Microgrid Cybersecurity: Protecting and Building the Grid of the Future

MICROGRID KNOWLEDGE

Why We Need Microgrid Cybersecurity: The Threat is Real

Superstorm Sandy launched a wave of microgrid advocacy by revealing how easily wind and water could crush a major metropolitan power grid. Five years later, North America saw similar destruction with Hurricanes Harvey, Irma, and Maria. As devastating as these events were, none compare to the threat of a major cyber attack on the American electrical utility grid.

This new threat is worse because it often comes with less warning than acts of nature, offering little time to prepare. It carries the potential to take down larger swaths of the electricity system for longer periods of time because of the risk of cascading failures. Security experts describe a cyber attack against the power grid as a form of asymmetrical warfare, the equivalent of destroying a society by cutting off delivery of food and water, healthcare, commerce, and communications. Contemporary economies run on electricity. Without electricity, they seize up.

"They can't beat us in the air; they can't beat us on the sea or ground. So they are going to go after us where we are vulnerable, and that is in protection of our infrastructure," William Anderson, a former Air Force assistant secretary and now a defense consultant who specializes in energy, told Microgrid Knowledge.

As in all warfare, prevention is the first strategy. But beyond prevention, we must prepare for the worst. This means creating systems for rapid response, shelter for affected civilians, and protection of critical assets should hackers disrupt our power systems at the generation, distribution, or transmission levels.

Microgrids are increasingly part of that recovery plan because they can provide an electrified oasis during a power outage. Microgrids can power a community's vital services – law enforcement; fire protection; medical care; distribution of water, food, and fuel; and communications. Some include a community center within their footprint, a shelter where the vulnerable can congregate to charge phones and connect with loved ones.

These islands of power are created by using utility-disconnectable and standalone power sources, such as backup generators, spot generation, renewables, and batteries to power out-of-service utility lines. Microgrids take over power distribution during grid outages or voltage instability, or they can be set up as temporary or mobile power distribution in emergency scenarios.

Microgrid cybersecurity coming, but quickly enough?

Communities, hospitals, utilities, the military, and others have started building microgrids, but not fast enough. If a massive cyber attack knocked out a large section of the grid today, restoration likely would take months or years. Navigant Research has identified 1,842 microgrid projects worldwide, many of which would protect critical services during grid outages, representing nearly 20 gigawatts (GW) of power production. To put that in perspective, the U.S. power grid generates 1,000 GW to serve our needs; New York City, alone consumes 10 GW. We clearly must pursue cybersecure microgrids more quickly.

Meanwhile, one incident after another underscores the urgency of the cybersecurity risk. In December 2015, an attack in the Ukraine highlighted the vulnerability of power grids, not just in that country but across the developed world. The Ukrainian grid was again attacked in December 2016. This time only a single substation was compromised. But the event was worrisome because attackers used a sophisticated cyber weapon nicknamed "Crash Override" that can easily be modified to attack a wide range of industrial facilities worldwide. One month later, the Ukraine experienced from another cyber attack, this one causing 225,000 people to lose power for several days. Three utilities were hacked, possibly by a hostile state or pro-government hacker agencies, such as "Sandworm" or "Electrum". The outages were caused by coordinated, remote cyber intrusions, "probably following extensive reconnaissance of the victim networks," as reported by the U.S. Department of Homeland Security.

More recently, we've seen that it's not just computer code that makes infrastructure vulnerable. It turns out that hackers may have a much wider playing field. For example, in Dallas, Texas, the city's 156 outdoor tornado sirens simultaneously and unexpectedly went off in April when hackers manipulated tonal codes, not computer code, in a 10-year-old radio system. For 90 minutes – until operators manually switched them all off – the sirens blared an unmistakable alarm illuminating the exposed state of our critical infrastructure.

It also has become clear that cyberterrorists can rely on human behavior to inadvertently aid and abet their destructive intentions. The "WannaCry" ransomware attack, which affected 200,000 systems in 150 nations on May 12, 2017, occurred largely because computer users failed to follow proper computer hygiene practices, say security experts. By neglecting to update common Microsoft software with regularly offered security patches, they left the door open to malware.

