Autoconfiguration of Microgrid Controls

Brandon Marcum, Ellery Blood, Jason Dearien, and Scott Manson
Schweitzer Engineering Laboratories, Inc.

Presented at the
Power and Energy Automation Conference
Seattle, Washington
March 3–4, 2020

Autoconfiguration of Microgrid Controls

Brandon Marcum, Ellery Blood, Jason Dearien, and Scott Manson, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper describes how an autonomous microgrid control and protection system is automatically configured without human involvement. Two variants of this solution are shared: one for a rapidly deployed, mobile power system, and one that integrates a fixed campus power system. Benefits of a distributed publish/subscribe protocol and a self-configuring automation system are shared. Software-defined networking (SDN) technology is used to ensure network security, rapid network adoption, and flow control configuration. Successful procurement and supply chain security methods are shared.**

I. Introduction

The Massachusetts Institute of Technology (MIT) Lincoln Laboratory and U.S. Army Research Laboratories have developed a new interoperable communications standard for controlling microgrid systems called Military Standard Tactical Microgrid System (MIL-STD-TMS). The authors validated the MIL-STD-TMS specification by building a prototype microgrid system. In the prototype, time-proven control and protection methods were blended with MIL-STD-TMS methods. This technology has been evaluated by the U.S. Department of Energy [1] and independent researchers [2], and it has received a research and development (R&D) award [3].

This paper describes how MIL-STD-TMS-compliant electronics automatically configure a microgrid protection and control system. Two variants of this solution are shared: one for a mobile power system, and one for a fixed campus power system. The technology outlined in this paper offers the following benefits:

- No single point of failure.
- Measured reductions in generator set (genset) fuel consumption and reduced emissions.
- Minimal training to configure or operate these plug-and-play systems.
- Interoperability with all makes, models, and sizes of military and commercial off-the-shelf (COTS) generators.
- Reduced accumulation of unburned hydrocarbon residue in the exhaust system, known as wet stacking, and reduced need for corresponding maintenance.
- Key electronic components that are identical at all gensets, making parts easily interchangeable.
- Electronics that meet strict cybersecurity control policies, such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Risk Management Framework (RMF), the National Institute of Standards and Technology (NIST) cybersecurity framework, and ISA 99.
- Load sharing and interoperability with any proprietary parallel generator system.
- A control method that allows gensets to be geographically dispersed to improve power resiliency.

II. The Challenge

Present reciprocating engine gensets, inverter-based renewable (IBR) systems, and grid-support battery (GSB) systems have many problems that limit their practical use in microgrid systems. These problems include single points of failure, procurement bottlenecks, fragile and noninteroperable control methods, and more. All the challenges explained in this section are corrected with the technology described in this paper.

Load-sharing lines between gensets are a potential single point of failure. Conventional high-speed load-sharing communications lines cannot transmit further than a few meters, requiring that all paralleled gensets be co-located to ensure power system frequency and voltage stability.

Gensets, IBRs, and GSBs use outdated proportional integral derivative (PID) control loop techniques. Microgrids with gensets, electronic loads, IBRs, or GSBs commonly have frequency and voltage instabilities [4]. This causes gensets to have increased fuel usage and emissions.

Procurement managers throughout the world are commonly locked into a specific genset brand and model for an entire fleet due to proprietary load sharing and control interfaces. Interoperability is not possible with the present equipment being procured. This creates cost overruns and single-manufacturer vulnerabilities. This lock into a specific brand and model is caused by genset manufacturers because their technology does not interoperate with other genset manufacturers. Dissimilar or mismatched gensets and inverters must be capable of working in parallel for a resilient procurement program.

All parallel engine control methods used in tactical microgrids today employ a technique called isochronous (ISO) load sharing. This method puts all gensets into an ISO mode that depends on a high-speed communications line for stabilization. If this communications line fails, the system will have frequency and voltage instabilities. For this reason, North American utilities do not allow these control techniques on their power systems. These techniques are inherently destabilizing, impractical to maintain, unreliable, and do not allow interoperation between diverse manufacturer gensets, IBRs, or GSBs.

Gensets are oversized given maximum power demands. This causes large fuel waste, shortens operational time due to excessive fuel consumption, pollutes unnecessarily, wastes money, and prematurely destroys engines with wet stacking. This waste necessitates the transport of extra fuel through war-torn or impoverished locations, putting human lives at risk.

Most microgrid operators are not electric power system experts, yet modern genset, IBR, and GSB configuration and maintenance is complicated. This discrepancy makes it time-consuming and expensive to configure a reliable and resilient microgrid in remote locations. Equipment specification, designs, field installation, repairs, and field commissioning require that specialists spend significant time traveling and in the field.

Cybersecurity challenges for legacy genset communications systems include open protocols, managed switches, and nonsecure ports, and there are logistical difficulties that come with operating system maintenance and anti-malware and software updates.

III. Cooperative Research and Development

The MIT Lincoln Laboratory and U.S. Army Research Laboratories developed the MIL-STD-TMS interoperability communications system standard. Power system experts validated the specification by building a prototype MIL-STD-TMS microgrid system. During the prototype project proving the communications interoperability, additional research and development solved a great number of U.S. Department of Defense (DoD) mobile power problems.

