

EN60 ^{v3.20}

Cyber Risk Assessment

New and existing industrial systems
in the energy, oil & gas sector

An EN program initiative with ARPEL

ENERGY
OIL
GAS

Context. Consequences. Decisions.

Assess risk. Make informed decisions.

Apply the WBS methodology to assess industrial cyber risks, define the system under consideration and guide risk reduction in accordance with ISA/IEC 62443.

IDENTIFY

Define systems, assets and potential consequences.

ASSESS

Evaluate vulnerabilities and realistic risk scenarios.

RECOMMEND

Develop actions aligned with risk tolerance.

ISA/IEC 62443 | NERC/CIP | C2M2

EN50
EN60
EN61
EN62
EN70
EN99

Learning objectives

At the end of the EN60 course, you will be able to:

- 01** Understand the requirements of the ISA/IEC-62443 series of standards for the Cyber Risk Assessment (ASSESSMENT) phase.
- 02** Understand the requirements of popular regulations, such as, NERC/CIP, C2M2 and others.
- 03** Develop clarity about the deliverables to be produced at the end of each of the activities.
- 04** Develop all activities successfully, making optimal use of resources and time.
- 05** Correctly identify the system under consideration, whether these systems are existing or future.
- 06** Evaluate the organization's capabilities, its good practices, and identify potential opportunities for improvement.
- 07** Identify all potential consequences to be avoided and mitigated during decision-making.
- 08** Develop reasonable and appropriate vulnerability studies for accurate risk assessment.
- 09** Participate in and/or lead a detailed cyber risk assessment based on realistic consequences.
- 10** Make good decisions consistently with other industrial risk disciplines.
- 11** Develop a clear and effective action plan for risk reduction according to the company's risk matrix and risk tolerance.

Build the basis for effective risk reduction

EN50

EN60

EN61

EN62

EN70

EN99

Detailed technical scope

Assessment foundations and system definition / 01-09

- 01** Interpret the requirements of the WBS methodology to meet the requirements of the standards and make good decisions.
- 02** Understand the necessary activities to be carried out during the Cyber Risk Assessment (ASSESSMENT) phase.
- 03** Understand the inputs needed before starting each activity.
- 04** Understand the outputs to be produced because of each activity.
- 05** Establish and know the expectations, roles and responsibilities of each participant.
- 06** Estimate the time, duration, and resources required to complete the risk assessment.
- 07** Analyze, understand, and model zones and conduits.
- 08** Accurately identify the complete list of cyber-assets that make up the system under consideration, including Hardware, Virtual Machines and Software.
- 09** Employ passive, non-intrusive methods and techniques to identify cyber-assets and develop vulnerability studies in existing 7x24 or future systems.

WBS methodology • Systems • Zones and conduits

EN50

EN60

EN61

EN62

EN70

EN99

Detailed technical scope

Vulnerabilities, consequences and recommendations / 10-18

- 10** Identify public vulnerabilities (existing in global databases), private vulnerabilities (specific to the particular installation of the SuC), and zero-day vulnerabilities.
- 11** Classify vulnerabilities such as administrative, cyber, and physical.
- 12** Model the Industrial Cybersecurity risk matrix to be used to calculate Industrial Cyber Risk in a repeatable and auditable way.
- 13** Develop an organizational maturity assessment against global best practices, including ISA/IEC-62443 and regulations for energy, oil, and gas.
- 14** Develop security breach assessments against global best practices, including ISA/IEC-62443 and others.
- 15** Model the company's physical assets and identify all potential consequences through hazard identification and criticality analysis.
- 16** Participate in and/or conduct a detailed cyber risk assessment according to the ISA/IEC-62443-3-2 risk assessment methodology.
- 17** Produce the necessary recommendations to reach the tolerable risk for the organization.
- 18** Produce the necessary reports with the necessary and sufficient recommendations at the level of processes, technology, systems, policies, procedures, and best practices.

Course contents

Complete syllabus published on the EN60 course page

- 01 Introduction to industrial risk assessment.**
 - ISA/IEC-62443 standards
 - Popular regulations (NIST, NERC, C2M2,...)
- 02 Necessary objectives, concepts and definitions.**
- 03 Activities to be developed to correctly evaluate risks.**
 - Necessary inputs and outputs to be produced with each activity.
- 04 Identification and evaluation of the government layer (GOV).**
 - Strengths and weaknesses,
 - Potential opportunities for improvement.
- 05 Identification and evaluation of the system under consideration (SUC).**
 - Zones and Ducts,
 - Vulnerabilities,
- 06 Identification and evaluation of industrial processes (AUC).**
 - Criticality or high-level risk assessment,
 - Identification of potential consequences.
- 07 Detailed risk assessment, results to be produced.**
 - Operational (industrial) risk matrices,
 - Determination of objective security levels (SLT)
 - Preparation of risk scenarios,
 - Risk assessment and mitigation decision-making.
 - Evaluation of the effectiveness and efficiency of existing countermeasures.
 - Determination of compensatory countermeasures.
 - Optimal segmentation of the SUC.
- 08 Preparation of necessary reports and reports.**

Plan your participation

Requirements, learning resources and recognition

Requirements

It is recommended to have taken and passed the EN50 course.

Deliverables

- Course Material.
- Access to Educational Campus.
- Complementary material in digital form is available on the educational campus.

Course essentials

Version 3.20

1.6 CRE credits

5 lessons / 1 quiz

Digital course materials

Certificates

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

Cyber Risk Assessment Practitioner in New and Existing Industrial Systems

CRE credits: 1.6

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 Cyber Risk Assessment in New and Existing Industrial Systems

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 EN60 training course and has completed the final evaluation test with a good grade, verifying that said participant has assimilated the new knowledge.



Learn. Build. Advance.

Course details and availability:

[wisecourses.com/courses/en60en320/](https://www.wisecourses.com/courses/en60en320/)

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