

2162

OPERATE AND MAINTAIN · VERSION 3.20

Secure Operation and Industrial Cybersecurity Maintenance

Monitoring and protecting zones and conduits in manufacturing



WBS Methodology

Monitoring · Change management · Maintenance

ISA/IEC 62443

Secure operation

1.6 CRE

Knowledge credits

3 languages

Spanish · Portuguese · English

Develop the tools needed to monitor and maintain the security levels defined for each zone and conduit of the system under consideration (SUC), supporting secure plant operation and sustaining protection against changes, new vulnerabilities, and threats.

01 / COMPETENCIES

Learning outcomes

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

- Support secure plant operation by designing and implementing strategies for monitoring, detection, alerts, and decisive response management while avoiding false positives.
- Integrate corporate SOC-OT applications for the bidirectional exchange of security information.
- Design and implement improvement strategies and maintain appropriate regular updates to industrial systems.
- Design and implement change management processes for industrial systems while maintaining security levels without degradation.
- Plan and perform preventive maintenance activities for industrial systems to maintain the security of zones and conduits.
- Design and manage backup and recovery plans and systems.
- Conduct periodic security audits of industrial systems within their zones and conduits.
- Conduct periodic audits to ensure compliance with international standards in accordance with corporate policies and procedures.
- Identify improvement opportunities and evaluate the performance of the organization's risk management program.

Sustaining security over time

Security levels can degrade over time. Changes in plants and systems, new vulnerabilities, and emerging threats require vigilance, updates, and appropriate change management. The course focuses on manufacturing, harmonizing ISA/IEC 62443 with applicable frameworks and regulations such as NIST and C2M2.

02 / COURSE CONTENT

Monitoring, response, and changes

01 **Notifications and alerts**

Configure security notifications and alerts based on the AMRS technical specification from the preceding implementation phase.

02 **Alert management**

Manage alerts according to criticality, priority, areas, zones, and conduits.

03 **Response with contextual information**

Develop and implement procedural instructions to respond to each security event or alert using contextual information.

04 **Integration with process alarms**

Integrate with industrial process alarm systems in accordance with ISA 18.2.

05 **Integration with corporate systems**

Develop and implement security strategies based on external events, including news, updates, security policy changes, and other developments.

06 **Engineering change management**

Assess the risks of engineering changes, requests, and internal needs affecting existing systems. Verify target security levels (SL-T).

07 **Periodic risk reassessment**

Perform periodic, scheduled industrial cybersecurity risk assessments for zones and conduits according to target and achieved security levels (SL-T/A).

03 / COURSE CONTENT

Maintain, recover, and audit

08 Risk profile and threats

Maintain and update the risk profile and the general catalog of threats and threat actions.

09 Vulnerability knowledge

Update knowledge bases of technological vulnerabilities (CVE).

10 RMS redundant architecture

Configure and test the operation of the RMS system's redundant architecture.

11 Historical behavior

Analyze the historical behavior of zones and conduits and prepare reports and documentation.

12 Backup and recovery

Develop the design and technical specification for implementing the backup management plan and recovery procedures for existing industrial systems. RMS is not a backup and recovery solution: third-party applications and the capabilities of each industrial system are required.

13 Integration and automation

Integrate with third-party systems through application programming interfaces (API) and automate workflows in compliance with ISA 95 requirements.

14 Periodic audits

Verify the performance of countermeasures and mitigation actions in existing systems. Assess security gaps and maturity models in industrial operations.

04 / PREPARATION

Audience, prerequisites, and materials

Who should attend?

- Personnel in beverages, water, steel, food, pharmaceuticals, and other industries who are involved in protecting critical infrastructure and control systems.
- 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 or middle management levels.
- Instructors specializing in related disciplines.

Prerequisite: passing course 2161

Completion of course 2161 and a passing result are required.

Recommended knowledge

- ISA/IEC 62443 industrial cybersecurity and information security standards in the ISO 27000 family.
- Industrial risk management, ISA/IEC 61511, and functional safety.
- ISA 18.2 industrial process alarm management and ISA 95 industrial systems information management.
- National regulations or standards, such as NIST, NERC, and other applicable requirements.
- Corporate project management and cultural change management.
- Other industrial risk disciplines, 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 2162.
- Documents, videos, and supplementary materials for further study.
- Access to the educational campus to download supplementary information and software.

05 / PROFESSIONAL DEVELOPMENT

Knowledge and experience

Two stages of recognition linked to training and practical application.

01 / KNOWLEDGE CERTIFICATE

Practitioner in Secure Operation and Preventive and Corrective Cybersecurity Maintenance 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 Secure Operation and Preventive and Corrective Cybersecurity Maintenance 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/2162sp320/

Sources: official 2162 SP 3.20 course page and datasheet DS.TR.2162.S.320 (October 2025). Certificate titles follow the course page, translated into English. Editorial edition: October 2026.