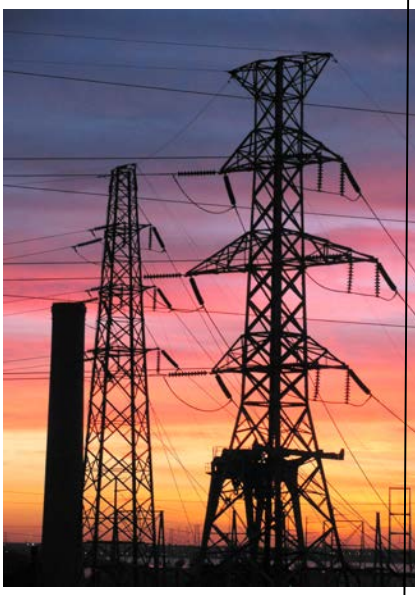

A Reasoned Approach for Risk Identification, Assessment, and Mitigation Strategies for Power System Physical Events

Strategies for Ensuring Compliance with NERC's CIP-014 Standard & A Resilient Grid

February 10, 2015

By: David W. Hilt P.E.
President – Grid Reliability Consulting

Introduction

The Bulk Electric System in North America, and indeed in all developed countries, is critical in order for our modern societies to effectively function. When we consider what would continue to operate without electricity, the need to ensure the continued operation of the electric grid becomes apparent. In short, modern societies have become completely dependent on the availability of electric energy to power everything from water supply to modern medicine and everything in between including the delivery of other forms of energy.

The Department of Homeland Security has recognized the importance of electric power delivery in their classification of critical infrastructures as directed by the President of the United States. In their report, energy is at the top of the list of 18 critical infrastructures and the report includes a note that all 17 other critical infrastructures below it require energy to be functional. According to the Department of Homeland Security:

> *"The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identifies the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the nation.*
>
> *The reliance of virtually all industries on electric power and fuels means that all sectors have some dependence on the Energy Sector. The Energy Sector is well aware of its vulnerabilities and is leading a significant voluntary effort to increase its planning and preparedness."*

This paper discusses a reasoned approach to ensuring the electric grid is resilient protected from physical attack and, by extension, cyber-attack. Protection of the electric grid, clearly one of the most critical infrastructures, involves a number of key stakeholders. The electric grid serves a critical public purpose but is operated by numerous organizations in North America with oversight from regulatory agencies both federal and state. While electric utilities have a key role, it is not their role alone to ensure the electric grid is protected.

In the United States, the Department of Homeland Security and the Department of Defense in addition to the Department of Energy and the Federal Energy Regulatory Commission all have a role in identifying and disseminating threats to the electric grid and protecting the grid from significant threats. Electric utilities also have a key role since their facilities are those subject to potential attack and while utilities cannot protect the electric grid from some types of attack, a reasonable level of protection must be afforded to those facilities that are studied and identified as the most critical. It is necessary to understand where the role of the utilities ends and where the role of the government begins in regards to terror attacks on the electric grid. Electric utilities and the electric system are extremely large, complex, and diverse yet resilient to some degree in design.

However, the system cannot be physically protected from all events. Events such as those that occurred in New York City on September 11, 2001 cannot be prevented by installing barriers or additional security. However, electric utilities should identify their most critical facilities and provide a reasoned and reasonable level of protection from attack, both physical and cyber.

The Federal Energy Regulatory Commission (FERC) on March 7, 2014 issued an Order requiring the development of physical security standards for critical electric grid facilities within 90 days. The intent of that standard is to enhance the resiliency and reliability of the electric grid. The order issued by FERC required 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 be developed to address significant potential threats.

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

The reliability standard as approved requires owners and operators of the Bulk-Power System to perform the following to protect physical security.

1. First, the Reliability Standards requires owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities."

   FERC stated that a critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment.

   To accomplish this task, a screening process in included in the standard and an analysis is required on those facilities passing the screen. However, this paper will discuss not only meeting the letter of the standard, but rather understanding the risk not only to the grid but also to other critical infrastructures served by the electric grid.

2. Second, the Reliability Standard requires owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities.

   FERC noted that the threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target and that owners or operators will need to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated.

