THREE-LAYERED APPROACH TO PHYSICAL SUBSTATION SECURITY: DETECT, DETER, AND DEFEND

By Megan Happel

Bullets rained over four substations on Christmas Day, 2022, leaving 15,000 Washington residents without power and causing over $3 million in damages. The attackers held no grudge against the utilities, but instead recklessly fired at substations until they found the one that would cut off power to a store they wanted to rob.

While this crime resulted in an expensive and inconvenient power outage, it could have been worse. When malicious actors are more deliberate and strategic in their attacks, they have the potential to become much more devastating.

"I've been talking to a lot of physical security specialists and subspecialists," said Jason Pfaff, vice president of innovation at POWER Engineers. "And this is the trend that they're worried about. The sophistication of people having knowledge about our energy grid and being more coordinated in attacks is something that really, really concerns us. It's no longer just one substation that they're eyeing. They're eyeing multiple substations to cause a lot of damage."

In light of this disturbing trend, the North American Electric Reliability Corp. established the CIP-014 standard to ensure a base level of protection for the nation's critical infrastructure. By identifying and protecting the assets that, if rendered inoperable, would cause catastrophic or cascading failure, utilities can be more prepared for potential attacks.

Unfortunately, since every substation differs in surrounding terrain, equipment configuration, and critical asset identification, deciding exactly how to protect them is not easy, even with the guidance of CIP-014. However, because of new and emerging technology, utilities can now consider their options with the help of a three-layered approach to physical substation security: detect, deter, and defend.

Flames erupt from a damaged transformer.

Layer One: Detect

In the event of an attack, it is vital to catch the assailants early. The sooner law enforcement is involved, the sooner the situation can be resolved. To do this, utilities must keep a close eye on the area surrounding their substations. According to Pfaff, information systems are the key to early detection.

"Thermal sensors and stereo cameras are getting really advanced," Pfaff said.

Much like human eyes, a stereo camera uses multiple paired lenses, each with an image sensor, to perceive depth and capture three-dimensional images. Artificial intelligence programs that are used for optic recognition, combined with computers, can monitor and scan through these camera feeds to detect abnormalities. Ground radar, which can be set up to surveil a specific area, gives the artificial intelligence more information by tracking movements and relaying precise locations, including how far an object of interest is from critical assets.

Once a threat has been identified, the artificial intelligence system can trigger alarms, notify law enforcement, and send real-time updates on the exact location of the threat to the proper authorities.

"In the future, I suspect we will see unmanned aerial vehicles play a role in substation security through automated launch and deployment once a threat is detected," Pfaff said. "They can fly to the threat location and be the eyes on the ground for law enforcement."

Layer Two: Deter

As inconvenience increases, so does deterrence when it comes to physical security. If there are enough obstacles, a plan to attack may fall apart before it begins. One of the biggest ways to deter potential attacks is to minimize temptation by removing line of sight.

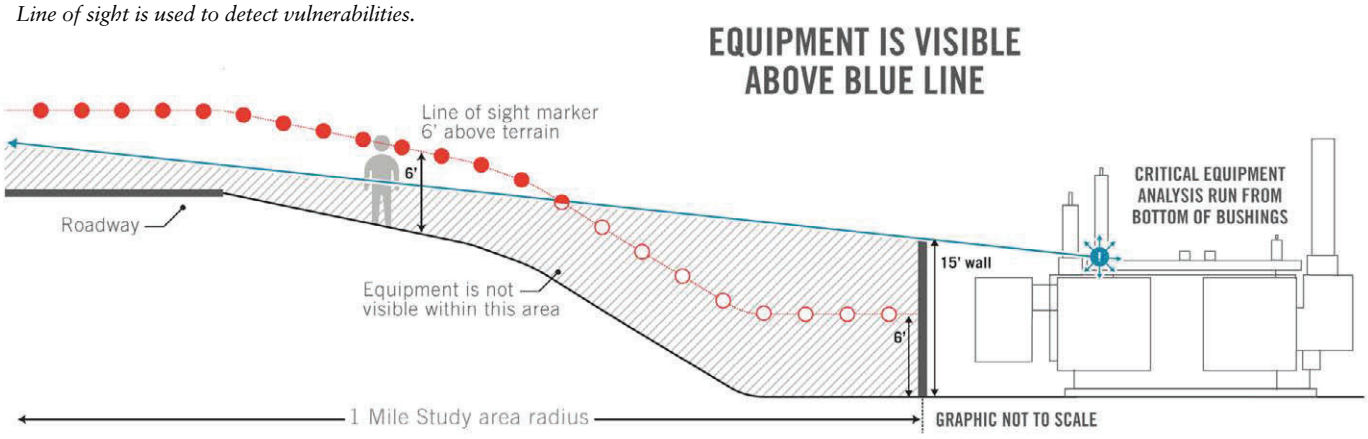
There are several ways to limit the view of critical assets from outside of a substation. An obvious option is to erect a ballistic wall. However, when considering the entire perimeter of a substation, this option can become very costly.

