# ICS410: ICS/SCADA Security Essentials

**Length**: 5 Days

**Summary:** The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

**Who should attend:** Individuals who influence the attack surface and are responsible for or support efforts to maintain a secure, safe and reliable Industrial Control System environment. The roles performed by personnel specific to this field can be divided into four domains: IT (includes OT support), IT security (includes OT security), engineering, and corporate, industry, and professional standards.

**This course will provide you with:**

- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professional

## COURSE CONTENT

**Day 1: ICS Overview**
- History and overview of ICS
- Field and network components
- Communications
- ICS application overview
- Industry models
- ICS drivers and constraints
- Physical security and safety systems

**Day 2: ICS Attack Surface**
- Overview of attacks
- Attacks on HMIs, control servers, network communications, remote devices

**Day 3: Defending ICS Servers and Workstations**
- ICS Server/Workstation technologies
- Microsoft Windows based systems
- Unix and Linux based systems

**Day 4: Defending ICS Networks and Devices**
- Network fundamentals
- IP Concepts and behaviors
- Firewalls and perimeters
- Wireless
- Cryptography for ICS
- Controller and field-device security

**Day 5: ICS Governance and Resources**
- Information assurance foundations
- Computer security policies
- Contingency and continuity planning
- Risk assessment and auditing
- Password management
- ICS Incident Handling
- Resources