White paper

After Metcalf: Building physical grid security

The rise of cyber attack as a threat to critical infrastructure has been met with a broad response across the public and private sectors and nowhere is this more evident than in the electric power industry. Still, while much attention has been placed on the cyber threat, to date the actual impact of such incursions has been limited. The overwhelming majority of damage to utility systems, not to mention customer outages, is done in the physical world.

Major storms like Hurricane Sandy, which impact more than 10 percent of a given utility's customers, are rare. The industry term for these events is "high impact, low frequency" (HILF) but consumers may be more familiar with the considerably more media-friendly "black swan." Whatever the wording, these events historically have presented the greatest challenge for the industry.

In response, utilities have established mutual assistance programs to share spare equipment, work crews and other assets. The industry has also adopted increasingly sophisticated IT solutions to manage storm response, and now is poised to apply a new generation of tools to mitigating storm impacts before they occur.

Until recently, however, the risk of a deliberate physical attack remained obscured by the looming threat of cyber attack. But one event changed that and its name has become a rallying cry for improving physical grid security: Metcalf.

The PG&E substation located near San Jose, California was the target of an assault on April 16, 2013. The attackers first cut phone lines before opening fire on seventeen large transfor¬mers. The shooting went on for approximately twenty minutes. While power to Silicon Valley was never disrupted, one substation transformer was offline for nearly four weeks. Although reported at the time, the story only gained national visibility months later when the true nature of the incident was revealed and industry experts began to publicly raise questions around grid resilience.

More recently, attention has focused on the potential for coordinated attacks targeting both physical assets and the IT and communication systems that support them simultaneously. Utilities today have a good handle on single-contingency events, but the prospect of a multi-site, multi-vector attack remains a source of great concern.

Taking action

Responding to a coordinated attack was the subject of "Grid Ex II," a simulation exercise conducted by NERC with more than 2,000 individual participants from 234 organizations across the US, Mexico and Canada. The combined physical/cyber attack scenario played out over two days in November 2013, followed by a tabletop exercise among a smaller group of senior utility executives and government officials. The resulting list of recommendations was expansive, if somewhat predictable.

Many centered on improving situational awareness, aligning procedures and easing the flow of information between the various players. One recommendation—continue to build relationships with relevant government stakeholders to establish communication procedures prior to a crisis—provides an example.

In a sense, the industry has been here before. In the wake of the 2003 Northeast Blackout, utilities underwent a period of introspection driven by an uptick in regulatory and public scrutiny. The process yielded two main results. The first was a trend toward greater information sharing, which has been aided by an increase in IT system capabilities, and the second was a set of mandatory reliability standards enforced by a quasi-governmental organization that took the place of the voluntary regime overseen by the industry itself.

Without question, we are in a better place today. Still, the particular threat of a coordinated physical attack on critical grid assets deserves special attention, and that is what the industry and its regulators are giving it now. FERC has put forth suggested standards for grid security similar to those established for reliability—including penalties for non-compliance. Initiatives like Grid Ex will continue to refine utility response to physical attacks and identify areas for improvement.

Suppliers to the industry likewise will continue to build robust security into the products and systems they provide. But to better understand where we are headed, it's instructive to look at where we are now.

Drivers for better outage management

It may seem obvious that blackouts cost the utility (e.g., unserved electricity, overtime pay, truck rolls, and in some areas the impact of performance-based rates), but improving outage management also has a huge impact on the utility's consumers.

Figures vary widely by industry, but according to an analysis by the Galvin Electricity Initiative, the average cost of a one-hour interruption ranges from $41,000 for a mobile phone network to over $2.5 million for a credit card provider. Sandy was the most costly storm since hurricane Katrina, producing $62 billion in economic losses, but that same year there were ten more outages in the US that cost in excess of $1 billion each.

There are also non-economic drivers for better outage management. Mostly these have to do with rising customer (and in turn, regulator) expectations regarding utilities' communication during the restoration process. Indeed, in the utility business today there is perhaps no greater sin than poor communication during an outage regarding the extent of damage and the estimated recovery time. People expect updates via conventional and social media, voice mail and text message. Even if the news is bad, the more important thing now appears to be delivering it in a timely way across multiple platforms.

Effective communication during a storm is one thing, but when we are dealing with deliberate attacks—whether cyber, physical or both—a new challenge emerges. After all, how do you know when an attack is "finished?" Indeed, a highly orchestrated effort might even take into account the utility's initial response in order to maximize impact through a second attack.

The outage lifecycle

The following is excerpted from a Ventyx/GTM Research white paper entitled, "Coping with Extreme Weather Events," and breaks storm-related activities down into four processes. This model offers a good starting point for handling physical attacks on grid assets.

Review and planning – On "blue sky" days utilities can model historical data, simulate stress on particular feeders, substations and the wider grid; carry out system improvements; and update training for customer service reps, work crews, dispatchers and operators.

Prediction and preparation – As a storm approaches, utilities evaluate expected damage and assign field crews and equipment to be staged at strategic locations. They also begin outage communications and might perform some switching operations in anticipation of projected damage. Control might also be delegated to coordinators at individual staging sites.

Assessment and restoration – This category is comprised of three separate stages. First is automation, in which switches, reclosers and other automated equipment respond to faults and reroute power to minimize the outage area. Next comes evaluation and dispatch, which encompasses managing customer calls, field surveys, damage assessments, prioritization, crew assignment and communication with customers and other entities such as emergency services. Lastly is field work performed by mobile crews to correct faults and restore power.

