

2160

ASSESSMENT · VERSION 3.20

Industrial Cybersecurity Risk Assessment

New and existing systems in manufacturing industries



WBS Methodology

Zones and conduits · Consequences · Mitigation

ISA/IEC 62443

Risk assessment

1.6 CRE

Knowledge credits

3 languages

Spanish · Portuguese · English

A practical methodology for industrial cybersecurity risk assessment supports consistent decisions and the development of resilient infrastructure. The course applies WBS to the risk assessment phase of the lifecycle for both existing and new systems.

01 / COMPETENCIES

Learning outcomes

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

- Understand and interpret the requirements of the ISA/IEC 62443 series of standards for the cybersecurity risk assessment phase.
- Clearly define the deliverables to be produced upon completion of each activity.
- Successfully perform assessment activities, optimizing resources and time while focusing effort on activities that add value.
- Correctly identify the system under consideration, whether existing or planned, starting at the engineering stages.
- Assess organizational capabilities, good practices, and opportunities for improvement.
- Identify potential consequences to be avoided or mitigated during decision-making.
- Develop reasonable and appropriate vulnerability studies for an accurate risk assessment.
- Collaborate in, participate in, or lead a detailed cybersecurity risk assessment based on realistic scenarios and consequences.
- Make decisions consistent with other industrial risk disciplines.
- Develop or support a clear, effective, efficient, and sufficient action plan to reduce risks in accordance with the organization's risk matrix and risk tolerance.

First phase of the lifecycle

Comprehensive risk assessment for new or existing systems, addressing the organization, control systems, and industrial processes.

02 / COURSE CONTENT

Assessment syllabus

01 **Introduction to industrial risk assessment**

ISA/IEC 62443 standards. Common regulations and frameworks: NIST, NERC, C2M2, and others. Essential objectives, concepts, and definitions.

02 **Activities and deliverables**

Activities required to perform risk assessment correctly. Necessary inputs and outputs to be produced by each activity.

03 **Governance layer (GOV)**

Identification and assessment of strengths, weaknesses, and opportunities for improvement.

04 **System under consideration (SUC)**

System identification and assessment: zones, conduits, and vulnerabilities.

05 **Industrial processes (AUC)**

Identification and assessment of industrial processes. Criticality or high-level risk assessment and identification of potential consequences.

06 **Detailed risk assessment**

Operational and industrial risk matrices.
Determination of target security levels (SLT).
Development of risk scenarios.
Risk assessment and mitigation decisions.
Assessment of the effectiveness and efficiency of existing countermeasures.
Determination of compensating countermeasures.
Optimal segmentation of the SUC.

07 **Documentation of results**

Preparation of the required reports and documentation.

03 / APPLYING THE METHODOLOGY

Detailed technical scope

- Interpret WBS methodology requirements to comply with standards and make sound decisions.
- Understand the activities required during the cybersecurity risk assessment phase.
- Understand the inputs required before starting each activity.
- Understand the outputs to be produced as a result of each activity.
- Establish and understand each participant's expectations, roles, and responsibilities.
- Estimate the timing, durations, and resources needed to complete the risk assessment.
- Analyze, understand, and model zones and conduits.
- Accurately identify the complete inventory of cyber assets in the system under consideration, including hardware, virtual machines, and software.
- Use passive, nonintrusive methods and techniques to identify cyber assets and develop vulnerability studies for existing systems operating 24/7 or for future systems.
- Identify public vulnerabilities recorded in global databases, private vulnerabilities specific to the particular SUC installation, and zero-day vulnerabilities.
- Classify vulnerabilities as administrative, cyber, or physical.
- Model the industrial cybersecurity risk matrix to calculate risk in a repeatable and auditable manner.
- Develop an organizational maturity assessment against global best practices, including ISA/IEC 62443 and regulations for energy, oil, and gas.
- Develop security gap assessments against global best practices, including ISA/IEC 62443 and others.
- Model the company's physical assets and identify potential consequences through hazard identification and criticality analysis.
- Participate in or lead a detailed cybersecurity risk assessment using the ISA/IEC 62443-3-2 methodology.
- Produce the recommendations needed to achieve the organization's tolerable risk level.
- Produce reports with necessary and sufficient recommendations on processes, technology, systems, policies, procedures, and best practices.

04 / LEARNING EXPERIENCE

Exercises and preparation

Optional practical exercises

The course can be taken with or without exercises. Depending on the delivery format (on demand, in person, or virtual), activities may include instructor demonstrations or participant exercises with instructor guidance.

- Identify devices using automated and manual techniques and tools.
- Interpret the actual SUC configuration and model zones and conduits.
- Identify technological (CVE), procedural or administrative, and physical or mechanical vulnerabilities using specialized tools.
- Interpret the results of a HAZOP study or an industrial process risk study.
- Perform an initial or high-level risk assessment (HLRA).
- Perform a detailed risk assessment of zones and conduits (CPHA).
- Produce reports and documentation with improvement recommendations for the SUC, the plant, and the organization.

Prerequisites

There are no specific prerequisites. Knowledge or experience in some of the following areas is recommended:

- Industrial process supervision and automation; protocols such as Modbus, Profibus, EtherNet/IP, OPC, or others; experience with industrial plants and processes.
- Safety instrumented systems and functional safety; ISA84 committee standards and ISA/IEC 61511; ANSI/ISA 5.1 symbols; ISA95 industrial information and data flow management.
- ISA/IEC 62443 industrial cybersecurity (ISA99), information security and data networks; the ISO 27000 family.
- Project management (PMBOK), cultural change management, and other industrial risk disciplines, such as worker safety and environmental safety.

Included materials

Course materials, access to the educational campus, and supplementary digital materials available on the platform.

05 / PROFESSIONAL DEVELOPMENT

Knowledge and experience

Two stages of recognition linked to training and practical application.

01 / KNOWLEDGE CERTIFICATE

Practitioner in Cybersecurity Risk Assessment for New and Existing 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 Risk Assessment for New and Existing 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/2160sp320/

Sources: official 2160 SP 3.20 course page and datasheet DS.TR.2160.S.320 (October 2025). Certificate titles follow the course page, translated into English. Editorial edition: October 2026.