# 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.pass4itsure.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**

Which is the BEST practice when establishing security zones?

Available Choices (select all choices that are correct)

A. Security zones should contain assets that share common security requirements.

B. Security zones should align with physical network segments.

C. Assets within the same logical communication network should be in the same security zone.

D. All components in a large or complex system should be in the same security zone.

Correct Answer: A

Security zones are logical groupings of assets that share common security requirements based on factors such as criticality, consequence, vulnerability, and threat. Security zones are used to apply the principle of defense in depth, which means creating multiple layers of protection to prevent or mitigate cyberattacks. By creating security zones, asset owners can isolate the most critical or sensitive assets from the less critical or sensitive ones, and apply different levels of security controls to each zone according to the risk assessment. Security zones are not necessarily aligned with physical network segments, as assets within the same network may have different security requirements. For example, a network segment may contain both a safety instrumented system (SIS) and a human-machine interface (HMI), but the SIS has a higher security requirement than the HMI. Therefore, the SIS and the HMI should be in different security zones, even if they are in the same network segment. Similarly, assetswithin the same logical communication network may not have the same security requirements, and therefore should not be in the same security zone. For example, a logical communication network may span across multiple physical locations, such as a plant and a corporate office, but the assets in the plant may have higher security requirements than the assets in the office. Therefore, the assets in the plant and the office should be in different security zones, even if they are in the same logical communication network. Finally, all components in a large or complex system should not be in the same security zone, as this would create a single point of failure and expose the entire system to potential cyberattacks. Instead, the components should be divided into smaller and simpler security zones, based on their security requirements, and the communication between the zones should be controlled by conduits. Conduits are logical or physical connections between security zones that allow data flow and access control. Conduits should be designed to minimize the attack surface and the potential impact of cyberattacks, by applying security controls such as firewalls, encryption, authentication, and authorization. References: How to Define Zones and Conduits1 Securing industrial networks: What is ISA/IEC 62443?2 ISA/IEC 62443 Series of Standards3

**QUESTION 2**

Which is a PRIMARY reason why network security is important in IACS environments?

Available Choices (select all choices that are correct)

A. PLCs are inherently unreliable.

B. PLCs are programmed using ladder logic.

C. PLCs use serial or Ethernet communications methods.

D. PLCs under cyber attack can have costly and dangerous impacts.

Correct Answer: D

Network security is important in IACS environments because PLCs, or programmable logic controllers, are devices that control physical processes and equipment in industrial settings. PLCs under cyber attack can have costly and dangerous impacts, such as disrupting production, damaging equipment, compromising safety, and harming the environment. Therefore, network security is essential to protect PLCs and other IACS components from unauthorized access, modification, or disruption. The other choices are not primary reasons why network security is important in IACS environments. PLCsare not inherently unreliable, but they can be affected by environmental factors, such as temperature, humidity, and electromagnetic interference. PLCs are programmed using ladder logic, which is a graphical programming language that resembles electrical schematics. PLCs use serial or Ethernet communications methods, depending on the type and age of the device, to communicate with other IACS components, such as human- machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCSs). References: ISA/IEC 62443 Standards to Secure Your Industrial Control System training course1 ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide2 Using the ISA/IEC 62443 Standard to Secure Your Control Systems3

**QUESTION 3**

What does Layer 1 of the ISO/OSI protocol stack provide?

Available Choices (select all choices that are correct)

A. Data encryption, routing, and end-to-end connectivity

B. Framing, converting electrical signals to data, and error checking

C. The electrical and physical specifications of the data connection

D. User applications specific to network applications such as reading data registers in a PLC

Correct Answer: C

Layer 1 of the ISO/OSI protocol stack is the physical layer, which provides the means of transmitting and receiving raw data bits over a physical medium. It defines the electrical and physical specifications of the data connection, such as the voltage levels, signal timing, cable types, connectors, and pin assignments. It does not perform any data encryption, routing, end-to-end connectivity, framing, error checking, or user applications. These functions are performed by higher layers of the protocol stack, such as the data link layer, the network layer, the transport layer, and the application layer. References: ISO/IEC 7498-1:1994, Section 6.11; ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 3.1.12

**QUESTION 4**

Which of the ISA 62443 standards focuses on the process of developing secure products?

