IMPLEMENT

EN61 - Implement

Design and Implementation of Cybersecurity Recommendations in Zones and Conduits

The purpose of the EN61 course is to manage the development and incorporation of the necessary and sufficient actions to mitigate all intolerable risks identified during the risk assessment, complying with the requirements of the ISA/IEC-62443 series of standards in a manner consistent with the other disciplines of industrial risk. In addition, if necessary, comply with the requirements of popular regulations.

The proper implementation of compensatory protections, with minimal interference in plant activities, is essential for those systems that are in operation with the main objective of creating industrial infrastructures resilient to all types of threats, even the most persistent.

Elaboration of industrial cybersecurity specifications (CSRS) and influencing the design of industrial systems and the plant to ensure that industrial plants will be operated with all cyber risks mitigated from the start-up of the new system.

This course is developed with a focus on the energy, oil and gas industries. It means complying with all the requirements of the ISA/IEC-62443 series of standards, harmonizing with the typical regulations of these sectors, which are NERC, C2M2, TSA, and other popular regulations.

At the end of the course you will be able to:

- Understand and use the results of the Cyber Risk Assessment (ASSESSMENT).
- In existing systems, incorporate by design the recommendations obtained in the previous stage (ASSESSMENT).
- Define the optimal architecture, design the incorporation of necessary changes as a result of detailed risk analysis.
- Visualize, monitor, and manage cybersecurity progress for each area and pipeline as recommendations are incorporated.
- Visualize how the current security level (SLA) is approaching the target security level (SLT).
- Elaboration of Industrial Cybersecurity Specifications (CSRS) for Zones and Conduits.
- Prioritize the implementation of security recommendations based on the greatest contribution to risk reduction, cost, effort, Security Level Capability, etc..
- Even if the system operates below risk tolerance, you will be able to create policies to monitor and supervise incidents of the remaining risks.
- Define and configure the appropriate cybersecurity policies for each zone and pipeline necessary for the next stage of monitoring and maintenance (MAINTENANCE).

This course is developed with a focus on the energy, oil and gas industries. It means complying with all the requirements of the ISA/IEC-62443 series of standards, harmonizing with the typical regulations of these sectors, which are NERC, C2M2, TSA, and other popular regulations.

You will cover the following topics in the course:

- Design of Zones and Conduits to comply with the safety recommendations of the previous phase, ensuring risk mitigation with efficiency and effectiveness.
- Incorporate the requirements of standards and regulations, such as:
- ISA/IEC-62443 International Standards.
- National Standards, Laws and Regulations (NIST, NERC, C2M2, etc.)
- Developing your own rules and regulations.
- Design and development of Industrial Cyber Security Specifications (CSRS) in Zones and Ducts for systems in the engineering phase, complying with the FR, SR, and RE of the ISA/IEC-62443-3-3 standard.
- Implementation of security in Zones and Conduits, prioritizing countermeasures according to effectiveness and efficiency to mitigate residual cyber risk, maintaining consistency between:
- Procedural Countermeasures,
- Technological Countermeasures, and
- Physical Countermeasures.
- Manage the implementation of countermeasures for the effective, reliable and credible mitigation of Industrial Cyber Risk up to the Tolerable Risk by the organization.
- Design specifications for detection, monitoring and alerting systems (ARMS) for the rationalization of alerts and event response plans, minimizing false positives. This specification is the entry into the MAINTAIN (Operation and Maintenance) phase.
- For industrial systems with unmitigated risk,
- For industrial systems with risk mitigation.

Recognitions:

All participants who meet the course requirements and who 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 EN61 training course and has executed the final assessment test with a good grade, verifying that the participant has assimilated the new knowledge in a reasonable way.

Requirements:

It requires that you have taken and passed the EN60. It is recommended that the professional has knowledge of some of the following: International Cybersecurity Standards by industry consensus ISA/IEC-62443, Corporate Cybersecurity or Information Security Standards ISO-27000, Industrial Risk Management Standards such as ISA/IEC-61511, functional safety, National Regulations and/or standards such as NIST, NERC, and others; Experience in corporate project management and cultural change management, Other industrial risk management standards (worker safety, environmental safety, etc.).

At WiseCourses we are inspired by innovation in education to create training processes that are representative of the world we live in today. Create and support new systems by empowering educators and practitioners who gain the expertise.