

EN50 ^{v3.20}

Industrial Cybersecurity Management

Projects in the energy, oil & gas sector

An EN program initiative with ARPEL

ENERGY

OIL

GAS

Structure. Responsibility. Evidence.

Build a documented cybersecurity program

Apply the WBS methodology to organize activities, resources and deliverables across industrial cybersecurity projects.

PLAN

Define inputs, resources and priorities.

COORDINATE

Align responsibilities and track progress.

DEMONSTRATE

Document activities and implementation evidence.

ISA/IEC 62443 | NERC | C2M2 | TSA

EN50

EN60

EN61

EN62

EN70

EN99

Turn governance into practice

A shared methodology for industrial projects

The ability of any organization (end user or supplier) to develop and implement industrial cybersecurity management projects successfully, making optimal use of resources, in minimal time, with a clear visualization of progress, is no longer an option.

The modular approach of the WBS methodology, with the clarity it provides, makes it reliable, profitable, and predictable for everyone.

This course addresses the management of industrial cybersecurity, focusing on the energy, oil and gas industries. It means complying with all the requirements of the ISA/IEC-62443 series of standards, harmonizing with the typical regulations of these sectors, which are NERC, C2M2, TSA, and other popular regulations.

Who is it aimed at?

Recommended for all personnel in industrial sectors such as: energy, water, oil, gas, steel, food, pharmaceutical, and many others, which are related to the activities of protecting critical infrastructure and control systems.

The participation of IT security managers, system integrators, industrial control system providers, plant engineers, production and plant operation management, industrial security, specialists in security instrumented systems and maintenance personnel is recommended, whether they are high or middle management.

Course essentials

Version 3.20

0.8 CRE credits

8 lessons / 1 quiz

Digital course materials



Build your team's capability

Explore EN50 or request a corporate proposal.

EN50

EN60

EN61

EN62

EN70

EN99

Detailed syllabus

Program foundations / 01-04

01 Policies and procedures

Development of minimum necessary policies and procedures for the industrial cybersecurity program, CSMP.

02 Competencies and awareness

Development of necessary competencies, training programs and awareness of the entire organization.

03 Audit and improvement

Audit, compliance and continuous improvement.

04 Standards harmonization

Harmonization of the ISA/IEC-62443 series of standards with popular regulations (NERC, C2M2, TSA).



A shared methodology for industrial cybersecurity

Detailed syllabus

Lifecycle and implementation / 05-08

05 Life Cycle Phase

- Industrial Cybersecurity risk assessment and decision-making to mitigate non-tolerable risk.
- Design and implementation of security to protect all industrial assets and potential risk receptors.
- Operation and maintenance to maintain the minimum necessary security tolerable by the organization.

06 Supplier development

Development and classification of suppliers for Industrial security.

07 Engineering and validation

Process of engineering, design, purchasing, construction, testing and security validation in new systems.

08 Implementation strategy

Implementation strategy and essential recommendations that will save the company more than 50% in implementation effort and resources.

Full syllabus text from the EN50 course webpage.

EN50**EN60****EN61****EN62****EN70****EN99**

Learning objectives

At the end of the EN50 course, you will be able to:

- 01** Understand each of the activities that are necessary to develop to implement a mature industrial cybersecurity program, complying with international standards by industry consensus and popular regulations of the sector.
- 02** Understand the requirements and the minimum inputs necessary to start each of the activities appropriately, the necessary resources and a credible time estimate.
- 03** Understand the objectives and deliverables that are necessary to produce as results of the different activities and the corresponding reports as demonstration and evidence of said implementation.
- 04** How to demonstrate compliance with the ISA/IEC-62443-XX series of standards (and other regulations). Important for the organization that wants to certify the CSMP system.
- 05** Formalize and document the completion of each of the major activities of the CSMP program. Observe and analyze the results of everything you are doing.
- 06** Certify progress in a modular way. A Project Manager (PM) can use it to appropriately monitor progress across multiple plants and processes at the same time.
- 07** Generate the necessary evidence that the organization is complying with the implementation of a mature and complete Industrial Cybersecurity program.
- 08** Facilitate good decision-making to mitigate industrial cyber risks to protect the most valuable assets and create an industrial infrastructure resistant to all types of threats.
- 09** Produce and document the elements necessary to justify industrial cybersecurity investments adequately with the certainty that security risks are mitigated.

Plan your participation

Requirements, learning resources and recognition

Requirements

It has no specific requirements. It is recommended that the professional have knowledge of some of the following:

- Project Management according to PI/PMBOK methodology.
- International Cybersecurity Standards by industrial 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.).

Deliverables

Participants will receive the material digitally through the educational platform, including the following materials.

- Access to course lessons online.
- Various documents, videos, and complementary material so that participants can delve deeper.
- Access to educational campus to download additional information and software.

Certificates

A first certificate of knowledge is issued upon completion of the course.

Industrial Cybersecurity and Critical Infrastructure Life Cycle Management Practitioner

CRE credits: 0.8

The certification exam is taken in class at the end of the course. Available in Spanish, Portuguese, and English.

A second experience certificate is issued after practical implementation in real projects.

Expert in Life Cycle Management of Industrial Cybersecurity and Critical Infrastructures

CRE Credits: cumulative, depending on the duration of the activities carried out by the practitioner.

Recognitions

All participants who meet the course requirements and successfully pass the final exam with a good grade will be awarded a Digital Badge. The digital Badge certifies that the participant has attended the EN50 training course and has completed the final evaluation test with a good score, verifying that said participant has assimilated the new knowledge.



Learn. Build. Advance.

Course details, formats and availability: [wisecourses.com/courses/en50-oen-320/](https://www.wisecourses.com/courses/en50-oen-320/)

EN50**EN60****EN61****EN62****EN70****EN99**

An initiative with ARPEL

Supporting the Energy, Oil & Gas market



The EN training program was created as an initiative with ARPEL to support the Energy, Oil & Gas market. It develops industrial cybersecurity capabilities through a shared methodology for governance, risk assessment, engineering, implementation and operations.

About ARPEL

Founded in 1965, ARPEL is a nonprofit association bringing together oil, gas and renewable energy companies and institutions in Latin America and the Caribbean. It promotes cooperation, knowledge exchange, operational excellence and sustainable energy development across the region.

Its members include national and international operators, technology and service providers, and sector institutions. ARPEL supports industry collaboration and professional development through technical exchanges, mutual assistance and training tailored to industry needs.

ARPEL's strategic priorities

Operational excellence • Energy transitions
Sustainable management • Stakeholder engagement

Learn more about ARPEL

www.arpel.org/en/about-us

EN50**EN60****EN61****EN62****EN70****EN99**