COURSE OVERVIEW IE0234

Overview of OT Patch & Vulnerability Management & Automating Patch Deployment in OT Environments

H-STK© INCLUDED

Course Title

Overview of OT Patch and Vulnerability Management & Automating Patch Deployment in OT Environments

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

3.0 CEUs (30 PDHs) AWARD

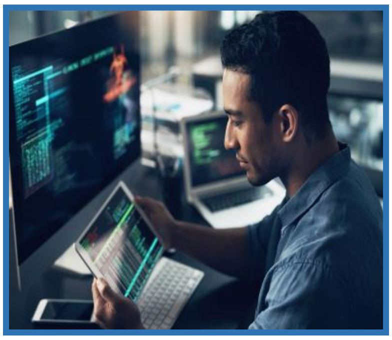
Course Reference

IE0234

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 Overview of OT Patch and Vulnerability Management and Automating Patch Deployment in OT Environments. It covers the key differences between IT and OT security and the importance of patch management in critical infrastructure; the common vulnerabilities in SCADA, DCS and PLC systems including risk-based vulnerability management in OT networks; the compliance and regulatory requirements for OT security and developing an effective OT patch management strategy; and the vulnerability scanning and risk assessment in OT networks as well as patch testing and validation in OT environments.

Further, the course will also discuss the patch deployment planning and change management for critical infrastructure patches; managing patches for vendor-supplied ICS components and securing remote access; the vendor patch validation and approval procedures; the rapid recovery strategies for unsuccessful patch deployments and rollback procedures and system restoration; and the benefits of automating patch deployment in critical systems and selecting the right automation tools for industrial networks.

During this interactive course, participants will learn to secure patch distribution and deployment strategies; use configuration management tools for automated patching; integrate AI and machine learning in patch management; apply remote patch management and cloud-based deployment; implement OT patch management audit and compliance checks; the real-time monitoring of patch effectiveness and continuous improvement in patch and vulnerability management; the emergency patch deployment and zero-day response and securing configuration and hardening of OT systems; the role of threat intelligence platforms in patch prioritization; and the emerging threats and challenges in OT cybersecurity.

Course Objectives

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

- Apply and gain an in-depth knowledge on OT patch and vulnerability management and automating patch deployment in operational technology (OT) environments
- Discuss the key differences between IT and OT security and the importance of patch management in critical infrastructure
- Identify the common vulnerabilities in SCADA, DCS and PLC systems including risk-based vulnerability management in OT networks
- Review the compliance and regulatory requirements for OT security and develop an effective OT patch management strategy
- Carryout vulnerability scanning and risk assessment in OT networks as well as patch testing and validation in OT environments
- Employ patch deployment planning and change management for critical infrastructure patches
- Manage patches for vendor-supplied ICS components, secure remote access and apply vendor patch validation and approval procedures
- Carryout rapid recovery strategies for unsuccessful patch deployments and rollback procedures and system restoration
- Discuss the benefits of automating patch deployment in critical systems and select the right automation tools for industrial networks
- Secure patch distribution and deployment strategies and use configuration management tools for automated patching
- Integrate AI and machine learning in patch management and apply remote patch management and cloud-based deployment
- Implement OT patch management audit and compliance checks as well as real-time monitoring of patch effectiveness and continuous improvement in patch and vulnerability management
- Apply emergency patch deployment and zero-day response and secure configuration and hardening of OT systems
- Define the role of threat intelligence platforms in patch prioritization and discuss the emerging threats and challenges in OT 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 patch and vulnerability management & automating patch deployment in OT environments compliance officers/regulatory managers, risk managers, OT security professionals, IT/OT convergence professionals, cybersecurity professionals, systems and network administrators, industrial engineers, incident response teams, technical support staff.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30%	Lectures
20%	Practical Workshops & Work Presentations
30%	Hands-on Practical Exercises & Case Studies
20%	Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Fee

US$ 5,500 per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Accommodation

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

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours

Certificate Accreditations

Certificates are accredited by the following international accreditation organizations: -

