COURSE OVERVIEW IE0210

Auditing Operational Technology/SCADA/ICS (Intermediate)

Course Title

Auditing Operational Technology/SCADA/ICS (Intermediate)

H-STK© INCLUDED

Course Date/Venue

May 18-22, 2025/The Victoria Meeting Room, The H Dubai Hotel, Sheikh Zayed Rd - Trade Centre, Dubai, UAE

Course Reference

IE0210

3.0 CEUs (30 PDHs) AWARD

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. Ahmed El-Sayed, PhD, MSc, BSc, is a **Senior Electrical & Instrumentation Engineer** with over **30 years** of extensive experience within the **Oil**, **Gas**, **Power**, **Petroleum**, **Petrochemical** and **Utilities** industries. His experience widely covers in the areas of **Flow Measurement** Devices, **Water Network** Pipe Materials & Fittings, **Mapping & Inventory** of Pipes & Fittings in the Water Supply System, **Water Distribution System** Operator, **Sewer System and Sewage Flows**, **Ultrasonic Inspection**, and **Advanced Visual Techniques** of Predictive Maintenance, Water Meter Reading (**MMR**), **Network Management & Supervision**, **Leakage Prevention & Control**, Waste Water Treatment, **Water Utility Regulation and Economics**, **Health & Safety Rules & Regulations**, **Safety Management**, **Accident Investigation**, Advanced Distributed Control System (**DCS**), **DCS** Operation & Configuration, **DCS** Troubleshooting, **DCS Yokogawa** ProSafe-RS Safety Instrumented System, **DCS Yokogawa** Centum VP, **DCS Emerson** DeltaV, **DCS GE Mark VI**, Programable Logic Controller (**PLC**), Supervisory Control & Data Acquisition (**SCADA**) Systems, **Process Control**, **Control Systems & Data Communications**, **Instrumentation**, **Automation**, **Valve Tuning**, Safety Instrumented Systems (**SIS**), Safety Integrity Level (**SIL**), Emergency Shutdown (**ESD**), **Telemetry** Systems, **Boiler Control & Instrumentation**, Advanced Process Control (**APC**) Technology, Practical **Fiber-Optics** Technology, **Compressor** Control & Protection, **GE Gas Turbines**, **Alarm** Management Systems, **Engine** Management System, **Fieldbus** Systems, **NEC** (National Electrical Code), **NESC** (National Electrical Safety Code), **Electrical Safety**, **Electrical Hazards** Assessment, **Electrical Equipment**, Electrical Transient Analysis Program (**ETAP**), Power **Quality**, Power **Network**, Power **Distribution**, **Distribution Systems**, **Power Systems Control**, **Power Systems Security**, Power **Electronics**, **Power System** Harmonics, **Power System** Planning, Control & Stability, **Power Flow** Analysis, **Smart Grid & Renewable** Integration, **Power System Protection & Relaying**, Economic Dispatch & Grid Stability Constraints in Power Plants, Electrical Demand Side Management (DSM), Electrical **Substations**, **Substation Automation** Systems & Application (IEC 61850), **Distribution Network** System Design, **Distribution Network Load**, Electrical **Distribution** Systems, **Load Forecasting** & System Upgrade (Distribution), **Overhead Power Line** Maintenance & Patrolling, High Voltage **Switching** Operations, Industrial **UPS Systems & Battery** Power Supplies, Electric **Motors & Variable Speed Drives**, **Generator** Maintenance & Troubleshooting, **Generator** Excitation Systems & AVR, **Transformer** Maintenance & Testing, Lock-Out & Tag-Out (**LOTO**), Confined Workspaces and **Earthing & Grounding**, He is currently the **Systems Control Manager** of **Siemens** where he is in-charge of Security & Control of Power **Transmission Distribution** & **High Voltage** Systems and he further takes part in the Load Records Evaluation & Transmission Services Pricing.

