

**COURSE OVERVIEW IE0210**  
**Auditing Operational Technology/SCADA/ICS (Intermediate)**

**Course Title**

Auditing Operational Technology/SCADA/ICS (Intermediate)

**Course Date/Venue**

Session 1: May 18-22, 2025/Boardroom 1,  
 Elite Byblos Hotel Al Barsha,  
 Sheikh Zayed Road, Dubai, UAE  
 Session 2: November 17-21, 2025/Fujairah  
 Meeting Room, Grand Millennium  
 Al Wahda Hotel, Abu Dhabi, UAE



**Course Reference**

IE0210

**Course Duration/Credits**

Five days/3.0 CEUs/30 PDHs

**Course Description**



***This practical and highly-interactive course includes various practical sessions and exercises. Theory learnt will be applied using one of our state-of-the-art simulators.***



This course is designed to provide participants with a detailed and up-to-date overview of Auditing Operational Technology/SCADA/ICS (Intermediate). It covers the standards and frameworks for OT security and auditing including OT system architectures and network protocols; the key risks and threats to OT environments and the role of auditing in OT environments; the proper tools and technologies for OT auditing and the scope of an OT audit; the pre-audit preparations and risk assessments; and auditing governance and policies in OT and OT network segmentation.



Further, the course will also discuss the physical security controls, audit plan and ICS inventory and asset management; the ICS network traffic and logs, authentication and access controls and security configurations in ICS systems; the vulnerability assessment and penetration testing in OT as well as incident detection and monitoring practices; the third-party and vendor risks audit and ensuring system resilience and availability; and the patch management policies and testing patch deployment processes.

During this interactive course, participants will learn to assess the risks of unpatched vulnerabilities and evaluate compensating controls for legacy systems; inspect physical connections and interfaces, evaluate tamper detection mechanisms, review maintenance and repair logs and verify adherence to OT hardware lifecycle management; the business continuity in OT environments, reporting OT audit findings and conducting a live audit simulation; the best practices for OT cybersecurity audits; and examining the emerging trends in OT security.

### **Course Objectives**

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain a comprehensive knowledge on auditing operational technology (OT), supervisory control and data acquisition (SCADA) and industrial control systems (ICS)
- Discuss the differences between OT, SCADA and ICS systems and the core components of ICS
- Review the standards and frameworks for OT security and auditing including OT system architectures and network protocols
- Identify the key risks and threats to OT environments and the role of auditing in OT environments
- Apply proper tools and technologies for OT auditing and define the scope of an OT audit
- Carryout pre-audit preparations and risk assessments, auditing governance and policies in OT and OT network segmentation
- Evaluate physical security controls, document the audit plan and assess ICS inventory and asset management
- Review ICS network traffic and logs, test authentication and access controls and evaluate security configurations in ICS systems
- Carryout vulnerability assessment and penetration testing in OT as well as incident detection and monitoring practices
- Audit third-party and vendor risks and ensure system resilience and availability
- Review patch management policies, test patch deployment processes, assess the risks of unpatched vulnerabilities and evaluate compensating controls for legacy systems
- Inspect physical connections and interfaces, evaluate tamper detection mechanisms, review maintenance and repair logs and verify adherence to OT hardware lifecycle management
- Discuss business continuity in OT environments, report OT audit findings and conduct a live audit simulation
- Employ best practices for OT cybersecurity audits and examine the emerging trends in OT security

### **Exclusive Smart Training Kit - H-STK®**



Participants of this course will receive the exclusive “Haward Smart Training Kit” (H-STK®). The H-STK® consists of a comprehensive set of technical content which includes **electronic version** of the course materials conveniently saved in a **Tablet PC**.

### **Who Should Attend**

This course provides an overview of all significant aspects and considerations of auditing operational technology/SCADA/ICS for cybersecurity professionals, industrial control system engineers, IT/OT convergence specialists, risk and compliance managers, incident response teams, operations and maintenance staff, consultants and auditors, regulatory authorities and other technical staff.

