COURSE OVERVIEW IE0182
Auditing Operational Technology/SCADA/ICS (Advanced)

Course Title
Auditing Operational Technology/SCADA/ICS (Advanced)

H-STK© INCLUDED

Course Date/Venue
Session 1: April 13-17, 2025/Boardroom 1, Elite Byblos Hotel Al Barsha, Sheikh Zayed Road, Dubai, UAE
Session 2: November 10-14, 2025/Fujairah Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE

Course Reference
IE0182

Course Duration/Credits
Five days/3.0 CEUs/30 PDHs

3.0 CEUs (30 PDHs) AWARD

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 (Advanced). It covers the differences between operational technology (OT), supervisory control and data acquisition (SCADA) and industrial control systems (ICS); the importance of OT security and auditing as well as OT/IT convergence and its challenges; and the OT architectures and the standards and frameworks in OT auditing.

Further, the course will also discuss the role of an auditor in OT/SCADA/ICS and identify OT threats; the vulnerabilities in OT/SCADA systems and risk assessment techniques for OT including governance and compliance; the OT audit planning and scoping, cybersecurity metrics and KPIs for OT; the network auditing, endpoint security in OT/SCADA and physical security audits; and the remote access practices, securing vendor and contractor access and identifying risks associated with cloud integration in OT.

During this interactive course, participants will learn the audit of OT incident response plans, penetration testing in OT/SCADA and ICS-specific security tools; the protocol analysis and auditing including configuration and patch management; the threat hunting in OT environments, securing supply chain auditing and reporting and presenting audit results; the techniques used by advanced persistent threats (APTs), plan operational resilience in ICS and integrating disaster recovery and OT security; the zero trust principles to ICS and identifying and accessing management in OT; the micro-segmentation for OT networks; and securing authentication and authorization mechanisms.

Course Objectives

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

- Apply and gain an advanced knowledge on auditing operational technology/SCADA/ICS
- Discuss the differences between operational technology (OT), supervisory control and data acquisition (SCADA) and industrial control systems (ICS)
- Explain the importance of OT security and auditing as well as OT/IT convergence and its challenges
- Describe OT architectures and discuss the standards and frameworks in OT auditing
- Define the role of an auditor in OT/SCADA/ICS and identify OT threats
- Recognize vulnerabilities in OT/SCADA systems and apply risk assessment techniques for OT including governance and compliance
- Apply OT audit planning and scoping, cybersecurity metrics and KPIs for OT
- Carryout network auditing, endpoint security in OT/SCADA and physical security audits
- Assess remote access practices, secure vendor and contractor access and identify risks associated with cloud integration in OT
- Audit OT incident response plans, apply penetration testing in OT/SCADA and identify ICS-specific security tools
- Employ protocol analysis and auditing including configuration and patch management
- Apply threat hunting in OT environments, secure supply chain auditing and report and present audit results
- Carryout techniques used by advanced persistent threats (APTs), plan operational resilience in ICS and integrate disaster recovery and OT security
- Apply zero trust principles to ICS, identity and access management in OT apply micro-segmentation for OT networks and secure authentication and authorization mechanisms

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 policy makers

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 Engineer** with **35 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, **PLC-HMI Controls**, Total Quality Management (**TQM**), Internal Audit Techniques in **TQM**, Quality Management System (**QMS**), **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**), **Waste Water System** Planning & Design, **Network Management & Supervision**, **Leakage Prevention & Control**, **Water Leak Detection**, Waste Water Treatment, **Water Utility Regulation and Economics**, **Water Network Systems**, **Health & Safety Rules & Regulations**, Safety Procedures in **Water Networks**, **Safety Management**, Principles of **Routine** and **Preventive Maintenance**, **Accident Investigation**, **Operation** & **Maintenance of Sewerage System**, 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

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	**PRE-TEST**
0815 – 0830	**Overview of OT/SCADA/ICS** Definitions & Differences Between OT, SCADA, & ICS • Evolution of OT Systems & Their Integration into It Environments • Key Components of OT (PLCs, RTUs, HMIs, etc.) • Common Protocols (Modbus, DNP3, OPC, etc.)
0830 – 0930	**Importance of OT Security & Auditing** Risks & Threats Unique to OT Environments • Consequences of OT/SCADA Breaches (e.g., Physical, Environmental & Economic) • Regulatory Drivers for OT Security (e.g., NERC CIP, IEC 62443, ISO 27001) • Case Studies of Major OT/SCADA Incidents
0930 – 0945	Break
0945 – 1100	**OT/IT Convergence & Its Challenges** Differences in Priorities: Availability versus Confidentiality • Integration Challenges in Hybrid Environments • Bridging the Knowledge Gap Between IT & OT Teams • Risk of Propagating IT Threats to OT Environments
1100 – 1230	**Understanding OT Architectures** Purdue Model for ICS Network Architecture • Levels of OT Environments & Data Flows • Segmentation & Zones in OT Networks (e.g., DMZ, Control Zones) • Designing Secure OT Architectures
1230 – 1245	Break
1245 – 1330	**Standards & Frameworks in OT Auditing** Overview of IEC 62443 Standards • Application of NIST SP 800-82 in ICS Environments • ISA/IEC-95 for Interoperability & Integration • Comparison of OT Security Frameworks with IT Frameworks
1330 – 1420	**Role of an Auditor in OT/SCADA/ICS** Key Responsibilities & Mindset of OT Auditors • OT Risk Assessment versus IT Risk Assessment • Challenges in Auditing Legacy Systems • Collaboration with OT Engineers & Operators
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

