HIGH POINT CENTER

# course : Process Control Cybersecurity

| | | | |
|---|---|---|---|
| **City :** | Cairo | **Hotel :** | Cairo Marriott Hotel & Omar Khayyam Casino |
| **Start Date :** | 2025-10-26 | **End Date :** | 2025-10-30 |
| **Duration :** | 1 Week | **Price :** | 3950 $ |

HIGH POINT CENTER

## Course Overview

Process control environments are increasingly becoming targets for cyber threats, particularly as industrial systems converge with modern IT networks. Unlike traditional IT assets, Industrial Automation and Control Systems (IACS) play a direct role in monitoring and controlling physical processes, making their protection critical to operational safety and business continuity.

Recent studies highlight the severity of these challenges. For example, research by Siemens and the Ponemon Institute revealed that three out of four oil and gas organizations in the Middle East have faced a cybersecurity compromise resulting in either data loss or operational disruption. Furthermore, nearly half of cyberattacks against Operational Technology (OT) environments are believed to go undetected. Given the oil and gas sector's strategic role in regional economies, the risks associated with IT/OT convergence are both significant and urgent.

The Process Control Cybersecurity Training Course provides participants with the essential knowledge and practical skills required to secure IACS and OT environments. The course addresses global cybersecurity standards, risk management practices, and effective countermeasures, while also equipping participants with diagnostic and incident response capabilities.

## Course Objectives

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

Identify the process control assets that require protection.

Understand the current industrial security environment and its unique challenges.

Explain the core principles of the IEC 62443 industrial security standard.

Conduct risk assessments and apply appropriate cybersecurity countermeasures.

Perform application diagnostics, troubleshooting, and incident response in OT environments.

## Target Audience

This course is designed for a wide range of professionals involved in industrial operations, cybersecurity, and process control, including:

Operations and Maintenance Personnel

Process Control Operators and Engineers

Plant and Project Managers

Instrumentation Technicians and Engineers

System Integrators
IT/OT Engineers and Managers in Industrial Facilities
Security, Safety, and Risk Management Professionals
Any professional addressing cybersecurity in industrial environments

## Methodology

The course employs proven adult learning techniques designed to maximize comprehension and retention.
Methods include:
Structured presentations and expert-led discussions.
Group exercises and simulations.
Case studies and scenario-based learning.
Practical paper exercises and evaluations at the end of each module.
Continuous engagement through Q&A and interactive sessions.

## Course Outline

Day One – Introduction and Cybersecurity Fundamentals
Overview of process control cybersecurity
The current industrial security environment
IT vs. OT: similarities and differences
Fundamentals of process control and communication networks
Threats, vulnerabilities, and attack pathways
Asset identification and impact assessment
Day Two – IACS Cybersecurity Lifecycle and IEC 62443
Phases of the IACS cybersecurity lifecycle (identification, design, operations)
Limitations of conventional IT approaches
IEC 62443 security standards and framework
Cybersecurity assurance levels (CAL)
Functional requirements and implementation strategies
Day Three – Addressing Security Risks and Countermeasures
Endpoint security: antivirus and anti-spyware
Firewalls, intrusion detection, and traffic analysis
Encryption and Virtual Private Networks (VPNs)
Authentication systems and password management
Access control and network segmentation

Day Four – Application Diagnostics and Troubleshooting
Interpreting device alarms and event logs
Identifying early warning indicators
Network intrusion detection systems (NIDS)
Network management and monitoring tools
Application alarms, whitelisting, and endpoint protection
Security Incident and Event Management (SIEM) tools
Day Five – Operating Procedures, Tools, and Incident Response
Management of change procedures in IACS environments
Configuration and patch management tools
Cybersecurity audits and compliance monitoring
Antivirus and whitelisting implementation
Developing and executing an incident response plan
Incident investigation, system recovery, and lessons learned

## Certificates

On successful completion of this training course, HighPoint Certificate will be awarded to the delegates.
Continuing Professional Education credits (CPE): In accordance with the standards of the National Registry of CPE Sponsors, one CPE credit is granted per 50 minutes of attendance.