2016 ISA Water/Wastewater and Automatic Controls Symposium

August 2 to 4, 2016 • Wyndham Lake Buena Vista Resort • 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 1-2, 2016 – Optional Short Course

Using the ISA/IEC 62443 Standards to Secure Your Control System

ISA Course IC32. Version 2.9

Course Description

Length: 2 days
Date: Mon-Tue, August 1-2, 2016
CEU Credits: 1.4
Course Hours: 8:00 a.m. – 4:00 p.m., includes lunch both days
Price: $1,330 for ISA Members, $1,665 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 wreaked 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 the ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009)- Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- **Risk Analysis:** Business Rationale | Risk Identification, Classification, and Assessment | The DNSAM Methodology
- **Addressing Risk with Security Policy, Organization, and Awareness:** CSMS Scope | Organizational Security | Staff Training and Security Awareness
- **Addressing Risk with Selected Security Counter Measures:** Personnel Security | Physical and Environmental Security | Network Segmentation | Access Control

- **Addressing Risk with Implementation Measures:** Risk Management and Implementation | System Development and Maintenance | Information and Document Management
- **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/ISA-62443-1-1 (ANSI/ISA-99.00.01-2007) - Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts & Models*
- *ANSI/ISA-62443-2-1 (ANSI/ISA-99.02.01-2009) - Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*
- *ANSI/ISA-62443-3-3 - Security for industrial automation and control systems: System security requirements and security levels*

About the Instructor

Kenneth Frische has over 28 years' experience in providing IT & OT solutions to Oil & Gas, Pharma, Food & Beverage, Packaging, Chemical, Water/Wastewater, Military, Discrete Manufacturing, and Correctional Facilities.

From hands-on coding to management and consulting, Kenneth Frische has worn many hats to include: IT Director, Solutions Architect, Enterprise Architect, Cyber Security Architect, Project Manager, Req/Tech Spec Writer, and Programmer Lead.

His domain expertise includes Process Control and HMI Systems Design and Development, MES integration, Database Management and Design, Business Intelligence / Data Analytics, Business Process Improvement, and Data Warehousing.

Kenneth Frische has a Computer Science degree from Purdue University, an MBA from the University of Oklahoma, and various industry certifications.
Kenneth Frische currently provides risk assessment services, cyber security consulting, and ISA 62443 IC32 training as a member of the Cyber Security Services department at aeSolutions.

Course Schedule

DAY	Topics, Exercises, Etc.	Time
Day 1 A.M.	Welcome Pre-Test Introduction to Control Systems Security and the ISA/IEC 62443 Standards Terminology, Concepts, Models and Metrics	0.25 hour 0.25 hour 1.50 hour 1.50 hours

Day 1 P.M.	Networking Basics – Part 1 Exercise #1 Networking Basics – Part 2 Exercise #2 Network Security Basics Exercise #3	0.50 hour 0.50 hour 0.50 hour 0.50 hour 1.00 hour 0.50 hour
Day 2 A.M.	Industrial Protocols Creating an ICS Security Management Program – Part 1 Creating an ICS Security Management Program – Part 2 Exercise 4	1.00 hour 1.00 hour 1.00 hour 0.50 hour
Day 2 P.M.	Implementing and Maintaining Secure Systems Designing / Validating Secure Systems Developing Secure Products and Systems Wrap-up Post-test	1.00 hour 1.00 hour 1.00 hour 0.25 hour 0.25 hour
		14 hours = 1.4 CEUs