Virtual Course

Industrial Cybersecurity Management for projects in the Energy, Oil and Gas sector

The ability of any organization (end user or supplier) to develop and implement successful industrial cybersecurity management projects, making optimal use of resources in a minimum amount of time and with clear visualization of progress, is no longer an option. The modular, clear approach of the WBS methodology makes it easy, reliable, cost-effective, secure, predictable and visible to everyone.

April, 18-19, 2023

10:00 a.m. to 2:00 p.m. (GMT-3)

Only for Arpel members companies

arpel ASSOCIATION OF OIL, GAS AND RENEWABLE ENERGY COMPANIES OF LATIN AMERICA AND THE CARIBBEAN

WiseCourses® Academy

At the end of the course, you will be able to:

- Understand each of the necessary activities to be developed in order to implement a consistent industrial cybersecurity program which complies with international standards by industry consensus and other national regulations.
- Understand the minimum requirements and inputs needed to properly initiate each of the activities, the resources needed, and a realistic time estimate.
- Understand the necessary objectives and deliverables to be produced as a result of the different activities, as well as the corresponding reports as demonstration and evidence of such implementation.
- Know how to demonstrate compliance with the ISA/IEC-62443-X-X series of standards (and other regulations). Important for the organization that wants to certify the CSMP system.
- Formalize and document the completion of each of the major activities of the CSMP program. Observe and analyze the results of everything that is being done.
- Certify progress in a modular way. Can be used by a Project Manager (PM) to properly monitor progress in multiple plants and processes at the same time.
- Generate the necessary evidence that the organization is in compliance with the implementation of a consistent, complete Industrial Cybersecurity program.
- Facilitate good decision making to mitigate Industrial Cyber risks, in order to protect valuable assets and create an industrial infrastructure that is resilient to all types of threats.
- Produce and document the necessary elements to adequately justify industrial cybersecurity investments with the certainty that security risks are mitigated.

Who is it aimed at?

- Recommended for all personnel in industrial sectors such as energy, water, oil and gas that are related to critical infrastructure protection activities and control systems.
- It is recommended for IT security managers, system integrators, industrial control system suppliers, plant engineers, production and plant operation management, industrial security, security instrumented systems specialists and maintenance personnel; whether senior or middle management.

Certificate: Industrial Cybersecurity & Critical Infrastructure Manager.

- CRE Credits: 0.8
- The certification exam is taken in class at the end of the course. Available in Spanish, Portuguese and English.

Modality and schedule:

This course is available in all modalities: face-to-face (at WisePlant Offices, at Client's Plant, at Academy) and Virtual (Synchronous, Asynchronous and On-Demand) modalities. Even face-to-face, the course requires participants to use the Educational Platform in order to access the abundant supplementary material and to take the Final Evaluation.

Duration: 8 hours with the teacher, including the final evaluation.

Summary of the main features of the course:

- Both the voice-over and the complete course material, which will be available for consultation in the Educational Campus (asynchronous), are in Spanish, Portuguese and English.
- It includes online practical exercises. Each attendee accesses remotely from the campus to a specialized computer networked with the rest of the computers in the course, to perform several practical exercises on Cybersecurity in networks with specific software and applications.
- Plenty of supplementary reading material (in original languages only).
- Virtual group study meetings until the exam is taken, even after the end of the course.
- All the opportunities you need to take the exam up to 6 months after the end of the course through the Prometric system.
- The attendee can log in to the Campus to consult the course material for a period of 1 year.
- Coaching, chat and blog 7×24 for a period of 1 year, to assist your organization in the implementation of the acquired practical knowledge.

Requirements:

No specific requirements. It is recommended that the professional has knowledge of some of the following: Project Management according to PI/PMBOK methodology, International Cybersecurity Standards by industry consensus ISA/IEC-62443, Corporate Cybersecurity or Information security standards ISO-27000, Industrial risk management standards such as ISA/IEC-61511, functional safety, National regulations and/or standards such as NIST, NERC, and others; Experience in corporate project management and cultural change management, Other industrial risk management standards (worker safety, environmental safety, etc.).

Registration link