GTC Transforming Emerging Economies
GTC Training Consulting Group
Ltd, 22 Kumasi Crescent,
Off Aminu Kano Crescent,
Wuse 2, Abuja.
Tel: +234(0) 9056761232
Email:enquiries@thegtcgroup.com
Web:www.thegtcgroup.com

Cybersecurity Fundamentals for Industrial Control

COURSE OVERVIEW

This course provides foundational cybersecurity knowledge tailored for Industrial Control Systems (ICS). It covers the unique threats, vulnerabilities, and risk management strategies relevant to critical infrastructure environments such as SCADA, DCS, and PLC systems. The course bridges cybersecurity basics with industrial-specific security challenges, preparing professionals to defend against evolving cyber threats targeting critical infrastructure. Participants will learn practical approaches to protect industrial networks, secure communication protocols, and maintain operational resilience in automated and connected industrial processes.

WHO SHOULD ATTEND?

This course is ideal for engineers, system architects, IT and OT professionals, automation specialists, and cybersecurity practitioners involved in industrial control, operational technology (OT) security, or responsible for safeguarding industrial networks and processes. It is also suited for technical teams supporting industrial automation, embedded systems, and IoT devices in industrial environments.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Identify and analyze cybersecurity threats and vulnerabilities specific to industrial control systems.
- Implement cryptographic methods and secure communication protocols adapted to ICS environments.
- Design secure architectures for industrial software and hardware systems.
- Apply network security principles and layered defence strategies for OT networks.
- Conduct security testing, vulnerability assessments, and risk management tailored to ICS.
- Develop and execute incident response plans and forensic procedures for industrial environments.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- Core cybersecurity principles as they apply to industrial control systems and critical infrastructure.
- Cryptography and communication security tailored for SCADA, PLC, and DCS protocols.
- Secure software development lifecycle and best practices specific to industrial software.
- Network segmentation, access control, and defence-in-depth strategies for OT networks.
- Security testing methodologies and vulnerability assessment tools for ICS environments.
- Regulatory compliance standards such as ISA/IEC 62443 and their application.
- Incident response planning, digital forensics, and mechanisms to maintain operational continuity during cyber incidents.
- Emerging threats like ransomware and advanced persistent threats (APTs) targeting ICS and how to mitigate them effectively.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.
1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded