BURNS McDONNELL

WHITE PAPER / **PROTECTING THE GRID FROM EMERGING THREATS**

IMPROVING PHYSICAL SUBSTATION SECURITY WITH COMPREHENSIVE PLANNING AND DESIGN

BY Robert J. Hope, CPP, ABCP, **Keegan Odle,** PE, AND **Shaun Tweed**

With the need for increased substation security on the rise, it has become apparent that an overarching look at a facility's current security plan and future security needs is required in order to optimize the protection of important assets.

Recent occurrences at substations in some parts of the country have raised significant concern about the security of the nation's electrical grid. In response, many utilities have initiated efforts to improve the physical security at their most critical substation facilities.

Substation security encompasses a broad spectrum of solutions that can be customized based on a utility's individual needs. Substation security initiatives must also be congruent with a company's overall security strategy. Major components of substation security include security planning, engineering considerations, and effects on permitting, real estate and the general public. These areas must be addressed before implementation and construction on security updates can begin.

When a utility engages in security planning, the first step is prioritizing assets — determining the need for and level of improvements to substation facilities. Asset prioritization is based on the importance each resource has in relation to continued operation of the grid, critical customers or areas serviced, and a utility's available capital or regulatory constraints.

Once facilities have been prioritized, utilities have a number of improvement options to consider, ranging from minimal changes to major construction. The engineering team evaluates the effects any physical changes might have on the substation site and equipment operation.

Any proposed improvements should trigger a review of permitting requirements and a comprehensive communications effort with public officials, local law enforcement, nearby landowners and other stakeholders.

Burns & McDonnell has assembled experienced teams — security consultants, engineers, permitting specialists and public affairs personnel — to address improvements to substation physical security and support improved protection of the nation's electrical grid by taking a comprehensive approach to increasing substation security.

SOLUTIONS

SECURITY PLANNING

Improving security at a substation is contingent upon many factors. And while there are many approaches to increasing security for substations, there are an even greater number of methods for attacking them. Therefore, given limited time and resources, a utility must prioritize its substations and components within those sites.

Substation prioritization requires identifying sites and components within sites using a pairwise comparison exercise to develop a ranking system based on the key missions of the owner. A pairwise comparison takes into account items such as the service area, specialty equipment on the site, replacement lead time and other metrics identified by the utility. The comparison generates a quantitatively prioritized list of substations based on the utility's specific objectives.

One approach to substation security seeks to conceal critical components within new facilities and to identify ways to improve the security posture of existing stations. The approach for each utility is based on its

A hardened substation might have physical barriers such as opaque fencing and concealing structures around critical equipment.

desired outcome if a security threat were to materialize. Prioritized assets can be secured in many ways, including cameras with event-based monitoring, perimeter detection devices, gunfire location systems or specialized access control devices. The right solution for a utility depends on its current security strategy, regulatory bodies that may govern security initiatives, and how well its current security program can support the initiative.

In addition to electronic security initiatives, many types of crime prevention through environmental design (CPTED) options can be used in conjunction with the electronic security options. CPTED can include ways to obscure assets within a facility through natural barriers such as hedges, clear zones or signage, or through outwardly pointed lighting. Whatever mitigation options are eventually selected, consideration will need to be given to the site permitting and effects on the community.

Physical security also needs to be enhanced with policies and procedures. Utilities should plan threat mitigation options that can escalate or de-escalate based on the ever-changing threat picture. The threat picture for a given substation can change rapidly; flexible security is necessary. An organization's ability to rapidly escalate the security posture of a given substation can enhance the resiliency planning for the individual substation and for the utility overall. Rapid escalation policies and

procedures for internal response and the support of law enforcement are fundamentally important.

When an adversary considers potential targets, many factors come into consideration. Two of those selection criteria are ease of reaching the target and the effect of success. Of these two criteria, a utility has the most control over the ease of reaching the target. Making the approach to a particular asset more difficult can result in a target shift — leading an adversary toward another target that can be more easily approached. While it is impossible to reduce risk to zero, measures can be implemented to motivate a shift away from the utility's critical assets. Unfortunately, in the security field, success is defined as a non-event. This reality can mean security systems are allowed to fall into disrepair. Organizational adherence to established policies and procedures can become degraded. This is why initiatives that are implemented need to fit within the organizational security strategy.

The substation security policies and procedures must be built upon the components of an effective security plan: deter, detect, delay and respond.

- Deter — The ability to prevent an event from happening. This is accomplished by generating a target shift. Tactics include appropriate signage, lighting and changing the physical presence of the facility.
- Detect — The ability to identify an adversary at the earliest possible moment to enable a response. Tools include lighting, motion detectors, cameras and other technology.
- Delay — The ability to put measures in place that slow down an adversary's access to critical assets. These measures need to increase the time required for an attacker to achieve success, allowing adequate response time before significant damage occurs. Measures include anti-ram devices, taller fences, walls or secondary fencing.
- Respond — The physical response to an event. Protocols need to be documented to establish a continuity of response to an event, and they should reflect actions from both internal and local law enforcement responders.

