Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

ISA-IEC-62443-IC32M MCQs
ISA-IEC-62443-IC32M TestPrep
ISA-IEC-62443-IC32M Study Guide
ISA-IEC-62443-IC32M Practice Test
ISA-IEC-62443-IC32M Exam Questions

PASS

killexams.com

ISA

ISA-IEC-62443-IC32M

ISA/IEC 62443 Cybersecurity Fundamentals Specialist Certification (Certificate 1)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/ISA-IEC-62443-IC32M

Question: 581

An OT network in a power plant uses a SCADA system to monitor turbine performance. The SCADA system communicates via DNP3 over TCP/IP, and an attacker attempts a man-in-the-middle (MITM) attack. Which ISA/IEC 62443-compliant measures can prevent this?

A. Configure DNP3 to use Secure Authentication (SAv5) with digital signatures
B. Deploy an Intrusion Detection System (IDS) to monitor DNP3 traffic anomalies
C. Enable IPsec with AES-256 encryption for DNP3 communications
D. Replace DNP3 with MQTT to reduce protocol vulnerabilities

Answer: A,B,C

Explanation: ISA/IEC 62443 advocates defense-in-depth for OT networks. DNP3 Secure Authentication (SAv5) uses digital signatures to verify message integrity, preventing MITM attacks. An IDS monitors DNP3 traffic for anomalies, enabling early detection of attacks, as per ISA/IEC 62443-3-3. IPsec with AES-256 encryption secures communications, ensuring confidentiality and authenticity. Replacing DNP3 with MQTT is not a direct solution, as MQTT has its own vulnerabilities and requires similar security measures, making it an unnecessary change.

Question: 582

A solar power plant conducts a risk assessment per ISA/IEC 62443-3-2. A photovoltaic inverter in a zone (SL-T 2) has a vulnerability allowing unauthorized configuration changes (CVSS 7.5). Which steps should be included in the risk assessment?

A. Assess the likelihood based on the inverter’s network accessibility
B. Document compensating controls, such as access control lists (ACLs)
C. Evaluate the impact on power generation if configurations are altered
D. Use the formula: Risk = Likelihood / Impact

Answer: A,B,C

Explanation: ISA/IEC 62443-3-2 requires a detailed risk assessment. Assessing

likelihood based on network accessibility determines the probability of exploitation. Documenting compensating controls like ACLs evaluates mitigation options. Evaluating the impact on power generation quantifies the consequences. The formula Risk = Likelihood / Impact is incorrect; ISA/IEC 62443 uses Risk = Likelihood × Impact for risk scoring.

Question: 583

A security policy for an IACS in a water utility requires user account management. Which measures align with ISA/IEC 62443-2-1?

A. Assign user accounts based on specific roles and responsibilities
B. Allow shared accounts for operators to simplify access
C. Implement account lockout after five failed login attempts
D. Review user access privileges every six months

Answer: A,C,D

Explanation: Assigning accounts based on roles ensures least privilege. Account lockout after failed attempts prevents brute-force attacks. Reviewing privileges every six months maintains security, per ISA/IEC 62443-2-1. Shared accounts increase risk and violate individual accountability principles.

Question: 584

An IACS supplier is preparing for ISASecure SDLA certification and must demonstrate compliance with ISA/IEC 62443-4-1. Which tools or methods must be used in the SDL process?

A. Static code analysis for all software components
B. Threat modeling using STRIDE methodology
C. Manual code reviews by a single developer
D. Automated vulnerability scanning during integration

Answer: A,B,D

Explanation: ISA/IEC 62443-4-1 requires robust SDL practices, including static code analysis to detect coding flaws, threat modeling (e.g., using STRIDE) to identify risks,

and automated vulnerability scanning during integration to ensure security. Manual code reviews by a single developer are insufficient, as peer or independent reviews are preferred.

