2170

DESIGN · VERSION 3.20

Security by Design for Control Systems

Engineers and service providers in manufacturing

From requirements to design

Zones and conduits · Components · CSRS

ISA/IEC 62443

Systems and components

1.6 CRE

Knowledge credits

3 languages

Spanish · Portuguese · English

Understand security by design at the system under consideration (SUC) level, from security levels to detailed design. Develop control systems that meet cybersecurity and functional requirements, and prepare detailed cybersecurity requirements specifications.

01 / COMPETENCIES

Learning outcomes

Upon completion of the course, you will be able to:

- Interpret the results of the detailed risk assessment.
- Develop a consistent conceptual design to influence plant design.
- Develop a detailed design in accordance with ISA/IEC 62443-3-3.
- Determine SL-A and SL-C for the current design of a system and specific components.
- Understand the security requirements (SR) and requirement enhancements (RE) of ISA/IEC 62443-3-3.
- Select security controls and harmonize them with applicable regulations.
- Create cybersecurity requirements specifications (CSRS).

Existing systems

Implement changes to zones and conduits to meet security requirements. Interpret the results of the plant's detailed risk assessment to introduce meaningful changes consistent with those requirements.

New systems

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

02 / COURSE CONTENT

Foundations of secure design

- What is security by design? Security levels by design.
- System-level security by design and its relationship to ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2.
- ISA/IEC 62443-2-4 requirements for service providers.
- The zones and conduits model: zones, conduits, networks, and their relationships.
- Security levels and types of security levels.
- Existing systems versus new systems.
- Engineering by design.
- Foundational requirements: basic requirements, security requirements, and requirement enhancements.
- Essential functions.
- Compensating countermeasures.
- Harmonization with applicable regulations.
- Objectives of ISA/IEC 62443-3-3.
- Types of devices or components.
- Objectives of ISA/IEC 62443-4-2.
- Product certification.

03 / COURSE CONTENT

Foundational requirements

CODE	REQUIREMENT	ACRONYM
FR1	Identification and authentication control	IAC
FR2	Use control	UC
FR3	System integrity	SI
FR4	Data confidentiality	DC
FR5	Restricted data flow	RDF
FR6	Timely response to events	TRE
FR7	Resource availability	RA

Certification and security levels

- ISASecure: product certification.
- Determine a product's security level capability (SL-C).
- Determine the achieved security level (SL-A) of a zone or conduit.

Case study: boiler control

Apply the course content to an industrial control system.

04 / PREPARATION

Prerequisites and materials

Recommended preparation: 2160 or EN60

Completion of either course with a passing result is recommended.

Recommended knowledge

- Industrial automation and control systems.
- ISA/IEC 62443 international industrial cybersecurity standards.
- Corporate cybersecurity or information security in the ISO 27000 family.
- Industrial risk management, ISA/IEC 61511, and functional safety.
- ISA 18.2 industrial process alarm management.
- ISA 95 industrial systems information management.
- National regulations or standards such as NIST, NERC, and other applicable requirements.
- Experience in corporate project management and cultural change management.
- Other industrial risk management standards, such as worker safety and environmental safety.

Deliverables

- Course materials.
- Access to the educational campus.
- Supplementary digital materials available on the educational campus.

05 / PROFESSIONAL DEVELOPMENT

Knowledge and experience

Two stages of recognition linked to training and practical application.

01 / KNOWLEDGE CERTIFICATE

Detailed Security Design for New and Existing Industrial Systems

Issued upon completion of the course. Provides 1.6 CRE credits. The certification examination is taken in class at the end of the course and is available in Spanish, Portuguese, and English.

02 / EXPERIENCE CERTIFICATE

Expert in Security Design for New and Existing Industrial Systems

Issued after practical implementation in real projects. CRE credits are cumulative and depend on the duration of the activities performed by the professional.

Digital badge

Participants who meet the course requirements and pass the final examination with a satisfactory grade receive a digital badge. It recognizes attendance at course 2170 and successful completion of the assessment, verifying acquisition of the new knowledge.

Learn. Build. Advance.

Explore the course and training options:

wisecourses.com/courses/2170-sp-320/

Sources: official 2170 SP 3.20 course page and datasheet DS.TR.2170.S.320 (October 2025). Prerequisites and certificate titles follow the course page, translated into English. Editorial edition: October 2026.