White paper

Five steps to substation physical security and resiliency

Of all the infrastructure Americans rely on every day, perhaps none is more vital to our way of life than the grid system that delivers energy to our homes and businesses. In 2013, Presidential Policy Directive 21 identified 16 areas of critical infrastructure. Energy is just one of the areas identified, but none of the others could exist without the energy sector. Even agriculture would require significant relearning of ancient farming techniques to adapt to a world without a reliable supply of power from high-quality sources.

The impact of an extended outage on an economy cannot be underestimated. For insight, look no further than the cost of regional, weather-related outages such as major hurricanes.

In 2012, a Congressional Research Service study estimated the inflation-adjusted cost of weather-related outages at $25 to $70 billion annually. The highest spike came in years with heavy weather-related events like Superstorm Sandy. Thankfully, despite the severity of the event, proper planning and quick reaction kept major outages confined, and power was restored to more than 95 percent of customers within a couple of weeks.

A new threat?

As if natural disasters aren't reason enough to be concerned, a number of physical attacks on substations over the last few years has many in the industry rethinking substation resiliency.

Less than one year after a high-profile incident in California where snipers took aim at a substation's transformers, the Federal Energy Regulatory Commission (FERC) issued Directive 146, directing the North American Electric Reliability Corporation (NERC) to craft reliability standards that require utilities to address the physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. It didn't take long. Less than three months later, the North American Electric Reliability Corporation (NERC) filed a petition for the approval of reliability standard NERC CIP-014.

It took many utilities even less time to respond. According to Craig Stiegemeier, Technology Director, Transformer Remanufacturing & Engineering Services, ABB Inc., "We talk to two types of utilities when we discuss NERC CIP-014 compliance. There are those waiting for rules to be handed down and those who were already putting plans in place even before NERC CIP-014 was finalized. It's safe to say we see more of the latter than the former these days. They know the possibility of a physical attack is on the rise, but hardening their substations can also help them meet existing reliability standards."

Five steps to substation resiliency

To help customers reach their substation security and resiliency goals, ABB has launched the *Substation Physical Security and Resiliency Initiative*, which covers five strategic elements that will help utilities restore power as quickly as possible after an event that causes physical damage to a substation.

These elements include:

- **Assessment:** Assess the substation and asset vulnerability to extreme weather events, intentional criminal attacks, geomagnetic disturbances (GMD), and electromagnetic pulses (EMP).
- **Hardening:** Provide hardened transformers and power equipment against malevolent attacks and extreme environments.
- **Monitoring**: Onsite monitoring for utilities to determine power disruptions in real-time on a local, regional and national scale.
- **Rapid repair:** Quickly restore large power transformers and critical substation equipment following a major manmade or natural event.
- **Rapid replacement:** When repairs cannot be performed, rapid replacement greatly decreases the amount of time required to replace critical substation equipment and restore power to the grid.

While the attack in California and other similar events have physical security top of mind for utility executives, ABB's *Substation Physical Security and Resiliency Initiative* was conceived as a roadmap for any utility looking to develop a solid disaster preparedness, response, and recovery plan, regardless of the type of physical disaster. The process a utility goes through as they create their plan closely mirrors the five elements of the ABB initiative.

Step #1: Assess potential vulnerabilities

The first step in any good disaster plan is to assess what could happen and the vulnerabilities within the system that need to be addressed. While the NERC requirements are focused on addressing a physical attack, substations fail for other reasons as well. Most of the utilities ABB works with approach the assessment and subsequent planning from a holistic perspective that includes physical attack, natural disasters or simply age-related failures.

Whether looking at NERC CIP-014 compliance or simply developing a disaster plan, the first step is to identify the critical substations. According to NERC, a critical facility is one that if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation, or cascading failures on the Bulk-Power System.

Once these substations have been identified, the next step is to examine the vulnerabilities within each facility. Utility leaders need to ask questions such as:

- **How easy would it be for an attacker to access the substation?** Often times, this includes an assessment of the surrounding area. A substation that is isolated or where surrounding buildings or landscaping provide cover for a potential attack might require additional security measures.
- **Are there secondary systems to prevent unauthorized entry?** If an attacker were to make it past the initial barrier, e.g., a security fence, are there additional barriers to entry into any buildings housing vital equipment?

