TransActions

a Publication of GDS Associates, Inc.

April/May 2014

Introducing the new TransActions...

We've given TransActions a makeover and new look. It's the same newsletter that GDS has been publishing since 1996, just better. Enjoy and read on...

Physical Security Threats and the U.S. Power Grid

SECURITY

Recently, physical security of the electrical power grid was thrust into the national limelight largely due to news media reports about the April 16, 2013 sniper attack on Pacific Gas & Electric's Metcalf Substation in San Jose, California. This well-orchestrated, strategic attack, which included disabling of telecommunications prior to shots being fired, lasted nearly 20 minutes with the last shots being fired 12 seconds after law enforcement arrived. The result of the attack is estimated to be $16 million in damages and a substation rendered inoperative for 27 days. No group has taken credit for this attack and law enforcement has very few leads. This event, coupled with former Federal Energy Regulatory Commission (FERC) Chairman Jon Wellinghoff's comments about the event being considered domestic terrorism, caught the attention of lawmakers. On March 12, 2014, the *Wall Street Journal* published an article by energy reporter Rebecca Smith highlighting the risk to the U.S. power grid if only nine of the country's 55,000 electric substations were to be knocked out by terrorists during a hot summer.[1]

While these recent events have played heavily into the FERC Order RD14-6-000, Directing Filing of Standards (issued March 7, 2014), to the North American Electric Reliability Corporation (NERC), these were only the most visible and highly publicized. The *Wall Street Journal* reported that there were 274 significant instances of vandalism or deliberate damage to electric infrastructure in the last 3 years. Most of the events were mainly linked to metal thieves; however, disgruntled employees and hunters also contributed to these incidents.

More notable events include the deliberate attacks of suspect Jason Woodring on Entergy and First Electric Cooperative in Arkansas. Woodring was indicted by a Federal Grand Jury on November 6, 2013 for his alleged attacks. From August to October of 2013, Woodring systematically sabotaged transmission and distribution facilities owned by Entergy and First Electric Cooperative. While these events, allegedly carried out by Woodring, are well

[1] Smith, R. (2014, March 12). U.S. Risks National Blackout From Small-Scale Attack, Federal Analysis Says Sabotage of Nine Key Substations is Sufficient for Broad Outage. The *Wall Street Journal*. Retrieved from http://online.wsj.com

Look for Us!

Upcoming Conferences

MAY 12-14
AESP Spring Conference
Baltimore, Maryland

MAY 18-21
2014 IEEE Rural Electric Power Conference
Fort Worth, Texas

JUNE 10-12
SAIA Summer Meeting
Biloxi, Mississippi

Upcoming Training Opportunities

MAY 12-16
ADVANCED STAKING TOPIC
Field and Excel Applications of Design Principles
Georgetown, Texas

JULY 22-23
NERC Standard PRC-005: Compliance Management
Chicago, Illinois

Upcoming Webinars

MAY 13
NESC Clearances from Grain Bins and Pools

JUNE 10
NESC Clearances on Structures

JULY 10
NESC Clearances for Joint Use with Communication

known and reported on by the media, there have been many more attacks that the industry is unaware of. These attacks typically have occurred on the oil and gas pipelines and because they are outside of the electric industry, they are not as widely known or highly publicized. The targeting of this critical infrastructure is meant to cause not only physical damage and disrupt economic commerce, but to make political statements.

With all this attention placed on physical security by lawmakers and regulatory agencies, what exactly does physical security mean and what does it entail?

Physical security is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.[2] In a nutshell, physical security describes measures to prevent or deter physical attacks and how to design facilities to be resilient or resistant to attack.

With mounting pressure for lawmakers, the FERC mandated NERC develop a mandatory and enforceable physical security reliability standard, CIP-014 (Standard), for the protection of critical facilities. In Docket No. RD14-6-000, FERC laid out the basic premise of the standard. It requires a **three step process** to physical security which consists of the following:

1. **Perform a risk assessment of their system to identify facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation, or cascading failures of the Bulk-Power System;**
2. **Critical facilities must evaluate potential threats and vulnerabilities to those facilities; and**
3. **Develop and implement a security plan to address potential threats and vulnerabilities.**

Additionally, FERC ordered NERC to develop a procedure for keeping this information confidential while allowing those entities who require access and appropriate oversight to ensure compliance.

