SCADA Systems Design and Cyber Security Implementation Training Course



14 - 18 Dec 2026

Cape town

4600 € (Per Person)

Ref: #ERE4418_273948

Course Introduction / Overview:

This course provides a comprehensive exploration of Supervisory Control and Data Acquisition (SCADA) systems, focusing on both secure design principles and robust cybersecurity implementation. In an era where industrial control systems (ICS) are increasingly targeted by cyber threats, a holistic understanding of both operational technology (OT) and security is paramount for protecting critical infrastructure. This program, offered by BIG BEN Training Center, bridges the critical gap between engineering design and cybersecurity defense. We delve into the foundational concepts of SCADA architecture, from PLCs and HMIs to communication protocols, and then build upon this with advanced cybersecurity strategies. Drawing on insights from leading experts like Eric J. Knapp and foundational texts such as "Industrial Network Security," the course navigates the complexities of securing these unique environments. Participants will learn to apply international standards like IEC 62443 and the NIST Cybersecurity Framework to real-world scenarios, ensuring they can design, implement, and maintain SCADA systems that are not only efficient and reliable but also resilient against modern cyber-attacks. This training moves beyond theory to provide actionable skills for safeguarding the industrial processes that power our world.

Target Audience / This training course is suitable for:

- Control Systems Engineers and Technicians.
- SCADA System Operators and Administrators.
- IT Security Professionals moving into OT environments.
- Industrial Automation Specialists.
- Network Engineers responsible for ICS networks.
- Plant Managers and Operations Supervisors.
- Cybersecurity Analysts and Consultants.
- Instrumentation and Control Professionals.
- Critical Infrastructure Protection Planners.
- Government and Regulatory Compliance Officers.

Target Sectors and Industries:

- Energy and Utilities (Electricity, Oil, and Gas).
- Water and Wastewater Management.
- Manufacturing and Industrial Automation.
- Transportation and Logistics (Rail, Airports, Ports).
- Pharmaceuticals and Chemical Processing.
- Building Management and Automation Systems.
- Telecommunications Infrastructure.
- Government agencies and public sector services.
- Food and Beverage Production.

Target Organizations Departments:

- Operations and Production.
- Information Technology (IT) and Cybersecurity.
- Engineering and Technical Services.
- Health, Safety, and Environment (HSE).
- Risk Management and Compliance.
- Maintenance and Reliability.
- Research and Development.
- Physical Security.
- Corporate Governance.

Course Offerings:

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

- Analyze the components and architectures of modern SCADA and ICS environments.
- Design secure SCADA network architectures using principles like segmentation and defense-in-depth.
- Identify common vulnerabilities within PLCs, HMIs, and industrial protocols.
- Apply the IEC 62443 and NIST Cybersecurity Framework to industrial settings.
- Develop and implement effective security policies for Operational Technology (OT).
- Configure industrial firewalls and intrusion detection systems for SCADA networks.
- Conduct risk assessments and vulnerability analysis specific to ICS.
- Develop a robust incident response plan for cybersecurity events in a SCADA environment.
- Secure remote access connections to critical industrial systems.
- Evaluate the security implications of IT and OT convergence.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that mastering SCADA security requires more than theoretical knowledge; it demands hands-on application. The course combines expert-led instruction with dynamic group discussions, allowing participants to share experiences and challenge concepts in a collaborative setting. A significant portion of the training is dedicated to analyzing real-world case studies of ICS cyber incidents, deconstructing attack vectors and successful defense strategies. Participants will engage in practical exercises and simulated lab environments that replicate common SCADA architectures, where they can apply design principles and security controls without risk to live systems. Team-based workshops will challenge attendees to develop security policies, design a secure network, and formulate an incident response plan for a hypothetical industrial plant. Continuous feedback is provided by the instructor, an industry veteran, ensuring that participants can directly relate the course material to the unique challenges they face in their own organizations. This blended approach ensures a deep and lasting understanding of the subject matter.

Course Agenda (Course Units):

Unit One: Fundamentals of SCADA and Industrial Control Systems

- Introduction to SCADA, DCS, and PLC Systems.
- Key Components: HMI, RTU, MTU, and Communication Links.
- Comparing IT and OT Environments and Security Priorities.
- Common Industrial Protocols (Modbus, DNP3, Profinet).
- The Purdue Model for Industrial Control System Architecture.
- Understanding Real-Time Operational Constraints.
- The Evolution of Industrial Networks and Connectivity.

Unit Two: Secure SCADA System Design and Architecture

- Principles of Secure-by-Design for Industrial Systems.
- Implementing Defense-in-Depth Strategies in OT.
- Effective Network Segmentation and Segregation.
- Designing Secure Zones and Conduits per IEC 62443.
- Secure Remote Access Solutions (VPNs, Jump Hosts).
- Architectural Considerations for System Redundancy and Availability.
- Physical Security Controls for SCADA Environments.

Unit Three: The ICS and SCADA Cyber Threat Landscape

- Identifying Threat Actors: Nation-States, Hacktivists, and Insiders.
- Common Attack Vectors Targeting Industrial Environments.
- Analysis of Major ICS Cyber Incidents (e.g., Stuxnet, Triton, Black Energy).
- Vulnerability Assessment for SCADA Components.
- Introduction to OT-Specific Malware and Ransomware.
- Leveraging Threat Intelligence for Proactive Defense.
- Understanding the ICS Cyber Kill Chain.

Unit Four: Implementing Cybersecurity Controls and Standards

- Applying the NIST Cybersecurity Framework to OT.
- Deep Dive into the IEC 62443/ISA-99 Standard Series.
- Configuring and Managing Industrial Firewalls and Unidirectional Gateways.
- Deploying Intrusion Detection and Prevention Systems (IDS/IPS) for OT.
- System Hardening for Workstations, Servers, and PLCs.
- Implementing Application Whitelisting and Access Control.
- Patch Management Strategies for Critical Systems.

Unit Five: Advanced Security, Incident Response, and Compliance

- Developing an ICS-Specific Incident Response Plan.
- Digital Forensics and Evidence Collection in OT Environments.
- Conducting Penetration Testing and Security Audits for SCADA.
- Managing Security for the Industrial Internet of Things (IIoT).
- Ensuring Regulatory and Standard Compliance.
- Building a Culture of Security within Operations.
- Future Trends and Challenges in SCADA Cybersecurity.

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:

As operational technology (OT) and information technology (IT) continue to converge, how can organizations culturally and technically bridge the gap to create a unified security posture without compromising operational safety and reliability?

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

This course distinguishes itself by holistically integrating two traditionally separate disciplines: system design and cybersecurity implementation. Unlike programs that focus solely on securing existing systems, this training begins with the principle of "secure-by-design," teaching participants how to build resilient and defensible SCADA architectures from the ground up. This foundational approach ensures that security is not an afterthought but a core component of the system lifecycle. Furthermore, the curriculum places a heavy emphasis on the practical application of global standards like IEC 62443 and the NIST Cybersecurity Framework, moving beyond theoretical discussion to hands-on, scenario-based learning. Participants learn not just what the standards say, but how to interpret and apply them within the unique constraints of an operational environment where availability and safety are paramount. The course content is meticulously structured to address the entire ecosystem, from securing individual PLCs and field devices to developing enterprise-level incident response plans. This comprehensive perspective, which bridges the gap between engineering and security, equips professionals with a versatile and strategic skill set that is immediately applicable and highly sought after in the industry.