. Some protection aspects may change too as now different protection zones can be created for selectivity and fault clearing.

4.4 Multi-microgrids

Like the single microgrid case, control for multiple microgrids can take on many forms, including transactive control, game theoretic control, device inheritance, and fully distributed control to name a few. Again, our goal is not to be prescriptive with how multi-microgrid systems are controlled, but instead to describe methods of building out microgrids to enable these types of interactions.

Systems consisting of multiple microgrids are even more complex than previously presented cases, and very few of these systems exist today, so they are not well understood. Commercial controllers today have limited interaction capability with controllers of other vendors, and interactions beyond the boundary of the microgrid are typically not considered. Coordinating controllers through a SCADA or Energy Management System (EMS) are likely the short-term solution to this problem but may not be the most practical in a system containing hundreds of microgrids.

A similar architecture to the single microgrid case can be adopted for multiple microgrids. Controllers can establish a secure channel with other controllers to interact, share information, and co-optimize to come to a more global optimal solution than if controllers operated independently. Also, in islanded mode, microgrid systems could share assets to create a larger island, serving more customers and potentially operating more efficiently and reliably. This functionality could be especially useful in areas of natural disaster, where multiple pockets of resilience created by microgrids could be combined and co-optimized to serve a greater number of civilians and rescue/recovery workers.

There is a small pilot, the California Energy Commission-funded Oakland EcoBlock project, underway in the San Francisco Bay area where the utility plans to enable sectionalizing a short, single-phase 2.7-kV (line-to-neutral) lateral distribution feeder and operating it as an island during grid outages. Under blue-sky conditions, the 150-kW battery resource can be dispatched as desired to support transmission or distribution level objectives, depending on tariff design and real-time needs. The goal of this project is to prototype block-level microgrids that are scalable and both offer grid-services in grid-connected mode and serving all microgrid critical loads for several days in case of an outage.

5 Enabling Technologies

A future which enables more flexible and effective microgrid controls and protection will be an enabling technology for all other topic areas of this report. Without effective methods of collecting information, understanding device dynamics, abstracting behavioral characteristics, and protecting infrastructure, it will be very difficult to achieve a future in which microgrids can achieve our targets for system resiliency and affordability. Creating a control and protection framework that is replicable will enable microgrids building blocks (Topic 3) and microgrids as a building block for the grid (Topic 4) and will leverage work done with co-simulation of microgrids (Topic 2), planning and design tools (Topic 6), and regulatory and business models for microgrids (Topic 7).

Work has already begun on many of the enabling technologies for the proposed future distribution grid, including:

- Standardized data models
- Device abstraction layers for simplified commissioning
- Microgrid control methods and multi-microgrid interactions
- Protection schemes that do not depend on fault current and are robust to changing network configurations
- Dynamic protection schemes based on changing electrical layout
- Formulations and software tool implementations for
    - Short-circuit contribution of power-electronic based resources (grid-forming and grid-following)
    - Protection and stability constrained operation of microgrids
    - Protection system design of microgrids that accounts for non-radial operation
- Power-electronic based resources control loop classification (grid-forming and grid-following)
- Imbalanced system controls
- High-voltage power electronics converters that allow for larger DC microgrids (data centers)
- Protection for DC microgrids
- Protection standards for microgrids
    - Standardized behavior of microgrid power-electronic based resources under fault, particularly current limiting
- Secure energy asset hardware and communications
- AI/ML for microgrid controls, operations, and protection

The Consortium for Electric Reliability Technology Solutions (CERTS) microgrid has explored some of these control and protection challenges on a small testbed and lesson learned from these experiments can help drive future research. All network and controller data related to the microgrid are publicly available as well as all waveform test data. This data spans all three phases of the project, when the microgrid was operating as an all grid-forming based microgrid, as well as when grid-forming power-electronic based resources were operating in parallel with synchronous machines. Furthermore, this data also captures an alternative approach to electrical protection within the microgrid that does not depend on being triggered by abnormally large electrical currents.

6 Summary of Research Targets & Goals for next 5 years

Here, the authors outline research goals needed to achieve the future vision laid out previously.

