Intrusion Detection Level I Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is one disadvantage of shock sensors in terms of performance?

A. They can detect all types of glass

B. They reduce sensor range up to 50%

C. They are more expensive than other sensors

D. They require constant calibration

2. Which of the following is a key consideration in security planning for an intrusion detection installation?

A. Maximum system cost

B. Customer's preferences

C. Coverage of vulnerable areas

D. Brand of equipment

3. Which of the following items may cause false alarms with CO detectors?

A. Cleaning solvents

B. Floor wax

C. Hair spray

D. All of the above

4. What feature must be implemented to avoid re-entry with the same credential?

A. Access Control

B. Anti-passback

C. Redundancy Check

D. Time Delay

5. According to statistics, which entrance is most likely to be used by an intruder to break into a house?

A. Side door

B. Back window

C. Front door

D. Garage door

6. Why is it important to check the compass before and after installing a magnetic contact on a boat?

A. To ensure the contact is properly secured

B. Magnets can affect compass readings

C. To avoid interference with the radio signals

D. To calculate the boat's speed more accurately

7. What factor can lead to false alarms in alarm systems?

A. High customer satisfaction

B. Infrequent testing of the system

C. Improperly set sensitivity levels

D. Use of outdated technology

8. According to regulations, which factor should be addressed to reduce false alarms in security systems?

A. Training of the users

B. Regular maintenance of the system

C. Robust entry protocols

D. All of the above

9. True or False: Reverse voltage spikes can cause contacts to fuse together, and this can often be corrected by tapping on the contact.

A. True

B. False

C. Depends on the type of contacts

D. Only in some cases

10. How many pre-configured zone types are available on an NX-8E control panel?

A. 10

B. 20

C. 30

D. 40

Answers

1. B
2. C
3. D
4. B
5. C
6. B
7. C
8. D
9. A
10. C

Explanations

1. What is one disadvantage of shock sensors in terms of performance?

A. They can detect all types of glass

B. They reduce sensor range up to 50%

C. They are more expensive than other sensors

D. They require constant calibration

Shock sensors are designed to detect vibrations caused by impacts or disturbances, such as breaking glass. While they are effective in certain applications, one notable disadvantage is that their performance can be limited in terms of detection range. When it is stated that they can reduce sensor range by up to 50%, this refers to the ability of the sensor to pick up vibrations from a distance. The physical characteristics of shock sensors can lead to a narrower effective detection zone, meaning they may not respond to disturbances that occur outside this reduced range. This limitation can make them less effective in larger areas where a wider detection capability is necessary to ensure comprehensive security coverage. Other types of sensors may provide broader detection capabilities without the range limitations that shock sensors face, allowing for more effective monitoring of larger spaces. Understanding this performance drawback can be crucial for selecting appropriate security measures based on specific environmental conditions or security needs.

2. Which of the following is a key consideration in security planning for an intrusion detection installation?

A. Maximum system cost

B. Customer's preferences

C. Coverage of vulnerable areas

D. Brand of equipment

In security planning for an intrusion detection installation, a fundamental aspect is the coverage of vulnerable areas. This is crucial because an effective intrusion detection system (IDS) is designed to identify and alert on potential security breaches where threats are most likely to occur. Identifying and prioritizing these vulnerable areas—such as entry points, high-value assets, and regions with a history of incidents—ensures that the system is focused on the most critical aspects of security. By concentrating on vulnerable areas, you can allocate resources effectively, optimizing the installation to detect unauthorized access while minimizing blind spots. This targeted approach enhances the overall effectiveness and reliability of the intrusion detection system, ensuring that it can respond promptly to threats in regions that pose the greatest risk. While considerations such as maximum system cost, customer preferences, and the brand of equipment are important in the overall context of an intrusion detection strategy, they do not directly influence the effectiveness of threat detection in the way that assessing and ensuring coverage of vulnerable areas does. This prioritization leads to a more robust security posture.

3. Which of the following items may cause false alarms with CO detectors?

A. Cleaning solvents

B. Floor wax

C. Hair spray

D. All of the above

Choosing "all of the above" is correct because each of the items listed has the potential to interfere with the operation of carbon monoxide (CO) detectors and trigger false alarms. Cleaning solvents often contain volatile organic compounds that can produce harmful fumes, potentially confusing the sensor of a CO detector. Similarly, floor wax might emit fumes when applied, which could mimic the presence of carbon monoxide, leading to unwanted alerts. Hair spray also releases aerosols and chemicals that may register on these detectors, causing them to react as if there were dangerous levels of CO present. Given that all three items share characteristics that could simulate CO readings, it's important for users of CO detectors to understand how various household products can lead to false alarms, ensuring proper maintenance and situational awareness of their environment.

4. What feature must be implemented to avoid re-entry with the same credential?

A. Access Control

B. Anti-passback

C. Redundancy Check

D. Time Delay

The correct choice addresses a critical aspect of maintaining secure access control in environments that utilize credential-based entry systems. Anti-passback is a security feature designed specifically to prevent the reuse of credentials in a way that allows an individual to gain unauthorized repeated access. Essentially, it ensures that once a credential has been used to enter a secure area, it cannot be used again until the individual exits and the state is reset, thereby blocking potential attempts of sharing credentials for re-entry. For example, in a secured building, if an employee swipes their card to enter a room, the anti-passback feature would prevent the same card from being used again until the employee has exited that room. This mechanism enhances security by preventing situations where one person could allow another unauthorized individual to enter through sharing their access credentials or by reusing them improperly. The other areas mentioned, while relevant to security and access controls, do not specifically address the issue of preventing the same credential from being reused for re-entry. Access control generally refers to overall measures to restrict or manage user rights and permissions within a system, while redundancy checks might focus on ensuring data integrity and availability but not preventing unauthorized access. Time delays can serve as a deterrent but do not inherently block re-entry with the same credentials.

