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.geekcert.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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which is the PRIMARY responsibility of the network layer of the Open Systems Interconnection (OSI) model?

Available Choices (select all choices that are correct)

A. Forwards packets, including routing through intermediate routers

B. Gives transparent transfer of data between end users

C. Provides the rules for framing, converting electrical signals to data

D. Handles the physics of getting a message from one device to another

Correct Answer: A

The primary responsibility of the network layer of the Open Systems Interconnection (OSI) model is to forward packets, including routing through intermediate routers. The network layer is the third layer from the bottom of the OSI model, and it is responsible for maintaining the quality of the data and passing and transmitting it from its source to its destination. The network layer also assigns logical addresses to devices, such as IP addresses, and uses various routing algorithms to determine the best path for the packets to travel. The network layer operates on packets, which are units of data that contain the source and destination addresses, as well as the payload. The network layer forwards packets from one node to another, using routers to switch packets between different networks. The network layer also handles host-to-host delivery, which means that it ensures that the packets reach the correct destination host. The other choices are not correct because:

B. Gives transparent transfer of data between end users. This is the responsibility of the transport layer, which is the fourth layer from the bottom of the OSI model. The transport layer provides reliable and error-free data transfer between end users, using protocols such as TCP and UDP. The transport layer operates on segments, which are units of data that contain the source and destination port numbers, as well as the payload. The transport layer also handles flow control, congestion control, and multiplexing.

C. Provides the rules for framing, converting electrical signals to data. This is the responsibility of the data link layer, which is the second layer from the bottom of the OSI model. The data link layer provides the means for transferring data between adjacent nodes on a network, using protocols such as Ethernet and WiFi. The data link layer operates on frames, which are units of data that contain the source and destination MAC addresses, as well as the payload. The data link layer also handles error detection, error correction, and media access control. D. Handles the physics of getting a message from one device to another. This is the responsibility of the physical layer, which is the lowest layer of the OSI model. The physical layer provides the means for transmitting bits over a physical medium, such as copper wire, fiber optic cable, or radio waves. The physical layer operates on bits, which are the smallest units of data that can be either 0 or 1. The physical layer also handles modulation, demodulation, encoding, decoding, and synchronization. References: The OSI Model ?The 7 Layers of Networking Explained in Plain English1 Network Layer in OSI Model2 OSI model3

QUESTION 2

Which communications system covers a large geographic area?

Available Choices (select all choices that are correct)

A. Campus Area Network (CAN)

B. Local Area Network (LAN)

C. Storage Area Network

D. Wide Area Network (WAN)

Correct Answer: D

A Wide Area Network (WAN) is a communications system that covers a large geographic area, such as a city, a country, or even several countries or continents1. WANs are often used to connect local area networks (LANs) and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations2. WANs use various communication infrastructures, such as public telephone lines, undersea cables, and communication satellites, to transmit data over long distances1. WANs are typically established with leased telecommunication circuits or less costly circuit switching or packet switching methods2. WANs are often built by Internet service providers, who provide connections from an organization\\'s LAN to the Internet2. The Internet itself may be considered aWAN2. References: Hardware and network technologies - CCEA LAN and WAN - BBC, Wide area network - Wikipedia.

QUESTION 3

Which is a physical layer standard for serial communications between two or more devices?

Available Choices (select all choices that are correct)

A. RS232

B. RS235

C. RS432

D. RS435

Correct Answer: A

RS232 is a physical layer standard for serial communication between two or more devices. It defines the electrical characteristics, timing, and pinout of connectors for serial data transmission. RS232 is widely used in industrial communication devices, such as PLCs, measuring instruments, and network servers. RS232 allows only one master and one slave to communicate on each line, and operates in a full duplex mode. RS232 has lower transmission speed, shorter maximum cable length, and larger voltage swing than later standards such as RS422 and RS485123 References: 1: Basics of RS232, RS422, and RS485 Serial Communication 2: RS-232 - Wikipedia 3: RS232 Serial Communication Protocol: Basics, Working and Specifications

QUESTION 4

Electronic security, as defined in ANSI/ISA-99.00.01:2007. includes which of the following?

Available Choices (select all choices that are correct)

A. Security guidelines for the proper configuration of IACS computers and operating systems

B. Computers, networks, operating systems, applications, and other programmable configurable components of the system

C. Personnel, policies, and procedures related to the security of computers, networks. PLCs, and other programmable configurable components of the system

D. Security guidelines for the proper configuration of IACS PLCs and other programmable configurable components of the system

Correct Answer: B

Electronic security, as defined in ANSI/ISA-99.00.01:2007, is the discipline that addresses the requirements and implementation of measures to counter threats to the confidentiality, integrity, and availability of the computers, networks, operating systems, applications, and other programmable configurable components of the system1. Electronic security covers the technical aspects of protecting the system from unauthorized access, modification, disruption, or destruction, as well as ensuring the availability and reliability of the system. Electronic security does not include the personnel, policies, and procedures related to the security of the system, which are part of the organizational security1. Electronic security also does not include the security guidelines for the proper configuration of the system components, which are part of the security program1. References: 1: ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models

QUESTION 5

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

ISA-IEC-62443 PDF Dumps   ISA-IEC-62443 Practice   ISA-IEC-62443 Study Guide
                                          Test