EUCI SYMPOSIUM

ENERGY SECURITY SYMPOSIUM:
Physical and Cyber Security for Power Production and Transmission Facilities

April 3-4, 2018
Courtyard by Marriott Denver Cherry Creek
Denver, CO

POST-CONFERENCE WORKSHOP

CIP-014 Compliance: Protecting the Power Grid from Physical Attack

WEDNESDAY, APRIL 4, 2018

> ***"I am usually reluctant to attend a 1 and a half day conference, but the information provided was excellent. Totally worth my time."***
>
> Manager of Safety & Security, East Kentucky Power Cooperative

TAG US #EUCIEvents
FOLLOW US @EUCIEvents

AUTHORIZED IACET PROVIDER

EUCI is authorized by IACET to offer 1.0 CEUs for the conference and 0.4 CEUs for the workshop.

OVERVIEW

Power companies today face unprecedented challenges when it comes to both physical and cyber security. Given the immense amount of power generated and critical role power generation and transmission facilities play in the nation's infrastructure, the cost of a security breach goes beyond mere financial damage – it can affect the safety of an entire region. For this reason alone, it is imperative for utilities and plant managers to initiate effective security protocols within their operating budgets.

Cyber security attacks on infrastructure targets are happening with increased sophistication and frequency. Each power generation site has a complicated collection of controls that may include both legacy systems and smart assets. Each system presents challenges that range from patching to the introduction of an entire array of not-well-understood vulnerabilities. Many plants are old, and upgrading them is more than a simple matter of adding new technologies. Old systems may need to be replaced or upgraded as well. When new technologies are built on top of legacy systems, new risks may emerge as different systems interact. Companies are taking a proactive approach to cyber security known as threat hunting which

The Energy Security Summit gives plant managers, plant operators, heads of physical, cyber and corporate security a full understanding of what is at stake when it comes to securing their plant and how they can ensure the safety and security of their operations. The symposium will cover the role of power generation plants and T&D facilities as part of the nation's critical infrastructure. Attendees will learn to recognize the external drivers and regulatory requirements for plant physical security. They will learn to organize their plants and substations for cyber and physical security as well as safety. Attention will be paid to how to assess and upgrade a facility's current security organization. Experts will review how to apply cyber security guidelines and advanced technologies for power generation and transmission security programs. Finally, there will be a "utilities Q&A" so attendees can ask their own questions of how utilities are handling their security protocols.

LEARNING OUTCOMES

- Reduce risk by securing critical infrastructure against human, physical, and cyber threats
- Examine costs and benefits of security investments
- Identify mitigation efforts that will ensure rapid recovery of plant operations in the case of security breaches
- Recognize where cyber security and physical security overlap
- Set benchmarks for intrusion detection, perimeter patrol, lighting
- Effectively upgrade security protocols when responsibilities are transferred from one department to another
- Bring older facilities up to current standards
- Explain the role power production and transmission facilities as part of the country's critical infrastructure
- Establish rapid response and recovery protocols in the case of a cyber security breach
- Define current threats to plant security based on recent incidents
- Discuss the intersection between plant safety and security
- Prepare for threats and resolve conflicts

WHO SHOULD ATTEND

Directors of Operations, Heads of Security, Cyber and Corporate Security Managers from Power Generation and Transmission Facilities, Security Companies, Software Companies, Law Firms, and Engineering Firms.

AGENDA

TUESDAY, APRIL 3, 2018

8:00 – 8:30 am **Registration and Continental Breakfast**

8:30 – 9:30 am **Power Production and Transmission as Critical Infrastructure**

More than 80 percent of the country's energy infrastructure is owned by the private sector, supplying fuels to various industries, households and businesses. The energy infrastructure contains more than 6,413 power plants which includes 3,273 traditional electric utilities and 1,738 nonutility power producers with approximately 1,075 gigawatts of installed generation. Electricity generated at power plants is transmitted over 203,930 miles of high-voltage transmission lines. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators nationwide; therefore, it is imperative for owners and operators to collaborate and coordinate to ensure the security and resilience of the grid due to its' complex operating structure and it's critical and essential function across virtually all critical infrastructure sectors. This presentation will discuss:

- Assessing security risks and threats to power plants
- Securing critical infrastructure from all hazards
- Enhancing critical infrastructure resilience
- Sharing information to enable risk-informed decision making
- Adopting, learning, and adaptation in the face of changing conditions

Shawn Graff, Regional Director, Region VIII, Office of Infrastructure Protection, Department of Homeland Security

9:30 – 10:30 am **A Forward Thinking Approach for Developing a Physical and Cyber Security Plan for Low Impact Assets**

Developing a physical and cyber security plan to implement at Low Impact generation sites is an exercise in planning for current state as well as future proofing for changes in physical infrastructure and changing requirements. Existing Low Impact assets have a broad range of capabilities, risks, age in equipment, and operational considerations even within the same entity. Developing an approach to ensure consistency, operational flexibility, and reduce overall cyber and physical risk is a challenge. This presentation will look at using a risk based approach to developing a program to implement Physical and cyber security plans to support existing and future low impact sites.