But cybersecurity solutions aren't always as simple as installing software updates. Utility operators and security experts worry about the possibility of hidden malicious code in the control systems managing the North American power grid. This complex electric network includes equipment from many parts of the world; the fear is that some of these components could contain ticking time bombs in the form of preset viruses or malware from hostile nations that are set to disrupt the grid at a later date.

Given the urgency of the situation, Microgrid Knowledge, in partnership with S&C Electric Company, has prepared this guide, "Microgrid Cybersecurity: Protecting and Building the Grid of the Future." We offer this guide for download, free of charge, and encourage readers to circulate the report link widely. In this guide, we explain how microgrids in general, and cybersecure microgrids in particular, offer protection during a cyber attack on our electric infrastructure.

Three examples of microgrid cybersecurity

Distributed architecture provides the core of microgrid cybersecurity, offering three forms of protection.

First, distributed assets are more difficult for cyber-terrorists to attack en masse than are centralized systems with a single point of failure -- a characteristic of the U.S. grid. Microgrids use distributed energy resources -- many different points of power generation – and are inherently segmented from the bulk grid. They can be further segmented into sub-grids that can operate autonomously or in concert and be isolated from each other and the bulk grid in case of cyber attack. To bring down a microgrid, attackers must discover and compromise multiple unconnected points. There is no single vulnerable bull's eye.

Second, microgrids offer inherent redundancies. Should one source of generation fail, another can take its place. For example, if solar panel management software is attacked, the microgrid could still generate electricity from its other sources, such as energy storage or combined heat and power.

Third – and central to this report – a new, advanced breed of microgrid, the cybersecure microgrid, elevates cyber protection and energy resiliency to a new level. It does so by incorporating the distributed asset concept into the software intelligence that manages the microgrid. Rather than having a single master control system, or "brain," the cybersecure microgrid has several. If bad actors penetrate the

microgrid and disable a controller, another controller can automatically step in to manage the system. This affords operators of cybersecure microgrids time to isolate the breach without disrupting the flow of power to the critical buildings and equipment the microgrid serves.

To fully appreciate the value of microgrid cybersecurity, it's necessary to first understand the centralized architecture upon which the larger grid has been built for a century. This makes clear why fear exists that a strategic cyber attack could topple the grid, especially as we enter the age of the "Internet of things," explained in the next chapter.

Chapter 2: Grid Cyber Attacks: How is Our Electric System Vulnerable?

The North American electric power grid has been described as a single enormous machine, one of the largest in the world, with about 1,000 GW of generation and 200,000 miles of transmission lines.

It is a single machine in the sense that all the parts have to work together. If there is a fault within any of those semi-autonomous grids, failures can ripple through the rest of the system. The system is built to be resilient and ride through faults – up to a point.

The grid's vulnerability was demonstrated on a large scale in 2003 when an overloaded transmission line sagged and touched a tree south of Cleveland, Ohio. Within minutes, a mix of equipment failure and human error left 50 million people without electricity and caused an estimated $6 billion in economic damage.

In the wake of that blackout, reliability rules were strengthened, and the grid is now in a better position to avoid or withstand a repeat of the 2003 event. But unfortunately, the range of threats has increased since then. Blackouts from cyber attacks raise the stakes, with the potential to cause even greater debilitation than storms or accidents.

Concern about grid security has grown with reports of cyber intrusions into commercial computer networks across a wide range of industries. There have been several high-profile attacks in recent years, including the hijacking of sensitive data from Sony Pictures in 2014, the breaching of digital defenses at J.C. Penney and Yahoo!, and the successful grid cyber attacks in the Ukraine in 2015 and again in 2016 and 2017. To date, the U.S. electric grid has not been disrupted by hackers, but that is not for lack of attempts. Many consider it only a matter of time until such an event.

In December 2016, The *Wall Street Journal* reported that American officials believe a 2014 cyber attack against the U.S. energy industry resulted in at least 17 companies being penetrated, including four electric utilities. A study by Cisco found that 70 percent of utility security professionals reported they have experienced at least one security breach.

Grid cyberattacks no longer theoretical concern

In an April 2017 article, the Council on Foreign Relations said that grid cyber attacks are no longer just a theoretical concern, and that rapid digitalization, low investment in cybersecurity, and a weak regulatory regime make the country even more vulnerable.

