ICS Cyber Security Workshop

Cyber-securing your industrial control systems

The threat is real.
The landscape is changing. Be prepared.

Since Stuxnet in 2010, and newer threats such as Dragonfly, attacks against industrial control systems (ICS) are in the news daily. The revelation of a steadily growing number of vulnerabilities and persistent hacker efforts to exploit them should concern every ICS operator. The costs to industry and the public are increasing daily in terms of dollars spent and lost, diverted technical resources, interrupted workflows and depleted confidence in the reliable operation of basic services. Perceptive business managers are acting fast to improve their protection before they become a statistic.

Ultra Electronics, 3eTI understands these issues. We have experienced cyber experts on staff, with years of frontline experience in systems security. Since 1995, 3eTI has created the security solutions used by major DoD customers to reduce costs, save energy, and streamline operations. Our experience and the growing demand of the wider private markets prompted 3eTI to develop an educational forum to educate businesses on how they can consistently thwart attacks for purposes of espionage, revenge or activism.

About the Workshop

The ICS Cyber Security Workshop is a highly customized educational session for identifying structures and challenges that foster vulnerabilities in specific ICS platforms. The workshops are designed for individual critical infrastructure companies as an interactive and collaborative program modeled to their unique requirements. Aided by highly trained technical facilitators, attendees receive a complete overview of the fundamentals of cyber network protection for industrial control and monitoring systems. They are introduced to strategies for balancing security requirements against cost and the challenges of legacy integration.

Who Should Attend

Workshop content is technical and appropriate for both senior management-level supervisors as well as operationally astute technical decision makers. Most participants are motivated by opportunities to learn about or apply best security practices to industrial network protection. They seek ways to reconcile diverse and sometimes conflicting security requirements, cost restrictions or existing integrations. All content is supported by appropriate references to relevant guidance from NIST Special Publication 800-82 "Guide to Industrial Control Systems (ICS) Security."

Benefits & Outcomes

In evaluating the **ICS Cyber Security Workshop**, relevant considerations include:

- **Cost and convenience:** Half-day group workshop sessions are valued at $2500 but are available free of charge when conducted at our corporate facility located immediately outside Washington DC. Special reduced rate* and no fee workshops are available for select industry groups and at select locations in the continental US.

- **Targeted and high-value content:** No two workshops are identical. Facilitators typically work with a small group of participants from the same organization, allowing 3eTI to structure confidential and proprietary content that is applicable to the specific audience.

- **Specific solutions and strategies:** Each session includes a detailed discussion of the companies' systems and structures for a high-level audit of their cyber risk factors. Participants will leave with a point-by-point overview of vulnerabilities and recommended methods for resolution.

- **Resources and support:** Participants benefit from access to case studies, technical documents, white papers and reports, as well as a facilitator follow up, to further their learning and fuel continued problem solving.

Agenda Structure & Highlights

These custom and individualized sessions are guided by the needs and interests of attendees as they relate to ICS cyber security. The workshop generally combines the following elements:

- Review of IEC 62443/ISO 27001 standards for security
- Discussion of commonly overlooked critical vulnerabilities
- Methods for aligning the threat landscape to today's hacker trends, techniques and technologies
- Evaluating strengths and shortcomings of multilayer and multivendor security
- Architecture risk assessment
- Simulated demonstration of ICS attacks and threat mitigation

How to Schedule

For more information, or to schedule a workshop, visit www.ultra-3eti.com/workshop or contact:

Yolanda S. Hicks, CAPM
Cyber Workshop Facilitator
yolanda.hicks@ultra-3eti.com
Direct: +1 301 944 1343
Mobile: +1 301 529 9208

---

* Workshops held at locations other than the Ultra Electronics, 3eTI headquarters may entail special scheduling consideration based on travel distance and facilitator per diem rates. Workshop fee and transportation expenses may apply but will be provided prior to scheduling.

Ultra Electronics, 3eTI
9713 Key West Avenue
Suite 500
Rockville, Maryland 20850
USA
Tel: +1 301 670 6779
www.ultra-3eti.com

3eTI

Ultra ELECTRONICS