ISA-IEC-62443 Q&As

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

Pass ISA ISA-IEC-62443 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/isa-iec-62443.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISA Official Exam Center

QUESTION 1

Security Levels (SLs) are broken down into which three types?

Available Choices (select all choices that are correct)

A. SL-1, SL-2, and SL-3

B. Target.capability, and achieved

C. Target.capability, and availability

D. Target.capacity, and achieved

Correct Answer: B

Security Levels (SLs) are a way of expressing the security performance of an industrial automation and control system (IACS) or its components. SLs are broken down into three types: target, capability, and achieved1. Target SL is the level of security performance that is required for a system or component to protect against a specific threat scenario. The target SL is determined by conducting a risk assessment that considers the likelihood and impact of potential security

incidents1.

Capability SL is the level of security performance that a system or component can provide based on its design and implementation. The capability SL is determined by evaluating the security functions and features of the system or component

against a set of security requirements1.

Achieved SL is the level of security performance that a system or component actually provides in its operational environment. The achieved SL is determined by verifying that the system or component is properly installed, configured,

maintained, and monitored1.

References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, page 3- 4.

QUESTION 2

What are the connections between security zones called?

Available Choices (select all choices that are correct)

A. Firewalls

B. Tunnels

C. Pathways

D. Conduits

Correct Answer: D

According to the ISA/IEC 62443 standard, the connections between security zones are called conduits. A conduit is defined as a logical or physical grouping of communication channels connecting two or more zones that share common security requirements. A conduit can be used to control and monitor the data flow between zones, and to apply security measures such as encryption, authentication, filtering, or logging. A conduit can also be used to isolate zones from each other in case of a security breach or incident. A conduit can be implemented using various technologies, such as firewalls, routers, switches, cables, or wireless links. However, these technologies are not synonymous with conduits, as they are only components of a conduit. A firewall, for example, can be used to create multiple conduits between different zones, or to protect a single zone from external threats. Therefore, the other options (firewalls, tunnels, and pathways) are not correct names for the connections between security zones. References: ISA/IEC 62443-3-2:2016 - Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design1 ISA/IEC 62443-3-3:2013 - Security for industrial automation and control systems - Part 3-3: System security requirements and security levels2 Zones and Conduits | Tofino Industrial Security Solution3 Key Concepts of ISA/IEC 62443: Zones and Security Levels | Dragos4

QUESTION 3

Which is an important difference between IT systems and IACS?

Available Choices (select all choices that are correct)

A. The IACS security priority is integrity.

B. The IT security priority is availability.

C. IACS cybersecurity must address safety issues.

D. Routers are not used in IACS networks.

Correct Answer: A

IT systems and IACS have different security priorities, requirements, and challenges. According to the ISA/IEC 62443 standards, the security priority for IT systems is confidentiality, which means protecting the data from unauthorized access or disclosure. The security priority for IACS is integrity, which means ensuring the accuracy and consistency of the data and the functionality of the system. A loss of integrity in an IACS can have severe consequences, such as physical damage, environmental harm, or human injury. Therefore, IACS cybersecurity must address safety issues, which are not typically considered in IT security. Safety is the ability of the system to prevent or mitigate hazardous events that can cause harm to people, property, or the environment. The ISA/IEC 62443 standards provide guidance and best practices for ensuring the safety and security of IACS, as well as the availability and reliability of the system. Availability is the ability of the system to perform its intended function when required, and reliability is the ability of the system to perform its intended function without failure. These properties are also important for IT systems, but they may have different trade-offs and implications for IACS. For example, an IACS may have stricter performance and availability requirements than an IT system, as a delay or disruption in the IACS operation can affect the industrial process and its outcomes. Additionally, an IACS may have longer equipment lifetimes and less frequent maintenance windows than an IT system, which can make patching and updating more difficult and risky. Furthermore, an IACS may use different technologies and architectures than an IT system, such as legacy devices, proprietary protocols, or specialized hardware. These factors can create compatibility and interoperability issues, as well as increase the attack surface andcomplexity of the IACS. Therefore, IT security solutions and practices may not be sufficient or suitable for IACS, and they may need to be adapted or supplemented by IACS-specific security measures. The ISA/IEC 62443 standards address these differences and provide a comprehensive framework for securing IACS throughout their lifecycle. References: 1: Security of Industrial Automation and Control Systems - ISAGCA 2: ISA/IEC 62443 Series of Standards - ISA 3: ISA/IEC 62443 Series of Standards | ISAGCA 4: Securing IACS based on ISA/IEC 62443 ?Part 1: The Big Picture

