Microgrid Systems: Design, Control Functions, Modeling, and Field Experience

S. Manson, K. G. Ravikumar, and S. K. Raghupathula
Schweitzer Engineering Laboratories, Inc.

Presented at the
Grid of the Future Symposium
Reston, Virginia
October 28–31, 2018

Previously presented at the
XIII Simposio Iberoamericano Sobre Proteccion de
Sistemas Electricos de Potencia, February 2017

Previously published in
Wide-Area Protection and Control Systems: A Collection of Technical Papers Representing Modern Solutions, 2017

Original edition released October 2016

Microgrid Systems: Design, Control Functions, Modeling, and Field Experience

S. Manson, *Senior Member, IEEE*, K. G. Ravikumar, *Member, IEEE*, and S. K. Raghupathula, *Member, IEEE*

***Abstract*—This paper describes the authors' experience in designing, installing, and testing microgrid control systems. The topics covered include islanding detection and decoupling, resynchronization, power factor control and intertie contract dispatching, demand response, dispatch of renewables, ultra-fast load shedding, volt/VAR management, generation source optimization, and frequency control.**

***Index Terms*—distributed power generation, islanding, grid resilience, microgrids, smart grids.**

I. Introduction

Microgrids are electrical grids capable of islanded operation separate from a utility grid. These grids commonly include a high percentage of renewable energy power supplies, such as photovoltaic (PV) and wind generation. Microgrids, therefore, commonly have problems related to their low system inertia and the intrinsic limitations of power electronic sources (PESs). Further compounding these problems is the fact that the modern electrical load base has an ever-growing percentage of power electronic loads (PELs). In the authors' experience, PELs do not provide natural grid stabilization like motor loads connected directly to a power system do. (Note that emulation of inertia by PES and PEL is possible; however, this technique is not yet in general use.)

High PEL and PES compositions have several characteristics that do not promote the stability of the electric power system. These electronic sources have control systems that act to self-preserve the thyristors or insulated-gate bipolar transistors (IGBTs) from damage. This self-preservation is accomplished by tripping the PES and PEL offline upon detection of spurious voltage or current waveforms. The fault ride-through capacity of the PES and PEL is significantly smaller than that of conventional rotating generation and loads.

The second problem commonly associated with PES and PEL relates to the control systems used to drive the power electronic interfaces. These control systems have uncertain behavior when islanded from a stiff utility grid. They are known to have interoscillations with mechanical shafts, electrical power system equipment, and other PESs and PELs [1]. These controls also limit the amount of fault current in a manner very unlike conventional power generation.

S. Manson, K. G. Ravikumar, and S. K. Raghupathula are with Schweitzer Engineering Laboratories, Inc., Pullman, WA 99163 USA (e-mails: scott_manson@selinc.com; krisgubb@selinc.com; saira@selinc.com).

The third problem associated with these PESs is that they provide no inertial contribution to the power system. Electrical rotating generators and motors have their rotational inertia coupled to the power system through the electromagnetic air gap formed between a rotor and stator. The combination of machine winding ratios (pole counts) and the electromagnetic forces in these air gaps allow all rotating machines on a power system to sum their individual inertias into a single grid inertia. Without the inertia associated with electrical machines, a power system frequency can change instantaneously, thus tripping off power sources and loads and causing a blackout.

Microgrid control systems (MGCSs) are used to address these fundamental problems. The primary role of an MGCS is to improve grid resiliency. Because achieving optimal energy efficiency is a much lower priority for an MGCS, resiliency is the focus of this paper. This paper shares best practices in the design, installation, and validation of MGCSs and summarizes the typical control and protection functions of an MGCS.

II. MGCS Design

An MGCS is an integrated system comprised of the following systems:

- Centralized and distributed control systems.
- Coordinated protection systems.
- Communications infrastructure.
- Power quality and revenue metering.
- Visualization systems.
- Engineering tools.
- Economic optimization systems.

A. Architecture

Fig. 1 shows a typical MGCS architecture in a layered representation. Layer 1 through Layer 4 are referred to together as the MGCS. The primary purpose of Layer 1 through Layer 3 is to improve grid resiliency. Layer 4 is the only level devoted to non-resiliency MGCS functions.

Layer 0 contains the equipment within the microgrid. Such as circuit breakers, transformers, transmission lines, cables, motors, traditional generation, renewable resources, and the like. The equipment at Layer 1 has hardwired connections to monitor and control this equipment, such as current transformers (CT), potential transformers (PT), and digital status and controls.

Layer 1 includes multifunction protective relays, remote I/O modules, and meters. Layer 1 devices provide all of the I/O, data collection, metering, protection, and physical control of

Layer 0 devices. All of the protection and some of the controls are programmed in these Layer 1 devices. Typical controls in Layer 1 include islanding detection, decoupling, and resynchronization. The microprocessors in the Layer 1 equipment provide a robust distributed control and protection system that mirrors the well-proven designs of the utility power system.