Available Choices (select all choices that are correct)

A. 62443-1-1

B. 62443-3-2

C. 62443-3-3

D. 62443-4-1

Correct Answer: D

The ISA/IEC 62443 series of standards is divided into four main parts, each covering a different aspect of industrial automation and control systems (IACS) cybersecurity1: Part 1: Terminology, Concepts, and Models Part 2: Policies and Procedures Part 3: System Requirements Part 4: Component Requirements The part 4 of the series focuses on the requirements for the secure development and maintenance of products that are used in IACS, such as controllers, sensors, actuators, network devices, software applications, and cloud services. The part 4 consists of two standards1:

**QUESTION 5**

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 6**

Which of the following is a cause for the increase in attacks on IACS?

Available Choices (select all choices that are correct)

A. Use of proprietary communications protocols

B. The move away from commercial off the shelf (COTS) systems, protocols, and networks

C. Knowledge of exploits and tools readily available on the Internet

D. Fewer personnel with system knowledge having access to IACS

Correct Answer: C

One of the reasons for the increase in attacks on IACS is the availability of information and tools that can be used to exploit vulnerabilities in these systems. The Internet provides a platform for hackers, researchers, and activists to share their knowledge and techniques for compromising IACS. Some examples of such information and tools are: Stuxnet: A sophisticated malware that targeted the Iranian nuclear program in 2010. It exploited four zero-day vulnerabilities in Windows and Siemens software to infect and manipulate the programmable logic controllers (PLCs) that controlled the centrifuges. Stuxnet was widely analyzed and reported by the media and security experts, and its source code was leaked online1. Metasploit: A popular penetration testing framework that contains modules for exploiting various IACS components and protocols. For instance, Metasploit includes modules for attacking Modbus, DNP3, OPC, and Siemens

S7 devices2. Shodan: A search engine that allows users to find devices connected to the Internet, such as webcams, routers, printers, and IACS components. Shodan can reveal the location, model, firmware, and configuration of these devices, which can be used by attackers to identify potential targets and vulnerabilities3. ICS-CERT: A website that provides alerts, advisories, and reports on IACS security issues and incidents. ICS-CERT also publishes vulnerability notes and mitigation recommendations for various IACS products and vendors4. These sources of information and tools can be useful for legitimate purposes, such as security testing, research, and education, but they can also be misused by malicious actors who want to disrupt, damage, or steal from IACS. Therefore, IACS owners and operators should be aware of the threats and risks posed by the Internet and implement appropriate security measures to protect their systems. References:

**QUESTION 7**

Which policies and procedures publication is titled Patch Manaqement in the IACS Environment?

Available Choices (select all choices that are correct)

A. ISA-TR62443-2-3

B. ISA-TR62443-1-4

C. ISA-62443-3-3

D. ISA-62443-4-2

Correct Answer: A

ISA-TR62443-2-3 is the technical report that describes the requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program. Patch management is the process of applying software updates to fix vulnerabilities, bugs, or performance issues in the IACS components. Patch management is an essential part of maintaining the security and reliability of the IACS environment. The technical report provides guidance on how to establish a patch management policy, how to assess the impact and risk of patches, how to test and deploy patches, and how to monitor and audit the patch management process. References: 1, 2, 3

**QUESTION 8**

What are the three main components of the ISASecure Integrated Threat Analysis (ITA) Program?

Available Choices (select all choices that are correct)

A. Software development security assurance, functional security assessment, and communications robustness testing

B. Software robustness security testing, functional software assessment assurance, and essential security functionality assessment

C. Communications robustness testing, functional security assurance, and software robustness communications

D. Communication speed, disaster recovery, and essential security functionality assessment

Correct Answer: A

The ISASecure Integrated Threat Analysis (ITA) Program is a certification scheme that certifies off-the-shelf automation and control systems to the ISA/IEC 62443 series of standards1. The ITA Program consists of three main components2:

Software Development Security Assurance (SDSA): This component evaluates the security lifecycle and practices of the product supplier, such as security requirements, design, implementation, verification, and maintenance. The SDSA

certification is based on the ISA/IEC 62443-4-1 standard. Functional Security Assessment (FSA): This component verifies the security functions and features implemented in the product, such as identification and authentication, access

control, encryption, audit logging, and security management. The FSA certification is based on the ISA/IEC 62443-4-2 standard. Communications Robustness Testing (CRT): This component tests the resilience of the product against network

attacks, such as denial-of-service, fuzzing, spoofing, and replay. The CRT certification is based on the ISA/IEC 62443-4-2 and ISA/IEC 62443-3-3 standards .

References:

1: ISASecure - IEC 62443 Conformance Certification - Official Site

2: ISASecure - IEC 62443 Conformance Certification - Official Site [3]: ISA/IEC 62443-4-1: Secure Product Development Lifecycle Requirements, ISA, 2018.