Power system experts determined the root cause of each deficiency and designed a safe, reliable, low-cost solution. By blending gigawatt utility scale controls and protection methods with the MIL-STD-TMS standard [5], a whole new level of reliable, safe, and economical power system was developed. This system

- Has no single point of failure.
- Does not limit acquisitions to a single manufacturer.
- Does not require onsite expert for PID tuning.
- Allows for geographic dispersal of gensets.
- Allows for minimally sized and highly efficient gensets from multiple manufacturers to interoperate.
- Provides superior grid power system resiliency, reliability, and power quality.

These systems are so simple to operate that high school interns have successfully operated a 440 kW power system comprised of eight gensets from four different manufacturers. The cybersecurity posture of the systems is also improved and simplified, and all mission-critical equipment is sourced exclusively from U.S. manufacturers. This work shows the power of linking industrial energy system experts with DoD researchers.

IV. MIL-STD-TMS

MIL-STD-TMS specifications call out an interoperable communications structure layered upon the proven Data Distribution Service (DDS) protocol. DDS is a publish/subscribe protocol that uses User Datagram Protocol (UDP) messaging between controllers. Each controller or gateway acts in one of the following MIL-STD-TMS roles:

1. Microgrid controller (MC)—sends configuration settings and coordination commands to other TMS-compliant devices.
2. Source power device (SRC)—gensets or other power-providing distributed energy resources (DERs).
3. Storage power device (STOR)—battery systems that store power for later use.
4. Distribution power device (DIST)—power distribution hardware that contains cabling and circuit breakers.
5. Load power device (LOAD)—electric power-consuming hardware that is able to publish its load-shed priority and request permission from the MC to start up.

The MIL-STD-TMS standard defines fixed data structures for each of these roles. This facilitates interoperable communications between all manufacturers.

Communication between the role members is automated and requires no human configuration. For example, when an authorized SRC (genset) is connected to the TMS local-area network (LAN), the SRC role provides a device announcement to the network. In this example, the MC automatically subscribes to the SRC after authentication of keys and starts communication of metering and control signaling. The MC sends configuration parameters to the SRC, thus facilitating acceptance on the microgrid with a known parameterization and control method.

V. Publish/Subscribe Communications

Configuration parameters and data sets are designed to allow any engine gensets to be converted to a MIL-STD-TMS. During the prototype work, four different genset models were integrated to be MIL-STD-TMS standard-compliant. All four models were from different genset manufacturers, and there were two of each model—two 30 kW models from Manufacturer A, two 30 kW models from Manufacturer B, two 100 kW models from Manufacturer C, and two 60 kW military tactical quiet generators (TQGs) from Manufacturer D.

In the prototype design, TMS interface controllers (gateways) were installed in all eight gensets and in distribution boxes, as shown in Fig. 1 and Fig. 2. The gateway selected has one outside port isolating the inside genset or distribution box communications. The inside communications consist of Ethernet port communication such as Modbus/Transmission Control Protocol (TCP) and IEC 61850 Generic Object-Oriented Substation Event (GOOSE) protocol, serial communication such as Modbus/Remote Terminal Unit (RTU) protocol over EIA 232 and EIA-485, and hardwired digital I/O.

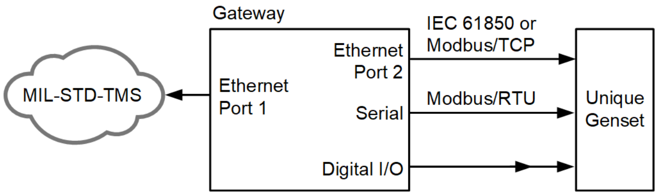

Fig. 1. Identical Gateways in Every Genset

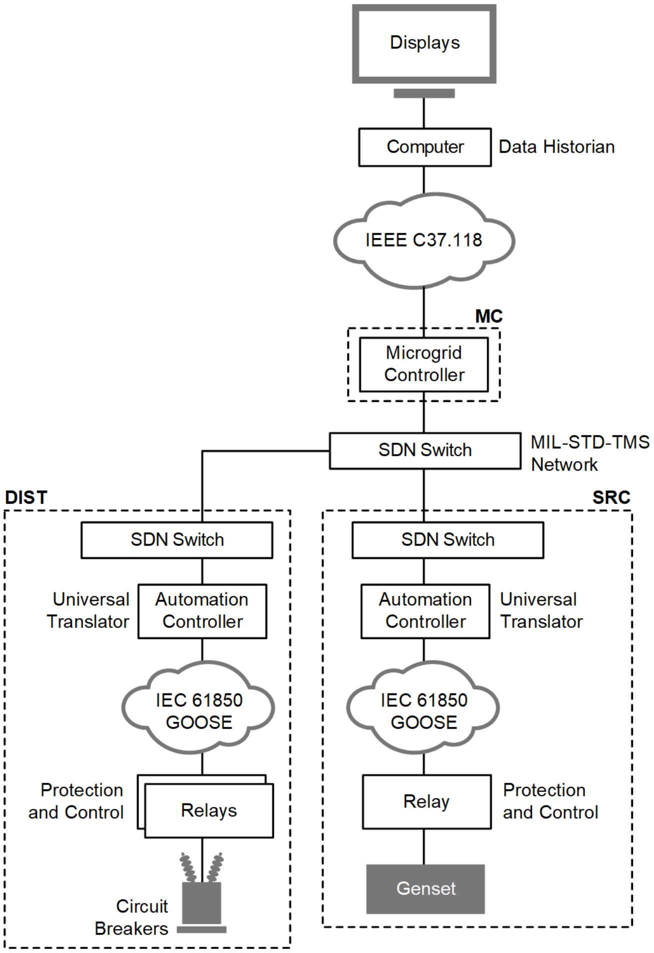

Fig. 2. Communications Architecture

Although inside communications to gensets were all unique to each manufacturer, all gateway hardware and software on all eight machines were identical. Identical controllers minimize the spare parts inventory requirements and allow components from different machines to be interchangeable. The only configuration required was specifying the role of the controllers prior to operation using eight microswitches on the controller.

