CONCEPT

Saudi NCA OTCC Compliance: OT/ICS Cybersecurity for Industrial Facilities in KSA



Saudi NCA OTCC Compliance: OT/ICS Cybersecurity for Industrial Facilities in KSA

Technical depth: Practitioner · **Practical mode:** Inspection walkthrough

Introduction

Refineries, power plants, water utilities and factories in Saudi Arabia run control systems that were designed for availability, not for connected threats, and the National Cybersecurity Authority NCA now requires them to meet the Operational Technology Cybersecurity Controls, OTCC-1:2022. Many facilities struggle to translate those controls into zones, remote access rules and evidence without disrupting production. This Core Concept course applies OTCC alongside IEC 62443 and NIST SP 800-82 to real plant architectures. Participants leave with an OTCC Compliance Gap Assessment and Remediation Plan for their own facility.

Course Objectives

- Classify a facility's OT assets and its OTCC criticality level, and determine which OTCC controls apply
- Map OTCC domains to IEC 62443 requirements and NIST SP 800-82 Rev. 3 guidance to design a single control set
- Implement asset inventory, network segmentation, secure remote access and OT monitoring to the standard OTCC expects
- Assess OT cyber risk, backup and incident readiness, and supplier security, and select a control for each gap
- Inspect a plant architecture against OTCC criteria and record findings with supporting evidence
- Produce an OTCC Compliance Gap Assessment and Remediation Plan ready for management approval and NCA assessment preparation

Target Audience

- Control system and automation engineers responsible for PLC, DCS and SCADA environments
- OT cybersecurity specialists implementing NCA OTCC and ECC controls in industrial facilities
- Industrial network and infrastructure engineers maintaining plant networks and remote access
- Cybersecurity governance and compliance specialists preparing OTCC evidence and self-assessments
- Maintenance, reliability and site IT staff who manage OT changes, backups and vendor access

Course Outline

Day 1: OT Landscape and the NCA OTCC Context in Saudi Arabia

- IT Versus OT Priorities and the Purdue Reference Model Levels
- ICS Components: PLC, DCS, SCADA, HMI and Safety Instrumented Systems
- OT Threat Landscape Mapped to MITRE ATT&CK for ICS
- NCA OTCC-1:2022 Scope, Applicability and Link to the NCA Essential Cybersecurity Controls ECC
- OTCC Facility Criticality Levels 1 to 3 and Control Applicability Matrix

Day 2: OTCC Domains and International OT Standards

- OTCC Domain Structure: Governance, Defence, Resilience and Third-Party Cybersecurity
- IEC 62443-2-1:2024 Security Programme Elements for Asset Owners
- IEC 62443-3-2 Zones, Conduits and Target Security Levels
- IEC 62443-3-3 System Security Requirements and Security Levels
- NIST SP 800-82 Rev. 3 Safeguards Mapped to OTCC Controls

Day 3: Implementing Core OT Controls

- OT Asset Inventory Using Passive Network Monitoring
- Network Segmentation, Industrial DMZ and Unidirectional Gateway Design
- Secure Remote Access with Jump Hosts and Multi-Factor Authentication
- OT Patch and Vulnerability Management with Compensating Controls
- OT Event Log Collection and Anomaly Monitoring Workflow

Day 4: OT Risk, Resilience and Supplier Security

- Cyber Process Hazard Analysis Combining HAZOP and IEC 62443-3-2 Risk Assessment
- OT Backup, Recovery and Golden Image Management
- OT Incident Response Playbook Aligned to the OTCC Resilience Domain
- Integrator and Vendor Security Requirements under IEC 62443-2-4
- OTCC Compliance Evidence Register and NCA Self-Assessment Preparation

Day 5: Facility Walkthrough and the Gap Assessment

- Facility Walkthrough: Zone and Conduit Diagram Verification
- Control Room and Engineering Workstation Inspection Checklist
- OTCC Control-by-Control Gap Scoring for a Level 2 Facility
- OTCC Compliance Gap Assessment and Remediation Plan Drafting
- Peer Review Panel and Remediation Plan Defence

Skills You Will Gain

- OT Asset Classification
- Zone and Conduit Design
- Industrial Network Segmentation
- OT Remote Access Control
- Cyber Process Hazard Analysis
- OT Incident Readiness
- OTCC Evidence Management
- OT Supplier Security Assurance

Why Attend This Course

- Return to work with an OTCC Compliance Gap Assessment and Remediation Plan for your own facility, already reviewed by peers
- Explain to plant management which OTCC controls apply at your facility's criticality level and why
- Spot weak segmentation, uncontrolled vendor access and missing backups during a site walk before an assessor does
- Compare OT security practice with engineers from oil and gas, power, water and manufacturing operators

Conclusion

Industrial facilities cannot secure what they have not inventoried, segmented and evidenced. This course moves from OT architectures and the NCA OTCC requirements in Saudi Arabia, through IEC 62443 and NIST SP 800-82, to the controls, risk methods and resilience measures that turn requirements into protected plant. The final day turns that material into an OTCC Compliance Gap Assessment and Remediation Plan that participants take back to site, giving them a prioritised and defensible route to compliance and a safer operation.