- **Where are the weak spots?** E.g., are there places where attackers would have relatively easy access to vulnerable equipment? In addition, is the facility close enough to the street or parking lot to allow attackers to disrupt communications systems without ever leaving their vehicle?
- **How would the utility know of an attack?** Are there early warning systems, or would the notification need to come from bystanders on the scene or from customers who have lost power? The earlier an attack can be detected, the faster it can be stopped and the damage mitigated.
- **Which systems could be made redundant?** From cooling systems to protection & control systems to communications, redundancy in vital systems can prevent a catastrophe.
- **What components would be hardest to replace?** The most immediate answer for most utilities would be the power transformer, but replacement of other vital components also needs to be considered. Inventorying a few of the harder to find parts, especially for older equipment, may be smart.

When the non-vital becomes vital

Modern substation monitoring and power flow management tools can help utilities avoid cascading power outages by redirecting power flow to other substations. In the initial assessment, it's also important to look at the power limits of non-critical substations to determine how much of the power requirements can be offloaded in the event of an attack. The average age of power transformers in the field is 30 to 40 years, and these non-critical substations may contain some of the oldest assets the utility has, as they are often the last to be scheduled for replacement.

Through the years, ABB has acquired the transformer business of some of the biggest names in the industry. "We have access to the design specifications of more than 70 percent of the transformers in use today," says Steigemeier. "This allows us to assess how much additional load an aging piece of equipment may be able to handle in the event of an emergency."

Step #2: Substation and equipment hardening

Once the vulnerabilities have been identified, the next step is to create a prioritized plan for addressing these vulnerabilities. Hardening can be broken down into two key categories: new designs and retrofitting of existing stations.

New designs: out of sight, out of mind

Utilities building new substations have a significant advantage – they can design their substations from the ground up to be resistant to physical attacks. "One of the best ways to protect the substation is to build it indoors," says Ulf Andersson, Director of Engineering, ABB Power Systems. "Technology innovations have allowed us to reduce the size of a substation by as much as 75 percent, and we've cut both electrical equipment exposure and noise emissions dramatically."

For utilities building large substations in populated areas, ABB is also seeing a dramatic increase in underground facilities. "We can put 98 percent of the substation volume below ground, making these facilities hard to target," says Andersson. "Not only are these substations more secure, they can also maximize space utilization in populated areas where land is at a premium."

Another way to increase grid security is to design smaller substations so that population centers are served by a larger number of them. "If you increase the number of critical substations from four to eight, it's going to be that much more difficult to launch a coordinated attack that can cripple the entire system," adds Steigemeier.

Retrofitting existing substations

It may be a challenge to build walls around an existing substation and next to impossible to move it underground, but according to Mike Eads, ABB Project Lead Engineer, you can still protect the most vulnerable components. "There are a variety of ways that a utility can retrofit an existing substation for tighter security. These include enhanced lighting systems, infrared camera systems, motion detection devices, redundant wireless communication, and physical barriers around critical equipment. Also smaller devices, such as the protection and communication devices, can be security fortified and hidden within existing control houses."

Reducing the amount of cabling in a substation also reduces risk. For example, using IEC 61850 communication protocols allows the utility to consolidate substation protection and control. "61850-8-1 GOOSE communications lets us eliminate the wiring for interbay control and breaker control/status," says Eads. "And, the 61850-9-2 Process Bus communications with modern sensor technology reduces hazardous current transformer cabling from the switch yard to the control house and reduces the substation footprint using fiber optic current sensors."

Indoor GIS substations blend architecture into the surrounding area for camouflage.

Strengthening the weakest link
While smaller vulnerabilities can be hidden, there's generally no hiding the weakest link in an existing substation – the transformers. "Transformers make attractive targets," says Steigemeier. "They're big. They're easy to hit. And they are the hardest to replace. One large transformer can cost millions of dollars and take months from design to commissioning."

