

2199

ALERT MANAGEMENT · VERSION 3.20

Industrial cybersecurity alert management

Applying ISA/IEC 62443 to industrial processes



Alerts in their industrial context

Rationalization · Prioritization · Response

ISA/IEC 62443

Industrial cybersecurity

ISA 18.2

Alarm management

Digital badge

Subject to final assessment

Monitoring, detecting, observing, and alerting on cybersecurity events in control systems requires preparatory activities to be properly performed. Context-based alert management supports secure plant operation and enables specific, rapid, and effective responses to be prepared.

01 / APPROACH

From event to response

Industrial context and consequences

Security alerts must be followed by decisive, immediate cyber incident management, with no tolerance for delays. Alerts must be classified and categorized based on a realistic assessment of risk and the context of the industrial process, without false positives. Responses must be specific and rapid to prevent potential consequences effectively and efficiently.

Correlation with the process

Cybersecurity alerts may or may not correlate with process disturbances and alarms or with the occurrence of consequences. Anticipating physical effects on the plant requires knowledge specific to the facility.

Alert rationalization

It is crucial to design and implement monitoring, alerting, and incident management systems without false alerts through a rationalization process based on plant-specific knowledge and the results of a detailed cyber risk assessment.

Mitigated and unmitigated risks

Monitoring, alerting, and responding to incidents in a system where all risks have been mitigated is significantly different from doing so in a system that still has unmitigated risks.

02 / LEARNING

Managing the entire lifecycle

Course objective

Understand the main activities and requirements of the security alert management lifecycle, in accordance with ISA/IEC 62443 and ANSI/ISA-18.2-2016, to develop, design, install, and administer a cybersecurity alert system for industrial processes.

The course presents alert management concepts, models, and criteria, applied to developing an alert philosophy, rationalization, basic design, advanced techniques, human-machine interface (HMI) design for alerts, and the evaluation of monitoring, detection, and response actions.

Participants will learn lifecycle activities with reference to ISA/IEC 62443 and ISA 18.2, and how to address common problems in security alert and process alarm systems.

Course benefits

- Learn best practices to improve alert system performance.
- Learn methods for resolving common alert management problems.
- Learn best practices for effective and successful implementation of an alert management system.
- Avoid false security alerts that do not lead to action or that cause distractions.
- Design responses to alerts before they occur, with rapid and precise actions.
- Learn metrics to measure alert management success and support continual improvement.

03 / OUTCOMES

From philosophy to improvement

Upon completing course 2199, participants will be able to:

- 01 Philosophy**
Develop an alert management philosophy.
- 02 Identification**
Identify alerts.
- 03 Rationalization**
Rationalize alerts, including their classification and prioritization.
- 04 Basic design**
Design basic alerts, including monitoring, detection, and notification.
- 05 Advanced techniques**
Determine when advanced alerting techniques should be used.
- 06 Documentation**
Document alerts for operations.
- 07 Performance evaluation**
Design reports to monitor and evaluate alert system performance.
- 08 Management of change**
Manage changes to alert systems.

04 / PREPARATION

Requirements and digital badge

No specific prerequisites

Recommended knowledge

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

Digital badge recognition

Participants who meet the course requirements and pass the final exam with a good grade will receive a digital badge. It recognizes attendance at course 2199 and successful completion of the final assessment, confirming that the new knowledge has been adequately understood.



Learn. Build. Advance.

Information on training and programs:

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

Source: datasheet DS.TR.2199.S.320, October 2025. Editorial edition: October 2026. Content based exclusively on the supplied document.