WHITE PAPER

Cyber and physical resilience for the power grid

Grid operators today take a holistic approach when considering the range of threats (cyber and physical, natural and human-caused) to their systems.

While each incursion is individually disruptive, experts agree the greatest threat to the electric grid is a combination of cyber and physical attack. For this reason alone, security measures to address both dangers must be coordinated. Fortunately new technologies including advanced sensors, analytics and the Internet of Things offer fresh tools that improve grid security and resilience whether in relation to natural or intentional disruptions.

This paper discusses various technologies and practices that can prevent outages and mitigate their impact if and when they do occur. We also discuss the role of government in ensuring grid security and the critical areas of focus for policymakers going forward.

Increasing threats, both cyber and physical

Outages and other less visible disruptions to the power grid come from three main causes, individually, or in combination:

- natural disasters like hurricanes, ice storms and floods;
- system malfunctions, typically caused by human error or system/equipment failure;
- intentional attack, whether cyber or physical

Examples of these modes of disruption unfortunately are easy to find. The cases below describe some of the most newsworthy in recent years, but what is important to understand is that both cyber and physical threats are increasing.

Natural disaster: Hurricane Sandy
On October 29, 2012, a storm of unprecedented size made landfall in the New York – New Jersey area, causing a power outage that spanned 17 states and over 8 million homes. The storm directly caused 72 deaths and another 87 indirectly, with 50 being directly attributed to power outages. Sandy caused $65 billion in damages.

Multiple system failure: 2003 Northeast Blackout
The Northeast Blackout of 2003, the largest in U.S. history, is said to have been caused by unpruned foliage and a faulty alarm system that failed to alert control room operators of the need to reroute power. Fifty-five million people in eight states and Canada lost power, many for two days. The case demonstrates the catastrophic impact of a physical event paired with compromised operator control systems.

Physical attack: Metcalf substation
In the early hours of April 16, 2013, gunmen severely damaged 17 large power transformers at a major northern California sub-station. The attack was well-

planned; the perpetrators scouted firing locations, targeted critical equipment, and cut fiber optic communication lines to disable on-site security and automation systems before the shooting began. The attack required several weeks and $15 million of repairs to correct, with only a fortunate series of factors keeping it from wreaking widespread and long lasting outages.

Cyber-attack: Ukraine grid takedown
On December 23, 2015, hackers gained access to three local utility control systems in Ukraine and executed a series of commands that caused blackouts affecting 225,000 customers. Investigations showed that the attackers had access to utility systems for six months prior to the attack, and had used a variety of techniques to gain access, avoid detection and ensure success. The effects were limited—power was restored within a few hours in most cases—but the incident was a warning against potential attacks of even greater sophistication and impact.

In terms of storms, climate science tells us we should expect more frequent and more severe storms in the coming years. Hurricane Sandy was important not only for its size and strength, but also because it exposed weaknesses in our approach to storm recovery. When emergency backup generators ran out of fuel, operators expected resupplies from local gas stations. However, because the pumps at local gas stations lacked the electricity to operate, both the gas stations and the backup generators that required their fuel were rendered useless.

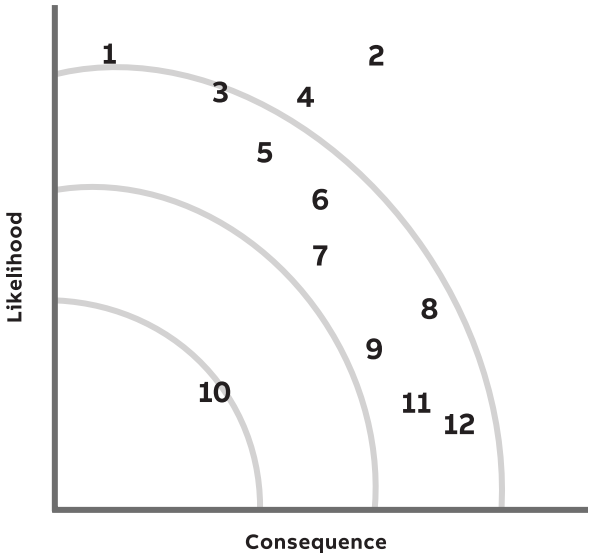
The aftermath of the storm prompted a review of what constitutes “critical infrastructure” in the context of an extended power outage (i.e., what facilities must be supported with some kind of alternative power source). Work in that area is ongoing.