As vulnerable as the grid is in its current state, it is becoming more susceptible to attack as we expand our energy-related network with smarter homes and cities that incorporate distributed energy, electric vehicles, and Internet-of-Things (IoT) appliances that include everything from laptops and cameras to cell phones, street lights, and thumb drives. A world of interconnected devices makes life more convenient, but these devices all rely on a rapidly growing number of interconnected digital interfaces. Those interfaces offer potential entry points for cyber attacks of all kinds.

This growing threat has captured the attention of the utility industry. The Edison Electric Institute (EEI), a utility-funded advocacy group, has launched a series of initiatives aimed at safeguarding the grid from cyber threats and is partnering with federal agencies to improve the industry's resilience to cyber attacks. EEI also is collaborating with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corp. (NERC), and federal intelligence and law-enforcement agencies to strengthen grid capabilities.

The U.S. Department of Energy (DOE) also is providing $15 million in funding to support the efforts of the American Public Power Association and the National Rural Electric Cooperative Association (NRECA), two advocacy groups that represent municipal, cooperative, and other public power utilities. The associations are using the funds to bolster the cybersecurity of their members, many of which are small, locally run utilities without adequate resources to manage cyber threats on their own.

The military prepares for grid cyber attacks with microgrids

There is acute awareness within the U.S. military of threats posed by grid cyber attacks. This has led military leaders to embrace microgrids as a way to reduce dependency on the utility grid for critical missions and on fossil fuels overall.

But the energy resiliency objectives of those microgrids would be undermined if the microgrids inadvertently opened those installations to cyber attacks. So the Department of Defense (DoD) has set strict security requirements for military facility systems, including microgrids; they must be much less vulnerable to cyber attack than the utility grid.

With those objectives in mind, in 2008 the DoD launched its Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) program. The program was designed to bolster the cybersecurity and energy efficiency of U.S. military installations by deploying advanced microgrids, and to transfer that knowledge to non-military critical infrastructure.

SPIDERS included three project phases demonstrating enhanced mission assurance at military installations, integrating smart grid technologies, distributed and renewable generation, and energy storage with a cybersecure microgrid architecture. To date, the DoD has already deployed more than a dozen microgrids in locations that include Joint Base Pearl Harbor-Hickam in Hawaii, Camp Pendleton in California, Fort Carson in Colorado, and Fort Belvoir in Virginia.

The microgrid at Camp Smith in Hawaii, which provides power for full base operations during an extended grid outage, offers an example of a microgrid with cyber attack defenses infused into the control system. As we'll see in the next chapter, these defenses are crucial to ensure the microgrid itself does not become a portal for cyber attack.

So how exactly does a microgrid ensure the flow of electricity during a cyber breach? Chapter 3 explains.

Chapter 3: The Cybersecurity Value of Microgrid Islanding

The value of microgrids as a cybersecurity defensive measure begins with their unique ability to operate in two different modes: connected to the electric grid or islanded from it as a self-contained system and independent power provider.

In most instances, a microgrid operates in grid-connected mode and its assets contribute to the strength of the overall grid. But if a fault in the utility grid causes a loss of power, a microgrid can disconnect from the grid and independently serve its customers via its on-site generation resources. This islanding ability makes microgrids very attractive for critical operations, such as emergency first responders, military operations, hospitals, airports, and water treatment facilities.

Microgrid islanding would come into play if cyber terrorists crippled the electric grid and caused a major power failure. Sensing the disruption, software technology would isolate the microgrid's local generation sources and loads from the trouble. Those local power sources within the microgrid's footprint would activate and supply electricity to the microgrid's customers. Often these power sources are some combination of renewable energy, batteries, combined heat and power, or emergency generators.

We have no examples of microgrid islanding occurring in North America during a cyberattack because – fortunately – the grid has never been crippled by a hack. But microgrids have demonstrated the value of islanding during other major calamities.

For example, in 2012 when Hurricane Sandy came ashore in New Jersey and ripped up the East Coast, 8 million electric customers lost power, but the lights stayed on at Princeton University because of the school's microgrid islanded.

