

COURSE OVERVIEW IE0239

OT Security Information and Event Management (SIEM)

Course Title

OT Security Information and Event Management (SIEM)

Course Date/Venue

Session 1: July 06-10, 2025/Boardroom 1, Elite Byblos Hotel Al Barsha, Sheikh Zayed Road, Dubai, UAE

Session 2: December 08-12, 2025/Fujairah Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE



Course Reference

IE0239

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 our state-of-the-art simulators.



This course is designed to provide participants with a detailed and up-to-date overview of OT Security Information and Event Management (SIEM). It covers the differences between IT and OT security; the common OT cyber threats and attack vectors; the fundamentals, architecture and deployment models; the log sources, data collection and compliance and regulatory requirements; planning an OT SIEM deployment and integrating SIEM with ICS and SCADA systems; the event correlation, threat detection, log normalization and parsing in OT SIEM; the real-time security monitoring with SIEM dashboards; and the network traffic analysis and OT anomaly detection.



During this interactive course, participant will learn the SIEM integration with threat intelligence feeds and early threat detection in OT networks; automating incident response using SIEM; the industrial intrusion detection systems (IDS); the AI and machine learning for SIEM in OT environments; the response and containment strategies for OT cyber incidents; the SIEM performance optimization, continuous security monitoring, compliance auditing and forensic investigation; the patch and vulnerability management integration; and the future trends in OT SIEM and industrial cybersecurity.

Course Objectives

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

- Apply and gain an in-depth knowledge on Operational Technology (OT) security information and event management (SIEM)
- Discuss the differences between IT and OT security including the common OT cyber threats and attack vectors
- Describe the fundamentals, architecture and deployment models of security information and event management (SIEM)
- Identify log sources and data collection in OT SIEM as well as compliance and regulatory requirements
- Plan an OT SIEM deployment and integrate SIEM with ICS and SCADA systems
- Apply event correlation, threat detection, log normalization and parsing in OT SIEM
- Carryout real-time security monitoring with SIEM dashboards including network traffic analysis and OT anomaly detection
- Employ SIEM integration with threat intelligence feeds and SIEM for early threat detection in OT networks
- Automate incident response using SIEM and recognize industrial intrusion detection systems (IDS)
- Apply AI and machine learning for SIEM in OT environments and response and containment strategies for OT cyber incidents
- Carryout SIEM performance optimization for OT networks, continuous security monitoring in OT SIEM and compliance auditing and forensic investigation with SIEM
- Employ patch and vulnerability management integration with SIEM and discuss the future trends in OT SIEM and industrial cybersecurity

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 OT security information and event management (SIEM) for OT network engineers, OT security engineers/architects, CISOs and security managers, cybersecurity analysts, IT/OT convergence teams, incident response teams, compliance officers, risk management professionals other technical staff.

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.

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.

- 
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.

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.

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:



Mr. Taiseer Ali, MSc, BSc, is a Senior Electrical & Telecommunications Engineer with over 30 years of extensive experience and academic experience as a University Professor specializing in High Voltage Electrical Safety, HV/LV Electrical System, Electrical Signal Analysis (ESA), Electrical Equipment Circuits, Electrical Safety, Electrical Drawing, Electrical Troubleshooting, HV/LV Equipment Inspection & Maintenance, Electrical Equipment, Electrical Motors & Drives, Power Systems & Auxiliary Power Systems, Power System Harmonics, Power Generation & Transmission, Power Distribution & Network, Electrical Substation Design, Power Cable Testing & Fault Location, Circuit Breakers & Switchgears, Electrical Distribution Design, Installation & Commissioning and HVDC Transmission & Control, HV Switchgear Operation & Maintenance, LV Distribution Switchgear & Equipment, Protection Relays, Wiring & Testing, Electronic Circuits, Electrostatic Discharge (ESD), Lock & Tag Out, Circuit Breakers & Switchgears, Portable Cables, Transformers, Gas Insulated Substations (GIS), HV Substation Inspection & Reporting, HV Cable Design, HV Electrical System Commissioning, HV Equipment Inspection & Maintenance, Distributed Control System (DCS) Applications & Troubleshooting, SCADA & Industrial Communication, Process Logic Controller (PLC), Load Flow Calculation, Cable Installation, Transformer Maintenance, Earthing, Bonding, Lightning & Surge Protection, UPS & Battery, Instrumentation & Control, Process Control & Instrumentation, Industrial Communication, Flow Measurement, Level Measurement, Temperature & Vibration Measurement, Measurement Instrumentation, Pressure Measurement, Analytical Instrumentation, Calibration & Testing Procedures, Final Control Elements, Control Loops Operation, Control Panels, Power Generation, Power Transformers, Uninterruptible Power Systems (UPS), Battery Chargers, AC & DC Transmission, Distribution Network, Grid Input Assessment, Load Flow, Short Circuit, Smart Grid, Grounding, Advanced Networking, Datron Maintenance, Cisco Internet, Data Base Access, Advanced Computer, AutoCAD, Standard Radio Devices, Advanced Calibration, Repair and Maintenance of VHF Portable Role, Combat Vehicle Reconnaissance 76mm and Target Engagement Using Simulaser.

