Outline

Deployment of Cyber security for Information Technology (IT) systems (financial, commercial and government) is an already a standard process. These systems are focusing on assurance of Confidentiality, Integrity and Availability (CIA), and use a broad range of defense measures such as antivirus, firewalls, and other measures. Reliable and safe operation of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) are considered critical to the functioning of businesses in countries and for wellbeing of their residents. According to the system architecture and the selected communication network. These systems provide near real time monitoring and control with time delays ranging between fractions of seconds to minutes. Until about a decade ago these critical infrastructure systems such as electricity, water, oil and gas, transportation were isolated from the internet and all types of external communications and the risk of cyber-attack was not even consider. Most attention was dedicate to assurance of operating Safety and Reliability, and the risk of cyber-attack and consequently protecting of these infrastructures was not consider. Deployment of cyber defense measures similar to those measured used for protecting IT systems from cyber-attack became an essential activity, especially after the widely publicized Stuxnet (nuclear facility attack) occurred in the mid of 2010.

Target Audience

The proposed training is aimed to upgrade the cyber security knowledge of wide range of people coming from the IT and the SCADA/ICS arena, and make them understanding of terms, technologies, attack and defense processes for better defending the computerized control under their responsibility.
You will acquire knowledge in the field of cyber technologies and defense measures, and this training format is highly Engineers involved with design, maintenance of critical plants

- People in charge of IT communication who need to know more on cyber defense
- SCADA/ICS engineers involved with design, maintenance of industrial plants
- Operators dealing with control of renewable and other power technology plants
- Operators of sewage plants, desalination and other chemical process plants
- Broad range of managers interested upgrading their technical knowledge

Upon completion of this well-structured cyber technology and defense training, you will be well prepared to apply for certification classes such as CISO, CISSP and other as applicable for your business activity and need of your organization.

**Contents**

**Module 1: Introduction to SCADA Technology**

- People in charge of IT communication who need to know more on cyber defense
- SCADA/ICS engineers involved with design, maintenance of industrial plants
- Operators dealing with control of renewable and other power technology plants
- Operators of sewage plants, desalination and other chemical process plants
- SCADA-Data Communication
- Complementing SCADA components
- Sensors and Field Control Devices
- Principles of PLC configuration

**Module 2: Introduction to SCADA-Cyber Security**
- Introduction to SCADA system Security Vulnerabilities
- Difference between SCADA and IT systems
- Brief introduction on security architectures
- Principles of Encryption and Authentication
- Cyber Defense measures for SCADA Systems
- Anomaly detection, Defense in Depth, etc.
- Principal operation of IDS, IPS, SIEM, DMZ, etc.
- Remote access for maintenance and support
- External and Internal attacking of SCADA systems
- MitM, DOS, DDoS, Cyber resiliency, GPS spoofing
- Security assessment, regulations, best practices
- Principles of Access and Identity management
- 21 steps to enhance Cyber security defense

**Module 3: Identity and Access management**
- Note: This part is mandatory section for CISSP Certification
- Physical and logical access control
- Identification and authentication of people and devices
- IaaS - Identity as a service (e.g. cloud service providers)
- 3rd party Identity service (on-premises solutions)
- Cyber-attack on Access Control systems
- Identity and access provisioning lifecycle