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Mr. Said Ghanem, MSc, BSc, is a **Senior Electrical & Instrumentation Engineer** with almost **20 years** of wide experience within the **Oil**, **Gas**, **Power**, **Petroleum**, **Petrochemical** and **Utilities** industry. His extensive experience widely covers in the areas of **Process Control & Instrumentation**, **Pressure & Temperature** Measurement, **Level & Flow** Measurement, **Control Valve & Actuator**, Distributed Control System (**DCS**), Programmable Logic Controllers (**PLC**), **Control System & Instrumentation**, **GE Steam Turbines**, **Speedtronic Mark II**, **V & VIe**, Control Systems, **GE Gas Turbine Frame V**, **Combined Cycle Power Plant**, **ABB DCS Control**, **Ansaldo Gas Turbine**, **Field Instrumentation & Calibration**, PLC Step7 Control Systems, **Transducers & Control Valves**, **Switches**, **Transmitters**, Proximity Sensors, Control Systems Cards, **Analog & Digital Multi-meters**, Druck DPI 610, Hand Pump, Hart Communicator 475, Two Ansaldo Gas Turbine Model AE94.2, Process, Control Philosophy ,Logic & Wiring Diagrams, Instrument Specifications & Data Sheets For Sensors, Control Valves, PRVs, Electrostatic Discharge (**ESD**), Digital & Microprocessor Based Instruments, Mark VI Control System Software Program (**Toolbox ST**), **Compact PCI Controller**, IO NET, IO Packs & Terminal Boards & Sulzer Turbines. Further, he is also well-served in Firefighting Systems, Smoke Detectors & Gas Detectors, Model Predictive Control (**MPC**) & Adaptive Control Strategies, **Control System** Optimization, **Real-Time Control System** Monitoring, **RCA** Methodologies, **Control Loops**, **Lean** Methodologies, Statistical Process Control (**SPC**), **Energy Efficiency & Process** Optimization, **Automation & Control** Systems, **Process** Safety & Troubleshooting, **Process** Safety Controls & Mitigation Strategies, **Rotating Equipment** (**Pumps**, **Turbines**, **Compressors**), Preventive Maintenance & Reliability-Centered Maintenance (RCM) and **Steam Generation** Systems.

During his career life, Mr. Said has held various significant positions as the **Instrumentation & Control Maintenance Engineer**, **Instrument Field Maintenance Engineer**, **Senior Instrument Maintenance Engineer**, **Lead Instrument & Control Engineer** and **Senior Trainer/Lecturer** from the Ministry of Electrical Energy, Egyptians Maintenance Company (EMC) and Belayim Power Station Petroleum Company (Petrobel).

Mr. Said has a **Master's** degree in **Electrical Engineering** and a **Bachelor's** degree in **Electrical**, **Communication & Electronic Engineering**. Further, he is a **Certified Instructor/Trainer** and has delivered numerous trainings, courses, workshops and conferences worldwide.

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	***Understanding OT Security & Industrial Control Systems (ICS)*** *Key Differences Between IT and OT Security ● Industrial Control Systems (ICS) Architecture Overview ● Challenges in Securing OT Environments ● OT Security and Compliance Requirements*
0930 – 0945	*Break*
0945 – 1045	***Overview of Patch Management in OT Systems*** *Importance of Patch Management in Critical Infrastructure ● Differences Between Patch Management in IT vs. OT ● Risk vs. Reward: When to Patch vs. When to Delay ● Impact of Patching on System Uptime and Reliability*
1045 - 1130	***Understanding Vulnerabilities in OT Environments*** *Common Vulnerabilities in SCADA, DCS, and PLC Systems ● Zero-Day Vulnerabilities and Their Impact on OT Networks ● Threat Intelligence and Vulnerability Databases (CVE, ICS-CERT) ● Case Studies: Major OT Cyber Incidents Due to Vulnerabilities*
1130 – 1230	***Risk-Based Vulnerability Management in OT Networks*** *Identifying and Classifying Vulnerabilities ● Risk Scoring and Prioritization Frameworks (CVSS, NIST) ● Aligning Patch Management with Risk Mitigation Strategies ● Using Threat Intelligence for Patch Planning*
1230 – 1245	*Break*
1245– 1330	***Compliance & Regulatory Requirements for OT Security*** *NIST 800-82: Guide to Industrial Control System Security ● IEC 62443: Security for Industrial Automation and Control Systems ● Cybersecurity Standards for OT Environments ● UAE and International OT Security Regulations*
1330 – 1420	***Case Study: OT Cybersecurity Breaches & Lessons Learned*** *Stuxnet Attack: Exploiting Unpatched Vulnerabilities ● TRITON Malware: Targeting ICS and Safety Instrumented Systems ● Colonial Pipeline Attack: IT-OT Convergence Risks ● Approach to Strengthening OT Cyber Resilience*
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	***Developing an Effective OT Patch Management Strategy*** *Key Steps in an OT Patch Management Lifecycle ● Patch Deployment Challenges in Critical Operations ● Patch Scheduling Without Disrupting Industrial Processes ● Establishing Patch Testing and Validation Procedures*
0830 – 0930	***Vulnerability Scanning & Risk Assessment in OT Networks*** *Passive vs. Active Vulnerability Scanning Techniques ● Identifying Security Gaps in SCADA/DCS/PLC Systems ● Risk-Based Decision Making for Patch Application ● OT-Specific Tools for Vulnerability Assessment*

