PRESCIENT TRANSMISSION SYSTEMS

Leaders in next generation power system concepts

Effective Physical Security for Electric Substations

Authors: Tony Sleva, President; Alyssa Sleva-Horine, Business Manager

Table of Contents

1. **Introduction** 1
2. **Physical Security Threat Types and Incidents** 2
3. **Substation Classifications** 4
4. **SHIELDR Principles** 5
5. **Evaluate the Effectiveness of SHIELDR** 11
6. **Determine Security Enhancements by Risk and Cost** 12
7. **Subject Matter Experts Assess Physical Security Improvements** 13
8. **Consider Physical Security at Nuclear Power Plants and DOD Facilities** 13
9. **Prescient's Perspective** 14
10. **About the Authors** 14

1. Introduction

The electric energy grid is a soft target. Vandals and thieves can look through chain link fences to assess vulnerabilities and locate high value materials. Paramilitary groups can conduct internet research to locate critical substations and view geographical features before conducting near site surveillance. Activists and rogue individuals have access to reports and assessments that electric utilities submit during zoning, siting, and permit hearings. Disgruntled employees have individual access to facilities and a wealth of knowledge of facility weaknesses; they also have experience opening circuit breakers and air break switches, and closing ground switches.

To make matters worse, TV news helicopter flyovers show the actual location of substations that have been vandalized, law enforcement publicizes the street address of facilities when asking for concerned citizens to come forward with information, and subject matter experts reveal information on nightly newscasts that make it easier for saboteurs to develop their nefarious plans.

Sabotage of industrial facilities is nothing new, stretching from the August 16, 1906 dynamiting of the Oregon Iron and Steel Company dam on the Tualatin River, OR, to the December 20, 2020 bombings of the AT&T telecommunications center in Nashville, TN, and well beyond on both ends of history. The electric energy grid has withstood most of its existence with minimal damage, excluding a few noteworthy events. However, with the number of extremist ideas spreading in the United States, electric utilities must rely on more than current physical security standards to continue to provide reliable power over the next 100+ years.

Traditional physical security concepts – Deter, Detect, Deny, Delay, Defend – are largely irrelevant when a single action by a single saboteur can create a multi-state blackout. Instead, electric utilities should implement Prescient's SHIELDR approach to improve physical security at substations. SHIELDR considers realistic physical security risks and costs associated with improvements. It blends substation security requirements with those required by the Department of Defense and nuclear power industry to create an updated approach to physical security.

2. Physical Security Threat Types and Incidents

Attacks on electric utility facilities are increasing. Disgruntled employees, paramilitary groups, activists, rogue individuals, thieves, and vandals present physical security risks at substations. Threat levels vary with economic conditions; civil, social, and political unrest; and the goal of the perpetrator. Physical security measures must be equal to the challenge presented by intruders. For example, threats presented by:

1. A disgruntled employee.

   Fortunately, the probability of a disgruntled employee sabotaging a substation is very low. On the other hand, the risk that a disgruntled employee can successfully sabotage a substation is very high. A disgruntled employee has insider knowledge and access to facilities. He or she can cause cascading conditions by closing one three phase, high voltage ground switch or by opening one three phase, high voltage switch.

   An example of a disgruntled employee sabotaging a facility is Brian Howard, a disgruntled FAA contract employee who sabotaged control center equipment and telecommunications systems in the Chicago Center FAA radar facility in Aurora, Illinois. Mr. Howard's insider knowledge and individual access to facilities allowed him to impart significant damage before any security alert was activated.

   In 2023, violent workplace incidents involving disgruntled employees and disgruntled former employees were reported across the US, including at: PSE&G (Public Service Electric and Gas) in Franklin, New Jersey; Family Dollar in St. Louis, Missouri; California Terra Garden, Inc. in Half Moon Bay, California; FMT Shipyard in Harvey, Louisiana; Top Golf in Denver, Colorado; KFC in Beech Grove, Indiana; Prairie View A&M in Prairie View, Texas; Walmart in Evansville, Indiana; Old National Bank in Louisville, Kentucky; Vandergriff Honda in Arlington, Texas; Redford Union High School in Detroit, Michigan; Department of Streets in Philadelphia, Pennsylvania; VCU Medical Center in Richmond, Virginia; Wendy's in Charlotte, North Carolina; Bar Lucca in Conshohocken, Pennsylvania; Carmel Mountain Post Office in San Diego, California; and 24 Hour Tire in Houston, Texas. Fortunately, only one of these incidents involved an electric utility; however, a risk that spans such different industries is a risk to electric utilities.