Question: 585

During an ISA/IEC 62443-3-2 assessment, a factory assigns an SL-T of SL-4 to a critical zone. Which factors contribute to this high SL-T?

A. High likelihood of nation-state attacks
B. Potential for catastrophic safety impacts
C. Use of legacy systems with known vulnerabilities
D. Limited budget for countermeasures

Answer: A,B,C

Explanation: Nation-state attacks increase threat likelihood, justifying SL-4. Catastrophic safety impacts raise the impact score. Legacy systems with vulnerabilities elevate risk, supporting a high SL-T. Budget constraints are not a factor in SL-T assignment.

Question: 586

An IACS operator is responding to a security incident per ISA/IEC 62443-2-1. The incident involves unauthorized access to a critical PLC. Which actions MUST be taken to align with the standard?

A. Contain the incident by isolating the affected PLC
B. Notify all employees of the incident details
C. Analyze the incident to identify root causes
D. Restore the PLC without forensic analysis E) Update the CSMS based on lessons learned

Answer: A,C,E

Explanation: ISA/IEC 62443-2-1 outlines incident response requirements. Containing the incident by isolating the affected PLC prevents further damage. Analyzing the incident to identify root causes is critical for prevention. Updating the CSMS based on lessons learned improves future resilience. Notifying all employees of details is not required, as

communication should be targeted. Restoring the PLC without forensic analysis risks missing critical evidence and is not compliant.

Question: 587

During the design phase of the Security Lifecycle for an IACS in a power plant, the cybersecurity team must select countermeasures to achieve Security Level 2 (SL2) per ISA/IEC 62443-3-3. Which countermeasures are appropriate?

A. Configure role-based access control (RBAC) with least privilege principles
B. Deploy a single firewall at the network perimeter
C. Implement network segmentation using VLANs and conduits
D. Use symmetric encryption for all data transmissions
E. Establish anomaly detection using IDS within critical zones

Answer: A,C,E

Explanation: Achieving SL2 requires protection against moderately skilled attackers. RBAC with least privilege ensures authorized access, network segmentation via VLANs and conduits isolates critical assets, and IDS detects anomalies within zones. A single firewall is insufficient for SL2, as defense-in-depth is required. Symmetric encryption, while secure, is less flexible than asymmetric encryption for IACS and not explicitly required for SL2.

Question: 588

A zero-day attack targets an IACS gateway, exploiting a flaw in its SSL implementation. The attacker sends crafted packets, causing a denial-of-service with the log entry SSL_ERROR_RX_RECORD_TOO_LONG. Which ISA/IEC 62443 measures are most effective?

A. Apply rate-limiting on incoming SSL connections
B. Deploy redundant gateways for failover
C. Implement protocol validation in the firewall
D. Update the gateway firmware to the latest version

Answer: A,B,C

Explanation: A zero-day attack on the SSL implementation requires immediate mitigation. Rate-limiting SSL connections, per ISA/IEC 62443-3-3, reduces the impact of denial-of-service by throttling malicious traffic. Deploying redundant gateways, aligned with ISA/IEC 62443-2-1 high-availability requirements, ensures continuity during an attack. Protocol validation in the firewall, per ISA/IEC 62443-3-3, detects and blocks malformed SSL packets. Updating firmware is ineffective for a zero-day, as no patch exists for the unknown vulnerability.

Question: 589

A CRS for an IACS in a power plant specifies SL-T 2 for a zone with HMIs. Per ISA/IEC 62443-3-3, which capabilities must be included?

A. Access control with strong passwords
B. Mandatory use of specific HMI software
C. Session timeout for HMI access
D. Traffic encryption between HMIs and servers

Answer: A,C,D

Explanation: SL-T 2, per ISA/IEC 62443-3-3, requires access control with strong passwords, session timeouts, and traffic encryption to protect HMIs. Specific HMI software is not mandated, as the CRS focuses on functional requirements.