During his career life, Mr. Taiseer has gained his expertise and thorough practical experience through handling challenging positions such as being the **Head of the Command Control & Communication Department, Head of the Academic and Technical Branch, Chief of the Frequency Branch, Commander, Electrical Engineer, Spectrum Management Engineer, Safety Engineer, Engineering Manager, Electrical Engineering Head, Quality Control Department Head, Engineering Supervisor and Lecturer/Instructor** for various companies and universities such as the Yarmouk University, C3 Directorate, JAF C3 Communication Workshops, Jordan Armed Forces Joint Officer and Military Communication College and multi-national companies and institutes.

Mr. Taiseer has a **Master's** degree in **Industrial Engineering/Engineering Management** and a **Bachelor's** degree in **Electrical/Communication Engineering**. Further, he is a **Certified Instructor/Trainer** and has delivered numerous trainings, courses, seminars and workshops internationally.

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.

Accommodation

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

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	<i>Registration & Coffee</i>
0800 – 0815	<i>Welcome & Introduction</i>
0815 – 0830	PRE-TEST
0830 – 0930	Overview of OT Security & Its Challenges <i>Differences Between IT versus OT Security • Common OT Cyber Threats & Attack Vectors • ICS/SCADA Security Challenges in Operations • Impact of Cybersecurity Breaches on Critical Infrastructure</i>
0930 - 0945	<i>Break</i>
0945 – 1045	Fundamentals of Security Information & Event Management (SIEM) <i>What is SIEM? Role in OT Security • Key Components of a SIEM System • Differences Between IT and OT SIEM Deployments • Benefits of SIEM for Industrial Operations</i>
1045 - 1145	SIEM Architecture & Deployment Models <i>On-Premises versus Cloud-Based SIEM for OT • Centralized versus Distributed SIEM Deployments • Data Collection Points in ICS/SCADA Environments • Integration with Industrial Firewalls, IDS/IPS, & SOCs</i>
1145 - 1230	Log Sources & Data Collection in OT SIEM <i>Logs from PLCs, RTUs, SCADA, & DCS Systems • Network Logs versus Host-Based Logs • Security Events from Firewalls, IDS/IPS, & Endpoints • Challenges of Collecting Logs from Legacy OT Systems</i>
1230 – 1245	<i>Break</i>
1245 – 1330	Compliance & Regulatory Requirements for SIEM in OT <i>NIST 800-82: Industrial Control System Security • IEC 62443: Security for Industrial Automation & Control Systems • Cybersecurity Standards & Compliance Framework • UAE Cybersecurity & Industrial Regulations</i>

1330 - 1420	Case Study: Major OT Cyber Incidents & SIEM Lessons Learned <i>Stuxnet: How SIEM Could Have Detected the Attack • TRITON Malware: Targeting Safety Instrumented Systems • Colonial Pipeline Attack: Ransomware in OT Environments • Strategy for Strengthening OT Cyber Resilience</i>
1420 - 1430	Recap <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	<i>Lunch & End of Day One</i>

Day 2

0730 - 0830	SIEM Deployment in an OT Environment <i>Planning an OT SIEM Deployment • Integrating SIEM with ICS & SCADA Systems • Data Flow & Event Correlation Strategies • Reducing False Positives in OT Security Alerts</i>
0830 - 0930	Event Correlation & Threat Detection <i>Event Correlation Rules in SIEM • Correlating Security Events from Different OT Sources • Identifying Anomalous Behavior in ICS Networks • Real-Time Detection of Malicious Activities</i>
0930 - 0945	<i>Break</i>
0945 - 1130	Log Normalization & Parsing in OT SIEM <i>Normalizing OT Logs for Unified Analysis • Parsing Raw Data into Structured Formats • SIEM Query Language & Rule-Based Parsing • Customizing Log Parsing for OT Systems</i>
1130 - 1230	Real-Time Security Monitoring with SIEM Dashboards <i>Designing Effective SIEM Dashboards for OT Networks • Key Security Indicators for Industrial Control Systems • Threat Visualization for OT Operators & SOC Teams • Customizing SIEM Dashboards for Requirements</i>
1230 - 1245	<i>Break</i>
1245 - 1330	Network Traffic Analysis & OT Anomaly Detection <i>Monitoring Industrial Protocols (Modbus, DNP3, OPC, Profinet) • Identifying Unauthorized OT Network Connections • Using SIEM for Detecting Lateral Movement Attacks • Case Study: Detecting an Intrusion in a SCADA Network</i>
1330 - 1420	SIEM Integration with Threat Intelligence Feeds <i>What Is Threat Intelligence, & Why It's Important? • Integrating SIEM with Global & Specific Threat Feeds • Real-Time Threat Hunting Using SIEM • Case Study: Preventing Zero-Day Exploits in OT Networks</i>
1420 - 1430	Recap <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	<i>Lunch & End of Day Two</i>

Day 3

0730 - 0830	SIEM for Early Threat Detection in OT Networks <i>Detecting Malware & Ransomware in Industrial Systems • Identifying Unauthorized Firmware Changes in PLCs • Using SIEM for Insider Threat Detection in OT • Case Study: Early Warning Detection of Industrial Espionage</i>
0830 - 0930	Automating Incident Response Using SIEM <i>Security Orchestration, Automation, & Response (SOAR) • Playbook-Driven Automated Response Actions • Integrating SIEM with Incident Response Tools • Reducing Response Time with Automated Threat Containment</i>

0930 - 0945	Break
0945 - 1130	SIEM & Industrial Intrusion Detection Systems (IDS) Role of IDS in ICS Security • IDS versus SIEM: Complementary Approaches • Integrating Industrial IDS with SIEM for Comprehensive Monitoring • Case Study: How an IDS-SIEM Integration Stopped a Cyber Attack
1130 - 1230	AI & Machine Learning for SIEM in OT Environments Applying AI to Detect OT Cyber Threats • Machine Learning-Based Behavioral Anomaly Detection • AI-Driven Predictive Threat Hunting in Industrial Networks • Case Study: Using AI for Proactive Threat Prevention
1230 - 1245	Break
1245 - 1330	Response & Containment Strategies for OT Cyber Incidents Isolating Affected Systems Without Disrupting Operations • Containment & Recovery Strategies for ICS Networks • Role of Incident Response Teams in Industrial Cybersecurity • Cyber Incident Response Framework
1330 - 1420	Hands-On Lab: Configuring an OT SIEM for Incident Detection Setting Up Event Correlation Rules • Analyzing Real-Time Security Alerts • Implementing Automated Response Workflows • Testing Incident Escalation & Containment Scenarios
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 - 0930	SIEM Performance Optimization for OT Networks Reducing Alert Fatigue & False Positives • Balancing Security with System Performance • Fine-Tuning Event Correlation Rules • Ensuring High Availability & Redundancy
0930 - 0945	Break
0945 - 1130	Continuous Security Monitoring in OT SIEM Implementing a 24/7 Security Operations Model • Role of Managed Security Service Providers (MSSP) in OT SIEM • Proactive Threat Intelligence & Continuous Learning • Case Study: Improving Security Monitoring for OT Infrastructure
1130 - 1230	Compliance Auditing & Forensic Investigation with SIEM Conducting OT Security Audits Using SIEM • Forensic Investigation Techniques in Industrial Networks • SIEM-Based Compliance Reporting for Regulatory Framework • Case Study: Digital Forensics in an OT Cybersecurity Breach
1230 - 1245	Break
1245 - 1420	Patch & Vulnerability Management Integration with SIEM Monitoring Unpatched Vulnerabilities in OT Systems • SIEM-Based Vulnerability Scanning & Risk Assessment • Automating Patch Deployment Notifications • Strategy for Continuous Security Patch Management
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	Future Trends in OT SIEM & Industrial Cybersecurity <i>Evolution of SIEM for ICS & SCADA Security • Cloud-Based SIEM Solutions for OT Environments • Role of Blockchain in Industrial Security Logging • Preparing for the Next Generation of OT Cyber Threats</i>
0830 – 0930	Hands-On Lab: Advanced SIEM Use Cases in OT <i>Setting Up SIEM-Based Threat Intelligence Feeds • Automating Response to Industrial Cyber Threats • Conducting a Full Security Investigation Using SIEM • Fine-Tuning SIEM Rules for Optimal Performance</i>
0930 - 0945	<i>Break</i>
0945 – 1100	SIEM Deployment Case Study
1100 – 1230	Group Exercise: Designing a SIEM Architecture for OT Security
1230 - 1245	<i>Break</i>
1245 - 1300	Hands-On Lab: Threat Hunting & Incident Response Using SIEM
1300 – 1315	Course Conclusion
1315 – 1415	POST TEST
1415 – 1430	<i>Presentation of Course Certificates</i>
1430	<i>Lunch & 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”, “HMI SCADA”, “Gas Ultrasonic Meter Sizing Tool”, “Liquid Turbine Meter and Control Valve Sizing Tool”, “Liquid Ultrasonic Meter Sizing Tool” , “Orifice Flow Calculator”, “Automation Simulator” and “PLCLogix 5000 Software”.