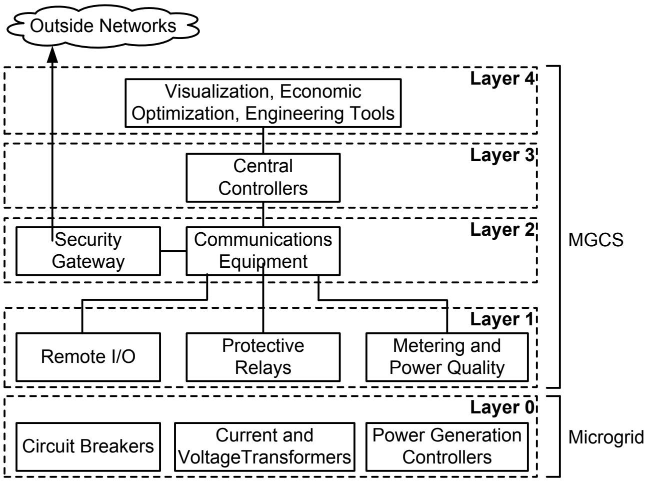

Fig. 1. MGCS Architecture

Layer 1 protection systems protect tremendously expensive assets such as transformers, buses, lines, generators, motors, heaters, capacitors, and switchgear. These protection systems can prevent or minimize catastrophic damage to equipment. Much of the Layer 0 equipment has long manufacturing lead times, thus, a properly coordinated Layer 1 protection system reduces microgrid downtime.

Layer 1 devices provide much of the diagnostic information of a power system, such as sequence of event (SOE) records, oscillography recordings, synchrophasor data collection, and more. The failure of equipment in higher layers does not have any effect on the functionality of the Layer 1 equipment.

Layer 2 communications equipment interrogates the protective relays, remote I/O modules, and meters and aggregates data to be transported to the centralized Layer 3 controllers. Security gateways at Layer 2 provide visibility of the MGCS to external users, businesses, or electric utilities. The MGCS communications backbone is constructed with Ethernet- or serial-based technology. The data flowing on these channels are segregated into real and non-real time channels to ensure deterministic and prompt delivery of status and controls data. The failure of equipment in higher layers does not have any effect on the functionality of the Layer 2 equipment.

The Layer 3 centralized controllers provide control functions that require status information from one or more Layer 1 devices. The algorithms in Layer 3 devices make decisions and send commands back to the Layer 1 equipment. Typical controls in Layer 3 include power factor control, intertie contract dispatching, demand response, dispatch of renewables, load shedding, volt/VAR management, generation source optimization, and frequency control. The failure of equipment in higher layers does not have any effect on the functionality of the Layer 3 equipment.

Layer 4 equipment includes diagnostic and engineering tools, such as automatic event report (oscillography) retrieval, detailed sequential events recorder (SER) reports, and settings management for all MGCS equipment. Human-machine interfaces (HMIs) provide the real-time status of the MGCS to operations and maintenance staff. Economic optimization, automated financial transactions, forecasting, and time-synchronization equipment reside at Layer 4. Failure of equipment in Layer 4 has no effect on the functionality of the lower, more critical layers.

B. Building a Reliable MGCS

This section details the accumulated experience of the authors in building hundreds of MGCSs focused on resiliency. Following these basic design principles has achieved MGCSs with design lifetimes of approximately 30 years.

Critical to low-cost, long-term ownership is the use of environmentally rated equipment. Caustic or salty environments require conformal coating of electronic boards. Equipment with large temperature ranges is required for outdoor enclosures. Resistance to electromagnetic interference (EMI) prevents misoperations caused by high levels of harmonics present from PES and PEL. Today, solid-state memory offers much higher reliability than rotating memory storage devices. Carefully match MGCS components with the environmental requirements.

Failures in the MGCS must be immediately identified in the equipment. All Layer 1 through Layer 4 equipment must continuously self-test the status of its memory, CPU, power supplies, or other failure modes. It must report internal errors outside the MGCS to alert maintenance staff of failures.

Reliability analysis techniques [2] commonly determine that the power supply to the MGCS electronics is the weakest link in reliability. The simplest way to improve MGCS reliability is to power all equipment directly from dc battery supplies. Uninterruptible power supplies (UPSs) that convert dc battery storage to ac voltages reduce the overall reliability of an MGCS; this is because they are an unnecessary component. Power supplies inside all MGCS equipment are oversized for long lifetimes (in Layer 1 through Layer 4) and should connect directly to battery dc.

Because Layer 4 systems are continuously monitored by operations staff, they are often given an undue amount of fiscal attention. This has led to many systems with wonderful visualization systems but poor grid resiliency. Designers are advised to focus first and foremost on Layer 1 through Layer 3 MGCS equipment and functionality.

