

COURSE OVERVIEW IE0575
Process Automation Networks & Systems Security

Course Title

Process Automation Networks & Systems Security

Course Date/Venue

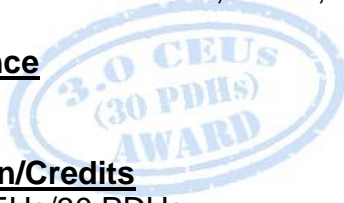
September 07-11, 2025/Tamra Meeting Room, Al Bandar Rotana Creek, Dubai, UAE

Course Reference

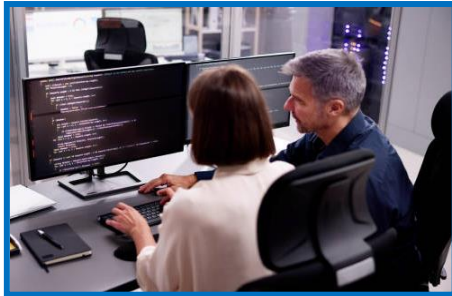
IE0575

Course Duration/Credits

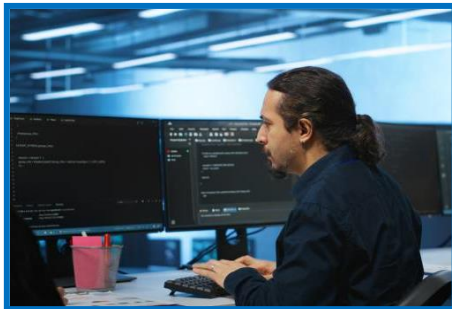
Five days/3.0 CEUs/30 PDHs



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 Process Automation Networks and Systems Security. It covers the industrial automation systems covering SCADA, DCS and PLC-based systems, layers of industrial automation, common communication protocols and control loops and feedback in industrial environments; the components of a process automation network (PAN); the differences between IT and OT systems; the typical network architecture of industrial systems and cyber threat landscape in OT environments; the role of project managers in secure automation deployments; and the key principles of cybersecurity.



Further, the course will also discuss the network security concepts, industrial protocol security issues, access control mechanisms and patch management and system updates; the security policies and standards covering NIST SP 800-82 for ICS, IEC 62443 (industrial network security), ISO 27001 and its relevance to OT and developing internal cybersecurity policies; the threat detection techniques, cybersecurity risk management and incident response in process automation networks; and the business continuity and disaster recovery.

During this interactive course, participants will learn the continuous monitoring and alerting, key log sources, audit trails and compliance evidence and tools for centralized log management; the secure system architecture and design, vendor management and secure procurement; the security testing in OT projects, integration of legacy systems, change management and configuration control and project lifecycle security considerations; the cybersecurity governance models and compliance and regulatory frameworks; developing cybersecurity roadmap, security awareness and training programs; and the metrics and continuous improvement.

Course Objectives

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

- Apply and gain an in-depth knowledge on process automation networks and systems security
- Discuss industrial automation systems covering SCADA, DCS, and PLC-based systems, layers of industrial automation, common communication protocols and control loops and feedback in industrial environments
- Identify the components of a process automation network (PAN) and the differences between IT and OT systems
- Recognize typical network architecture of industrial systems and cyber threat landscape in OT environments
- Discuss the role of project managers in secure automation deployments and the key principles of cybersecurity
- Recognize network security concepts, industrial protocol security issues, access control mechanisms and patch management and system updates
- Review security policies and standards covering NIST SP 800-82 for ICS, IEC 62443 (industrial network security), ISO 27001 and its relevance to OT and developing internal cybersecurity policies
- Carryout threat detection techniques, cybersecurity risk management, incident response in process automation networks and business continuity and disaster recovery
- Apply continuous monitoring and alerting, key log sources, audit trails and compliance evidence and tools for centralized log management
- Illustrate secure system architecture and design, vendor management and secure procurement
- Carryout security testing in OT projects, integration of legacy systems, change management and configuration control and project lifecycle security considerations
- Describe cybersecurity governance models and discuss compliance and regulatory frameworks
- Develop cybersecurity roadmap, security awareness and training programs and apply metrics and continuous improvement

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 process automation networks and systems security for cybersecurity professionals, operations managers and supervisors, instrumentation engineers, network engineers, IT professionals, control system engineers, automation engineers and technicians.

