The critical infrastructure represented by the electric grid is one of the most important assets that modern society depends on. The efforts of both industry and government to create a viable framework for protecting these assets are represented by the guidelines put forth by NERC and NIST, among others. Incidents such as the shootings at the PG&E Metcalf Substation or less-publicized losses of copper at many facilities have brought this subject to the forefront of utility concerns. The focus of this article is the principles of physical security related to the electric transmission or electric distribution substation. The need for a coordinated and integrated approach to both cyber and physical security is acknowledged but is beyond the scope of this article. Many utilities have taken proactive steps to address this critical subject by shifting strategies, investments, and perspectives through implementing the “hardening” of the most critical facilities, not the least of which is the substation environment.

Lessons from Chess
There is great value in adopting a well thought-out strategy for protection versus simply throwing technology and dollars at a quick tactical solution. The first step in the implementation of a protection strategy is a healthy respect for your opponent. A high degree of respect will drive the implementer towards creating a strategy that is, at its core, both effective and flexible. Any implementation has to be executed in such a way that it can easily be changed in both scale and function. Some correlations to the game of chess are very useful to this discussion.

Defense in depth. A defense in depth approach is a key element in both chess and substation security. This is represented in chess by an offensive piece, such as a bishop, being protected by a knight, which is in turn protected by the queen. The principle is that a frontline unit may be overrun or captured but the opponent will also be captured. This creates a deterrence that helps keep would-be intruders at bay for fear of capture or discovery. In addition, the breach of the perimeter doesn’t immediately give the perpetrator access to the desirable assets—more work is required.

Sacrifice. Often a chess player will be willing to sacrifice a pawn, or even a more valuable piece, knowing that the move will position or enable a forward-looking strategy that will achieve an advantageous position. As it relates to substation security, it may be worth positioning and sacrificing inexpensive and less important assets that can draw out and ultimately capture the attacker that is exploiting, stealing, or damaging valuable utility assets. This will “teach a lesson” to others who are observing the success or failure, thereby reducing the incentive to copy the destructive behavior.

Decoy. A chess strategist will always be thinking several moves ahead of the present play. It is clearly too expensive to cover all assets with a full complement of integrated security solutions. Therefore, one strategy should be
to evaluate where to best use available funds to protect the greatest percentage of critical or high-value facilities. However, it doesn’t have to stop there. The chess master might set up his opponent or “get into his mind” by making him second guess the outcome of a play or attack. The same can be done in the substation environment by strategically placing decoys that look just like the fully protected site. The decoy could be a camera placed so as to make the intruder think that a breach will cost him his identity. The utility could also use effective signage to advertise a greater coverage of security cameras and other technologies, giving attackers pause and possibly cause them to move on to a less “protected” facility.

Probing of defenses. Probing of the utility’s defenses is both inevitable and constant. This is true for both cyber and physical probing. An example of physical probing may be moving certain objects or striking certain objects that would generate a response thereby indicating a secure perimeter. Utilities are no longer protected by obscurity. The knowledge and exploitation of critical assets extend well beyond the former employee or even the neighborhood hack and are now part-time and possibly full-time jobs of some rogue nation-states. These new threats are well funded and motivated by a wide spectrum of incentives from fame to ideology to money. Fundamentally, there is no longer a way to gain reprieve from these onslaughts as the threats are sophisticated and relentless. The utility must develop the ability to quickly respond to these probes and continuously evaluate the overall utility’s security exposure.

Practice and patience. The final correlation to chess is that this game is for deep thinkers. People who are strategists, even-tempered (not reactionary), discerning, firm, and continuously learning seem to be the best candidates to successfully implement the needed security strategies. This problem requires much patience, careful planning, a willingness to allocate sufficient funds, and a broad cross-functional support team. Implementation cannot be done in a silo, so the person or organization tasked with this responsibility must be able to structure a partnership across many utility departments. This is every bit as critical as the technology itself. Important partnerships extend to vendors, consultants, as well as utility employees because these relationships will be critical as you find or practice with solutions until the right one for your company is found. Any team that has an individual that is intent on “going it alone” will certainly leave many vulnerabilities in their pathway that will be exploited by a crafty perpetrator.

Technology

Security technology is certainly a critical component of the overall strengthening of the utility’s position regarding its most critical assets. However, any effective utility strategy cannot focus only on the technology but must consider a broader spectrum of solutions that take into consideration many of the strategies described above. By itself, technology can usually be breached. A coordinated and integrated implementation is necessary for the success of any of security system implementation regarding process, procedures, and technology. The traditional methods of simply using perimeter protection, as sophisticated as they may be, are no longer viable by themselves. Today’s solutions must be context-based to allow operators a broader understanding of the threats to which they are expected to respond. A solution that combines the use of video analytics, dual-authenticated access control, surprise lighting, and perimeter detection can be implemented to bring a strong defense in-depth security profile. Additional protection can be added through audio signature analysis, a hardened perimeter, and employee/community awareness.

Access Control

Integrated Access Control is a NERC requirement necessary for medium to high critical sites and is essential to adequately secure ingress and egress at a facility. Again, any additional context that can be assessed around an incident is valuable information. So at a gate entry, for instance, the use of proximity readers, good lighting, and cameras should be the basic components of every design. More complicated and technically advanced models can be found for each component, such as biometrics access readers, but those types of decisions should have been made in the needs-assessment stage of the project. Or as another example, there may be a need to rebuild some of the fence or gate infrastructure to prepare for specialized security solutions such as fiber optics in the perimeter fencing.
Digital Video Management System

The use of a local digital video recording server (DVRS) gives the utility the ability to create an analytic decision matrix necessary for complex boundary algorithms. The benefit to having this computing power located in the DVRS is that the camera video can be analyzed by software that resides in the substation. This allows the utility to maintain a wide range of capabilities and survivability even if the station were to be isolated through sabotage to the communications networks.

A feature that is unique to one of the DVRS platforms that we have used is the capability for integration with the operations-based EMS/SCADA domain by using standard substation languages such as Modbus or DNP. This not only provides a key tool for the asset management process, but also allows security visibility to the system operators on a 24x7 basis.

Even though there may be high-resolution images stored on the local server, the bandwidth used to access this data from the security or systems operations center must be carefully managed. Communications system capacities need to be used sparingly and optimized to conserve bandwidth impact. Some systems allow the user to access lower-resolution images initially to reduce the burden on the wide area communications infrastructure. Higher-resolution images can then be downloaded on demand and as required.

The digital video management system is typically accessed via client application software loaded on workstations with multi-screen monitors for security or systems operations center viewing of the system activity.

A network-attached archive server should be used for long-term backup and storage of the security data. This data can then be referenced as needed by the user or as support for prosecution of attackers.

Video Cameras

There is a very wide spectrum of camera models being used in today’s diverse security environment. These range from infrared, thermal, and optical fixed to pan-tilt-zoom (PTZ) cameras of each variety, with many other variations and combinations available. Several strategies can be employed when locating a camera, depending on the specific areas being covered. In general, it is important to have overlapping zones where each camera is protected by another camera. This allows the operator to see what may have disabled or damaged an adjacent camera. Some customers prefer to have an analog PTZ that can manually zoom in on a given incident. Others have found that high-resolution fixed cameras give better visual detail and then utilize the digital zoom capability to enlarge an item of interest. Generally, the larger the optical sensor in a given camera the higher resolution is available and the better the low-light performance will be. This can be very beneficial as it allows the use of one device over a broader spectrum of conditions without having to deploy multiple devices to cover certain difficult conditions.

Lighting

The lighting platform used for station yard lighting and surprise lighting is very important to the overall security profile. Lighting can be used in many different ways. It can be used to flood an area to give the impression of being monitored. Lighting can also be used to shock or surprise a perpetrator, thereby spooking them and preventing them from continuing their activity. It can also be used on the perimeter only, leaving the interior of the yard cloaked in darkness.

There are also some lighting platforms, integrated with a 360-degree camera, with integral communications to allow coordinated control of other lighting and camera platforms. In addition, some LED lighting units can provide daylight quality illumination (> 83 CRI-True Color) that can significantly enhance the quality of the security images.

Audio

Audio can be used in many ways in the security portfolio of a utility. Audio can be used for real-time on-demand announcements or pre-recorded messages that can be triggered by an intrusion. A more sophisticated use is audio signature analysis, which is typically a post-incident tool but can give valuable information related to future events.

Security Operations Center

The placement of the security operations center, whether at the corporate office or system operations control center, is something that many utilities are addressing. With the regulatory requirement to increase the presence of both access security and video in the operations environment,
some key issues must be considered in conjunction with NERC CIP compliance, specifically as related to cybersecurity. This article, as stated earlier, is focused solely on physical security. However, the technology that enables physical security has to communicate with devices in the remote security operations center. Therefore, any physical security strategy must also comply with the policies and procedures for protecting the network used by the critical infrastructure. This serves to reduce the overall exposure of all aspects of the substation to compromise if implemented correctly.

The best approach to these overlapping requirements is to maintain an open discussion between groups that emphasizes the need to work cross-functionally to accomplish the desired security profile for the company’s critical assets. A collaborative and coordinated approach will serve the utility well as more scrutiny is being placed on classification of utility facilities that should fall under NERC CIP compliance.

Some real value is being pursued by organizations such as the Electric Power Research Institute to utilize new protocols under development, such as Secure DNP. These protocols serve to secure some of the more challenging scenarios, such as integration of serial devices (commonly used in the substation environment) with multiplexed packet-based communication networks. Embracing this approach benefits both utilities and vendors, thereby establishing a common standard across the country. When these standards are adopted, technology can be developed and deployed with confidence.

Choice of Team Members

The choice of team members is a critical aspect of a successful substation security implementation. First and foremost, a clear understanding of the unique and critical operational aspects of the electric utility environment must be in place. Any entity, vendor, or customer who does not fully understand or appreciate this complexity must be avoided. Secondly, there is often development that needs to be accomplished to provide an integrated system. This is especially true as the market changes to provide hardened options in the harsh utility environment. Any group or individual who is unable or unwilling to work across vendor lines or outside of their own environment should also be excluded. Situations such as this can make it very difficult for a project to achieve the comprehensive functionality required by the utility.

Continuous Review

In closing, whatever strategy or method is utilized to implement security, the utility must always be mindful of the constant need to question. A comprehensive and repeated review of principles, scenarios, strategies, solutions, and compromises must be part of a healthy physical security implementation. This will allow the utility to work toward creating the organization that has the necessary internal flexibility that is essential to combating the threats that are facing the utility today.

Stanford D. Torvik, P.E., is a senior communications engineer for TRC Engineers, Inc., a nationwide engineering services company providing power delivery, environmental, and infrastructure engineering services to a host of national clients. He received his BSEE in Communications and Control from the University of Texas at Austin. Stanford grew up on the beaches and rainforests of Madagascar. His daily experience was devoid of modern comforts, which quite possibly influenced his fascination with technology. He has more than 31 years of combined history from the electric utility sector and private business. His extensive executive experience with a background in utility operations, control systems, communications, and IT has served him well in dealing with the myriad of issues facing TRC’s energy utility customers. Torvik can be contacted at storvik@trcsolutions.com or 210.245.3714.

The author thanks Jeffery Fiske, Bill Hawk, and Nicholas Hayden for their contributions to this article.