White paper

Physical Security of the U.S. Electric Grid

An Attack on the Electric Grid

Just before 1 AM on April 16, 2013 several people launched an attack on the Pacific Gas and Electric (PG&E) Metcalf transmission substation, which provides power to Silicon Valley.

They began by lifting a metal cover and entering an underground vault that contained AT&T's fiber-optic telecommunications cables between the Metcalf substation and its command center, which they cut. Then fired AK-47 rifles into the substation's transformers. Shooting for nineteen minutes, they destroyed seventeen of the substation's giant transformers. And, at 1:50 AM, one minute before the police arrived, they disappeared.

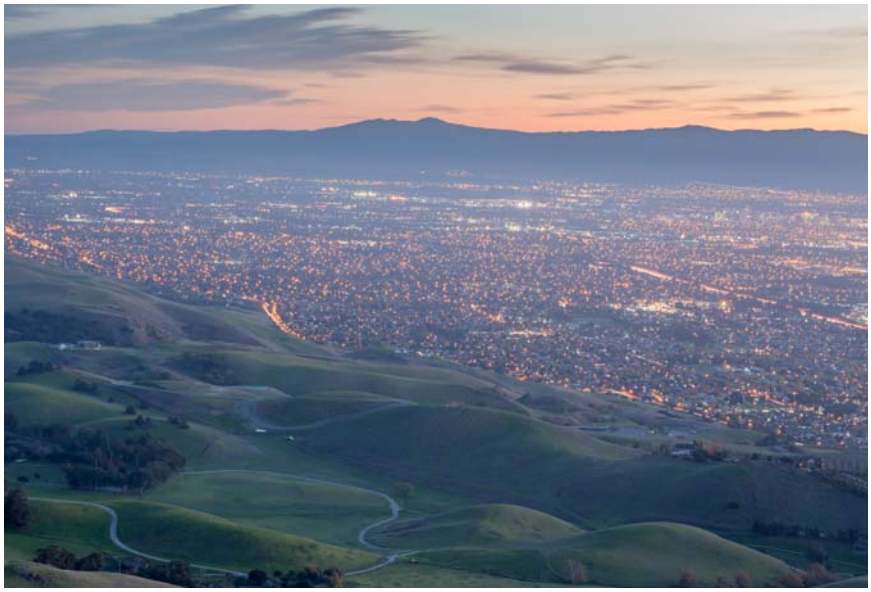

Figure 1 A 2013 attack targeted a substation which provides electricity to Silicon Valley

If it was an attempt to knock out power to Silicon Valley, the attack was unsuccessful. However, the truth is we don't know the attackers' motivation; they were never identified. There were surveillance cameras in place, but they were all aimed towards the substation, while the shooters stood just outside the perimeter. [1]

The only thing we know for sure is that it was a coordinated, planned attack. In the words of Mark Johnson, a PG&E vice president:

1.Koppel p. 17

> This wasn't an incident where Billy Bob and Joe decided, after a few brewskis, to come in and shoot up a substation. This was an event that well thought out, well planned and they targeted certain components.[2]

The chairman of the Federal Energy Regulatory Commission (FERC) at the time, Jon Wellinghoff, called the attack "the most significant incident of domestic terrorism involving the grid that has ever occurred."[3]

His concern wasn't so much because of the damage that occurred, but because of what the attack told us about the possibility of future attacks. Jon Wellinghoff believes that "the attackers may have been engaging in a rehearsal rather than a comprehensive sabotage operation."[4]

The Effects of a Coordinated Attack

A coordinated terrorist attack on the U.S. electric grid would be catastrophic. As the Department of Energy put it in a report, "The U.S. electric power grid is one of the Nation's critical life-line infrastructure on which many other critical infrastructure depend, and the destruction of this infrastructure can cause a significant impact to national security and the U.S. economy."[5]

Figure 2 Bringing down the U.S. electric power grid would bring down most of our critical life-line infrastructure

2.Koppel p. 18-19
3."Assault on California Power Station Raises Alarm on Potential for Terrorism"
4.Koppel p. 19
5."Large Power Transformers and the U.S. Electric Grid"

We are a nation entirely reliant on our electrical grid for everything from our food to our medical care. As one FEMA director explains:

> We're not a country that can go without power for a long period of time without loss of life. Our systems, from water treatment to hospitals to traffic control to all those things we expect every day, our ability to operate without electricity is minimal.[6]

Some projections of the impact of a nationwide blackout are nearly incomprehensible. One 2008 congressional report predicts that nine out of ten Americans would die from starvation, disease or societal breakdown within a year of nationwide blackout.[7]

Even more frightening is that disabling the U.S. electrical grid would not be terribly difficult to do. In fact it would take nothing more than a coordinated attack of the sort that occurred in the Metcalf substation. According to security specialist Paul W. Parfomak in a report submitted to Congress, "[t]ransformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage." Nor does Parfomak believe it would take much sophistication, noting that bad actor could easily "disable transformers from a distance using conventional rifles."