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:



Mr. Sydney Thoresson, PE, BSc, is a Senior Electrical & Instrumentation Engineer with over 30 years of extensive experience within the Petrochemical, Utilities, Oil, Gas and Power industries. His specialization highly evolves in Process Control Instrumentation, Process Instrumentation & Control, Process Control, Instrumentation, Troubleshooting & Problem Solving, Instrumentation Engineering, Process Control (PCI) & Safeguarding, Instrument Calibration & Maintenance, Instrumented Safety Systems, High Integrity

Protection Systems (HIPS), Process Controller, Control Loop & Valve Tuning, Compressor Control & Protection, Control Systems, Programmable Logic Controllers (PLC), SCADA System, PLC & SCADA - Automation & Process Control, PLC & SCADA Systems Application, Technical DCS/SCADA, PLC-SIMATIC S7 300/400: Configuration, Programming and Troubleshooting, PLC, Telemetry and SCADA Technologies, Cyber Security of Industrial Control System (PLC, DCS, SCADA & IED), Basics of Instrumentation Control System, DCS, Distributed Control System - Operations & Techniques, Distributed Control System (DCS) Principles, Applications, Selection & Troubleshooting, Distributed Control Systems (DCS) especially in Honeywell DCS, H&B DCS, Modicon, Siemens, Telemecanique, Wonderware and Adroit, Safety Instrumented Systems (SIS), Safety Integrity Level (SIL), Emergency Shutdown (ESD), Emergency Shutdown System, Variable Frequency Drive (VFD), Process Control & Safeguarding, Field Instrumentation, Instrumented Protective Devices Maintenance & Testing, Instrumented Protective Function (IPF), Refining & Rotating Equipment, Equipment Operations, Short Circuit Calculation, Voltage Drop Calculation, Lighting Calculation, Hazardous Area Classification, Intrinsic Safety, Liquid & Gas Flowmetering, Custody Measurement, Ultrasonic Flowmetering, Loss Control, Gas Measurement, Flowmetering & Custody Measurement, Multiphase Flowmetering, Measurement and Control, Mass Measuring System Batching (Philips), Arc Furnace Automation-Ferro Alloys, Walking Beam Furnace, Blast Furnace, Billet Casting Station, Cement Kiln Automation, Factory Automation and Quality Assurance Accreditation (ISO 9000 and Standard BS 5750). Further, he is also well-versed in Electrical Safety, Electrical Hazards Assessment, Electrical Equipment, Personal Protective Equipment, Log-Out & Tag-Out (LOTO), ALARP & LOPA Methods, Confined Workspaces, Power Quality, Power Network, Power Distribution, Distribution Systems, Power Systems Control, Power Systems Security, Power Electronics, Electrical Substations, UPS & Battery System, Earthing & Grounding, Power Generation, Protective Systems, Electrical Generators, Power & Distribution Transformers, Electrical Motors, Switchgears, Transformers, AC & DC Drives, Variable Speed Drives & Generators and Generator Protection. He is currently the Projects Manager wherein he manages projects in the field of electrical and automation engineering and in-charge of various process hazard analysis, fault task analysis, FMEA and HAZOP study.