### **Training Methodology**

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

- 30% Lectures
- 20% Practical Workshops & Work Presentations
- 30% Hands-on Practical Exercises & Case Studies
- 20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

### **Course Fee**

**US\$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

### **Accommodation**


Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

### Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

### Certificate Accreditations

Certificates are accredited by the following international accreditation organizations:-

- 
British Accreditation Council (BAC)

Haward Technology is accredited by the **British Accreditation Council for Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

- 
The International Accreditors for Continuing Education and Training (IACET - USA)

Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units (CEUs)** in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.



**Course Instructor(s)**

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:



**Dr. Alaa Abdel Kerim, PhD, MSc, BSc, is a Senior Electrical & Instrumentation Engineer with over 35 years of extensive experience in the Power & Water Utilities and Other Energy Sectors. He specializes in Electrical Safety, HV Cable Design, Cable Splicing & Termination, Cable Jointing Techniques, High Voltage Electrical Safety, Electrical Drawing & Schematics, Electrical Power, Electrical Wiring, Machines, Transformers, Motors, Power Stations, Substation Site Inspection, HV/MV Cable Splicing, High Voltage Circuit Breaker Inspection & Repair, Cable & Over Head Power Line, High Voltage Power System Safe Operation, High Voltage Safety, High Voltage Transformers, Safe Operation of High Voltage & Low Voltage Power Systems, Fundamentals of Electricity, Electrical Standards, Practical High Voltage Safety Operating Procedures, Modern Power System Protective Relaying, Electrical & Control System Testing, Design, Commissioning, Operation and Maintenance of Switchgears, Transformers, Substations, Medium & High Voltage Equipment and Circuit Breakers, Electrical Motors & Variable Speed Drives, Power System Equipment, Distribution Network System, Electric Distribution System Equipment, Practical Troubleshooting of Electrical Equipment & Control Circuits, Electrical & Control System Testing & Commissioning, LV/MV/HV Circuit Breakers Inspection & Maintenance, Electrical Power Substation Maintenance, Power Stations, Uninterruptible Power Systems (UPS), Battery Chargers and AC & DC Transmission, DCS, PLC, SCADA, HMI, Automation System, Process Control & Instrumentation, Hydrocarbon, Level & Flow Measurements, Analytical Instrumentation, Find Control Elements, Control Loop Operation, Data Acquisition & Transmission, Electronics Technology, Power Systems Control, Power Systems Security, Power Transmissions, Power Generation, Electrical Substations and MV/LV Electrical System.**

During his career life, Dr. Alaa has been practically and academically involved in different **Power System and Instrumentation international companies and Universities as a Senior Professor & Consultant, Instrumentation Engineer and Electrical Engineer.** His recent practical applications experience includes the design, supply, installation, operation of full **DCS, SCADA, PLC, HMI Automation System for Sumid Line Petroleum, Siemens USA, AREVA USA** to name a few. His experience also includes electrical coordination, protection level adjustments and electrical testing.

Dr. Alaa has a **PhD degree in Electrical Engineering** from the **Technical University of Gdansk, Poland** and has **Master's and Bachelor's degrees in Electrical Machine & Power Engineering** from **Cairo University and Helwan University**, respectively. Further, he is a **Certified Instructor/Trainer** and delivered numerous trainings and workshops worldwide.