QUESTION 4

Which is the PRIMARY reason why Modbus over Ethernet is easy to manaqe in a firewall?

Available Choices (select all choices that are correct)

A. Modbus uses a single master to communicate with multiple slaves usinq simple commands.

B. Modbus is a proprietary protocol that is widely supported by vendors.

C. Modbus uses explicit source and destination IP addresses and a sinqle known TCP port.

D. Modbus has no known security vulnerabilities, so firewall rules are simple to implement.

Correct Answer: C

According to the ISA/IEC 62443-2-4 standard, a training and security awareness program should include all personnel who have access to the industrial automation and control system (IACS) or who are involved in its operation, maintenance, or management. This includes vendors and suppliers, employees, temporary staff, contractors, and visitors. The purpose of the program is to ensure that all personnel are aware of the security risks and policies related to the IACS, and that they have the necessary skills and knowledge to perform their roles in a secure manner. The program should also cover the roles and responsibilities of different personnel, the reporting procedures for security incidents, and the best practices for security hygiene. References: ISA/IEC 62443-2-4:2015 - Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers1 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Training Course2

QUESTION 5

Which of the following is an industry sector-specific standard?

Available Choices (select all choices that are correct)

A. ISA-62443 (EC 62443)

B. NIST SP800-82

C. API 1164

D. D. ISO 27001

Correct Answer: C

API 1164 is an industry sector-specific standard that provides guidance on the cybersecurity of pipeline supervisory control and data acquisition (SCADA) systems. API stands for American Petroleum Institute, which is the largest U.S. trade association for the oil and natural gas industry. API 1164 was first published in 2004 and revised in 2009 and 2021. The latest version of the standard aligns with the ISA/IEC 62443 series of standards and incorporates the concepts of security levels, zones, and conduits. API 1164 covers the security lifecycle of pipeline SCADA systems, from risk assessment and policy development to implementation and maintenance. The standard also defines roles and responsibilities, security requirements, security controls, and security assessment methods for pipeline SCADA systems. References: API 1164: Pipeline SCADA Security, Fourth Edition, September 2021 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 2.2.2, Industry Sector-Specific Standards ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Specification, Section 2.2.2, Industry Sector-Specific Standards

QUESTION 6

Which of the following is an element of monitoring and improving a CSMS?

Available Choices (select all choices that are correct)

A. Increase in staff training and security awareness

B. Restricted access to the industrial control system to an as-needed basis

C. Significant changes in identified risk round in periodic reassessments

D. Review of system logs and other key data files

Correct Answer: ACD

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist resources, a CSMS is a Cybersecurity Management System that defines the policies, procedures, and practices for managing the security of an industrial automation and control system (IACS). A CSMS should be monitored and improved continuously to ensure its effectiveness and alignment with the changing risk environment and business objectives. Some of the elements of monitoring and improving a CSMS are: Increase in staff training and security awareness: This element involves providing regular and updated training and awareness programs for the staff involved in the operation, maintenance, and security of the IACS. Training and awareness can help improve the skills, knowledge, and behavior of the staff, and reduce the likelihood and impact of human errors, negligence, or malicious actions. Training and awareness can also help foster a positive security culture and increase the staff\\'s engagement and commitment to the CSMS12 Significant changes in identified risk found in periodic reassessments: This element involves conducting periodic risk assessments to identify and evaluate the current and emerging threats, vulnerabilities, and consequences that may affect the IACS. Risk assessments can help determine the appropriate security levels (SLs) and security requirements for the system under control (SuC) and its components. Risk assessments can also help identify any gaps or weaknesses in the existing security measures and controls, and prioritize the actions for risk mitigation or acceptance. Periodic risk assessments can help ensure that the CSMS is responsive and adaptive to the changing risk landscape and business needs13 Review of system logs and other key data files: This element involves collecting, analyzing, and reviewing the system logs and other key data files that record the events and activities related to the IACS. System logs and data files can provide valuable information and insights for security monitoring, detection, response, and recovery. They can also help identify any anomalies, incidents, or breaches that may compromise the security or performance of the IACS. System logs and data files can also help measure and evaluate the effectiveness and efficiency of the CSMS and its processes, and provide feedback and recommendations for improvement14 References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 4.3, Cybersecurity Management System (CSMS) ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program, Clause 5.3.2.1, Training and awareness ISA/IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, Clause 4, Security risk assessment process ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, Clause 4.3.3.7, Audit and accountabilit