2. Paramilitary groups.

   The probability of a paramilitary group sabotaging a substation is hard to define. It can be low or moderate depending on civil, social, and political conditions. On the other hand, the risk that a paramilitary group with an electric utility employee as a member can successfully sabotage a substation is high.

   Paramilitary groups have access to resources, both monetary and intellectual. Their structure, tactics, training, subculture, and function can be similar to those of the professional military. Their members often fervently support and defend their ideology.

   The sabotage of Metcalf Substation in California has the earmarks of a paramilitary group that maintained radio silence before and after the attack.

3. Activists.

   The probability of an activist sabotaging a substation is low; activists are more likely to sabotage less protected grid components, like transmission lines. The risk of success is low, but not impossible. Activists have access to intellectual resources, but their lack of insider knowledge limits the impact of their actions.

   For example, Michael Poulin of Spokane, Washington, a longtime peace activist, was sentenced to 27 months in prison for loosening bolts in the legs of about 20 transmission towers in California, Oregon, Washington, and Idaho. He claimed his goal was to show how vulnerable transmission lines are to terrorist attack.

4. Rogue Individuals.

   The probability of a rogue individual sabotaging a substation is low. The risk of success depends on the effort these individuals make to focus their actions. Several examples of actions taken by rogue individuals have occurred in the last few years, including:

   - Peter Karasev was indicted on October 19, 2023, on two counts of destruction of an energy facility and one count of use of fire or an explosive to commit a federal felony. He allegedly damaged PG&E transformers in San Jose, California on two occasions, Dec. 8, 2022, and Jan. 5, 2023.
   - Two suspected white supremacists were arrested in plot to attack five substations in Baltimore, Maryland in February 2023. Fortunately, these rogue individuals broadcast their plans on social media, and law enforcement was able to apprehend them before they attacked the substations.
   - In July 2020, a drone crashed on the roof of a building adjacent to a substation in Pennsylvania. On October 28, 2020, a bulletin released by the FBI, Department of Homeland Security and National Counterterrorism Center stated that the crashed drone was likely targeting the substation.

     The drone was carrying thick copper wire strung between two dangling nylon cords, likely designed to damage transformers or distribution lines. The camera and memory card had been removed, and other efforts had been undertaken to conceal its origin or ownership.

5. Thieves / Vandals.

   The probability of thieves and vandals accidentally sabotaging a substation is high. Thieves and vandals are opportunists looking for easy targets.

   For example, on December 24, 2023, Jason Wadusky entered Siegfried Substation near Allentown, Pennsylvania to steal the copper windings in a spare 230 KV / 69 KV transformer. Unfortunately for him, he became trapped in the transformer and called 911 for help. The burglary attempt damaged a vital transformer.

It's important to remember that the vulnerability of the electric energy grid changes seasonally, with the greatest risk during hot summer months. Cascading failures are likely to occur when circuit breakers fail to open during fault conditions.

Prescient's approach to substation security, SHIELDR, focuses on preventing a multi-state blackout when a saboteur causes a three phase short circuit on the electric grid.

3. Substation Classifications

Prescient classifies the 76,000 substations within the United States as NERC Critical, NERC Other, and Neighborhood.

1. Approximately 1000 NERC Critical Substations are currently operational in the United States. Physical security of these substations must comply with NERC Reliability Standard Physical Security CIP 014.

   NERC Reliability Standard CIP 014 states that the purpose is:

   > "To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection."

   CIP-014 is applicable to:

   - Transmission facilities operated at 500 kV or higher.
   - Transmission facilities that are operating between 200 kV and 499 kV at a single substation, where the substation is connected at 200 kV or higher voltages to three or more other transmission substations and has an "aggregate weighted value" exceeding 3000.

2. NERC Other Substations, of which there are approximately 5000 in the US, are subject to NERC oversight and other NERC Reliability Standards, such as FAC-008 Facility Ratings. NERC Other Substations do not meet the above listed CIP-014 criteria. NERC Other Substations operate above 100 KV. Physical security at NERC Other substations is at the discretion of the electric utility.
3. Neighborhood Substations operate below 100 KV and are exempt from NERC oversight. Physical security at neighborhood substations is at the discretion of the electric utility. Approximately 70,000 Neighborhood Substations exist throughout the US.