During Mr. Thoresson's career life, he has gained his thorough and practical experience through various challenging positions and dedication as the **Contracts & Projects Manager, Managing Director, Technical Director, Divisional Manager, Plant Automation Engineer, Senior Consulting Engineer, Senior Systems Engineer, Consulting Engineer, Service Engineer and Section Leader** from several international companies such as **Philips, FEDMIS, AEG, DAVY International, BOSCH, Billiton and Endress/Hauser.**

Mr. Thoresson is a **Registered Professional Engineering Technologist** and has a **Bachelor's degree in Electrical & Electronics Engineering** and a **National Diploma in Radio Engineering.** Further, he is a **Certified Instructor/Trainer, a Certified Internal Verifier/Assessor/Trainer** by the **Institute of Leadership & Management (ILM)** and an active member of the **International Society of Automation (ISA)** and the **Society for Automation, Instrumentation, Measurement and Control (SAIMC).** He has further delivered numerous trainings, courses, seminars, conferences and workshops

Course Program

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

Day 1: Sunday, 07th of September 2025

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	PRE-TEST
0830 – 0930	Overview of Industrial Automation Systems SCADA, DCS & PLC-Based Systems • Layers of Industrial Automation (Field, Control, Supervisory) • Common Communication Protocols (Modbus, Profibus, OPC) • Control Loops & Feedback in Industrial Environments
0930 – 0945	Break
0945 – 1030	Components of a Process Automation Network (PAN) Controllers (PLCs, RTUs, IEDs) • HMI & Operator Interfaces • Field Devices & Sensors • Communication & Data Transmission Infrastructure
1030 – 1130	Differences Between IT & OT Systems Objectives: Availability versus Confidentiality • Lifecycle & Vendor Dependencies • Protocols & Operating Environments • Risk Tolerance & System Updates
1130 – 1215	Typical Network Architecture of Industrial Systems Purdue Enterprise Reference Architecture Model • Segmentation of IT & OT Networks • Data Flow & Access Control Zones • Interfaces with ERP, MES & Cloud Systems
1215 – 1230	Break
1230 – 1330	Cyber Threat Landscape in OT Environments Types of Threats (Malware, Ransomware, Insider Threats) • Real-World Incidents (Stuxnet, Triton, NotPetya) • Threat Actors (Nation-States, Cybercriminals, Hacktivists) • Consequences of Attacks (Downtime, Safety, Financial Loss)
1330 – 1420	Role of Project Managers in Secure Automation Deployments Aligning Project Scope with Cybersecurity Objectives • Stakeholder Coordination (IT, OT, Vendors) • Integrating Cybersecurity into Project Lifecycle • Regulatory & Compliance Considerations
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, 08th of September 2025

0730 – 0830	Key Principles of Cybersecurity CIA Triad: Confidentiality, Integrity, Availability • Authentication, Authorization, Accounting (AAA) • Defense-in-Depth Approach • Zero Trust Model for OT Systems
0830 – 0930	Network Security Concepts IP Addressing & Subnets in OT • Firewalls & DMZ Configurations • VLANs & Network Segmentation • Intrusion Detection & Prevention
0930 – 0945	Break



0945 – 1100	Industrial Protocol Security Issues Unencrypted & Unauthenticated Protocols • Common Vulnerabilities in Modbus, DNP3, OPC • Secure Alternatives & Protocol Hardening • Protocol-Aware Firewalls
1100 – 1215	Access Control Mechanisms Role-Based Access Control (RBAC) • User Identity Management & Directory Services • Physical Security Integration • Managing Third-Party/Vendor Access
1215 – 1230	Break
1230 – 1330	Patch Management & System Updates Risks of Unpatched Systems • Downtime & Operational Constraints • Safe Patch Deployment Strategies • Asset Inventory & Update Tracking
1330 – 1420	Security Policies & Standards NIST SP 800-82 for ICS • IEC 62443 (Industrial Network Security) • ISO 27001 & Its Relevance to OT • Developing Internal Cybersecurity Policies
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, 09th of September 2025

