



OT CYBERSECURITY AND IEC 62443 INDUSTRIAL SECURITY TRAINING COURSE

REF: #CYB28555167



COURSE INTRODUCTION / OVERVIEW:

Operational technology now sits at the center of national infrastructure, manufacturing, energy, water, and transport, and the convergence of industrial control systems with enterprise IT networks has transformed how cyber risk reaches the plant floor. This OT cybersecurity training course gives participants a complete journey from A to Z, from understanding the architecture of industrial control systems, SCADA, DCS, and PLC environments to applying the IEC 62443 series of standards as a practical framework for securing industrial automation and control systems across their entire lifecycle. Participants will explore how threats such as ransomware, supply chain compromise, and targeted attacks on safety instrumented systems differ fundamentally from traditional IT incidents, where availability, safety, and physical consequences take priority over confidentiality. Drawing on the work of Eric D. Knapp and Joel Thomas Langill in their book *Industrial Network Security*, the course explains defense in depth, zones and conduits, and security levels in a way that connects theory to real operational decisions. Participants will learn to conduct OT risk assessments, define target security levels, build a cybersecurity management system aligned with IEC 62443-2-1, and evaluate system and component requirements under IEC 62443-3-3 and IEC 62443-4-2. BIG BEN Training Center has designed this industrial cybersecurity course to help organizations close the gap between engineering and security teams, strengthen operational resilience, and build a sustainable, standards-based OT security program that protects people, processes, and critical assets.

TARGET AUDIENCE / THIS TRAINING COURSE IS SUITABLE FOR:

- OT and ICS security engineers and specialists.
- Control systems, automation, and instrumentation engineers.
- SCADA, DCS, and PLC system administrators.
- IT security professionals moving into operational technology environments.
- Plant managers, operations managers, and maintenance leaders.
- Chief Information Security Officers and cybersecurity managers.
- Risk, compliance, and governance professionals in industrial organizations.
- Process safety and functional safety engineers.
- System integrators and industrial automation solution designers.
- Network engineers responsible for industrial and plant networks.
- Internal and external auditors reviewing industrial security controls.



TARGET SECTORS AND INDUSTRIES:

- Oil and gas, including upstream, midstream, and downstream operations facing high safety and regulatory demands.
- Electric power generation, transmission, and distribution utilities.
- Water and wastewater treatment and distribution facilities.
- Petrochemical, chemical, and refining plants with complex process control systems.
- Manufacturing and discrete production facilities adopting Industry 4.0 technologies.
- Pharmaceutical and life sciences production under strict quality and compliance requirements.
- Transportation, ports, airports, and rail signaling systems.
- Mining, metals, and heavy industry operations.
- Smart buildings, data centers, and facility management systems.
- Government agencies, regulators, and national critical infrastructure authorities, and equivalent public bodies.

TARGET ORGANIZATIONS DEPARTMENTS:

- OT and industrial cybersecurity departments.
- Information security and cyber defense departments.
- Engineering and automation departments.
- Operations and production departments.
- Maintenance and reliability departments.
- Health, safety, and environment departments.
- Risk management and compliance departments.
- Internal audit departments.
- Procurement and supply chain departments managing industrial vendors.
- IT infrastructure and network departments.



COURSE OFFERINGS:

By the end of this course, the participants will have able to:

- Explain the architecture of industrial control systems and the key differences between IT and OT security priorities.
- Interpret the structure, roles, and parts of the IEC 62443 series of standards.
- Conduct a structured OT cybersecurity risk assessment aligned with IEC 62443-3-2.
- Define security zones, conduits, and target security levels for industrial environments.
- Design a defense-in-depth architecture for industrial networks using segmentation and secure remote access.
- Apply foundational requirements and system security requirements from IEC 62443-3-3.
- Build and maintain an industrial cybersecurity management system aligned with IEC 62443-2-1.
- Evaluate vendor and component security using IEC 62443-4-1 and IEC 62443-4-2.
- Develop OT incident detection, response, and recovery plans that protect safety and availability.
- Prepare a practical roadmap for IEC 62443 compliance and continuous improvement.

COURSE METHODOLOGY:

This course follows an applied, scenario-driven learning approach that blends structured expert instruction with intensive hands-on practice, so that participants leave with skills they can transfer directly to their own industrial environments. Each day opens with focused presentations that explain core OT cybersecurity principles and the relevant parts of IEC 62443 in clear, practical language, followed by guided discussions that connect each concept to real operational challenges. Detailed case studies of well-documented industrial cyber incidents allow participants to analyze attack paths, identify missed controls, and propose corrective measures based on the standard. Teamwork is central to the experience: participants work in small cross-functional groups that mirror the collaboration needed between engineering, operations, and security teams, completing exercises such as mapping zones and conduits for a sample plant, assigning target security levels, and drafting sections of a cybersecurity management system. Interactive sessions include tabletop incident response simulations, risk assessment workshops, and structured debates on trade-offs between security, safety, and availability. Throughout the program, trainers provide continuous, constructive feedback on group outputs and individual contributions, while short knowledge checks at the end of each unit reinforce key learning points. BIG BEN Training Center ensures that every activity is linked to measurable objectives, so participants can confidently apply IEC 62443 practices and strengthen industrial cybersecurity maturity in their organizations.