Most microgrids are brought online as partially constructed systems. This can pose complications for central control systems that are designed for all grid assets to be online. MGCS designs must therefore incorporate software switches to enable the protection and controls to be enabled and commissioned incrementally. For example, load shedding algorithms existing at Layer 3 must be designed to operate properly with only part of the I/O commissioned. Another example is that assets must be protected from destruction with protective relays at Layer 1, regardless of the commissioned state of a central microgrid controller.

It is preferable that all central control schemes run on separate devices. By having these algorithms run autonomously, the loss or modification of one system will not affect the others. Fault tree analysis shows that single points of failure greatly reduce system availability. Thus, the reliability of an MGCS is increased by distributing central controls among several fully independent hardware modules.

The MGCS shown in Fig. 1 yields a very modular, expandable, and easily commissioned system. Integrating a new Layer 1 controller can take place while all other systems are running. Modifications to an existing control system must not affect other systems.

PES and PEL are commonly dispersed across large geographic, and often remote, regions. This puts Layer 1 equipment large distances from Layer 3 and Layer 4 equipment. Layer 2 equipment must therefore be capable of long-distance communications.

Using fault-tolerant code in Layer 3 controller algorithms greatly enhances system reliability. One example is called self-healing data selection. This technique works by switching the data used by the algorithms from the primary to secondary source when the quality or status of the primary source changes. One example of self-healing is that load shedding systems should select an alternative load to shed when the algorithm cannot verify the status of the first-choice load.

Some form of data quality and time-stamping is also required. Poor data quality requires the algorithm to either select another source or shut down the algorithm. Old time stamps indicate unacceptable communications latency and may also require reselection of a data source or shutting down. Some examples of a poor data quality indication include the following:

- Out of range, unrealistic, or intermittent data.
- Communications failures or latencies between layers.
- Layer 0 equipment not responding to commands.
- Equipment alarms.

Essential to any successful MGCS integration and long-term ownership is proper documentation. Inadequate documentation makes it impossible to hand over ownership to new engineers and invariably causes early obsolescence of an MGCS. The long-term success of any MGCS supplier is dependent upon its ability to teach end users to troubleshoot and maintain their own systems. Long-term and expensive maintenance contracts are not required if an MGCS is properly designed and documented.

Designers must specify a comprehensive testing plan for each layer of the MGCS. The procedure of testing usually involves multiple factory acceptance tests (FATs) at interface equipment suppliers, a dynamic FAT of the central controller, field installation and commissioning, and a unified site acceptance test (SAT).

C. Cybersecurity

No paper on MGCS is complete without a cautionary note on security. For MGCSs, a defense-in-depth cybersecurity architecture must be used to ensure the resiliency of the MGCS as well as keep out malicious and unauthorized communications. Compliance to National Institute of Standards and Technology (NIST) or North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) criteria further complicate the design, installation, and ownership of these systems. The following summarize the authors' successful implementation of rigorous security systems on many MGCSs. In no way is this section comprehensive, because the art and science of cybersecurity is an ever-changing field.

Security perimeters must be defined on every project. Both physical means, such as a fence, and virtual means must be employed to prevent intrusion. The best security perimeter is an "air gap," wherein no outside networks are connected to the MGCS. Unused communications ports are shut down. Industrial fiber-optic connectors prevent all but the most skilled from physical connection to the MGCS communication systems. Non-typical fiber-optic wavelengths can be selected to prevent a mistaken connection with the outside world. All physical communications ports should be kept behind locked doors.

Sometimes outside systems require status information from an MGCS. Security appliances used to bridge networks are expensive to keep up to date because new types of attacks require new countermeasures. These security appliances are the first to be attacked, and as such the authors prefer single directional (unsolicited) serial data traffic emanating from the MGCS for sending data to an outside entity. Universal asynchronous receiver/transmitter (UART) integrated circuits used only as transmitters do not respond to remote controls when their receivers have no hardwired line connected. This design has no way to respond to command messaging from the outside world.

Should remote engineering access or control be required for the MGCS, these unidirectional serial communications methods will not work. The typical solution for this is firewalls that provide secure remote administrative access to all Level 4 equipment via virtual private networks (VPNs). The cost of this sort of remote access and control must be carefully evaluated because the costs of maintaining such equipment far outweigh the initial installation and commissioning costs. Keeping rule sets and firmware up to date on the firewall equipment requires information technology (IT) professionals to perform periodic audits and updates; all of this comes with a hefty price tag.

Another key tenet to any comprehensive cybersecurity program is security against incidental misoperation. For example, induced voltages and ground plane rise caused by power system fault conditions can cause wired message packages to be distorted. Radios, PESs, and PELs commonly emit sufficient energies to cause malformed digital messages. Hardware used in the MGCS must be type tested for difficult

EMI environments to guard against misoperation. Protocols that are purpose-built for the substation power system environment are also required. Some power system protocols include additional security features that prevent misoperation under these adverse conditions; industrial, commercial, and business protocols do not have these features.