The NERC critical classification, while important from a regulatory point of view, masks the fact that expensive and damaging statewide blackouts can be caused by saboteurs at many substations that are exempt from NERC CIP-014. Prolonged neighborhood blackouts, which damage electric utilities' reputation and customer satisfaction, can be caused by saboteurs at any neighborhood substation.

4. SHIELDR Principles

Prescient has developed an approach to dramatically improve the physical security of electric substations referred to as **SHIELDR**, which is an acronym for **S**trategically **H**arden, **I**solate, **E**xamine on **L**ocation, **D**uplicate, and **R**eact & Recover.

SHIELDR is based on the concept that electric utility security professionals need to consider the knowledge, tools, skills, and motives of saboteurs before selecting methods to deter, detect, deny, delay, and defend components in substations. In other words, preparing for physical security threats by understanding the adversary, their skills, and their motives.

Security professionals need to recognize that substations are different than banks in that bank robbers wait for bags to be filled with cash and then attempt to escape capture. Substation saboteurs, on the other hand, can create a multistate blackout before they exit a substation.

SHIELDR principles acknowledge that vast amounts of data are available on the internet and can be found by any of the threat types outlined in section 2. SHIELDR requires electric utilities to plan for worst case scenarios with strategic, flexible plans that acknowledge limitations. Recognizing that improved physical security is a team effort, SHIELDR requires that many subject matter experts participate.

- **S**trategically **H**arden

  Substation security can be improved by strategically hardening substation infrastructure. For example, place components in neighborhood compatible, low-profile buildings, as seen in Figure 1; provide off street parking for vehicles; install sally ports at access points such as those in Figure 2; and eliminate aerial components within ½ mile of the substation.

  Circuit breakers, transformers, and high voltage switches can be hardened by equipping cabinet doors with three point locking mechanisms and tamper resistant crossbars, as in Figure 3.

  Transformers can be hardened by installing bullet proof heat exchangers like those in Figure 4, motorized transformer cooler isolation valves, and plug–jack, high voltage, electrical connections as seen in Figure 5.

  Prescient's physical security assessments help electric utilities determine the optimal areas to strategically harden substation components throughout their service area.

Figure 1: Neighborhood compatible substation

Figure 2: Sally port with cover - unrestricted area gates open / secure area gates closed.

Figure 3: Control cabinet door with crossbars

Figure 4: Bullet proof heat exchanger (partial view)

Figure 5: Plug-jack connector (replacement for transformer and circuit breaker bushings)

- **I**solate

  Substation security can be improved by isolating redundant components within each substation. This begins with designating service groups (A, B, C, etc.), eliminating line of fire corridors, and installing fire walls, bulkhead doors and electrical isolators (commonly referred to as tie circuit breakers) between service groups. Figure 6 is a satellite view of a neighborhood substation with four transformers in separate vaults.

  Electric utilities should copy the nuclear power industry by physically separating redundant protective relaying schemes, batteries, DC circuit breaker panels, and DC fuse panels. Although the current practice of placing redundant protective relays in the same room and cables for redundant protective relaying schemes in the same cable tray is economical, the risk of common mode failure during an intrusion is significant.

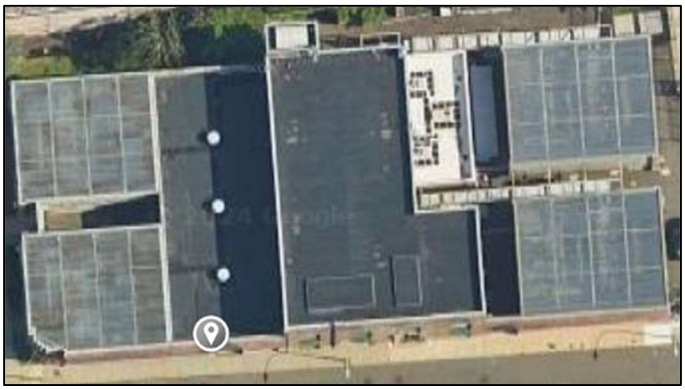

Figure 6: Neighborhood substation with four transformer vaults

The transformer vaults in the neighborhood substation in Figure 6 are equipped with chain link (fencing material) covers. The vaults house transformers, high voltage circuit breakers, and high voltage cable terminations.

Prescient's assessments help electric utilities implement strategic, location specific isolation techniques to enhance physical security of substations.

- **E**xamine on **L**ocation

  The "Examine on Location" step requires electric utilities to perform annual simulated intrusion and sabotage drills. These drills verify the effectiveness of physical security against a disgruntled employee, a paramilitary group, an activist or rogue individual, and a vandal. Drills include the simulated response of local law enforcement, electric utility security, and electric utility linemen and technicians.

  To prepare for simulations and real threats, each substation must have several security features installed: cameras, key card access systems, and position switches on entry doors, gates, cabinet access doors, and removeable panels. Updated regulations should mandate that employees never enter a substation alone, so single person alarms should also be installed.

To perform an intrusion simulation, Prescient's team would act as an intruder, for example as a paramilitary group that had conducted thorough research to determine the ideal substation to attack for maximum damage to the grid and surrounding area. We would present a script with our simulated "plan of attack" to the electric utility's Head of Security. This will ensure that the security department is aware of all steps of the simulation.

Prescient would work with a utility security manager to simulate all aspects of the intrusion per the script. For example, if the script indicates that an intruder can break through a door in 5 minutes, the security manager would open the door five minutes after arrival at the substation on the day of the simulation. If the script indicates that an intruder can climb over a chain link fence in 30 seconds, the security manager would open the substation gate 30 seconds after arrival at the substation on the day of the simulation.

After the simulated intrusion, the security manager would verify that all security features operated as expected: security cameras captured the intrusion; position switches on entry doors, gates, cabinet access doors, and removable panels actuated; key card access systems were operable; single person alarms actuated; and personnel responded as planned, including law enforcement, utility security, and utility linemen and technicians.

These annual "Examine on Location" drills will demonstrate that physical security, including simulated response efforts, meets expectations. The script would simulate substantial damage to the selected substation should security features and personnel fail to respond as expected.

- **D**uplicate

  All transmission class substations should be equipped with redundant protective relaying schemes that are housed in different rooms. All single points of failure should be documented and justified. This will eliminate single points of failure.

  The concern is that an intruder can create a statewide blackout by sabotaging components in a single transmission substation, whether or not the substation is classified as a NERC critical substation. Figure 7 shows a sabotaged substation control house. This was a single point of failure because it was the only control house.

  All neighborhood substations should be constructed so that intruders do not have easy access to more than one service group when they enter a substation. A service group can be a high volage circuit breaker, a large power transformer, medium voltage switchgear, and protective relaying schemes. When a neighborhood substation is equipped with four large power transformers, each transformer should form part of a service group.

  Components in neighborhood substations that can catch fire or that are difficult to replace should be equipped with redundant, physically separated, protective relaying schemes. In open air substations, obstacles (jumbo blocks, bollards, etc.) should be placed between roadways and large oil filled transformers so that automobiles and light trucks cannot be crashed into transformers, whether intentionally or by accident. Figure 8 shows an accidental automobile crash that led to a transformer fire in a 138 KV substation.

Figure 7: Sabotaged substation control house

Figure 8: Automobile crash with transformer fire in 138 KV substation

- **R**eact & Recover

  With increased security features installed at substations, security personnel can monitor substations for intruders and people with unapproved access. In addition, operations staff can easily monitor substations and components. By relying on both alarms and monitoring techniques, intrusions can be detected within seconds.

  In the event of an intrusion at a substation, security personnel would notify local law enforcement and utility linemen and technicians. They should also notify operations staff, who will likely have also detected an intrusion due to their monitoring protocol. Security personnel should have the tools to distinguish between a vandal, a saboteur, and a potentially disgruntled employee.

Operations staff can alert local law enforcement, as well as utility linemen and technicians, if they detect abnormal behavior onsite and have not yet been contacted by security personnel. Operations staff will request onsite assistance and will not enter a substation until security personnel are on site and prepared to neutralize the intruder.

When an intruder is detected in a transmission substation, first responders – security personnel and local law enforcement – should plan to be at the substation within 15 minutes. Utility linemen and technicians should plan to arrive at the same time, but remain outside the substation in a safe location until the situation is deemed safe by first responders. If first responders and utility personnel are unable to respond to an intrusion alert within 15 minutes due to the location of the substation or other factors, the physical security design at the substation should be further evaluated and enhanced.

When an intruder is detected in a neighborhood substation, first responders – security personnel and local law enforcement – should plan to be at the substation within 30 minutes, especially on critical load days. Utility linemen and technicians should arrive at the same time, but wait for first responders to assess the intrusion before entering the substation. If first responders and utility personnel are unable to respond to an intrusion alert within 30 minutes, the physical security design should be further evaluated and enhanced.