The process discussed here will accomplish exactly that and will meet this requirement. To fully accomplish this evaluation requires several actions including; a) site visits and inspection of specific substations; b) review of the design standards and physical layouts; c) assessment of spare inventory and locations; d) assessment of communications, and; e) evaluation of protective relaying, control cabling, etc. From this effort, the components that are most at risk from someone with knowledge of the electric system components and what types of attacks can be realistically contemplated will be identified.

3. Third and finally, owners and operators must develop and implement a security plan to address potential threats and vulnerabilities.

   Based on the information obtained from the relative risk of the facilities and electric system elements and associated components to the bulk electric system and the information from the site visits regarding what can be realistically contemplated, a sound and reasoned physical security plan can be developed.

   Additionally, the standard requires an independent review of the Physical Security Plan.

The electric power systems were built over many decades primarily to serve the needs of customers. The importance of the system as a critical infrastructure has become more acute in recent years with significant weather related events and possible acts of vandalism or even terrorism against the system. Further, the system was not designed or built with a focus on hardening the system against such attacks.

The challenge is to define a process and a reasoned response to the application of this new reliability standard

Getting Started

To begin any journey, it is best to know the destination and then plot the course. The same is true with any project related to physical security of the electric grid and, more importantly, the components that are the electric grid. The following steps are necessary to develop a reasoned approach to grid physical security from physical attack.

1. **Assemble the necessary expertise**

   Electric substations and related facilities are extremely complicated and are comprised of a number of different elements in addition to the high voltage equipment itself. To understand what may be at risk, a number of disciplines will likely be necessary. They include:

   - Management and Customer Service
   - Equipment and Substation Design and Construction
   - Protection and Control

- System Planning and Analysis
- Communications
- Physical Security
- Regulatory
- Remediation/Mitigation Design

2. Identification of goals for physical security

Establishing the goals for physical security is not a small task. The approach can be simply the desire to meet the requirements established in the NERC reliability standard. However, the reliability standard is focused strictly on the impacts to the bulk electric system, NERC's purview. As an electric utility, there are customer, state and local, public health and safety, business continuity, and possible other issues that may be worthy of consideration.

The first task of the team should be to identify the goals for the specific utility, including the need to meet the requirements of the reliability standard.

Several goals can be considered in the event of a physical attack. They include:

- Ensuring service to critical customers and loads

  Loads served by the electric system have differing levels of criticality and may be the actual target of a physical attack on the grid. It would be presumptuous to assume that the goal of an attacker is the utility itself. Utilities considering physical security may want to consider those loads and evaluate the need to ensure the reliability of service to those loads for public health, safety, and welfare, but also for the political and economic impact of interrupting the product or service of the customer.

- Impact on other critical infrastructures

  In addition to the loads considered, in some cases the target may be focused on other infrastructures such as transportation, water and sewer, banking and finance, military, etc. For example, subway and other transportation systems in major metropolitan areas cease to function without electricity. The diagram below depicts the interdependencies in an urban area[1].

[1] Critical Infrastructure Interdependency Modeling: Survey of U.S. and International Research – Idaho National Labs - August 2006

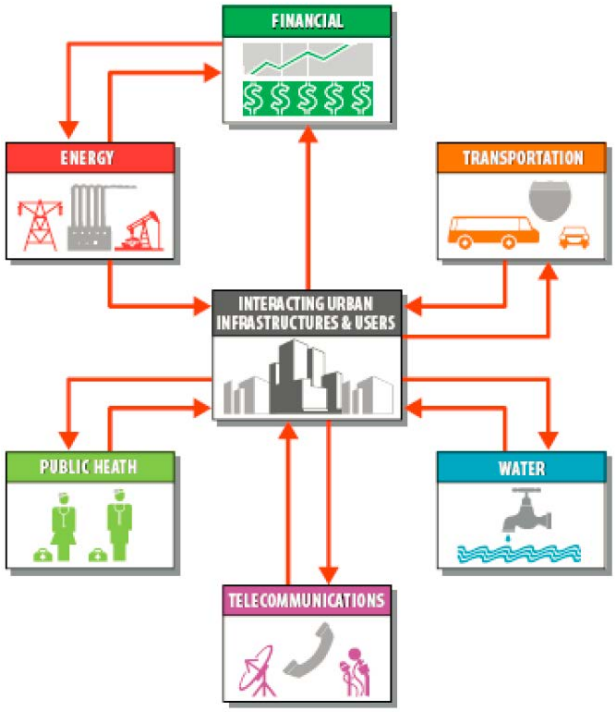

Figure 1 – Infrastructure Dependencies

- Minimizing restoration time

  While the electric grid has been designed to account for single contingencies and blackstart and emergency operation plans have been developed, the assumptions for such a scenario following a terror attack are likely to be significantly different. The strategy for system spares and spare parts inventory will also likely be different.