**Course Program**

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

**Day 1**

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	<b>PRE-TEST</b>
0815 – 0830	<b>Overview of Operational Technology (OT) &amp; ICS</b> Differences Between OT, SCADA & ICS Systems • Core Components of ICS (PLCs, RTUs, HMI, Sensors) • Unique Characteristics of OT versus IT Systems • Common Industries & Applications (Power, Water, Manufacturing)
0830 – 0930	<b>Standards &amp; Frameworks for OT Security &amp; Auditing</b> Overview of NIST 800-82 for ICS Security • ISA/IEC 62443 Standards for Industrial Security • ISO 27001 Applied to OT Environments • Regulatory Compliance (NERC CIP, GDPR, etc.)
0930 – 0945	Break
0945 – 1100	<b>OT System Architectures &amp; Network Protocols</b> ICS System Architecture & Purdue Model Layers • Common OT Protocols (Modbus, DNP3, OPC-UA) • Secure versus Insecure Communication in OT Networks • Typical Attack Surfaces in ICS Protocols
1100 – 1230	<b>Key Risks &amp; Threats to OT Environments</b> Common Threats (ransomware, insider threats, misconfigurations) • Recent Case Studies (e.g., Colonial Pipeline, Triton Malware) • Physical Security Vulnerabilities • The Role of Supply Chain Risks
1230 – 1245	Break
1245 – 1330	<b>Role of Auditing in OT Environments</b> Goals & Objectives of OT Auditing • The Auditor’s Perspective: Risk-Based versus Compliance-Based Audits • Differences in Auditing IT versus OT • Collaboration with Engineering Teams & Operators
1330 – 1420	<b>Tools &amp; Technologies for OT Auditing</b> Overview of OT-Specific Audit Tools • Use of Packet Analysis Tools (Wireshark, TShark) • Physical Inspection Tools for ICS Devices • Tools for Mapping ICS Networks
1420 – 1430	<b>Recap</b> Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day One

**Day 2**

0730 – 0830	<b>Defining the Scope of an OT Audit</b> Identifying Audit Boundaries (Networks, Devices, Systems) • High-risk Areas in OT/ICS Environments • Key Stakeholders: IT, OT & Engineering Teams • Determining Audit Objectives & Success Criteria
0830 – 0930	<b>Pre-Audit Preparations &amp; Risk Assessments</b> Gathering Documentation (Network Diagrams, Policies) • Assessing Historical Incidents & Logs • Evaluating Regulatory Requirements • Conducting a High-Level Risk Assessment
0930 – 0945	Break





0945 – 1100	<b>Auditing Governance &amp; Policies in OT</b> <i>Reviewing ICS Security Policies • Alignment with Corporate Governance Frameworks • Evaluating Incident Response Plans &amp; Disaster Recovery • Communication Protocols Between IT &amp; OT</i>
1100 – 1230	<b>Understanding OT Network Segmentation</b> <i>Evaluating the Implementation of the Purdue Model • Identifying Segmentation Gaps • Use of Firewalls and DMZs in OT Environments • Secure Remote Access for OT Systems</i>
1230 – 1245	Break
1245 – 1330	<b>Evaluating Physical Security Controls</b> <i>Site Visits &amp; Physical Asset Inventory • Access Control Systems for ICS Devices • Environmental Controls for ICS Infrastructure • Reviewing Surveillance &amp; Monitoring Systems</i>
1330 – 1420	<b>Documenting the Audit Plan</b> <i>Creating a Detailed Audit Checklist • Setting Timelines &amp; Milestones • Assigning Responsibilities within the Audit Team • Communicating the Audit Scope with Stakeholders</i>
1420 – 1430	<b>Recap</b> <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow</i>
1430	Lunch & End of Day Two

**Day 3**

0730 – 0830	<b>Assessing ICS Inventory &amp; Asset Management</b> <i>Verifying ICS Asset Inventories • Reviewing Device Configurations &amp; Firmware Versions • Identifying Unauthorized or Rogue Devices • Validating Patch Management Processes</i>
0830 – 0930	<b>Reviewing ICS Network Traffic &amp; Logs</b> <i>Capturing &amp; Analyzing Network Traffic • Identifying Suspicious Activities or Anomalies • Reviewing Logs from Firewalls, Switches &amp; ICS Devices • Using Log Correlation Tools to Identify Trends</i>
0930 – 0945	Break
0945 – 1100	<b>Testing Authentication &amp; Access Controls</b> <i>Reviewing User &amp; Operator Access Permissions • Evaluating Multi-Factor Authentication (MFA) Implementations • Testing Default Accounts &amp; Passwords • Analyzing Role-Based Access Control Policies</i>
1100 – 1230	<b>Evaluating Security Configurations in ICS Systems</b> <i>Reviewing PLC/RTU Programming Logic for Vulnerabilities • Assessing Configurations for HMI &amp; SCADA Servers • Identifying Unused or Open Ports • Testing Encryption in Communications</i>
1230 – 1245	Break