Once the role is specified, the electronics automatically configure all communications, controls, and protection for the unique genset manufacturer. There is no software required to configure these systems. DERs, relays, and controllers automatically configure communication and set up control configuration among one another, thereby allowing the system to autoconfigure and run without human involvement.

Upon initial startup, each gateway or controller publishes its device announcement message, whereby it identifies its role and capabilities. Depending on the role, the device publishes unique configuration, metering, monitoring, and control data sets (topics). The controller(s) operating in the MC role receive these configuration messages and build an internal model of the microgrid configuration and capabilities. All TMS controllers and gateways periodically republish this information so that new devices that join the network will have knowledge of other participating controllers.

During operation, the power device TMS controllers running in the SRC, DIST, STOR, and LOAD roles continuously publish their state and measurement messages. These messages provide a comprehensive operational picture of the microgrid to the MC. This picture includes not only load and generation balance, but also machine health information such as coolant temperature and wet-stack residue accumulation level.

The MC evaluates these data and develops a high-level dispatch and operation strategy. This strategy is transmitted to the gateways via various messages, which direct the controllers to perform such actions as adjusting their power/frequency droop curves, connecting/disconnecting generation from the grid, shutting down/starting up generation, and connecting/disconnecting loads.

The MC further evaluates the machine health information to alert operators of condition-based maintenance indicators. Furthermore, if enabled, the MC automatically initiates wet-stack mitigation operations and/or preventive actions such as machine derating or shutdown.

During all these activities, the MC is publishing operational data via IEEE C37.118 protocol to an IEEE 2030.8-compliant continuous data collection historian. This historian provides real-time trends for operator awareness and permanent archiving to facilitate post-event analysis and adjustment of control parameters.

VI. Mobile Microgrids

Rapidly deployed, mobile power systems without connections to a bulk electric power system are typically comprised of diesel reciprocating engine generator sets. The gensets range from 15 to 200 kW each, and the total power system load is up to 1,000 kW. Mobile power is commonly used in forward operating bases, disaster relief, industrial mining operations, remote villages, island nations, and oil drilling operations. Many of these microgrids use IBRs and GSBs to reduce genset fuel usage.

Mobile genset dispatch is autonomously performed by the MC, which dispatches all SRCs. There are five MC modes for the operator to select:

1. Rapid stop (shutdown mode). This stops all power sources for a rapid demobilization of the facility.
2. Normal resiliency (equal percentage load sharing). These controls ensure nominal frequency and voltage are maintained and that watts and volt-amperes reactive (VARs) are shared between DERs of any size or from any manufacturer.
3. Optimal fuel usage (start/stop control). These controls temporarily suspend operation of unnecessary gensets, allowing the remainder of gensets to operate at a higher efficiency. Testing has shown that fuel usage can be reduced between 10 and 73 percent by employing these methods.
4. Optimal resilience mode (emergency mode). This brings all gensets and GSBs online for the maximum durability of the power system, ensuring that destruction of one or more DERs does not compromise the flow of reliable, high-quality energy to the loads. Basic physics demands that optimal

resiliency and optimal fuel usage modes are mutually exclusive. Because these modes cannot exist simultaneously, users must select which mode they desire depending on site conditions.

5. Maintenance mode (wet-stacking mitigation mode). This mode is used to de-foul the engines one at a time. This is achieved through modifications to the power dispatch plan and does not require the addition of load banks or isolation of the generator undergoing wet-stack mitigation.

These simplified controls are sufficient to control power systems with diverse loads, highly cyclic loads, diverse gensets, IBRs, and GSBs.

Fig. 3 shows a TQG with energy packet controls and MIL-STD-TMS communications. TQGs with the controls upgrade shown in Fig. 3 parallel and seamlessly share load with any genset, IBR, or GSB.

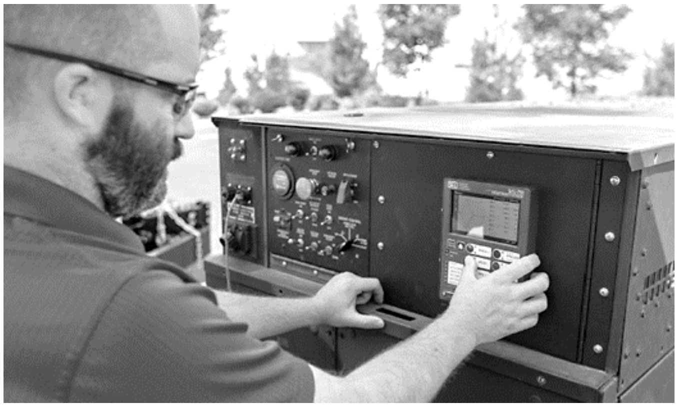

Fig. 3. TQG After a Controls Upgrade

VII. Situational Awareness

Time-synchronized, condition-monitoring systems are provided on a single heads-up display. This system records historical data for over 20 years of continuous runtime of the microgrid. The single display in Fig. 4 shows network traffic, cooling water temperatures, oil pressures, power values, frequencies, voltages, reactive power, phase angles, and machine wet-stack fouling conditions.