0930 – 0945	Break
0945 – 1100	***Patch Testing & Validation in OT Environments*** *Establishing a Secure Patch Testing Environment • Simulating Patch Deployment on a Digital Twin • Testing Patches for Compatibility with ICS and PLCs • Best Practices for Patch Testing and Rollback*
1100 – 1230	***Patch Deployment Planning & Change Management*** *Coordinating Patch Deployment with Operational Teams • Version Control and Patch Rollback Procedures • Change Management for Critical Infrastructure Patches • Minimizing Downtime While Applying Security Patches*
1230 – 1245	Break
1245 – 1330	***Third-Party Vendor Patching & Supply Chain Security*** *Managing Patches for Vendor-Supplied ICS Components • Risks of Third-Party Software in OT Systems • Securing Remote Access for Vendor Maintenance Activities • Vendor Patch Validation and Approval Procedures*
1330 – 1420	***Incident Response Planning for Patch Failures*** *Common Patch Failures and Their Impact on Operations • Rapid Recovery Strategies for Unsuccessful Patch Deployments • Rollback Procedures and System Restoration • Case Study: Patch Failure and Recovery in an ICS Network*
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	***Basics of Automated Patch Management for OT Systems*** *Benefits of Automating Patch Deployment in Critical Systems • Challenges of Automating Patching in Legacy OT Infrastructure • Selecting the Right Automation Tools for Industrial Networks • Digital Transformation Strategy for OT Security*
0830 – 0930	***Secure Patch Distribution & Deployment Strategies*** *Segmentation of OT Networks for Patch Distribution • Secure Channels for Patch Delivery and Installation • Air-Gapped System Considerations in Patch Deployment • Ensuring Patch Integrity with Cryptographic Hashing*
0930 – 0945	Break
0915 – 1100	***Using Configuration Management Tools for Automated Patching*** *Role of Configuration Management in OT Security • Popular OT Patch Management Tools (WSUS, SCCM, Ansible, SaltStack) • Automating Patch Scheduling with Centralized Control • Case Study: Automating Security Updates for Industrial Controllers*
1100 – 1230	***Integrating AI & Machine Learning in Patch Management*** *AI-Based Threat Detection and Patch Prioritization • Machine Learning for Predictive Patch Deployment • Self-Healing OT Systems with Automated Remediation • Real-World Applications of AI in Industrial Cybersecurity*
1230 – 1245	Break