MGCS equipment must have strong, multilevel passwords; strict port time-outs; and automatic reporting of attempted access to equipment. All systems must monitor and record every access and/or change to each device. Remote access to all equipment should be blocked unless the local operations staff intentionally put equipment into remote mode.

Risk management requires transparent communication of risks from supplier to user. Service bulletins must inform the user of risks of misoperation, loss of data, or possible outside intrusion caused by defects found in a product.

Background screening, training, and regular employee monitoring must be done by all suppliers. Suppliers have the obligation to keep track of every component and setting in their system. All systems must be traceable back to a supplier, a specification, and a test sequence.

The complications and cost associated with antivirus protection, white-listing, keeping the operating system (OS) up to date, and system testing can be staggering. For example, a central controller using a commercial OS requires a complete retest and revalidation for every OS patch that is applied. For MGCSs to have more than 30-year design lifetimes, Level 1 through Level 3 devices should be embedded operational devices instead of devices with commercially available OSs.

III. Control Functions

The authors have a history of developing new and innovative MGCS control and protection algorithms. This section focuses on the essential methods and algorithms used to achieve grid resiliency.

A. Grid-Connected Controls

MGCSs simultaneously manage several points of common coupling (PCCs) to an adjacent utility grid. The MGCS can provide support to the utility when operating in this connected mode. The available functionality when operating in grid-connected (non-island) mode is described as follows.

Automatic generation control (AGC) algorithms dispatch the power output of distributed power resources to maintain power interchange at the PCCs within predetermined limits. AGC algorithms dynamically recalculate energy resource set points under all system bus configurations (topologies). The dispatch of resources is accomplished via a number of methods, including economic dispatch, renewable prioritization, grid resiliency, utility operating reserve, or demand response methods. AGC can operate to buy or sell exact amounts of power on an intertie. Additionally, an advanced AGC scheme can control the system to maintain the intertie value at zero during periods when system separation is likely (e.g., extreme weather conditions).

Peak shaving algorithms dispatch energy sources, such as batteries and conventional generation, to relieve transmission corridor congestion. For example, battery system discharging occurs during peak usages times, while charging is accomplished during minimal usage times.

A power factor control system (PFCS) is used to regulate the reactive power output of distributed energy resources to maintain reactive power interchange at the PCC while maintaining system voltages within predetermined limits. PFCSs dynamically dispatch on-load tap changers (OLTCs), capacitors, synchronous generator excitation systems, static synchronous compensators (STATCOMs), and other reactive current-producing assets. PFCSs must follow IEEE 1459-2000, the standard for calculating power factor.

The MGCS must detect island formation and, in some cases, actively decouple a power system to create a microgrid island. Automatic island detection systems use breaker status indications, disconnect switch statuses, voltage measurements, current measurements, and synchrophasor measurements to automatically detect when grid islands are formed. The island detection system handles any number of system topology bus-connection scenarios. The outcome of an island detection can be one of two options: 1) shut down the islanded microgrid by stopping generation (known as anti-islanding), or 2) modify the mode and dispatch of islanded generation sources to keep the microgrid alive (known as islanding).

Automatic decoupling systems intentionally island microgrids from a utility. Decoupling is most commonly performed after a fault outside the PCC to stop intergrid instabilities, to prevent damage to distributed energy supplies, or for a contractual requirement between two entities. This intentional islanding can have a cascading effect, forming additional microgrids that are composed of their own distributed energy sources and loads. This decoupling is typically accomplished by opening circuit breakers at the PCC. Modern automatic decoupling schemes typically include frequency, rate-of-change of frequency, and directional power elements (32). Combinations of several protection elements are commonly coordinated to improve sensitivity and selectivity.

B. Islanded Controls

After a microgrid island is formed, the MGCS modifies the mode and dispatch of islanded generation and provides immediate load balancing through load shedding, generation shedding, load runback, and generation runback. These actions keep the frequency and voltage within allowable parameters for any number of islands. These systems are sometimes referred to as load management schemes.

Load and generation shedding schemes quickly stabilize system frequency during periods of sudden loss of generation and/or load. Load shedding systems automatically reduce electrical loads in response to island events or loss of distributed power generation. Modern load and generation shedding and runback schemes dynamically select loads based on live power measurements, operator-selectable prioritization, and changing bus topology conditions.

Contingency-based load shedding, generation shedding, load runback, and generation runback (CBLSGSLRGR) schemes operate when a breaker is opened under current flow. CBLSGSLRGR schemes track every combination of system topology and bus configuration by dynamically tracking the system state of the microgrid. These schemes are well-described in the literature [3] [4] [5]. Contingency-based load and generation shedding responds in less than one power system cycle to prevent frequency and/or voltage collapse.