In contrast to storms, which are frequently predicted, cyber security breaches may be difficult or even impossible to anticipate. Cyber-attacks typically leverage previously unidentified system vulnerabilities known as “zero-day exploits,” so-named for the number of days the given weakness has been known to system vendors and owners. Cyber-attacks also have the potential of using utility systems against recovery efforts once an initial attack has been instigated, delivering misinformation to grid operators.

Figures from the Department of Homeland Security show a nearly 50 percent increase in cyber-attacks against critical infrastructure targets between 2012 and 2015. With the proliferation of connected devices and the associated potential for them to be used as a point of entry, experts expect continued growth in cyber-attacks, especially against grid assets.

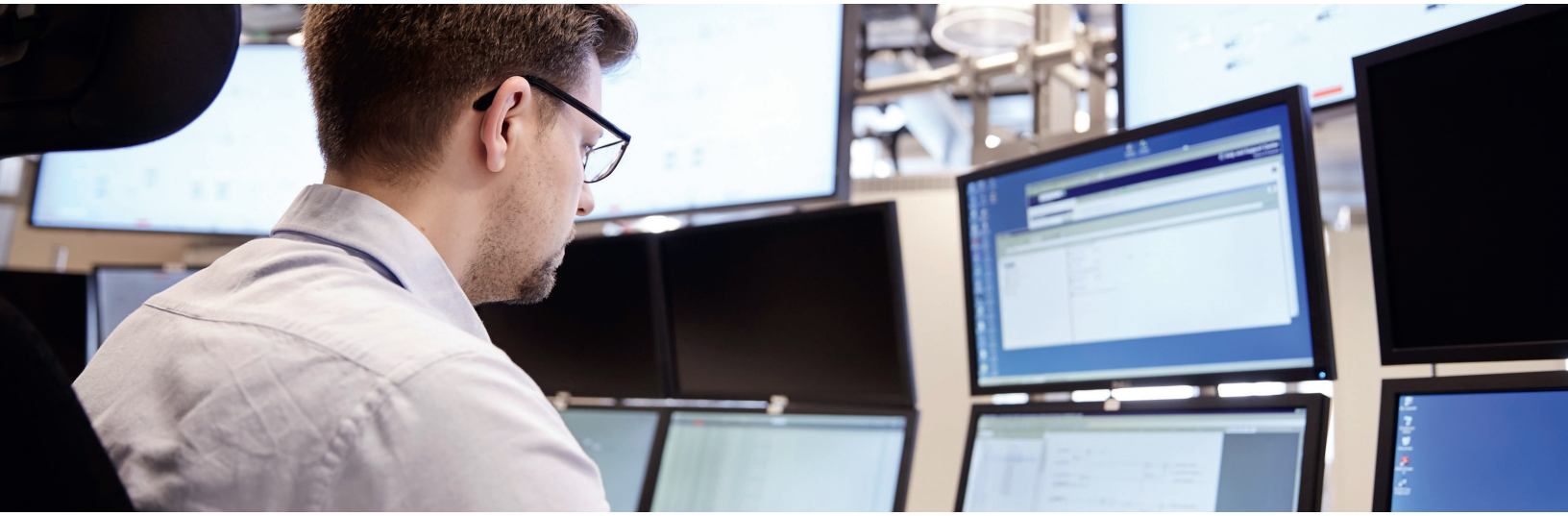
NERC data from 2014 shows that out of a total of 245 cyber-attacks on critical infrastructure, 79 (32 percent) were directed at the energy sector. As the chart in Figure 1 shows, cyber-attack is second only to natural disasters in terms of combined likelihood and consequence in relation to the grid.

