BURNS McDONNELL

WHITE PAPER / **ELECTRONIC AND PHYSICAL SECURITY IMPROVEMENTS FOR CIP-014**

EVALUATING PROCESS IMPROVEMENTS FOR SUBSTATION SECURITY

BY Robert J. Hope

Securing the consistent operation and delivery of electricity is key to the protection of our everyday life. As threats to substation security evolve over time, utilities need to readjust the implementation process of CIP-014 requirements in order to accommodate the unique substation environment.

Over the last two years, there has been a large shift in the focus and approach to designing the electrical grid to maintain its resiliency and address security. The electrical grid has always been designed with strength in its redundancy. If an electrical transmission line or electrical substation experiences an unplanned outage, the grid will isolate the affected infrastructure and re-route power to the end user as best it can.

The majority of these types of events are caused by acts of nature or the simple failure of equipment and material due to age and stress. Most of these situations are relatively short in duration, but sometimes it takes days. Aging infrastructure and catastrophic acts of nature have always been the greatest threat to the grid.

With the rapidly changing landscape of technology in the United States today, electricity is no longer an item of convenience. Our everyday life and the country's economy depend on the consistent operation and delivery of electricity. Without electricity, our day-to-day lives would be significantly affected and, in some cases, could lead to civil unrest.

In the past, threats to the grid have always been a security consideration, but primarily focused on acts of vandalism and theft. However, the conversation regarding the types of threats to the electrical power system has changed since the attack on PG&E's Metcalf Substation on April 16, 2013. A coordinated and well-planned assault on Metcalf successfully took multiple power transformers offline in a matter of minutes.

This event went relatively unnoticed until an article published by the *Wall Street Journal* in February 2014 detailed the events of the attack. The resulting media attention on the Metcalf event prompted the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC) and the industry as a whole to take a serious look at the security of the electrical grid. FERC, NERC and the electrical utility industry have responded with proper consideration and attention to the grid's physical security by creating CIP-014.

Most utilities that are subject to the compliance requirements of CIP-014 are well underway in the process. Assessments to determine affected sites, as well as threat and risk assessments, have been completed. Through those activities, security plans and implementation schedules were developed and are in the process of being implemented.

The implementation process can lead to difficulties, as many utilities learned that this operating environment is quite different from what they were accustomed to in the past. Not only are there different assessment needs and methodologies, but the recommendations developed in these assessments have introduced means and methods not traditional to the substation environment, requiring a different thought process. These realities, if not managed and properly planned for, can cause difficulty in mitigation option implementation, program longevity and strategy effectiveness.

MITIGATION SELECTION

The CIP-014 process clearly illustrated that the days of walking a site with a clipboard and security checklist may have passed. The operational and political impact from an event can be far-reaching. The threat environment today is very different from the threat environment of 10 or 20 years ago. Threats both domestic and from abroad have become more diverse, and their means and methods of attack have expanded.

Assessment methodologies on CIP-014-regulated sites included threat vectors such as direct fired weapons (e.g., rifles and rocket propelled grenades (RPGs)), as well as improvised explosive devices and vehicle-borne improvised explosive devices. These are methods that were not really considered a mere 10 years ago. While there is no definitive information as to the who and why for the attack on the Metcalf Substation, one thing was clear: there are vulnerabilities inherent to the substation industry that need to be addressed at these high-impact sites to maintain confidence and resiliency in the U.S. grid.

Unfortunately, success in a security program is much like success in a safety program. Success is defined by a non-event. In the safety realm, it is easy to identify existing hazards, mitigation methods and success at the end of the day when no one was hurt and no near misses occurred. Security doesn't have that luxury. The bad guys are not necessarily seen prior to attack initiation. Regardless of this fact, the goal of corporate security is a non-event, i.e., nothing happened today.

Because of these facts, mitigation initiatives need to take into account the operational tempo of the organization, the maturity of the current security to support future plans, and the ability to manage and maintain the security program. Mitigation of vulnerabilities in a diverse threat operating environment can range from complex strategies of sensors and cameras to more basic strategies of walls and barriers, and most commonly in the substation industry, a hybrid of the two.

The R4 Threat and Risk Assessment of CIP-014 is crafted in a manner that enables system operators to implement mitigation options that are congruent with the active threat environment. Regardless of the threat environment, the direction most elected by utilities is to expand their operational control and observation outside of their perimeter eliminate lines of sight to those critical assets that could most affect the station and/or have the longest lead time to restore to service, and eliminate low-impact access to the sites as a whole.