Good policies and procedures that support an overall substation security strategy lead to implementation of that strategy in the field. Implementation requires sound engineering and detailed coordination among the organization's security group, system operators, permitting agencies, the general public and other stakeholders.

ENGINEERING CONSIDERATIONS

Prioritizing substation assets is a utility's first step in developing a security plan to protect its transmission and distribution systems.

Engineers will approach asset protection in substation security in several ways. One option is to locate critical equipment in the substation where it cannot be easily seen or accessed, providing "out of sight, out of mind" protection. This approach supports two of the four basic metrics of a security plan — deter and delay. The easiest and most common method of providing this level of protection is to create a physical barrier between the equipment and its surroundings.

When implementing a physical barrier around critical infrastructure, consider these factors:

- Air-insulated substations use wind and natural air flow to assist with cooling. A physical barrier placed too close to an asset can de-rate the power of that equipment by preventing this air flow.
- Electrical clearances must be scrutinized when installing an asset barrier to consider the effects of corona and potential for flashover, particularly at the extra-high voltage (EHV) level.

If a utility has chosen to protect an asset from gunfire from outside the site, the design should account for the topography around the location. The development of a "design basis threat" through a line-of-sight evaluation at a specified distance around the substation will determine the required height of the physical barrier.

Beyond asset protection, installing monitoring and surveillance equipment at strategic locations in and around a substation can be an effective way to

increase security. The range of available equipment is wide; monitoring systems can be as sophisticated as thermal and motion detecting cameras or as simple as an alarm on an enclosure door. Asset criticality, current security strategy, and supporting policies and procedures will dictate device selection.

Changes to substation footprints or surrounding wall heights might require permitting evaluations or design changes to accommodate required clearances.

High-voltage substations often encompass many acres, creating a large footprint to monitor. Some companies might find that a comprehensive monitoring system isn't feasible. In this case, a substation owner might monitor common access locations and areas of the site that are most vulnerable.

When adding physical security measures to a substation, the considerations include:

- The required communications bandwidth for new monitoring or surveillance equipment. A significant upgrade in these systems will often require additional fiber-optic cable installation. This can be a costly addition to the project but necessary for proper device implementation and detection of an event.
- Hardening of the substation perimeter. The majority of substations are protected with an 8-foot-high chain-link fence. This type of fence protects the public from the substation, not the substation from the public. Attaching fabric mesh to the existing perimeter fencing can create a visual barrier. While this might prevent the public from seeing assets in the substation, it also prevents law-abiding residents or utility personnel from reporting suspicious activity within the substation.
- Increasing the height of the perimeter barrier or replacing the chain-link fence with a more impenetrable material. Implementing these structures requires a detailed analysis of the electrical clearances to existing substation equipment, overhead transmission lines and underground distribution lines. Often, overhead distribution lines will need to be routed underground to exit the site. Additional transmission structures may need to be installed or existing structures may need to be elevated to provide adequate clearance.
- The area below the perimeter fence. Large gaps below the perimeter fence create exposure and opportunity for tunneling. The remedy would be to install a concrete dig-in barrier or to bury the base of the fence fabric below grade. This type of installation can have adverse effects on the site drainage and stormwater runoff plans.

Beyond the fence perimeter, other features can enhance substation security. Large drainage pipes and culverts should be evaluated as access points into the yard. Long access roads with direct paths to substation gates create potential ramming opportunities and site intrusion. Anti-ramming systems are an option if access points and gates cannot be modified. Anti-ramming devices can be as basic as using methods of slowing vehicular speed, or as complex as pop-up barriers at entry points. Once again, current security strategy, asset criticality and available funding will drive mitigation method selection.

Many layers of protection can increase security of a substation to help defend against potential threats. Engineers can evaluate each substation's existing footprint, recommend design solutions and develop individual physical security plans to increase protection at each substation based on the utility's systematic prioritization of each facility.

PERMITTING, REAL ESTATE AND PUBLIC INVOLVEMENT

Just as a utility should perform an asset prioritization to determine which facilities are grid-critical and lack sufficient security, a utility should also conduct an assessment of all local, state and federal permitting, as well as a rights and restrictions review of existing and future real estate needs.

Once potential limitations are identified, utilities should further investigate current and planned projects to determine if their stakeholder engagement strategies will in any way affect the outcome of other critical projects. It is not uncommon for a project to become associated with a completely unrelated second project, resulting in complications for both at the permitting or regulatory level. As such, the utility should include input from internal participants, such as planners, permitters, communications strategists and governmental affairs representatives, when developing the overall project plan. A collaborative, forward-thinking approach to developing this plan can lessen the potential collateral damage or, at the very least, limit the unknown outcomes.

