



Industrial Cybersecurity (IEC 62443)

Instrumentation, Control & Automation

QGT-INS-116 | Foundation | 5 or 10 days | Online, classroom, in-house

Course overview

Industrial Cybersecurity (IEC 62443) is an introduction that builds a solid working knowledge in Industrial Cybersecurity (IEC 62443). It covers the principles, the requirements of ISA, IEC 61511, IEC 61508 and IEC 62443, and the practical methods used on site, with case studies from operations in the Gulf, Africa and worldwide. Available online, in the classroom in 60 cities, or in-house.

What participants will be able to do

- Explain the principles, terminology and scope of Industrial Cybersecurity (IEC 62443)
- Apply the relevant requirements of ISA, IEC 61511, IEC 61508 and IEC 62443
- Use practical tools, checklists and calculations with confidence
- Recognise common problems, risks and root causes and choose the right corrective action
- Prepare an improvement plan for their own site or organisation

Who should attend

Designed for instrument and control engineers, technicians and control room staff, new joiners and anyone who needs a solid grounding in the subject.

Course outline (5 days)

Day 1: Principles and terminology

Scope, key definitions and how Industrial Cybersecurity (IEC 62443) fits into daily operations

Day 2: Codes, standards and requirements

What ISA, IEC 61511, IEC 61508 and IEC 62443 require, and how to read them

Day 3: Methods, tools and calculations

Step-by-step methods, checklists and worked examples

Day 4: Operation, inspection and common problems

Typical failures, warning signs and what to do about them

Day 5: Case studies, workshop and assessment

Group exercise on real cases and a final knowledge check

What the 10-day edition adds

Day 6: Applied project, part 1 – Apply the week-one methods to a case from your organisation

Day 7: Data and digital tools – Software, spreadsheets and digital tools used in practice

Day 8: Lessons from incidents and audits – What investigations and audit findings teach

Day 9: Applied project, part 2 – Complete, test and refine your solution

Day 10: Presentations and final assessment – Present to the group and complete the final assessment

Fees (USD per participant)

Duration	Live online	Classroom	In-house
5 days	\$3,000	\$5,500	On quote
10 days	\$5,500	\$9,900	On quote

Fees include course material and certificate of completion; classroom fees include refreshments and lunch. In-house training is priced per group.

Dates and cities 2027–2030

Dates	City	Format	Duration	Fee
1–5 Feb 2027	Bangkok	Classroom	5 days	\$5,500
11–22 Apr 2027	Kuwait City	Classroom	10 days	\$9,900
29 Aug – 2 Sep 2027	Jeddah	Classroom	5 days	\$5,500
17–28 Oct 2027	Muscat	Classroom	10 days	\$9,900
8–12 Nov 2027	Online (live)	Online (live)	5 days	\$3,000
17–21 Jan 2028	Milan	Classroom	5 days	\$5,500
5–16 Jun 2028	Beirut	Classroom	10 days	\$9,900
13–17 Nov 2028	Paris	Classroom	5 days	\$5,500
20 Nov – 1 Dec 2028	Edinburgh	Classroom	10 days	\$9,900
27 Nov – 1 Dec 2028	Online (live)	Online (live)	5 days	\$3,000
12–16 Mar 2029	Frankfurt	Classroom	5 days	\$5,500
6–17 Aug 2029	Zurich	Classroom	10 days	\$9,900
8–12 Oct 2029	Singapore	Classroom	5 days	\$5,500
22 Oct – 2 Nov 2029	Nairobi	Classroom	10 days	\$9,900
29 Oct – 2 Nov 2029	Online (live)	Online (live)	5 days	\$3,000
29 Apr – 3 May 2030	Tbilisi	Classroom	5 days	\$5,500
9–20 Jun 2030	Kuwait City	Classroom	10 days	\$9,900
14–18 Oct 2030	Lagos	Classroom	5 days	\$5,500
28 Oct – 8 Nov 2030	Dublin	Classroom	10 days	\$9,900
18–22 Nov 2030	Online (live)	Online (live)	5 days	\$3,000

How to register

Register online or scan the code

<https://qimmatrainig.com/courses/industrial-cybersecurity-iec-62443/>

WhatsApp: +971 50 697 0908

Email: training@qimmatrainig.com