In the event that an intrusion occurs at a transmission substation and facilities are compromised, the energy grid must be restored within 24 hours. Utility linemen and technicians first on the scene should have a plan of action to restore the grid within this timeframe. Some facilities may remain out of service until repairs are completed. If the energy grid cannot be restored within 24 hours, the physical security design at the substation should be further evaluated and enhanced.

In the event that an intrusion occurs at a neighborhood substation and facilities are compromised, the functionality of the substation must be restored within 72 hours. Restoration can be via transfers to other neighborhood substations. Some facilities may remain out of service until repairs are completed. If the functionality of the substation cannot be restored within 72 hours, the physical security design should be further evaluated and enhanced.

Prescient's physical security assessment will help utilities who fail to meet the response or restoration requirements of transmission substations or neighborhood substations to further enhance their security measures. Prevention is much better than restoration.

To ensure all threats and intrusions are detected, substation monitoring must occur on a continuing basis, every day. Employees should be notified that new physical security protocols require they are monitored whenever they enter a substation. With single person alarms installed, security personnel and law enforcement will immediately be notified when a person is unaccompanied in a substation for more than five minutes. This will prevent a single disgruntled employee from entering a substation without authorization in order to sabotage it.

5. Evaluate the Effectiveness of SHIELDR

Once an electric utility has implemented new physical security elements based on the SHIELDR principles, Prescient can evaluate the effectiveness of these enhancements. Prescient uses the SHIELDR Effectiveness Evaluation Matrix to determine the updated physical security effectiveness.

Each SHIELDR parameter will be evaluated on a scale of 1-5 and an effectiveness score will be tabulated.

1 – Ineffective
2 – Maybe Effective
3 – Uncertain
4 – Somewhat Effective
5 – Highly Effective

When the SHIELDR effectiveness score is

- 20 or more, physical security is highly effective.
- Between 15 and 20, physical security is effective.
- Less than 15, physical security is ineffective.

The table below is an example of the SHIELDR Effectiveness Evaluation Matrix. This matrix compares the effectiveness of current physical security practices to security practices after electric utilities have implemented SHIELDR principles.

SHIELDR Effectiveness Evaluation Matrix					
	Threat				
SHIELDR Method	Traditional Approach	Disgruntled employee	Paramilitary group	Activist	Thief / Vandal
Strategically Harden	2	4	4	3	3
Isolate	2	4	5	5	3
Examine on Location	1	5	5	5	5
Duplicate	1	5	5	5	5
React & Recover	1	5	4	4	5
Effectiveness	**7**	**23**	**22**	**22**	**21**

6. Determine Security Enhancements by Risk and Cost

Electric utilities want to determine the most strategic enhancements to the physical security of their substations based on potential risk factors and the cost of each enhancement. Enhancing every aspect of every substation will be costly and excessive. Instead, through our physical security assessment, Prescient's team determines specific improvements that electric utilities can implement to alleviate specific risks. Electric utilities can then decide what they prefer to implement at substations, with overall cost in mind.

Prescient's tabulates the potential actions of saboteurs and intruders, and actions that can be taken to improve physical security at substations. The cost of improvements is also considered. Table 1 is an example of such a tabulation.

Table 1: Risks and Improvements to Substation Physical Security

Risk	Recommended Improvement	Cost
Disgruntled employee closes a three phase ground switch.	Replace ground switch ganged drive rods with three individual drive rods.	Low
Disgruntled employee opens a three phase high voltage switch.	Replace high voltage switch ganged drive rods with three individual drive rods.	Low
Paramilitary group uses small weapon fire to puncture transformer oil coolers.	1. Place barriers around transformers. 2. Install motor operated valves in oil lines.	1. Low 2. Moderate
Activist flies a drone dangling a copper wire over a transmission substation.	Connect Kevlar rope between tops of lightning masts and dead end structures so that there is no clear path for a drone.	Moderate
Thief removes ground grid conductors.	Replace stolen conductors with copper clad steel conductors.	Low

The risks outlined in Table 1 have already occurred in the electric utility industry. Intruders and saboteurs will consider incidents that have been reported in other industries to inspire their attacks on the electric power grid.

Some incidents that occurred inadvertently, could be perpetrated by a disgruntled employee. For example, utility employees and contractors have inadvertently closed the wrong three phase ground switch and placed three phase faults on the transmission grid. Similarly, utility employees and contractors have advertently opened high voltage switches before they opened the associated circuit breaker and placed three phase faults on the transmission grid.

