2161

IMPLEMENTATION · VERSION 3.20

Industrial Cybersecurity Design and Implementation

New and existing systems in manufacturing industries

WBS Methodology

Zones and conduits · CSRS · Risk mitigation

ISA/IEC 62443

Design and implementation

1.6 CRE

Knowledge credits

3 languages

Spanish · Portuguese · English

Turn risk assessment results into effective protection: design and implement the actions needed to mitigate intolerable risks, with minimal interference in plant activities and in alignment with other industrial risk disciplines.

01 / COMPETENCIES

Learning outcomes

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

- Understand and use the results of the cybersecurity risk assessment.
- Incorporate the recommendations obtained during the assessment phase into the design of existing systems.
- Define the optimal architecture and design the integration of changes required by the detailed risk analysis.
- Visualize, monitor, and manage cybersecurity progress for each zone and conduit as recommendations are implemented.
- Visualize how the achieved security level (SLA) approaches the target security level (SLT).
- Develop industrial cybersecurity requirements specifications (CSRS) for zones and conduits.
- Prioritize the implementation of security recommendations according to their contribution to risk reduction, cost, effort, and security level capability, among other factors.
- Create policies to monitor and oversee incidents associated with remaining risks, even when the system operates below the risk tolerance threshold.
- Define and configure appropriate cybersecurity policies for each zone and conduit for the subsequent monitoring and maintenance phase.

From assessment to secure design

Developing CSRS helps shape the design of industrial systems and the plant so that cyber risks are mitigated from startup. For operating systems, implementing compensating protections aims to reduce risks with minimal interference in plant activities.

02 / COURSE CONTENT

Design, implement, and protect

01 **Zone and conduit design**

Design to meet the security recommendations from the previous phase, ensuring efficient and effective risk mitigation.

02 **Standards, regulations, and internal requirements**

Incorporate requirements from the ISA/IEC 62443 series; applicable national standards, laws, and regulations (NIST, C2M2, FDA, and others); and develop internal standards and rules.

03 **Industrial cybersecurity specifications**

Design and develop CSRS for zones and conduits in systems at the engineering stage, meeting the foundational requirements (FR), system requirements (SR), and requirement enhancements (RE) of ISA/IEC 62443-3-3.

04 **Alerts and incident response**

Rationalize alerts to maintain active oversight of security events requiring attention while avoiding false positives. Develop a plan for timely incident response without delays.

05 **Countermeasure implementation**

Implement security in zones and conduits, prioritizing countermeasures by their effectiveness and efficiency in mitigating residual cyber risk. Maintain consistency across procedural, technological, and physical countermeasures.

06 **Risk mitigation management**

Manage countermeasure implementation for effective, reliable, and credible mitigation of industrial cyber risk until the organization's tolerable risk level is reached.

07 **Detection, monitoring, and alerts (ARMS)**

Design specifications to rationalize alerts and define event response plans while minimizing false positives. Apply these to systems with both unmitigated and mitigated risk. This specification is an input to the operation and maintenance phase.

03 / PREPARATION

Audience, prerequisites, and materials

Who should attend?

- Professionals involved in the design or implementation of industrial systems, industrial networks, monitoring, industrial cybersecurity, detection, access control, segmentation, and other aspects of industrial systems security.
- IT security managers, systems integrators, industrial control system suppliers, plant engineers, production and operations management, industrial safety personnel, safety instrumented systems specialists, and maintenance personnel at senior and middle management levels.

Recommended preparation: course 2160

Completing and passing course 2160 is recommended.

Recommended knowledge

- ISA/IEC 62443 international industrial cybersecurity standards.
- Corporate cybersecurity or information security standards in the ISO 27000 family.
- Industrial risk management standards, such as ISA/IEC 61511, and functional safety.
- National regulations or standards applicable to the sector.
- Experience in corporate project management and cultural change management.
- Other industrial risk management standards, such as worker safety and environmental safety.

Deliverables and digital access

Participants receive digital materials through the learning platform:

- Access to the online lessons of course 2161.
- Documents, videos, and supplementary materials for further study.
- Access to the educational campus to download supplementary information and software.

04 / PROFESSIONAL DEVELOPMENT

Knowledge and experience

Two stages of recognition linked to training and practical application.

01 / KNOWLEDGE CERTIFICATE

Practitioner in Cybersecurity Design and Implementation for Industrial Systems

Awarded after completing the course and passing the assessment. Provides 1.6 CRE credits. The examination is taken in class at the end of the course and is available in Spanish, Portuguese, and English.

02 / EXPERIENCE CERTIFICATE

Expert in Cybersecurity Design and Implementation for Industrial Systems

Issued after demonstrating experience through active participation in real projects that use the methodology. CRE credits are cumulative and depend on the duration of the activities performed.

Digital badge and supervised experience

Participants who meet the course requirements and successfully pass the final examination receive a digital badge recognizing attendance and the knowledge acquired.

For experience recognition, participants must demonstrate practical involvement and accumulate the minimum required hours in the corresponding activities under the supervision of a certified project leader.

Learn. Build. Advance.

Explore the course and training options:

wisecourses.com/courses/2161-sp-3v20/

Sources: official 2161 SP 3.20 course page and datasheet DS.TR.2161.S.320 (October 2025). Sector focus, prerequisites, and certifications follow the course page. Editorial edition: October 2026.