Securing Oil and Gas Industrial Control Systems Training Course



20 - 24 Dec 2026

Amman

3800 € (Per Person)

Ref: #OG2466_225336

Course Introduction / Overview:

The convergence of Information Technology (IT) and Operational Technology (OT) has created unprecedented efficiencies in the oil and gas sector, but it has also exposed critical Industrial Control Systems (ICS) to significant cyber threats. This specialized training course provides a comprehensive A-to-Z exploration of the principles and practices required to secure these vital systems. We delve into the unique challenges of protecting SCADA, DCS, and PLCs in upstream, midstream, and downstream operations, moving beyond generic IT security to address the specific protocols, legacy systems, and physical safety implications of the industrial environment. As discussed by leading expert Andrew Ginter in works like "SCADA Security: What's Broken and How to Fix It," the approach to OT security must be fundamentally different. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the knowledge to build a robust defense-in-depth strategy, aligning with international standards like IEC 62443. Participants will gain practical skills to identify vulnerabilities, implement effective controls, and manage incidents, ensuring the resilience and integrity of critical national infrastructure against a backdrop of evolving cyber risks.

Target Audience / This training course is suitable for:

- Control Systems Engineers and Technicians.
- SCADA and DCS Operators.
- IT and Cybersecurity Professionals working with OT environments.
- Process Safety and Automation Engineers.
- Plant and Operations Managers.
- Instrument and Control Technicians.
- Corporate Risk and Compliance Officers.
- Industrial Network Architects.
- Health, Safety, and Environment (HSE) Managers.
- Government and Regulatory Agency Staff.

Target Sectors and Industries:

- Oil and Gas (Upstream Exploration and Production).
- Oil and Gas (Midstream Transportation and Storage).
- Oil and Gas (Downstream Refining and Processing).
- Petrochemical and Chemical Manufacturing.
- Liquefied Natural Gas (LNG) Plants.
- Offshore and Onshore Drilling Operations.
- Pipeline Operators.
- Governmental bodies and energy sector regulators.

Target Organizations Departments:

- Operations and Production.
- Information Technology (IT) and Cybersecurity.
- Engineering and Maintenance.
- Health, Safety, and Environment (HSE).
- Risk Management and Compliance.
- Automation and Process Control.
- Physical Security.
- Project Management.

Course Offerings:

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

- Differentiate between IT and OT security objectives, priorities, and constraints.
- Analyze the specific cyber threats and vulnerabilities facing the oil and gas industry.
- Apply the Purdue Model to design secure industrial network architectures.
- Implement key principles from the IEC 62443 and NIST Cybersecurity Frameworks.
- Assess and mitigate risks in legacy and modern Industrial Control Systems.
- Develop strategies for secure remote access to OT environments.
- Conduct vulnerability assessments tailored for sensitive industrial systems.
- Create and implement a comprehensive ICS incident response plan.
- Foster a strong cybersecurity culture that bridges the IT and OT divide.
- Evaluate security controls for industrial protocols like Modbus, DNP3, and OPC.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum engagement and practical application. This course moves beyond theoretical lectures to immerse participants in the real-world challenges of ICS security. The program is built on a foundation of interactive presentations, expert-led discussions, and collaborative group exercises. Participants will analyze detailed case studies of actual cyber incidents in the energy sector, deconstructing attack vectors and response strategies to draw actionable lessons. Team-based activities will focus on practical tasks such as conducting a cyber risk assessment for a model refinery, designing a segmented network based on the Purdue Model, and simulating an incident response tabletop exercise. This hands-on approach ensures that participants not only understand the concepts but can also apply them directly to their operational environments. Continuous feedback and Q&A sessions are integrated throughout the course, fostering a dynamic learning environment where theoretical knowledge is transformed into tangible, job-ready skills.

Course Agenda (Course Units):

Unit One: Foundations of ICS and OT Security in Oil and Gas

- Introduction to Industrial Control Systems (ICS) and Operational Technology (OT).
- Key differences between IT and OT security priorities and environments.
- Overview of SCADA, DCS, PLCs, and SIS in the oil and gas context.
- Specific cyber threats targeting upstream, midstream, and downstream operations.
- Historical ICS cyber incidents and their impact on the energy sector.
- Understanding the consequences of a cyber-attack on safety and production.
- The critical role of cybersecurity in process safety management.

Unit Two: Security Frameworks and Secure Architecture

- Introduction to the Purdue Enterprise Reference Architecture (Purdue Model).
- Applying network segmentation and segregation in OT environments.
- Deep dive into the ISA/IEC 62443 series of standards.
- Utilizing the NIST Cybersecurity Framework (CSF) for critical infrastructure.
- Defining security zones, conduits, and security levels.
- Architecting a defense-in-depth strategy for an oil and gas facility.
- Secure integration of IT and OT networks.

Unit Three: Implementing Technical Security Controls in OT

- Configuring and managing industrial firewalls and unidirectional gateways.
- Implementing secure remote access solutions for vendors and engineers.
- Application whitelisting and system hardening for industrial endpoints.
- Managing patches and updates in a 24/7 operational environment.
- Physical security controls for control rooms and critical assets.
- Securing industrial network protocols (e.g., Modbus TCP, DNP3).
- Introduction to Intrusion Detection Systems (IDS) for OT networks.

Unit Four: Threat Detection, Vulnerability Management, and Intelligence

- Developing an OT-specific vulnerability management program.
- Passive asset discovery and network monitoring techniques.
- Safe and non-disruptive methods for vulnerability scanning in ICS.
- Leveraging threat intelligence to understand adversary tactics.
- Log collection and analysis using SIEM for OT environments.
- Recognizing indicators of compromise (IOCs) in an industrial network.
- Conducting effective security assessments and audits.

Unit Five: Incident Response, Recovery, and Governance

- Developing a comprehensive ICS Incident Response (IR) plan.
- Roles and responsibilities of the Cyber Security Incident Response Team (CSIRT).
- Incident containment, eradication, and recovery strategies for OT.
- Forensic readiness and evidence handling in an industrial setting.
- Creating and testing disaster recovery and business continuity plans.
- Building a corporate governance model for OT cybersecurity.
- Promoting a strong security awareness and training culture across the organization.

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:

Considering the increasing integration of IIoT devices in oil and gas operations, how does the traditional air-gapped security model need to evolve to address new, unforeseen threat vectors?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond generic cybersecurity principles to offer a highly specialized focus on the unique operational realities of the oil and gas industry. Unlike broader programs, every module is contextualized with sector-specific examples, from the risks facing offshore platforms to the vulnerabilities in pipeline control systems. The curriculum is built around the practical application of globally recognized standards like IEC 62443, ensuring participants learn not just the "what" but the "how" of implementing a robust security posture. A key differentiator is the deep emphasis on the IT/OT convergence challenge, providing actionable strategies for bridging the cultural and technical gap between enterprise and industrial teams. Rather than just listing tools, the course focuses on developing a strategic mindset, enabling participants to build a resilient, defense-in-depth architecture tailored to their specific environment. The use of real-world case studies from the energy sector provides an unparalleled level of insight, preparing professionals to anticipate, detect, and respond to the sophisticated threats targeting critical infrastructure.