1245 – 1330	***Remote Patch Management & Cloud-Based Deployment*** *Cloud vs. On-Premises Patch Management for OT Systems ● Secure Remote Patch Deployment Using Zero-Trust Architecture ● Implementing Multi-Factor Authentication (MFA) for Patch Access ● Approach to Securing Remote Patching*
1300 – 1420	***Hands-On Lab: Automating Patching in a Simulated OT Environment*** *Setting Up an OT Patch Management Tool ● Simulated Patch Testing and Deployment ● Monitoring Patch Performance and Validating Updates ● Troubleshooting and Optimizing Patch Automation Workflows*
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	***OT Patch Management Audit & Compliance Checks*** *Ensuring Compliance with Cybersecurity Framework ● Conducting Internal and External Patch Audits ● Generating Reports for Regulatory Compliance ● Best Practices for Maintaining Patch Logs*
0930 – 0945	*Break*
0930 -1115	***Real-Time Monitoring of Patch Effectiveness*** *Setting Up Security Information and Event Management (SIEM) ● OT-Specific Threat Monitoring Solutions ● Correlating Patch Data with Threat Intelligence Feeds ● Case Study: Identifying Post-Patch Vulnerabilities*
1115 – 1230	***Continuous Improvement in Patch & Vulnerability Management*** *Lessons Learned from Past Patch Deployments ● Implementing a Continuous Patch Improvement Cycle ● Key Metrics for Measuring Patch Effectiveness ● Roadmap for OT Patch Management Strategy*
1230 – 1245	*Break*
1245 – 1420	***Emergency Patch Deployment & Zero-Day Response*** *Identifying and Responding to Zero-Day Vulnerabilities ● Emergency Patch Approval Workflow for Critical Infrastructure ● Isolating High-Risk Systems During Emergency Patching ● Case Study: Responding to a Zero-Day Exploit in an OT Network*
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 – 0830	***Secure Configuration & Hardening of OT Systems*** *Implementing Secure Baseline Configurations ● Hardening SCADA, DCS, and PLC Systems Against Exploits ● Restricting Unnecessary Services and Network Ports ● Best Practices for Secure OT Network Architecture*
0830 – 0930	***Threat Intelligence & Future Trends in OT Security*** *Role of Threat Intelligence Platforms in Patch Prioritization ● Emerging Threats and Challenges in OT Cybersecurity ● Future of AI and Blockchain in OT Patch Management ● Vision for Cyber-Resilient Industrial Operations*

0930 - 0945	*Break*
0945 – 1100	***Real-World Case Studies of OT Patch Management Success and Failures***
1100 – 1230	***Group Exercise: Patch Risk Analysis and Deployment Strategy***
1230 – 1245	*Break*
1245 – 1345	***Hands-On Lab: Implementing Automated Patch Deployment in an OT Lab***
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

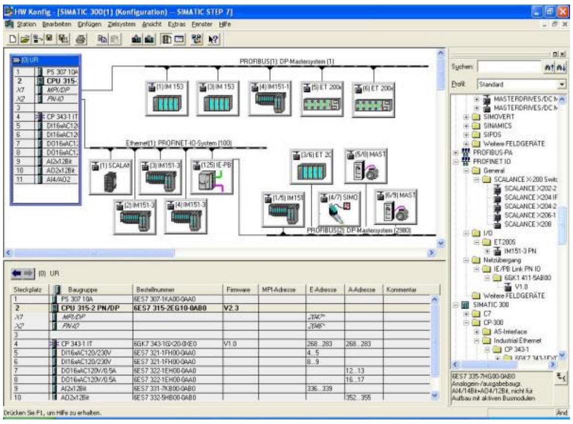
Siemens S7-1200 Simulator

Siemens S7-400 Simulator

Siemens SIMATIC S7-300

Siemens S7-200 Simulator

GE Fanuc Series 90-30 PLC Simulator



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

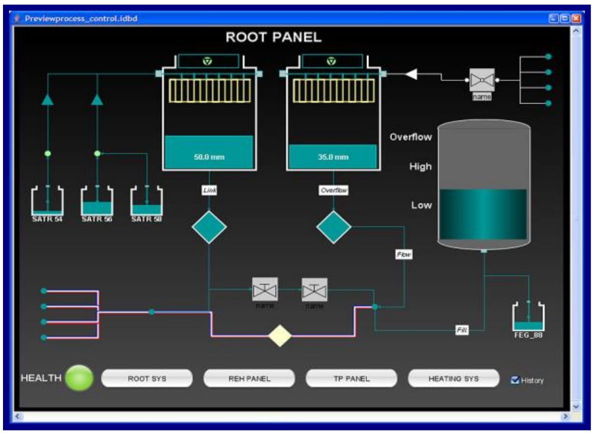
Station Bearbeiten Einfügen Zielsystem Ansicht Extras Fenster Hilfe