- Compliance with the NERC Reliability Standard

  Compliance with the reliability standard should be a goal but not the primary goal. If utilities do sound threat and risk assessments followed by development of physical and cyber protection plans, compliance with the NERC reliability standards can be assured.

In order to achieve any of these goals it is necessary to evaluate the vulnerabilities and risks of facilities and components to a physical attack and to identify options to harden the appropriate substations and facilities including mitigating the impact against acts of vandalism like the one at Metcalf substation in California.

3. Threat Assessment

Before beginning to assess the vulnerability of the system or facilities and components that make up the facilities, a determination of the types of threats that are to be defended against must be

established. As has been discussed, it is unreasonable to believe that the entire electric grid can be protected from all threats. Even protecting electric substations, control centers, and generating stations cannot be accomplished for all threats from the ground, the air, and electronically. In a reasoned approach, the types of threats will need to be identified. Many utilities and certainly nuclear facilities have been hardened to a substantial degree from vehicular entry, personnel entry, and in some cases from limited ballistic attack. The degree of protection and the physical protection plan will ultimately require a solid understanding of the types of threats that are to be protected against.

4. Risk Assessment

Risk assessments require multiple levels of understanding. One of the highest level risks is the focus of the NERC reliability standard, that is, the risk of electric system instability, cascading, or uncontrolled separation. Such an analysis can be completed with some effort using power system modeling techniques. In accordance with NERC's mission, this goal focuses on the risk to the bulk electric system and bulk electric system reliability. However, such a goal does not recognize the risk factors discussed earlier such.

- Critical loads
- Other critical infrastructures
- Public health and safety
- Business continuity
- System restoration

As an example, the following chart depicts the interdependencies of some critical infrastructures. This chart, produced by Idaho National Labs[2], shows how a simple mapping of the interdependencies is undertaken and an identification of the criticality of the electric system on other infrastructures. In the case of a risk assessment for grid resiliency, including physical security and risk of a physical attack, such an assessment would be useful.

[2] Critical Infrastructure Interdependency Modeling: Survey of U.S. and International Research – August 2006

Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	
		Key: H High M Medium L Low							

C

Figure 2 – Sample Infrastructure Interdependency Matrix

Conducting the Analysis

With the framework for the analysis established, the next series of steps implements the process established with the parameters identified. Of course, the parameters can be adjusted if necessary. The end result will be the identification of the specific facilities at risk, the individual components that pose the greatest risk, and recommendations for developing the physical protection plan. The steps are continuously numbered from above for clarity.

5. Risk to the Bulk Electric System

The risk of instability, cascading, or uncontrolled separation is a well understood concept. NERC's reliability standards related to transmission system planning, the TPL series, will address some of this concept. NERC's CIP-014 Reliability Standard for Physical Security includes a screening to be used to identify the minimum set of facilities to be considered. This

screening is only based on voltage and the number of circuits emanating from the facility. While this can serve as a proxy for criticality, the most critical families to the grid may or may not be identified.

The Transmission Planning series of reliability standards, the TPL Standards, require analysis of the system with no contingencies and single contingencies to preserve the ability to serve all firm loads. The standards also require consideration of delayed clearing of system events to ensure power system stability among other things even for an "extreme disturbance". However these standards do not meet the requirements of CIP-014 for planning purposes. CIP-014 requires the consideration of the impacts to the bulk electric system should the facility become damaged or inoperable. Recognizing that a facility will contain multiple busses and elements, the TPL standards, even for an extreme disturbance, may not have considered the entire facility outage. For example, a major transmission substation may include 500 kV, 230 kV, and 115 kV elements in the facility. The consideration of the impact of a complete outage of these facilities is not required in the TPL standards unless it that scenario is considered as an extreme disturbance by the utility.

One of the key reasons these studies are not undertaken is the probability of such an extreme disturbance has been considered extremely low. Further, the ability of traditional power system analysis tools to quickly and easily analyze such an event is limited.