NERC has 90 days from posting in the Federal Register to develop and submit the proposed Standard to the FERC. In order to meet the quick deadline, the Standard Drafting Team (SDT) requested and was granted a waiver of certain provisions of the Standard development process, specifically a reduction in the comment and balloting period. In addition, the SDT held a technical conference in Atlanta on April 1, 2014 to get industry input. The SDT applied this input in development of the Standard throughout the remainder of the week. Additional steps taken by the SDT to ensure timely development of the Standard include:

1. **Specific focus on items in the order itself;**
2. **Utilize existing documentation or standards as an initial screening criteria; and**
3. **Synergies in process (such as combination meeting and drafting team development).**

The SDT developed a draft Standard in advance of the April 1, 2014 meeting. The main items addressed in the draft Standard include:

1. **Bright line criteria for what elements need to be evaluated**
2. **Requirement to perform, at least every 30 months, a risk assessment of its transmission substations, through a transmission planning analysis, to identify:**
3. **Require a Transmission Owner to notify a Transmission Operator of a Control Center that has been determined to operationally control a substation that has been deemed critical that is not operated by the Transmission Owner**
4. **Require a 3rd party verification of the risk assessment performed**
5. **Require any identified substation and/or Control Center to be evaluated for potential physical threats and vulnerabilities**
6. **Develop and implement a physical security plan for identified assets**
7. **The physical security plan must have an independent 3rd party review**
8. **Implementation of procedures to protect sensitive and confidential information is required as well**

While it is impossible to predict the exact content of the Reliability Standard, it is very clear entities will need to assess their Facilities to determine if they qualify as a critical facility. Items utilized in the determination of the criticality of the Facilities include: **instability**, **uncontrolled separation**, and **cascading failures that have critical impact on the operation of the interconnection**. **If criticality is determined, development of a physical security plan to defend against threats of attacks, actual attacks, and vulnerabilities is required.**

Most electric utilities have performed Risk Based Assessments (RBAs), as part of NERC Reliability Standard CIP-002, that take into account items utilized in the determination of critical facilities including stability and continued on page 5

[2] *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02, 8 November 2010 (As Amended Through 15 March 2014), p. 205.

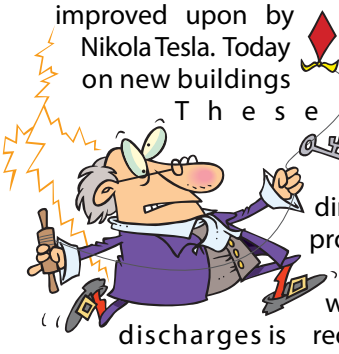
Controlling Lightning Induced Outages On Overhead Lines

Overvoltage protection, often called lightning protection, plays an important role in the design and operation of an electric system. Power distribution systems are asked to perform flawlessly in some of the most hostile weather environments.

For many areas in North America, 20% of all power outages can be directly attributed to lightning. Not only does lightning cause an inconvenience to a customer, it typically damages utility electrical equipment as well as potentially, retail customers' personal residences and electronics. Good lightning protection helps save equipment and reduces outages; while inadequate lightning protection costs money.

Understanding Lightning

In 1749, Benjamin Franklin invented a pointed lightning rod conductor, also called a "Franklin rod," as part of his ground-breaking exploration of electricity. The patent on Franklin rods was later improved upon by Nikola Tesla. Today on new buildings Franklin Rods are still used for lightning protection. These early inventors understood lightning as static electricity which could to a degree be directed safely to earth. In order to protect the electric system from lightning, an understanding of what lightning is and how it discharges is required. During thunderstorm conditions, the positive charges in a cloud tend to migrate toward the top of the cloud while the negative charges concentrate in the bottom. A thunder cloud can be 6 to 7 miles tall, which gives it the capacity to generate a tremendous charge, measured in millions of volts.