The microgrid operated until power was restored to the main grid – a day and a half later – providing necessary electric power and heating needs. Because of the microgrid, Princeton became a refuge where police, firefighters, paramedics, and other emergency services workers could charge phones and equipment. Local residents were also invited to warm up, recharge phones and use the wireless Internet service at a hospitality center the university made available.

It's not only hurricanes and cyberattacks that threaten the electric grid. Many power outages are caused by more common thunderstorms, ice storms, and scheduled brownouts. Individually and in aggregate, these disruptions can significantly affect a grid customer. In one example, a microgrid in California powered the community of Borrego Springs for nine hours after a transmission line was damaged by lightning. Here again, microgrid islanding proved itself as a way to ensure power supply.

Nested microgrids being developed in Chicago, New York, and Pittsburgh, among other locations

These are some examples of microgrids exhibiting the ability to provide backup power, resiliency, and redundancy. In these cases, the microgrids stand alone. Offering even greater promise are microgrids that are linked together or 'nested' with other nearby microgrids.

Still a nascent approach – but one that offers superior opportunity for resiliency (the main goal of cybersecurity) -- nested microgrids are electrically interconnected so that power can be interchanged. They can share and switch between power sources to ensure optimal efficiency. For example, a solar-powered microgrid might pull the load on a sunny day while a nearby microgrid with a combined heat and power plant would take over on a stormy day.

Resiliency, a benefit often associated with microgrids, describes the ability to avert power failure or restore service quickly after a disaster.

In Chicago, Commonwealth Edison has proposed a microgrid in the Bronzeville neighborhood. When completed, it will provide resiliency and security for local residents, as well as for the hospital and police and fire headquarters. The Bronzeville microgrid would also nest with an existing microgrid at the Illinois Institute of Technology that has been in operation since 2013.

In New York, the town of New Paltz has proposed a $12 million modular microgrid that would comprise 10 independent zones or nodes, with each having its own energy resources to serve one or more critical facilities. In all, the New Paltz nested microgrid would serve 25 critical facilities.

It's clear that microgrids offer protection during a cyberattack because of their islanding ability, in essence creating a gap between the electrical systems under attack and the microgrids' own assets. But microgrids are also built upon software and data communications, and if microgrids are intended to protect against the risk of cyberattacks on the utility grid, it's essential that the microgrid itself is protected from those attacks.

Designing a truly cybersecure microgrid

In this respect, it is important to recognize that the very elements that make a microgrid resilient can also make it vulnerable. Microgrids often include distributed energy resources (DERs), such as solar panels, that require inverters to send power to consumers or the grid. One of the key enabling features of a microgrid, in fact, is the two-way data communications among the microgrid participants and with the grid to which it is connected.

Those control and communication functions can create vulnerabilities by increasing the microgrid's attack surface -- in essence presenting portals for cyber intrusions – and undermining the very resiliency that a microgrid is designed to provide.

A hacked microgrid could even be a portal that opens the grid itself to cyber attacks. At the least, building a microgrid that is not cybersecure would be a poor investment. At the worst, it could precipitate or aggravate a catastrophe.

However, it is important to underscore that a truly cybersecure microgrid overcomes these vulnerabilities. What are the microgrid design elements needed to accomplish that? That is the subject of the next chapter.

Chapter 4: How to Create a Cybersecure Microgrid and Protect the Macrogrid, Too

Cybersecurity should be a prime consideration at the outset of microgrid design. If a microgrid is being installed for resilience, it doesn't make sense for it to increase the vulnerability of its customers or the main grid.

In comparison with the centralized model widely used for primary power grids, microgrids use a distributed architecture with multiple systems that communicate with each other. This distributed architecture innately includes power redundancy and resiliency. The microgrid controls also provide a basic level of security because they are distributed, with no single point of failure that could result in the loss of the entire system. As discussed, advanced microgrids are able to compensate for loss of one or more control points.

An advanced microgrid design includes switchgear, generation sources, energy storage, and other equipment that communicates seamlessly using a supervisory software control system. The controller is the brain and nervous system of a microgrid. Its software gathers a wealth of data from microgrid participants and makes and communicates operational and safety decisions for the microgrid and communicates instructions to its connected assets. The controller also coordinates and manages its resources and relationship with the central grid to operate at maximum efficiency at all times.