During his career life, Dr. Ahmed has been actively involved in different Power System Activities including Roles in Power System Planning, Analysis, Engineering, **HV Substation** Design, Electrical Service Pricing, Evaluations & Tariffs, Project Management, Teaching and Consulting. His vast industrial experience was honed greatly when he joined many International and National Companies such as **Siemens**, **Electricity Authority**, Egyptian Electricity Holding, Egyptian Refining Company (ERC), **GASCO**, Tahrir Petrochemicals Project, and **ACETO** industries as the **Instrumentation & Electrical Service Project Manager**, **Energy Management Engineer**, **Department Head**, **Assistant Professor**, **Project Coordinator**, **Project Assistant and Managing Board Member** where he focused more on dealing with Technology Transfer, System Integration Process and Improving Localization. He was further greatly involved in manufacturing some of **Power System** and **Control & Instrumentation Components** such as Series of Digital Protection **Relays**, MV **VFD**, **PLC** and **SCADA** System with intelligent features.

Dr. Ahmed has **PhD**, **Master's** & **Bachelor's** degree in **Electrical Engineering** from the **University of Wisconsin Madison**, **USA** and **Ain Shams University**, respectively. Further, he is a **Certified Instructor/Trainer**, a **Certified Internal Verifier/ Assessor/Trainer** by the **Institute of Leadership and Management** (**ILM**), an active member of IEEE and ISA as well as numerous technical and scientific papers published internationally in the areas of Power Quality, Superconductive Magnetic Energy Storage, SMES role in Power Systems, Power System **Blackout** Analysis, and Intelligent Load Shedding Techniques for preventing Power System Blackouts, HV **Substation Automation** and Power System Stability.

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: ***Sunday, 18th of May 2025***

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0815 – 0830	***Overview of Operational Technology (OT) & ICS*** *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	***Standards & Frameworks for OT Security & Auditing*** *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	***OT System Architectures & Network Protocols*** *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	***Key Risks & Threats to OT Environments*** *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	***Role of Auditing in OT Environments*** *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	***Tools & Technologies for OT Auditing*** *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	***Recap*** *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: ***Monday, 19th of May 2025***

0730 – 0830	***Defining the Scope of an OT Audit*** *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	***Pre-Audit Preparations & Risk Assessments*** *Gathering Documentation (Network Diagrams, Policies) • Assessing Historical Incidents & Logs • Evaluating Regulatory Requirements • Conducting a High-Level Risk Assessment*
0930 – 0945	*Break*

0945 – 1100	***Auditing Governance & Policies in OT*** *Reviewing ICS Security Policies • Alignment with Corporate Governance Frameworks • Evaluating Incident Response Plans & Disaster Recovery • Communication Protocols Between IT & OT*
1100 – 1230	***Understanding OT Network Segmentation*** *Evaluating the Implementation of the Purdue Model • Identifying Segmentation Gaps • Use of Firewalls and DMZs in OT Environments • Secure Remote Access for OT Systems*
1230 – 1245	*Break*
1245 – 1330	***Evaluating Physical Security Controls*** *Site Visits & Physical Asset Inventory • Access Control Systems for ICS Devices • Environmental Controls for ICS Infrastructure • Reviewing Surveillance & Monitoring Systems*
1330 – 1420	***Documenting the Audit Plan*** *Creating a Detailed Audit Checklist • Setting Timelines & Milestones • Assigning Responsibilities within the Audit Team • Communicating the Audit Scope with Stakeholders*
1420 – 1430	***Recap*** *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 Two*

Day 3: ***Tuesday, 20th of May 2025***

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

1245 – 1330	***Vulnerability Assessment & Penetration Testing in OT*** *Conducting Passive Vulnerability Scans in OT Networks • Identifying Misconfigurations & Unpatched Systems • Safe Practices for Penetration Testing in ICS • Documenting Vulnerabilities & Associated Risks*
1330 – 1420	***Incident Detection & Monitoring Practices*** *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	***Recap*** *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: Wednesday, 21st of May 2025

0730 – 0830	***Auditing Third-Party & Vendor Risks*** *Reviewing Vendor Access Policies • Evaluating Supply Chain Risks • Assessing Compliance with SLAs & Contracts • Auditing Vendor Patching & Updates*
0830 – 0930	***ICS Patch & Update Management*** *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	***Auditing ICS Physical Devices*** *Inspecting Physical Connections & Interfaces • Evaluating Tamper Detection Mechanisms • Reviewing Maintenance & Repair Logs • Verifying Adherence to OT Hardware Lifecycle Management*
1100 – 1230	***Business Continuity in OT Environments*** *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	***Reporting OT Audit Findings*** *Structuring an Audit Report (Executive Summary, Technical Findings) • Risk Prioritization & Scoring Methodologies • Providing Actionable Recommendations • Communicating Findings to Technical & Executive Audiences*
1420 – 1430	***Recap*** *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: Thursday, 22nd of May 2025