1245 – 1330	<b>Vulnerability Assessment &amp; Penetration Testing in OT</b> Conducting Passive Vulnerability Scans in OT Networks • Identifying Misconfigurations & Unpatched Systems • Safe Practices for Penetration Testing in ICS • Documenting Vulnerabilities & Associated Risks
1330 – 1420	<b>Incident Detection &amp; Monitoring Practices</b> Evaluating the Use of OT-Specific IDS/IPS • Reviewing SOC Integration with ICS Environments • Analyzing the Effectiveness of Alerting & Escalation • Testing OT Cybersecurity Incident Response Drills
1420 – 1430	<b>Recap</b> Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day Three

**Day 4**

0730 – 0830	<b>Auditing Third-Party &amp; Vendor Risks</b> Reviewing Vendor Access Policies • Evaluating Supply Chain Risks • Assessing Compliance with SLAs & Contracts • Auditing Vendor Patching & Updates
0830 – 0930	<b>ICS Patch &amp; Update Management</b> Reviewing Patch Management Policies for OT • Testing Patch Deployment Processes • Assessing the Risks of Unpatched Vulnerabilities • Evaluating Compensating Controls for Legacy Systems
0930 – 0945	Break
0945 – 1100	<b>Auditing ICS Physical Devices</b> Inspecting Physical Connections & Interfaces • Evaluating Tamper Detection Mechanisms • Reviewing Maintenance & Repair Logs • Verifying Adherence to OT Hardware Lifecycle Management
1100 – 1230	<b>Business Continuity in OT Environments</b> Reviewing BCP (Business Continuity Plan) for ICS Systems • Testing Failover & Redundancy Mechanisms • Evaluating the Impact of OT Downtime on Operations • Incident Communication Plans with Internal & External Stakeholders
1230 – 1245	Break
1245 – 1420	<b>Reporting OT Audit Findings</b> Structuring an Audit Report (Executive Summary, Technical Findings) • Risk Prioritization & Scoring Methodologies • Providing Actionable Recommendations • Communicating Findings to Technical & Executive Audiences
1420 – 1430	<b>Recap</b> Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow
1430	Lunch & End of Day Four







**Day 5**

0730 – 0830	<b>Conducting a Live Audit Simulation</b> <i>Simulating an End-To-End OT Audit • Assigning Roles &amp; Responsibilities • Testing Different Audit Scenarios • Documenting Findings During the Simulation</i>
0830 – 0930	<b>Case Studies on Real-World OT Incidents</b> <i>Major OT Cyber Incidents • Lessons Learned from Case Studies • Applying Audit Techniques to Prevent Similar Incidents • Discussion &amp; Group Analysis</i>
0930 – 0945	Break
0945 – 1100	<b>Vulnerability Analysis Exercise</b> <i>Using Tools like Wireshark to Analyze ICS Traffic • Identifying Vulnerabilities in a Simulated OT Network • Proposing Mitigation Strategies • Discussing Limitations &amp; Challenges of OT Audits</i>
1100 – 1230	<b>Best Practices for OT Cybersecurity Audits</b> <i>Building Relationships with OT &amp; Engineering Teams • Balancing Operational Needs with Audit Requirements • Continuous Learning in Evolving OT Environments • Leveraging Industry Resources &amp; Forums</i>
1230 – 1245	Break
1245 – 1345	<b>Examining Emerging Trends in OT Security</b> <i>The Impact of Industry 4.0 &amp; IoT on OT Systems • Artificial Intelligence in ICS Monitoring • Threats from Quantum Computing • Future-Proofing OT Systems</i>
1345 – 1400	<b>Course Conclusion</b> <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course</i>
1400 – 1415	<b>POST-TEST</b>
1415 – 1430	<i>Presentation of Course Certificates</i>
1430	<i>Lunch &amp; End of Course</i>