While a microgrid's diverse resources increase its resilience, the complex control and communication systems required to coordinate the equipment also have the potential to increase its vulnerability – if proper cybersecurity is not implemented. For true resilience, cybersecurity protections must be built into the microgrid from its inception.

Resiliency through cybersecurity

"True microgrid cybersecurity requires that there is no single point of failure in the system, as there is in centralized architecture," said Erik Svanholm, CEO of IPERC, a subsidiary of S&C Electric, which offers a cybersecure microgrid controller, the GridMaster® Microgrid Control System. "Resiliency is provided by failover of the "master" from one distributed controller to another. Putting intelligence and processing power at the endpoints allows localized communications and control which means a smaller network footprint that can be secured and monitored."

Svanholm describes a "Defense in Depth" (DiD) approach, which calls for the use of a large number of security countermeasures, all working together in a layered, coherent way to protect against every imaginable form of cyberattack while allowing legitimate microgrid communications and data-handling activity to proceed unimpeded.

The first line of defense occurs at the perimeter of the microgrid, with the objective of keeping attackers out altogether. Here, a useful start might be something simple, such as sensors that log and alert if microgrid assets have been physically tampered with. Firewalls and intrusion-detection systems also seek to keep intruders out and identify attempts (and successes) to penetrate the network perimeter. Hardware hardening, in the form of removing unnecessary software and services, and disabling unneeded communications and data ports (particularly USB ports) on the computers hosting the control software, adds another, host-based layer of "perimeter" security.

This is where security stops for most legacy industrial control systems and many contemporary microgrid control systems. If attackers penetrate the network perimeter shell, they gain access to easily legible, exposed data streams and archives, and can design and deploy devastating malicious code.

Standard energy industry protocols were not written with cybersecurity in mind, so the vast majority of them send data in the clear. Many more layers of defense must be built into the system so all is not lost if the network perimeter is breached. And if those security measures weren't included in the original control code's DNA, it is almost impossible to add them later without significant reengineering of software and testing of interoperability with microgrid participants, including utility systems. This gives operators of large, expensive industrial control systems an unpleasant choice: They can apply modern external protections to exposed older software and hope they are never breached – a low-cost, high-risk solution -- or replace the entire control system with a newer, much more secure product.

In contrast, attackers who succeed in penetrating sophisticated control systems using a DiD approach are met with a variety of integrated defenses to keep them from doing harm even while they are inside. Operating systems, software, and firmware are hardened by disabling or removing code, protocols, and services that aren't specifically required to operate the microgrid. Stored data and communications among microgrid components are encrypted so intruders can't read, intercept, or manipulate the control traffic, configuration files, and archives. Whitelisting is a security protocol where only pre-approved devices are allowed system access. And even if a new device appears on a DiD-protected microgrid network and passes the whitelist test, the software still executes a series of authentication exercises to validate that any device trying to communicate on the microgrid is a legitimate participant.

A cybersecure microgrid also enables monitoring of internal communications and system processes to identify abnormal events during operations. This includes real-time alerts and the creation of security audit logs for operator awareness of the system's security posture, its level of availability, and potential anomalies, all without affecting the microgrid's operation. Those alerts and audit logs can also be incorporated into a utility's Security Information and Event Management (SIEM) system.

Microgrid connections to the utility grid require additional secure gateways, or de-militarized zones (DMZs), and firewalls dedicated to securing that connection point. Where feasible, unidirectional gateways (e.g., data diodes) can be used where bi-directional communications aren't necessary. Direct connections between a microgrid and the utility or to the Internet should never be used.

No shortcut to cybersecurity

All of these methods are just examples of dozens of countermeasures used in DiD-based control systems to establish strong cybersecurity for advanced microgrids. Most of the defensive approaches used are well-known in security circles and are widely used for many applications. But deploying so many protections simultaneously, and coherently, so the system is all but airtight except for the precise data movements needed for the microgrid to function, is extremely difficult to achieve and takes years of software and hardware development. There is no shortcut to effective cybersecurity.

"A significant challenge for utilities is that many do not have budget lines specifically for cybersecurity. So they naturally tend toward the pragmatic approach 'if it ain't broke, don't fix it,'" said David Chiesa, senior director of global business development at S&C Electric Company. "They are managing systems that are intended to remain in place for decades, not years. So they require a cyber solution that can be integrated into a new system, yet be interoperable with legacy assets."