0730 – 0830	Threat Detection Techniques Signature-Based versus Behavior-Based Detection • Use of SIEM & Event Correlation • OT-Specific Anomaly Detection Systems • Integrating Logs from HMI, PLC & Firewalls
0830 – 0930	Cybersecurity Risk Management Identifying OT Assets & Vulnerabilities • Risk Assessment Tools (Qualitative & Quantitative) • Risk Prioritization & Mitigation Strategies • Residual Risk & Risk Acceptance
0930 – 0945	Break
0945 – 1100	Incident Response in Process Automation Networks Establishing an OT Incident Response Plan • Roles & Responsibilities in An IR Team • Containment, Eradication & Recovery Phases • Coordination with IT & External Responders
1100 – 1215	Business Continuity & Disaster Recovery OT-Specific BCP/DRP Components • Backup Strategies for PLC & HMI Configurations • Failover Systems & Redundancy • Testing & Maintaining Recovery Procedures
1215 – 1230	Break
1230 – 1330	Security Monitoring & Auditing Continuous Monitoring & Alerting • Key Log Sources (Controllers, Firewalls, Applications) • Audit Trails & Compliance Evidence • Tools for Centralized Log Management
1330 – 1420	Case Studies: Notable OT Security Incidents Deep Dive into Stuxnet • Ukrainian Power Grid Attack • Triton Malware Targeting Safety Systems • Lessons Learned for Project Managers
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, 10th of September 2025

0730 – 0830	Secure System Architecture & Design <i>Designing with Security from the Start (Secure by Design) • Redundancy versus Vulnerability Exposure • Air-Gapping & Unidirectional Gateways • Network Segmentation (Zone/Conduit Model)</i>
0830 – 0930	Vendor Management & Secure Procurement <i>Evaluating Vendor Security Practices • Secure Delivery & Installation Procedures • Contracts & Service-Level Agreements (SLAs) • Managing Supply Chain Risk</i>
0930 – 0945	Break
0945 – 1100	Security Testing in OT Projects <i>Penetration Testing versus Vulnerability Scanning • Testing Constraints in Live Systems • Factory Acceptance Testing (FAT) Security Components • Post-Installation Security Validation</i>
1100 – 1215	Integration of Legacy Systems <i>Challenges in Securing Older Devices • Use of Compensating Controls • Wrapping Legacy with Secure Gateways • Planning Future Upgrades in Phases</i>
1215 – 1230	Break
1230 – 1330	Change Management & Configuration Control <i>Documenting & Approving Changes • Secure Configuration Baselines • Impact Analysis on Network Security • Configuration Backup & Recovery</i>
1330 – 1420	Project Lifecycle Security Considerations <i>Security in Initiation & Planning • Risk & Requirement Identification • Cybersecurity During Commissioning • Secure Handover & Documentation</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	Lunch & End of Day Four

Day 5: Thursday, 11th of September 2025

0730 – 0830	Cybersecurity Governance Models <i>Defining Governance for OT Security • Roles of IT, OT, PMO & Executive Leadership • Policies & Standards Enforcement • Audit Preparation & Management Review</i>
0830 – 0930	Compliance & Regulatory Frameworks <i>National Critical Infrastructure Mandates • GDPR & Data Handling in Process Control • Industrial-Specific Standards (ISA, IEC, NERC CIP) • Internal versus External Compliance Audits</i>
0930 – 0945	Break
0945 – 1030	Developing a Cybersecurity Roadmap <i>Identifying Long-Term Goals • Creating Milestones & Timelines • Resource & Budget Planning • Strategic Alignment with Enterprise Goals</i>
1030 – 1130	Security Awareness & Training Programs <i>Developing OT-Specific Training • Addressing Operator & Engineer Behavior • Training for Contractors & Third Parties • Tabletop Exercises & Incident Drills</i>

1130 – 1215	Metrics & Continuous Improvement <i>Defining Cybersecurity KPIs • Monitoring Incident Trends & Response Time • Benchmarking Against Industry Best Practices • Lessons Learned & Feedback Loops</i>
1215 – 1230	<i>Break</i>
1230 – 1345	Final Project Exercise & Presentation <i>Group Activity: Designing a Secure Automation Network • Applying Risk Analysis & Architecture Design • Presenting Mitigation & Compliance Strategies • Peer Feedback & Trainer Evaluation</i>
1345 – 1400	Course Conclusion <i>Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course</i>
1400 – 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



