Cybersecurity Training for Operational Technology Operators

YOKOGAWA
Co-innovating tomorrow™

Course Code
COTO

Course Overview
This course equips plant and field operators with foundational cybersecurity awareness and practical know how to help protect Industrial Automation and Control Systems (IACS) from evolving cyber threats. Operators are often the first to notice irregularities in system behavior; therefore, their understanding of cybersecurity risks and adherence to secure operating practices are crucial in maintaining safe and reliable plant operations.

Participants will understand their critical role in cybersecurity, know how to detect potential threats, and apply secure mindsets consistently to support their organization's operational technology (OT) security posture.

Who Can Take This Course
Control room operators, plant operators, and field technicians involved in day-to-day monitoring and operation of OT systems - Distributed Control System (DCS), Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC).

Course Methodology
Lectures, discussions and short quizzes.

Course Outline
You will learn

Lesson 1: Introduction to Industrial Automation and Control Systems (IACS) Cybersecurity
- What is IACS and how does it differ from IT systems?
- Importance of cybersecurity in IACS environments
- Overview of cybersecurity standards

Lesson 2: Understanding the IACS Environment
- Operational technologies used in IACS
- Industrial communication protocols
- The Purdue Model for IACS network segmentation

Lesson 3: Understanding Cybersecurity Risks in IACS
- Common threats in industrial environments
- Examples of OT security breaches and their impacts
- Case studies of real-world examples of IACS cyber incidents

Lesson 4: Operator Responsibilities and Safe Practices
- Role of operators in a secure IACS environment
- Access control
- Locking screens and sessions
- Reporting abnormal system behaviour or suspicious activity
- Only using approved software, tools, and USBs
- Following plant change management protocols

Lesson 5: Secure use of Human Machine Interfaces (HMIs), Workstations and SCADA
- Proper login/logout procedures
- Identifying indicators of compromise
- Knowing when and how to escalate
- Avoiding accidental cyber incidents
- Cyber hygiene and daily routine

Lesson 6: Reporting and Incident Awareness
- What is a cyber incident from an operator's perspective?
- How to report anomalies quickly and clearly?
- What not to do during a suspected cyber event?
- Operator’s role in supporting incident response

Duration
1 day

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 Policy Statement
Request for withdrawal must be made in writing to Yokogawa Engineering Asia Pte Ltd. Candidate under sponsorship of company must submit withdrawal request written by authorized representative of company. Refund will only be given on advanced notice from course commencement date.

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%

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