# 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 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 2**

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 3**

Authorization (user accounts) must be granted based on which of the following?

Available Choices (select all choices that are correct)

A. Individual preferences

B. Common needs for large groups

C. Specific roles

D. System complexity

Correct Answer: C

Authorization is the process of granting or denying access to a network resource or function. Authorization (user accounts) must be granted based on specific roles, which are defined as sets of permissions and responsibilities assigned to a user or a group of users. Roles should be based on the principle of least privilege, which means that users should only have the minimum level of access required to perform their tasks. Roles should also be based on the principle of separation of duties, which means that users should not have conflicting or overlapping responsibilities that could compromise the security or integrity of the system. Authorization based on individual preferences or common needs for large groups is not recommended, as it could lead to excessive or unnecessary access rights, or to inconsistent or conflicting policies. Authorization based on system complexity is also not a good criterion, as it could result in overcomplicated or unclear roles that are difficult to manage or audit. References: ISA/IEC 62443-3-3:2013 - Security for industrial automation and control systems - Part 3-3: System security requirements and security levels1 ISA/IEC 62443-2-1:2010 - Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program2 ISA/IEC 62443-4-1:2018 - Security for industrial automation and control systems - Part 4-1: Product security development life-cycle requirements3

**QUESTION 4**

Which of the following attacks relies on a human weakness to succeed?

Available Choices (select all choices that are correct)

A. Denial-of-service

B. Phishing

C. Escalation-of-privileges

D. Spoofing

Correct Answer: B

Phishing is a type of cyberattack that relies on a human weakness to succeed. Phishing is the practice of sending fraudulent emails or other messages that appear to come from a legitimate source, such as a bank, a government agency, or a trusted person, in order to trick the recipient into revealing sensitive information, such as passwords, credit card numbers, or personal details, or into clicking on malicious links or attachments that may install malware or ransomware on their devices. Phishing is a common and effective way of compromising the security of industrial automation and control systems (IACS), as it can bypass technical security measures by exploiting the human factor. Phishing can also be used to gain access to the IACS network, to conduct reconnaissance, to launch further attacks, or to cause damage or disruption to the IACS operations. The ISA/IEC 62443 series of standards recognize phishing as a potential threat vector for IACS and provide guidance and best practices on how to prevent, detect, and respond to phishing attacks. Some of the recommended countermeasures include: Educating and training the IACS staff on how to recognize and avoid phishing emails and messages, and how to report any suspicious or malicious activity. Implementing and enforcing policies and procedures for email and message security, such as using strong passwords, verifying the sender\\'s identity, and not opening or clicking on unknown or unsolicited links or attachments. Applying technical security controls, such as antivirus software, firewalls, spam filters, encryption, and authentication, to protect the IACS devices and network from phishing attacks. Monitoring and auditing the IACS network and devices for any signs of phishing attacks, such as anomalous or unauthorized traffic, connections, or activities, and taking appropriate actions to contain and mitigate the impact of any incidents. References: ISA/IEC 62443-1-1:2009, Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models1 ISA/IEC 62443-2-1:2009, Security for industrial automation and control systems - Part 2-1: Establishing an industrial automation and control systems security program2 ISA/IEC 62443-2-4:2015, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers3 ISA/IEC 62443-3-3:2013, Security for industrial automation and control systems - Part 3-3: System security requirements and security levels4 ISA/IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components5

**QUESTION 5**

Which activity is part of establishing policy, organization, and awareness?

Available Choices (select all choices that are correct)

A. Communicate policies.

B. Establish the risk tolerance.

C. Identify detailed vulnerabilities.

D. Implement countermeasures.

Correct Answer: A

According to the ISA/IEC 62443 Cybersecurity Fundamentals Specialist course, establishing policy, organization, and awareness is one of the four steps of the IACS cybersecurity lifecycle. This step involves defining the cybersecurity policies, roles, and responsibilities, as well as communicating them to the relevant stakeholders. It also involves

establishing the risk tolerance level, which is the acceptable level of risk for the organization. Communicating policies and establishing the risk tolerance are both activities that are part of this step. Identifying detailed vulnerabilities and implementing countermeasures are activities that belong to the next steps of the lifecycle, which are assessing the current situation and implementing the cybersecurityprogram, respectively. References: ISA/IEC 62443 Cybersecurity Fundamentals Specialist course, Module 2: IACS Cybersecurity Lifecycle1