Figure 01 NERC Threat Landscape (Public Utilities Fortnightly, September 16, 2016)



1 Squirrels
2 Natural disasters
3 Physical attack/theft
4 Cyber attack
5 Insider threat/catastrophic human error
6 Coordinated physical & cyber attack
7 Supply chain disruption or compromise
8 Pandemics
9 Geomagnetic disturbance
10 Direct energy weapon
11 CBR attack
12 High-attitude EMP
13 Nuclear

While no major combined cyber and physical attack has been made public, the damage a well-coordinated cyber/physical attack could inflict may be severe, especially if adversaries have knowledge of how a particular segment of the grid operates. Such a multi-faceted threat landscape requires a comprehen-sive and diverse security strategy.



How do we protect the grid?

Security professionals identify four stages in address-ing a security challenge: deter, detect, delay/defeat and respond. There are many technologies currently available to support each stage of the security pro-cess. However, it is important to keep in mind that any one technology goes only so far. Process, procedures and the cultivation of a safety/security culture must underpin grid protection.

Deter
Deterrence involves both physical and cyber measures to pre-vent an outage before a disruption occurs, including:

- **Site security**
  The traditional methods for physically protecting a facility include fences, security cameras, motion detectors, locks, lighting, etc.

- **Air-gapped computer systems**
  Placing computers used in essential control applications on a secure network is one of the time-tested basics of cyber securi-ty. The term “air gap” is literal: the control network is physically separate from the business network or other internet-connected devices. The only access to an air-gapped system is via a com-puter physically connected to the protected network.

- **Wireless communications**
  Wi-fi offers an alternative to fiber optic or other wired systems. Substations equipped with wireless communications are less susceptible to being disabled, enhancing the reliability of on-site sensors, security cameras and other alert systems. Wireless can also be used to back up traditional communications and create system redundancy when wired communications are disrupted.

- **Submersible switchgear**
  Switches that can survive flooding and even operate underwater are available for flood-prone areas where it may not be feasible to elevate an entire facility. Certain areas impacted by Hurricane Sandy have been rebuilt using this type of equipment.

- **Underground power lines**
  Long used in housing developments for aesthetic reasons, underground lines offer clear advantages in terms of resistance to storms. There is a price premium as compared to overhead lines, but with storms occurring more frequently and with greater strength, utilities have begun re-assessing the cost-benefits of underground lines.

- **Underground/indoor substations**
  These facilities have historically been used to bring high-voltage power into city centers via a compact, secure and visually appealing facility. The security advantages—a controlled environment in a smaller footprint that hides a substation—are an added bonus.

- **Concrete poles**
  Able to withstand high winds, concrete poles offer an improvement over the traditional wood. During Hurricane Matthew, Duke Energy lost 1,900 wood poles, which in turn accounted for much of the utility’s 294 miles of downed lines. Utilities are replacing old wood poles with concrete in many areas.

Detect
Detection involves identifying potential threats. This is an area that has benefitted tremendously from the advances in sensors, communications and analytic technologies.

- **Automated metering infrastructure (AMI)**
  Automated metering was developed to reduce the time and resources required to gather consumption data, improve accuracy and encourage energy efficiency. However, electronic meters equipped with communications capability are now used to pinpoint outages. Grid operators using AMI receive precise, real-time pictures of power outage locations to enable faster power restoration.

- **Fault detection**
  Using a combination of physical sensors, analytics, and communications it is now possible for utilities to remotely receive a fault alert and narrow the fault to a precise location for automated or manual correction. This technology can also feed directly into a customer communications program to provide users with updates on restoration times.

- **Network security monitoring (NSM)**
  User identification and authorization is the obvious first step in any cyber security regime. As the name implies, NSM extends to 24/7 monitoring of utility computer systems for irregular activity. In the 2015 cyber-attack on Ukraine's power grid, the hackers actually executed a test prior to the assault, a test that went unnoticed at the time but would have been flagged immediately using NSM due to a massive spike in network traffic. Importantly, such activity could be anything—including perfectly legitimate processes—that goes outside the bounds of typical operations. NSM processes generate many alerts so part of the challenge with these systems involves using a combination of computer analysis and human evaluation to identify the threats.

- **Asset management**
  In many cases, systems originally designed to perform one function can deliver a substantial benefit to cyber security and recovery objectives. For example, asset monitoring systems designed to prevent failures and reduce maintenance costs are also used in a security context. Field devices can feed data to NSM systems creating awareness of events that in turn enable operators to take action (or not) as needed.