(0) UR

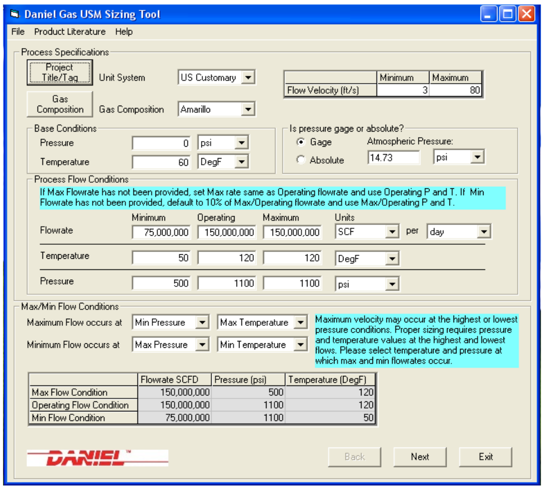
Steckplatz	Baugruppe	Bestellnummer	Firmware	MPI-Adresse	E-Adresse	A-Adresse	Kommentar
1	PS 307 10A	6ES7 307-1KA00-0AA0					
2	CPU 315-2 PN/DP	6ES7 315-2EG10-0AB0	V2.3				
X7	MPI/DP				2047*		
X2	PN-IO				2046*		
3							
4	CP 343-1 IT	6GK7 343-1GX20-0XE0	V1.0		268...283	268...283	
5	DI16xAC120/230V	6ES7 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	

Drücken Sie F1, um Hilfe zu erhalten.

Siemens SIMATIC Step 7 Professional Software



HMI SCADA



Process Specifications

Unit System: US Customary

Gas Composition: Amarillo

	Minimum	Maximum
Flow Velocity (ft/s)	3	80

Base Conditions

Pressure: 0 psi

Temperature: 60 DegF

Is pressure gage or absolute?
● Gage ○ Absolute
Atmospheric Pressure: 14.73 psi

Process Flow Conditions

If Max Flowrate has not been provided, set Max rate same as Operating flowrate and use Operating P and T. If Min Flowrate has not been provided, default to 10% of Max/Operating flowrate and use Max/Operating P and T.

	Minimum	Operating	Maximum	Units
Flowrate	75,000,000	150,000,000	150,000,000	SCF per day
Temperature	50	120	120	DegF
Pressure	500	1100	1100	psi

Max/Min Flow Conditions

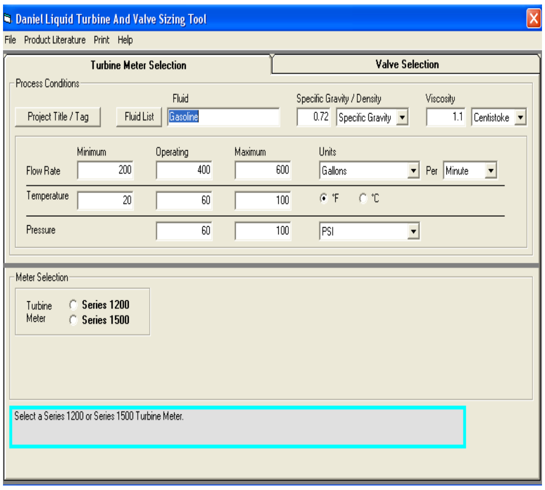
Maximum Flow occurs at: Min Pressure, Max Temperature

Minimum Flow occurs at: Max Pressure, Min Temperature

Maximum velocity may occur at the highest or lowest pressure conditions. Proper sizing requires pressure and temperature values at the highest and lowest flows. Please select temperature and pressure at which max and min flowrates occur.

	Flowrate SCFD	Pressure (psi)	Temperature (DegF)
Max Flow Condition	150,000,000	500	120
Operating Flow Condition	150,000,000	1100	120
Min Flow Condition	75,000,000	1100	50

