



A Strategic Framework for Electric Infrastructure Protection

By Randall R. Nason, P.E.

The events of 9/11 caused a turning point in the way we view the protection of our electric infrastructure. The resulting federal directives put in place a robust public and private partnership to address this critical infrastructure. However, the passage of the Energy Policy Act of 2005 (The Energy Bill) in August of 2005 defined a path that will clearly change our current approach to electric infrastructure security. The establishment of an Electric Reliability Organization (ERO) and the shift to mandatory and enforceable security standards require a new level of strategic focus on electric utility security programs.

Historically, the focus on the electric infrastructure began with Presidential Decision Directive 63 (PDD-63, 1998) and continued on with Homeland Security Presidential Directive – 3 (HSPD-7, 2003). The two of these combined called for a joint effort between the public and private sector to protect these largely privately held assets. Specific actions called for included:

- A framework for cooperation between the private sector and federal agencies in pursuing the vital mission of protecting critical infrastructures;
- The U.S. Department of Energy being assigned as the lead agency for the energy sectors; and
- The designation by the DOE of the North America Electric Reliability Council (NERC) as the sector coordinator for the Electricity Sector (ES).

This assignment of NERC as the electric sector coordinator was appropriate and very much in line with their historical role in the industry. As stated on their web site (www.nerc.com) NERC's *mission is to ensure that the bulk electric system in North America is reliable, adequate and secure*. Operating successfully as a voluntary organization since 1968 and relying on reciprocity, peer pressure and the mutual self-interest of all those involved, NERC has helped to make the North American bulk electric system the most reliable in the world.

Current NERC security program guidelines and cyber security standards (CIP-002 through 009) were written in the NERC framework of voluntary adherence in order to contribute to the mutual self interest of the industry. However, with the passage of the Energy Bill and the upcoming identification of the Electric Reliability Organization, (ERO), certain portions of the electric industry may soon be subject to enforceable security standards. While this nothing new to that portion of the industry with nuclear generating resources, this is a new environment for the rest of the industry.

The Electric Infrastructure

Strictly from a physical security standpoint, an electric system can be considered in three categories: power supply, power delivery, and facilities. The power supply category includes the power generation facilities and the associated equipment such as fuel storage or delivery components, power transformers, and heat

dissipation facilities. Power supply facilities contain all of those items that make site security difficult such as:

- **Site Size:** Power plant sites can cover tens and in some cases hundreds of acres. This is the result of generally locating more than one power generation facility on a given site as well as the large areas required for cooling towers, cooling ponds, coal storage yard, and associated coal handling equipment. The large size of most sites can make effective perimeter security difficult to provide in a cost-effective manner.
- **Critical Components:** Power supply sites also contain a number of critical, long lead time items that, if damaged, could result in the power plant facility being out of production for an extended period of time.
- **Large Population:** A power supply facility is a site of constant activity required to keep the generation facilities operating at optimum efficiency. During times of major maintenance outage, the population of the site can increase by several thousand individuals in an effort to keep the downtime to a minimum. This brings into focus all of the security related issues associated with a surge in the site population and the necessary segregation of uncleared contract personnel to only those areas required in the performance of their work.

The power delivery category would include those components necessary to deliver the power from the point of power generation to the consumer. This basically involves a variety of components, the most common of which are transmission and distribution lines and transformers. These transmission and distribution assets represent the most visible, vulnerable, and accessible aspect of the power delivery system. Fortunately, in relative terms, the lines themselves can be easily repaired with minimal disruption to consumers. Conversely, the transformers in the power delivery category are often equally accessible and vulnerable; however, replacement lead times tend to be on the order of months and in certain cases can extend into the twelve to eighteen-month range.

The facilities category is straightforward. The electric grid is dotted with facilities ranging from large corporate headquarters and data centers to small, unmanned buildings in substation yards containing control and protective equipment. Similar to the point-of-presence (POP) sites, so common with long-haul communications, many of these facilities are located in highly remote locations.

How to Secure the System

While the details of the solution to electric infrastructure security are elusive, the general approach and principles are well established and accepted. First, there must be a clear commitment at the corporate level to pursue over the long term an effective program to mitigate the risks to that company's system. Electric utilities, especially those owning and operating nuclear power plants, have long had corporate level security programs; however, the recent emphasis on security as reflected in the recent legislation will require all electric utilities to address security at a higher level. This may involve a complete re-thinking of the current approach to security and the organizational framework supporting the security program. All

organizations will be required to examine critically the experience and capabilities of their staff to handle a quantum increase in the sophistication and importance of their security program. In many cases, additional talent will need to be acquired.

Second, there needs to be a focused effort to categorize all assets according to their risk. Certainly the power supply/generating facilities would be at the top of the list in terms of risks because of their embedded investment, vulnerability to disruption, impact on system operation and continuity of power delivery, and long lead time to repair. Conversely, distribution feeders would be toward the low end of the list because they have very little impact on business continuity, and require minimal capital investment and lead time to repair. Sorting out all of the other components in between is where the challenge lies and where it will be essential for utility personnel to be involved in the process.

Third, facility category specific design standards will need to be developed to address the specific risk and facility features represented in that category. As a broad example, the standard designs for the power supply/generation facilities will need to include everything from integrated access control and CCTV assessment/surveillance to ballistic protection around critical components, perimeter fencing, and lighting. Simply checking an individual's identification badge at the entrance to the plant will no longer be acceptable. In developing the design standards, it is imperative that a clear threat definition be developed in order to drive the standard design development. Very simply, unless a threat is defined, there can be no sense of sufficiency (qualitative or otherwise) of the resulting standard designs. There must be some sort of benchmark against which a proposed design can be evaluated.

Fourth, each electric utility should look to existing emergency response programs to augment the elevated security posture. A prime example is the utility's response to natural disasters such as tornadoes, hurricanes, or ice storms. While it can be argued that the result of a malevolent attack on a utility system would be quantitatively different from that resulting from a tornado or hurricane, the common point would be the damage or destruction of components critical to the supply of electric power to consumers. Utilities have long relied on system redundancy and a spare parts inventory to address those events promulgated by natural disasters. Improved redundancy schemes and augmented spares stockpiles could be used to mitigate the impact of a malevolent act that could not reasonably be expected to be prevented under current societal and economic conditions.

Fifth, great care must be taken that as these large security projects are undertaken, they are implemented in strict accordance with definitive plans and specifications. As the security industry matures and the ability of our system integration partners increases, there is a general tendency to briefly outline project requirements and then turn the implementation of those requirements over to an integrator for unhindered implementation. Unfortunately, as a consultant, I have received numerous calls from clients describing such a situation in which the outcome was different than expected. Due to the size and complexity of these projects, time and effort must be expended in developing definitive design and specification packages to ensure that the funds expended will result in the necessary increase in security for the utility organization. This is not only a safeguard to ensure that the utility organization obtains the desired result in terms of security system performance, but is also a safeguard for the utility and its ratepayers. In most instances, the state jurisdictional authority over

the electric utility will want to review, and in some cases approve, a definite security plan before the projected expenditures can be placed into the rate base. Any deficiency in the design and implementation process could jeopardize regulatory approval.

Sixth, company-wide security awareness programs should be implemented to ensure that all employees understand the importance of security and their role within the program. Utility organizations need to understand that the enhanced security program will change their culture and it is their responsibility to prepare their employees to understand the

change and to continue to operate efficiently within this new environment. This is especially true in the area of cyber security. While considerable sophistication is required to address the complete spectrum of cyber threats, much progress can be made through prudent practices of the authorized users.

The existing and evolving NERC guidelines provide an excellent framework to guide and nurture the development of enhanced physical and cyber security programs within the electric industry. Actual development and implementation of these programs will be based on well-established

security engineering and design principles. Some electric utility organizations will need to enhance internal capabilities in order to implement and support security programs of this magnitude. This process may be accelerated due to the establishment of an ERO and the adoption of security standards for the industry.

Randy Nason, P.E., is a Vice President of C.H. Guernsey & Company in Oklahoma City, Oklahoma. He can be reached at 405.416.8213 or Randy.Nason@chguernsey.com