- Developing a program that supports existing aging low impact assets and future development
- Using a risk assessment to identify controls based on individual sites
- Developing programs that separate controls for physical and cyber security plans
- Implementing controls that can be implemented across high, medium, and low impact assets but scaled to impact level
- Presenting an example using DTE Energy's medium and low impact generations sites implementation program

Mike Reterstorf, IT Manager in NERC Compliance Office, DTE Energy

10:30 – 11:00 am **Networking Break**

11:00 – 11:45 am **Assessing Plant Physical Security: The Newcomer's Perspective**

- Assessing an established organization for security risk factors
- Fortification of existing intrusion detection
- Intrusion detection and monitoring
- Policies and programs
- Integrating company culture with new initiatives

Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority
Justin Allar, Security Systems Supervisor, Platte River Power Authority

AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

11:45 am – 12:30 pm **Intersections: The Overlap Between Safety and Security**

- Regulatory compliance and what drives it
  - o NERC/FERC requirements
  - o OSHA requirements
- Duty to protect employees
  - o Threats of workplace violence
- Emergency management and incident response
  - o Roles of safety professionals vs. security professionals

Jason Maldonado, Security, Emergency Management & Safety Management, Platte River Power Authority
Justin Allar, Security Systems Supervisor, Platte River Power Authority

12:30 – 1:30 pm **Group Luncheon**

1:30 – 2:30 pm **Collaborative R&D in Securing Power Generation**

The increasing sophistication and frequency of cyber security attacks on infrastructure targets is another example of the unprecedented challenges to power generators today. In response, regulations around the globe are requiring an active cyber security strategy for all power generation, significantly more complex than traditional controls network segregation (i.e. "air-gapping").

The core cyber security challenge is that each power generation site is deploying more digital Industrial Control System (ICS) assets from a variety of vendors as a result of obsolescence, and to take advantage of performance gains. These various digital systems and components are more highly integrated than ever before resulting in a larger cyber security attack surface. The rapidly evolving threat landscape and sophisticated ICSs present both a technical and organizational challenge for developing, implementing, and maintaining a successful cyber security program. On top of the numerous technical challenges, cultural and programmatic gaps need to be addressed in a consistent and coordinated approach.

EPRI's Generation Sector has been leveraging industry resources and R&D efforts in the Nuclear and Power Delivery programs to tailor research to power generation. Included in this presentation will be the following:

- NIST Level 4, decentralized hardware-based Remote Access Solution that could streamline management of interactive remote access
- Utilizing proven enterprise architecture techniques to facilitate IT/OT integration in Power Generation
- Research into real-time detection capabilities to better automate threat detection
- A new technical assessment optimization methodology that protects against emerging threats and the added costs of changing regulation
- Collaborative activities with other sectors including resiliency efforts against cyber and EMP threats

Most importantly, EPRI has been developing a community of industry peers dedicated to securing power generation. This presentation will describe how others in the industry can leverage this resource.
Justin Thibault, Senior Technical Leader, EPRI

AGENDA

TUESDAY, APRIL 3, 2018 (CONTINUED)

2:30 – 3:00 pm **Networking Break**

3:00 – 4:00 pm **Confronting Active Shooters in a Utility Setting: Preparing for Threats**
The presentation will provide methods on how to train and drill for an active shooter in and out of the workplace. Some topics that will be covered will include, recognizing signs of an active shooter before an incident happens, how to act on the signs, how to increase your chances for survival in a moment of crisis, and providing tips on how to conduct active shooter drills.

- Active shooter/killer trends
- Active killer response and developing the survival mentality
- Tips on how to perform an active shooter drill

Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District

4:00 – 5:00 pm **Conflict Resolution Training for Utilities**
This session covers conflict resolution in the workplace, primarily teaching how to deal with difficult customers in stressful situations to avoid escalation. Actual footage of events will be used as well as group discussion.

- What training are we giving co-workers to de-escalate dangerous situations?
- Identify stressful situations that employees could encounter
- Determine an appropriate time to contact law enforcement

Tim Kacena, Physical Security Specialist – Investigator, Nebraska Public Power District

5:00 pm **End of Day One**

WEDNESDAY, APRIL 4, 2018

8:00 – 8:30 am **Continental Breakfast**

8:30 – 9:30 am **Threat Hunting for Cyber Risks**
Implementing a complex layered security approach with multiple reporting tools alerting on infections and signatures is no longer an acceptable security approach. Everyone likes to use the words "proactive security" but what exactly does that mean? This talk will go over a proactive security approach known as threat hunting, how it varies from current cybersecurity practices, what it's going to take to implement, and how threat hunting can improve your cybersecurity landscape.

