ISA™

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

TARGET
your cyber vulnerabilities

PROTECT
your critical control systems

Early-Bird Discount
Save $250
when you register by 15 December!

System Wide Awareness Training

High level industrial communications and cybersecurity training designed for Process Professionals!

Coming to North Carolina!

Setting the Standard for Automation™

Arm yourself against **CYBERATTACK!**

Designed for I&C Personnel, Engineers, Managers, Technicians, System Integrators, and Maintenance Personnel, ISA's System Wide Awareness Training Camp brings the knowledge you need to protect operational control systems from cyberattack.

Over four dynamic weeks, ISA will bring this world-class industrial data communications and cybersecurity training to North Carolina. Take hands-on, highly-intensive classes and learn from leading industry experts in one convenient location. Choose the course or courses that best meet your needs.

You will gain:

- Essential knowledge needed to safeguard control systems from attacks resulting in plant shutdown or operational disruptions
- An understanding of the differences between information technology (IT) and process operational technology (OT) security measures
- Improved awareness of system inter-relationships and dynamics in industrial plant communications and security
- CEU and PDH credits for each course successfully completed
- A discount rate when you register for multiple courses*

S.W.A.T. Course Schedule

Research Triangle Park, NC

WEEK 1 (30 JANUARY – 3 FEBRUARY)
IT Survival Basics for I&C Personnel (TS04)

WEEK 2 (6-10 FEBRUARY)
Industrial Data Communication Systems (TS06)

WEEK 3 (13-17 FEBRUARY)
Industrial Networking & Cybersecurity (TS12)

WEEK 4 (20-24 FEBRUARY)
Course 1: **Using the ISA/IEC-62443 Standards to Secure Your Control Systems (IC32)**
Course 2: **Assessing the Cybersecurity of New or Existing IACS Systems (IC33)**

Class size is limited, and registrations will be filled on a first-come, first-served basis.

Register Today!
Visit: www.isa.org
NCSWAT17B
Email: info@isa.org
Call: +1 919-549-8411

*Register for more than one course and the ISA Multi-Registration rate will apply for additional courses.

WEEK 1:

IT Survival Basics for I&C Personnel (TS04)

Dates: 30 January–3 February

This course will provide I&C personnel with a basic understanding of IT concepts and technology including Ethernet networking, switches, routers, servers, PCs and firewalls, as well as wireless Ethernet networks and TCP/IP communications. The student will learn how to configure them and how cybersecurity is applied to protect them.

Who Should Attend?

- I&C Technicians
- Control system engineers
- I&C Managers
- I&C Maintenance personnel

Course Topics:

- Ethernet communications, switch technology, and configuration
- Setting up VLAN and QoS configurations
- ARP and DHCP protocols that make Ethernet LANs work
- IPv4 addressing and subnet configuration
- TCP and UDP port numbers, protocols, and message delivery
- Ethernet-based Industrial Protocol standards
- Insecure legacy Microsoft networking functions
- Microsoft Active Directory in a plant environment
- Firewalls and how they can be applied in a plant environment
- Vulnerability scanning and tools
- IEEE 802.11 WLANs and wireless security configuration
- And More…

Course Resources (included with registration):

- General familiarity with PCs and Windows OS
- Basic DC electronic/electrical circuit knowledge

Course Details:

Course No.: TS04
Length: 5 Days
CEUs (PDHs): 3.5 (35)

Registration:
$3,080.00 ISA Member
$3,465.00 Affiliate Member
$3,855.00 Non-Member/Community Member
$3,080.00 Multi-Registration Rate

> I appreciated that the instructor had actual field experience in the subject matter.
>
> **TS04 Student**

WEEK 2:

Industrial Data Communication Systems (TS06)

Dates: 6–10 February

Starting from the basics, this course gives you the tools to design and maintain industrial communications systems on your plant floor. You'll learn the underlying principles behind today's industrial communications systems, including Modbus, Data Highway Plus, Ethernet, and TCP/IP. Real-life examples and case histories provide insight into the facts behind control networks and how to apply and maintain them effectively in your plant.

