

EN62 ^{v3.20}

Monitoring and Maintenance of Industrial Cybersecurity

Operations, security levels, zones and conduits

An EN program initiative with ARPEL

**ENERGY****OIL****GAS**

Monitor. Respond. Maintain.

Sustain security throughout operations

Maintain security levels through monitoring, change management, preventive maintenance, backup and recovery, and periodic assessments in energy, oil and gas systems.

MONITOR

Manage events and alerts with industrial context.

RESPOND

Coordinate response plans and security information.

MAINTAIN

Manage change, updates, recovery and ongoing risk.

ISA/IEC 62443 | ISA 18.2 | ISA 95

EN50

EN60

EN61

EN62

EN70

EN99

Sustain security in daily operations

Monitoring and maintenance for industrial systems

Develop all the necessary tools to implement the Monitoring and Maintenance of the Security Levels defined for each of the Zones and Ducts of the Systems Under Consideration (SuC) for a safe and smooth operation.

Security levels tend to degrade over time and at the same time, changes in plants and systems become necessary, new vulnerabilities are discovered and new threats appear. Maintaining surveillance, updating systems, carrying out adequate change management, monitoring the security of assets, responding to events and alerts assertively, are some of the activities to be carried out in this phase.

This course is developed 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.

Course essentials

Version 3.20

16 instructor-led hours

1.6 CRE credits

EN61 prerequisite

8 lessons / 1 quiz



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.

Teachers specialized in related careers.

EN50
EN60
EN61
EN62
EN70
EN99

Learning objectives

At the end of the EN62 course, you will be able to:

- 01** Design and implement strategies and systems for monitoring, detection, alerts, and response plan management assertively without false positives.
- 02** Integrate with corporate SOC-OT applications for bidirectional exchange of security information.
- 03** Design and implement industrial systems update strategies appropriately.
- 04** Design and implement change management processes in industrial systems, maintaining security levels without degrading.
- 05** Plan preventive maintenance activities on industrial systems for the safety of zones and conduits.
- 06** Design and manage backup plans and systems and recovery plans.
- 07** Develop periodic safety audits on industrial systems in zones and conduits.



Detailed syllabus

Monitoring, response and risk management / 01-07

01 Notifications and security alerts

Configuration of notifications and security alerts based on the AMRS technical specification from the previous IMPLEMENT phase.

02 Alert prioritization

Management of security alerts according to criticality and priority of zones, and conduits.

03 Contextual response procedures

Preparation and implementation of procedural instructions to respond to each of the security alerts with context information.

04 Process alarm integration

Integration with industrial process alarm systems, according to ISA 18.2 standard.

05 Corporate systems integration

Integration with corporate systems to develop and implement security strategies based on external events, including news, updates, changes in security policies and others.

06 Engineering changes

Risk assessment of engineering changes, requests and internal needs on existing systems, verification of objective security levels (SL-T).

07 Periodic risk evaluation

Periodic and scheduled evaluation of Industrial Cyber Risks in Areas and Ducts according to the security level (SL-T/A).

Detailed syllabus

Maintenance, integration and periodic reviews / 08-14

08 Risk profiles and threats

Maintenance and updating of the risk profile and the general catalog of threats and threat actions.

09 Vulnerability knowledge

Updating and knowledge bases of Technological Vulnerabilities (CVEs).

10 Redundant architecture

Configuration and testing in the operation of the redundant architecture of the ZCM system.

11 Historical behavior

Analysis of historical behavior of Zones and Conduits and preparation of reports.

12 Backup and recovery

Design and technical specification for the implementation and preparation of the backup management plan and recovery procedures for existing industrial systems. (The ZCM system is not a Backup & Restore solution, requires third-party applications, and takes advantage of the abilities of each of the industrial systems)

13 APIs and workflows

Integration with third-party systems using API (Applications Programming Interface) and automation of workflows, complying with the requirements of the ISA 95 standard.

14 Periodic reviews

Development of periodic authorship on:

- Existing industrial systems for verification of the operation of countermeasures and mitigation actions.
- Security gaps in industrial operations.
- Maturity Models in Industrial Operations.

Plan your participation

Prerequisites, certificates and recognition

Requirements

Have taken and passed the EN61 course.

Recommended background

Recommended knowledge includes ISA/IEC-62443, ISO-27000, ISA/IEC-61511 and functional safety, industrial process alarm management (ISA 18.2), industrial systems information management (ISA 95), NIST and NERC, corporate project and cultural change management, and other industrial risk disciplines such as worker and environmental safety.

Deliverables

Participants receive digital materials through the educational platform:

- Access to course lessons online.
- Various documents, videos and complementary material for deeper study.
- Access to the educational campus to download complementary information and software.

Certificates

A first certificate of knowledge is issued upon completion of the EN62 course.

Practitioner of Safe Operation and Preventive and Corrective Maintenance of Cybersecurity in 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 Safe Operation and Preventive and Corrective Maintenance of Cybersecurity in 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 EN62 training course and has taken the final evaluation test with a good grade, verifying that said participant has assimilated the new knowledge.

**Learn. Build. Advance.**wisecourses.com/courses/en62en320/**EN50****EN60****EN61****EN62****EN70****EN99**

Learning experience

Delivery formats, practical exercises and ongoing support

Modality and schedules

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

Duration: 16 hours with the teacher, including the final evaluation.

Course highlights

- 01** Available in Spanish and Portuguese languages, both the voiceover and the complete course material. The course material will be available to consult on the Educational Campus (asynchronous) both in Spanish and in Portuguese and English.
- 02** Includes practical online exercises. Each attendee accesses remotely from the campus a dedicated computer networked with the rest of the course computers to perform several practical Cybersecurity exercises on networks with specific software and applications.
- 03** Abundant complementary reading material.
- 04** Virtual group study meetings until taking the exam, even after the course has ended.
- 05** The assistant can enter the Campus to consult the course material for a period of 1 year.
- 06** Coaching, chat and blog 7×24 for a period of 1 year, assisting in the implementation of the practical knowledge acquired in your organization.

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