2013 ISA Water/Wastewater and Automatic Controls Symposium

Crowne Plaza Orlando-Universal Hotel.....Orlando, Florida, USA……**August 6 to 8, 2013**
Presented by the ISA Water/Wastewater Industries Division – ***www.isawwsymposium.com***
Technical co-sponsors: WEF Automation and Info Tech Committee and the Florida AWWA Section

August 5-6, 2013 – Optional Short Course

In-Depth SCADA Cyber Security

Using the ANSI/ISA99 Standards to Secure Your Control System

ISA Course IC32. Version 2.5

Course Description

Length: 2 days
Date: Mon-Tues, August 5-6, 2013
CEU Credits: 1.4
Course Hours: 8:00 a.m.–3:30 p.m., includes lunch both days
Price: $1115 for ISA Members, $1395 List

Description:

The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wrecked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.

You will be able to:

- Discuss the principles behind creating an effective long term program security
- Interpret the ANSI/ISA99 industrial security guidelines and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- Describe the principles of security policy development
- Explain the concepts of defense in depth and zone/conduit models of security
- Analyze the current trends in industrial security incidents and methods hackers use to attack a system
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

You will cover:

- **Understanding the Current Industrial Security Environment:** What is Electronic Security for Industrial Automation and Control Systems? | How IT and the Plant Floor are Different and How They are the Same
- **How Cyberattacks Happen:** Understanding the Threat Sources | The Steps to Successful Cyberattacks
- **Creating A Security Program:** Critical Factors for Success | Understanding *ISA99 Part 2: Establishing an Industrial Automation & Control Systems Security Program*

- **Using ISA99.00.02—Risk Analysis:** Business Rationale | Risk Identification, Classification, and Assessment | The DNSAM Methodology
- **Using ISA99.00.02—Addressing Risk with Security Policy, Organization, and Awareness:** CSMS Scope | Organizational Security | Staff Training and Security Awareness
- **Using ISA99.00.02—Addressing Risk with Selected Security Counter Measures:** Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control
- **Using ISA99.00.02—Addressing Risk with Implementation Measures:** Risk Management and Implementation | System Development and Maintenance | Information and Document Management
- **Using ISA99.00.02—Monitoring and Improving the CSMS:** Compliance and Review | Improve and Maintain the CSMS

Classroom/Laboratory Exercises:

- Develop a business case for industrial security
- Conduct security threat analysis
- Investigate scanning and protocol analysis tools
- Apply basic security analysis tools software

Includes ISA Standards:

- *ANSI/ISA99.00.01-2007 - Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*
- *ANSI/ISATR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems*
- *ANSI/ISA99.02.01-2009 - Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*

About the Instructor

John Cusimano, CFSE, CISSP is director of exida's security services division. A process automation safety, security and reliability expert with more than twenty years of experience, John leads a team devoted to improving the security of control systems for companies worldwide. He has conducted or supervised numerous cyber security assessments of industrial control and SCADA systems in a variety of industries including chemical, water/wastewater, oil & gas, and electric power. John is chairman of ISA 99 WG4 TG2 Zones & Conduits committee and co-chair of ISA 99 WG4 TG6 Product Development committee. He represents exida as a voting member on the ISA-99 standards committee on control system security and the ISA Security Compliance Institute's Technical Steering Committee. John is also active in a variety of other ISA99, ISA84, and ICSJWG working groups. John is also a qualified Achilles™ communication robustness test engineer. Prior to joining exida, John led market development for Siemens' process automation and safety products and held various product management positions at Moore Products Co. John started his 25+ year career at Eastman Kodak Company, where he implemented and managed automation projects. John has a B.S. degree in Electrical & Computer Engineering from Clarkson University and holds a CFSE and CISSP certification.

Course Schedule

DAY	Topics, Exercises, Etc.	Time
Day 1	Welcome	0.25 hour
A.M.	Pre Instructional Survey	0.25 hour
	What is the threat?	0.50 hour
	Your site/Plant/Facility	0.25 hour
	Industrial Networking Basics	0.75 hour
	Exercise #1-Investigate your connection	0.50 hour
	Break	0.25 hour
	How do attackers attack?	0.50 hour
	Exercise #2- Investigate the network- map	0.50 hour
	Lunch	1.00 hour
Day 1	Defenses	0.50 hour
P.M.	ISA 99/IEC 62443	0.50 hour
	Security Process- Seven Steps	0.25 hour
	Exercise # 3-Wireshark	0.75 hour
	Break	0.25 hour
	Defense in Depth/Detection in Depth	1.00 hour
	Day 1 Progress Survey	0.25 hour
Day 2	Vulnerability & Risk Assessments	0.75 hour
A.M.	Regulations, Standard, Recommended Practices	0.75 hour
	Break	0.25 hour
	Defense Architectures	1.00 hour
	Exercise #4- MBSA	0.25 hour
	Maintaining Cyber Security	0.50 hour
	Lunch	1.00 hour
Day 2	Networking & Device Hardening	0.50 hour
P.M.	Exercise #5 Policy Settings	0.75 hour
	Break	0.25 hour
	Asking for Cyber Security	0.50 hour
	Questions/Next Steps	0.75 hour
	References	0.25 hour
	Post-Course Survey	0.50 hour
	Course & Instructor Assessment/Survey	0.20 hour
		14 hours = 1.4 CEUs