6.1 1-3 years:

- Building and testing of testbeds and field validations for networked microgrids, as started by active DOE projects
- Participation in ongoing standards efforts for microgrid protection schemes and communication schemas. This includes standards for microgrid protection, such as the Institute for Electrical and Electronics Engineers (IEEE) 2030.12, standards for microgrid and generator grounding, and standards for DC microgrid protection.
- Characterization of power-electronic based generation in grid-forming and grid-following modes, including transitions between modes and under faults
- Analyze how generator grid support functions (ride-throughs, 2800 functions, etc.) impact the microgrid protection system
- Modelling and simulation of resiliency of multi-microgrid systems
- Developing analytical methods to determine effective grounding resistance and reactance for power electronic-based systems
- Development of a regulatory roadmap for how multi-owner microgrids can be controlled
- Development of fast fault detection schemes for DC microgrids, including arc fault detection, and fault location in DC systems
- Improved DC circuit breaker technologies, such as solid-state circuit breaker development, and testing of DC fault extinguishing devices
- Develop framework for coordination between the microgrid protection and Advanced Distribution Management System (ADMS)
- Research for improved cyber security of protection communication and communication between the protective devices and the microgrid controller or Distribution Management System (DMS).

6.2 3-5 years:

- Identify a method of enabling discovery and dynamically adding new generation assets into existing microgrid controllers
- Include Internet-of-Things (IoT) load controls for customer loads into microgrid controller controls and constraints.

- Improvements for microgrid grounding, such as novel microgrid protection schemes for detection of ground faults with a good grounding source, new power electronics based grounding sources, and improved performance of power-electronic based controls under unbalanced non-symmetrical grid conditions.
- Demonstrate novel protection and control methods through large-scale co-simulation of AC, DC, and hybrid microgrids
- Algorithms for optimal protection design in microgrids based on generation locations, Point of Common Coupling (PCC), fault current, and critical loads. This includes design techniques to determine appropriate protection settings for real-time applications, planning, or adaptive protection. The design and setting algorithms could include machine learning algorithms using historical fault and outage data.
- Development of new protection schemes for meshed microgrid architectures and microgrids in secondary networks. The protection scheme must be able to handle reverse power to distinguish between generation from the microgrid and reverse current from a fault being supplied through the network. This includes hardware-in-the-loop testing of microgrid protection schemes in secondary networks.
- Autonomous self-healing protection schemes for a fractal grid
- Advancement of commercial short circuit current software to include grid-forming models and the ability to analyze microgrid protection

6.3 5 years:

- Lab and field demonstrations of networked microgrid controls and protection
- Effective Human-Machine-Interface (HMI) and processing of data to support power system operators
- Research and designs of new protection techniques, schemes, and equipment for DC, networked, and hybrid microgrids
- Coordinated operation of generator controls with protective relays
- Generic protection schemes and devices for microgrid deployments
- Development and demonstration of communication-based microgrid protection schemes integrating additional sensing technologies (fault indicators, Phasor Measurement Unit (PMU), etc.)
- Automated compliance testing for protective devices using digital twins and Hardware In the Loop (HIL).

7 Why Should DOE be Funding These Goals and Vision

Today’s microgrid controllers, distributed generation, and protective devices tend to be purpose-built, and also do very well at achieving that designed purpose. As a side effect of this, much time is spent perfecting a given technology as opposed to innovating. Utilities also tend to be risk-averse; often utilizing products they know and trust over equipment with new capabilities. Most utilities have a “show me” policy regarding hardware, as any technology that fails will likely have a detrimental effect on its customers’ costs and quality of service. This results in low motivation for vendors to constantly change their product line beyond minor improvements.

In this environment, the DOE can play a crucial role in spurring research to push beyond the industry standard for higher reliability for customers during outages and higher power quality for data centers. Working with vendors and utilities, the labs can demonstrate technologies in simulation, hardware-in-the-loop, co-simulation, and field deployments, potentially reducing apprehension for adoption of the technology. Also, some components, such as microgrid controllers for multiple microgrids, are still in the early stages of R&D, and need more time dedicated to them to flesh out the full capabilities.

To build a grid environment which is more interoperable, controllable, and reliable requires partnering with many utilities and vendors across the country and having them work together towards this vision. Otherwise, we end up with individual components which are solid, but were never designed to work together, resulting in a more costly, inefficient grid.

References

Albinali, H. F., A. P. Meliopoulos, and C. Vournas. 2017. "Dynamic state estimation-based centralized protection scheme." 2017 IEEE Manchester PowerTech. 1–6. doi:10.1109/PTC.2017.7981259.

Ali, Z., et al., "Fault Management in DC Microgrids: A Review of Challenges, Countermeasures, and Future Research Trends," in IEEE Access, vol. 9, pp. 128032-128054, 2021, doi: 10.1109/ACCESS.2021.3112383.

Choi, Sungyun, and A. P. Sakis Meliopoulos. 2017. "Effective Real-Time Operation and Protection Scheme of Microgrids Using Distributed Dynamic State Estimation." IEEE Transactions on Power Delivery 32: 504–514. doi:10.1109/TPWRD.2016.2580638.