**Simulator (Hands-on Practical Sessions)**

Practical sessions will be organized during the course for delegates to practice the theory learnt. Delegates will be provided with an opportunity to carryout various exercises using one of our state-of-the-art simulators “Allen Bradley SLC 500”, “AB Micrologix 1000 (Digital or Analog)”, “AB SLC5/03”, “AB WS5610 PLC”, “Siemens S7-1200”, Siemens S7-400” “Siemens SIMATIC S7-300”, “Siemens S7-200” “GE Fanuc Series 90-30 PLC”, “Siemens SIMATIC Step 7 Professional Software”, and “HMI SCADA”.



**Allen Bradley SLC 500 Simulator**



**Allen Bradley Micrologix 1000 Simulator (Digital)**



**Allen Bradley Micrologix 1000 Simulator (Analog)**



**Allen Bradley SLC 5/03**



**Allen Bradley WS5610 PLC Simulator PLC5**



**Siemens S7-1200 Simulator**



**Siemens S7-400 Simulator**



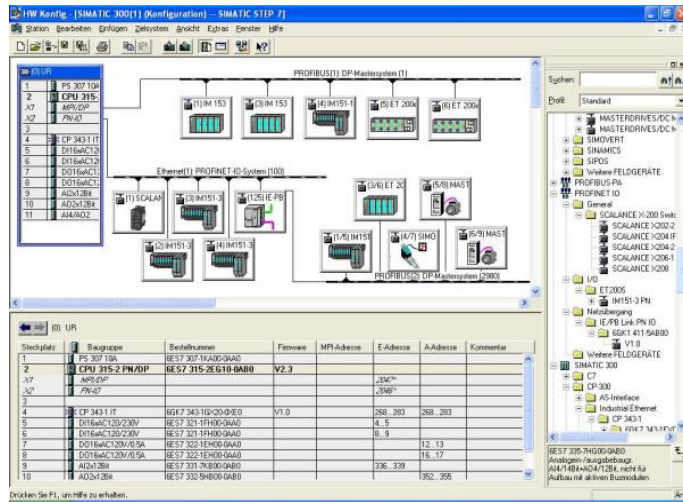
**Siemens SIMATIC S7-300**



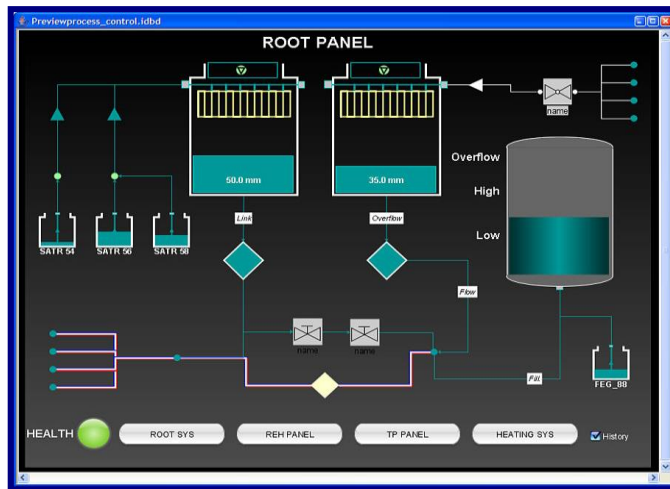
**Siemens S7-200 Simulator**



**GE Fanuc Series 90-30 PLC Simulator**



### Siemens SIMATIC Step 7 Professional Software



### HMI SCADA

#### Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: [mari1@haward.org](mailto:mari1@haward.org)