Multiple reviews in the pre-planning phase are recommended so the utility has the necessary data to make the most informed decision on how best to protect its facilities. One such review is to perform a thorough investigation of existing real estate rights and restrictions. This investigation, coupled with a comprehensive analysis of surrounding property values and availability, along with recent land assessment and value comparisons, will better identify land limitations and restrictions as security options are considered. Ultimately, having a complete picture of what the rights are, what limitations exist and how much potential expansion could cost are essential factors in making a sound business case for any physical change in the facility's footprint or ingress/egress.

In addition to the physical land review, detailed stakeholder mapping of all affected property owners within a designated radius of the substation is advisable, along with documenting any other individual or group that might raise concerns about this type of project. The project team should assist in developing a list of potentially high-profile individuals or known concerned parties that might require additional engagement or education regarding the project. Analysis should not only include those believed to be potential opponents to the project but also those who have shown a propensity to be pro-energy and pro-infrastructure. Collectively, this exercise identifies known opponents to utility projects within the service area, potential pro-community-action participants, and any other metrics identified by the client. Security is a sensitive matter and can become a highly visible topic very quickly.

Regardless of which solutions a utility enacts to increase security at its facilities, stakeholder engagement, governmental affairs, proactive legislative action, site permitting, community effects and public perception need to be considered. At some point, the question of "What do you know that we don't?" will be asked. The utility has to balance its facility hardening measures with the government's and public's need to know.

Additionally, if the chosen security measure includes items such as sound monitoring or video surveillance, the utility should anticipate a negative reaction from potentially affected stakeholders. Although cameras, motion sensors and lighting might not require a permit to install, they might affect members of the public who live or work near a substation. For that reason, consideration should be given to the implications any changes could have on the public. Particular attention should be paid to those who live or conduct business near the substation, perhaps within reach of the sound/video equipment. In today's political climate, with growing public interest in corporate and governmental privacy intrusion, potential fallout and methods of responding to or proactively educating stakeholders should be assessed as part of the overall project plan.

In evaluating the tangible permitting requirements, it is important to note that changes to a substation's footprint that might require digging, trenching, or adjustments

and changes to fence heights can require additional non-environmental and environmental permits. These might include land use (conditional/special use), wetland delineation, cultural resources and stormwater pollution prevention plans. Any footprint change to a previously approved site would likely require additional permitting or an amendment to a pre-existing, approved site plan.

The permitting timeline — which can be extensive and complex — should be part of the discussion with the engineers when determining what design changes will be made to increase security at each substation. Depending on the situation, permitting can take from a few weeks to more than a year, and many project-related tasks cannot progress until the project has met all permitting and regulatory requirements. Time is needed for necessary meetings with permitting entities, permit applications and approvals, and to plan and carry out any required public hearings.

Depending on which solutions are to be implemented, meetings with local law enforcement, public officials and residents may need to be incorporated into the schedule. Preliminary meetings with law enforcement will have already occurred when strategies, policies and procedures are developed and modified. Many permits require adherence to guidelines that include multiple meetings with planning boards, where the public can share concerns and ask questions in an open forum. The utility should have an understanding of the level of publicity these forums could receive and evaluate the community's need to know versus meeting the requirements to obtain the requisite permits.

The utility asset owner should be prepared to provide permitting, government affairs and public involvement specialists on every project. Team members should meet with planning boards, elected officials and local law enforcement regarding each project to gather and provide information, develop an action plan, and determine the level and means of communication that will be used to relay project details.

CONCLUSION

Substation physical security is a serious and highly visible issue. Solutions require a team of security specialists, engineers and permitting/land staff to address the comprehensive needs of those projects. Working together, we can improve grid security and continue to provide safe, reliable and affordable service to utility customers.

Burns & McDonnell has a diverse workforce and can provide all of the resources needed to complete a substation security upgrade project from start to finish. 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 of the project needs.

BIOGRAPHIES

ROBERT J. HOPE, CPP, ABCP, is a senior project manager for Burns & McDonnell's Global Security Services group, responsible for helping organizations identify security threats, and evaluate and mitigate risks by implementing sound security measures. With more than 15 years of experience in overall security operations, he specializes in the design, delivery, training and operation of security operation centers and speaks regularly on security topics.

KEEGAN ODLE, PE, is a project director in the substation department of Burns & McDonnell's Transmission & Distribution Group. He is an electrical engineer specializing in the design of electric power substations and has been involved in the design of substations ranging from 12.47-kV to 500-kV. His responsibilities include project management, engineering management, physical substation design, protection and control design, specifications preparation, underground distribution design, and regular communication between clients and vendors.

SHAUN TWEED is an associate and regional practice manager for the Environmental Studies & Permitting Group of Burns & McDonnell, based in Richmond, Va. He assists clients — from electric utilities to governments to private industry — in meeting challenges in the public eye. His responsibilities across the Southeast include meeting needs in electrical transmission reliability and expansion, environmental and non-environmental permitting, community relations and public involvement, land acquisition, GIS services, database and systems support, surplus property disposition, encroachment resolution, and land use planning.

12629-PTG-1016