|  |
| --- |
| Assignment 1 |
|  |
| |  |  | | --- | --- | | **Submitted to: Kunwar Taimur** | | |  | | | **Submitted by: Muhammad Usman** | | |  | | | **Class: BS SE (EVE)** | | |  | | | **Roll no: 2521340** | | |  | | |  |  | |  |  | |

|  |
| --- |
|  |



|  |  |
| --- | --- |
|  | **GOVERNMENT COLLEGE UNIVERSITY FAISALABAD** |

|  |  |
| --- | --- |
| **Description: Gc uni logo.jpg** | **Department of Software Engineering GCUF** |

**Assignment 1: Case Study Security Alarm system**

**Read the following case study of a security system and answer the questions**

**below. You can make necessary assumptions. But state them clearly.**

**Description:**

Design a Security Alarm system for Software Engineering Department. There will be

two modes of the system. One will sense fire, and other will be used to detect

unauthorized access in the department. System should consist of smoke sensors and

electronic keys for the doors. In case of a fire breakout, system should trigger alarms.

And in case of unauthorized access, system should close all the main entrance doors

as well as the Labs doors and send a message to administrator.

**Question 1: What are emergent properties of this system?**

**Answer:**

**Emergent properties** refer to the characteristics or behaviors that arise from the interactions and relationships between the components of a system, rather than from the individual components themselves. These properties often become apparent at the system level and cannot be directly attributed to any single component in isolation. Emergent properties are typically the result of complex interactions, feedback loops, and synergies that occur within a system.

1. **Functional Emergent properties**

One of the primary functional emergent properties of the security alarm system is its ability to effectively respond to critical situations, such as fire outbreaks and unauthorized access attempts. The integration of smoke sensors ensures timely detection of any potential fire hazards, leading to the prompt triggering of the alarm system to alert occupants and authorities. Similarly, the electronic key system provides an additional layer of security, allowing authorized personnel seamless access while immediately restricting unauthorized entry attempts.

**In short**

* The system can detect fire and unauthorized access.
* The system can trigger alarms in case of fire.
* The system can close all the main entrance doors and lab doors in case of unauthorized access.
* The system can send a message to the administrator in case of unauthorized access.

These emergent properties are not explicitly defined in the system requirements, but they arise from the interaction of the different components of the system. For example, the ability of the system to send a message to the administrator in case of unauthorized access arises from the interaction of the smoke sensors, electronic keys, and alarm system controller.

1. **Non-Functional Emergent properties**

In terms of non-functional emergent properties, the security alarm system must exhibit a high level of reliability to maintain the safety and security of the department. This reliability entails consistent and accurate functionality of both the smoke sensors and the electronic key system. Moreover, the system must prioritize security to prevent any unauthorized access, ensuring the protection of sensitive data and resources within the department. Additionally, the system's responsiveness is crucial, as it should trigger immediate alerts and notifications to concerned parties, providing them with the necessary information to take appropriate actions swiftly.

**In Short**

* The system is reliable, meaning that it will work as expected most of the time.
* The system is secure, meaning that it is difficult for unauthorized individuals to disable or tamper with the system.
* The system is easy to use, meaning that it is easy for authorized individuals to arm and disarm the system.

These emergent properties are also not explicitly defined in the system requirements, but they are important for the overall effectiveness of the system. For example, if the system is not reliable, it may not be able to detect a fire or unauthorized access when it is needed most.

**Question 2: Is there any way that failure in one component might affect other components? How?**

**Answer:** Yes, there are many ways that failure in one component of a security alarm system might affect other components. Here are a few examples:

* **Failure of a smoke sensor**: If a smoke sensor fails, the system may not be able to detect a fire. This could lead to the fire spreading and causing damage to the department.
* **Failure of an electronic key:** If an electronic key fails, authorized individuals may not be able to enter the department. This could disrupt their work and make it difficult for them to respond to emergencies.
* **Failure of the alarm system controller:** If the alarm system controller fails, this would prevent the system from triggering alarms in case of fire or unauthorized access. It would also prevent the system from sending a message to the administrator in case of unauthorized access.
* **Failure of the communication network:** If the communication network connecting the different components of the system fails, the system would not be able to function properly. This is because the system needs to be able to communicate with the different sensors and controllers in order to detect and respond to threats.

In addition to these specific examples, failure in any one component of the security alarm system could also lead to cascading failures of other components. For example, if a smoke sensor fails and the system does not detect a fire, this could lead to the fire spreading and damaging other components of the system, such as the alarm system controller or the communication network.

It is important to note that the specific ways in which failure in one component of a security alarm system might affect other components will vary depending on the design and implementation of the system. However, the general principle is that any component of a complex system has the potential to affect other components of the system.

**How to minimize the risk of failure:**

There are a number of things that can be done to minimize the risk of failure in a security alarm system, such as:

* **Using redundant components:** This means using multiple components to perform the same task. For example, using multiple smoke sensors to detect fire or using multiple communication networks to connect the different components of the system.
* **Using high-quality components:** This means using components that are designed and manufactured to be reliable.
* **Regular maintenance:** This means inspecting and testing the system on a regular basis to identify and repair any potential problems.

By taking these steps, it is possible to significantly reduce the risk of failure in a security alarm system and ensure that the system is able to function properly when it is needed most.

**Question 3: Can you find some way so that this alarm might trigger?**

**Answer: T**o ensure that the security alarm system triggers effectively in response to fire or unauthorized access, several strategies can be employed to enhance its reliability and responsiveness. Here are some ways to optimize the alarm system's triggering:

1. **Redundancy in Sensors:** To improve the likelihood of the alarm triggering in case of fire, consider adding more smoke sensors to the system. Distribute these sensors strategically throughout the department, especially in areas with a higher fire risk, such as near fire exits and areas where flammable materials are stored. Multiple sensors enhance the system's ability to detect fires accurately and promptly.
2. **Diverse Sensor Types:** Implement a variety of smoke sensor types, such as optical smoke sensors and ionization smoke sensors. Different sensor technologies are sensitive to various types of fires (e.g., fast-burning vs. smoldering fires), increasing the system's chances of detecting fires quickly and effectively.
3. **Enhanced Authentication Methods:** To improve the alarm's response to unauthorized access, add more electronic keys to the system, and place them on all doors within the department, including interior doors. This comprehensive approach ensures that authorized personnel can access different areas of the department as needed.
4. **Multi-Factor Authentication:** Employ a range of authentication methods for electronic keys, such as PIN codes, proximity cards, and biometric scanners. Multi-factor authentication adds an extra layer of security, making it more difficult for unauthorized individuals to gain access and further enhancing the alarm system's security measures.
5. **Manual Triggering Feature:** Integrate a manual triggering feature into the system, allowing authorized individuals to manually activate the alarm when they suspect a fire or encounter unauthorized access. This provides an additional layer of control and responsiveness in critical situations, enabling immediate action when necessary.
6. **Machine Learning Predictive Models:** Implement machine learning to make the alarm system more intelligent and proactive. Train a machine learning model to analyze historical data from the smoke sensors and electronic keys. The model can identify patterns and anomalies that may indicate the likelihood of a fire or unauthorized access. By predicting incidents based on data patterns, the system can trigger alarms preemptively.
7. **Emergency Power Backup:** Install a reliable emergency power supply or backup system to ensure the alarm system remains operational during power outages or electrical failures. This guarantees continuous functionality when needed most, even in adverse conditions.

By employing these strategies and potentially combining them, the security alarm system can be significantly enhanced to increase the likelihood of triggering in response to fire and unauthorized access incidents, providing a more comprehensive and robust security solution for the Software Engineering Department.