Since like charges repel, the negative charges on the ground get pushed away by the force of the negative charges in the bottom of the cloud. This leaves the ground positively charged and since opposite charges attract, the negative charges of the cloud move toward the positive charges of the ground. This first invisible stroke is called the step leader. A negative step leader extends down from the cloud and a positive step leader extends up from objects on the earth. As soon as the negative and positive portions of the step leader connect, the path to the ground is completed and the negative charges race down the path causing a visible lightning stroke, referred to as the return stroke. The fast moving charges conduct until the negative charge is neutralized to earth. Once this has happened, the lightning flash ends.

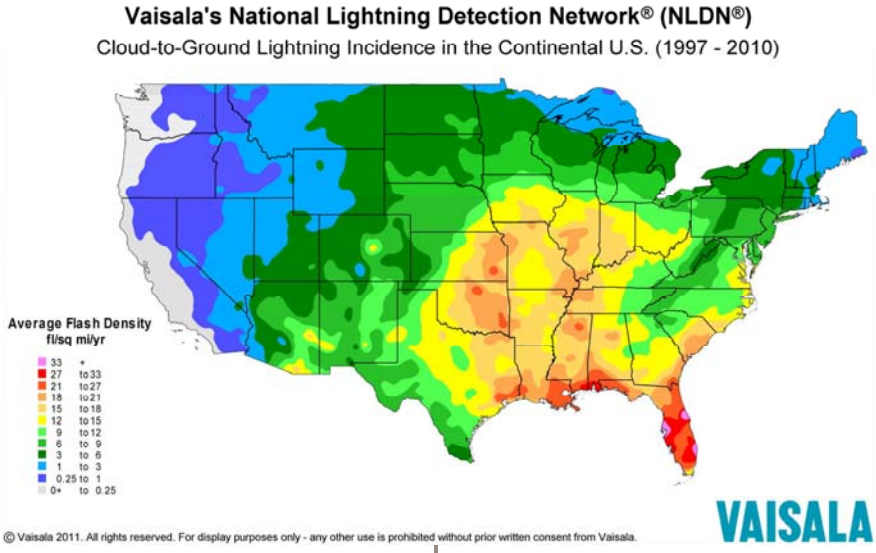


Figure 1: Ground Flash Density for the United States for a period of 1997-2010

Lightning's Electrical Characteristics

When a lightning discharge occurs, electrons flow in the plasma of the lighting. This flow of electrons is commonly referred to as an electrical current. This electrical current is an extremely fast wave of energy. Peak current will occur in 8 micro-seconds (0.000008 seconds or 8 µs). These fast moving waves require lightning arresters to operate extremely fast when subject to a current/voltage surge. Further failures of components on the system occur nearly instantaneously.

Ground Flash Density (GFD)

The frequency of lightning will determine influence an electric utility's investment in lightning protection. For many years a lightning detection network has been deployed in North America. These networks use AM radio frequency to provide detailed ground flash density maps measured in ground flashes per square kilometer per year. In addition this network can provide the date, time, location, number of strokes, and estimated stroke peak current. **Figure 1** is an example of the ground flash density for the United States for a period of 1997-2010.

As the flash density (flashes per square kilometer per year) increases, the likelyhood of a lightning strike to a power line or near a power line increases. Note, that the flash density along the west coast is very low and therefore lightning is

much less likely to occur in California when compared to Florida.

Lightning Strikes to a Distribution Line

Lightning can strike a distribution system in one of two ways. It can strike an object in close proximity to the line resulting in an induced strike, or it can strike directly on the line. Induced voltages are more common than direct lightning strikes. A direct lightning strike to a line will likely result in peak voltage exceeding 1,000 kV which exceeds the typical 300kV insulation voltage of most distribution lines resulting in an insulation flashover which is often described as a ball of fire on the top of the pole.

Because utility poles are not always the tallest structures in the area an electric utility system is more likely to experience an induced strike. Tall trees will shield power lines from direct lightning strikes. A roadway with a power line at the edge of the road right-of-way with a line of trees adjacent to the power line is an example of shielding. Research has shown that a row of 66-foot tall (20m) trees located within 50 feet (15m) of a pole line will provide nearly 100% shielding (i.e. no direct strikes to the power line). However, shielding provided by trees does not mean a flashover will not occur. Lightning can induce voltages onto the distribution system when the lightning strike is near the distribution line. An average lightning strike with 30,000 amps striking an object 100 feet from a theoretical distribution line can induce 350 kV on to the distribution line.

