

EN70 ^{v3.20}

Security By Design

For control systems engineers and service providers
in energy, oil & gas

An EN program initiative with ARPEL

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

Specify. Design. Verify.

Build security into control system design

Translate risk assessment results into cybersecurity requirements, system architectures and component selections for new and existing industrial systems.

SPECIFY

Develop cybersecurity requirements specifications.

DESIGN

Address system and component security requirements.

VERIFY

Determine security levels for products, zones and conduits.

ISA/IEC 62443-3-3 | ISA/IEC 62443-4-2

EN50

EN60

EN61

EN62

EN70

EN99

Security at the system level

From risk assessment to engineering requirements

The EN70 training course main objective is to explain security by design at the SuC Level. Starting from the Security by Design levels and after that getting into Security By Design at System Level. Every engineer who oversees the design of control systems should learn how to comply with security requirements as well as functional requirements. Understand and/or develop detailed cybersecurity requirement specifications.

Existing Systems. Introduce changes into zones and conduits to meet security requirements. Understand the results of the detailed risk assessment at the plant to create meaningful changes in the zones and conduits that meet the requirements.

New Systems. Design the control system to meet security requirements. Select components, assemble, install, configure hardware and software components to meet security requirements.

Course essentials

Version 3.20

1.6 CRE credits

EN60 recommended

8 lessons / 1 quiz

Digital course materials



Engineering focus

Control systems engineers and service providers must address both functional requirements and cybersecurity requirements. EN70 connects detailed risk assessment, specifications, system design and component selection.

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

Learning objectives

At the end of the EN70 course, you will be able to:

- 01** Interpret the results of the detailed risk assessment.
- 02** Perform a consistent conceptual design to influence the design of the plant.
- 03** Perform a detailed design in compliance with the ISA/IEC-62443-3-3.
- 04** Determine SL-A and SL-C of the current design of a particular system and components.
- 05** Understand all the Security Requirements (SR) and Requirements Enhancements (RE) within the ISA/IEC-62443-3-3.
- 06** How to choose security controls and harmonize with popular regulations.
- 07** Create Cybersecurity Requirements Specifications (CSRS).



Design security into new and existing systems

EN50

EN60

EN61

EN62

EN70

EN99

Detailed syllabus

Concepts, definitions and system design

01 Concepts and Definitions

- What is Security by Design.
 - Levels of Security by Design.
- Explain security by design for system security and the relationship with the ISA/IEC-62443-3-3 and ISA/IEC-62443-4-2.
- ISA/IEC-62443-2-4 Requirements for Service Providers.
- Zones and Conduits Model. Zone, Conduit, Networks, etc.
- Security Levels. Types of Security Levels.
- Existing vs. New Systems.
- Engineering By Design.
- Foundational Requirements.
 - Base Requirements.
 - Security Requirements.
 - Requirements Enhance.
- Essential Functions.
- Compensating Countermeasures.
- Harmonize with Popular Regulations.
- ISA/IEC-62443-3-3 Objectives.
- Types of Devices (Or Components).
- ISA/IEC-62443-4-2 Objectives.
- Product Certification.

Detailed syllabus

Foundational requirements and applied design

02 Foundational Requirements.

FR1 = Access Control (IAC)

FR2 = Usage Control (UC)

FR3 = System Integrity (SI)

FR4 = Data Confidentiality (DC)

FR5 = Restrict Data Flow (RDF)

FR6 = Timely Event Response (TRE)

FR7 = Resource Availability (RA)

03 ISA Secure. Product Certification.

04 Determining the SLC of a product

05 Determining the SLA of a zone or conduit

06 Case Study: Boiler Control

Plan your participation

Requirements, learning resources and recognition

Requirements

It is recommended to have taken and passed the EN60 course.

Recommended background

Industrial Automation and Control Systems; 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; other industrial risk disciplines, including worker and environmental safety.

Deliverables

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

Certificates

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

Detailed Design of Security 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 the Design of Security 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 EN70 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/en70en320/

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