# ISA-IEC-62443$^{Q\&As}$

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

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

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

**QUESTION 1**

Which is the implementation of PROFIBUS over Ethernet for non-safetv-related communications?

Available Choices (select all choices that are correct)

A. PROFIBUS DP

B. PROFIBUS PA

C. PROFINET

D. PROF1SAFE

Correct Answer: C

PROFINET is the implementation of PROFIBUS over Ethernet for non- safety-related communications. It is a standard for industrial Ethernet that enables real-time data exchange between automation devices, controllers, and higher-level systems. PROFINET uses standard Ethernet hardware and software, but adds a thin software layer that allows deterministic and fast communication. PROFINET supports different communication profiles for different applications, such as motion control, process automation, and functional safety. PROFINET is compatible with PROFIBUS, and allows seamless integration of existing PROFIBUS devices and networks123 References: 1: What is PROFINET? - PI North America

2: PROFINET - Wikipedia 3:

PROFINET Technology and Application - System Description

**QUESTION 2**

What is the purpose of ISO/IEC 15408 (Common Criteria)?

Available Choices (select all choices that are correct)

A. To define a security management organization

B. To describe a process for risk management

C. To define a product development evaluation methodology

D. To describe what constitutes a secure product

Correct Answer: C

ISO/IEC 15408, also known as the Common Criteria for Information Technology Security Evaluation, is an international standard that provides a framework for evaluating the security of IT products and systems. The purpose of the standard is to define a common set of requirements for the security functions and assurance measures of IT products and systems, and to establish a common methodology for conducting security evaluations. The standard allows users to specify their security needs and expectations in a Security Target (ST), which may be based on one or more Protection Profiles (PPs) that define security requirements for a class of products or systems. Vendors can then implement or claim compliance with the ST or PPs, and have their products or systems evaluated by independent testing laboratories against the security criteria defined in the standard. The standard also defines a scale of Evaluation Assurance Levels (EALs) that indicate the degree of confidence in the security of the evaluated product or system. The standard is intended to facilitate the development, procurement, and use of secure IT products and systems, and to promote the recognition and acceptance of evaluation results across different countries and regions. References: ISO/IEC 15408-1:2009 - Common Criteria Evaluation for IT Security - Nemko1 Common Criteria - Wikipedia2 ISO/IEC Standard 15408 -- ENISA3

**QUESTION 3**

What is defined as the hardware and software components of an IACS?

Available Choices (select all choices that are correct) A. COTS software and hardware

B. Electronic security

C. Control system

D. Cybersecuritv

Correct Answer: C

According to the ISA/IEC 62443-1-1 standard, an industrial automation and control system (IACS) is defined as a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an

industrial process. The hardware and software components of an IACS include the control system, which is the combination of control devices, networks, and applications that perform the control functions for the industrial process. The control

system may consist of various types of devices, such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMI), remote terminal

units (RTU), intelligent electronic devices (IED), sensors, actuators, and other field devices. The control system may also use commercial off-the-shelf (COTS) software and hardware, such as operating systems, databases, firewalls, routers,

switches, and servers, to support the control functions and communication.

References:

ISA/IEC 62443-1-1:2009, Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models, Clause 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 3.2.12

**QUESTION 4**

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 5**

Which of the following is the BEST reason for periodic audits?

Available Choices (select all choices that are correct)

A. To confirm audit procedures

B. To meet regulations

C. To validate that security policies and procedures are performing

D. To adhere to a published or approved schedule

Correct Answer: C

Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References: Periodic audits are an essential part of the ISA/IEC 62443 cybersecurity standards, as they help to verify the effectiveness and compliance of the security program. According to the ISA/IEC 62443-2-1 standard, periodic audits should be conducted to evaluate the following aspects1: The security policies and procedures are consistent with the security requirements and objectives of the organization The security policies and procedures are implemented and enforced in accordance with the security program The security policies and procedures are reviewed and updated regularly to reflect changes in the threat landscape, the IACS environment, and the business needs The security performance indicators and metrics are measured and reported to the relevant stakeholders The security incidents and vulnerabilities are identified, analyzed, and resolved in a timely manner The security awareness and training programs are effective and aligned with the security roles and responsibilities of the personnel The security audits and assessments are conducted by qualified and independent auditors The security audit and assessment results are documented and communicated to the appropriate parties The security audit and assessment findings and recommendations are addressed and implemented in a prioritized and systematic way Periodic audits are not only a means to meet regulations or adhere to a schedule, but also a way to validate that the security policies and procedures are performing as intended and achieving the desired security outcomes. Periodic audits also help to identify gaps and weaknesses in the security program and provide opportunities for improvement and enhancement. References: