Adequate Security Measures Require Extensive Review

David Hilt

The US electric system has become an integral part of our daily lives, so much so that we rarely consider how to live without it. The US Department of Homeland Security, as directed by the White House, has identified the critical infrastructures in the United States. The current list includes 17 critical infrastructures with energy at the top of the list. Indeed, the Department of Homeland Security has also noted that the remaining critical infrastructures require energy to operate.

Of course, the electric grid, while highly reliable, was designed on the basis of serving electric customers, supporting electricity markets, and serving industry’s needs. Today, however, the electric grid itself is integral to our modern society and to our health, safety, and welfare. Recent large-scale system events have focused attention on the resiliency of the electric grid in North America. Simply put, the modern society that we live in cannot exist without the electric grid to supply the services and other critical infrastructures supporting our way of life.

Recent events, including the April 2012 shooting attack on a major 500/230/115-kilovolt substation on the West Coast, have focused the attention of the federal government, regulators, and industry on the need for grid resiliency as well as cyber and physical security. The physical attack event resulted in damage to major power system transformers and cost millions of dollars to repair, in addition to exposing the grid to unnecessary risks. The physical attack incident has reinforced concerns on the part of the federal government, the electric industry, and the public that the electric industry still needs to take additional steps to ensure the physical security of the electric system.

As a result, on March 7, 2014, the Federal Energy Regulatory Commission (FERC) issued an order requiring the development of physical security standards within 90 days, the intent of which is to enhance the resiliency and reliability of the electric grid. This order requires at least three steps:

- Risk assessments must be performed to identify “critical facilities.”
- Potential threats and vulnerabilities should be assessed for those facilities.
- A security plan should be developed to address significant potential threats.

The reliability standard developed by the North American Electric Reliability Corporation (NERC), the FERC-approved Electric Reliability Organization, was approved by FERC with an effective date of July 1, 2015. The standard, CIP-014, Physical Security, will present a number of challenges to utilities, including independent verification of risk and protection plans.

ELECTRIC GRID RESILIENCY

Reliability of the bulk electric system is a well-understood concept, but resiliency is relatively new. Perhaps Terry Boston of PJM has the best analogy for what resiliency means as a concept.
infrastructure investment on the order of $1.5–$2.0 trillion by 2030. Further, in order to avoid power outages from component and equipment failures, analysts believe the industry will repair/replace 0.5–1.0 percent of transmission mileage annually over the next two decades. With approximately 283,000 transmission miles in North America, the annual repair/replacement of 1 percent of transmission mileage, at a cost of approximately $1 million per mile represents nearly $3 billion per year in repair/replacement investment.

In addition, the American Society of Civil Engineers estimates that “the United States will invest $566 billion by 2020 in electricity infrastructure.”

GRID RESILIENCY ASSESSMENT NEEDS

With the level of investment predicted in the transportation and distribution (T&D) infrastructure, the question becomes how to best allocate the resources to gain the most return for the investment in terms of grid resiliency. Owners and operators of T&D systems will need to develop a program that can show measurable improvement in system performance through system planning, design, operations, and preparation for extreme events, while ensuring that costs to implement the program provide a measurable benefit. Such an effort requires a thorough, structured, multistep process to develop a comprehensive grid resiliency program, with each step dependent on the outcome of the previous step. Further, such an effort can provide insights into where to improve physical security and address the risk from a physical attack, such as the attack on the West Coast.

Starting such an effort requires some definition of the goals and objectives of a grid resiliency program—its goals, metrics, and resource needs. Establishing a team is a necessary first step, in order to do the following:

- Review available data
- Identify applicable industry data
- Review and identify preliminary measures of success (e.g., customers impacted, length of outages, frequency of outages, and similar items) that can serve as metrics for the program
- Project and provide detail to the subsequent steps in the grid resiliency effort

This “scoping effort” will determine the data and information needed and what information is
available and will define the overall performance goals for the system on a proactive and reactive basis, based on actual system outage history. This effort will also identify metrics to measure success.

A risk assessment and characterization effort begins with a review of historical system events and identification of the causes of those events from available data. This research will assist in determining if certain events in specific areas of the system are likely or could be considered as imminent for recurrence. Some examples could include hurricanes, lake-effect snow storms, ice storms, patterns for wind storms or tornadoes, flooding, or similar events.

The goals and objectives of a sound grid resiliency program should include five key elements:

- Identification of risks and design criteria
- System planning, design, and equipment and facilities specifications and designs
- Retrofit and maintenance of equipment and facilities
- Operating strategies and training programs
- Recovery planning, equipment and supplies inventory, and training

Key parts of these elements are discussed below.

**IDENTIFICATION OF RISKS AND DESIGN CRITERIA**

Developing a grid resiliency program requires consideration of the types of events that can challenge the resiliency of the grid in the local area of operations, and those events that should be included in the design of the system, equipment, and facilities. To identify the events, an analysis of historical operation is needed. This analysis primarily includes an identification of where those events occurred on the system, and what events are to be included in the design of the system, equipment and facilities.

Risks to the system, based on the types of events, other key infrastructure interdependencies, and system performance (design) criteria can then be identified based on the actual system, using automated tools that analyze the system impacts from the events. These look beyond the traditional single-contingency and extreme-disturbance methods. For large systems, the risks can be different in different parts of the system. Knowledge and data are imperative to assess the risks to the system based on local events.

Physical attacks on key facilities can be evaluated even though they have not occurred through a structured approach. The NERC CIP-014 standard requires a risk-assessment phase to identify the critical facilities that, if rendered inoperable, would result in instability, cascading, or uncontrolled separation. This analysis is not for a single contingency normally used for system planning purposes, but rather for an extreme disturbance. A process will be necessary that will evaluate the risk of instability, uncontrolled separation, or cascading to the portion of the bulk electric system under review.

Such a process may include ranking of criticality relative to the remainder of the interconnection, a review of individual components within the system, a review of the physical design and construction of facilities and the associated vulnerabilities, and identification of elements and components within the identified critical facilities that may need to be further protected.

**PLANNING AND DESIGN FOR RESILIENCY**

Planning and design of the electrical system, equipment, and facilities require an understanding of the events and the potential impacts on the entire grid. Planning and design of the electric system for resiliency using the risks and design criteria is a multistep process. The NERC Transmission Planning Standards include some design basis for single and multiple contingencies as well as consideration of extreme disturbances. Resiliency is about extreme disturbances, and the challenge is determining what systems, loads, and other characteristics should be considered in the design of a more resilient system.

With the key risks to the system and the critical facilities identified, system studies can be completed to improve the system, develop operational plans and equipment specifications, improve facility designs, and assess the appropriate inventory of spare parts and equipment. The processes should include a repeatable and uniform methodology to identify which bulk electric system facilities are most critical to electric system operations and infrastructure security.

To effectively understand grid resiliency, it is equally important to understand the impact of the grid and electric supply to other critical infrastructures and loads. The critical
infrastructures in our modern society are highly interdependent and extremely dependent on the continuous supply of electric energy. Storms as well as physical and cyberattacks may result in significant impacts to other critical infrastructures. When assessing the risk of a physical attack, for example, consideration of the critical loads that may be outaged as a result of the attack should be considered.

Such an analysis is done in addition to the traditional contingency analysis used by utilities and should result in a more appropriate categorization of the risk of outages. Further, traditional contingency analysis may not capture the mutual effects of multiple bus or line outages at a single facility, including those owned by others.

### PHYSICAL PROTECTION

The risk assessment and characterization effort will need to look to possible future events based on the historical data and other potential risks such as a physical attack. While it is not possible to predict when and where future events will occur, it is possible to identify the buses and branches in the system that, as a result of their location, configurations, and electrical characteristics, pose the greatest risk for large-scale outages. These results can then be used to tailor grid resiliency efforts to focus on those facilities with the greatest risk for future events.

To assess the risk of a physical attack, the facilities with the greatest impact or risk based on their ranking can be further focused upon, analyzing components within the facilities that may pose a risk. These can include communication facilities (fiber optic terminations, microwave towers, and other facilities), control wiring (cables, cable ducts, and locations), fencing and visual screening, equipment locations, spare inventory and location, control buildings, and security and monitoring.

### CONSTRUCTING FOR RESILIENCY

New facilities should be constructed with grid resiliency in mind.

Equipment specifications, facility design criteria, and construction practices can be developed to ensure an appropriate level of resiliency. However, the system is not new and is not built to these new criteria. Understanding the current design criteria as well as the condition or health of system components and equipment is a necessary component of grid resiliency programs.

Reviewing any equipment or component failure data, condition and maintenance data, and field inspections provide valuable insights into component-level failure risks. To improve system resiliency based on the condition assessment, priorities can be established based on the risks identified. Further, it may be worthwhile to retrofit some key facilities to meet the revised design criteria for physical protection or other factors (e.g., flood-level protection), enhance inventory and spare equipment at specific locations, and evaluate maintenance practices of certain equipment and facilities.

### SUMMARY

Electric grid reliability is not a new concept, and designing for reliability has taken the industry a long way to ensuring resiliency. However, given the level of criticality of the electric grid to all other infrastructures, additional effort is required to ensure a resilient grid. These steps include meeting the requirements of the NERC CIP standards that establish requirements for cyber and physical security.

Progressive electric utility planners and operators will take steps beyond those required by the standards to ensure resiliency to their customers and stakeholders. These steps include understanding (1) the history and patterns of events on the systems involved, (2) the risk the system and other infrastructures of rendering facilities inoperable, (3) the mutual effect of nearby facilities on the grid for combined outages, (4) the impact to other critical infrastructures and critical loads, and (5) the components within the substations and other facilities that pose the greatest risk. From such an understanding, system planning, facility designs and retrofits, and physical and cyber protection plans can be effectively developed, implemented, managed, and maintained.

Grid resiliency is an ongoing process and will require continual reevaluation to ensure the threats, risks, and hardening measures have not changed. Further, training on the need for grid resiliency should be provided to all involved. Complacency about the grid’s resiliency is easily established due to its high level of reliability but is hard to overcome without periodic training to establish thought processes for resilient planning, design, and operation.