  For example, if a relay setting is changed, grid operators can compare it to a work order history for that device and determine whether or not it warrants investigation. Even a once-a-day transmission from a sensor tracking the condition of the oil inside a transformer offers value as a daily check that the unit is online and working properly. This may not seem like much, but it is a vast improvement over conventional on-site inspections.

Delay/Defeat
This security step is primarily associated with intentional attacks, although in many cases technology that improves resistance to attack also improves resistance to weather events.

- **Dry transformers**
  Traditional transformers use flammable oil as an insulator. While solid insulation materials won't necessarily prevent a failure, dry transformers can greatly mitigate damage by eliminating the potential for explosion should an incident occur.

- **Ballistic coatings**
  In the wake of the Metcalf substation attack, manufacturers set out to harden high-risk equipment (e.g., power transformers) against sniper attacks. One result is a special coating that effectively absorbs bullet impacts and reduces spalling (fragmentation) to limit damage to surrounding equipment and personnel.

- **Distributed intelligence**
  Research and development efforts are under way across the industry to create more sophisticated and harder-to-defeat security systems for industrial applications. One of these, a Department of Energy project named CODEF, is specifically aimed at reducing the scope and impact of a cyber-attack on utility control systems.

  CODEF uses physics and engineering logic to evaluate a given command from a utility control center to determine if the command would create an unsafe condition. The intelligence behind the system is installed not in the control center but in the substation. CODEF allows equipment in nearby substations to "compare notes" and in the event an unauthorized user gains access to the utility's control system, any malicious command would be ignored. Due to its decentralized nature, an attacker would have to disable the system at each substation individually as opposed to breaking it once at the control system level.

  CODEF has yet to be commercialized, but is nearing completion of proof-of-concept.

- **Microgrids**
  We describe this important category in more detail below as a "response," but microgrids can also act to delay a physical or cyber-attack simply by virtue

of their decentralized nature. Like nodes on the internet, if one portion of the grid goes down, a microgrid can be designed to continue operating in island mode. An attacker seeking to disable a facility served by a microgrid embedded in a local utility system would need to infiltrate and disrupt both the microgrid itself and the surrounding power system.

Respond

Once a storm or attack is identified, grid operators have a variety of tools at their disposal to mitigate the effects. Importantly, many of the tools have more to do with practices and procedures than with any particular technology.

- **Data forensics and incident response**
  This engages a rapid reaction force of cyber security experts, engineers and operators to provide on-the-ground technical assistance and support post-mortem analysis and official in-vestigations.

- **Distribution grid automation**
  This is a broad term that encompasses some of the technologies described above as “detect” solutions. The information provided by automated metering systems or fault location can also be used to prioritize and manage restoration efforts. For example, automated systems known as FLIR (fault location, isolation and restoration) can identify a fault and automatically trigger switches for remote power restoration.

  For areas without automated recovery capabilities, FLIR systems can pinpoint the location of faults so that work crews spend less time looking for downed lines or tripped switches and more time repairing them. Integrated systems that combine mobile workforce management (MWFM) with FLIR are available today.

- **Equipment pools and cooperative agreements**
  Utilities already have cooperative agreements to share resources like work crews and some types of equipment (e.g., cutouts, reclosers). These measures have proven essential to recovery in the wake of major storms. However, regions differ in terms of their equipment needs and the types of physical threats, so the ability of any one utility to assist another is limited.

- **Recovery transformers**
  Power transformers are the lynchpins of any power system. However, large power transformers (LPTs) have long manufacturing lead times (up to 18 months) and are individually engineered and built for the specific site and application to which they are deployed. Because the units are costly and spares are generally not eligible for rate recovery, utilities maintain limited numbers of spares. This means the loss of multiple LPTs in strategic locations poses a significant risk of a long-term, wide-spread power outage.

  A great deal of effort has been made toward making transformers less vulnerable (e.g., ballistic coatings and explosion-resistant components) and mitigating the effects of their loss. One project by the Department of Homeland Security produced an LPT designed as three separate single-phase units rather than one large three-phase transformer. This approach allows the units to be smaller and lighter so they can be quickly trans-ported and installed to restore power flow while a customized replacement unit is manufactured.