Course Topics:

- **What is Data Communications?:** ISO/OSI Reference Model | Terminology Basics
- **Serial Communications:** Modem Principles | The EIA-232E Standard | Beyond 232: EIA-422/423/485/530 Standards
- **The Analog TelCo system including circuit types and Modems**
- **The Digital TelCo system T1/T3 circuits, ISDN, xDSL, Frame Relay, X.25 networks, ATM and SONET**
- **Data Link Layer Basics:** Data Encoding | Error Detection/Correction Schemes
- **Industrial Protocols:** Modbus and Modbus/IP, DNP3.0 and DF-1
- **LAN Technologies:** Overview of Ethernet Technology | Ethernet Cabling and Configuration Rules | Repeaters, Bridges, Routers, and Gateways
- TCP/IP basics | Is Ethernet Ready for the Plant Floor? | Industrial Ethernet Design Techniques
- **Fiber optics:** standards, cables, applications, limitations
- **Wireless Industrial Communications:** SP100, Wireless HART, Wireless Fieldbus, Wireless Profibus
- **Inside the Proprietary PLC Networks:** MB+ and DH+ LAN design
- **Data Exchange using** OPC for inter-system data exchanges
- **Troubleshooting Industrial Networks and Fieldbuses:** Five Rules for Troubleshooting | Troubleshooting with Statistics | Troubleshooting Tools

Course Resources (included with registration):

- *Industrial Data Communications, Latest Edition*

Course Details:

Course No.: TS06
Length: 4.5 Days
CEUs (PDHs): 3.2 (32)

Registration:
$3,080.00 ISA Member
$3,465.00 Affiliate Member
$3,855.00 Non-Member/Community Member
$3,080.00 Multi-Registration Rate

> The working, hands-on labs helped me see the actual data.
>
> **TS06 Student**

WEEK 3:

Industrial Networking & Security (TS12)

Dates: 13–17 February

In this course, you will learn about the latest developments in networking, including practical tips on designing, implementing and testing TCP/IP-based networks and how to apply them securely and reliably in an Industrial environment. You will discuss the functions and purposes of the elements used to create and protect an industrial network including switches, routers, firewalls and Intrusion detection/prevention systems. This course will expand your practical knowledge of LAN, WAN, and Web technologies. It illustrates what is safe and practical for today's plant floor, including Internet technologies such as web servers, TCP/IP, and fiber optics. Special focus will be placed on the questions of security in the industrial setting drawing on the work of the SP-99 committee and NIST. The course will cover the details of IP addressing and how functions and protocols such as DHCP, DNS, ARP/RARP and fast spanning tree are essential to make such networks function. The course will include network troubleshooting and the use of network diagnostic tools.

Course Topics:

- **TCP/IP networking over Ethernet, over serial links (PPP) and through other networks**
- **Making Networks Reliable:** Redundancy/Name services/Fault tolerance/Spanning tree
- **Secure Architectures:** layering based on function, firewall placements, use of DMZs, patch/virus update management
- **Understanding Packets and Protocols:** Understanding IP, TCP and UDP and Application protocols
- **Building a Plant Floor Web Server using HTML, XML, client/server side scripting**
- **Network Security Issues:** Risks and Vulnerabilities | Attack methods and technologies
- **Applying:** Virus Protection | Firewall Basics | Encryption Basics
- **Advanced security:** VPN technology and application, VLAN technology and application, static/dynamic routing
- **Firewall technology:** Basic/advanced, ACL definitions, stateful inspection, HIDS/NIDS
- **User Authentication:** strong authentication, password strategies, multi-factor, centralized policy management
- **Practical Industrial Intranet Applications using SP99 recommendations and standards**

Course Details:

Course No.: TS12
Length: 4.5 Days
CEUs (PDHs): 3.2 (32)

Registration:
$3,080.00 ISA Member
$3,465.00 Affiliate Member
$3,855.00 Non-Member/ Community Member
$3,080.00 Multi-Registration Rate

> The instructor was very knowledgeable and dealt thoroughly with student questions.
>
> **TS12 Student**

WEEK 4:

certificate program

Industrial Cybersecurity Training

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

Dates: 20–21 February

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.