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

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

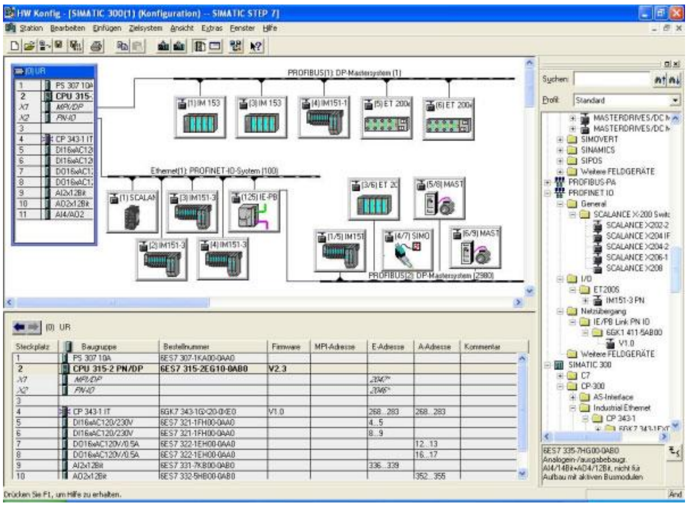
Siemens S7-1200 Simulator

Siemens S7-400 Simulator

Siemens SIMATIC S7-300

Siemens S7-200 Simulator

GE Fanuc Series 90-30 PLC Simulator



HW Konfig - [SIMATIC 300(1) (Konfiguration) -- SIMATIC STEP 7]

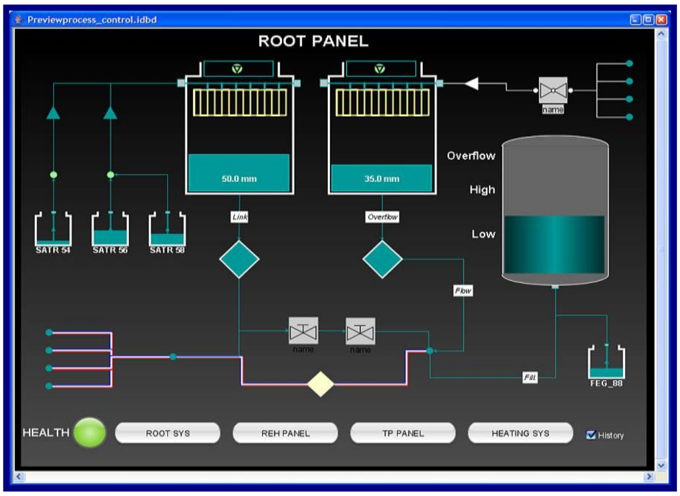
(0) UR

Steckplatz	Baugruppe	Bestellnummer	Firmware	MPI-Adresse	E-Adresse	A-Adresse	Kommentar
1	PS 307 10A	6ES7 307-1KA00-0AA0					
2	**CPU 315-2 PN/DP**	**6ES7 315-2EG10-0AB0**	**V2.3**				
X1	*MPI/DP*				*2047**		
X2	*PN-IO*				*2046**		
3							
4	CP 343-1 IT	6GK7 343-1GX20-0XE0	V1.0		268...283	268...283	
5	DI16xAC120/230V	6ES7 321-1FH00-0AA0			4...5		
6	DI16xAC120/230V	6ES7 321-1FH00-0AA0			8...9		
7	DO16xAC120V/0.5A	6ES7 322-1EH00-0AA0				12...13	
8	DO16xAC120V/0.5A	6ES7 322-1EH00-0AA0				16...17	
9	AI2x12Bit	6ES7 331-7KB00-0AB0			336...339		
10	AO2x12Bit	6ES7 332-5HB00-0AB0				352...355	

6ES7 335-7HG00-0AB0
Analogein-/ausgabebaugr.
AI4/14Bit+AO4/12Bit, nicht für Aufbau mit aktiven Busmodulen

Drücken Sie F1, um Hilfe zu erhalten.

Siemens SIMATIC Step 7 Professional Software



HMI SCADA

Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org