TRAINING DAYS 2017

Using the ISA/IEC 62443 Standards to Secure Your Control Systems (IC32)

Milan, July 3th –4th

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.

Not sure this particular course is for you?

A pre-instructional survey is available for you to evaluate your level of understanding of the course material and to show you the types of questions you'll be able to answer after completing the course

YOU WILL 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
- **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

INFO & COST:

LENGHT:
2 days

COST:
for ISA members€ 1.295.
(non-ISA members pay € 1.595; ISA membership pay € 120)
Prices are inclusive Certicate of Completion, all catering and the printed ISA-99 standard with a value of about $ 400,- , prices are exclusive VAT (The Netherlands) or VAT will be transferred (other European Countries).
Exam ISA/IEC 62443 Cyber Security Fundamentals Specialist; € 195,- excl.VAT.
All courses taught entirely in English (incompany training can be taught in the Dutch, German, French or Spanish language).

DURATION:
1 half day

LOCATION:
Prometric Testing Center visit www.prometric.com/ISA

The Venue Address

Tocq Hotel, Via Alessio di Tocqueville 7/D
20152 Milan, Italy
Phone: +39 02 62071
Web: www.tocq.it

Directions

Arrival by plane:
Malpensa Airport (MI)
Approx. 70 km from Milan, connected to the center of the city by the Malpensa Express train arriving at Cadorna Station in 40 min.
Linate Airport (MI)
Approx. 10 km from the center of Milan, connected to the heart of the city (San Babila stop) by bus 73 in 15 min.
Arrival by train: Milano Centrale Station
Approx. 3,2 km to hotel.

Contacts

ISA ITALY SECTION
Viale Campania, 31 20133 Milano
Tel. +39 02 54123816 | Mail: isaitaly@aisisa.it

The ISA/IEC 62443 CyberSecurity Certificate exam

is closed book – no reference material will be allowed in the exam room.
A calculator will be provided for you on the computer at the testing center. You will not be able to bring any personal items into the exam room.
A secure location will be provided for you to store your belongings while you take the exam, but the space is limited.
Report to the testing center 30 minutes prior to your exam time to sign-in and receive testing instructions. You must bring the Prometric confirmation and identification in order to sit for your exam.
The exam is only available electronically through a Prometric testing center. To view the locations that are available in the Prometric network for ISA/IEC 62443 CyberSecurity certificate exams, visit www.prometric.com/ISA. You may reschedule your exam only once with no penalty, but you must do so 2 days (48 hours) prior to the exam date in the US and Canada, or 5 days (120 hours) prior to the exam date in all other Prometric locations. A € 150,- reschedule fee will apply if you do not cancel your appointment in advance. You must complete all testing within the eligibility period, or you will have to complete the course again in order to pursue the certificate.
When successfully passing the exam, you will receive the ISA/IEC 62443 Cyber Security Fundamentals Specialist certificate.
The certificate will be treated as actual for a period of 3 years. After this, you need to retake the exam to extend your certificate.
All courses taught entirely in English.

We look forward to welcoming you to our training

Organized by

AIS ASSOCIAZIONE ITALIANA STRUMENTISTI

ISA Italy Section

Supported by

BAGGI®

www.aisisa.it