This single display provides predictive, condition-based maintenance indicators, which alert operators to potentially hazardous situations before they become a danger.

VIII. Energy Packet Control

One of the more challenging problems to solve has been PID and ISO load-sharing control methods used in gensets. Genset manufacturers today predominantly use PID and ISO methods. ISO PID techniques require precise control-loop tuning and commonly exhibit frequency and voltage instabilities when gensets from different manufacturers run in parallel to one another. Electric utilities prohibit ISO control of gensets while connected to the grid, making host nation connections with any diesel genset impractical.

The oil and gas industry and utilities long ago discovered that ISO techniques are inadequate. The large reliable power systems in both heavy industry and electrical utilities have interconnect standards that specifically forbid ISO control. ISO parallel controls require high-speed control signaling between gensets and geographically close generators. These methods are known to fail to allow interoperation between manufacturers and to operate poorly with renewable energy sources, batteries with inverters, and power electronic loads (e.g., data centers).

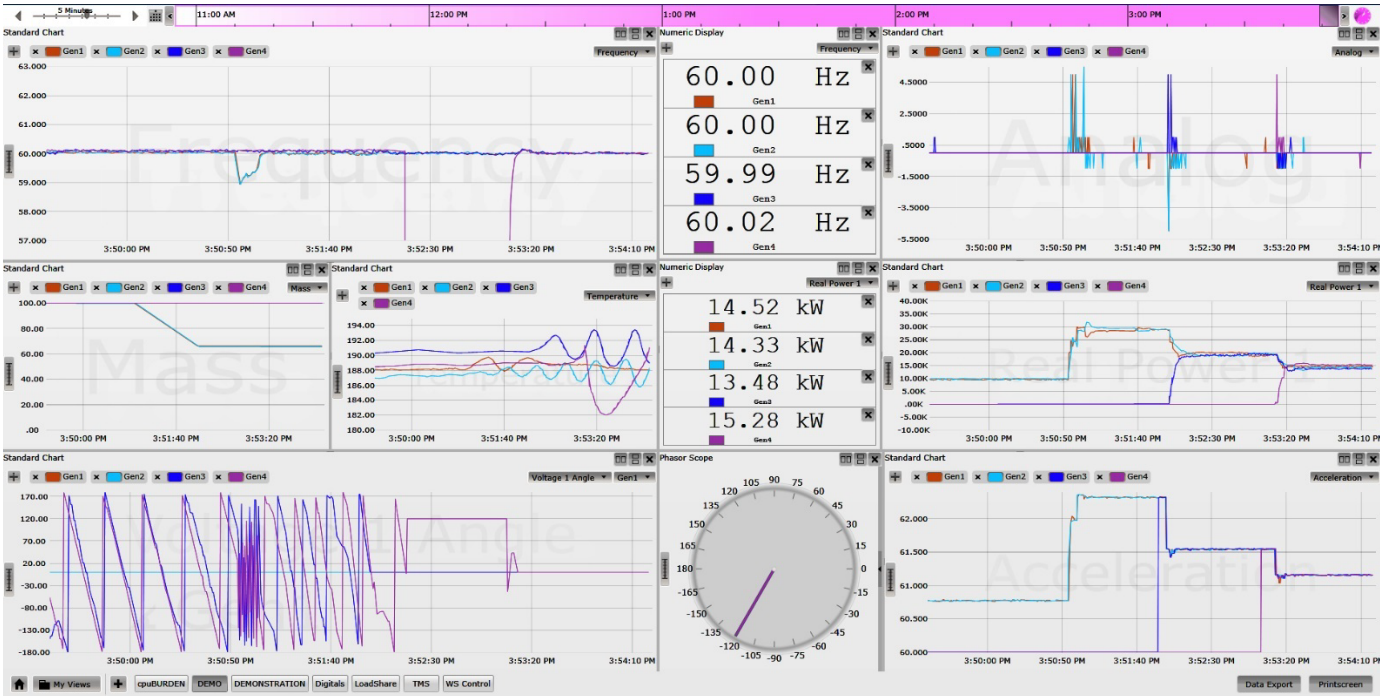

Fig. 4. Time-Synchronized Condition Monitoring

PID controls commonly exhibit frequency and voltage instability modes when powering modern electronic loads. PID controls are inherently dependent on inertia, i.e., the rotating mass of the gensets and loads. As the loads become primarily power electronic, these PID control methods are proven to destabilize the power system [4].

Fig. 5 shows two 30 kW gensets that were synchronized (paralleled) and then shared load via a twisted pair communications cable. These units use a conventional ISO PID control method using Controller Area Network (CAN) bus communications between the gensets. Note the oscillation (hunting) in power (kW) and frequency. This hunting wastes fuel, reduces engine life, and is precariously close to tripping the gensets. These oscillations are reducing the resilience of this power system.

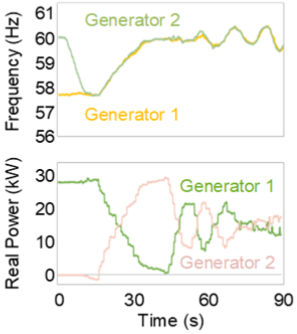

Fig. 5. Conventional Load Sharing

Energy packet controls are the preferred alternative to inertia dependence, PID control, ISO paralleling methods, power electronic (inverter) batteries, PV, and electronic loads (synonymous with “negative R” loads or P/Q loads). The same two gensets from Fig. 5 are shown under energy packet controls in Fig. 6 in the same parallel load-sharing scenario. The transient responses shown in the figures demonstrate that energy packet control provides superior resilient power system performance.

