Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Cybersecurity Training

Safeguarding industrial automation and control systems

www.isa.org/Web2014/CYBETRN

Setting the Standard for Automation™

Expert-led training with real-world application from a global leader in industrial cybersecurity

Given the increasing reliance on open standards and interconnectivity in industrial networks and control systems, the risks of cyberattack are growing and present serious threats to economic and national security.

Large-scale cyberwarfare—through acts of espionage, sabotage, and terrorism—could dismantle a nations' power grids, transportation and telecommunications systems, financial networks, manufacturing, and government functions.

As a widely recognized, world leader in cybersecurity standards development and training, the International Society of Automation (ISA) provides the proven expertise and know-how to help safeguard industrial automation and control systems. As an example, the US government is looking to integrate ISA's industrial automation and control systems standards (ANSI/ISA-62443) as part of its national cybersecurity initiative.

ISA's world-renowned cybersecurity experts provide the comprehensive, practical instruction needed to immediately apply your knowledge in the workplace, and through a wide variety of learning formats:

- **One-day classroom courses**
- **Multi-day classroom courses**
- **Multi-week, online, instructor-assisted courses**
- **Live webinars**
- **Pre-recorded webinars**

In addition, to ensure flexibility and to meet varying customer needs, ISA offers cybersecurity training at a variety of locations: at ISA headquarters in North Carolina, at ISA's many regional training centers, and onsite directly at customer facilities.

Who is ISA?

Founded in 1945, ISA is a global organization that serves automation and control professionals through standards development, certification, education, training, publishing, and technical conferences and events. To learn more about ISA, visit www.isa.org/Web14/CYBETRN.

ISA Training: World-class subject-matter expertise

ISA's courses are known and respected worldwide for their unbiased, practical approach to technology application. For more than 65 years, ISA has built on its proven track record of identifying the real-world training needs of organizations and automation and control professionals, and working with leading content experts to deliver rapid, customized solutions.

Taking an ISA training course will:

- Enhance on-the-job training
- Fill in missing knowledge gaps
- Teach you the Hows and Whys
- Provide continuing education credits
- Expand your professional network

Introducing the NEW
ISA99/IEC 62443
Cybersecurity
Fundamentals
Specialist
Certificate Program!
See page 5

Table of Contents

Save with ISA's Multi-Registration Rate!

When you register for more than one course offering in a single registration—whether you are registering yourself for two or more different courses, or registering you and at least one colleague for either the same or a different course—the ISA Multi-Registration rate can be applied to the additional registrations. Learn more at **www.isa.org.Training/MultiReg.**

Who is ISA?

Founded in 1945, ISA is a global organization that serves automation and control professionals through standards development, certification, education and training, technical publications, and technical conferences and events. To learn more about ISA, visit **www.isa.org/web2014/CYBETRN.**

Introduction to Industrial Automation Security and the ANSI/ISA-62443 Standards

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 one-day course teaches you the basics of the ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems* standard and how it can be applied in the typical factory
or plant.

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 IACS environment
- Define elements of the ANSI/ISA-62443 standard for establishing an IACS 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 policy development and key risk mitigation techniques
- And more…

YOU WILL COVER:

- Understanding the Current Industrial Security Environment
- How IT and the Plant Floor are Different and How They are the Same
- Current Security Standards and Practices
- Creating a Security Program
- And more…

COURSE DETAILS:

Course No.: IC32C
Length: 1 day
CEUs: 0.7
Price: $535 ISA Member
$565 Affiliate Member
$595 Community Member/List
$535 Multi-Registration Rate

Save on training when you join ISA!

ISA members save 20% and ISA Automation Affiliate members save 10% on the Community Member/List price for all ISA training courses and products.