Multiple simultaneous or closely timed breaker openings pose significant challenges to designers of CBLSGSLRGR schemes. For example, after a line fault the state of a power grid is changing rapidly. Power flows are changing near instantaneously, rotors are swinging, multiple circuit breakers open sequentially, system impedances change, transient and subtransient effects from rotational machines occur, and the more fragile PES and PEL shut down. Compounding this problem is that Layer 1 equipment has filtering, debounce, delay, and asynchronous updates in power measurements and message propagation to a central controller. Thus, during these times of rapid power system changes, the CBLSGSLRGR algorithms must operate without real-time information. Without mitigation, these transient problems will cause the CBLSGSLRGR scheme to misoperate. MGCS designers must ensure that suppliers have provided adequate protection against these inevitable events. Testing of CBLSGSLRGR algorithms under the duress of this condition is a primary rationale for the real-time closed-loop testing described later in this paper.

Load runback and shedding are used when islanding events result in insufficient generation on a microgrid, such as during an islanding event during import of power from a PCC. Under these conditions, power system frequency can quickly fall out of control and result in a power outage. Load runback schemes reduce but do not entirely shut off loads. Load runback schemes require adjustable loads, such as pumps on adjustable speed drives, building ventilation fans, and heaters. Load shedding schemes trip loads off by opening circuit breakers.

Generation runback and shedding are used when islanding events result in excessive generation on a microgrid, such as an islanding event during export of power to a PCC. Under this condition, power system frequency can quickly rise out of control and result in a power outage. Generation runback schemes reduce the output of distributed generation faster than PES and rotation governor frequency controls can, thus keeping the generation online. Generation shedding schemes trip circuit breakers to get power supplies offline, and runback schemes bypass frequency control systems and send feed-forward commands directly to valve controls.

Frequency-based load and generation shedding methods have recently advanced with inertia compensation and load-tracking (ICLT) schemes. ICLT schemes track system inertia, load composition, frequency, and rate of change of frequency in their calculations [6]. ICLT schemes have the added robustness of not requiring any breaker status data to make real-time island and state measurement decisions. ICLT schemes are a critical backup to CBLSGSLRGR schemes because CBLSGSLRGR schemes do not detect broken wiring in a circuit breaker, shorted CT windings, dc battery failures, or a long list of control system and mechanical problems that shut down power systems without opening breakers.

Of particular importance in all MGCS control strategies is the continuous and dynamic monitoring of the active (P) and reactive (Q) power capabilities of conventional and PES generation on a microgrid. These P and Q capabilities must be ascertained for both momentary capability and longer-term capacities. Fig. 2 shows a typical set of capability curves for a combustion turbine and a battery storage system that must be dynamically monitored by a MGCS.

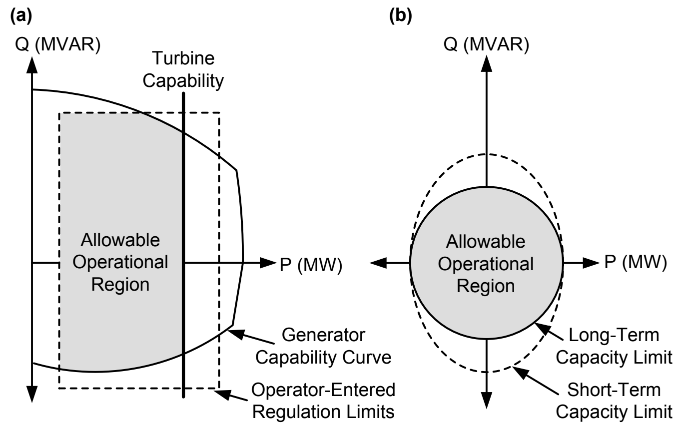

Fig. 2. Dynamic Capability Monitoring in a Typical Combustion Turbine Driven Generator (a) and a Typical Battery Storage System (b)

Islanded microgrids do not have a strong utility connection to control the power system frequency. For this condition, MGCSs use advanced AGC techniques, as shown in Fig. 3, to hold system frequency at nominal while simultaneously maintaining distributed generation outputs within an allowable operational region, as shown in Fig. 2. When a distributed generation source is switched into stiff frequency control (also known as isochronous operation), the AGC system dispatches all nonfrequency regulating sources to keep the isochronous units within an allowable operational region.

MGCS central controllers have volt/VAR algorithms that regulate the reactive power output of distributed energy resources to maintain islanded bus voltages within predetermined limits. These systems dynamically dispatch OLTCs, capacitors, excitation systems, electronic inverters, and others reactive current-producing assets.

MGCSs contain both unit synchronization and system synchronization systems. After either a manual or automatic initiation, these systems automatically reduce slip, phase angles, and voltage differences before automatically closing a circuit breaker.

Unit synchronization schemes adjust slip, phase angles, and voltage differences by sending control set points to a single distributed energy supply. These schemes are most commonly provided in a single Layer 1 protective relay. The relay automatically closes the circuit breaker once acceptable slip, phase angles, and voltage differences are detected.