[4]: ISA/IEC 62443-4-2: Technical Security Requirements for IACS Components, ISA, 2019.

[5]: ISA/IEC 62443-4-2: Technical Security Requirements for IACS Components, ISA, 2019.

[6]: ISA/IEC 62443-3-3: System Security Requirements and Security Levels, ISA, 2013.

**QUESTION 9**

What is a commonly used protocol for managing secure data transmission over a Virtual Private Network (VPN)?

Available Choices (select all choices that are correct)

A. HTTPS

B. IPSec

C. MPLS

D. SSH

Correct Answer: B

IPSec is a commonly used protocol for managing secure data transmission over a VPN. IPSec stands for Internet Protocol Security and it is a set of standards that define how to encrypt and authenticate data packets that travel between two or more devices over an IP network. IPSec can operate in two modes: transport mode and tunnel mode. In transport mode, IPSec only encrypts the payload of the IP packet, leaving the header intact. In tunnel mode, IPSec encrypts the entire IP packet and encapsulates it in a new IP header. Tunnel mode is more secure and more suitable for VPNs, as it can protect the original source and destination addresses of the IP packet from eavesdropping or spoofing. IPSec uses two main protocols to provide security services: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data integrity and source authentication, but not confidentiality. ESP provides data integrity, source authentication, and confidentiality. IPSec also uses two protocols to establish and manage security associations (SAs), which are the parameters and keys used for encryption and authentication: Internet Key Exchange (IKE) and Internet Security Association and Key Management Protocol (ISAKMP). IKE is a protocol that negotiates and exchanges cryptographic keys between two devices. ISAKMP is a protocol that defines the format and structure of the messages

used for key exchange and SA management. References: ISA/IEC 62443-3-3:2018, Section 4.2.3.7.1, VPN1 ISA/IEC 62443-4-2:2019, Section 4.2.3.7.1, VPN ISA/IEC 62443 Cybersecurity Fundamentals Specialist Study Guide, Section 5.3.2, VPN ISA/IEC 62443 Cybersecurity Fundamentals Specialist Exam Specification, Section 5.3.2, VPN

**QUESTION 10**

Whose responsibility is it to determine the level of risk an organization is willing to tolerate?

Available Choices (select all choices that are correct)

A. Management

B. Legal Department

C. Operations Department

D. Safety Department

Correct Answer: A

According to the ISA/IEC 62443 standards, the level of risk an organization is willing to tolerate is determined by the management, as they are responsible for defining the business and risk objectives, as well as the security policies and procedures for the organization. The management also has the authority to allocate the necessary resources and assign the roles and responsibilities for implementing and maintaining the security program. The legal, operations, and safety departments may provide input and feedback to the management, but they do not have the final say in determining the risk tolerance level. References: ISA/IEC 62443-2-1:2010 - Establishing an industrial automation and control systems security program, section 4.2.1.

**QUESTION 11**

Which layer in the Open Systems Interconnection (OSI) model would include the use of the File Transfer Protocol (FTP)?

Available Choices (select all choices that are correct)

A. Application layer

B. Data link layer

C. Session layer

D. Transport layer

Correct Answer: A

The File Transfer Protocol (FTP) is an application layer protocol that moves files between local and remote file systems. It runs on top of TCP, like HTTP. To transfer a file, 2 TCP connections are used by FTP in parallel: control connection and data connection. The control connection is used to send commands and responses between the client and the server, while the data connection is used to transfer the actual file. FTP is one of the standard communication protocols defined by the TCP/IP model and it does not fit neatly into the OSI model. However, since the OSI model is a reference model that describes the general functions of each layer, FTP can be considered as an application layer protocol in the OSI model, as it provides user services and interfaces to the network. The application layer is the highest layer in the OSI model and it is responsible for providing various network services to the users, such as email, web browsing, file

transfer, remote login, etc. The application layer interacts with the presentation layer, which is responsible for data formatting, encryption, compression, etc. The presentation layer interacts with the session layer, which is responsible for establishing, maintaining, and terminating sessions between applications. The session layer interacts with the transport layer, which is responsible for reliable end-to-end data transfer and flow control. The transport layer interacts with the network layer, which is responsible for routing and addressing packets across different networks. The network layer interacts with the data link layer, which is responsible for framing, error detection, and medium access control. The data link layer interacts with the physical layer, which is responsible for transmitting and receiving bits over the physical medium. References: File Transfer Protocol (FTP) in Application Layer1 FTP Protocol2 What OSI layer is FTP?3

**QUESTION 12**

Which steps are part of implementing countermeasures?