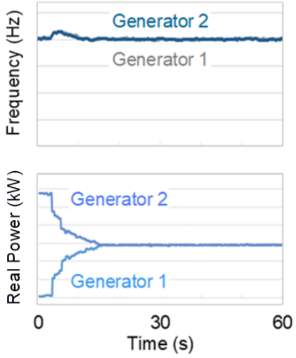

Fig. 6. Energy Packet Load Sharing

Energy packet control methods do not require a human to tune the controllers. They are faster to configure, and all gensets can be factory-set with a guarantee of interoperability with any other manufacturer gensets, inverter, or host nation.

Energy packet controls have a reduced dependence on inertia and, thus, no retuning requirement as power systems are assembled and reassembled. Inertia, load compositions, and impedances can change dramatically without requiring DER PID to be retuned.

Energy packet controls were applied by software running in the automation controller gateways and relay at every genset.

IX. Cybersecurity Underlayment

The communications between the power device TMS controller and other controllers within that device (e.g., protective relay, voltage regulator, governor, etc.) are performed on a segregated network. The TMS controller acts as a network gateway and firewall between internal device communications and the TMS network. All communications between devices on the TMS LAN are accomplished via the TMS protocol running on a DDS publish/subscribe network layer.

Automation controllers act as universal translators (protocol gateways) between SRC, MC, and DIST per the predefined TMS data structures. They also provide firewalled security and a physical network isolation barrier between the MIL-STD-TMS LAN and the communication within an SRC, MC, or DIST. The architecture is shown in Fig. 2.

The pilot project included a cybersecurity underlayment to secure the MIL-STD-TMS-based solutions. After examining conventional network security approaches, the team chose a design that uses three components: automation controllers, protective relays, and a software-defined networking (SDN) Ethernet switch (shown in Fig. 2). This design is a proven, practical solution [6] designed for the transmission and distribution substations of North America. Automation controllers are used in power system utility substations around the world and are commonly part of NERC CIP-compliant substation designs at critical facilities [7].

Protective relays have a minimal real-time operating system, and the automation controllers have embedded whitelisting controls. No computers or commercial operating systems were used in any TMS role (MC, DIST, SRC, etc.). One commercial operating system was used in the historian.

SDN underlayment technology is used to lock down the network and to identify intrusions. As shown in Fig. 7, any traffic not explicitly configured in the SDN Ethernet switch is routed to a heads-up display acting as an intrusion detection monitoring system.

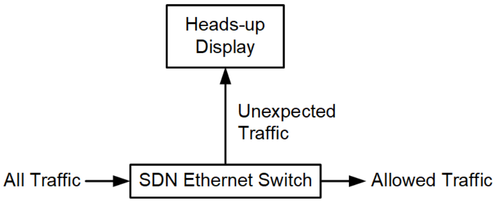

Fig. 7. SDN Redirects Unexpected Traffic to a Heads-up Display

SDN provides faster network recovery times than Rapid Spanning Tree Protocol (RSTP) or equivalent proprietary techniques. The authors have found RSTP recovery times to exceed the timing requirements for critical microgrid protection and control systems. During this time, network storms are common because the traditional Ethernet switch sends all traffic out of all ports during reconfiguration. SDN technology, under the exact same network failure scenario, was found to have less than 0.1 ms failover times, no loss of traffic, and no network storms.

In the 2017 worldwide microgrid shootout sponsored by the Department of Energy (DOE) National Renewable Energy Laboratory (NREL) [1], the NREL cyber red team was not able to gain entrance to an SDN network. This has been verified multiple times by DoD attack teams. SDN underlayment technology is designed to obsolete Ethernet network attack toolkits.

X. Learn-and-Lock Networks

Learn-and-lock SDN technology was adapted for MIL-STD-TMS networks. This allows rapid network adoption and flow control configuration without requiring intimate knowledge of Ethernet.

The procedure to perform learn-and-lock SDN configuration is as follows:

1. A physical key is inserted into each SRC, MC, and DIST box. This resets SDN Ethernet switch configurations and enables remote configuration of the SDN master controller.
2. The SDN master controller is enabled, and passwords are entered.
3. The SDN master controller adopts SDN switches, learns the network connections, and configures flows that the user sequentially accepts.
4. Physical keys are removed, locking configurations in switches.
5. The SDN master controller is shut off.

XI. Campus Microgrids

Campus microgrids benefit from the MIL-STD-TMS communication, SDN security, and microgrid control solution. Example use cases are university campuses, small distributed industrial campuses, military bases (garrisons), and more. This variant is a fixed campus power system of interconnected DERs, scaling to many hundreds of interoperable reciprocating and turbine gensets, battery-backed inverters, and intermittent (renewable) inverter-based power sources. Campus MIL-STD-TMS designs provide the improved resilience, reduced fuel usage, cybersecurity, simplicity, power quality improvements, and easy scaling of mobile microgrids.

Campus systems are slightly different from the mobile solution in that they are designed to retrofit existing onsite backup power gensets and switchgear to quickly convert an existing facility into a microgrid. For example, Fig. 8 shows several alternatives to the conventional automatic transfer switch (ATS) methods used for gensets worldwide.