5. According to statistics, which entrance is most likely to be used by an intruder to break into a house?

A. Side door

B. Back window

C. Front door

D. Garage door

The front door is most often used by intruders as their point of entry into a house. This is significant for several reasons. Firstly, the front door is frequently positioned in a visible and accessible location, which means it may also be overlooked by passersby. Many people assume that a front door is the most secure entry point, leading homeowners to focus their security efforts on other entrances. Additionally, intruders may believe that the front door is a less suspicious entry point, especially if they arrive during normal hours when people are less likely to perceive them as a threat. Many individuals have the habit of leaving the front door unlocked for convenience, making it an easy target. While other entrances like side doors, back windows, and garage doors can also be used in break-ins, statistics show that intruders prefer the front door due to factors such as visibility, convenience, and the psychological assumption that it is securely locked and therefore less likely to be used. Understanding this can aid homeowners in strengthening security measures specifically at the front entry points of their homes.

6. Why is it important to check the compass before and after installing a magnetic contact on a boat?

A. To ensure the contact is properly secured

B. Magnets can affect compass readings

C. To avoid interference with the radio signals

D. To calculate the boat's speed more accurately

Checking the compass before and after installing a magnetic contact on a boat is important primarily because magnets can affect compass readings. A magnetic contact, by its nature, can create a magnetic field that interferes with the operation of the compass. This interference can result in inaccurate heading information, which is crucial for navigation. Ensuring the compass is functioning correctly after installation helps verify that the magnetic contact does not disrupt navigational accuracy, allowing the boat operator to maintain safe and efficient course plotting. The other options do not directly relate to the impact of installing a magnetic contact on navigational tools. While securing the contact and ensuring proper operation are essential, they do not pertain to the specific concern of compass accuracy. Similarly, issues related to radio signals or calculating speed are not relevant to the magnetic influence on compass readings, making the focus on magnet interference the key reason for checking the compass in this scenario.

7. What factor can lead to false alarms in alarm systems?

A. High customer satisfaction

B. Infrequent testing of the system

C. Improperly set sensitivity levels

D. Use of outdated technology

Improperly set sensitivity levels can lead to false alarms in alarm systems because these settings determine how responsive the system is to potential security threats. If the sensitivity is set too high, the system may register benign activities—such as pets moving around, small animals, or even environmental changes—as threats, resulting in frequent false alarms. Conversely, if the sensitivity is too low, actual security incidents may go undetected. Adjusting the sensitivity levels appropriately is crucial for striking a balance between security and minimizing unnecessary alerts, thereby ensuring that the system only triggers alarms in response to genuine threats.

8. According to regulations, which factor should be addressed to reduce false alarms in security systems?

A. Training of the users

B. Regular maintenance of the system

C. Robust entry protocols

D. All of the above

To effectively reduce false alarms in security systems, it is essential to consider a comprehensive approach that includes training of the users, regular maintenance of the system, and robust entry protocols. Training of users is crucial as it ensures that personnel understand how to operate the security system correctly and are aware of the common causes of false alarms. Proper training helps to minimize human errors, such as triggering an alarm inadvertently. Regular maintenance of the system is also critical as it ensures that all components are functioning correctly. This involves checking for hardware malfunctions, software updates, and ensuring that all sensors are calibrated properly. When the system is well-maintained, there is a lower chance of failure leading to false alarms. Robust entry protocols are important as they define how individuals can access secured areas, reducing instances where unauthorized access could result in alarms being triggered unnecessarily. Well-defined protocols can help in ensuring that only authorized personnel interact with the system in a way that minimizes the potential for alarms. Considering all these factors collectively contributes to a more efficient security system and significantly reduces the incidence of false alarms. Thus, a holistic approach that addresses all these areas is the best strategy for enhancing the reliability of security systems.

9. True or False: Reverse voltage spikes can cause contacts to fuse together, and this can often be corrected by tapping on the contact.

A. True

B. False

C. Depends on the type of contacts

D. Only in some cases

The statement regarding reverse voltage spikes causing contacts to fuse together is indeed true. When electrical contacts experience a sudden reverse voltage spike, it can create an excess of heat at the contact points, which may lead to welding or fusing of the contacts. This phenomenon occurs because the excessive current can cause the materials in the contacts to melt or stick together. The action of tapping on the contact can sometimes restore functionality by physically separating the fused contacts or breaking a circuit that may have formed due to the fusion. This method provides a quick, temporary fix that can allow the device to function again until a more permanent solution can be applied. It's important to note, however, that this is not a foolproof method and may not work in all scenarios, particularly if the contacts have sustained significant damage. Understanding this behavior is crucial in intrusion detection systems and other electronic components, as it highlights the importance of protecting circuits from voltage spikes, either through surge protection measures or by using components that can withstand such conditions.

10. How many pre-configured zone types are available on an NX-8E control panel?

A. 10

B. 20

C. 30

D. 40

The NX-8E control panel is designed to offer flexibility and extensive functionality in security systems. It features a total of 30 pre-configured zone types, which allows for a variety of applications tailored to specific security needs. Each zone type can be customized to correspond with the designated access control or detection functions, such as motion detectors, door contacts, or glass break sensors. Having a wide range of zone types enhances the system's adaptability, ensuring it can handle different types of sensors and configurations in various environments. This extensive selection helps system installers and administrators to optimize the security setup according to the specific requirements of the premises being protected. The functionality of this feature exemplifies the importance of flexibility in intrusion detection systems and underscores the advanced capabilities of the NX-8E control panel.