Course Topics:

- **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

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*

Course Details:

Course No.: IC32
Length: 2 Days
CEUs (PDHs): 1.4 (14)

Registration:
$1,440.00 ISA Member
$1,620.00 Affiliate Member
$1,800.00 Non-Member/ Community Member
$1,440.00 Multi-Registration Rate

> The course was very effective in illustrating the cybersecurity lifecycle as well as highlighting industry best practices and standards.
>
> **IC32 Student**

WEEK 4:

Industrial Cybersecurity Training

Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

Dates: 22–24 February

The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1 these assessments need to be performed on both new (i.e. greenfield) and existing (i.e. brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS).

> This is a course that all control engineers should take. Our profession needs to be more knowledgeable about cybersecurity threats and be prepared to implement mitigation strategies on the IACS we are responsible for maintaining.
>
> **IC33 Student**

Who Should Attend:

- Control systems engineers and managers
- System Integrators
- IT engineers and managers of industrial facilities
- IT corporate/security professionals
- Plant Safety and Risk Management

Course Topics:

- Identify and document the scope of the IACS under assessment
- Specify, gather or generate the cybersecurity information required to perform the assessment
- Identify or discover cybersecurity vulnerabilities inherent in the IACS products or system design
- Organize and facilitate a cybersecurity risk assessment for an IACS
- Identify and evaluate realistic threat scenarios
- Identify gaps in existing policies, procedures and standards
- Establish and document security zones and conduits
- Develop a cybersecurity requirements specification (CRS)

Recommended Pre-Requisite:

ISA Course IC32 or equivalent knowledge/experience

Course Details:

Course No.: IC33
Length: 3 Days
CEUs (PDHs): 2.1 (21)

Registration:
$2,000.00 ISA Member
$2,250.00 Affiliate Member
$2,500.00 Non-Member/ Community Member
$2,000.00 Multi-Registration Rate

Each certificate program includes specialized training on ISA/IEC 62443 and an exam that is offered through the Prometric testing centers. Those who register for the training course and the certificate program and pass the exam will be issued an ISA certificate specifying that they have successfully completed that certificate program.

Certificate Program Fee: $185 in addition to the course registration fee.

ISA/IEC 62443 Cybersecurity Certificate Programs

Certificate 1:
ISA/IEC 62443 Cybersecurity Fundamentals Specialist
Certificate 2:
ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
Certificate 3:
ISA/IEC 62443 Cybersecurity Design Specialist
Certificate 4:
ISA/IEC 62443 Cybersecurity Maintenance Specialist
ISA/IEC 62443 Cybersecurity Expert:
Individuals who achieve Certificates 1, 2, 3, and 4 are designated as ISA/IEC 62443 Cybersecurity Experts.

Learn more about these certificate programs, eligibility criteria, renewal, and upcoming courses at www.isa.org/certificateprograms

GET ON THE S.W.A.T. TEAM!

Course Schedule

WEEK 1 (30 JANUARY – 3 FEBRUARY)
IT Survival Basics for I&C Personnel (TS04)

WEEK 2 (6-10 FEBRUARY)
Industrial Data Communication Systems (TS06)

WEEK 3 (13-17 FEBRUARY)
Industrial Networking & Cybersecurity (TS12)

WEEK 4 (20-24 FEBRUARY)
Course 1: Using the ISA/IEC-62443 Standards to Secure Your Control Systems (IC32)
Course 2: Assessing the Cybersecurity of New or Existing IACS Systems (IC33)

Class size is limited, and registrations will be filled on a first-come, first-served basis.

Register TODAY at
www.isa.org/SWATNC17

ISA is accredited by the International Association for Continuing Education and Training (IACET). ISA complies with the ANSI/IACET Standard, which is recognized internationally as a standard of excellence in instructional practices. As a result of this accreditation, ISA is authorized to issue the IACET CEU.

ACCREDITED IACET PROVIDER

Provider #1001262

EP30-6826-1016

International Society of Automation
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

EARLY-BIRD Discount

Register by 15 December 2016 and save $250!

All ISA S.W.A.T. courses will be filled on a first-come-first-served basis. Don't miss your chance to attend this unique ISA training event!

Register today at **www.isa.org/SWATNC17.**
Reference promo code: NCSWAT16B.