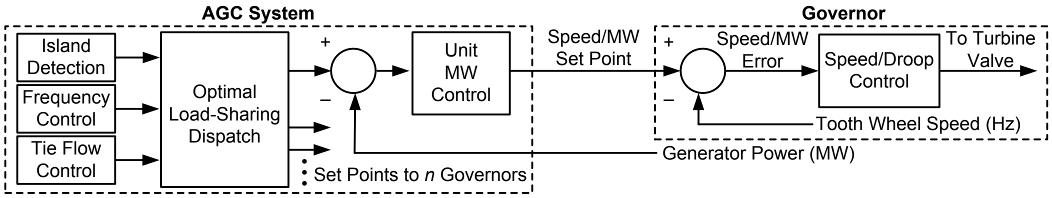

Fig. 3. Typical AGC Strategy

System synchronization schemes resynchronize two or more islanded microgrids. These systems adjust slip, phase angles, and voltage differences between the two grids by sending control set points to any number of distributed energy supplies [7]. These schemes require several relays, I/O modules, and a central controller. Relays at each synchronization point automatically close the circuit breaker once acceptable slip, phase angles, and voltage differences are detected.

C. Adaptive Protection

The distributed generation of a microgrid can create a complicated protection coordination problem. Utility distribution circuits have unidirectional power flows that greatly simplify the coordination of protection systems. Some loads in a microgrid can become sources (batteries and flywheels). Fault current levels can be dramatically different in grid-connected versus islanded operation.

Differential schemes (87) and zone-interlocked schemes can be configured to work for all operational conditions of both grid-connected and islanded modes. Differential techniques are less sensitive to fault levels, thus overlapping bus, transformer, and cable differential schemes are a very popular choice. Zone-interlocked schemes use directional elements and communications to form schemes that can improve selectivity and operating times [8]. Designers are advised to be aware that 87 elements must be supervised by harmonic and other restraint elements to prevent misoperation during load and transformer energization.

Time coordination schemes must be set for all grid-connected and islanded mode conditions and can become very complicated and expensive. Time coordination schemes must adapt to the different fault currents, grounding conditions, and topology of a microgrid. Fault currents of a utility are typically tens of thousands of amperes, whereas smaller distributed generation, such as PES, often provides little or no fault current. The fault currents of an islanded grid can become very close to the upper load limits, making proper time-overcurrent type coordination difficult and sometimes impossible. The loss of a transformer can change grounding conditions from solidly grounded to no grounding, thus making ground fault detection very difficult. Microgrids that island with different formations of cables, sources, feeders, and load buses can require a complete topology tracking supervisory system to advise protection relays of which settings to use.

IV. Control System Validation

Modeling and real-time closed-loop modeling of microgrid power systems is essential in determining the efficacy of MGCS protection and control schemes.

PESs and PELs do not generate continuous fault current at levels similar to synchronous generators. This can create serious (and dangerous) protection coordination problems. MGCSs must therefore be tested with real-time, Electromagnetic Transients Program-style (EMTP-style) modeling of the combined protection and controls system to validate that all protection and control systems function safely.

With all of the possible permutations in state and time that a power system can take on, it is essential to test all MGCSs prior to installation. This section describes a real-time simulation of a power system being connected directly to a MGCS, as shown in Fig. 4. The MGCS shown in Fig. 4 is most commonly the Layer 3 central MGCS controller. The real-time power system model (RTPSM) is a full EMTP that provides real-time changes in power, frequency, rotor angle, voltage, and load reactions to frequency and voltage.

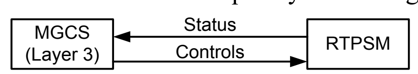

Fig. 4. Closed-Loop Testing Environment

A. Modeling Methods

The RTPSM represents the behavior of only Layer 0 equipment. The RTPSM predicts the electrical, magnetic, and mechanical dynamics of power sources, loads, transformers, generators, turbines, and associated Layer 0 control systems. Accurate electrical and magnetic phenomena require a simulation time step of 80 microseconds or faster. Governors, hydraulics, steam control, and mechanical valves can be modeled at slower simulation time steps.

The advantage of running the test in real time is that a model operates sufficiently fast to test all the closed-loop control and protection systems. Because the RTPSM is real-time, thousands of test cases are run, providing site personnel with a great amount of confidence that all systems will react as expected under the most adverse scenarios.

User-attended FATs with the testing arrangement of Fig. 4 are strongly recommended. The microgrid owner's intimate knowledge of their power system is useful in testing tough corner-case scenarios; an owner will commonly recall unusual phenomena to be modeled with the RTPSM. The FAT also serves as a fast training program for operators of the MGCS. Because thousands of tests cases are run, an operator can gain more experience from an RTPSM FAT than from a decade of field work.