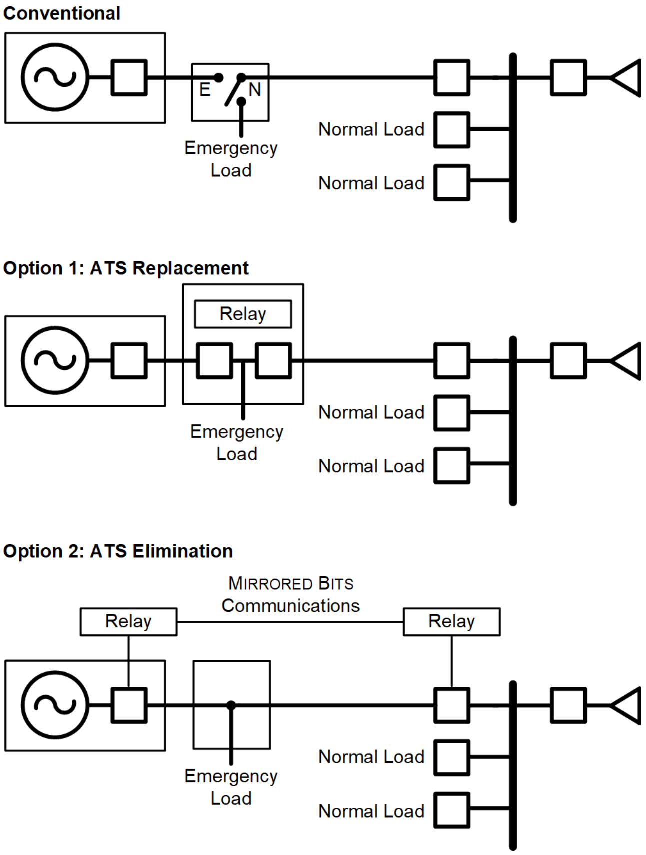

Fig. 8. Converting Emergency Diesel Genset With ATS to Microgrid

In Option 1, the ATS is replaced by a new panel that contains one multifunction protective relay and two controllable circuit breakers. In Option 2, the ATS is eliminated and existing circuit breakers at the genset and the switchgear are controlled by two intelligent multifunction relays. In both cases, a site genset can be used to backfeed a microgrid.

In this solution, the base is isolated from a bulk electric power system (host nation country) by a multifunction relay and circuit breaker at the point of common coupling (PCC) with the bulk electric power system. The PCC relay provides seamless islanding and compliance with IEEE 2030.7, IEEE 2030.8, and IEEE 1547 [8] [9] [10].

XII. Parris Island Microgrid

The U.S. Marine Corps (USMC) Recruit Depot Parris Island microgrid project in South Carolina was a collaborative project between the USMC, Engineering Procurement Construction (EPC), and a protective relay manufacturer. In addition to substantial site upgrades, the facility proved interoperability between PV, batteries, turbines, and reciprocating diesel gensets. Parris Island uses the MC control algorithms integrated into the MIL-STD-TMS prototype.

The plot in Fig. 9 shows a day of Parris Island microgrid operation. Green and purple represent the megawatt output of two PV fields, yellow is the megawatt charge/discharge of a battery-backed inverter (energy storage), red is the state of charge of the battery, blue is the output from a site turbine, and orange is the utility import megawatts. The battery system stores excess energy from the PV output, lessening the evening load. The turbine stays on baseload unless a major upset occurs. The PV, turbine, and battery system work together to reduce utility charges.

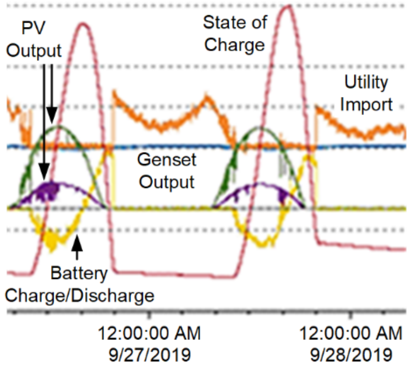

Fig. 9. Parris Island Integrated DER Results

XIII. Resilient Procurement

Interoperability is not possible with the gensets being procured today. Procurement teams are advised to specify MIL-STD-TMS gateways and control configurations to ensure interoperability. This allows procurement teams much greater negotiating power in the purchase of costly new gensets.

Older equipment can be retrofitted to be MIL-STD-TMS-compliant. Some older gensets like the TQG technology procured by the DoD can be modified in less than 30 minutes to comply with the MIL-STD-TMS standard. Commercial gensets usually take 8 to 16 hours of wiring and installation to convert to MIL-STD-TMS technology.

Incremental procurement means being able to slowly retrofit one building, one ATS, and one generator at a time to convert a campus to a microgrid. Gensets and ATS gear can be retrofitted to MIL-STD-TMS one at a time; usually, they can be retrofitted with a single one-day outage. This process allows a crew to economically scale up a facility one generator at a time, minimizes technology adoption risks, and allows the purchase of upgrades in small, affordable increments.

The Parris Island microgrid project used resilient procurement methods similar to those practiced by the oil and gas industry and utility power systems for decades. The USMC specified that best-in-class electronics (the brains of the power system) be embedded into third-party, low-cost switchgear, transformers, reclosers, distribution gear, gensets, IBRs, and GSBs. For the USMC, this means that mission-critical electronics, software, networking equipment, inverters, controllers, and protective relays are sourced from trusted U.S. manufacturers. Switchgear, transformers, cables, engines, and generators (also known as commoditized assets comprised of copper and steel) are procured based on financial considerations. Procurement (acquisition) teams are advised to specify MIL-STD-TMS suppliers with a proven supply chain security program. Best practices for such a program are described in the appendix.

