Industrial Control Systems (ICS) Cybersecurity

OGT-1025 · 5 days · 30 CPD hours · English

API ASME

OVERVIEW

This training course on **Industrial Control Systems (ICS) Cybersecurity** gives participants a structured, practical understanding of the subject and how it is applied in operating oil, gas and energy businesses. It combines industry standards and proven methods with real operational case studies.

Delegates leave able to apply the techniques immediately in their own organisation, with the confidence to challenge assumptions and improve the way work is planned, executed and reviewed.

OBJECTIVES

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

- Explain the core principles, terminology and standards that underpin the subject
- Apply recognised methods and tools to real operational problems
- Evaluate risks, costs and benefits when making technical and commercial decisions
- Interpret data and reports to support evidence based recommendations
- Contribute confidently to multidisciplinary teams and improvement initiatives

TRAINING METHODOLOGY

This training course uses a mix of proven adult learning techniques: structured presentations, worked examples, industry case studies, group exercises, facilitated discussion and practical problem solving. Delegates are encouraged to bring examples from their own operations.

ORGANISATIONAL IMPACT

- Improved technical decision making across the organisation
- Reduced operational, safety and commercial risk exposure
- Consistent application of international standards and best practice
- Better planning, cost control and asset performance
- A stronger internal capability and knowledge base

PERSONAL IMPACT

- Greater confidence in your technical and professional judgement
- Practical tools you can apply immediately in your role
- A clearer view of how your work connects to business performance

- Recognised professional development towards your career goals

WHO SHOULD ATTEND

This training course is suitable for a wide range of professionals working in or alongside Cybersecurity, in particular:

- Engineers, specialists and technical leads
- Supervisors, team leaders and department managers
- Planners, analysts and project professionals
- Anyone preparing to take on wider responsibility in this area

COURSE OUTLINE

Day 1

- Session objectives and key concepts
- Applicable codes, standards and industry practice
- Worked examples and case studies
- Group exercise and discussion
- Review and knowledge check

Day 2

- Session objectives and key concepts
- Applicable codes, standards and industry practice
- Worked examples and case studies
- Group exercise and discussion
- Review and knowledge check

Day 3

- Session objectives and key concepts
- Applicable codes, standards and industry practice
- Worked examples and case studies
- Group exercise and discussion
- Review and knowledge check

Day 4

- Session objectives and key concepts
- Applicable codes, standards and industry practice
- Worked examples and case studies
- Group exercise and discussion
- Review and knowledge check

Day 5

- Session objectives and key concepts

- Applicable codes, standards and industry practice
- Worked examples and case studies
- Group exercise and discussion
- Review and knowledge check

SCHEDULED DATES

Dates	Venue	Format	Fee
07 - 11 Dec 2026	Khamis Mushait, Saudi Arabia	In person	$5,500
01 - 05 Feb 2027	Al Khobar, Saudi Arabia	In person	$5,400
01 - 05 Mar 2027	Oslo, Norway	In person	$5,800
01 - 05 Mar 2027	Dammam, Saudi Arabia	In person	$5,800

CERTIFICATE

A Certificate of Completion is awarded to delegates who attend and complete the course.