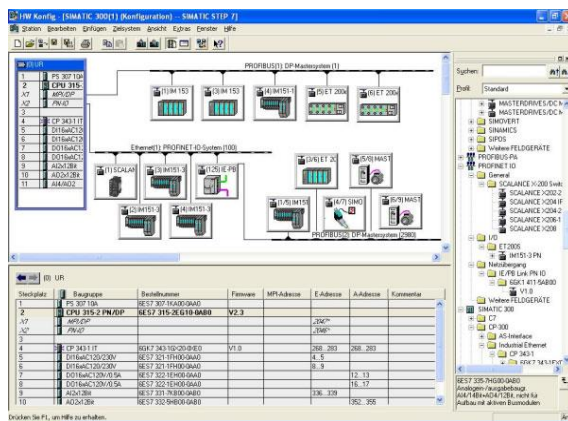
Siemens SIMATIC S7-300



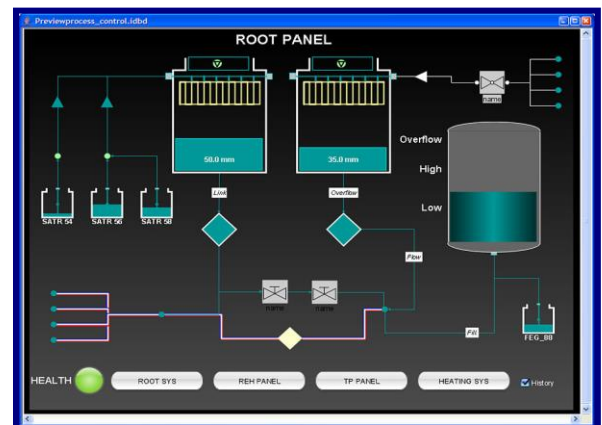
Siemens S7-200 Simulator



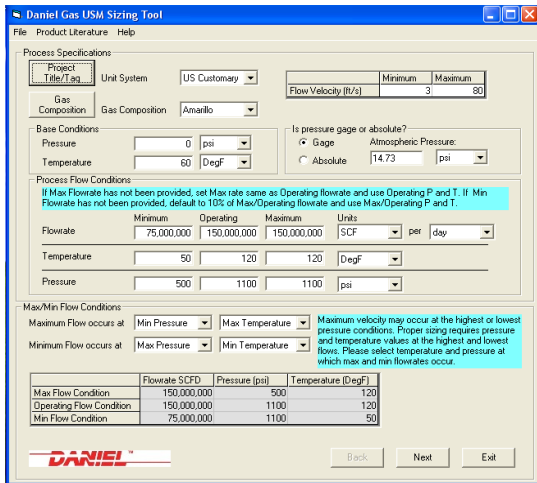
GE Fanuc Series 90-30 PLC Simulator



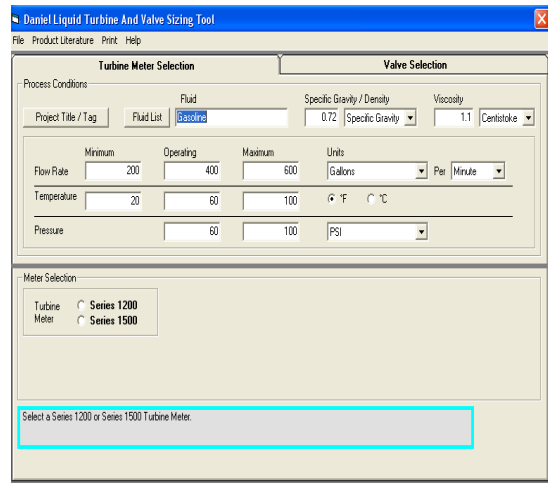
Siemens SIMATIC Step 7 Professional Software