Includes ISA Standards:

- ANSI/ISA-62443-1-1 (99.00.01)-2007: *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* ***(A $155 Value!)***
- ANSI/ISA-62443-2-1 (99.02.01)-2009: *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***
- ANSI/ISA-62443-3-3 (99.03.03)-2013: *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* ***(A $260 Value!)***

2014 SCHEDULE

Research Triangle Park, NC.....4 March
Part of the ISA FPID Symposium
Orlando, FL ..... 5 August
Part of the ISA WWAC Symposium

Register or learn more at **www.isa.org/Web14/CYBETRN**

Be one of the first to earn the ISA99/IEC 62443 Cybersecurity Fundamentals Specialist designation!

Announcing the NEW ISA99/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program

ISA has developed a knowledge-based certificate recognition program designed for professionals involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology and an understanding of the material embedded in the ISA99/IEC 62443 standards:

ISA99/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program.

PROGRAM REQUIREMENTS

ISA99/IEC 62443 Cybersecurity Fundamentals Specialist designations and certificates will be awarded to individuals who meet the following program requirements:

- Successfully complete an intensive two-day, classroom training course from ISA: Using the ANSI/ISA-62443 Standards to Secure Your Industrial Control System (IC32)—course information listed on the next page.
- Earn a passing score on the 75-question multiple-choice exam.

PROGRAM PRE-REQUISITES

There are no required prerequisites for this program; however, it is highly recommended that applicants have:

- Three to five years of experience in the IT cybersecurity field with some experience in an industrial setting—with at least two years specifically in a process control engineering setting
- Some level of knowledge or exposure to the ANSI/ISA-62443 standards

PROGRAM PRE-REQUISITES

- Understanding the Current Industrial Security Environment
- How Cyber Attacks Happen
- Creating a Security Program
- Risk Analysis
- Addressing Risk with Security Policy, Organization, and Awareness
- Addressing Risk with Selected Security Counter Measures
- Addressing Risk with Implementation Measures
- Monitoring and Improving the CSMS
- Designing/Validating Secure Systems

RENEWAL

Because these are certificates and not certifications, they do not have to be "renewed"; however, a certificate will only be considered current for three years. In order to extend the current status of a certificate, you will be required to score 70% or above on a 20-question **ISA999/IEC 62443 Certificate Knowledge Review Exam**.

Learn more about this NEW certificate program, eligibility criteria, renewal, and upcoming courses at **www.isa.org/ISA99Certificate**.

Register or learn more at **www.isa.org/Web14/CYBETRN**

Using the ANSI/ISA-62443 Standards to Secure Your Control System

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/ISA-62443 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 security program
- Interpret the ANSI/ISA-62443 industrial security guidelines and apply them to your operation
- Explain the concepts of defense-in-depth, zone, and conduit models of security
- Analyze the trends in industrial system security incidents and methods hackers use to attack
- Define the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks
- And more…

YOU WILL COVER:

- How Cyberattacks Happen
- Creating A Security Program
- Risk Analysis
- Addressing Risk
- Monitoring and Improving the CSMS
- And more…

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

Required for ISA99/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program
(See page 5.)

COURSE DETAILS:

Course No.: IC32
Length: 2 Days
CEUs: 1.4
Price: $1,205 ISA Member/Group Rate
$1,360 Affiliate Member
$1,510 Community Member/List
$1,205 Multi-Registration Rate

Includes ISA Standards and Technical Reports:

- ANSI/ISA-62443-1-1 (99.00.01)-2007: *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* ***(A $155 Value!)***
- ANSI/ISA-62443-2-1 (99.02.01)-2009: *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***
- ANSI/ISA-62443-3-3 (99.03.03)-2013: *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* ***(A $260 Value!)***

Recommended Resource: ISA Text: *Industrial Network Security* by David J. Teumin

2014 SCHEDULE

Research Triangle Park, NC	5–6 February; 14–15 August
Burbank, CA	1–2 April
Columbia, IL	3–4 June
Houston, TX	1–2 December
Newark, DE	1–2 October

Register or learn more at **www.isa.org/Web14/CYBETRN**

Cybersecurity for Automation, Control, and SCADA Systems

The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) systems 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/ISA-62443 standards can be used to protect your critical control systems. You will also explore 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:

- Identify the principles behind creating an effective long-term security program
- Interpret the ANSI/ISA-62443 industrial security guidelines and apply them to your operation
- Learn the basics of risk and vulnerability analysis methodologies
- Explain the principles of security policy development
- Define the concepts of defense-in-depth, zone, and conduit models of security
- Analyze the trends in industrial system security incidents and methods hackers use to attack
- Identify the principles behind the key risk mitigation techniques, including anti-virus and patch management, firewalls, and virtual private networks

YOU WILL COVER:

- **Week 1/Module 1:** Defining Industrial Cybersecurity
- **Week 2/Module 2:** Risk Assessment
- **Week 3/Module 3:** Threats and Vulnerabilities
- **Week 4/Module 4:** Security Policies, Programs, and Procedures
- **Week 5/Module 5:** Understanding TCP/IP, Hackers, and Malware
- **Week 6/Module 6:** Technical Countermeasures
- **Week 7/Module 7:** Architectural and Operational Strategies
- **Week 8:** Final Course Examination

COURSE MATERIALS:

- Course Noteset and Syllabus
- ISA Standards and Technical Reports:
  - ANSI/ISA-62443-1-1 (99.00.01)-2007: *Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models* ***(A $155 Value!)***
  - ANSI/ISA-62443-2-1 (99.02.01)-2009: *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***
  - ANSI/ISA-62443-3-3 (99.03.03)-2013: *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* ***(A $260 Value!)***

Recommended Resource: ISA Text: *Industrial Network Security* by David J. Teumin

COURSE DETAILS:

Course No.: IC32E
Length: 8 Weeks
CEUs: 1.4
Price: $1,205 ISA Member/Group Rate
$1,360 Affiliate Member
$1,510 Community Member/List
$1,205 Multi-Registration Rate

2014 SCHEDULE

Online .....27 January – 21 March;
21 July – 12 September;
24 March – 16 May;
22 September – November

Register or learn more at **www.isa.org/Web14/CYBETRN**

Industrial Networking and Security

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. This course 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 ISA99 standards committee and the National Institute of Standards and Technology (NIST).

YOU WILL BE ABLE TO:

- Identify standards for analog dial-up connections and modems
- Apply TCP/IP protocols, addressing, and troubleshooting
- Estimate where web technologies can safely be used for process control
- Identify security technologies such as firewalls, proxy servers, virus scanning, and intrusion protection
- Perform basic security scanning on your networks and perform "hardening" of your computers
- And more...

YOU WILL COVER:

- TCP/IP Networking
- Secure Architectures
- Packets and Protocols
- Building a Plant Floor Web Server
- Network Security Issues
- And more...

CLASSROOM/LABORATORY EXERCISES:

- Use TCP/IP diagnostic tools in Windows-2000/XP
- Use network analyzers to troubleshoot
- Configure a security firewall for the plant floor
- Perform a basic security scan on a target system
- And more...

COURSE DETAILS:

Course No.: TS12
Length: 5 days
CEUs: 3.5
Price: $2,590 ISA Member/Group Rate
$2,915 Affiliate Member
$3,240 Community Member/List
$2,590 Multi-Registration Rate

2014 SCHEDULE

Research Triangle Park, NC.....24–28 February; 16–20 June
Burbank, CA.....18–22 August
Houston, TX.....17–21 November

"The class was excellent in examining vulnerabilities"
—Matthew Davidson, Technician

Register or learn more at **www.isa.org/Web14/CYBETRN**

Industrial Automation Cybersecurity: Principles and Application

NEW!

This advanced course will expand your practical knowledge of cybersecurity technologies as applied to an industrial setting. The course will familiarize you with the latest developments in cybersecurity, including practical guides to design, implementation, and testing industrial networks and applications to ensure their security and reliability in an industrial production environment. Course topics include the use of Internet technologies, web servers, TCP/IPV6, fiber optics, intrusion protection systems (IPS), virtual private networks (VPNs), and cryptography.

Note: This is an advanced course with a minimum satisfactory completion of ISA courses TS06 and TS12 (or equivalent in experience/training) as a mandatory prerequisite for successful completion of this course.