Because they are such an attractive target, transformers have been the focus of debate in Congress. Bills such as H.R. 2244 propose a strategic transformer reserve to protect the grid against any number of events such as physical attack, cyber attack, weather events, etc., that could render a transformer inoperable and threaten the grid.

Emily Heitman, North American Vice President and General Manager of Commercial Operations for Medium and Large Power Transformers in North America testified before Congress at a House Energy and Commerce Subcommittee hearing saying, "Large power transformers (LPTs) carry almost 70 percent of the nation's electric power. They are essential to maintaining grid reliability. Replacement of these LPTs can take anywhere from 12 to 24 months. This could be especially disruptive during a widespread outage where multiple transformers need replacement. Quick access to spare LPTs would dramatically reduce the risk of a prolonged outage."

Another alternative would be to manufacture transformers that are less vulnerable, and ABB is designing transformers with a number of additional features that will harden them against physical attack including:
- Ballistic resistant tank walls
- Shielded accessories on the exterior of the tanks
- Use of dry composite bushings instead of porcelain oil-filled bushings
- Redundant cooling systems

Rifles seem to be a weapon of choice for attacks on substations. One of ABB's more recent innovations is AssetShield™. This ballistic protection system can be used to lessen damage to equipment

"Large power transformers carry almost 70% of the nation's electric power. They are essential to maintaining grid reliability. Quick access to spare large power transformers would dramatically reduce the risk of a prolonged outage."

- Emily Heitman, ABB Transformers

such as transformers, switchgear, circuit breakers, reclosers and capacitors by reducing the kinetic energy and spalling (fragmentation) of a bullet.

When a sniper takes aim at an oil-filled porcelain bushing, the results can be catastrophic. The bushing can explode and send porcelain shards flying 40 yards or more, potentially damaging other assets and injuring people. In addition, the conductor lead and porcelain can fall into the transformer, creating an electrical short that ignites a fire. Using solid, oil-free bushings eliminates the risk of fire and porcelain shards.

Step #3: Substation monitoring

Monitoring involves both keeping a physical eye on what's going on at the substation, as well as electronics to identify incursions or power disruptions in real time and the extent of their impact.

"Because of recent incidents, many utilities are adding measures such as security guards and entry and exit logging to their existing substations," said Andersson. "For both new and existing substations, we're also adding a number of devices including cameras, motion detectors, and fence sensors that can alert the utility to a breach. While these technologies have been around a long time, they are getting more sophisticated, and we're seeing a lot more interest in them than before."

"The key is to make these systems as invulnerable as possible," adds Eads. "Criminals will try to disable anything that might allow the authorities or the utility to determine what's happening at the substation. The more you can secure these systems, hide them, or build in redundancies, the more resilient your substation is going to be."

So much of substation operations and monitoring relies on electronic communications that it must be part of the plan as well. "Our approach isn't so much based on detecting whether the interference is malicious or unintentional, as it is about finding a way around it," says Bert Williams, Global Marketing Director at ABB Wireless.

Williams cites three ways advanced communications equipment like ABB's Tropos wireless mesh network architecture can help:
- **Self-healing technology.** When a link between active nodes becomes disrupted in ABB's wireless mesh architecture, the mesh routers identify the problem and automatically switch to an alternative path, effectively routing around the disruption.
- **Multiple-bands.** Having multiple radio bands builds in redundancy. If there is interference on one band, routers can immediately switch to another.
- **Automatic interference avoidance.** ABB's SmartChannel technology automatically scans multiple channels within the same band, analyzing interference trends and looking for the most stable, reliable channel.
- **Multi-layer security.** As with wired networks, wireless networks need to be ready for anything. Tropos Wireless Communications technology includes a multi-layer, defense-in-depth security model with login reporting, evil-twin monitoring, DoS identification, and compliance reporting and mitigation.

Step #4: Rapid repair

Thankfully, not all attacks are so damaging that they require complete replacement of equipment. For example, if an attacker were to disable a transformer's cooling systems, substation monitoring can alert the utility to

ABB, in collaboration with the Department of Homeland Security and the Electric Power Research Institute (EPRI), developed a portable recovery power transformer called RecX that can be shipped to locations around the country to restore power supply quickly.

a problem so they can reroute power and reduce the load on the compromised assets before any real damage occurs. Once power is safely rerouted, the focus turns to repairs.

