GTC International Consulting Limited
Riverbank House
1 Putney Bridge Approach
Fulham, London, SW6 3BQ
T: +44(0)2037055710
E:enquiries@thegtcgroup.com
W: www.thegtcgroup.com

Cybersecurity and SCADA System Integrity in Power Plant Operations

COURSE OVERVIEW

This course provides an in-depth understanding of how to secure critical power generation and distribution infrastructure from evolving cyber threats. The course curriculum delves into the intersection of cybersecurity, operational technology (OT), and power engineering, emphasizing practical frameworks for assessing vulnerabilities, implementing robust defenses, and maintaining the integrity of SCADA systems. Participants will gain insight into the architecture of SCADA networks, threat vectors that exploit these systems, and modern strategies for intrusion detection, access control, and incident response.

WHO SHOULD ATTEND?

This course is designed for power plant engineers, SCADA operators, control system engineers, cybersecurity specialists, IT/OT integration professionals, risk managers, maintenance supervisors, plant managers, and government regulators involved in the protection of energy assets. It is equally valuable for project engineers, grid operators, consultants and professionals seeking to integrate cybersecurity best practices, monitoring, and resilience planning within power plant operations.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Identify common cybersecurity vulnerabilities and threats in power plant control systems.
- Implement layered defense mechanisms to protect SCADA systems from cyber intrusions.
- Apply global cybersecurity standards (NIST, IEC, ISO) to power plant operations.
- Utilize AI and analytics tools for real-time threat detection and response in OT environments.
- Develop incident response plans and cybersecurity risk management frameworks.
- Integrate cybersecurity considerations into plant design, maintenance, and modernization projects.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- The structure and operation of SCADA and Industrial Control Systems within power plant networks.
- The major cyber threat vectors targeting critical energy infrastructure.
- How to design and implement resilient cybersecurity architectures for OT environments.
- The principles of network segmentation, encryption, and secure remote access in SCADA systems.
- Techniques for real-time monitoring, anomaly detection, and automated incident response.
- Best practices for integrating IT and OT cybersecurity strategies.
- The role of AI, machine learning, and predictive analytics in strengthening cyber defense mechanisms.

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.