Dewadasa, J. Manjula, Arindam Ghosh, and Gerard Ledwich. 2008. "Distance protection solution for a converter controlled microgrid." Proceedings of the 15th National Power Systems Conference.

Dewadasa, M., A. Ghosh, and G. Ledwich. 2008. "Line protection in inverter supplied networks." 2008 Australasian Universities Power Engineering Conference. 1–6.

Ferrari, M., M. Starke, J. Smith, J. Pereira and M. Montejano, "Experimental Validation of a 40kW, 480V Point-to-Point DC Interlinks for Controller-Agnostic, Interoperable Networked Microgrids," 2025 IEEE Applied Power Electronics Conference and Exposition (APEC), Atlanta, GA, USA, 2025, pp. 637-644, doi: 10.1109/APEC48143.2025.10977294.

Lin, Yashen, Joseph Eto, Brian Johnson, Jack Flicker, Robert Lasseter, Hugo Villegas-Pico, Gab-Su Seo, Brian Pierre, and Abraham Ellis. 2020. Research Roadmap on Grid-Forming Inverters. National Renewable Energy Laboratory.

Liu, C.C., et al., "Microgrid Building Blocks: Concept and Feasibility," in IEEE Open Access Journal of Power and Energy, vol. 10, pp. 463-476, 2023, doi: 10.1109/OAJPE.2023.3282188.

Liu, Yu, A. P. Sakis Meliopoulos, Rui Fan, and Liangyi Sun. 2015. "Dynamic State Estimation based protection of microgrid circuits." 2015 IEEE Power Energy Society General Meeting. 1–5. doi:10.1109/PESGM.2015.7286513.

McDermott, Thomas, Bharat Vyakaranam, Rui Fan, Priya Thekkumparambath Mana, Travis Smith, Zhi Li, Joshua Hambrick, and Arthur Barnes. 2018. "Protective Relaying for Distribution and Microgrids Evolving from Radial to Bi-Directional Power Flow." Proceedings 2018 Western Protective Relay Conference. Spokane, WA.

Meliopoulos, A. P. S., G. J. Cokkinides, P. Myrda, Y. Liu, R. Fan, L. Sun, R. Huang, and Z. Tan. 2017. "Dynamic State Estimation-Based Protection: Status and Promise." IEEE Transactions on Power Delivery 32: 320–330. doi:10.1109/TPWRD.2016.2613411.

Mohammadi, F. et al., "Robust Control Strategies for Microgrids: A Review," in IEEE Systems Journal, vol. 16, no. 2, pp. 2401-2412, June 2022, doi: 10.1109/JSYST.2021.3077213.

San, G., Wenlin Zhang, Xiaoqiang Guo, Changchun Hua, Huanhai Xin, Frede Blaabjerg, “Large-disturbance stability for power-converter-dominated microgrid: A review,” Renewable and Sustainable Energy Reviews, Volume 127, 2020, 109859, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2020.109859.

Schneider, Keven, Harsha Nagarajan, Annabelle Pratt, Mathew Reno, Ben Ollis, Francis Tuffner, Sai Nandanoori, et al. 2020. Preliminary Design Process for Networked Microgrids. Pacific Northwest National Laboratory.

Sundararajan, A., G. Liu, M. Starke, R. K. Moorthy and C. Irwin, "Networked Microgrid Ownership, Data, and Control Implications: Challenges and Open Questions," 2024 IEEE Power & Energy Society General Meeting (PESGM), Seattle, WA, USA, 2024, pp. 1-5, doi: 10.1109/PESGM51994.2024.10688903.

United States Census Bureau 2024. “Understanding Differential Privacy.” https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html

Venkata, S. S. (Mani), Matthew J. Reno, Ward Bower, Scott Manson, James Reilly, and George W. Sey Jr. 2019. "Microgrid protection: Advancing the state of the art." techreport, Sandia National Laboratories.

Xie, X., Jan Shair, Jef Beerten, Lingling Fan, Oriol Gomis-Bellmunt, Petr Vorobev, Robin Preece, Shahil Shah, Xiongfei Wang, Yang Wang, Vladimir Terzija, “Guest Editorial: Control interactions in power electronic converter dominated power systems,” International Journal of Electrical Power & Energy Systems, Volume 155, Part A, 2024, 109553, ISSN 0142-0615, https://doi.org/10.1016/j.ijepes.2023.109553.

U.S. DEPARTMENT
of ENERGY

For more information, visit: energy.gov/xxxx

DOE/Publication Number • Month Year