Question: 590

A chemical plant is implementing ISA/IEC 62443 standards to secure its DCS. During the cybersecurity lifecycle's assess phase, the team identifies a critical PLC controlling a reactor with an unpatched vulnerability (CVSS score 8.5). The PLC communicates via Modbus/TCP over an unsecured Ethernet network. Which actions align with ISA/IEC 62443-3-2 requirements to mitigate risks in this scenario?

A. Allocate the PLC to a dedicated security zone with defined conduits
B. Apply a firewall rule to restrict Modbus/TCP traffic to specific IP addresses
C. Immediately patch the PLC firmware to eliminate the vulnerability
D. Replace the PLC with a new model supporting OPC UA with encryption

Answer: A,B

Explanation: ISA/IEC 62443-3-2 emphasizes segmenting IACS into security zones and conduits to manage risk. Allocating the PLC to a dedicated zone with defined conduits isolates it, reducing exposure. Restricting Modbus/TCP traffic via firewall rules enhances network security by limiting unauthorized access. Patching the PLC firmware may not be immediately feasible due to operational constraints or validation requirements, and the standard prioritizes risk management over immediate patching. Replacing the PLC with an OPC UA-supported model is a long-term solution but not directly required by 62443-3-2 for immediate risk mitigation.

Question: 591

A chemical plant's DCS experiences intermittent outages due to a malware-induced CPU overload on controllers. Which ISA/IEC 62443-compliant measures ensure availability?

A. Deploy redundant controllers with automatic failover
B. Use default-allow policies to ensure control traffic flow
C. Implement resource monitoring and throttling on controllers
D. Apply ISA/IEC 62443-4-2-compliant endpoint hardening

Answer: A,C,D

Explanation: Redundant controllers with failover maintain system availability during outages, per ISA/IEC 62443-3-3. Resource monitoring and throttling prevent CPU overloads, supporting availability. Endpoint hardening per ISA/IEC 62443-4-2 reduces malware impact by securing controllers. Default-allow policies increase attack surfaces, contradicting ISA/IEC 62443's security principles.

Question: 592

A pharmaceutical plant's IACS uses a legacy PLC with unencrypted Modbus/Plus protocol. During a 62443-3-2 risk assessment, the team assigns a high-risk score due to potential data interception. Which mitigation strategies align with the standard?

A. Deploy an IDS to monitor Modbus/Plus traffic for anomalies
B. Encrypt Modbus/Plus traffic using a gateway with TLS
C. Segment the PLC into a dedicated security zone

D. Replace Modbus/Plus with a proprietary protocol

Answer: A,C

Explanation: ISA/IEC 62443-3-2 emphasizes risk reduction through zoning and monitoring. Deploying an IDS monitors Modbus/Plus traffic for anomalies, detecting potential attacks. Segmenting the PLC into a dedicated zone isolates it, reducing interception risks. Encrypting Modbus/Plus via TLS is not natively supported and requires impractical custom solutions. Replacing with a proprietary protocol is not recommended, as 62443 prioritizes standardized approaches.

Question: 593

A chemical plant's IACS is undergoing a cybersecurity audit. The auditor identifies that the Distributed Control System (DCS) uses Modbus TCP over an unsegmented network, and the system lacks role-based access control (RBAC). Which measures align with ISA/IEC 62443 to secure the IACS?

A. Configure a firewall to filter Modbus TCP traffic using deep packet inspection
B. Implement network segmentation to isolate DCS from the enterprise IT network
C. Replace Modbus TCP with a proprietary protocol to reduce attack surface
D. Deploy RBAC with least privilege principles for DCS operators

Answer: A,B,D

Explanation: Securing an IACS per ISA/IEC 62443 involves multiple layers of protection. Configuring a firewall with deep packet inspection enhances network security by analyzing Modbus TCP packets for malicious content, aligning with defense-in-depth. Network segmentation isolates the DCS, reducing the risk of lateral movement from compromised IT systems, a key requirement in ISA/IEC 62443-3-3. Implementing RBAC ensures operators access only necessary functions, adhering to the least privilege principle in ISA/IEC 62443-2-1. Replacing Modbus TCP with a proprietary protocol is not recommended, as it may introduce compatibility issues and does not inherently improve security without additional measures.

