2014 ISA Water/Wastewater and Automatic Controls Symposium

August 5 to 7, 2014………Crowne Plaza Orlando-Universal Hotel………Orlando, Florida, USA
Presented by the ISA Water/Wastewater Industries Division – ***www.isawwsymposium.com***
Technical co-sponsors: Florida AWWA Section, the WEF Automation and Info Tech Committee ,
Florida Water Environment Association, Instrumentation Testing Association, and ISA Tampa Bay Section

August 5, 2014 – Optional Short Course

Introduction to SCADA Cyber Security and the ANSI/ISA99 Standards

ISA Course IC32C

Course Description

Length: 1 day
Date: Mon, August 5, 2014
CEU Credits: 0.7
Course Hours: 8:00 a.m. – 4:00 p.m., includes lunch
Price: $535 for ISA Members, $685 List

Description:

Understanding how to secure factory automation, process control, and Supervisory Control and Data Acquisition (SCADA) networks is critical if you want to protect them from viruses, hackers, spies, and saboteurs.

This seminar teaches you the basics of the ANSI/ISA99 Security for Industrial Automation and Control Systems standards and how these can be applied in the typical factory or plant. In this seminar, you will be introduced to the terminology, concepts, and models of ANSI/ISA99 Cyber Security. As well, the elements of creating a Cyber Security management system will be explained along with how these should be applied to industrial automation and control systems.

You will be able to:

- Discuss why improving industrial security is necessary to protect people, property, and profits
- Define the terminology, concepts, and models for electronic security in the industrial automation and control systems environment
- Define the elements of the of ISA99 Part 2: Establishing an Industrial Automation and Control Systems Security Program
- Define the core concepts of risk and vulnerability analysis methodologies
- Define the concepts of defense in depth and the zone/conduit models of security
- Explain the basic principles behind the policy development and key risk mitigation techniques
- Explain why improving industrial security will be necessary to protect people, property, and profits

You will cover:

- **Understanding the Current Industrial Security Environment:** What is Electronic Security for Industrial Automation and Control Systems? | Trends in Security Incidents
- **How IT and the Plant Floor are Different and How They are the Same**
- **Current Security Standards and Practices**
- **Creating A Security Program:** Critical Factors for Success | Understanding ISA99 Part 2: Establishing an Industrial Automation and Control Systems Security Program

- **Using ISA99.00.02—Risk Analysis:** Business Rationale | Risk Identification, Classification, and Assessment
- **Using ISA99.00.02—Addressing Risk with Security Policy, Organization, and Awareness:** CSMS Scope | Organizational Security | Staff Training and Security Awareness | Business Continuity Plan | Security Policies and Procedures
- **Using ISA99.00.02—Addressing Risk with Selected Security Counter Measures:** Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control: Account Administration, Authentication, and Authorization
- **Using ISA99.00.02—Addressing Risk with Implementation Measures:** Risk Management and Implementation | System Development and Maintenance | Information and Document Management | Incident Planning and Response
- **Using ISA99.00.02—Monitoring and Improving the CSMS:** Compliance and Review | Improve and Maintain the CSMS

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*
- *ANSI/ISA99.03.03-2013: System Security Requirements and Security Levels*

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 control system products, systems, sites and corporations.

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 ISA S99, ISA S84, 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 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		
A.M.	Seminar Introductions	
	Pre-Instructional Survey	0.25 hour
	Section 1: Understanding the Industrial Security Environment	0.75 hour
	Section 2: How IT and the Plant Floor Compare	0.50 hour
	Section 3: Security Standards and Practices in IT and Industry	0.50 hour
	Section 4: Creating A Security Program	0.50 hour
	Section 5: Using ISA99.00.02 – Risk Analysis	0.75 hour
Day 1		
P.M.	Section 6: Using ISA99.00.02 – Addressing Risk with Security Policy, Organization, and Awareness	0.75 hour
	Section 7: Using ISA99.00.02 – Addressing Risk with Selected Security Counter Measures	0.75 hour
	Section 8: Using ISA99.00.02 – Addressing Risk with Implementation Measures	0.75 hour
	Section 9: Using ISA99.00.02 – Monitoring and Improving the CSMS	0.75 hour 0.50 hour
	Overall Course Review/Objectives	0.25 hour
	Post-Instructional Survey	
	Final Course Evaluation	
		7 hours = 0.7 CEUs