<u>SEC600</u>:
Process Control Software, Hardware Security and Cyber Security

Duration:	**1 Day Classroom or 4 hours Online**
Audience:	**Process Control Engineers, Supervisors, Managers, DCS/PLC Technicians/Operators and Laboratory Technicians.**
Prerequisites:	**None**
Course Material:	**Training slides and hand-outs.**

Course Description and Objectives:

Modern-day process control systems need to be secured and protected against unauthorized personnel, hackers and potentially malicious attackers. Cyber security understanding, needs and a defensive plan is increasingly important these days. Plant and process data must be protected from competitors or contractors having temporary access to the control systems. Viruses, worms etc., can infect and bring-down an entire process control network if the control system is not adequately and appropriately protected. User IDs, access control for new employees, leaving employees, contractors etc. need to be properly implemented and enforced. Control room access, magnetic card access, DCS/PLC access etc., need to be properly enforced in the modern control room and process control environment. This course is a must for process control management and staff in order to protect data, protect the entire control system and ensure safe and reliable operation.

Learning Outcomes:

This course focuses on important process control system security concepts. It helps to staff the control systems team correctly to ensure that control systems security is properly enforced at the plant. The course discusses security forms that can be used to get signatures from various staff members for facilitating securities enforcements. Forms you get from the course can be directly used immediately at the plant. The course provides information to make the plant control system safe and secure. The following topics are covered in this course:

- Industrial process control network architecture
- The concept of L0 – L4 (levels of industrial process control networks)
- Process control system security
- Password, user IDs and handling of shared passwords Passwords, user accounts and automatic password expiration Protecting non-24-hour manned process control consoles
- Control room access controls, DCS/PLC configuration access controls, Personnel security
- Preventing unauthorized access
- Protecting proprietary data and intellectual property, attorney reviews
- Sharing control room with different competing technologies
- Satisfying licensor requirements regarding patents and proprietary technology Virus patches and updates
- Remote access security and control, remote process control support and monitoring Developing securities and control forms for management approval
- Developing the required management approval authority for security and controls Protecting proprietary data from offices and control rooms
- Developing teams to manage process control systems and audits
- How to conduct formal process control audits to ensure control system reliability