Haward Technology Middle East

COURSE OVERVIEW IE0242
Operating System Hardening for OT Environments

Course Title
Operating System Hardening for OT Environments

Course Date/Venue
July 06-10, 2025/Safir Meeting Room, Divan Istanbul, Taksim, Turkey

Course Reference
IE0242

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 Operating System Hardening for OT Environments. It covers the differences between IT and OT security; the operating system hardening and threat landscape for OT systems; the regulatory and compliance standards for OT security; the risk assessment and security baselines for OT operating systems; the hardening strategies for Windows and Linux in OT; the secure installation and patch management, secure user and account management and secure remote access for OT systems; and the network segmentation, isolation strategies, hardening services and processes.

During this interactive course, participants will learn the secure boot and trusted execution and hardening application security in OT systems; the secure logging and monitoring for OT systems, endpoint protection and malware defenses; the. file system and storage hardening, secure industrial protocols and communication and lateral movement and privilege escalation; the incident response plan for OT systems, security forensics and threat intelligence in OT; the business continuity and disaster recovery for OT security; and the compliance audits and security assessments.

Course Objectives

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

- Apply and gain a good working knowledge on operating system hardening for operational technology (OT) environments

- Explain the differences between IT and OT security including operating system hardening

- Recognize threat landscape for OT systems as well as regulatory and compliance standards for OT security

- Apply risk assessment and security baselines for OT operating systems

- Carryout hardening strategies for Windows and Linux in OT

- Implement secure installation and patch management, secure user and account management and configuring secure remote access for OT systems

- Illustrate network segmentation, isolation strategies, hardening services and processes

- Implement secure boot and trusted execution and hardening application security in OT systems

- Recognize secure logging and monitoring for OT systems, endpoint protection and malware defenses

- Apply. file system and storage hardening, secure industrial protocols and communication and prevent lateral movement and privilege escalation

- Develop an incident response plan for OT systems and security forensics and threat intelligence in OT

- Carryout business continuity and disaster recovery for OT security including compliance audits and security assessments

- Automate OS hardening and security policies and implement group policies for secure configurations

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 operating system hardening for OT environments for operational technology managers, compliance and risk managers, OT/ICS security engineers, network security professionals, industrial control system (ICS) engineers, system administrators for OT, IT/OT convergence specialists, OT system integrators, cybersecurity analysts/professionals for OT, vulnerability management specialists, incident response and forensics teams, industrial automation and SCADA operators, IT support staff for OT systems and security auditors for OT environments.

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: -

- **BAC** 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.

- **IACET** 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 Fee

US$ 6,000 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. Barry Pretorius is a **Senior Instrumentation Engineer** with almost **45** years of extensive experience within the **Oil**, **Gas**, **Petrochemical**, **Refinery** & **Power** industries. His expertise widely covers in the areas of **Cyber Security** Practitioner, **Cyber Security** of Industrial Control System, **IT Cyber Security** Best Practices, **Cybersecurity** Fundamentals, **Ethical Hacking & Penetration Testing**, **Cybersecurity** Risk Management, **Cybersecurity** Threat Intelligence, **OT Whitelisting** for Better Industrial Control System Defense, **NESA** Standard and Compliance Workshop, **OT**, **Cyber Attacks** Awareness - Malware/Ransom Ware / Virus /Trojan/ Philsing, **Information Security Manager**, **Security System** Installation and Maintenance, Security of Distributed Control System (**DCS**), Process Control, Instrumentation, Safeguarding & Security, Programmable Logic Controller (**PLC**), **Siemens PLC** Simatic S7-400/S7-300/S7-200, **PLC & SCADA** for Automation & Process Control, **Artificial Intelligence**, **Allen Bradley PLC** Programing and Hardware Trouble Shooting, Schneider **SCADA System**, **Wonder Ware**, **Emerson**, **Honeywell**, **Honeywell** Safety Manager PLC, **Yokogawa**, Advanced **DCS Yokogawa**, **Endress & Hauser**, Field Commissioning and Start up Testing Pre Operations, System Factory Acceptance Test (**FAT**), System Site Acceptance Test (**SAT**), **SCADA HMI & PLC** Control Logic, Implementation, Systems Testing, Commissioning and Startup, **Foxboro DCS & Triconics, SIS** Systems, **Drives**, Motion Control, **Hydraulics**, **Pneumatics and Control Systems** Engineering, **Electrical & Automation Control Systems**, **HV/MV Switchgear, LV & MV** Switchgears & Circuit Breakers, **High Voltage Electrical Safety**, **LV & HV Electrical System**, **HV Equipment** Inspection & Maintenance, **LV Distribution Switchgear & Equipment**, **Electrical Safety**, **Electrical** Maintenance, **Transformers**, **Medium & High Voltage Equipment**, **Circuit Breakers**, **Cable & Overhead Line** Troubleshooting & Maintenance, **Electrical Drawing & Schematics**, **Voltage Distribution**, **Power Distribution**, **Filters**, **Automation System**, **Electrical Variable Speed Drives**, **Power** Systems, **Power Generation**, **Diesel Generators**, **Power Stations**, Uninterruptible Power Systems (**UPS**), **Battery Chargers**, **AC & DC Transmission**, **CCTV** Installation, **Data & Fire Alarm** System, **Evacuation** Systems and **Electrical Motors & Variable Speed Drives**, & Control of Electrical and Electronic devices.

During Mr. Pretorius's career life, he has gained his practical experience through several significant positions and dedication as the **Senior Technical Analyst, Team Leader, Pre-operations Startup Engineer, Automation System's Software Manager, Automation System's Senior Project Engineer, PLC Specialist, Site Manager, Senior Project & Commissioning Engineer, Technical Director, Project Engineer, Radio Technician**, **A T E Technician** and **Senior Instructor/Trainer** from various companies like the ADNOC Sour Gas, Ras Al Khair Aluminum Smelter, Johnson Matthey Pty. Ltd, Craigcor Engineering, Unitronics South Africa Pty (Ltd), Bridgestone/Firestone South Africa Pty (Ltd) and South African Defense Force.

Mr. Pretorius's has a Higher Diploma in **Electrical Engineering Heavy Current**. Further, he is a **Certified Instructor/Trainer** and delivered numerous trainings, courses, workshops, seminars and conferences 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 – 0745	*Registration & Coffee*
0745 – 0800	*Welcome & Introduction*
0800 – 0815	***PRE-TEST***
0815 – 0930	***Overview of Operational Technology (OT) Security*** *Differences Between IT and OT Security ● Common Threats in OT Environments ● Impact of Cyber Threats on Petroleum Operations ● Regulatory and Compliance Requirements for OT Security*
0930 – 0945	*Break*
0945 – 1045	***Introduction to Operating System Hardening*** *Definition and Importance of OS Hardening ● OS Hardening vs. Standard Security Measures ● Challenges of OS Hardening in Industrial Control Systems (ICS) ● Key Hardening Strategies for Windows and Linux*
1045 - 1130	***Threat Landscape for OT Systems*** *Overview of Cyber Threats to Industrial Control Systems ● Common Attack Vectors Targeting OT Networks ● Case Studies of Industrial Cybersecurity Incidents ● Threat Model for OT Environments*
1130 – 1230	***Regulatory & Compliance Standards for OT Security*** *IEC 62443 and NIST Cybersecurity Framework ● ISO 27001 and Compliance Requirements ● UAE Cybersecurity Regulations for Critical Infrastructure ● Industry Best Practices for OT Security*
1230 – 1245	*Break*
1245– 1330	***Risk Assessment & Security Baselines for OT Operating Systems*** *Identifying Security Risks in OT Networks ● Vulnerability Assessment for OT Operating Systems ● Security Configuration Baselines (CIS Benchmarks, STIGs) ● Approach to OT Security Risk Management*

1330 – 1420	**Hardening Strategies for Windows & Linux in OT** *Security Considerations for Windows in OT Environments ● Security Considerations for Linux in OT Environments ● Comparing Windows and Linux Hardening Approaches ● Selecting an OS Hardening Strategy for Industrial Systems*
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	**Secure Installation & Patch Management** *Best Practices for Secure OS Installation ● Patch Management in OT Environments ● Managing Security Updates Without Disrupting Operations ● Patch Management Policy for OT Systems*
0830 – 0930	**Secure User & Account Management** *Least Privilege Access Principle (LPA) ● Role-Based Access Control (RBAC) Implementation ● Securing Administrative and Service Accounts ● Multi-Factor Authentication (MFA) in OT Networks*
0930 – 0945	*Break*
0945 – 1100	**Configuring Secure Remote Access for OT Systems** *Risks of Remote Access in OT Environments ● Best Practices for Secure Remote Access ● VPNs and Zero Trust Architectures in OT ● Remote Access Security Policies*
1100 – 1230	**Network Segmentation & Isolation Strategies** *The Purdue Model for Industrial Control Systems ● Segmenting IT and OT Networks ● VLANs, Firewalls, and DMZs for OT Security ● Secure Communication Protocols for OT Networks*
1230 – 1245	*Break*
1245 – 1330	**Hardening Services & Processes** *Disabling Unnecessary Services and Features ● Secure Configuration of Background Processes ● System Resource Hardening for Stability and Security ● Guidelines for Service Optimization in OT*
1330 – 1420	**Implementing Secure Boot & Trusted Execution** *Secure Boot in Windows and Linux ● Trusted Platform Module (TPM) and Hardware Security ● Protecting Bootloaders and Kernel Integrity ● Secure Boot Policies for OT Environments*
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	**Hardening Application Security in OT Systems** *Securing Industrial Applications and SCADA Systems ● Whitelisting and Application Control Policies ● Restricting Unauthorized Software Installation ● Application Security Policies for OT*

0830 – 0930	**Secure Logging & Monitoring for OT Systems** *Importance of Logging and Monitoring in OT Security ● Configuring Secure Audit Logs ● Centralized Logging Solutions (SIEM, Syslog, Event Logs) ● Incident Detection and Response Strategies*
0930 – 0945	*Break*
0915 – 1100	**Endpoint Protection & Malware Defenses** *Deploying Antivirus and Endpoint Detection & Response (EDR) ● Securing OT Systems Against Ransomware and Malware ● Sandboxing and Behavioral Analysis Techniques ● Endpoint Security Framework for OT Systems*
1100 – 1230	**File System & Storage Hardening** *Encrypting Sensitive OT Data ● Implementing File Integrity Monitoring (FIM) ● Securing Network Storage and Backup Systems ● Secure Storage and Data Retention Policies*
1230 – 1245	*Break*
1245 – 1330	**Securing Industrial Protocols & Communication** *Common OT Communication Protocols (Modbus, DNP3, OPC-UA) ● Secure Configuration of Protocols in Industrial Networks ● Preventing Protocol Spoofing and Man-in-the-Middle Attacks ● Secure Communication Framework for OT Systems*
1300 – 1420	**Preventing Lateral Movement & Privilege Escalation** *Attackers' Tactics for Lateral Movement in OT Networks ● Preventing Privilege Escalation Through OS Hardening ● Network Access Controls to Restrict Lateral Movement ● Internal Threat Detection and Response Plan*
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	**Developing an Incident Response Plan for OT Systems** *Incident Detection and Response Strategies ● Cyber Kill Chain and MITRE ATT&CK Framework ● Building an OT-Specific Incident Response Plan ● Incident Response Readiness for OT*
0830 – 0930	**Security Forensics & Threat Intelligence in OT** *Conducting Forensic Analysis on OT Systems ● Capturing and Analyzing OT Network Traffic ● Threat Intelligence Sharing and Reporting ● Approach to Threat Intelligence in OT*
0930 – 0945	*Break*
0930 -1115	**Business Continuity & Disaster Recovery for OT Security** *Creating Redundant and Resilient OT Systems ● Backup Strategies for Critical OT Infrastructure ● Disaster Recovery Planning for OT Networks ● Testing and Validating Recovery Plans*
1115 – 1230	**Compliance Audits & Security Assessments** *Performing OS Hardening Audits in OT Systems ● Using Security Benchmarks for Compliance (CIS, NIST, IEC 62443) ● Conducting Vulnerability Assessments and Penetration Testing ● Internal and External Security Audits*
1230 – 1245	*Break*

1245 – 1420	**Automating OS Hardening & Security Policies** *Automating OS Security Updates and Patching ● Implementing Group Policies (GPOs) for Secure Configurations ● Scripting Security Configurations with PowerShell & Bash ● Automation Strategy for OT Cybersecurity*
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*

Day5

0730 – 0930	**Case Study: Real-World OT Cyber Incidents & Lessons Learned** *Review of Major OT Cyber Attacks (Stuxnet, Triton, BlackEnergy) ● Lessons Learned for OS Hardening in Operations ● Response to Evolving Cyber Threats ● Future Roadmap for OS Security*
0930 - 0945	*Break*
0945 – 1100	**Hands-on Lab: OS Hardening for Windows in OT** *Implementing Secure Configuration Policies ● Disabling Unnecessary Services and Features ● Setting Up Secure Firewall Rules ● Creating a Hardened Windows Image for OT*
1100 – 1230	**Hands-on Lab: OS Hardening for Linux in OT** *Secure User Account and Access Control Setup ● Configuring SELinux and AppArmor ● Implementing Secure Logging and Monitoring ● Creating a Hardened Linux Image for OT*
1230 – 1245	*Break*
1245 – 1345	**Final Security Assessment & Audit** *Evaluating OS Security Configurations ● Conducting Security Baseline Compliance Checks ● Identifying and Fixing Security Gaps ● Preparing for OT Security Certification*
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", "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
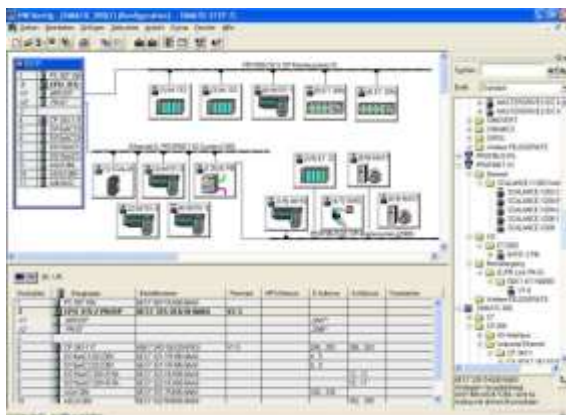
Siemens SIMATIC Step 7 Professional Software
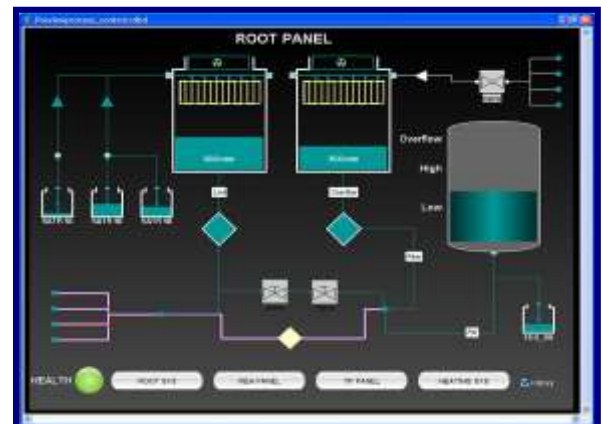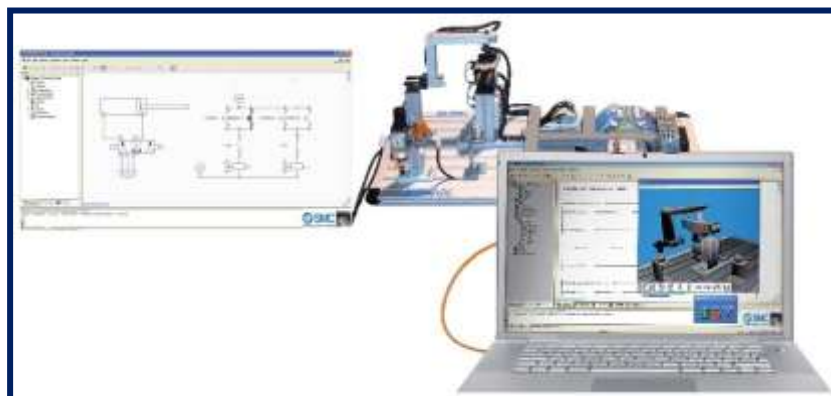

HMI SCADA

Gas Ultrasonic Meter (USM) Sizing Tool Simulator
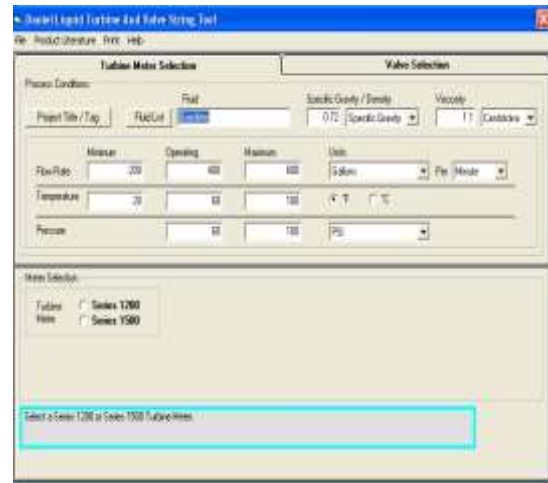
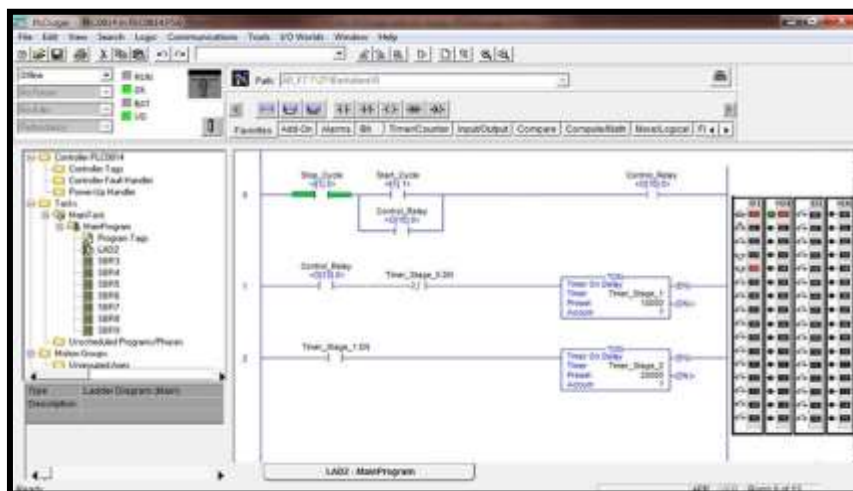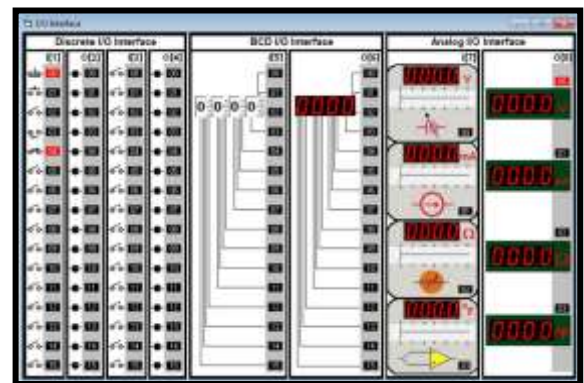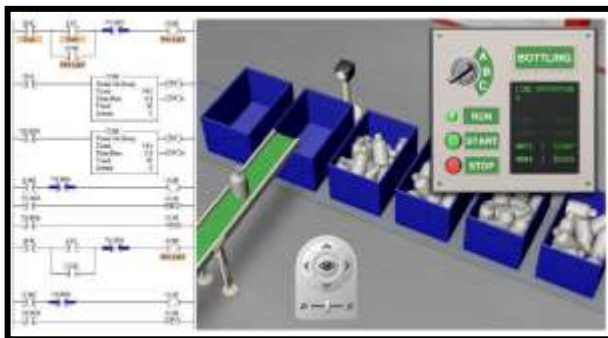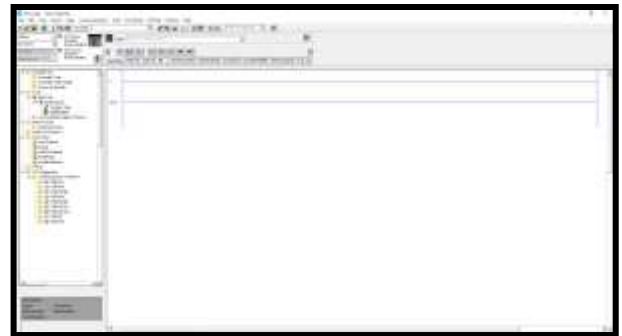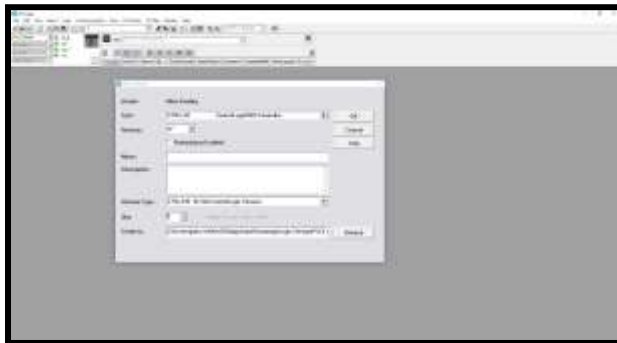**Liquid Turbine Meter and Control Valve Sizing Tool Simulator**

Liquid Ultrasonic Meter Sizing Tool Simulator

Orifice Flow Calculator Simulator

AutoSIM – 200 Automation Simulator

PLCLogix 5000 Software

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