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



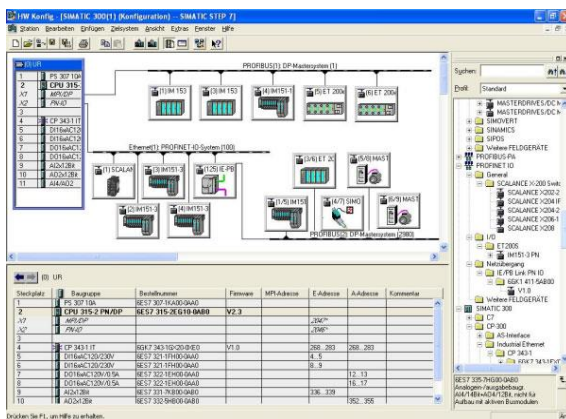
Siemens SIMATIC S7-300



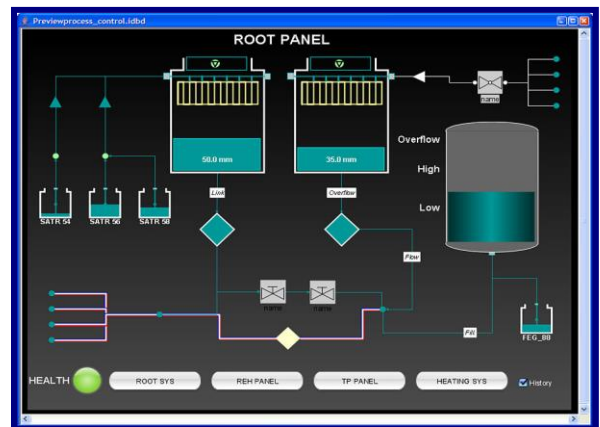
Siemens S7-200 Simulator



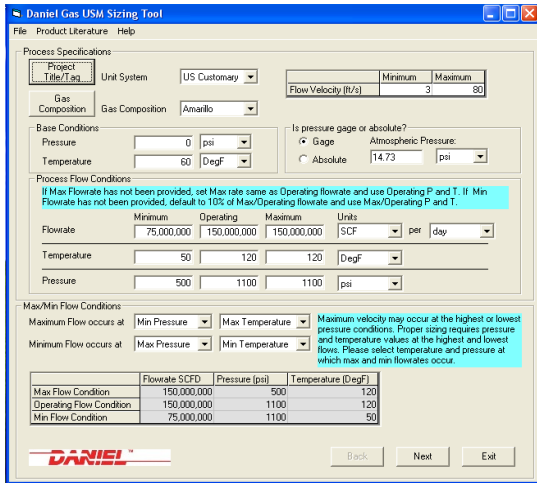
GE Fanuc Series 90-30 PLC Simulator



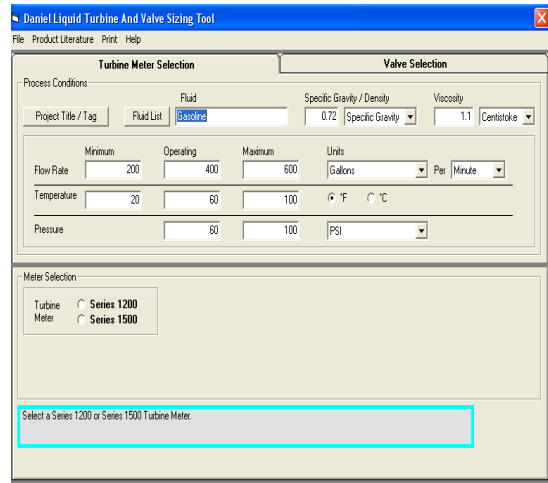
