2018 ISA Water/Wastewater and Automatic Controls Symposium

August 7 to 9, 2018 • Hyatt Regency Bethesda • Bethesda, Maryland, USA
Presented by the ISA Water/Wastewater Industries Division – ***www.isawwsymposium.com***
Technical co-sponsors: Chesapeake AWWA Section, the WEF Intelligent Water Technology Committee , Chesapeake Water Environment Association, and ISA Baltimore-Washington Section

August 6-7, 2018 – Optional Short Course

IACS Cybersecurity Operations & Maintenance: Secure Your Control System

ISA Course IC37S

Course Description

Length: 2 days
Date: Mon-Tues, August 6-7, 2018
CEU Credits: 1.4
Course Hours: 8:00 a.m. – 4:00 p.m., includes lunch both days
Price: $1,440 for ISA members, $1,620 for affiliates, $1,800 list & community members

Description:
The third phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) focuses on the activities associated with the ongoing operations and maintenance of IACS cybersecurity. This involves network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures implemented in the Design & Implementation phase. This phase also includes security management of change, backup and recovery procedures and periodic cybersecurity audits.

This course will provide students with the information and skills to detect and troubleshoot potential cybersecurity events as well as the skills to maintain the security level of an operating system throughout its lifecycle despite the challenges of an every changing threat environment.

You will be able to:

- Perform basic network diagnostics and troubleshooting
- Interpret the results of IACS device diagnostic alarms and event logs
- Implement IACS backup and restoration procedures
- Describe the IACS patch management life cycle and procedure
- Apply an antivirus management procedure
- Define the basics of application control and white listing tools
- Define the basics of network and host intrusion detection
- Define the basics of security incident and event monitoring tools
- Implement an incident response plan
- Implement an IACS management of change procedure
- Conduct a basic IACS cyber security audit

You will cover:

- Introduction to the ICS Cybersecurity Lifecycle
  - Identification & Assessment phase
  - Design & Implementation phase
  - Operations & Maintenance phase

- Network Diagnostics and Troubleshooting
  - Interpreting device alarms and event logs
  - Early indicators
  - Network intrusion detection systems
  - Network management tools
- Application Diagnostics and Troubleshooting
  - Interpreting OS and application alarms and event logs
  - Early indicators
  - Application management and whitelisting tools
  - Antivirus and endpoint protection tools
  - Security incident and event monitoring (SIEM) tools
- IACS Cybersecurity Operating Procedures & Tools
  - Developing and following an IACS management of change procedure
  - Developing and following an IACS backup procedure
  - IACS configuration management tools
  - Developing and following an IACS patch management procedure
  - Patch management tools
  - Developing and following an IACS antivirus management procedure
  - Antivirus and whitelisting tools
  - Developing and following an IACS cybersecurity audit procedure
  - Auditing tools
- IACS incident response
  - Developing and following an IACS incident response plan
  - Incident investigation
  - System recovery

Classroom/Laboratory Exercises:

- Asset Inventory
- ICS Device Hardening
- Disabling USB Storage Devices
- Restrict access to USB drives
- Application Control / Whitelisting
- Microsoft Windows Software Update Services (WSUS)
- PLC backup and configuration management
- Change Management (MOC form)
- Event Detection Tracking and Log Monitoring
- Vulnerability Scanning
- Network Packet Capture Analysis
- Troubleshooting and Forensics

About the Instructor

Wally Magda is an internationally recognized cyber and physical security expert for Industrial Control Systems (ICS) with over 35 years of experience. His deep security experience spans military nuclear missile command and control systems, intelligence agencies and enterprise cyber security.

Wally has been involved with the NERC CIP standards from the early days of UA 1200. As a regional NERC CIP compliance auditor he has performed over 100 NERC CIP on and off site audits in the roles of Audit Team Lead and team member.

He recently retired from the Western Electricity Coordinating Council (WECC) and now conducts Industrial Control System (ICS) basic and advanced cyber and physical security training courses.

Wally's utility career began as an Instrumentation, Control and Electrical (ICE) Tech. He then progressed to managing ICS as a process control engineer. Seeing the need for cyber security professionals to assist the industrial control vertical business units he stepped into the enterprise level cyber security realm. Wally has conducted numerous cyber and physical security assessments for electric, natural gas, chemical, LNG and manufacturing facilities.

Wally has presented at conferences and events such as the ICSJWG, IEEE, FBI InfraGard, UTC Telecom, WECC CIPUG and ISSA-COS. He is an ISSA Senior Member recognized for his contributions to the security community such as voluntarily teaching CISSP and Security+ prep courses at a local technical university.

Education & Certs:

- Bachelor of Science (BSc) degree in Management Information Systems (MIS)
- CAP - Certified Automation Professional (ISA)
- GICSP - Global Industrial Cyber Security Professional (SANS GIAC)
- GSEC - GIAC Security Essentials (SANS GIAC)
- PSP - Physical Security Professional (ASIS)
- CISSP - Certified Information Systems Security Professional (ISC2)
- CISA - Certified Information Systems Auditor (ISACA)
- ISA99/IEC 62443 Cybersecurity Certificate (ISA)
- IAM & IEM (NSA)
- GROL +RADAR (FCC)

Course Schedule

DAY	Topics, Exercises, Etc.
Day 1 A.M.	Welcome and Pre-Instructional Survey Introduction to the ICS Cybersecurity Lifecycle Section 1: Review of the Assess Phase Section 2: Review of the Design Phase Section 3: IACS Asset Management Exercise #1: Asset Inventory Section 3: System Hardening Exercise #2: ICS Device Hardening Exercise #3: Disabling USB Storage Devices
Day 1 P.M.	Exercise #4: Whitelisting Section 3: Access Control & Remote Access Section 3: Patch Management Exercise #5: WSUS demo Section 3: Malware Management Exercise #6: PLC backup and configuration management Exercise #7: Complete a MOC form Section 3: Information & Documentation Management
Day 2 A.M.	Daily Progress Reviews & Overview of Day 2 Objectives Section 3: Change Management Section 3: Physical Security Exercise #8: What's wrong with this picture Section 4: Detecting Abnormal Activity Section 4: Network and Host Intrusion Detection Section 4: Monitoring Logs Exercise #9: Event Detection, Tracking, and Log Monitoring Section 4: Periodic testing / auditing Exercise #10: Vulnerability scanning
Day 2 P.M.	Section 5: Incident Response Lifecycle Section 5: Incident Response Planning Section 5: Incident Management Section 5: Post Incident Analysis & Forensics Exercise #11: Network packet capture analysis Exercise #12: Troubleshooting and Forensics Review of Overall Course Objectives Post-Instructional Survey Final Course Evaluation