Cybersecurity Training for Operational Technology Engineers

YOKOGAWA
Co-innovating tomorrow™

Course Code

COTE

Course Overview

This course provides engineers with the knowledge and practical know-how needed to secure Industrial Automation and Control Systems (IACS) against evolving cyber threats. With increasing IT/OT convergence and the rising frequency of cyber incidents in IACS, engineers must understand not only technical controls but also architecture, governance, and compliance requirements that shape secure operations.

Participants will learn about secure system architectures, apply risk-based approaches, implement hardening and access control measures, and support incident response and recovery efforts.

Who Can Take This Course

This training is intended for engineers involved in the design, deployment, and maintenance of industrial control systems.

Course Methodology

Lectures, discussions and short quizzes.

Course Outline

You will learn

Lesson 1: Fundamentals of Industrial Automation and Control Systems (IACS) Cybersecurity

- Overview of IACS and OT vs. IT systems
- Unique cybersecurity challenges in IACS
- High-impact incidents

Lesson 2: Architecture and Risk-Based Design

- The Purdue Model and its application in IACS
- Designing zones and conduits
- Assigning Security Levels based on risk
- Security Level Targets (SL-T) vs. Security Level Capability/Achieved/Required (SL-C/A/R)
- Threat and risk assessments (TRA)

Lesson 3: Technical Security Controls

- System hardening practices:
- Patch management and compensating controls in OT
- Secure network design:
- Secure remote access
- Configuration file protection and version control
- Backup and recovery with integrity checks

Lesson 4: Access Control and Identity Management

- Role-Based Access Control (RBAC)
- Managing user accounts on engineering systems
- Secure credential storage and password policies
- Just-in-time access for maintenance

Lesson 5: Incident Response & Recovery

- Cyber incident lifecycle in OT
- Incident containment and recovery
- Investigation facilitation
- Coordination with IT, legal, and plant safety
- Disaster recovery planning and testing

Lesson 6: Compliance and Governance

- Key concepts of security program
- Understanding roles and responsibilities (Asset Owner, Integrator, Service Provider)
- Cybersecurity policies, procedures, and reporting chains

Duration

2 days

Certification

Participant who attains at least 75% attendance will be awarded Certificate of Attendance.

Venue

Yokogawa Engineering Asia Pte. Ltd.
5 Bedok South Road
Singapore 469270

Enquiries

Training Administrator
DID: (65) 6249 3608
Main: (65) 6241 9933
Email: YEA-SG-TSC@yokogawa.com

Refund Scheme

Written Notice of Withdrawal is received	Percentage of Refund
Two weeks or more prior to course commencement date	100%
Less than two weeks prior to course commencement date	50%
On or after the course commencement	0%

All product names mentioned are registered trademarks or trademarks of Yokogawa Electric Corporation.

Yokogawa Engineering Asia Pte. Ltd.
5 Bedok South Road
Singapore 469270

Please note that the contents of this brochure are subject to change without notice.

YOKOGAWA Co-innovating tomorrow™