YOU WILL BE ABLE TO:

- Apply the TCP/IPV6 protocols, addressing, and troubleshooting
- Locate web technologies where they can be used securely for process control
- Develop network security architectures and explain how to use layering and segmentation to improve security
- Use security technologies such as firewalls, VPNs, virtualization, virus scanning, and intrusion protection from a security perspective
- Industrially harden and secure your networks and perform "team red" testing of your systems
- And more...

YOU WILL COVER:

- TCP/IPV6 Networking
- Making Networks Secure
- Secure Architectures
- Building a Secure Plant Floor Web Server
- Security Management
- Practical Cybersecurity Applications
- And more...

CLASSROOM/LABORATORY EXERCISES:

- Configure industrial network security parameters and settings
- Use network analyzers/sniffers/scanners to troubleshoot
- Use web technology to securely display plant data
- Configure a managed switch/router/firewall/VPN for the plant floor
- And more...

COURSE DETAILS:

Course No.: TS13
Length: 4.5 days
CEUs: 3.2
Price: $2,590 ISA Member/Group Rate
$2,915 Affiliate Member
$3,240 Community Member/List
$2,590 Multi-Registration Rate

Includes ISA Standard: ANSI/ISA-62443-2-1(99.02.01)-2009, *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program* ***(A $215 Value!)***

2014 SCHEDULE

Research Triangle Park, NC..... 10–14 March; 28 July – 1 August
Houston, TX..... 13–17 October
King of Prussia, PA..... 19–23 May

Register or learn more at **www.isa.org/Web14/CYBETRN**

Control Systems Security and ANSI/ISA-62443 Webinar Series

Improve your ANSI/ISA-62443 knowledge with these 90-minute, live webinars!

Save up to 25%

when you register for all three webinars in this series at one time! To take advantage of the series pricing, you must call ISA Customer Service at +1 919-549-8411 to register as this offer is not available online.

Cybersecurity Risk Assessment for Automation Systems

Course No.: IC32CW1
Dates: 19 March and 18 June
Risk analysis is an important step in creating a cybersecurity plan for your automation system. Risk analysis not only identifies security vulnerabilities but also provides the business case for the countermeasures that reduce risk. This webinar introduces control engineers to the concepts of risk analysis and how they are applied to industrial manufacturing and control systems based on the ANSI/ISA-62443 standards. This webinar is also valuable for IT professionals who wish to learn the special considerations for performing risk analysis on automation systems.

Using Firewalls and Security Zones on the Plant Floor

Course No.: IC32CW2
Dates: 26 March and 25 June
The network firewall is one of the most important tools in any cybersecurity designer's toolbox. This webinar introduces the industrial controls engineer to the world of firewall system design, focusing on how these devices can be effectively deployed on the typical plant floor to help meet the ANSI/ISA-62443 security standards.

A Tour of the ANSI/ISA-62443 Security Standards

Course No.: IC32CW3
Dates: 2 April and 9 July
This webinar introduces you to the ANSI/ISA-62443 Security for Industrial Automation and Control Systems standards and how these are organized. You will be given a brief introduction to the terminology, concepts, and models of ANSI/ISA-62443 cybersecurity and elements of creating a cybersecurity management system.

WEBINAR DETAILS (PER SEMINAR):

You can provide these live quality seminars at your location for an unlimited number of participants for one low site fee:

Pricing (per site): $235 ISA Member
$265 Affiliate Member
$295 Community Member/List
$235 Multi-Registration Rate

Can't attend? Missed the live events?
Recorded versions of these sessions are also available, and are free for ISA members.

New for 2014! Watch for our Industrial Cybersecurity Boot Camp for Managers—**Coming Soon!**

Register or learn more at **www.isa.org/Web14/CYBETRN**

ISA Cybersecurity Tech Pack

Improve cybersecurity defenses and better confront the growing dangers of cyberwarfare with the ISA Cybersecurity Tech Pack.