- **Microgrids and distributed energy resources (DERs)** Microgrids are small power systems equipped with their own source of generation and

can be used in remote locations or embedded within larger grids. They have attracted much attention in recent years as a way for critical facilities such as hospitals to remain operating even when the surrounding grid goes down. The key, however, is that they must be able to island themselves from the grid. Otherwise an energized microgrid could create hazardous conditions for workers performing repairs on the surrounding system.

Microgrids have typically been used in campus environments or at industrial facilities that produce their own power. With advances in control technologies, energy storage and renewable generation (e.g., solar), they are becoming economically viable for a wider range of applications.

Challenges and considerations for policy makers

The technologies described in this paper offer a range of benefits with regard to grid security, but as noted at the outset, technology is only part of the solution. Indeed, some of the challenges to grid security lie in regulation and public policy.

State policy
Because states retain primary authority over the electric grid within their boundaries, utilities must gain approval for most grid investments from state public utility commissions. PUCs should take into account the security benefits—economic and other-wise—of grid investment proposals. This would enable a more robust cost-benefit analysis and encourage utilities to pursue grid security projects.

States must also modernize their regulations governing who can sell power and how. Distributed energy resources, from grid-connected residential solar to community microgrids, are too often inhibited by rules established decades before these technologies were mainstream.

Federal policy
The federal government also has a role to play in advancing grid security. Annual funding supports investments in federally owned power systems and is occasionally punctuated by one-time infrastructure spending initiatives, most recently through the American Recovery and Reinvestment Act of 2009. The discussion behind these investments should include security impacts/benefits as a matter of course.

In the aftermath of a federally-recognized disaster, the Stafford Act governs how disaster funds may be spent. In rebuilding damaged portions of the electric grid, recipients of disaster funding should be allowed to replace damaged equipment with current technologies that have greater security and resiliency capabilities than what was originally in place.

As described above, grid security technologies have undergone tremendous advancements in recent years, but ongoing research and development efforts by the federal government in partnership with industry will drive continued progress. Healthy federal R&D budgets are therefore essential.

Federal tax policy also has a significant impact on the scale and scope of grid investments, especially for investor-owned utilities. Better aligning tax policy, such as capital depreciation, with how modern electrical infrastructure is deployed would encourage wider adoption of technologies that boost grid security.

Finally, federally-defined “critical infrastructure” receives special attention from government. As noted earlier, Hurricane Sandy forced us to reconsider what falls under this heading. Federal policymakers should take a holistic view of what constitutes critical infrastructure as they work to re-characterize various types of facilities.

Investments in grid modernization pay off

The government has invested billions of dollars on grid modernization in recent years, and the industry has invested tens of billions more. Ample evidence shows that these efforts in modernization, security and resiliency are having a real impact. The U.S. government reports that every $1 million in direct spending on grid modernization and hardening generates $2.5 million to $2.6 million in GDP growth thanks mostly to avoided (or reduced) outages. Individual utilities have reported similarly compelling results.

For example, Florida Power & Light has invested $2 billion since 2006 on grid modernization. FPL estimates that during Hurricane Matthew those investments prevented 55,000 outages and allowed the utility to restore service within 24 hours to 99% of the more than 1 million customers who lost power. Similar recovery efforts in the past took as long as 15 days.

Consolidated Edison invested $1 billion following Hurricane Sandy in 2012 with a focus on improving grid resilience in New York City. ConEd estimates that more than 65,000 customer blackouts have been

avoided thanks to these upgrades. If a storm of similar impact were to hit now, that figure would likely increase dramatically.

The U.S. power grid has served as an engine of prosperity for more than 100 years, but the infrastructure that comprises it is aging while the threats against it are growing. More remains to be done to address these trends. With the right incentives and regulatory framework, the U.S. power industry will be well-positioned to ensure the grid continues to support the safety, security and economic well being of the country.

—

For more information contact:
Jim Creevy
Vice President, Government Relations
Jim.creevy@us.abb.com

Asaf Nagler
Senior Director, Government Relations
Asaf.nagler@us.abb.com

—

9AKK107045A6738 REV A 18.5.2010 #14995