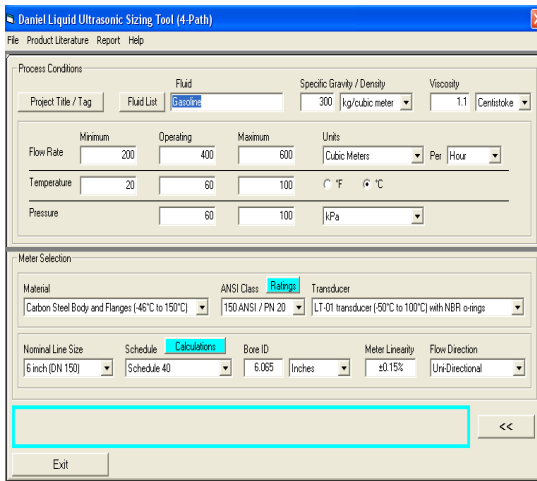
HMI SCADA



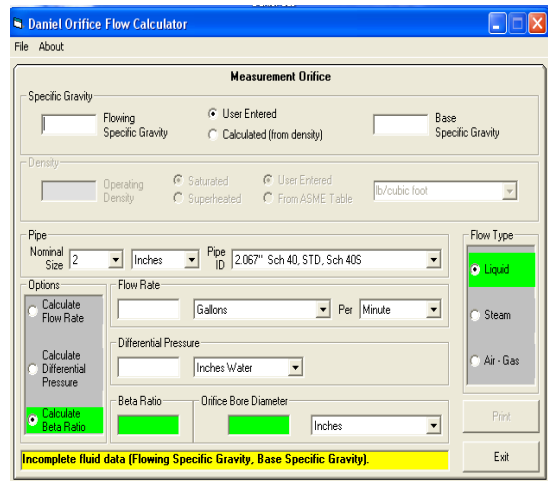
Gas Ultrasonic Meter (USM) Sizing Tool Simulator



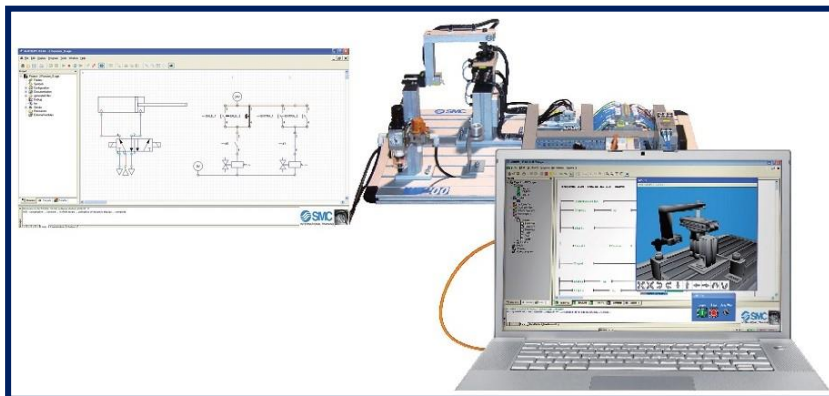
Liquid Turbine Meter and Control Valve Sizing Tool Simulator