"Our clients come to us often asking how they can reduce the construction costs for security walls while maintaining physical security," Pfaff said. "The answer is to build only what's needed."

Pfaff and his team at POWER Engineers have been working on a line-of-sight-based inspection tool to assist utilities in doing just that. Building a digital twin—a 3D digital representation of a substation and its surrounding terrain—within the tool displays line of sight to critical assets and shows how changing physical aspects of a substation can minimize the view of its assets.

The digital twins are created using a combination of drones and lidar technology. These models are then dropped into a game, or real-time, engine where mitigation can be simulated and studied

Line of sight is used to detect vulnerabilities.



under different threat conditions. By placing hit markers on critical assets, the software will highlight the areas of the asset that are visible from outside, and barriers can be dropped in to see how the line of sight changes.

"We can use this tool to test assumptions," Pfaff said. "In real time, we can show clients what would happen if we moved a wall closer, or lowered the height. Since this is all taking place on a video conference call with a team of engineers and security specialists, we can get a good idea of how those changes might affect the overall construction costs before construction even begins."

Testing assumptions with digital twin technology recently saved a utility $1.5 million in construction costs.

A 3D-generated digital twin as viewed from a real-time engine.

Layer Three: Defend

A much-debated alternative to solid ballistic walls is expanded metal fencing. Much like a traditional chain-link fence, anyone standing outside of a substation can look through this type of fence and see critical assets, which is why some utilities are wary of it. However, unlike chain-link, expanded metal fences are much harder to climb and will fragment bullets, preventing them from hitting their intended target. The see-through nature of this fence also has a benefit for first responders, allowing them to see what is happening within the substation before they enter and reducing the possibility they will be ambushed by intruders.

Within the substation, utilities also have the ability to defend individual assets using solutions such as modular ballistic barriers or ballistic plate steel transformer wraps.

"We're seeing more and more ballistic walls being used on our system integration testing projects, specifically for transformers," Pfaff said. "You can put them up next to the transformer to reduce the overall visibility of the asset, and since they are modular, you can set them up in a loose design, or move them up and down to ensure good airflow."

Staying Ahead

"Our biggest problem in security is we're always one step behind," Pfaff said. "For the future, we are looking at inputting our digital twins into virtual reality programs so we can have people who are trained in military tactics try to attack the substation in a simulation."

This will allow utilities to better understand their specific vulnerabilities when it comes to coordinated attacks. Pfaff also emphasized the untapped potential of critical infrastructure protection (CIP) teams in both brownfield and greenfield substation construction projects.

"Our CIP specialists could really help out if they were brought into the site-planning and engineering process earlier," he said. "Designers don't often think like bad actors, but they [CIP specialists] do. We can run analyses using digital twins during the general arrangement and engineering efforts long before construction even begins, and our CIP team can help point out vulnerabilities in as early as the siting phase."

Unfortunately, no substation will ever be 100% protected, but by staying on top of vulnerabilities, utilities have a better chance of detecting and deterring bad actors to defend critical assets. NWPPA

Megan Happel is a content developer, writer, and editor at POWER Engineers, Inc. She can be contacted at megan.happel@powereng.com.