However, methods exist to identify where the system would become unstable and by extrapolation, any additional elements in that facility would also likely result in instability, cascading, or uncontrolled separation.

Another approach can evaluate the "sensitivity" of a facility to such events based on the power flow and power system stability models by considering the rate of change of key factors in the analysis during steps in the power system stability analysis if there is a desire to further refine the ranking or criticality of the facility. Large instantaneous changes in MW flows and in MVAR flows as well as voltage promote instability and in varying degrees can be used to define additional measures. Such an approach is useful to further categorize or rank the facilities based on criticality. The impact to the electric grid is only one of the factors mentioned above. Such a ranking of criticality may be useful in order to include factors external to the electric grid such as critical loads, impacts on other critical infrastructures, etc. and to capture the impacts of spare equipment inventory and location, blackstart restoration paths, etc. in a defensible and repeatable manner.

6. Evaluate Risks to Critical Loads and Other Infrastructures

Considering the impact to critical loads, other infrastructures including those of the utility itself, and on system restoration is certainly beyond the requirements of the NERC standard. However, from a perspective of prudence recognizing the criticality of the energy delivery infrastructure, consideration of these impacts should be consider as well as from a business continuity perspective. To evaluate the risks to critical loads and other infrastructures, the sample matrix described above identifies the facilities based on an overall electric system

criticality. A specific matrix based on the factors that are to be included in the specific analysis is created identifying each facility considered and its ranking of criticality to the bulk electric system. From that, modifiers to the ranking for consideration of the additional external factors (including black start and system restoration factors) can be developed based on the insight and knowledge of the utility personnel about the system, critical loads, etc. and will serve as an addition to the base electric system criticality to produce an overall criticality ranking of the facilities. Of course, some facilities that may not be required by the NERC standard may be included if there is a basis for their inclusion. The NERC standard will allow such additions based on these factors, but is not required at this time.

This effort considers other real world and interdependent infrastructure risks from a perspective that is greater than the just the bulk electric system. The analysis should also consider factors not previously considered in the power flow analysis including common mode failures and the resulting risk. Examples might include consideration of the loss of communications at a facility, particularly if the facility is a communication hub.

Some factors to be considered include:

- Communication facilities – Communication personnel will need to identify communication paths including those to the control center for voice and data from the substation and include those risks in the assessment and criticality ranking. The impact of outaging the substation and the communication facilities, including other critical infrastructures as appropriate, will be considered.
- Spare Equipment – Loss of major system components can be devastating and the availability and location of spare equipment can influence the criticality of certain elements of the bulk power system. It will be necessary to identify any equipment replacement impacts on the facilities and include those impacts in the ranking of criticality including the possibility of damaging the spare equipment if it is stored on site.
- Blackstart generation and cranking paths – System planning and/or operations personnel may want include all blackstart generation and cranking paths in the analysis and identify the criticality of the substation for restoring the system.
- Protection Systems and Special Protection Systems – Protection systems and special protection systems in place can influence criticality should those systems be disabled or fail by severing communications or other actions such as removing certain input parameters. Furthermore, assessment on how equipment (e.g. transformer) protection to potential events and acts of vandalism affects system vulnerability will be provided.
- Critical loads – Identification of any critical loads that may not be served as a result of the loss of specific facilities or combinations of facilities should be considered. These can include loads including loads serving control and dispatch or call centers.
- Fuel Supply – Loss of natural gas supply can impact generation served from a given pipeline. Many compressor stations no longer operate on natural gas due to environmental regulations and have been converted to electric operation. Consideration of the need to identify any specific issues related to fuel supply as a result of any outages is prudent.

- Mutual Impacts – Often electric utilities are interconnected with potentially other critical facilities in close proximity. While the NERC standard focuses only on one company's facilities, for grid resiliency it would be worthwhile to look at nearby facilities including those of other companies.
- Other factors as deemed appropriate – Each system and utility is unique. This report provides some examples of factors to be considered. Others may be identified and included as appropriate.

