FUNDAMENTALS OF CYBER SECURITY FOR NUCLEAR PLANTS

April 25-26, 2017
Hilton Baltimore
Baltimore, MD

OVERVIEW

Like other parts of critical infrastructure, nuclear power faces cyber security threats, and the Nuclear Regulatory Commission (NRC) has mandated that these threats be addressed ultimately through an agreed upon approach through NEI 08-09. However, because of the dangers nuclear presents, operators face much greater challenges in providing needed cyber security controls for critical digital assets (CDAs). New digital components are being implemented that are challenging many preconceived notions of how technology is used in a nuclear plant. As the options for access and control become more complicated, so does security. Threats are evolving at a rapid pace, and with national security and nuclear safety on the line, the industry is racing to keep up. As the mandatory NRC regulations are being revised to address industry challenges, the industry is still responsible for its plants from design basis threats from cyber security vulnerabilities. Notwithstanding growing questions and concerns from Owner and Utility Boards of Directors over cyber security at their nuclear plants, each inspection of early milestone commitments yields new insight into the NRC's concerns over cyber security in the nuclear industry.

This course is an in-depth introduction to cyber security issues facing the nuclear industry and plant assets today. It is meant as a primer to give the necessary background for all staff to understand the concepts and complexities of cyber security and compliance with NEI cyber security controls.

LEARNING OUTCOMES

- Identify current cyber security threats facing nuclear power plants
- Analyze cyber threats and vulnerabilities
- Define, assess and manage cyber security risk for nuclear plants
- Review and analyze NRC cyber security controls
- Discuss NRC cyber security inspection techniques and interpretations
- Identify key NEI 08-09 implementation strategies
- Discuss the convergence of maintenance/operations/engineering/security/cyber security departments, internal communication strategies and building cross-functional teams

> **"This course provided a stellar introduction with tools, techniques and methodologies that can be integrated into my organization's efforts to bolster our cyber defenses."**
>
> Senior Cyber Security Specialist, Tennessee Valley Authority

> **"This is an excellent, eye opening course which many manager should take to recognize the threats and requirements for mitigation and regulatory compliance."**
>
> Executive Advisor, Canadian Nuclear Safety Commission

AGENDA

TUESDAY, APRIL 25, 2017

12:30 – 1:00 pm   **Registration**

1:00 – 2:30 pm   **Hacking and Hardware – Understanding Cyber Threats to Nuclear Power Plants**
- Current cyber security threats facing nuclear plants
- Common vulnerabilities and consequences
- Predictions of future cyber security challenges

2:30 – 3:00 pm   **Networking Break**

3:00 – 5:00 pm   **The Old and New: A Primer on the Technology Architecture of a Nuclear Power Plant and How It is Changing**
- Core assets and Critical Digital Assets (CDA)
- Levels 1-4
- Integration and containment challenges
- Securing the communications network
- Analyzing cyber threats and vulnerabilities
  - Field equipment and communications
  - Wide-area-network communications
  - Portable Media Devices
  - Vendor access to CDAs

WEDNESDAY, APRIL 26, 2017

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

8:30 – 10:00 am   **NRC 10 CFR 73.54, Regulatory Guide 5.71, NEI 08-09, and NRC Inspection Manual Chapters**

10:00 – 10:30 am   **Networking Break**

10:30 am – 12:30 pm   **Continuation of NRC 10 CFR 73.54, Regulatory Guide 5.71, NEI 08-09, and NRC Inspection Manual Chapters**

12:30 – 1:30 pm   **Group Luncheon**

1:30 – 3:00 pm   **Plant-Wide Cyber Security: Moving Beyond Cyber Security as an IT Problem**
- Alternative controls
- Internal communication strategies
- Building a cross-functional team
  - Roles and responsibilities
  - Cyber across operations/maintenance/engineering
  - Licensing
- Creating a culture of security
- Leveraging plant cyber security for utility or owner NERC CIP requirements

> **"**
>
> *"Very good overview of the cybersecurity issues, regulations and compliance approaches."*
>
> President, Jones Partners, Ltd.

AGENDA

WEDNESDAY, APRIL 26, 2017 (CONTINUED)

3:00 – 3:30 pm　　　　　**Networking Break**

3:30 – 5:00 pm　　　　　**Pulling It All Together**
- Practical lessons learned and techniques for implementing and maintaining a cyber security program for both information technology (IT) and operational technology (OT)
- Addressing cyber security for corporate functions
- Conduct mini-exercises based on potential scenarios

5:00 pm　　　　　**Course Adjourns**

INSTRUCTOR

Robert Schuler
Manager, Cyber Security Strategy, Accenture

Mr. Schuler is a Cyber Security Strategy and Technical Thought Leader with Accenture Strategy in the United States. He has over 19 years of cyber security risk management and systems security engineering experience across multiple industries. Over this period, he has become a recognized expert in cyber security guidance for control systems, including Nuclear Energy Institute (NEI) 08-09 and NEI 13-10.

Mr. Schuler has key expertise in helping industry clients define their needs and translate them into actionable program goals. He has a strong history of guiding teams toward shared agreement, facilitating process refinement, and aligning organizational culture with program expectations.

Mr. Schuler's industry outreach activities have included frequent speaking engagements delivering nuclear and utility control system cyber security courses and speaking on industry panels, where his technical knowledge and interactive style is helping key industry participants reach a shared understanding of cyber security threats, compliance standards, and how to enhance security architectures while meeting regulatory objectives.

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

REQUIREMENTS FOR SUCCESSFUL COMPLETION OF PROGRAM

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

This course will use PowerPoint presentations and group discussions.

PROCEEDINGS

The proceedings of the course will be published, and one copy will be distributed to each registrant at the course.

EVENT LOCATION

A room block has been reserved at the Hilton Baltimore, 401 W Pratt St, Baltimore, MD 21201, for the nights of April 23-25, 2017. Room rates are $229 plus applicable tax. Call **1-443-573-8700** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 23, 2017 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

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 course.

REGISTER 3, SEND THE 4TH FREE

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

> *"Used real world issues to make it interesting."*
>
> Nuclear Oversight Audit Team Leader, Exelon Nuclear

Please make checks payable to: "PMA"

EVENT LOCATION

A room block has been reserved at the Hilton Baltimore, 401 W Pratt St, Baltimore, MD 21201, for the nights of April 23-25, 2017. Room rates are $229 plus applicable tax. Call **1-443-573-8700** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is March 23, 2017 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

PLEASE REGISTER

○ **FUNDAMENTALS OF CYBER SECURITY FOR NUCLEAR PLANTS** COURSE:
APRIL 25-26, 2017: US $1395
EARLY BIRD on or before APRIL 7, 2017: US $1195

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   Account Number

Billing Address   Billing City   Billing State

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

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

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 24, 2017 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.