Gas Ultrasonic Meter (USM) Sizing Tool Simulator



Process Conditions

Fluid: Gasoline

Specific Gravity / Density: 0.72 Specific Gravity

Viscosity: 1.1 Centistoke

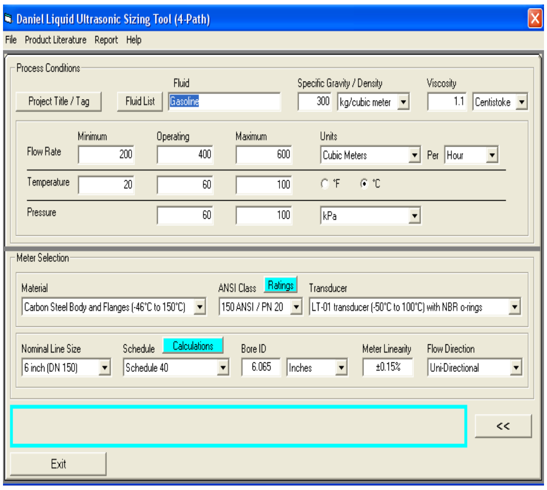
	Minimum	Operating	Maximum	Units
Flow Rate	200	400	600	Gallons Per Minute
Temperature	20	60	100	● °F ○ °C
Pressure		60	100	PSI

Meter Selection

Turbine Meter ○ Series 1200 ○ Series 1500

Select a Series 1200 or Series 1500 Turbine Meter.

Liquid Turbine Meter and Control Valve Sizing Tool Simulator



Process Conditions

Fluid: Gasoline

Specific Gravity / Density: 300 kg/cubic meter

Viscosity: 1.1 Centistoke

	Minimum	Operating	Maximum	Units
Flow Rate	200	400	600	Cubic Meters Per Hour
Temperature	20	60	100	○ °F ● °C
Pressure		60	100	kPa

Meter Selection

Material: Carbon Steel Body and Flanges (-46°C to 150°C)

ANSI Class: 150 ANSI / PN 20

Transducer: LT-01 transducer (-50°C to 100°C) with NBR o-rings

Nominal Line Size: 6 inch (DN 150)

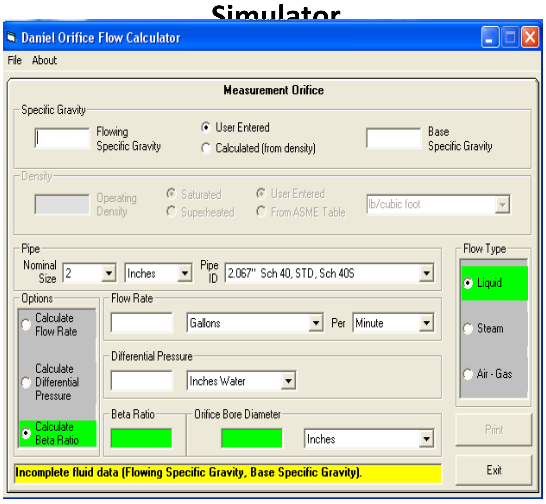
Schedule: Schedule 40

Bore ID: 6.065 Inches

Meter Linearity: ±0.15%

Flow Direction: Uni-Directional

Liquid Ultrasonic Meter Sizing Tool Simulator



Measurement Orifice

Specific Gravity

Flowing Specific Gravity:
● User Entered ○ Calculated (from density)
Base Specific Gravity:

Density

Operating Density:
Saturated / Superheated
User Entered / From ASME Table
lb/cubic foot

Pipe

Nominal Size: 2 Inches

Pipe ID: 2.067" Sch 40, STD, Sch 40S

Flow Type: ● Liquid ○ Steam ○ Air - Gas

Options: ○ Calculate Flow Rate ○ Calculate Differential Pressure ● Calculate Beta Ratio

