

# FUNDAMENTALS OF CYBER SECURITY FOR NUCLEAR PLANTS

**November 14-15, 2018**  
**EUCI Conference Center**  
**Denver, CO**

“

*“The threat of cyber related events is growing. This course was an eye-opener. The instruction given provided a great overview of cyber threats and protection.”*

Engineer, Oak Ridge  
National Laboratory

RELATED EVENT:

**FUNDAMENTALS OF CYBER SECURITY FOR UTILITIES**

November 13-14, 2018 | Denver, CO



**TAG US #EUCIEvents**  
**FOLLOW US @EUCIEvents**



EUCI is authorized  
by IACET to offer  
1.0 CEUs for the  
course

## 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 and NEI 13-10. However, because of the potential impacts to safety and security, 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 and approaches are revised to address industry challenges, the industry is still responsible for its plants and protecting 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 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

---

- Discuss current value at risk from 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 and NEI 13-10 implementation strategies
- Discuss the convergence of Maintenance/Operations/Engineering/Security/Cyber security departments, internal communication strategies and building cross-functional teams
- Review practical techniques for risk management and data protection
- Articulate holistic cyber security program strategies focused on prevention

## WHO SHOULD ATTEND

---

Utility and energy company staff from the following departments:

- Directors and C-Suite Executives
- Compliance and Regulatory Managers
- Licensing
- Legal and Regulatory Staff
- Information Technology and Information Security
- Operations, Engineering, and Maintenance
- Administrative and Support Staff
- Control Systems

As well as:

- Attorneys and Regulators
- Regional NRC Staff
- Contractors and Vendors

# AGENDA

---

WEDNESDAY, NOVEMBER 14, 2018

- 12:30 – 1:00 pm**      **Registration**
- 1:00 – 2:30 pm**      **Hacking and Hardware – Understanding Cyber Threats to Nuclear Power Plants and the Value at Risk**
- 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 – 4:00 pm**      **Continuation of Value at Risk: Threats to Nuclear Power Plants**
- 4:00 – 5:00 pm**      **Plant-Wide Cyber Security Part A: Moving Beyond Cyber Security as an IT Problem**
- Top concerns in the nuclear industry
  - Interesting approaches to license commitments

THURSDAY, NOVEMBER 15, 2018

- 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 – 12:00 pm**      **Plant-Wide Cyber Security Part B: Moving Beyond Cyber Security as an IT Problem**
- Best practices for nuclear cyber security
  - Preparing for Milestone 1-Milestone 7 inspections
  - NEI 08-09 Strategy & Technology
  - Core assets and Critical Digital Assets (CDAs)
  - Levels 1-4
  - CDA grouping
  - SCIS/SCIP
  - Cyber rvaluation
  - SCIP development and assessment
  - NEI 13-10
  - Presenting to the CSAT
  - Cyber program roles and responsibilities
  - Internal communication strategies
  - Building a cross-functional team
- 12:00 – 1:00 pm**      **Group Luncheon**
- 1:00 – 2:30 pm**      **Continuation of Plant-Wide Cyber Security Part B: Moving Beyond Cyber Security as an IT Problem**
- 2:30 – 3:00 pm**      **Networking Break**

# AGENDA

---

THURSDAY, NOVEMBER 15, 2018 (CONTINUED)

**3:00 – 5:00 pm**

**Integrating Cyber Security across the Plant**

- Enterprise roles and responsibilities
- Internal cyber security strategy
- Cyber security integration across the plant
- End-to-end cyber security from back office to core business

**5:00 pm**

**Course Adjourns**

# COURSE INSTRUCTOR

---

## Rob Schuler

**Cyber Strategy Manager, Accenture Security**

Mr. Schuler is a Cyber Security Strategy Manager and Technical Thought Leader with Accenture Security in the United States. He has 20 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 utility control systems.

Mr. Schuler has key expertise in helping clients to define their needs and translate them into actionable program goals. He has a strong history of identifying and unifying technical teams of diverse backgrounds and delivering program excellence.

Mr. Schuler's industry outreach activities have included frequent speaking engagements delivering 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 build secure, best-practice architectures while meeting compliance objectives.



***"The course was accessible while managing to provide depth and breadth with surprising efficiency."***

Graduate Student  
Researcher, University  
of California, Berkeley



***"An excellent learning experience in a short time."***

Postdoctoral Scholar, University of California,  
Berkeley

## 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

---

This course will use PowerPoint presentations and group discussions.

## EVENT LOCATION

---

### **EUCI Conference Center**

4601 DTC Blvd., B-100  
Denver, CO 80237

## NEARBY HOTELS

---

### **Preferred Hotel**

#### **Hyatt Place Denver Tech Center**

8300 E. Crescent Parkway, Greenwood Village, CO 80111 (0.9 miles away)

Call Central Reservations at **888-492-8847** and ask for the corporate rate of \$159 under the **Group Code: EUCI**.

or visit [https://denvertechcenter.place.hyatt.com/en/hotel/home.html?corp\\_id=102338](https://denvertechcenter.place.hyatt.com/en/hotel/home.html?corp_id=102338) for the corporate rate using the

**Group Code: EUCI**

#### **Hyatt Regency Denver Tech Center**

7800 E. Tufts Ave  
Denver, CO 80237  
Phone: 303-779-1234  
0.3 miles away

#### **Hilton Garden Inn Denver Tech Center**

7675 E. Union Ave  
Denver, CO 80237  
Phone: 303-770-4200  
0.6 miles away

#### **Denver Marriott Tech Center**

4900 S. Syracuse St  
Denver, CO 80237  
Phone: 303-779-1100  
0.7 miles away

## 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 this course may send 1 FREE for every 3 delegates registered. Please note that all registrations must be made at the same time to qualify.



# EVENT LOCATION

## EUCI Conference Center

4601 DTC Blvd., B-100  
Denver, CO 80237

**See nearby hotels on page 5**

## PLEASE SELECT

**SPECIAL PRICE FOR BOTH FUNDAMENTALS OF CYBER SECURITY FOR UTILITIES AND FUNDAMENTALS OF CYBER SECURITY FOR NUCLEAR PLANTS**  
NOVEMBER 13-15, 2018: US \$2195  
EARLY BIRD on or before OCTOBER 26, 2018: US \$1995

**FUNDAMENTALS OF CYBER SECURITY FOR NUCLEAR PLANTS COURSE**  
NOVEMBER 14-15, 2018, US \$1395  
EARLY BIRD on or before OCTOBER 26, 2018: 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

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.

### 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 October 12, 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