EXPANDING CONTROL AND OBSERVATION

One of the keys of a successful security program is situational awareness. This is most often accomplished by substation operators through increasing their operational control and observation activities outside of their existing perimeters. The goal of this increased awareness is to detect a potential adversary as early as possible, so a response can be initiated that either interdicts the threat prior to the event or responds quickly to minimize the negative effect to the substation, buying security margin. Most often this is accomplished through the use of advanced analytics on both high-resolution infrared illuminated and thermal fixed and pan-tilt-zoom cameras; detection tools such as ground-based radar; and/or other ground- or fence-based sensors (vibration detection). By providing earlier detection supported by assessment tools, such as cameras, the security operations center can make a determination as to friend or foe and initiate the appropriate response.

These technologies are highly technical, require certified integrators to install, program and commission, and need consideration and input from various work groups prior to identifying device locations. Locations can be driven by site constraints, terrain and coverage capabilities of each device utilized. The selected integrator assists with assigning device locations, as well as with the integration of multiple systems for a unified alarm, video surveillance and access control system.

The most common location for these devices is around the site perimeter. This provides the cameras the most unobstructed view outside the perimeter in which to detect if analytics are utilized and/or assess alarms that are received. These locations, while advantageous from a security perspective, can cause issues with nearby facilities in regard to privacy concerns and getting the appropriate power and data to the device, which may require trenching on the site. Additionally, perimeter-based devices may be in close proximity to incoming lines, which can significantly affect the functionality and life cycle of the device. The effects of these incoming lines can vary based on the type and manufacturer. Therefore, it is best to understand the limitations of proposed devices during device layout and location activities.

It is also important to understand that high-resolution cameras can use a significant amount of data and bandwidth. To support this requirement, a full understanding of the communication availabilities or limitations of the site needs to be known. Where shortfalls are identified, alternatives exist, such as microwave, cellular or the potential option of fiber expansion. Other options include considering on-site video storage, which can be recalled as needed, as well as lowering frame rates and resolution to accommodate communication limitations while still meeting the needs of the security organization. Many utilities have separated

the security network from the operational network. This minimizes, or even eliminates, the throttling of bandwidth that can take place during high data traffic periods, which may affect device performance and reduce the number of people who can access the data.

At locations where utilities have identified specific threats and/or site constraints that limit mitigation options, some utilities are looking to implement shot detection. This type of technology can certainly play a role within a security strategy. By detecting a shot, not the negative effects of the impact, operators have the ability to take assets offline in an attempt to minimize asset damage. Once again, these systems are very technical and need specialized assistance in layout, implementation and maintenance.

Lastly, it is important that the security group and the security operations center are capable of monitoring and responding to the alarms. As the numbers of these types of systems and devices increase, the computing capabilities of the workstations in the security operations center will increase to support alarm response The response provided by the security personnel must be supported by clear, maintained procedures. This ensures both the accuracy and continuity of response to alarms at critical sites.

ELIMINATE LINES OF SIGHT AND LOW-IMPACT SITE ACCESS

It was overheard once that substation fencing was 10 percent of the cost and 5 percent of the thought. This was congruent with the time, as our threat model was based on theft, vandalism and trespass. Traditionally, an electrical substation is encompassed by a seven- or eight-foot-tall chain-link fence with a two-inch mesh. Assets within the station can easily be identified and accessed, and there are clear lines of sight for an adversary exterior to the perimeter.

While the threats of theft, vandalism and trespass are still present, the consideration of a more complex adversary needs to be considered, and physical protection starts at the perimeter. Low-impact access is defined as access that can be gained through the use of basic tools, such as snips, or can easily be scaled or climbed. To address this vulnerability, many utilities have elected to proceed with a hardened perimeter that is either a hardened fence or wall-based.

There has been significant debate regarding traditional wall construction with ballistic-rated material when erecting a new perimeter or just around critical assets. The answer really lies in the organization's security strategy and current threat environment. When we examine the events of the Metcalf Substation, we identify that an adversary was moving and shooting, engaging known targets of interest, and adjusting shots where possible based on audible and visual feedback, i.e., the sights and sounds of a leaking or arcing transformer or asset. Should those attributes be eliminated, the act of putting rounds consistently on target to disable an asset becomes much more difficult.

For example, if only a screening wall (non-ballistic) is erected around an asset, it is safe to assume a bullet can pass through the wall and still impact the asset. However, the adversary will not be able to determine if they are even hitting the target reliably or in a critical area, thereby taking away or greatly reducing the audible and visual stimuli. In other terms, we are devaluing the target from the method of engaging an asset with a firearm. While circumstances or site constraints exist that can dictate ballistic-rated material as the best solution, many utilities continue to evaluate alternatives that help manage cost and still provide a high level of protection.