Siemens SIMATIC Step 7 Professional Software



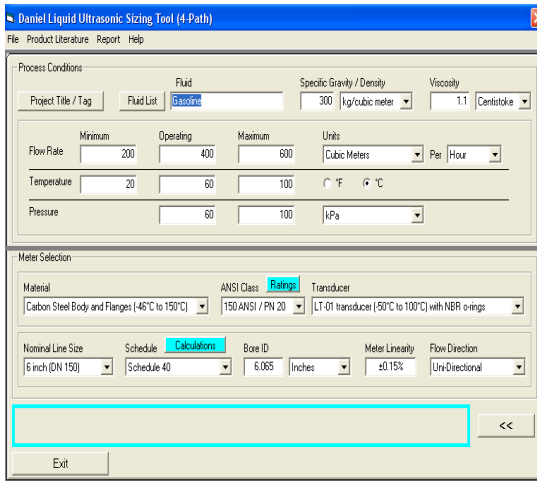
HMI SCADA



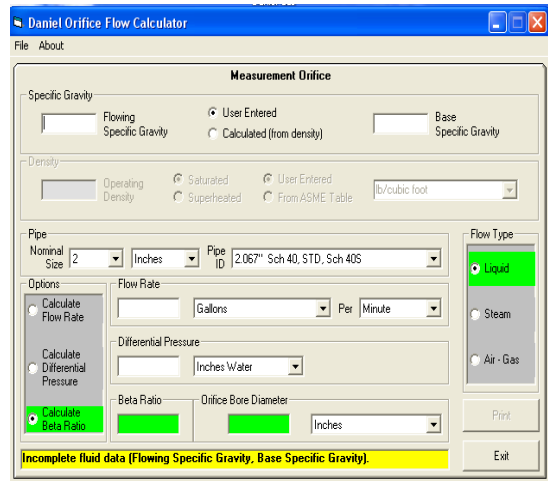
Gas Ultrasonic Meter (USM) Sizing Tool Simulator



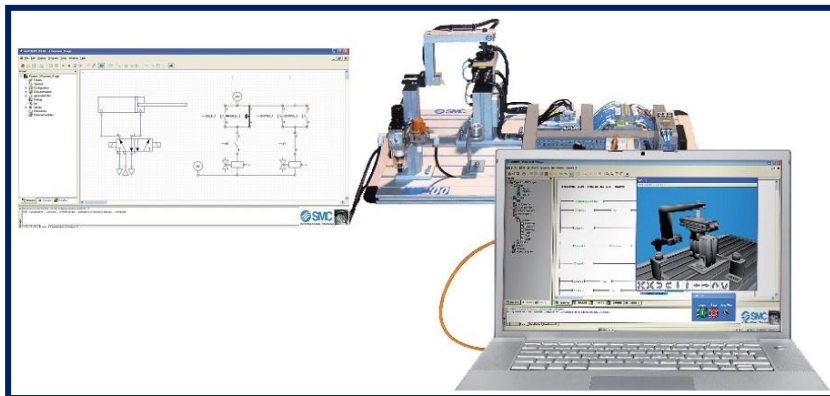
Liquid Turbine Meter and Control Valve Sizing Tool Simulator



