As substation attacks continue, utilities of all sizes are considering their options to protect the grid from malicious individuals and organizations
Photo 1483614 © Chris Hellyar | Dreamstime.com

Unlock CIP-014 For Comprehensive Security

Although NERC CIP-014 applies to critical infrastructure, it has great value as a foundation for building resiliency plans for all substations.

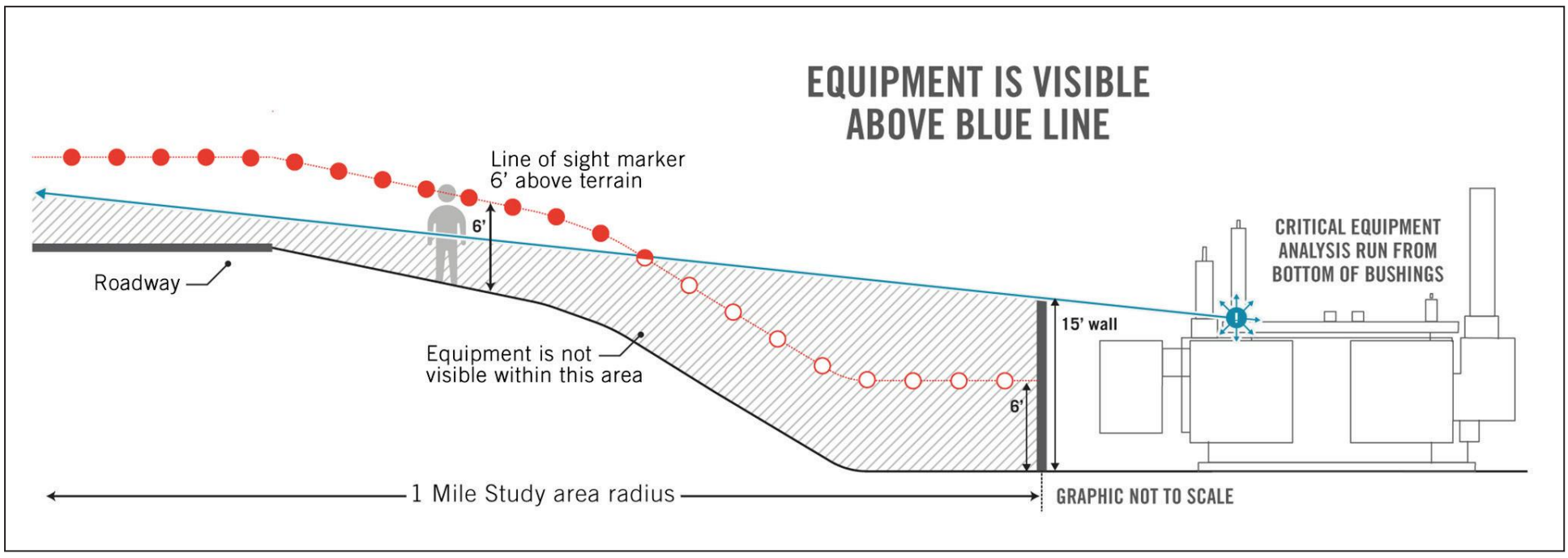
By **MEGAN HAPPEL**, POWER Engineers Inc.

The North American Electric Reliability Corporation Critical Infrastructure Protection standards govern the critical infrastructure of all entities that materially impact the reliability of the bulk electric system. The goal of the Critical Infrastructure Protection (CIP) standards is to ensure appropriate security controls are in place to protect the bulk electric system, along with its users and customers, from threats that could impact the system's timely and effective functioning. These threats may include cyberattacks and physical attacks.

The North American Electric Reliability Corporation (NERC) CIP-014 standard, in particular, was developed to protect transmission stations, substations and their associated primary control centers from physical attacks. If these critical assets were rendered inoperable or damaged because of a physical attack, widespread instability, uncontrolled separation or cascading failure within an interconnection could cut power to millions of users. CIP-014 aims to prevent this by identifying the transmission substations with the greatest need for protection — that is, the substations that would cause the most issues if they failed.

"However, the value of this standard goes beyond keeping critical assets secure," said Chris Ott, physical substation security expert at POWER Engineers Inc. "Those responsible for infrastructure outside of CIP-014's jurisdiction would do well to adopt these security requirements for their out-of-scope systems, too."

While the standard recognizes which assets are most critical, its language on substation security is intentionally vague so as not to give bad actors hints on how to navigate around security systems. However, that ambiguity leads to gaps regarding which substations are considered critical. For example, energy customers like the U.S. Department of Defense, law enforcement,



Line of sight is used to detect vulnerabilities. Graphic by POWER Engineers, Inc.

big tech companies, and medical and health care facilities fall outside of the standard's criteria — yet no one would argue they are critical utility customers that need reliable power.

Unidentified Infrastructure

Regardless of how they are classified, substations with smaller load capacity or lower voltage can adopt the practices CIP-014 requires for critical assets. The criteria may not be exactly the same, but utilities can use CIP-014 to create a risk identification and mitigation strategy.

The NERC CIP compliance standards rate substations deemed critical on a scale of low, medium and high, but an expanded ranking could be applied to substations that fall outside of the standard. Ott of POWER Engineers suggests utilities create five evaluation tiers, applying 1 to the most critical locations and 5 to the least critical. These rankings could be based on factors such as potential lost revenue, outage restoration times, replacement asset availability, public safety, types of customers and public relations mitigation.

For example, a substation that feeds a hospital, a sheriff's department and a big tech customer could be considered a highly critical location from a lost-revenue and service-needs standpoint. Likewise, a location with multiple transformers that have yearslong lead times for replacement might be given a higher

A 3-D generated digital twin. A digital twin, or a 3-D virtual representation of a substation, is a highly accurate tool for finding line of sight. Graphic by POWER Engineers, Inc.

ranking, or priority, than other substations and, therefore, would have its security evaluated earlier. Ranking substations in this way enables utilities to address security concerns at all relevant locations systematically.