When it is determined that a hardened perimeter is a security tactic to be implemented, the first step is to determine the look, feel and operation of the perimeter system. There is a wide variety of hardening material that can be installed. Some utilities may decide a solid perimeter with 100 percent opacity, and potentially a ballistic rating, is the correct approach. This can be a viable option, as it can either completely or significantly eliminate sight lines to critical assets based on terrain and greatly reduce low-impact site access. However, these types of perimeters can be costly to implement.

Another owner may determine a steel mesh with cut- and climb-resistant properties is the best approach. This type can have the same attributes of reducing lines of sight and low-impact access, but without the ballistic-rated or resistant component. Others may elect to raise the existing fence, use a tighter mesh and place ballistic barriers around those critical assets. There is no right or wrong approach; it just needs to be congruent with the security plan and address the vulnerabilities identified in the R4 assessment.

The final decision should not be made in a vacuum by a single group at a utility. Each owner and operator should engage its engineering, security, permitting, communications, construction, and operations and maintenance departments to arrive at the best solution as they all will have specific concerns. The engineering teams will identify potential conflicts, obstructions, civil features and site access modifications. At the same time, security professionals should also review the site access, potential station vulnerabilities and ideal monitoring locations for security integrators. The permitting team should inform the engineering and security groups of ordinances and restrictions for the locality that could create delays in the construction process.

Once the site review is completed with the project team, the engineering teams will collect all notes and generate the overall security execution plan for the station. This execution plan will detail enhancements to the perimeter, potential perimeter installation conflicts, clearance violations, considerations from the security team and security integrators, modifications required to existing assets and concerns from the permitting specialists. This detailed plan will be the basis for the project moving forward and should be routed for approval to all parties upon completion. Before the execution plan is finalized, additional site surveys may need to be conducted to mitigate identified problems that may cause delays in construction or affect the overall effectiveness of the implemented program.

When the execution plan is finalized, detailed design and permitting will begin. The substation engineering group will modify the station as needed for the installation of the perimeter fence, and the transmission line team will begin the line mitigation process. The permitting teams should promptly convey any findings from local ordinances or requirements to all affected parties. Some cases may need a full site plan review, wetlands and environmental impact studies, or even special use permits that can take significant time to process. Knowing these considerations allows for a more accurate phasing schedule for the project. It is important to understand ahead of time and convey to the affected parties, such as the construction teams, to address the full scope of work, potential required outages and limitations on construction practices dictated by the site and permitting requirements.

Finally, when construction begins, the physical presence of the substation will generate questions from the community, such as what they need to know and whether there are any dangers to consider. A consistent message and communication protocol, such as who on-site to contact for inquiries, needs to be established for all crews working at the station to help maintain message continuity to the public.

CONCLUSION

Protecting our nation's critical assets is a priority today as our threat environment becomes more diverse. This includes the transmission and distribution sector of our infrastructure. Though the steady and consistent delivery of electrical power in the United States is often taken for granted by many, the absence of this resource for an extended period of time could be detrimental to civil order and confidence in the industry. While the events at the Metcalf Substation illustrated vulnerabilities, these vulnerabilities can be mitigated.

There is no panacea to address the issues of substation security. Each utility needs to determine a solution that is right for them to address their threat environment and is conducive to the sites. Threats can adapt and change means and methods faster than most industries can change a security posture. Success comes from taking positive steps to improve a security posture in order to devalue the target to the adversary. While many of these initiatives are new to many entities, through proper advance planning and the establishment of an executable security plan, the improvements can be undertaken successfully.

These improvements are highly visible and require the right team to be successfully planned and implemented. Comprehensive solutions such as these require a team of engineers, security personnel, permitting specialists, communications groups and construction crews to properly execute the project.

Burns & McDonnell has completed many successful substation security projects with a variety of requirements and methods. We have a diverse workforce and can provide all of the resources needed to complete a substation security project from conception to completion. Our teams are composed of security consultants, engineers, permitting specialists, and public involvement and government affairs personnel who deliver a comprehensive package to meet all project needs in one place.

BIOGRAPHIES

ROBERT J. HOPE is section manager for the Security Services Department at Burns & McDonnell. He is responsible for providing leadership and experienced counsel in all areas of security and Threat and Risk Assessments for public and private sector organizations. Robert and his team have taken an active role in many substation hardening efforts across the country specific to CIP-014 and have developed a methodology specific to the regulation and industry. Robert is a sought-after speaker for topics such as NERC CIP, CIP-014, CFATS, force protection and physical security. His team develops all-encompassing security strategies for clients, inclusive of threat and risk identification and evaluation, consequence assessment, electronic security design and implementation support, development of policies, and procedures customized and tailored toward the business and regulatory needs of clients. Robert is a veteran of the U.S. Marine Corps.

12090-CIP-0716