B. Fit-for-Purpose Modeling

Model development for the RTPSM of a microgrid system can take from weeks to years, depending on the complexity and accuracy requirements. Modeling engineers should therefore build fit-for-purpose models that are the simplest model possible to accurately replicate the field behaviors and interactions with the MGCS.

To accurately model dynamic microgrid phenomena, RTPSM mechanical, electrical, and magnetic models must be derived from first-principle physics. Validation reports must be accompanied with the mathematical derivation of model components. Microgrid modeling specialists now have proven and validated first-principle RTPSM models for systems such as flywheel storage, wind generation, battery storage, turbine and reciprocating driven (conventional) generation, governors, exciters, PV controls, dump loads, dispatchable loads, battery storage, and power electronic devices.

Once a complex and first-principle model has been validated with field results, it is common to find simplifications for these modeling blocks that expedite overall model development and have no impact on model accuracy. These simplifications take decades of experience and significant field testing to validate.

The nature of the MGCS algorithm being tested can significantly affect the RTPSM electrical, mechanical, and magnetic models developed. For example, an AGC system may take 30 seconds to return the frequency to nominal after an event; this sort of control scheme is much slower than rotating machinery transient and subtransient electrical time constants, thus a less detailed generator and motor electromechanical model will suffice. There are many quality papers available to guide MGCS modeling engineers in their efforts to build the simplest possible models that depict relevant dynamic behaviors [9]. For example, Fig. 5 is a fit-for-purpose model of an islanded microgrid power system that was sufficiently accurate to replicate frequency instabilities caused by a steam governor low-load instability [10].

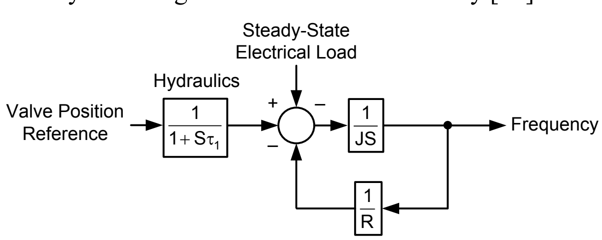

Fig. 5. Simplified Power System Model

Fig. 5, however, would not be an adequate model for transient rotor angle stability studies.

C. Model Validation

Model validation is the process of proving that a microgrid model accurately depicts pertinent dynamic electrical, magnetic, and mechanical behaviors. It is typical to build detailed models of steam boiler controls, governor hydraulic systems, gas turbine valve nonlinearities, wind turbine blade controls, PV reactive power controls, battery charging controls, generator transient models, complex load models, and more. These models can be only considered accurate enough once live performance test data are collected from real equipment and compared with model performance. To make RTPSMs match field performance requires rigorous validation, which commonly takes more effort than building the model itself.

Fig. 6 shows a comparison of frequency responses for a complete microgrid model versus data captured from a live field event. This model was deemed accurate enough because the peak and steady-state frequency were very close. Note that the transients difference between 5 and 20 seconds in Fig. 6 are different; this is acceptable because this had no impact on the MGCS strategies being deployed.

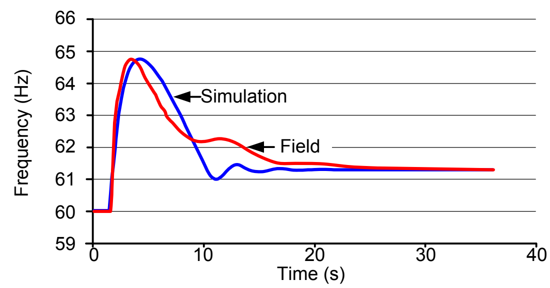

Fig. 6. Simulated and Field Frequency Response

RTPSM developers must prove that their models accurately depict field phenomena. This evidence is best compiled into a model validation report to be delivered before the FAT occurs. This report usually has individual validations of the following genres of behavior: steady-state electrical conditions, short-circuit conditions, power generation active and reactive power controls, utility power system models, and load dynamics.

Steady-state electrical conditions are validated by the tabulation of power flow results. These results should include bus voltages, island frequencies, active and reactive power flows, and generator outputs. These tabulated values are compared to the known operation of similar microgrids and known flows of installed equipment. Several cases should be provided, including PCC open, islanded conditions, and cases with some power production offline. These data validate that the electrical impedances, nominal load levels, distribution of load to feeders, normal operating status of breakers, and isolation switches are correct.

Short-circuit conditions are validated by the tabulation of phase-to-ground and phase-to-phase fault values at several locations in the microgrid. These tabulated values are compared to known operations of similar microgrids and known fault levels of installed equipment. Several cases should be provided, including PCC open, islanded conditions, and cases with some power production offline. These data validate the electrical transient impedances, magnetic models, grounding schemes, and the simplified models of the utility beyond the PCC.

RTPSMs of power generation and load and associated frequency, power, voltage, and stabilization control systems are validated by plotting modeling data against data captured in the field. Field data are typically collected from modern microprocessor-based protective relays, digital governor controls, and digital field excitation controls. Common tests to run are load rejection and load pickup tests; these must be run in both islanded and grid-connected modes.