Electric utilities categorize costs as Capital Costs that are included in rate bases and Operations and Maintenance Costs that are yearly expenses. The concern is that both Capital expenditures and Operations and Maintenance expenses will increase as physical security increases.

Strategic physical security measures at existing substations can be implemented at less than the cost of a new, enhanced security, perimeter fence. Strategic physical security measures at new substations should be less than 5% of the cost of a new substation cost.

Operating and Maintenance expenses can be minimized by utilizing the services of security professionals, such as EyeQ Monitoring, to provide video surveillance and intrusion detection.

Though both capital and operating and maintenance expenses are important to consider, electric utilities must also consider other important costs: repairing or replacing damaged equipment, settling multi-million dollar lawsuits, and financial losses to customers due to blackouts. Prudent improvements to physical security can be determined based on both the cost to implement enhancements and the potential cost of sabotage-related damages. Prescient helps electric utilities implement the most effective physical security measures in the most cost-effective manner.

7. Subject Matter Experts Assess Physical Security Improvements

Once improved physical security at substations has been designed and implemented, it must be assessed by a team of subject matter experts. These experts should include:

- Civil Engineering Team that evaluates site design.
- Structural Engineering Team that evaluates building and structure design.
- Physical Electrical Team that evaluates component placement and operation.
- Protection and Control Team that evaluates wiring and control scheme design.
- System Operators who establish limiting conditions of operation during normal, maintenance and emergency conditions.
- Security personnel who establish monitoring and react parameters.
- Prescient Transmission Systems to validate SHIELDR security assessments.

The most important feature of the physical security assessment team is the ability to evaluate incidents that have occurred at other electric utilities and at other industries, and apply lessons learned to physical security improvement measures.

8. Consider Physical Security at Nuclear Power Plants and DOD Facilities

Physical security requirements for nuclear power plants and Department of Defense facilities are more exacting than physical security requirements for substations. These requirements should be understood and emulated at electric substations. One key difference is that armed guards are found at nuclear power plants and DOD facilities. However, armed law enforcement that respond to intrusions in a timely manner are key to enhancing physical security at substations.

Like nuclear and DOD physical security regulations, electric utilities must consider overhead accessibility of substations. For example, when a highway bridge is built next to a transmission substation, the transmission substation should be covered so that objects cannot be thrown off the bridge into the substation.

Line of fire evaluations are another important aspect of physical security that are routinely considered by DOD physical security professionals. For example, when a parking garage is built next to a neighborhood substation, line of fire between the parking deck and transformer oil coolers must be evaluated so that a paramilitary group cannot easily shoot at the oil coolers.

9. Prescient's Perspective

Traditional physical security professionals use barrier analysis to establish the effectiveness of the methods they employ. Their focus, and the focus of electric utilities, is minimization of component damage. Their approach assumes that when damaged equipment is isolated from the electric grid, the risk to the electric grid ends.

Prescient uses mesh and node analysis to establish the resilience and robustness of the electric energy grid. The difference is that with mesh and node analysis, the impacts of saboteurs and other perpetrators are considered across a wide area. This approach assumes that when a saboteur closes a three phase ground switch in transmission substation customers are impacted. Fan and pump motors slow down, air conditioner motors stall, and phase angles increase between local and remote generators.

Modifying transmission substations and neighborhood substations to implement the SHIELDR methodology can seem cost prohibitive. However, as electric utilities build new substations and replace aging substations, the SHIELDR approach to improved physical security can be implemented cost effectively.

10. About the Authors

Tony Sleva is a seasoned engineering manager, electrical engineer, project manager, and a thought leader in next-generation power system concepts. His contributions extend beyond leadership, encompassing roles as a continuing education instructor, training program developer, forensic investigator, author, and research engineer. At Prescient Transmission Systems, Tony spearheads the development of innovative services and technologies, focusing on areas such as wildfire risk assessment, power outage prevention, and broader advancements in power system engineering.

Alyssa Sleva-Horine is the lead technical editor and business manager for Prescient Transmission Systems. She is an advocate for climate-friendly, next generation solutions for the electric energy grid.

Prescient Transmission Systems provides consulting services for electric utilities in a variety of areas, including physical security, wildfire risk reduction, renewable energy integration, electric vehicle integration, system modeling, and energy balancing. Our focus is on making improvements to the grid using today's data collection technology more effectively.

As subject matter experts, our staff has assessed equipment failures for electric utilities, energy producers, insurers, and large industrial customers. We are passionate about sharing our vision of the next generation electric energy grid. We see change as an opportunity as we prepare for a future with climate change.