It's important for utilities – and others – to be aware that the business case differs for cybersecurity, and for microgrids themselves, from the standard energy infrastructure they procure.

"The cost of ensuring cybersecurity should be viewed as a form of insurance. Just as microgrids protect against disruptions to the utility grid, cybersecurity is insurance for the safe, secure, and reliable operation of microgrids," Chiesa said. "Having robust cybersecurity systems will pave the way for the proliferation of microgrids that enhance and strengthen the grid in the face of hazards, both natural and man-made."

Today's cybersecure microgrids emerged out of years of work by the military. In the next chapter, we interview one of the key figures behind their development.

Chapter 5: Microgrid Cybersecurity: Fighting Asymmetrical Warfare

It's common to find seeds of advanced technology within work by the military. Microgrid cybersecurity is no exception, as we see in this interview with Darrell Massie, who holds a doctorate in civil engineering and is the founder and chief technology officer of Intelligent Power & Energy Research Corporation (IPERC), an S&C Electric Company subsidiary.

The threat of cyberattacks targeting the U.S. electric grid is rising, and hackers have become increasingly sophisticated. Historically, hackers broke into systems as a sport to show off and test their skills. But over the years they increasingly capture personal and financial information for monetary gain. More recently, foreign governments have been responsible for a growing number of cyberattacks. The *Wall Street Journal* recently reported that the malicious software that shut down power in parts of Ukraine's capital last year could be repurposed to target the U.S. grid.

"In the hands of our enemies, cyberattacks can be a crippling weapon against the United States. Cyberattacks are currently being utilized as a new form of terrorism and asymmetrical warfare," said Massie. "The Ukraine cyberattack was a spectacular display of the damage cyber attackers are able to achieve today. That attack not only focused the public's attention on how vulnerable an electric grid can be, but it also verified the grid's high value as a target."

This threat is recognized by utility executives at the highest level, but many have been understandably reluctant to air their concerns publicly. This attitude is changing as utility regulators and even the utilities themselves begin to mandate higher levels of cybersecurity. The industry also is realizing the massive disruption and financial repercussions that could result from a Ukrainian-style cyberattack on the U.S. grid. A 2015 report by insurance company Lloyd's of London estimated that if a cyberattack were to plunge the Eastern Seaboard of the U.S. into darkness, the economic impact could be as high as $1 trillion.

The Ukraine attack led to valuable lessons, according to Massie. The hacked utility publicly listed its equipment vendors, which allowed hackers to determine key specifications of its installed grid components. The hackers then hijacked common Microsoft files to gain control of the utility's industrial control systems. Once inside, they used publicly available vendor information to rewrite control software to change device settings while indicating normal status on the user interface screens utility operators were watching.

The security of distributed architecture

The Ukraine attack underscores a basic concept in cybersecurity. "An attacker goes for the easiest target. A centrally designed system can be easily overrun in an event storm," said Massie.

One of the solutions is moving to a more distributed architecture. But many existing microgrids have not done this, so they are not necessarily cybersecure, according to Massie.

"Most control systems in use today were designed long before cybersecurity was a concern and, therefore, contain no security features. The common tactic used in an attempt to secure existing control systems is to simply deploy firewalls at the system perimeter. This is the electronic equivalent to a Band-Aid," said Massie. "Every firewall can be breached. Therefore, control systems need to continue operating even with the attacker inside. We test and operate our control systems under this premise."

A cybersecure microgrid is governed not by a single central master controller, but rather by many interconnected controllers. Should one controller become compromised for any reason, it can be sequestered and another will take over its duties. There are backups to the backup.

By contrast, if a microgrid relies on a single central controller, should that one fail, the entire system is disabled.

"Almost every competing control system has a central control point. Our GridMaster controller is different in that it is distributed. If hackers knock out one controller, another takes over," Massie said.

The distributed control approach goes back to IPERC's roots. Massie served in the U.S. Army for 27 years, and one of the challenges he faced was getting power into the field in places such as Bosnia, Iran, and Iraq. Those deployed power systems faced an additional challenge in that they would be moved suddenly and even split into different locations. That started Massie down a path to figure out how those systems could be "dynamically reconfigured" so service could be restored with plug-and-play simplicity.