0730 – 0830	**Identifying & Understanding OT Threats** Threat Actors in OT (e.g., Nation-States, Cybercriminals, Insiders) • Physical Threats to ICS Components • Cyber-Physical Risks & Cascading Failures • Insider Threats & Human Factors
0830 – 0930	**Vulnerabilities in OT/SCADA Systems** Legacy Systems & Unsupported Devices • Weak or Default Configurations in OT Protocols • Lack of Patch Management & Update Practices • Over-Reliance on Insecure Remote Access
0930 – 0945	Break

0945 – 1100	***Risk Assessment Techniques for OT*** *Conducting Asset Inventories & Risk Mapping • Identifying Crown Jewel Assets & Critical Dependencies • Threat Modeling & Likelihood Analysis • Risk Prioritization for Remediation*
1100 – 1230	***Governance & Compliance in OT*** *Role of Policies & Procedures in OT Environments • Compliance with Industry Standards (e.g., GDPR, HIPAA, SOX in ICS Contexts) • Establishing a Governance Framework for OT Security • Cross-Functional Roles in Governance (e.g., IT, OT, Compliance)*
1230 – 1245	*Break*
1245 – 1330	***OT Audit Planning & Scoping*** *Defining Audit Objectives & Scope • Gathering Pre-Audit Information • Tailoring Audit Methods to OT Environments • Engaging Stakeholders in the Planning Phase*
1330 – 1420	***Cybersecurity Metrics & KPIs for OT*** *Measuring OT/ICS Security Posture • Key Performance Indicators for OT Environments • Using Data to Inform Security Investments • Reporting OT Audit Findings to Executives*
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

0730 – 0830	***Network Auditing in OT Environments*** *OT Network Discovery & Inventory Tools • Verifying Segmentation & Isolation of OT Zones • Monitoring Traffic Flows & Protocol Usage • Detecting Unauthorized Connections or Devices*
0830 – 0930	***Endpoint Security in OT/SCADA*** *Assessing PLCs, HMIs, & Engineering Workstations • Configuration Reviews & Firmware Assessments • Detecting Malware in OT Endpoints • Evaluating Endpoint Hardening Practices*
0930 – 0945	*Break*
0945 – 1100	***Physical Security Audits*** *Physical Access Controls for OT Environments • Securing Control Rooms & Critical Equipment • Reviewing Surveillance Systems for ICS Facilities • Environmental Security (e.g., Power, Cooling, Fire Safety)*
1100 – 1230	***Remote Access & Third-Party Risks*** *Assessing Remote Access Practices • Securing Vendor & Contractor Access • Risks Associated with Cloud Integration in OT • Remote Desktop & VPN Configuration Reviews*
1230 – 1245	*Break*

1245 – 1330	***Auditing OT Incident Response Plans*** *Verifying Incident Response Readiness • Testing Playbooks for OT-Specific Incidents • Communication Protocols During OT Incidents • Integration of IT & OT Incident Response Processes*
1330 – 1420	***Penetration Testing in OT/SCADA*** *Limitations & Risks of OT Pen Testing • Safe Methods for Vulnerability Scanning in OT • Emulating OT-Specific Attack Scenarios • Reporting Findings & Recommendations*
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