1. Microgrids

While much of New York, New Jersey and surrounding areas were struggling to restore power following hurricane Sandy, the lights were already on at Princeton University. The campus operates its own microgrid and after successfully islanding from the main grid, Princeton was able to sustain itself using its own generators. The University ended up providing a staging area for first responders to charge laptops, mobile phones and other electronics.

Since Sandy, interest in microgrids has surged, primarily due to the added reliability the offer. Concern over the volatility of fuel prices, and indeed availability of liquid fuels in a crisis, has driven additional interest in microgrids as a means to incorporate renewable power generation like solar PV. As we saw in the case of Sandy, tanks full of diesel and gasoline don't do much good if you don't have the means to pump the fuel.

Repair and closeout – Following the final restoration, an outage management system aggregates, processes and records required compliance data, and field crews perform permanent repairs and grid hardening.

What is immediately apparent from the Ventyx/GTM Research lifecycle is that outage response is extremely labor-intensive, despite the ever-expanding capabilities of outage management systems and other IT tools found in utility control rooms. Even if we take cost out of the discussion for the moment, it still is not practical to simply throw more resources at the problem. Utilities need other ways to address physical attacks, especially outside of the response process itself.

Building resilience

The term "resilience" is often used to make the distinction that outages will always occur so while prevention is important, it's helpful also to focus on what can be done to quickly bounce back. But in the case of deliberate attacks, the most important work is arguably what is done before an incident happens.

Accordingly, what follows is a brief discussion of resilience-enhancing technologies that we have divided into four stages of resilience.

Deter – This first stage refers to steps a utility can take to make a physical attack less likely or less appealing to a would-be attacker. Underground cables are one obvious choice—if you can't access the equipment, you can't damage it. Similarly, gas-insulated substations can be located indoors or underground thanks to their small footprint. The same characteristics that make GIS small also make them extremely reliable in normal operations. Ground stability devices are also available to prevent disruptions caused by geomagnetic storm-induced currents (GIC) and electromagnetic pulses (EMP). These devices would also provide protection from attacks using an EMP as a weapon.

Detect – Clearly, the first step in responding to a physical attack is realizing one is happening. This is the realm of specialized security systems that, in addition to video surveillance, employ a variety of sensors such as acoustic sensors that can detect gunshots or optical sensors that can pick up reflections from binoculars or a rifle's scope. These systems should operate on a dedicated communications platform separate from the operational networks of the facility.

Additionally, sophisticated asset health systems are now beginning to be deployed to monitor critical assets and some of the capabilities could be applied to a security context. If the temperature of a transformer unexpectedly exceeds a certain threshold, for example, or it suddenly loses a large quantity of oil, the asset health system might then issue an alarm to grid operators or other response personnel indicating a possible attack was under way.

No single variable can accurately detect an incursion every time, so defense in depth is the best approach. Even vibration sensors on substation fences could send up false alarms if something (e.g., wind, wildlife) comes into contact with the fence.

Another aspect to consider is communications. The first action taken by the Metcalf attackers was to cut the substation's phone lines, presumably to sever communications between on-site security systems and the PG&E control room. If, however, a substation uses a wireless network to gather and send video, sensor readings, etc., there is less exposure to disruption from physical action. Also, mesh networks allow communications to be reconfigured if one node goes down, and they can accom¬modate high-volume traffic with low latency.

Delay – Once an attack has begun, and assuming the utility is aware of it, the next line of defense is to delay the onset of damage. This may seem counter-intuitive—how do we make an attack proceed more slowly?—but there are some types of equipment that are less vulnerable to certain types of abuse. Dry type bushings in transformers, for example, do not use oil for cooling and so have the ability to take a bullet and continue functioning.

Respond – To this point, all of the defensive measures we've identified have been passive in terms of human intervention, but clearly there is only so much that automation can do. Response actions are largely driven by human decision making, and here information is paramount. Tools that enhance situational awareness are vital, and transmission and distribution control systems are becoming more and more robust every day. Now, transmission applications focused on grid resilience are in development to extend the capabilities of asset health solutions already available.

It's also important to remember that the response to an attack necessarily involves multiple working groups, not all of whom are utility employees. This extends to emergency personnel, local government and federal agencies, but also to industry suppliers. Well established equipment suppliers typically have some type of emergency service offering that might cover any number of contingencies. Expedited repair services, spare units and a global supply network for parts are just a few of the capabilities that a supplier of transmission and distribution equipment might bring to bear.

A good start, but more to do

Utilities face daunting challenges as they set about hardening a grid that was designed in a different time and still largely operates that way. However, a combination of advances in primary equipment, sensor and communication technology, and perhaps most importantly, analytics, offers some solutions. We may soon see a new generation of proactive control systems that integrate a range of security features with normal operations. Such systems will use highly advanced algorithms that in turn rely on powerful computers, but real challenge lies in improving operator decisions by providing the most relevant information.

For more information, please contact:

ABB Inc.

Marty MacDonald
Director, US Federal Government Initiative
12040 Regency Parkway
Cary, North Carolina 27518
E-Mail: marty.macdonald@us.abb.com

new.abb.com/us/gov

9AKK106103A7943