As a widely recognized, world leader in cybersecurity standards development, training and educational resources, ISA provides the proven technical expertise and know-how to help safeguard industrial automation and control systems. In fact, ISA and its sister organization, the Automation Federation, are currently assisting the Obama administration and US federal agency officials in developing the initial version of a national cybersecurity framework—as called for by President Obama in February of this year.

WHAT IS INCLUDED IN THE ISA CYBERSECURITY TECH PACK?

The ISA Cybersecurity Tech Pack combines critical industry technical papers and PowerPoint presentations written and presented by world-renowned cybersecurity and automation systems experts. The Tech Pack also contains notable ISA technical publications, including the popular *Industrial Network Security* book by David Teumim and ISA's new book, *Industrial Automation and Control Systems Security Principles* by Ronald Krutz. As an added bonus, we have rounded out the Tech Pack with a collection of informative cybersecurity articles from *InTech* magazine.

TECHNICAL PAPERS:

- *Cyber Security Implications of SIS Integration with Control Networks*
- *Practical Nuclear Cyber Security*
- *Establishing an Effective Plant Cybersecurity Program*
- *LOGIIC Benchmarking Process Control Security Standards*
- *Stronger than Firewalls: Strong Cyber-Security Protects the Safety of Industrial Sites*
- *Integrated Perimeter and Critical Infrastructure Protection with Persistent Awareness*
- *Applying ISA/IEC 62443 to Control Systems*
- *Establishing an Effective Plant Cybersecurity Program*
- *Getting Data from a Control System to the Masses While Maintaining Cybersecurity—The Case for "Data Diodes"*
- *Reconciling Compliance and Operation with Real Cyber Security in Nuclear Power Plants*
- *Wastewater Plant Process Protection—Process Hazard Analysis*
- *Water/Wastewater Plant Process Protection: A different approach to SCADA cyber security*
- *Using Cyber Security Evaluation Tool (CSET) for a Wastewater Treatment Plant*
- *Improving Water and Wastewater SCADA Cyber Security*
- *An Overview of ISA-99 & Cyber Security for the Water or Wastewater Specialist*

TECHNICAL BOOKS:

- *Industrial Automation and Control Systems Security Principles* by Ronald L. Krutz
- *Industrial Network Security, Second Edition* by David J. Teumim

INTECH MAGAZINE ARTICLES:

- "ISA Fully Engaged in Cybersecurity"
- "Leveraging DoD wireless security standards for automation and control"
- "13 ways through a firewall: What you don't know can hurt you"
- "Defense in Depth"
- "Executive Corner: What's on YOUR mind?"
- "The Final Say: Securing industrial control systems"
- "Uninterruptible power supplies and cybersecurity"
- "Physical Security 101: Evolving 'defense in depth'"
- "Web Exclusive: Control network secure connectivity simplified"
- "The Final Say: Network security in the Automation world"
- "Executive Corner: Defense in depth: It's more than just the technology"
- "Web Exclusive: Stuxnet: Cybersecurity Trojan horse"

To learn more about or purchase the Cybersecurity Tech Pack, visit **www.isa.org/CYBETechPack**

Capitalize on ISA's leadership in cybersecurity by ordering this compilation of valuable cybersecurity technical papers, publications, and InTech articles—containing the practical insights you can immediately apply in the workplace.

Register or learn more at **www.isa.org/Web14/CYBETRN**

Bring ISA cybersecurity training right to you!
All of ISA's cybersecurity training courses can be taught at your company location through ISA's Onsite Training. Contact ISA at **+1 919-549-8411** or at **info@isa.org** for more information.

Founded in 1945, the International Society of Automation (www.isa.org) is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide Members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities. Based in Research Triangle Park, North Carolina, ISA develops standards, certifies industry professionals, provides education and training, publishes books and technical articles, and hosts conferences and exhibitions for automation professionals. ISA is the founding sponsor of the Automation Federation (www.automationfederation.org).

EP30-2624-1213

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

Get the security and data communications training you need from the ANSI/ISA-62443 experts!
Register or learn more at www.isa.org/Web14/CYBETRN