There are industry-led efforts to make finding replacement parts easier and faster. Most notable is the Edison Electric Institute's SpareConnect program. This is a voluntary program in which members agree to share equipment, including bushings, fans, and auxiliary components in the event of an attack.

"The SpareConnect program is a good idea, but some of the transformer equipment is getting old. Finding an exact replacement for a part from the same model transformer is going to be a challenge for many utilities," says Rich Bocim, ABB's Vice President of Commercial Operations, Transformers. "Thankfully, ABB maintains designs for over 70 percent of the transformers in use today. Our cache of designs can help utilities find equivalent replacement parts, even for equipment that hasn't been manufactured in years."

ABB is also working to reduce the length of time it takes to complete repairs. In the case of extensive repairs, some manufacturers require the transformer to be shipped back to the factory. Although that may be less expensive than maintaining a spare transformer on site, with all the logistical issues involved in getting the transformer back to the factory, the delays can be significant. ABB's TrafoSite repair services bring the factory to the site.

Step #5: Rapid replacement

The California incident involved 17 transformers and was expensive, but repairs were completed in a matter of weeks. An attack that destroyed, instead of just crippling, vital power equipment could have a more devastating effect as it can take months to source a replacement.

As mentioned earlier, bills such as H.R. 2244 would create a stockpile of transformers that could be used in an emergency, but there is still a challenge of funding.

Edison Electric Institute has a private alternative called the Spare Transformer Equipment Program (STEP) where utility members volunteer to provide spare transformers to other members in the event of an attack. As with SpareConnect, the voluntary nature of the program may present challenges when the heat is on. And, with both H.R. 2244 and STEP, there is a problem of predicting when and where a transformer will be needed, what type of transformer will be required, and how to get it there as quickly and cost effectively as possible.

ABB is working on the challenge from another perspective by designing large power transformers that are faster to manufacture and more easily transportable. "We've taken a modular approach that overcomes transportation and dimensional limitations for transformers up to 345 kV, 400 kV, and 525 kV systems," says Stiegemeier. "These transformers provide the same level of power, but don't have the same logistical issues, such as permits, as the older, larger designs. Not only can we get them on site faster, they are easier and faster to install and commission."

"If an individual utility decides to keep redundant transformers on-hand, or if the government were to mandate stockpiling, these smaller, more mobile versions make the most sense. It will be far easier to get them to where they need to be than the older designs." In fact, Steigemeier is so bullish on the new designs that he believes the conventional design larger transformers will eventually become a thing of the past.

Time for an all-of-the-above approach

We may never know whether the California incident was a dry run for a larger coordinated attack or simply "sport" for a small band of hooligans. The perpetrators were never caught. Thanks to the work the utility had already done to make their grid resilient, the damage was limited to a short-term local power outage instead of cascading through the grid. Perhaps what we should be even more thankful for is the wake-up call incidents like these have given us to the vulnerabilities our assets face every day in the field.

Of course, physical attacks aren't the only threat to the grid. Perhaps, John R. Norris, FERC Commissioner, said it best in his concurrence to the FERC 146 directive:

"I believe that the more prudent approach is to focus on building a smarter and more agile grid, incorporating better communication and coordination, to mitigate against the multiple forms of risks that we face, including...physical and cyber threats, geomagnetic disturbances, electromagnetic pulses, and natural disasters. Such a multi-functional approach will enhance grid resiliency, which I believe is the best way to protect our grid from physical threats and vulnerabilities."

Those of us in the energy industry may be tired of the phrase "an all-of-the-above approach," but sometimes it is the best strategy. If in creating a disaster preparedness, response, and recovery plan, we end up strengthening our substations against all manner of events, it is well worth the effort.

9AAK10103A5954

Contact us

ABB Inc.
Power Grids
901 Main Campus Drive
Raleigh, NC 27606

www.abb.us