COURSE AGENDA (COURSE UNITS):

UNIT ONE: FOUNDATIONS OF OT CYBERSECURITY AND INDUSTRIAL CONTROL SYSTEMS

- Introduction to operational technology and its role in critical infrastructure.
- Components of industrial control systems including SCADA, DCS, PLC, RTU, and HMI.
- The Purdue Enterprise Reference Architecture and its security relevance.
- Key differences between IT and OT security priorities and constraints.
- Industrial communication protocols such as Modbus, DNP3, OPC UA, and PROFINET.
- IT and OT convergence and the expanding industrial attack surface.
- The OT threat landscape including ransomware, insider threats, and nation-state actors.
- Lessons learned from major industrial cyber incidents.

UNIT TWO: UNDERSTANDING THE IEC 62443 SERIES OF STANDARDS

- Purpose, scope, and evolution of the IEC 62443 series.
- Structure of the standard across general, policies and procedures, system, and component parts.
- Roles of asset owners, system integrators, and product suppliers.
- Key concepts including foundational requirements and security levels.
- Defense in depth as a guiding principle of IEC 62443.
- The relationship between IEC 62443, ISO/IEC 27001, and the NIST Cybersecurity Framework.
- Mapping IEC 62443 requirements to the industrial automation lifecycle.
- Common misconceptions and challenges in adopting the standard.



UNIT THREE: OT RISK ASSESSMENT, ZONES, CONDUITS, AND SECURITY LEVELS

- Risk assessment methodology according to IEC 62443-3-2.
- Identifying the system under consideration and critical industrial assets.
- Defining security zones and conduits for industrial networks.
- Threat modeling and vulnerability analysis in OT environments.
- Evaluating consequences for safety, environment, production, and reputation.
- Determining target, capability, and achieved security levels.
- Integrating cybersecurity risk with process hazard analysis and functional safety.
- Documenting cybersecurity requirements specifications.

UNIT FOUR: SECURE INDUSTRIAL NETWORK ARCHITECTURE AND TECHNICAL CONTROLS

- System security requirements and security levels under IEC 62443-3-3.
- Network segmentation, industrial firewalls, and demilitarized zones.
- Secure remote access for vendors and engineering teams.
- Identification, authentication, and use control for industrial users and devices.
- Patch management and vulnerability handling in operational environments.
- Asset inventory, configuration management, and system hardening.
- Continuous OT network monitoring and anomaly detection.
- Component security requirements under IEC 62443-4-2 and secure development under IEC 62443-4-1.

UNIT FIVE: OT CYBERSECURITY MANAGEMENT, INCIDENT RESPONSE, AND COMPLIANCE ROADMAP

- Establishing a cybersecurity management system aligned with IEC 62443-2-1.
- Governance, roles, responsibilities, and policies for OT security.
- Security awareness and competency development for engineering and operations staff.
- OT incident response planning, detection, containment, and recovery.
- Business continuity and disaster recovery for industrial operations.
- Supplier and supply chain security management.
- Measuring OT cybersecurity maturity and preparing for audits and certification.
- Building a practical IEC 62443 implementation and continuous improvement roadmap.



FAQ:

QUALIFICATIONS REQUIRED FOR REGISTERING TO THIS COURSE?

There are no requirements.

HOW LONG IS EACH DAILY SESSION, AND WHAT IS THE TOTAL NUMBER OF TRAINING HOURS FOR THE COURSE?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

SOMETHING TO THINK ABOUT:

If an industrial facility achieves every technical security level defined by IEC 62443 yet engineers and security teams still define risk in fundamentally different ways, can the organization truly claim to be secure, or does genuine OT resilience depend more on shared judgment than on compliance itself?

WHAT UNIQUE QUALITIES DOES THIS COURSE OFFER COMPARED TO OTHER COURSES?

This course stands apart because it treats OT cybersecurity as an engineering discipline rather than an extension of traditional IT security. Many programs focus narrowly on tools or on abstract compliance checklists, while this course builds a deep understanding of why industrial environments demand a different mindset, where safety, availability, and physical consequences shape every security decision. Participants do not simply read about IEC 62443; they apply it step by step, moving from risk assessment and zone and conduit design to security level selection, management system development, and supplier evaluation, all through realistic industrial scenarios. The course bridges the long-standing gap between control engineers and cybersecurity professionals by placing both perspectives in the same exercises, encouraging a shared language and shared ownership of risk. Practical examples drawn from energy, water, manufacturing, and oil and gas illustrate how attacks unfold in real plants and how well-designed controls could have changed the outcome. The academic depth of the content is balanced with immediate workplace relevance, so participants return with a clear roadmap they can present to leadership and begin implementing. BIG BEN Training Center combines expert facilitation, structured collaboration, and continuous feedback to deliver an industrial cybersecurity learning experience that strengthens individual competence and organizational resilience, helping participants become confident leaders of IEC 62443 adoption within their organizations.