XIV. Proven Technology

The prototype project was the merger of the MIL-STD-TMS standard and a long-standing microgrid control and protection system. Each of the points in Fig. 10 represents a completed microgrid project accomplished by a 50-person engineering team.

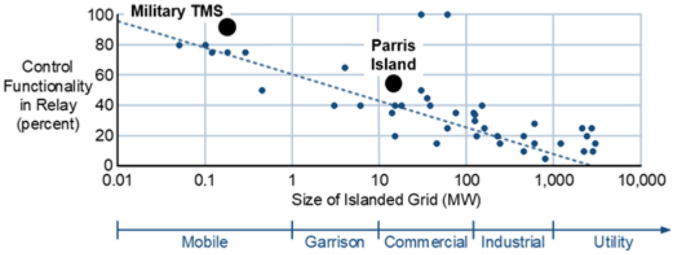

Fig. 10. Completed Microgrid Projects

The x-axis is the amount of onsite generation on each microgrid. The y-axis is the percent of control functionality performed in protective relays. One hundred percent means all functions are performed in the relays; zero percent means all functions are performed in a centralized automation controller.

This scatter plot shows that smaller power systems are predominately controlled by protective relays. Larger power systems involving more relays require a comprehensive central MC [11] [12] [13].

The authors believe that most microgrids less than 10 MW can benefit from the MIL-STD-TMS technology.

XV. Conclusion

The MIL-STD-TMS prototype project has shown superior resilience and, hence, greater reliability and better power quality for the end user. SDN systems provide superior cybersecurity, intrusion detection, and faster network healing times.

Procurement teams can achieve cost reduction with the interoperable nature of the MIL-STD-TMS standard. Teams are cautioned to vet suppliers with established and proven supply chains.

XVI. Appendix: Security Best Practices

A. Security From the Ground Up

Multifunction protective relays are the primary control, protection, and automation devices used in the transmission, generation, and distribution substations of the U.S. bulk electric grid. U.S. utilities strongly prefer relays that are invented, researched, developed, manufactured, assembled, tested, and supported in the U.S. [14] over those from other countries. Manufacturers must have a culture of cybersecurity rooted in the concepts of least privilege, need-to-know, and defense-in-depth. Access to manufacturing facilities must be tightly controlled, and 24/7 security must monitor all buildings and access.

The design of multifunction relay hardware, firmware, and supporting software must be subjected to a rigorous peer-review process to ensure the devices correctly satisfy end user needs, do not include unnecessary features, and are as simple as possible to use.

A thorough device testing regimen is exhaustive. Threat model analysis is used to review full system architecture. All source code must be reviewed for correctness of function and implementation, then subjected to automated and manual testing designed to detect errors that could result in malfunction or vulnerability. Automated code inspection is used to augment peer code reviews. Version control ensures that all source code, specification documents, and drawings are maintained in a secure, access-controlled repository.

Unit testing ensures that all code modules are exercised and satisfy the design specification. Functional tests are performed on the device or system by automated tools and human testers to verify that units perform as expected on a function-by-function basis. Negative testing (e.g., fuzz testing) is used to prove that the system does not misoperate. For example, deliberately distorted data are sent to external interfaces, attempting to induce an error condition. Vulnerability scanning tools are also used to test mission-critical devices. Validation testing ensures that the device functions as intended in realistic use cases.

Software is digitally signed using an extended validation code-signing certificate with a key securely held in a hardware security module. Firmware can be authenticated by comparison with a reference hash value available from the manufacturer.

Multifunction relays and automation controllers are architecturally different. Relays operate with an embedded environment that includes safeguards to detect alteration of programming and prevent malware infection or other corruption. Automation controllers use an embedded operating system that whitelists applications at the kernel level to prevent alteration.

When a manufacturer identifies a defect in a device that could cause a misoperation, failure, or vulnerability, end users should be quickly notified with a service bulletin that describes the problem, risk to the user, and mitigation steps.

B. Supply Chain Security

Manufacturers of mission-critical electronics must embed supply chain security in their principles of operation. Suppliers must be viewed as part of the manufacturing process and educated in the mission, values, and processes of a manufacturer.

An essential step in ensuring supply chain security (cyber and otherwise) and quality is to form lasting, collaborative relationships with each supplier. Manufacturers should clearly communicate their expectations, while at the same time cultivating a commitment to the success of the supplier. Forming strategic relationships results in wins for all parties. A successful supplier selection process requires input from R&D, quality, purchasing, and security teams, ensuring that every supplier and component is vetted from different perspectives.

Manufacturers should use a trust-but-verify approach to conduct onsite audits of suppliers to verify that security safeguards and quality processes conform to their own understanding and expectations, and to better understand risks to supplier business models. Supplier assessment and monitoring is continuous and extends to cybersecurity and financial health.

It is essential to maintain a detailed record of every device manufactured. Recording where each device is installed allows a manufacturer to rapidly notify users about potential quality or security concerns. Device serial number, firmware, and subassemblies must be tracked. Manufacturers must know who built it, when it was built, which plant built it, what assembly lines it was built on, and what test station was used. Manufacturers must track who bought it, the identity of the end user, how it was shipped, and who is supporting the device.