QUESTION 7

In which layer is the physical address assigned?

Available Choices (select all choices that are correct)

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 7

Correct Answer: B

According to the OSI model, the physical address is assigned in the layer 2, also known as the data link layer. The physical address is a unique identifier for each device on a network, such as a MAC address or a serial number. The data link layer is responsible for transferring data between adjacent nodes on a network, using the physical address to identify the source and destination of each frame. The data link layer also provides error detection and correction, flow control, and media access control. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Prep, section 2.2; ISA/IEC 62443 Standards to Secure Your Industrial Control System, section 3.1.2.

QUESTION 8

Which is one of the PRIMARY goals of providing a framework addressing secure product development life-cycle requirements?

Available Choices (select all choices that are correct)

A. Aligned development process

B. Aligned needs of industrial users

C. Well-documented security policies and procedures

D. Defense-in-depth approach to designing

Correct Answer: A

One of the primary goals of providing a framework addressing secure product development life-cycle requirements is to ensure that the development process of industrial automation and control systems (IACS) products is aligned with the security objectives and requirements of the ISA/IEC 62443 series of standards. The framework defines a secure development life-cycle (SDL) that covers all the phases of product development, from security requirements definition, to secure design, implementation, verification, validation, defect management, patch management, and product end-of-life. The framework also provides guidance on how to document and demonstrate compliance with the SDL requirements, as well as how to assess the security performance of the products using security levels. By following the framework, product suppliers can improve the security of their products and reduce the risk of vulnerabilities and exploits that may compromise the safety, integrity, reliability, and security of IACS. References: ISA/IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Product security development life-cycle requirements1 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components2

QUESTION 9

In a defense-in-depth strategy, what is the purpose of role-based access control?

Available Choices (select all choices that are correct)

A. Ensures that users can access systems from remote locations

B. Ensures that users can access only certain devices on the network

C. Ensures that users can access only the functions they need for their job

D. Ensures that users correctly manage their username and password

Correct Answer: C

Role-based access control (RBAC) is a method of restricting access to resources based on the roles of individual users within an organization. RBAC assigns permissions and responsibilities to roles, rather than to individual users, and then assigns users to those roles. This way, users can only perform the actions that are relevant and necessary for their role, and not access or modify any other resources that are beyond their scope of authority. RBAC is one of the security countermeasures that can be implemented in a defense-in-depth strategy, which is a layered approach to protect industrial automation and control systems (IACS) from cyber threats. RBAC can help prevent unauthorized access, misuse, or sabotage of IACS resources, as well as reduce the risk of human error or insider attacks. References: ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels, Clause 5.3.2.11 ISA/IEC 62443-2-1:2010, Security for industrial automation and control systems Part 2-1: Establishing an industrial automation and control systems security program, Clause 6.2.2.32 ISA/IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Product security development life-cycle requirements, Clause 5.2.3.23 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems

- Part 4-2: Technical security requirements for IACS components, Clause 4.2.3.24

QUESTION 10

Which organization manages the ISASecure conformance certification program?