After years of working on the technology issues, Massie realized the answer required a fundamental rethinking of microgrid software architecture. A single central controller wouldn't work but a distributed control strategy, a kind of strength in numbers, would. Furthermore, the inherent resiliency and cybersecurity features of a distributed control system were just as attractive for permanent microgrids at installations as they were for mobile field units. Massie took that concept and made it the basis of IPERC. In 2007, recognizing the growing threat of cyberattacks, IPERC began designing and testing distributed control systems with embedded cybersecurity.

IPERC was, therefore, ready when the Department of Defense solicited bids for its three-phase microgrid cybersecurity program through its SPIDERS program. IPERC's control system was selected for all three phases of that project and the company led the design of controls, communications, and cybersecurity for the capstone phase.

Over the next five or six years of the program, IPERC further refined its cybersecure microgrid controller with the dedicated funding from the Department of Defense, Department of Energy, and Department of Homeland Security.

"We have passed every security test the DoD has thrown at our control system because we embed our cybersecure architecture from the start," Massie said.

GridMaster controller's unique military designation

IPERC's GridMaster microgrid controller is the only one on the market that has received, now twice, the military's respected "Authorization to Operate," or "ATO," which validates the security posture of the system and authorizes general ongoing use at a military facility. The ATOs were awarded after

demonstration of security implementation using the DoD Risk Management Framework (RMF) and rigorous testing by several DoD cybersecurity teams.

What lies ahead? Massie foresees future microgrid controls autonomously repairing themselves and adapting to unexpected communication or configuration changes. Only a system comprised of distributed controllers will have the capability to achieve this kind of microgrid self-healing.

As the threats to the grid heighten, cybersecure microgrids present a method to assure that electricity will continue to flow, starting with critical infrastructure such as emergency first responders, hospitals, food and water supply, and communications. It's a long road to deploy enough microgrids to provide this assurance across the country. It's time to pick up the pace.

Chapter 6

Case Study: First Cybersecure Microgrid Controller Installed by Midwestern Utility

A 1.475-MW test project is being described by a Midwestern utility and a key partner as one of the most technologically advanced utility-scale microgrids in North America. In addition to advanced controls, the microgrid includes wind, solar, natural gas generation, and energy storage.

The microgrid deployment occurs at a time of heightened worldwide concern about hacking, following a ransomware attack in May 2017 that spread across 150 nations, infecting hundreds of thousands of businesses and institutions from British hospitals to FedEx in the U.S. and car factories in France.

Microgrid 'firsts'

Besides being the first (and still only) microgrid controller to be given a DoD ATO, this is the first utility-owned microgrid to include an advanced cybersecure microgrid controller, manufactured by S&C Electric Company subsidiary, IPERC.

The microgrid achieves two additional technology "firsts," according to S&C, which handled engineering, procurement, construction, and commissioning:

1. The installation marks the first time a microgrid is serving paying customer loads on a utility distribution feeder in North America. The microgrid's generation can be islanded to serve only the local customers, or it can operate in grid-tied mode to provide ancillary services to the grid.
2. It is the only known utility-scale microgrid in the nation capable of seamlessly transitioning the power source for an entire distribution circuit from the microgrid to the grid, according to S&C's Chiesa. This prevents the normal short outages as the microgrid switches between grid-tied and islanded mode.

This microgrid also is one of the few in the world that operates at utility-scale voltages, between 4 kV and 34.5 kV, with multiple levels of control, according to the utility. The microgrid is being used by the utility to test monitoring and control methods for aggregating clean energy with advanced automation and battery storage.

Written by Microgrid Knowledge Editorial Team,
© 2017 S&C Electric Company

About S&C Electric Company

S&C, with global headquarters in Chicago, USA, is applying its heritage of innovation to address challenges facing the world's power grids and is thus shaping the future of reliable electricity delivery. The mission of employee-owned S&C is to continually develop new solutions for electricity delivery, fostering the improved efficiency and reliability required for the intelligent grid. Additional information about S&C is available at sandc.com.

Connect with us:

S&C Electric Company

October 30, 2017 © S&C Electric Company 2017, all rights reserved