By designing a high level of critical impulse flashover voltage (CFO) of a structure, it is possible for the structure to withstand induced voltage surges from lightning. In general, the goal is to maintain at least a CFO of 300 kV. However, areas with poor soils characterized as having high impedance, will require a CFO closer to 420 kV.

Distribution Line Insulation Level

The CFO is a combination of the insulation capabilities include porcelain insulators, wood, fiberglass, and polymer insulators. Each element has its own insulation strength for fast traveling lightning surges. When the different insulating components are used in series it is important to remember that the resulting insulation is not simply the sum of each component's insulation level.

Obviously, increasing the CFO will improve the lightning performance for both direct and indirect lightning strikes. It is important to properly design the distribution system to maximize the CFO from each element. For example, a simple 12 kV tangent structure where the pole top insulator is in series with 30 inches of the wood when measured from the bottom of the metallic pole top pin to the grounding conductor at the neutral attachment can have a CFO of 285 kV. However, grounded down guys are major factor in reducing a structure's CFO because they are generally attached high on the pole near the phase conductor. This reduces the amount of wood insulation between the phase associated hardware and the grounded down guy. When a grounded guy is attached 15 inches from the phase associated hardware the CFO is reduced to 195 kV. A better design option is to install a guy strain insulator which will increase the CFO of the structure to 300 kV. This simple addition greatly improves the ability of the structure to withstand a lightning flashover.

Spacing of Line Arresters

Adding lightning arresters will further help mitigate flashovers. The closer together the arresters are located, the shorter the distance the current surge has to travel and therefore develops a lower voltage surge magnitude. Lightning arresters can greatly reduce flashovers from induced lightning surges. A spacing of 1,600 feet (every 4th or 5th pole) provides nearly an 80% reduction in flashovers as compared to a line without surge arresters. Decreasing the spacing to 800 feet (every 2nd or 3rd pole) doubles the investment in arresters with little improvement in system performance. For direct lightning strikes, the lightning arresters would have to be placed on nearly every pole to prevent the voltage from exceeding the CFO of the structures.

Conclusion

The combination of a high CFO (greater than 300 kV) coupled with properly spaced lightning arresters will greatly reduce the number of outages caused by lightning. The need for additional lightning arresters and high CFO levels is dictated by the ground flash density where the line is located and the desire to reduce lightning caused outages. ■

For more information or to comment on this article, contact:

Kevin Mara, P.E.,
Principal Engineer
Hi-Line Engineering
a GDS Company - Marietta, GA

608.354.0188 or
kevin.mara@gdsassociates.com

For a copy of the full lightning presentation by Mr. Mara at the **2014 NRECA TechAdvantage Conference**, visit the GDS website at **www.gdsassociates.com**

power flow. For utilities that have undergone these types of assessments, they should now consider refreshing the results of those assessments as part of an evaluation process to determine physical security criticality. If a physical security criticality is determined, the electric utility should pursue additional studies that may also include Protection System coordination efforts.

...it is still prudent to evaluate your Facilities' vulnerabilities to attacks and develop a physical security plan as part of best practices and enhanced reliability for the retail customers the utility serves.

While the FERC does not foresee a large number of entities' facilities falling into the critical facility classification, it is still prudent to evaluate your facilities' vulnerabilities to attacks and develop a physical security plan as part of best practices and enhanced reliability for the retail customers the utility serves. ■

For more information or to comment on this article, please contact:

John Pasierb, Senior Project Manager
GDS Associates, Inc. - Marietta, GA

770.799.2380 or
john.pasierb@gdsassociates.com

About the author

John Pasierb is a Senior Project Manager with GDS Associates. Mr. Pasierb has extensive experience in access control, security monitoring, operations security, perimeter security, risk assessments, and security surveys. He is a certified law enforcement officer with 14 years law enforcement experience. Mr. Pasierb has attended law enforcement classes on terrorism and homegrown threats.

TransActions is a service of **GDS Associates, Inc.** a multi-service consulting and engineering firm formed in 1986.