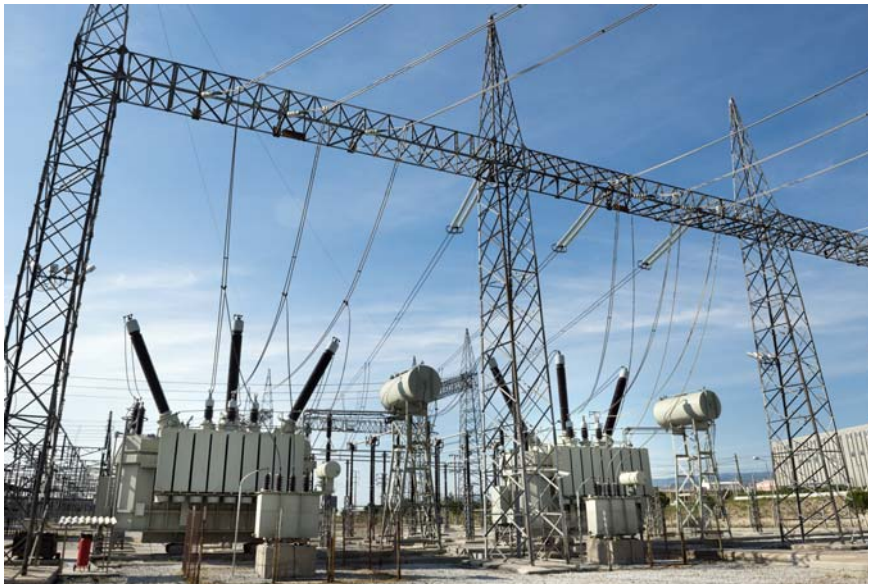

Figure 3 The transformers that make up the electrical grid are easily disabled with only a basic knowledge of their design

6.Koppel, p. 117
7.Koppel, p. 22

The coordination would not be terribly difficult either. As the Federal Energy Regulatory Commission (FERC) put it in a memo, “[d]estroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer.”[8]

That 18 months would be more than enough time to test the congressional report prediction that only one out of ten Americans would survive a year without electricity.

Efforts to Physically Secure the Grid

Many believe that a successful attack on the US electrical grid is only a matter of time. The Metcalf attack created an awareness of the need for physical security on the electrical grid. In March 2014, FERC directed the North American Electric Reliability Corporation (NERC), which promotes mandatory standards for the federally jurisdictional bulk power system, to propose standards that require utilities with critical assets to take steps to address physical security vulnerabilities. This was done, and FERC approved the standards.

However, those standards did not include specific physical security requirements. As George Cotter notes in a 2015 white paper provided to the National Security Agency and the Department of Energy: “FERC and NERC exclude any steps utilities must take for minimum protection of facilities; leaving it to utilities and compliance officials to determine.”[9]

There have been several legislative efforts by Congress to provide physical security requirements, but those have been generally opposed by the public power industry. As the American Public Power Association (APPA) put it, while they support “physical security initiatives at the bulk power system and distribution levels, we do not support a federally legislated ‘one-size-fits-all’ mandate.”

8.“U.S. Risks National Blackout From Small-Scale Attack”
9.“Security in the North American Grid: A Nation at Risk”

Their reason for this is “the retail nature of distribution systems, and the vast differences in the configuration, size, and ownership of the 3,000 distribution utilities in the U.S.”[10] Homeland Security agrees, telling the *Wall Street Journal* “it is up to utilities to protect the grid.”[11]