A warranty program can be used to improve supplier quality. A long warranty period guaranteeing repair or replacement for the life of a device provides an incentive for users to return devices as they fail. Returned devices are analyzed by experts until root cause is identified, allowing R&D and manufacturing teams to constantly improve designs.

Manufacturers must ensure every critical subcomponent can be sourced from at least two vetted suppliers. Components should be obtained from U.S. suppliers whenever feasible. Suppliers subject to control by potential geopolitical adversaries must be avoided. All software must be created internally, providing a quality control advantage along with the ability to make rapid fixes and enhancements. Vertical integration enhances oversight and custody of devices, from R&D design through the complete manufacturing process. This control mitigates the chances of malicious code or components making their way into mission-critical devices.

Suppliers must autonomously and continuously scan the threat landscape outside their own company. A devoted 24/7 security operations center, in concert with a business intelligence unit, works to enhance security. These teams must scour an array of public and private threat and other intelligence streams to detect cybersecurity or physical threats to supply chains and internal infrastructure.

XVII. Acknowledgment

The authors acknowledge the U.S. Army Corps of Engineers Construction Engineering Research Laboratory (CERL), the U.S. Army Combat Capabilities Development Command (C5ISR), and MIT Lincoln Laboratory for their close cooperation.

XVIII. References

[1] NREL, “Unique Procurement Process Expands Microgrid Research Capabilities at the ESIF,” February 2018. Available: https://www.nrel.gov/news/program/2018/procurement-expands-microgrid-research-capabilities-at-esif.html.

[2] Navigant Research, “Navigant Research Leaderboard: Microgrid Controls – Assessment of Strategy and Execution for 15 Microgrid Controller Vendors,” 2018. Available: https://www.navigantresearch.com/reports/navigant-research-leaderboard-microgrid-controls.

[3] MIT Lincoln Laboratory, “Ten Lincoln Laboratory Technologies Earn 2019 R&D 100 Awards,” November 2019. Available: https://www.ll.mit.edu/news/ten-lincoln-laboratory-technologies-earn-2019-rd-100-awards.

[4] S. Manson and D. Anderson, “Practical Cybersecurity for Protection and Control System Communications Networks,” proceedings of the 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, AB, Canada, September 2017.

[5] Department of Defense Interface Standard MIL-STD-TMS, Tactical Microgrid Standard, February 2017.

[6] S. Manson, B. Kennedy, and M. Checksfield, “Solving Turbine Governor Instability at Low-Load Conditions,” proceedings of the 2015 IEEE Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

[7] North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. Available: nerc.com.

[8] IEEE 2030.7, IEEE Standard for the Specification of Microgrid Controllers.

[9] IEEE 2030.8, IEEE Standard for the Testing of Microgrid Controllers.

[10] IEEE 1547, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power System Interfaces.

[11] K. G. Ravikumar, S. K. Raghupathula, and S. Manson, “Complete Power Management System for an Industrial Refinery,” proceedings of the 2015 IEEE Petroleum and Chemical Industry Technical Conference, Houston, TX, October 2015.

[12] E. Roy Hamilton, J. Undrill, P. S. Hamer, and S. Manson, “Considerations for Generation in an Islanded Operation,” *IEEE Transactions on Industry Applications*, Vol. 46, Issue 6, Nov.-Dec. 2010, pp. 2289–2298.

[13] S. Manson, K. G. Ravikumar, and S. K. Raghupathula, “Microgrid Systems: Design, Control Functions, Modeling, and Field Experience,” proceedings of the 2018 Grid of the Future Symposium, Reston, VA, October 2018.

[14] Newton-Evans, “Worldwide Study of the Protective Relay Marketplace in Electric Utilities: 2019-2022.” Available: newton-evans.com.

XIX. Biographies

Brandon Marcum received his BS in computer engineering from Washington State University. He is presently a Project Engineer I specializing in automation at Schweitzer Engineering Laboratories, Inc. He previously served as an explosive ordinance disposal (EOD) specialist in the Washington Army National Guard and as an application designer at Digilent, Inc., a subsidiary of National Instruments.

Ellery Blood, Ph.D., received both an MS and PhD in electrical and computer engineering from Carnegie Mellon University, an MS degree in mechanical engineering from the Naval Postgraduate School, and a BS degree in computer and systems engineering from Rensselaer Polytechnic Institute. He is presently a senior research engineer at Schweitzer Engineering Laboratories, Inc. (SEL), where he provides strategic support of synchrophasor and event analysis software products as well as research into wide-area monitoring and control, areas in which he holds four patents. Prior to SEL, he taught systems engineering as an assistant professor at the U.S. Naval Academy and is an active Naval Reservist supporting the Office of Naval Research.

Jason Dearien received his BS from the University of Idaho in 1993. After graduation, he was a founding member of a small startup software contracting business. Later, he was involved in ASIC development at a fabless semiconductor company, working on compression and error correction technologies. In his 18 years at Schweitzer Engineering Laboratories, Inc., he has led various product development projects and is presently a principal engineer in the R&D communications department, focusing on network communications with SDN.

Scott Manson received his MS in electrical engineering from the University of Wisconsin–Madison and his BS in electrical engineering from Washington State University. Scott is presently the engineering services technology director at Schweitzer Engineering Laboratories, Inc. In this role, he provides consulting services on control and protection systems worldwide. Scott is a registered professional engineer in 5 states and holds 11 patents.