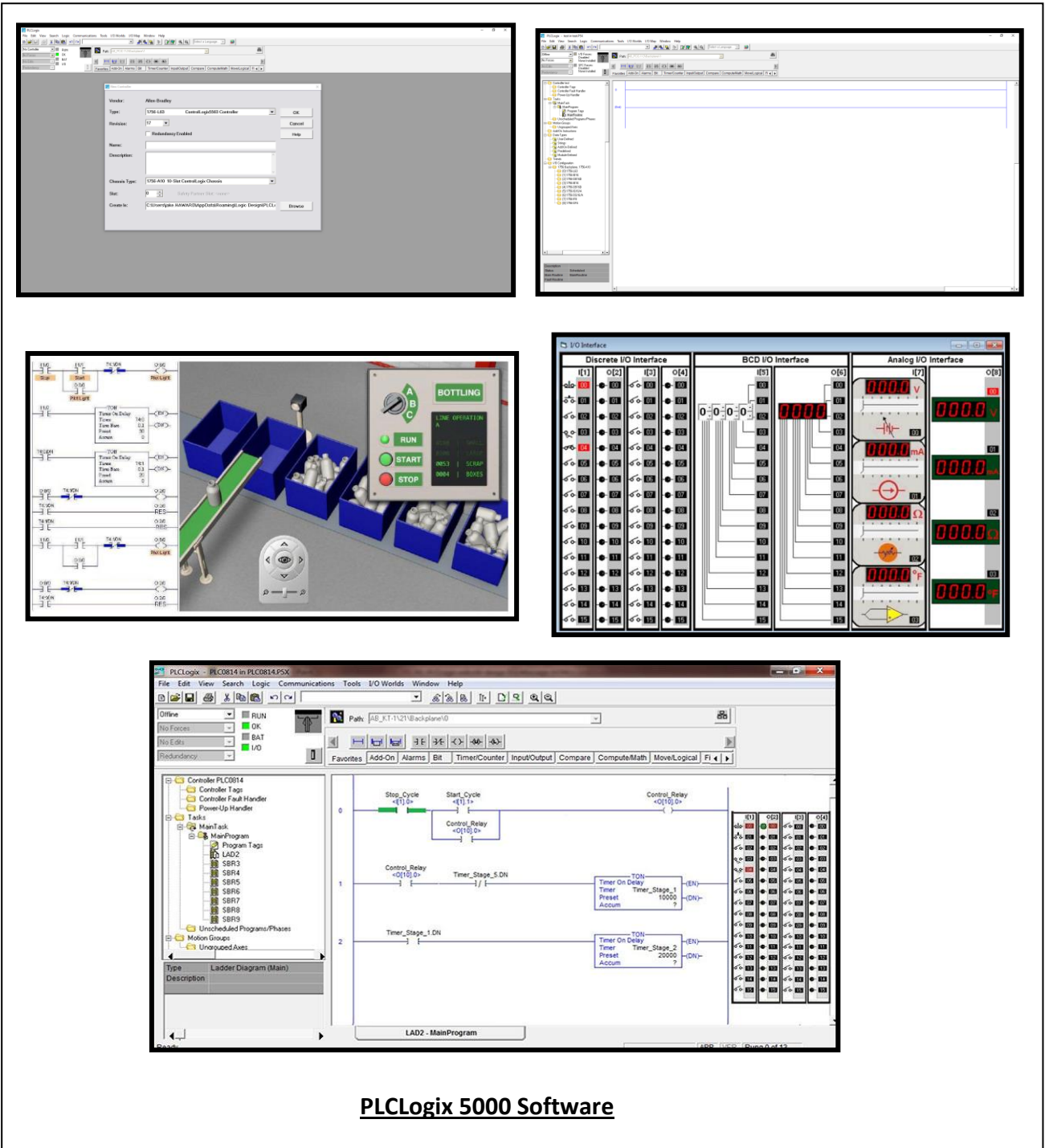
Liquid Ultrasonic Meter Sizing Tool Simulator



Orifice Flow Calculator Simulator



AutoSIM – 200 Automation Simulator



The image displays several screenshots from the PLCLogix 5000 software interface:

- Hardware Configuration:** A dialog box for configuring a PLC rack, showing details like Vendor (Allen Bradley), Type (1756-L53 ControlLogix 5300 Controller), and Redundancy (Enabled).
- I/O Interface:** A panel showing Discrete I/O, BCD I/O, and Analog I/O modules with their respective bit and value indicators.
- 3D Model:** A 3D rendering of a bottling machine with a control panel labeled 'BOTTLING' featuring RUN, START, and STOP buttons, and a 'LINE OPERATION A' indicator.
- Ladder Logic:** A screenshot of the LAD2 - MainProgram showing a control sequence with inputs like Stop_Cycle and Start_Cycle, and outputs like Control_Relay, utilizing timers (Timer_Stage_1 and Timer_Stage_2).

PLCLogix 5000 Software

Course Coordinator

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