# Process Control Cybersecurity

## INTRODUCTION

- This Process Control Cybersecurity training seminar will address the most important issues related to the protection of assets in a process control environment. Unlike traditional IT (information technology) systems, process control assets include IACS (Industrial Automation and Control Systems) which need to be protected.
- Recently, three out of four organizations in the oil and natural gas industry in the Middle East have experienced a security compromise that resulted in the loss of confidential data or Operational Technology (OT) disruption. This is according to a recent study by Siemens and the Ponemon Institute. Another finding in the report is that – organizations believe that roughly one in every two cyber-attacks against the OT environment actually goes undetected. The report also notes that the oil and gas industry is the target of as much as one-half of all cyberattacks in the Middle East and given its importance for the region's economies, the risks faced by the industry are all the more pressing. OT, which encompasses systems that monitor and control physical devices and industrial processes, is increasingly interconnected with IT networks. In spite of all its benefits, this IT/OT convergence is opening up new avenues for attacks.

GLOMAC

This training seminar will highlight:

- Process Control Assets to be protected
- The Current Industrial Security Environment
- The Process Control Security Standard IEC 62443
- Risk Assessment and Cybersecurity Counter-measures
- Application diagnostics, troubleshooting, and incidence response

## OBJECTIVES

At the end of this training seminar, you will learn to:

- List what process control assets need to be protected
- Understand the Current Industrial Security Environment
- List and explain the main components of the process control security standard IEC 62443
- Understand how to perform risk assessment and apply cybersecurity counter-measures
- Learn how to perform application diagnostics, troubleshooting, and incidence response

## TRAINING METHODOLOGY

- This Process Control Cybersecurity training course will utilize a variety of proven adult learning techniques to ensure maximum understanding, comprehension and retention of the information presented. This would include, but not be limited to; effective presentations, open discussions, simulations, paper exercises, individual and group exercises, as well as small subject evaluations at the completion of every chapter. Questions are encouraged at all times.

## ORGANISATIONAL IMPACT

- Discovering of threats, vulnerabilities affecting a process or plant
- Performing appropriate asset identification and impact assessment
- Using and implementing the standard IEC 62443
- Performing appropriate risk analysis and risk identification
- Addressing security risks
- Protecting process and plant assets
- Implementing process control security counter-measures
- Performing application diagnostics and troubleshooting
- Implementing cybersecurity operating procedures and incident response
- Implementing a cybersecurity process
- Having staff that can make valuable input pertaining to Cybersecurity Operating Procedures & Tools and Incident Response

GLOMAC

## PERSONAL IMPACT

- On this Process Control Cybersecurity training course, participants will gain knowledge and learn to apply themselves, fully, in matters pertaining to Process Control Cybersecurity. Such skills and knowledge should result in better career prospects within the organization, and will play a meaningful role in their abilities to be leaders in their field of expertise.

From a personal impact point of view, this training course will increase your knowledge and experience involving:

- Cybersecurity principles
- The main cybersecurity standards
- Cybersecurity best practices
- The main cybersecurity counter-measures
- Techniques for cybersecurity diagnostics and troubleshooting
- Cybersecurity operating procedures & tools
- Procedures for cybersecurity incident response
- Your ability to show to your organization that you are a valuable team member, and that you can be further developed for senior roles, where necessary
- In addition, delegates will have an opportunity to share cybersecurity experiences and knowledge with fellow delegates and the Instructor.

## WHO SHOULD ATTEND?

This training course is suitable to a wide range of professionals but will greatly benefit:

- Operations and Maintenance Personnel
- Process Control Operators, Engineers
- Process, Plant, and Project Managers
- Process Engineers and Managers
- Instrumentation Technicians and Engineers
- System Integrators
- IT/OT Engineers and Managers Industrial Facilities
- IT/OT Corporate / Security Professionals
- Plant Safety, Security, and Risk Management
- Security Personnel in all categories
- Any individual that needs to address issues in the ever expanding and complex field of cybersecurity in the industrial environment

## Course Outline

### Introduction and Cybersecurity Fundamentals

- Introduction to Process Control Cybersecurity
- Understanding the Current Industrial Security Environment
- How IT and OT (Operational Technology) in the Plant Floor are Different and How They are the Same
- Overview of Process Control
- Overview of Industrial Communication Systems and Networks
- How Cyber-attacks Happen:  Threats, Vulnerabilities, Attacks
- Asset Identification and Impact Assessment

### Introduction to the IACS Cybersecurity Lifecycle and ISA99 / IEC 62443

- Identification & Assessment Phase
- Design & Implementation Phase
- Operations & Maintenance Phase
- Limits of a Conventional IT Approach
- The IEC 62443 Security Approach and Standards
- Risk Analysis Risk Identification, Classification, and Assessment
- CAL (Cybersecurity Assurance Levels)
- Functional Requirements of IEC 62443

GLOMAC

## Addressing Security Risks: Process Control Security Counter-measures

- Antivirus, Anti-spyware
- Firewalls, Traffic Analyzers
- Passwords - Authentication Systems
- Access Control - Intrusion Detection / Prevention

## Application Diagnostics and Troubleshooting

- Interpreting Device Alarms and Event Logs
- Early Indicators
- Network Intrusion Detection Systems
- Network Management Tools
- Interpreting OS and Application Alarms and Event Logs
- Application Management and Whitelisting Tools
- Antivirus and Endpoint Protection Tools
- Security Incident and Event Monitoring (SIEM) Tools

## IACS Cybersecurity Operating Procedures & Tools and Incident Response

- Developing and Following an IACS Management of Change Procedures
- IACS Configuration Management Tools
- Developing and Following an IACS Patch & Antivirus Management and Cybersecurity Audit Procedures
- Patch Management Tools
- Antivirus and Whitelisting Tools
- Auditing Tools
- Developing and Following an IACS Incident Response Plan
- Incident Investigation and System Recovery