Available Choices (select all choices that are correct)

A. American Society for Industrial Security

B. Automation Federation

C. National Institute of Standards and Technology

D. Security Compliance Institute

Correct Answer: D

The ISASecure conformance certification program is managed by the Security Compliance Institute (ISCI), a non-profit organization established in 2007 by a group of industry stakeholders, including end users, suppliers, and integrators. ISCI\\'s mission is to provide a common industry-accepted set of device and process requirements that drive device security, simplifying procurement for asset owners and device assurance for equipment vendors12. References: 1: ISASecure

- IEC 62443 Conformance Certification - Official Site 2: Certifications - ISASecure

---

QUESTION 11

Which of the following is an example of separation of duties as a part of system development and maintenance?

Available Choices (select all choices that are correct)

A. Changes are approved by one party and implemented by another.

B. Configuration settings are made by one party and self-reviewed using a checklist.

C. Developers write and then test their own code.

D. Design and implementation are performed by the same team.

Correct Answer: A

Separation of duties is a security principle that aims to prevent fraud, errors, conflicts of interest, or misuse of resources by dividing critical tasks or functions among different people or teams. It is one of the foundational requirements (FRs) of the ISA/IEC 62443 standards for securing industrial automation and control systems (IACSs). According to the ISA/IEC 62443-2-1 standard, separation of duties includes the following system requirements (SRs): SR 2.1: Security management policy SR 2.2: Personnel security SR 2.3: System development and maintenance SR 2.4: Incident response and recovery SR 2.5: Compliance and review Among these SRs, the one that is most related to the example of system development and maintenance is SR 2.3. SR 2.3 requires that the IACS shall provide the capability to ensure that the development and maintenance of the system and its components are performed in a secure manner. This means that the IACS should have a mechanism to control the access and authorization of developers, testers, integrators, and maintainers who work on the system and its components. It also means that the IACS should have a mechanism to verify and validate the quality and security of the system and its components before, during, and after the development and maintenance processes. Therefore, an example of separation of duties as a part of system development and maintenance is that changes are approved by one party and implemented by another. This ensures that the changes are authorized, documented, and reviewed by someone who is not involved in the implementation. This reduces the risk of introducing errors, vulnerabilities, or malicious code into the system and its components. References: ISA/IEC 62443-2-1:2010, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program1 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Certificate Program2 ISA/IEC 62443 Cybersecurity Library3 Using the ISA/IEC 62443 Standards to Secure Your Control Systems4

QUESTION 12

Which factor drives the selection of countermeasures?

Available Choices (select all choices that are correct)

A. Foundational requirements

B. Output from a risk assessment

C. Security levels

D. System design

Correct Answer: B

The selection of countermeasures is driven by the output from a risk assessment, which identifies the risks and their associated likelihood and consequences for each zone and conduit in the industrial automation and control system (IACS). The risk assessment also determines the target security level (SL-T) for each zone and conduit, which represents the desired level of protection against the identified threats. The countermeasures are then selected based on the SL-T and the existing security level (SL- A) of the zone and conduit, as well as the cost and feasibility of implementation. The countermeasures should aim to reduce the risk to an acceptable level by increasing the SL- A to meet or exceed the SL-T. References: ISA/IEC 62443-3-2:2018 - Security risk assessment for system design, ISA/IEC 62443-3-3:2013 - System security requirements and security levels, ISA/IEC 62443 Cybersecurity Fundamentals Specialist Training Course

QUESTION 13

Which statement is TRUE reqardinq application of patches in an IACS environment?

Available Choices (select all choices that are correct)

A. Patches should be applied as soon as they are available.

B. Patches should be applied within one month of availability.

C. Patches never should be applied in an IACS environment.

D. Patches should be applied based on the organization\\'s risk assessment.

Correct Answer: D

Patches are software updates that fix bugs, vulnerabilities, or improve performance or functionality. Patches are important for maintaining the security and reliability of an IACS environment, but they also pose some challenges and risks. Applying patches in an IACS environment is not as simple as in an IT environment, because patches may affect the availability, integrity, or safety of the IACS. Therefore, patches should not be applied blindly or automatically, but based on the organization\\'s risk assessment. The risk assessment should consider the following factors: 1 The severity and likelihood of the vulnerability that the patch addresses The impact of the patch on the IACS functionality and performance The compatibility of the patch with the IACS components and configuration The availability of a backup or recovery plan in case the patch fails or causes problems The testing and validation of the patch before applying it to the production system The communication and coordination with the stakeholders involved in the patching process The documentation and auditing of the patching activities and results References: ISA TR62443-2-3 - Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment

---

QUESTION 14

Which of the following refers to internal rules that govern how an organization protects critical system resources?