0730 – 0830	***ICS-Specific Security Tools*** *Overview of Ot-Focused Tools (e.g., Nozomi Networks, Claroty, Dragos) • Using Network Monitoring Tools for ICS • OT Vulnerability Scanning Tools • Log Analysis Tools for OT/SCADA*
0830 – 0930	***Protocol Analysis & Auditing*** *Modbus, DNP3, & OPC Protocols • Identifying Misconfigurations in ICS Protocols • Capturing & Analyzing ICS Network Traffic • Tools for Protocol Decoding & Analysis*
0930 – 0945	*Break*
0945 – 1130	***Configuration & Patch Management*** *Reviewing Patch Management Practices for ICS • Auditing PLC, HMI & Server Configurations • Managing Configuration Backups Securely • Challenges in Patching OT Systems*
1130 – 1230	***Threat Hunting in Ot Environments*** *Behavioral Analytics for Anomaly Detection • Hunting for Known Ot-Specific Malware (e.g., Stuxnet, Triton) • Indicators of Compromise in OT Systems • Proactive Detection Strategies for OT Threats*
1230 – 1245	*Break*
1245 – 1330	***Secure Supply Chain Auditing*** *Risks in the OT Hardware & Software Supply Chain • Assessing Vendor Security Practices • Third-Party Risk Management Frameworks • Securing Firmware & Software Updates*
1330 – 1420	***Reporting & Presenting Audit Results*** *Structuring Audit Reports for OT Audiences • Tailoring Recommendations for OT Engineers & Managers • Highlighting Quick Wins versus Long-Term Fixes • Building Executive-Level Summaries*
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

0730 – 0830	***Hands-On Case Studies*** *Review of a Real-World OT/SCADA Environment • Identifying Risks & Vulnerabilities in a Simulated Setup • Drafting Audit Findings & Recommendations • Team-Based Exercises for Audit Scenarios*
0830 – 0930	***Advanced Threats to OT/SCADA*** *Emerging Threats (e.g., AI-Driven Attacks, Ransomware Targeting OT) • Techniques Used by Advanced Persistent Threats (APTs) • Sector-Specific Threats (e.g., Energy, Transportation, Water) • Preparing for Next-Generation OT Risks*
0930 – 0945	*Break*
0945 – 1145	***Resilience & Business Continuity in OT*** *Planning for Operational Resilience in ICS • Integrating Disaster Recovery & OT Security • Testing & Refining Business Continuity Plans • Lessons Learned from Real-World Disruptions*
1145 – 1230	***OT Security in a Zero Trust Framework*** *Applying Zero Trust Principles to ICS • Identity & Access Management in OT • Micro-Segmentation for OT Networks • Secure Authentication & Authorization Mechanisms*
1230 – 1245	*Break*
1245 – 1345	***Future of OT/SCADA/ICS Auditing*** *Trends in OT Security Technologies • Impacts of 5G & IoT on OT Systems • Regulatory Changes & Their Implications • Role of AI & ML in OT Security & Auditing*
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

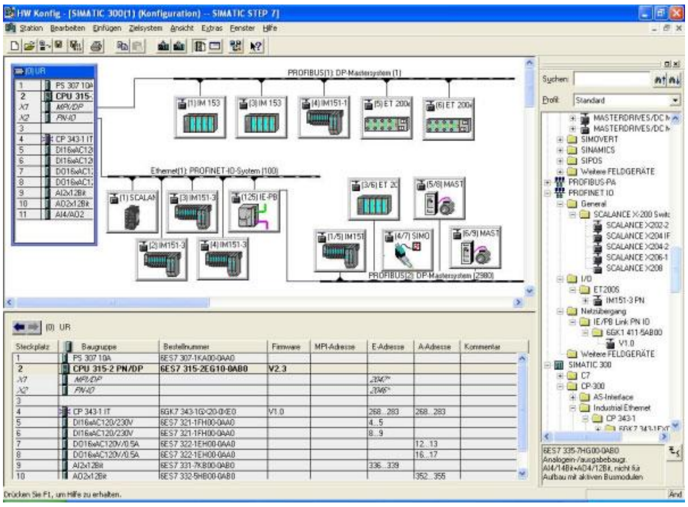
Siemens S7-1200 Simulator

Siemens S7-400 Simulator

Siemens SIMATIC S7-300

Siemens S7-200 Simulator

GE Fanuc Series 90-30 PLC Simulator



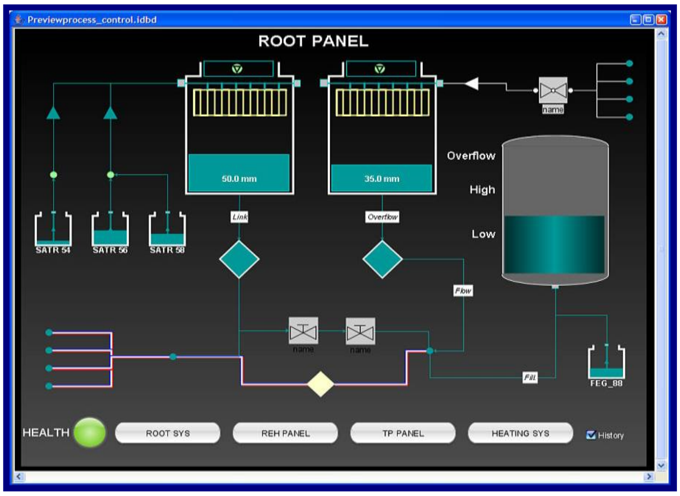
(0) UR

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