Question: 594

An IACS operator plans to apply a patch to a DCS during a scheduled outage. According

to ISA/IEC 62443-2-3, which configurations must be validated post-patching to ensure system integrity? (Select all that apply)

A. Network communication protocols
B. Role-based access control settings
C. Physical access controls to the DCS
D. System performance metrics

Answer: A,B,D

Explanation: Post-patching validation, per ISA/IEC 62443-2-3, includes checking network communication protocols to ensure connectivity, verifying role-based access control settings to maintain security, and monitoring system performance metrics to confirm functionality. Physical access controls are not typically affected by software patches, making this option incorrect.

Question: 595

A manufacturing facility is developing a CRS for a new IACS per ISA/IEC 62443-3-2. The system must achieve SL-T 3 for a zone containing critical PLCs. Which requirements should be specified in the CRS?

A. Audit logging for all user actions
B. Mandatory use of specific PLC models
C. Network intrusion detection systems
D. Two-factor authentication for remote access

Answer: A,C,D

Explanation: The CRS for SL-T 3 must include security capabilities like audit logging, network intrusion detection, and two-factor authentication to meet ISA/IEC 62443-3-3 requirements for monitoring and access control. Specific PLC models are not required, as the CRS focuses on functional security requirements.

Question: 596

A system integrator is designing an IACS network for a power plant, following ISA/IEC 62443-1-1 zone and conduit models. The design includes a DMZ separating the

enterprise network from the IACS. Which actions align with shared responsibility principles for securing the DMZ?

A. Asset owner defines DMZ access control policies
B. Product supplier provides firewalls with SL-C level 3 capabilities
C. Service provider monitors DMZ traffic for anomalies
D. System integrator implements VLANs within the IACS network

Answer: A, B, C

Explanation: The asset owner defines access control policies for the DMZ to align with business and security objectives (ISA/IEC 62443-1-1). Product suppliers provide components, like firewalls, meeting specific security level capabilities (ISA/IEC 62443-4-2). Service providers monitor traffic for anomalies as part of maintenance (ISA/IEC 62443-2-1). VLAN implementation within the IACS network is internal and not specific to the DMZ.

Question: 597

In an OPC Classic-based IACS, a security breach occurs due to weak DCOM authentication. Which OSI layers are critical for securing DCOM?

A. Application layer
B. Network layer
C. Presentation layer
D. Session layer

Answer: A,C,D

Explanation: DCOM, used by OPC Classic, operates at the application layer for data exchange and authentication settings. The presentation layer handles data formatting and encryption, critical for securing DCOM. The session layer manages DCOM connections, ensuring secure session establishment. The network layer focuses on routing and is not directly involved in DCOM security.

Question: 598

An attacker uses social engineering to obtain credentials for a cloud-connected PLC in a manufacturing plant. Which of the following countermeasures align with ISA/IEC 62443-3-3 to prevent unauthorized access?

A. Implement MFA for PLC administrative access
B. Deploy a SIEM system to detect suspicious login attempts
C. Conduct annual social engineering training for operators
D. Use AES-256 encryption for PLC data transmissions

Answer: A,B,C

Explanation: ISA/IEC 62443-3-3 focuses on system security. MFA strengthens PLC access control, per SR 2.1 (authentication). A SIEM system detects suspicious login attempts, aligning with SR 6.1 (audit and accountability). Annual social engineering training reduces credential theft risks, per SR 2.2 (security awareness). AES-256 encryption secures data transmissions (SR 1.1) but does not prevent unauthorized access via stolen credentials, making it less relevant to this scenario.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.