Flow Rate: Gallons Per Minute

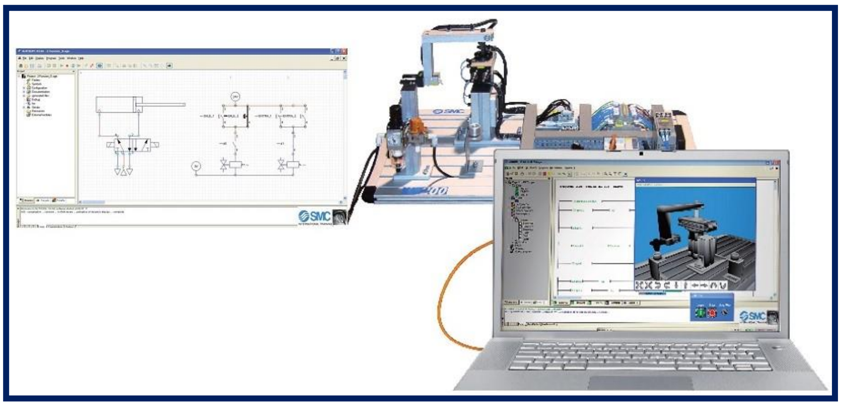
Differential Pressure: Inches Water

Beta Ratio

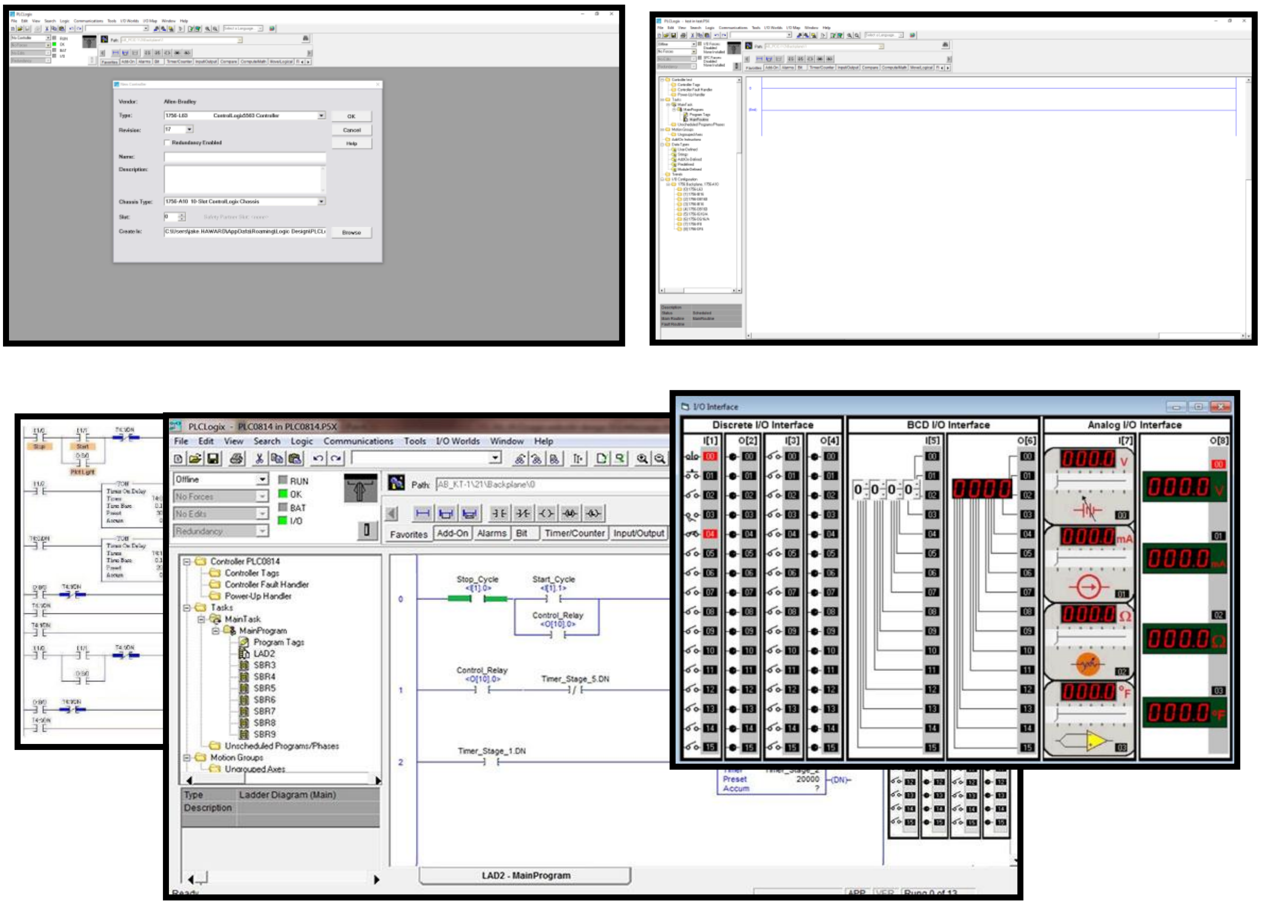
Orifice Bore Diameter: Inches

Incomplete fluid data (Flowing Specific Gravity, Base Specific Gravity).

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