7. Identification of Component Risks

Electric substations and other facilities that make up the electric grid consist of many components. These components include everything from the high voltage equipment itself to control wiring and communication equipment. Once the facilities that represent the greatest risk have been identified, an analysis of what might be targeted within those facilities is not only required by the standard, but also necessary to develop an effective physical protection plan. While restricting access to a facility and installing barriers to prevent unauthorized vehicle or personnel entry is one step, it does not necessarily protect the facility from external threats. For example, installing large boulders around the perimeter of a substation may prevent unauthorized vehicle access through the fence, but it may also provide cover for a sniper.

Several key steps are recommended for identification of the component risks within a substation. However, ultimately the facility must be assessed with an on-site visit and will need to be periodically re-assessed.

Substation Design, Equipment, and Protection System Risks

Substation equipment and protection system experts will need to make an assessment of the design standards, if any, of the substations including layout, barriers, cabling, transmission protection and control systems, AC and DC supply, and communications. Much of the initial work can be completed by reviewing design standards, drawings, schematics, and other information available. This information can be used to focus the effort in the field when evaluating the terrain and surrounding area for risk.

On-Site Visit to Identify Specific Components at Risk

Given that each facility is different, in a different location with differing surroundings, it is necessary to visit and evaluate substations and other critical facilities identified in the risk assessment and selected by the processes above to the risk of physical attack. This effort will document substation designs and vulnerabilities of standardized designs as well as each substation visited based on the risk raking and vulnerability to the grid identified above. The risk from attack for the various substation and facilities components including spare equipment, communications, protection, and other elements will be necessary.

Developing the Physical Protection Plan

The NERC Reliability Standard, CIP-014 requires the development of physical protection plan and review of that plan be completed by individuals holding certain physical security credentials. The next step in the process is to engage the physical protection personnel with the design personnel to develop a physical protection plan. Additional fencing, screening, or barriers may be considered along with enhanced monitoring and alarming. Relocation of critical spares and hardening of communication circuit exits may be part of the plan. Also, training of personnel should be a part of the plan as the best security is only as strong as the weakest link. If secured gates are installed and then left open for convenience, the security is defeated.

8. Develop Recommendations for Mitigation of Component Risks and Protection Strategies

Based on the work completed to identify the types of threats to be addressed, the risk to the electric grid and other loads, infrastructures, etc., and the component level risks identified through the review of designs, specifications, drawings, etc., it is now possible to develop specific recommendations for protection of components that have been identified as at risk to a physical attack that can be realistically contemplated. These recommendations will be based on the relative risk of the facilities and electric system elements and associated components to the bulk electric system and the information from the site visits regarding what can be realistically contemplated. The recommendations will include the identification of appropriate protection strategies for the components identified.

From these recommendations a physical protection plan can be developed and implemented.

Conclusion

Developing a sound physical protection plan to effectively protect the electric grid requires a thoughtful and sound process. The process needs to be repeatable and flexible to allow for adjustments to address new and emerging threats. However, the electric utility cannot protect the electric grid from all threats due to the physical size and complexity of the electric grid. Governments must play a role in identifying and mitigating those threats that physical protection at the facilities cannot begin to address.

Utilities, however, should take reasonable and prudent actions not only to the meet the requirements of NERC's Physical Protection standard but also for the integrity of the systems we all depend on and their own business continuity.

The approach described here is a reasoned approach to identifying the goals, threats, and risks, and analyzing their systems, hopefully in conjunction with joint facility owners, and the infrastructure interdependencies to develop a sound physical protection plan.

About the Author

David Hilt has nearly 40 years of experience in electric power system engineering, operation, and regulatory activities. He has been a manager responsible for the design, specification, and

construction of electric substations from distribution to EHV including protective relaying. He has also managed transmission and resource planning activities for a major Midwestern electric and natural gas utility providing expert testimony before FERC and state regulators for transmission expansion and 20 year resource plans. Mr. Hilt has directed the development and installation of state estimation and OASIS systems for a Midwestern Reliability Coordination Center. As a Vice President at NERC, he led the development of the compliance monitoring and enforcement program for the bulk-power system reliability standards in North America working closely with the industry, FERC, and Canadian regulatory authorities. He also developed audit programs and event analysis and investigation prorocess. While at NERC he led the investingation of the August 2003 blackout in the Northeastern United States and Canada providing the technical input to the U.S. – Canada Power System Outage Task Force report and other key system events. Mr. Hilt's recent experience includes assessment of risk from physical attack and grid resiliency with major systems involving major metropolotian areas including the assessemnt of electric systems and individual substations and their components.