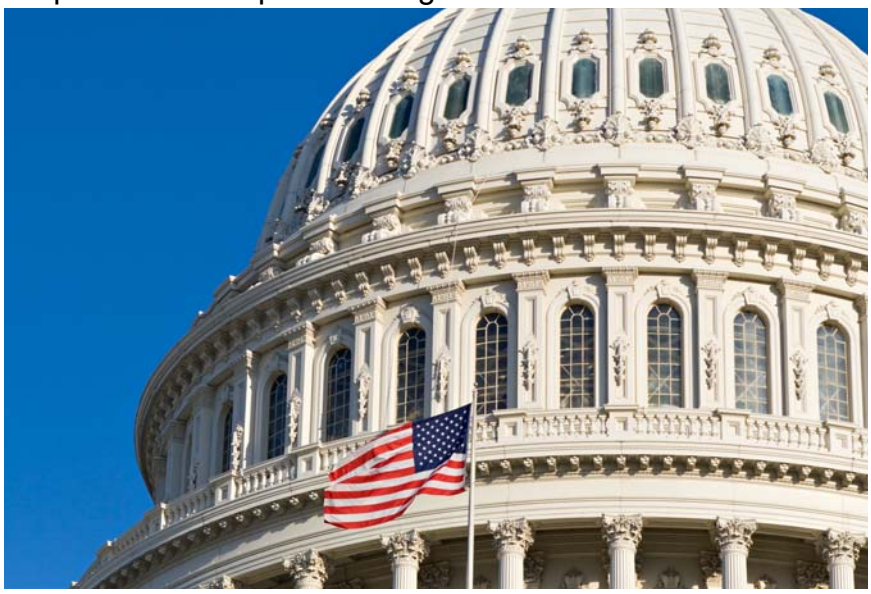

Figure 4 Congress has attempted legislation, but as of now there are no physical security requirements for electric grid components

What that means is that the physical security of electric grid components is still primarily the responsibility of each of the distribution system owners. As a consequence, the physical security varies widely based on individual interpretation of the 2014 FERC standards and the resources available.

Recognizing the catastrophic consequences of any threat to the U.S. electrical grid, there have been executive orders aimed at securing the grid from both Presidents Obama and Trump, but neither addressed physical security; President Obama’s targeted the threat of space weather events,[12] and President Trump’s addressed cybersecurity.[13]

Both of those are legitimate concerns, but many believe that a physical attack is a far greater danger. As Rebecca Smith writes in The Wall Street Journal:

> "A lot of people in the electric industry have been distracted by cybersecurity threats," said Stephen Berberich, chief executive of the California

10.“Physical Security and the Electric Sector.”
11.“Assault on California Power Station Raises Alarm on Potential for Terrorism”
12.“Executive Order - Coordinating Efforts to Prepare the Nation for Space Weather Events”
13.“Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”

> Independent System Operator, which runs much of the high-voltage transmission system for the utilities. He said that physical attacks pose a "big, if not bigger" menace.[14]

Part of the reason for this belief is that coordinated physical attacks on the electric grid are a known terrorist tactic. Though it never reached fruition, the Irish Republican Army planned exactly this kind of coordinated attack against six transmission substations in the United Kingdom in 1997.[15] Likewise, according to a report from the Electric Power Research Institute, there were 2,500 attacks on transmission lines and 500 attacks on substations committed by terrorist groups between 1996 and 2006.[16]

Increasing Physical Security

Many utilities are already enhancing the physical security of the critical components in their distribution systems. There are effective security solutions available.

Perimeter fences can be can be reinforced using wireless point-to-point photoelectric detectors to create a perimeter beam system. Because the photoelectric detectors are battery-powered, there's no need to run power to them, so that trenching and the running of cable is eliminated.

Inside the perimeter, wireless motion detectors can also be installed to provide protection in case an intruder makes it inside the perimeter. Again, they would be battery-powered, and could be easily mounted to cover sensitive locations or the entire facility.

All detectors on the property, both the external photoelectric detectors and the internal motion detectors, then can also be set to trigger pan–tilt–zoom (PTZ) cameras. This would allow the cameras to capture and record video of any intruders and

14."Assault on California Power Station Raises Alarm on Potential for Terrorism"
15."Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations"
16."Assault on California Power Station Raises Alarm on Potential for Terrorism"

provide it to the central monitoring station so that action can be taken.

Figure 5 Critical components of the electric grid can be secured with wireless detectors connected to PTZ cameras

Guards on the property can also be provided with wireless panic buttons. The panic buttons would operate on the same wireless network as the detectors and allow guards to alert the central monitoring station in the case of an emergency.

Conclusion

A coordinated terrorist attack would be catastrophic, but there other equally valid reasons to secure electrical substations. Copper theft and vandalism can be incredibly costly and cause months or years of downtime.

This is especially true in the case of high voltage transformers, which are roughly fifty-percent copper and electrical steel. Each must be custom made for a particular site, costs millions of dollars, and, because they weigh somewhere between 100 and 400 tons, can only be transported by special railroad cars, of which there are only about two dozen in the entire country.[17]

Nor are high voltage transformers the only potential targets of theft and vandalism. Damage to wind turbines or theft of solar panels from solar farms can cost hundreds of thousands of

17.“Large Power Transformers And The U.S. Electric Grid”

dollars, and many of these are located in remote areas and remain unprotected.

Figure 6 Solar panel theft and wind turbine vandalism can also be protected against

Whatever the reason for increasing security in an electrical grid component, there are cost-effective solutions available. Inovonics has been developing and manufacturing commercial security products for thirty years. Our networks are designed and optimized to support exactly this kind mission critical infrastructure.

For more information about Inovonics commercial wireless solutions, contact us at sales@inovonics.com