Available Choices (select all choices that are correct)

A. Formal guidance

B. Legislation

C. Security policy D- Code of conduct

Correct Answer: C

A security policy refers to internal rules that govern how an organization protects critical system resources, such as industrial control systems (ICS). A security policy defines the objectives, scope, roles, responsibilities, and requirements for

securing the ICS environment, as well as the procedures and guidelines for implementing, monitoring, and enforcing the security measures. A security policy also establishes the baseline for assessing and managing the security risks to the

ICS, and for ensuring compliance with relevant standards, regulations, and best practices. A security policy is a key component of the ICS security program, and it should be documented, communicated, and reviewed regularly.

The other choices are not correct because:

A. Formal guidance. Formal guidance refers to external sources of information and recommendations that can help an organization improve its ICS security posture, such as standards, frameworks, guidelines, and best practices. Formal guidance is not an internal rule, but rather a reference that can be used to develop, implement, and evaluate the

security policy and controls. For example, the ISA/IEC 62443 series of standards provide formal guidance on how to secure ICS from cyber threats1.

B. Legislation. Legislation refers to external laws and regulations that impose legal obligations and penalties on an organization for its ICS security performance, such as the NERC CIP standards for the electric sector2, or the EU NIS Directive for critical infrastructure operators3. Legislation is not an internal rule, but rather a compliancerequirement that must be met by the organization. Legislation may also influence the security policy and controls, as the organization needs to align its security objectives and practices with the legal expectations and consequences. D. Code of conduct. A code of conduct refers to a set of ethical principles and values that guide the behavior and decision-making of an organization and its employees, such as honesty, integrity, respect, and accountability. A code of conduct is not an internal rule for protecting critical system resources, but rather a general norm for conducting business and maintaining a positive reputation. A code of conduct may also support the security policy and culture, as it can foster a sense of responsibility and trust among the ICS stakeholders. References:

1: ISA/IEC 62443 Standards to Secure Your Industrial Control System

2: NERC Critical Infrastructure Protection Standards

3: EU Network and Information Systems Directive

QUESTION 15

What is OPC?

Available Choices (select all choices that are correct)

A. An open standard protocol for real-time field bus communication between automation technology devices

B. An open standard protocol for the communication of real-time data between devices from different manufacturers

C. An open standard serial communications protocol widely used in industrial manufacturing environments

D. A vendor-specific proprietary protocol for the communication of real-time plant data between control devices

Correct Answer: B

OPC stands for Open Platform Communications, and it is a series of standards and specifications for industrial telecommunication based on Object Linking and Embedding (OLE) for process control. It allows the communication of real-time data between devices from different manufacturers using various data transportation technologies, such as Microsoft\\'s OLE, COM, DCOM, .NET, XML, and TCP123. OPC is not a protocol itself, but rather a standardized approach for data connectivity supported by the OPC Foundation3. OPC is widely used in industrial automation and control systems, as well as other industries, to achieve interoperability and integration between different applications and devices3. A is incorrect, because OPC is not a field bus protocol, but rather a standard for data exchange between devices that may use different field bus protocols, such as Modbus, Profibus, or Ethernet/IP2. C is incorrect, because OPC is not a serial communications protocol, but rather a standard that can use various data transportation technologies, including serial, Ethernet, or wireless2. D is incorrect, because OPC is not a vendor- specific proprietary protocol, but rather an open standard that can be implemented by any vendor or device that supports the OPC specifications3. References: 1: Open Platform Communications - Wikipedia 2: What is OPC Protocol - The Automization 3: What is OPC?

-OPC Foundation

Test Questions