V. Conclusion

The essential requirements for a successful MGCS deployment include the following:

- An architecture that allows for easy testing, high reliability, and proven maintainability.
- System resilience achieved before designing economic optimization systems.
- Cybersecurity designs, methods, and processes followed during the entire lifecycle of the MGCS.
- Active and reactive power dispatch programs that work seamlessly as the grid transfers between islanded and grid-connected modes of operation.
- Active and reactive power dispatch programs that keep power generation supplies within allowable long-term operational limits.
- Automatic de-coupling and separation at all PCCs.
- Subcycle wide-area load and generation shedding systems that keep a microgrid alive during all loss of PCC, distributed generation, or load.
- A proven ICLT scheme to act as a backup load and generation shedding scheme.
- System-wide synchronization schemes that automatically recombine any number of separate islanded grids.
- Coordinated protection during all possible grid-connected and islanded operation modes.
- Dynamic models that are mathematically based on first-principle physics, are validated against field captured data, and have undergone customer-witnessed factory acceptance testing.

VI. References

[1] T. Fujii, H. Masuda, Y. Ogashi, M. Tsukakoshi, and M. Yoshimura, "Study of Subsynchronous Torsional Interaction With Voltage Source Inverter Drive for LNG Plant," proceedings of the 2011 IEEE Industry Applications Society Annual Meeting, Orlando, FL, October 2011.

[2] G. W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," proceedings of the 4th Annual Substation Automation Conference, College Station, TX, April 1998.

[3] W. Allen and T. Lee, "Flexible High-Speed Load Shedding Using a Crosspoint Switch," proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.

[4] E. R. Hamilton, J. Undrill, P. S. Hamer, and S. Manson, "Considerations for Generation in an Islanded Operation," proceedings of the 56th Annual Petroleum and Chemical Industry Technical Conference, Anaheim, CA, September 2009.

[5] S. Manson, A. Khatib, M. Checksfield, and P. Duffield, "Case Study: Simultaneous Optimization of Electrical Grid Stability and Steam Production," proceedings of the 61st Annual Petroleum and Chemical Industry Technical Conference, San Francisco, CA, September 2014.

[6] S. Manson, "Systems and Methods for Under-Frequency Blackout Protection," U.S. Patent 9,008,850, April 14, 2015.

[7] S. M. Manson, A. Upreti, and M. J. Thompson, "Case Study: Smart Automatic Synchronization in Islanded Power Systems," proceedings of the 51st Annual Industrial & Commercial Power Systems Technical Conference, Calgary, AB, Canada, May 2015.

[8] F. K. Basha, R. Palaniappan, A. Balasubramanian, R. Anne, M. J. Thompson, and K. L. Oliver, "Implementation of Reliable High-Speed Islanding Detection, Zone Interlocking, and Source Selection Schemes Using Smart Algorithms," proceedings of the 51st Annual Industrial & Commercial Power Systems Technical Conference, Calgary, AB, Canada, May 2015.

[9] A. R. Khatib, M. Appannagari, S. Manson, and S. Goodall, "Load Modeling Assumptions: What Is Accurate Enough?" proceedings of the 62nd Annual Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

[10] S. Manson, B. Kennedy, and M. Checksfield, "Solving Turbine Governor Instability at Low Load Conditions," proceedings of the 62nd Annual Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

VII. Biographies

Scott Manson received his M.S.E.E. in electrical engineering from the University of Wisconsin–Madison and his B.S.E.E. in electrical engineering from Washington State University. Scott is currently the engineering services technology director at Schweitzer Engineering Laboratories, Inc. (SEL). In this role, he provides consulting services on control and protection systems worldwide. He has experience in power system protection and modeling, power management systems, remedial action schemes, turbine control, and multi-axis motion control for web lines, robotic assembly, and precision machine tools. Scott is a registered professional engineer in Washington, Alaska, North Dakota, Idaho, and Louisiana.

Krishnanjan Gubba Ravikumar received his M.S.E.E. degree from Mississippi State University and his B.S.E.E. from Anna University, India. He is presently working as a supervising engineer in the Schweitzer Engineering Laboratories, Inc. engineering services division, focusing on model power system development and testing for special protection systems. His areas of expertise include real-time modeling and simulation, synchrophasor applications, remedial action schemes, and power electronic applications. He has extensive knowledge of power system controls and renewable distributed generation. He is a member of the IEEE and the Eta Kappa Nu Honor Society.

Sai Krishna Raghupathula received his M.S.E.E. degree from University of Idaho. He is currently a regional manager for the engineering services division of Schweitzer Engineering Laboratories, Inc. (SEL). He is an electrical engineer who specializes in control system design, power management systems, remedial action schemes, power system controls, system integration, power electronics, and consulting services.