- What is Threat Hunting
- Current Cyber Practices (Reactive) vs Threat Hunting(Proactive)
- Review use cases where this has occurred, where in certain environments a "hack proof" defense can be created
- What's it going to take
  - Analyst functions
  - Network Analysis
  - Host Analysis
- Is this possible in an ICS Environment?

Fred Bonewell, Chief Safety and Security Officer, CPS Energy

AGENDA

WEDNESDAY, APRIL 4, 2018 (CONTINUED)

9:30 – 10:30 am **Implementing Substation Physical Security Risks and Controls**

For years security departments have worked with law enforcement in response to copper thefts from substations. The Metcalf substation ballistic attack in 2013 along with other criminal and terrorist threats have brought to light substation risks and made it clear that robust physical security of substations is needed to protect against disruption of operations. At critical sites, controls must deter, detect, delay, communicate and allow for a prompt response. A defense in depth strategy is required to reduce risks and vulnerabilities associated with unauthorized access to personnel, equipment, systems and materials. This session will cover processes needed to effectively mitigate substation physical security risks:

- To effectively mitigate substation physical security risks:
- Working closely with operational functions to understand and document substations criticality to operations, and tier accordingly
- Identifying and delineating control requirements for each tier considering risks of unauthorized access to substations and operational impacts
- Assessing capital expenditures and subsequent maintenance costs
- Conducting periodic site security assessments to identify new vulnerabilities and tracking any issues that are identified until they are addressed
- Developing processes to continuously assess criminal and terrorist risks that may threaten substations and creating new risks mitigation strategies

Mark Bullock, Director of Security, Commonwealth Edison

10:30 – 11:00 am **Networking Break**

11:00 am – 12:00 pm **Mitigate Risk to Generation Assets through an Assessment Program**

Strategic enhancements to the existing Physical Security Assessment process can result in improved analysis of physical security application and risk management at generation facilities. This session covers an approach that was developed to deploy protection measures through corporate governance to minimize security risk.

- To effectively mitigate physical security risks
- collaborate with Business Unit and operational functions to understand and document criticality to operations, and tier accordingly
- Identify and standardize minimum Security Protection Standards as countermeasures elements of the Security Assessment process
- Implement a prototype system to facilitate proof of concept in Security Assessment performance
- Perform periodic Site Security Assessments based on tier to validate protection measures
- Determine acceptable risk tolerance level
- Develop and Implement Program Governance for a uniform methodology of performing Security Assessments to mitigate risk

Michelle Draxton, Manager of Generation Security, Exelon Corporate and Information Security Services

12:00 pm **Symosium Concludes**

POST-SYMPOSIUM WORKSHOP

CIP-014 Compliance: Protecting the Power Grid from Physical Attack

WEDNESDAY, APRIL 4, 2018

12:30 – 1:00 pm **Workshop Registration**

1:00 – 5:00 pm **Workshop Timing**

OVERVIEW

Securing the North American power grid is a top priority for both regulators and utilities. While the industry remains focused on grid resilience, physical security threats remain that could affect generation, transmission, and distribution operations. A coordinated and simultaneous attack on multiple high voltage transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. While adversaries are becoming more informed and highly capable, we will discuss recent physical security events, NERC CIP-014 compliance, and strategies to reduce overall threats and vulnerabilities.

LEARNING OUTCOMES

- Find out what industry is doing today to better protect critical electric infrastructure and identify emerging threats facing substations, generating plants, and energy control centers
- Implement the NERC CIP-014 standard, mitigation strategies, and effective compliance
- Recognize how utilities can incorporate deter, detect, and delay into their physical security program to meet compliance and become a "hard target"

WORKSHOP AGENDA

12:30 – 1:00 pm **Registration**

1:00 – 2:30 pm **Physical Threats to the Grid**
Participants will learn about recent physical attacks against energy infrastructure, including an in-depth analysis of the 2013 California substation shooting, which was the catalyst for the NERC CIP-014 standard. Also discussed will be how to conduct a proper threat and vulnerability assessment that will feed into a comprehensive physical security response plan.
We will Discuss:
- Physical Attack Scenarios
- The April 16, 2013 Metcalf Substation Shooting
- The Insider Threat
- Emerging Threats Including Drones and Civil Unrest

2:30 – 3:00 pm **Coffee Break**

WORKSHOP AGENDA

3:00 – 5:00 pm

Deter, Detect, Delay, Assess, Communicate, and Respond Under NERC CIP-014
Learn how to incorporate the information from a threat and vulnerability assessment and apply it to a mitigation strategy and future road map. Participants will learn specifics about the NERC-014 standard, how to achieve compliance, and ensuring you have properly protected the "crown jewels".
We will Discuss:

- Physical Security Technologies Being Used in Industry
- How to Create a Robust Physical Security Plan
- CIP-014 R4, R5, and R6 Insights
- Engaging the Regulator and Information Sharing

5:00 pm

Workshop Concludes

WORKSHOP INSTRUCTOR

Brian Harrell

CPP, Vice President of Security, AlertEnterprise

Brian Harrell, CPP, is the Vice President of Security at AlertEnterprise, a technology and advisory firm that provides critical infrastructure owners with consultation on physical and cybersecurity protections. He is the former Operations Director of the Electricity ISAC and Director of Critical Infrastructure Protection Programs at the North American Electric Reliability Corporation (NERC) where he was charged with helping protect North America's electric grid from physical and cyber-attack. Brian was a Standard Drafting Team (SDT) member for the NERC physical security standard, CIP-014. Brian has spent time during his career in the US Marine Corps, US Department of Homeland Security, and various private sector agencies with the goal of protecting the United States from security threats. Brian is also a Senior Fellow at The George Washington University Center for Cyber & Homeland Security (CCHS) where he provides insight and analysis on homeland security, counterterrorism, and cybersecurity issues.

REQUIREMENTS FOR SUCCESSFUL COMPLETION

Participants must sign in/out each day and be in attendance for the entirety of the course to be eligible for continuing education credit.

INSTRUCTIONAL METHODS

Powerpoint presentations and case studies will be used throughout this conference

IACET CREDITS

EUCI has been accredited as an Authorized Provider by the International Association for Continuing Education and Training (IACET). In obtaining this accreditation, EUCI has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of good practice. As a result of their Authorized Provider status, EUCI is authorized to offer IACET CEUs for its programs that qualify under the ANSI/IACET Standard.

EUCI is authorized by IACET to offer 1.0 CEUs for the conference and 0.4 CEUs for the workshop.

EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are $139 plus applicable tax. Call **1-303-757-8797** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 5, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

REGISTER 3, SEND THE 4TH FREE

Any organization wishing to send multiple attendees to this event may send 1 FREE for every 3 delegates registered. Please note that all registrations must be made at the same time to qualify.

REGISTRATION
to register CLICK HERE or

Call: 201 871 0474
fax: 253 663 7224
email: register@pmaconference.com/
web: http://pmaconference.com/
Mail: POB 2303 Falls Church Va 22042

Please make checks payable to: "PMA"

PLEASE REGISTER

- ◯ **BOTH ENERGY SECURITY SYMPOSIUM AND POST-CONFERENCE WORKSHOP:** APRIL 3-4, 2018: US $1795
  Early bird on or before March 16, 2018: US $1595
- ◯ **ENERGY SECURITY SYMPOSIUM ONLY**
  APRIL 3-4, 2018: US $1395
  Early bird on or before March 16, 2018: US $1195
- ◯ **POST-CONFERENCE WORKSHOP ONLY**
  APRIL 4, 2018: US $595
  Early bird on or before March 16, 2018: US $495
- ◯ I'M SORRY I CANNOT ATTEND, BUT PLEASE EMAIL ME A LINK TO THE CONFERENCE PROCEEDINGS FOR US $395

How did you hear about this event? (direct e-mail, colleague, speaker(s), etc.)

Print Name | Job Title

Company

What name do you prefer on your name badge?

Address

City | State/Province | Zip/Postal Code | Country

Phone | Email

List any dietary or accessibility needs here

CREDIT CARD INFORMATION

Name on Card | Billing Address

Account Number | Billing City | Billing State

Exp. Date | Security Code (last 3 digits on the back of Visa and MC or 4 digits on front of AmEx) | Billing Zip Code/Postal Code

OR Enclosed is a check for $ _____ to cover _____ registrations.

EVENT LOCATION

A room block has been reserved at the Courtyard by Marriott Denver Cherry Creek, 1475 S Colorado Blvd, Denver, CO 80222, for the nights of April 2-3, 2018. Room rates are $139 plus applicable tax. Call **1-303-757-8797** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 5, 2018 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

Substitutions & Cancellations
Your registration may be transferred to a member of your organization up to 24 hours in advance of the event. Cancellations must be received on or before March 2, 2018 in order to be refunded and will be subject to a US $195.00 processing fee per registrant. No refunds will be made after this date. Cancellations received after this date will create a credit of the tuition (less processing fee) good toward any other EUCI event. This credit will be good for six months from the cancellation date. In the event of non-attendance, all registration fees will be forfeited. In case of course cancellation, EUCI's liability is limited to refund of the event registration fee only. For more information regarding administrative policies, such as complaints and refunds, please contact our offices at (201) 871-0474.