Destruction Can Inform Security

Ott applied a five-tiered scale to assets at his former utility, just one tactic he employed to make the substations more secure. Others he developed by drawing on his 20 years of experience, which began in the military.

"My original job in the Marine Corps was to provide power generation and distribution for field expedient camps," he recalled. "Later, I volunteered for a unit that did experimental war game exercises. This unit brought together a variety of experts who used their expertise for mission planning in both real and theoretical cases. For each one, we had to analyze variable locations, infrastructure types and military asset availability before deciding on the most appropriate method to cripple the infrastructure. I was the expert in power distribution."

After Ott left the military, he received an electronics engineering degree, worked as a security system design implementation contractor for many years and eventually found himself at a utility where he became immersed in the commercial utility space.

"I joined that utility shortly after the Metcalf substation attack in 2013, around the time when the CIP-014 standard was first announced," Ott noted. "Because of my military experience and knowledge of how grid architecture and infrastructure worked, I became the subject matter expert of that standard for the company."

Digital Twin Technology

According to Ott, some of the most promising physical substation security solutions in recent years stem from 3-D modeling technology.

"Digital twin technology is a game changer for security," Ott said. "By identifying the line of sight that bad actors might use to cause damage, you can build exactly what's needed, where it is needed."

A digital twin, or a 3-D virtual representation of a substation, is a highly accurate tool for finding line of sight.

"We map out the substation and the surrounding terrain using geospatial technology and reconstruct it in a virtual reality environment within a game engine," Ott explained. "This interactive model then helps us identify the locations outside of the substation where critical assets are visible. We can then manipulate the number, size and location of barriers or other mitigation tactics to test our clients' assumptions and see exactly which changes will be the most effective and efficient in blocking line of sight before we build."

A substation in Austria at night. Utilities should take a calculated and educated approach to mitigations to find the most acceptable balance between security and cost. Photo 262839930 © Wolfgang Spitzbart | Dreamstime.com

In addition to testing the effectiveness of solutions like barriers and landscape alterations, digital twins also can be used to place cameras in and around the perimeter of a substation. The same game engine can help to map out the line of sight of the cameras and identify potential blind spots before they are installed.

Ott describes the experience of viewing a digital twin as similar to that of playing a first-person video game. The user can explore the virtual space freely by moving to view the substation from different angles and distances, as if they were a character in a game. This feature is especially useful when it comes to greenfield substation projects, as users can view and evaluate a substation that does not exist yet through the lens of virtual reality. Brownfield substation projects can benefit from digital twin technology, too, since the technology can be used to virtually manipulate and test the environment without involving real-world materials or build time. It is a revolutionary way to identify and solve vulnerabilities.

That being said, vulnerabilities can change as bad actors find new ways to achieve their goals, which is why "you can't forget to test your mitigations," Ott said. "Whether it be a mock attack or a reevaluation of the property after mitigations are in place, you need to check your work, and you need to check it routinely. Find a trusted and credentialed organization that understands power delivery and where failure points could reside. Hire them to discover your vulnerabilities before a bad actor does."

Spend Only What's Needed

Not every malicious individual with a firearm can land a successful series of rounds on a target past 500 yards (457 m). The experience and training necessary to be reliably accurate at long ranges is expensive, which limits how many people are capable of causing damage from that distance. However, this does not mean the threat is nonexistent. Substation attacks are continuing to happen, and while the cost to completely eliminate line of sight at smaller substations is not always feasible, for many, it could be the very thing that prevents a catastrophe.

"It's better to pay for security upfront," Ott noted, "because if you don't pay for it now, you'll end up paying more for it later."

The December 2022 attack on two Duke Energy substations in North Carolina caused millions of dollars in damages and left tens of thousands of people without power for the better part of a week. Around the same time, another attack targeted four Washington substations, with two of the substations reporting a combined US$3 million in damages and an estimated 36-month period to complete repairs. There has been a disturbing rise in the number of substation attacks, and even a small substation could be the next target. Especially if they are not protected. Utilities should take a calculated and educated approach to mitigations to find the most acceptable balance between security and cost.

"Using a digital twin replication model can significantly reduce the build cost of security-related mitigation," Ott said. "I'd go as far as to say that it would only cost fractions of a penny on the dollar to use a digital twin to test these mitigations compared to what it would cost to test them in real life. In fact, it has been proven to save significant money overall."

By building only what is needed, utilities can reduce construction and engineering costs without sacrificing security.

"I worked on a pilot project that replicated and showed mitigations in this technology," Ott recalled. "Just the pilot saved the company anywhere between $12 million and $13 million because we were able to try out various mitigations and send them to the engineering staff who were able to identify the most cost-effective solution out of the options depicted — without ever breaking ground. This is a huge and viable way to save money."

Looking Ahead

"Unfortunately, the world is not getting safer," Ott observed. "The grid is aging and utilities are looking for the best-cost solutions for solving this problem."

Although CIP-014 applies to critical infrastructure, it has great value as a foundation for building resiliency plans for all substations. As substation attacks continue, utilities of all sizes are considering their options to protect the grid from malicious individuals and organizations. Using technology like digital twins is one way to stay one step ahead of the bad guys. TDW

MEGAN HAPPEL (*megan.happel@powereng.com*) is a content developer, writer and editor for POWER Engineers. She specializes in transforming complex engineering projects into concise, relevant content for a wide variety of audiences and channels. She holds both a bachelor's degree in engineering management and a bachelor's degree in scientific and technical communication from Michigan Technological University.