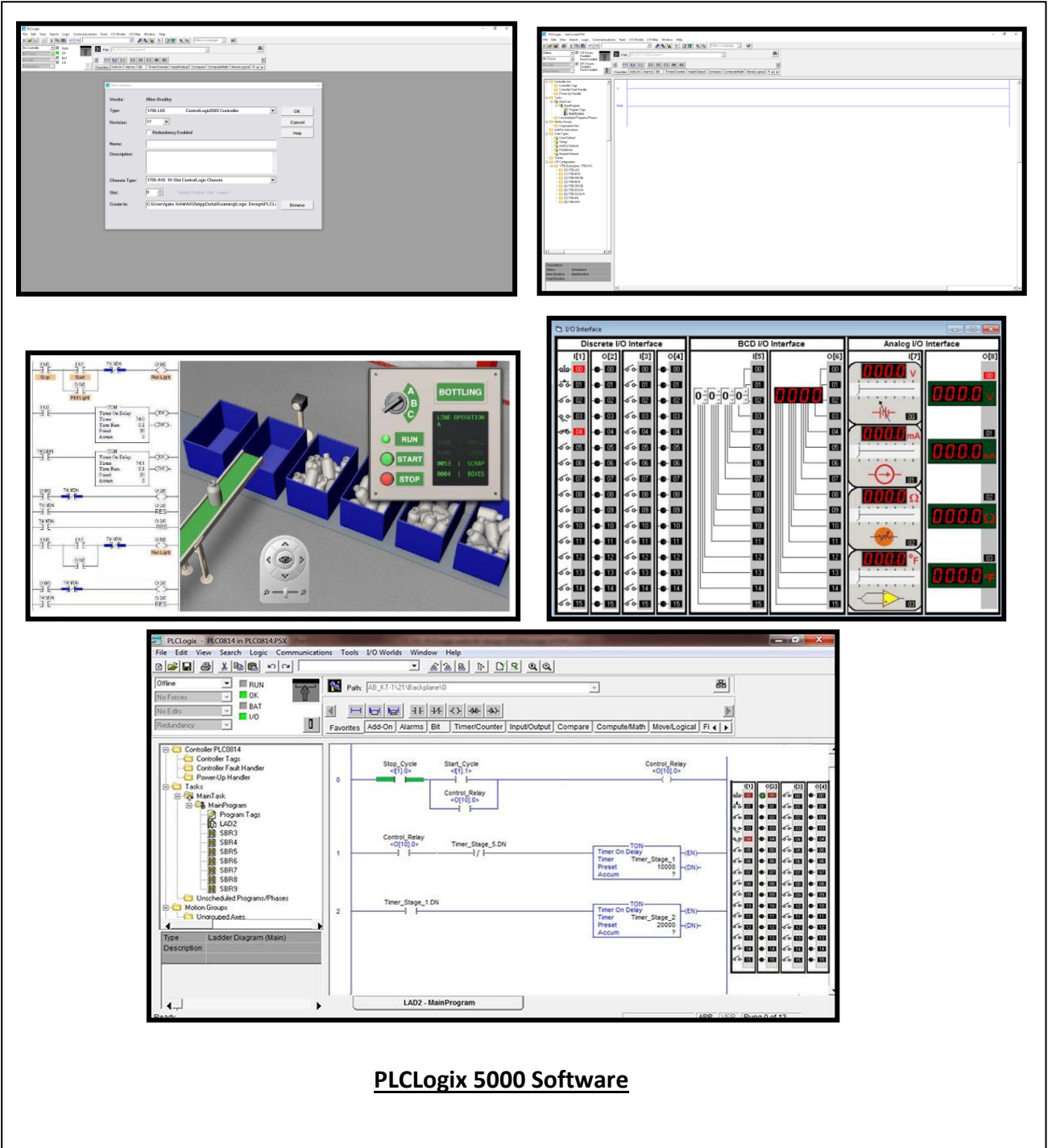
Liquid Ultrasonic Meter Sizing Tool Simulator



Orifice Flow Calculator Simulator



AutoSIM – 200 Automation Simulator



The image displays several screenshots of the PLCLogix 5000 software interface. The top-left screenshot shows a hardware configuration dialog box for a PLC module. The top-right screenshot shows a project tree and a blank workspace. The middle-left screenshot shows a 3D simulation of a bottling line with a control panel. The middle-right screenshot shows the I/O interface with discrete, BCD, and analog modules. The bottom screenshot shows the main ladder logic editor with a program tree on the left and a ladder diagram in the center.

PLCLogix 5000 Software

Course Coordinator

Mari Nakintu, Tel: +971 230 91 714, Email: mari1@haward.org