Available Choices (select all choices that are correct)

A. Establish the risk tolerance and select common countermeasures.

B. Establish the risk tolerance and update the business continuity plan.

C. Select common countermeasures and update the business continuity plan.

D. Select common countermeasures and collaborate with stakeholders.

Correct Answer: A

According to the ISA/IEC 62443-3-2 standard, implementing countermeasures is one of the steps in the security risk assessment for system design. The standard defines a comprehensive set of engineering measures to guide organizations through the process of assessing the risk of a particular industrial automation and control system (IACS) and identifying and applying security countermeasures to reduce that risk to tolerable levels. The standard recommends the following steps for implementing countermeasures: Establish the risk tolerance: This step involves determining the acceptable level of risk for the organization and the system under consideration, based on the business objectives, legal and regulatory requirements, and stakeholder expectations. The risktolerance can be expressed as a target security level (SL-T) for each zone or conduit in the system. Select common countermeasures: This step involves selecting the appropriate security countermeasures for each zone or conduit, based on the SL-T and the existing security level (SL-A) of the system. The standard provides a list of common countermeasures for each security level, covering the domains of physical security, network security, system security, and application security. The selected countermeasures should be documented and justified in the security risk assessment report. References: ISA/IEC 62443 Cybersecurity Series Designated as IEC Horizontal Standards, Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2

**QUESTION 13**

Why is OPC Classic considered firewall unfriendly?

Available Choices (select all choices that are correct)

A. OPC Classic uses DCOM, which dynamically assigns any port between 1024 and 65535.

B. OPC Classic is allowed to use only port 80.

C. OPC Classic works with control devices from different manufacturers.

D. OPC Classic is an obsolete communication standard.

Correct Answer: A

OPC Classic uses DCOM, which dynamically assigns any port between 1024 and 65535. Comprehensive OPC Classic is a software interface technology that uses the Distributed Component Object Model (DCOM) protocol to facilitate the transfer of data between different industrial control systems. DCOM is a Microsoft technology that allows applications to communicate across a network. However, DCOM is not designed with security in mind, and it poses several challenges for firewall configuration. One of the main challenges is that DCOM does not use fixed TCP port numbers, but rather negotiates new port numbers within the first open connection. This means that intermediary firewalls can only be used with wide-open rules, leaving a large range of ports open for potential attacks. This makes OPC Classic very "firewall unfriendly" and reduces the security and protection they provide. References: Tofino Security OPC Foundation White Paper Step 2 (for client or server): Configuring firewall settings - GE Secure firewall for OPC Classic - Design World

**QUESTION 14**

Which is a commonly used protocol for managing secure data transmission on the Internet?

Available Choices (select all choices that are correct)

A. Datagram Transport Layer Security (DTLS)

B. Microsoft Point-to-Point Encryption

C. Secure Telnet

D. Secure Sockets Layer

Correct Answer: AD

Datagram Transport Layer Security (DTLS) and Secure Sockets Layer (SSL) are both commonly used protocols for managing secure data transmission on the Internet. DTLS is a variant of SSL that is designed to work over datagram protocols such as UDP, which are used for real-time applications such as voice and video. SSL is a protocol that provides encryption, authentication, and integrity for data transmitted over TCP, which is used for reliable and ordered delivery of data. Both DTLS and SSL use certificates and asymmetric cryptography to establish a secure session between the communicatingparties, and then use symmetric cryptography to encrypt the data exchanged. DTLS and SSL are widely used in web browsers, email clients, VPNs, and other applications that require secure communication over the Internet. References: ISA/IEC 62443 Standards to Secure Your Industrial Control System, Module 3: Introduction to Cryptography, pages 3-5 to 3-7 Using the ISA/IEC 62443 Standards to Secure Your Control System, Chapter 6: Securing Communications, pages 125-126

**QUESTION 15**

How many element qroups are in the "Addressinq Risk" CSMS cateqorv?

Available Choices (select all choices that are correct)

A. 2

B. 3

C. 4

D. 5

Correct Answer: B

The "Addressing Risk" CSMS category consists of three element groups: Security Policy, Organization and Awareness; Selected Security Countermeasures; and Implementation of Security Program1. These element groups cover the aspects of defining the security objectives, roles and responsibilities, policies and procedures, awareness and training, security countermeasures selection and implementation, and security program execution and maintenance1. The "Addressing Risk" CSMS category aims to reduce the security risk to an acceptable level by applying appropriate security measures to the system under consideration (SuC)1. References: 1: ISA/IEC 62443-2-1: Security for industrial automation and control systems: Establishing an industrial automation and control systems security program