

EN99 ^{v3.20}

Industrial Cybersecurity Alert Management

Applying ISA/IEC 62443 to security events and alerts

An EN program initiative with ARPEL

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

Rationalize. Prioritize. Respond.

Make security alerts actionable

Design and manage industrial cybersecurity alerts in the context of plant risk, process conditions and predefined response actions.

RATIONALIZE

Define alert philosophy, justification and classification.

PRIORITIZE

Relate alerts to risk and the industrial process.

RESPOND

Prepare specific actions and evaluate performance.

ISA/IEC 62443 | ANSI/ISA-18.2-2016

EN50

EN60

EN61

EN62

EN70

EN99

Alerts in the industrial context

Connect security events, plant risk and response actions

Cybersecurity requires monitoring, detecting, monitoring, and alerting based on many cybersecurity events that occur in control systems.

This activity, necessary to accompany the safe operation of the plant, requires a series of fundamental activities that must be correctly executed prior to its implementation.

The generation of security alerts is followed by assertive, immediate management of cyber incidents with no tolerance for delays. Alerts must be classified and categorized according to a realistic risk possibility and in context with the industrial process, without false positives. Responses must be specific and quick to ensure preventive, effective, and efficient avoidance of potential consequences.

The generation of cybersecurity alerts (cyber incidents) may or may not have a correlation with process disturbances and alarms and finally the occurrence of potential consequences. Developing the ability to anticipate physical facts about the plant requires specific knowledge that can only be achieved with specific knowledge of the plant.

It is crucial to design and implement surveillance, alert, and incident management systems – without false alerts – through a security alert rationalization process, based on specific knowledge and the result of the detailed cyber risk assessment.

Additionally, when monitoring, alerting, and responding to cybersecurity incidents, it is significantly different to do so on a system that has all its risks mitigated, than on a system that does not.



EN50

EN60

EN61

EN62

EN70

EN99

Course objectives and benefits

The security alert management lifecycle

The objective of the course is to know the main activities and requirements of the Security Alert Management Life Cycle in accordance with ISA/IEC-62443 and ANSI/ISA-18.2-2016, for the development, design, installation, and administration of a Cybersecurity Alert System in industrial processes.

To meet this objective, the concepts, models and conceptualization for the handling and management of alerts will be presented, and the application of these criteria for the development of the alert philosophy, alert rationalization, basic alert design, advanced alert techniques, HMI design for alerts, monitoring evaluation, detection, and response actions.

Participants will learn the activities of the alert management lifecycle with reference to the ISA/IEC-62443 and ISA/18.2 standard and how to address common problems of security alert and process alarm management systems. Key benefits of attending this course include:

- 01** Learn best practices to improve alert system performance.
- 02** Learning methods to solve common alert management problems.
- 03** Learn about best practices for effective and successful implementation of the alert management system.
- 04** Avoid generating false security alerts that lead to no action or distractions.
- 05** You design responses to security alerts before they occur with fast and accurate responses.
- 06** Learn the metrics to measure success in alert management and continuous improvement.

Learning outcomes

At the end of the EN99 course, participants will be able to:

- 01** Develop an alert management philosophy.
- 02** Identify alerts.
- 03** Streamline alerts, including classification and prioritization.
- 04** Design basic alerts, their monitoring, detection, and notification.
- 05** Determine when advanced warning techniques should be used.
- 06** Document alerts for operations.
- 07** Design reports monitoring and evaluating the performance of the alert system.
- 08** Manage changes to alert systems.

Who is it aimed at?

- Engineering personnel who perform specification, maintenance or updating of process alarm systems.
- Industrial cybersecurity personnel who carry out specification, maintenance or updating of cybersecurity alert systems.
- Process engineering, control and operation personnel of industrial process plants.
- Corporate Cybersecurity and/or Industrial Information Security Personnel.

Detailed syllabus

Foundations, philosophy and rationalization / 01-03

01 Introduction.

- Vision over time of the Design of an Alert System.
- History of Accidents referred to Alert Management.
- Importance of Alert Management.
- Principles, Guides, Standards and Best Good Practices.
- Management of an Alert System based on ISA/IEC-62443 and ISA/18.2-2016.

02 Philosophy and Alert Identification.

03 Rationalization of alerts.

- Preparation of alert rationalization.
- Justification of the alerts.
- Alert prioritization.
- Alert classification.

Detailed syllabus

Design, implementation and operation / 04-06

04 Alarm design.

- Alert status.
- Types of alerts.
- Configuration and Monitoring.
- Alert times and messages.

05 Implementation of the alert system.

- HMI design.
- Alert display.
- Existing solutions for alert management.
- Success stories of alert systems.

06 Considerations for operation and maintenance of the alert system.

Plan your participation

Formats, requirements, certificates and recognition

Course essentials

16 total hours | 1.6 CRE credits

In person and/or virtual

Requirements

It has no specific requirements.

Recommended knowledge includes industrial process alarm management (ISA/18.2), ISA/IEC-62443, ISO-27000, ISA/IEC-61511 and functional safety, national regulations and standards such as NIST and NERC, corporate project and cultural change management, and 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.

Practitioner in design, implementation, safe operation and maintenance of the security alert and incident response system

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 design, implementation, safe operation and maintenance of the security alert and incident response system

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 EN99 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.

[wisecourses.com/courses/en99en320/](https://www.wisecourses.com/courses/en99en320/)

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