INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Safety Measures and Security Features in Building: Case Study

[1]Mayur M. Kale, [2]Prof. Chinmay Burange

[1,2]Department of Architecture, P. R. Pote College of Architecture, Amravati, Maharashtra, India

[1]mayurkaleeee@gmail.com, [2]cburange@gmail.com

Article History

Received on: 10 April 2022

Revised on: 18 April 2022

Accepted on: 31 May 2022

Keywords: Safety Measures, Security Features, Buildings Security, Protective Devices

e-ISSN: 2455-6491

Production and hosted by
www.garph.org

ABSTRACT

Keen Buildings are systems of associated gadgets and computer program in charge of consequently overseeing and controlling a few building capacities such as HVAC, fire cautions, lighting, shading and more. These frameworks advanced from generally electronic and mechanical components to complex frameworks depending on IT and remote innovations and systems. This uncovered shrewd buildings to unused dangers and dangers that have to be listed and tended to. Investigate endeavors have been tired a few regions related to security in shrewd buildings but a clear outline of the inquire about field is lost. In this paper, we show the comes about of a precise writing survey that gives a careful understanding of the state of the craftsmanship in investigate on the security of keen buildings. We found that the field of savvy buildings security is developing altogether in complexity due to the numerous conventions presented as of late which the inquire about community is as of now considering.

1. INTRODUCTION

The safety and security of a building are something that must be at the top of every organization's priority. Protecting equipment, resources, and other assets within the building, as well as ensuring those working and operating within the building are safe, is something that cannot be ignored. If organizations aren't careful, they can end up with outdated or inefficient security measures that mean security or safety can be compromised. Although every building is different, and the requirements for security systems may vary, there are a few things every building should think about when evaluating its current security When it comes to protecting public buildings, industrial property, or private houses, structural measures or protection using security guards often have their limitations. Making additional use of electric or electronic protective devices is, therefore, a sensible idea. In order to extend the reaction times, buildings are protected from perimeter protection to the monitoring of open spaces, facades, and roofs, right through to the monitoring of indoor spaces.

Protection of human life while safeguarding buildings, assets, and inventories is the principal function of a commercial alarm system. Recognizing that fire, smoke, and gas leaks and continual threats, industry leaders have made significant strides in developing new detection and early warning are essential elements of any commercial building.

The system should be designed for easy integration with a wide range of security and safety systems, combining intrusion detection, video monitoring, access control, and building management into a single easy-to-use solution. The platform is a natural integrator, ideal for commercial and public buildings, complexes, and distributed organizations.

2. Security Design Concept

The building design is based on specific functional criteria. From the function, the design evolves. Examples of building functions include encouraging efficient job performance, supporting user needs, keeping users safe from hazardous conditions, and protecting occupants from crime and other violent acts. Safety in buildings is mandated by building codes and standards that establish how buildings are to perform during abnormal conditions (example-fires, hurricanes, floods, and earthquakes). Building security, on the other hand, is about assets (people, information & poetry) that can be protected from the effect of malevolent acts carried out by individuals or groups of individuals (for example violent people, criminals, extremists, and terrorists). The primary components of security are the detection and deterrence of malevolent threats before they can be carried out. In the event they are carried out, an additional critical component involves the provision of appropriate response and recovery actions.

A. Access Control

Access control methods are used to monitor and control traffic through specific access points and areas of the secure facility. This is done using a variety of systems including CCTV surveillance, identification cards, security guards, and electronic/mechanical control systems such as locks, doors, and gates or by natural means.

B. Closed-Circuit Television (CCTV)

CCTV has become a necessity for organizations to ensure they can spot unwelcomed visitors and track potential threats to the building. CCTV and IP CCTV systems can be suited to any budget and come in a range of advanced features to help create tailored surveillance for your building premises.

CCTV equipment comes in a range of features and designs to suit any building's requirements. CCTV solutions can also often be accessed and managed remotely so you can monitor and analyze surveillance footage wherever you are.

C. Electronic Access Control Systems

These systems provide commercial access control security by allowing entrance with a keypad, card reader, fingerprint scan, or other biometric access control. The easy-to-use software can be used to track who enters the building and when, and permissions can be granted or removed at any time, from anywhere—no need to change commercial locks when keys are lost or an employee or tenant departs. Electronic door lock systems allow for automatic open and close times, shift access (employee access during specific times and days), and holiday schedules. They can also be used on multiple doors, providing the ability to track individual employees or tenants throughout the entire building in order to increase both security and accountability.

D. Fire Detection Systems

A fire alarm system has a number of devices working together to detect and warn people through visual and audio appliances when smoke, fire, carbon monoxide, or other emergencies are present. These alarms may be activated automatically from smoke detectors, and heat detectors or may also be activated via manual fire alarm activation devices such as manual call points or pull stations. Alarms can be either motorized bells or wall mountable sounders or horns.

They can also be (speaker strobes) which sound an alarm, followed by a voice evacuation message which warns people inside the building not to use the elevators. Fire alarm sounders can be set to certain frequencies and different tones including low, medium, and high, depending on the country and manufacturer of the device.

E. Sprinkler Systems

A fire sprinkler system is an active fire protection method, consisting of a water supply system, providing adequate pressure and flow rate to a water distribution piping system, onto which fire sprinklers are connected. Although historically only used in factories and large commercial buildings, systems for homes and small buildings are now available at a cost-effective price. Fire sprinkler systems are extensively used worldwide, with over 40 million sprinkler heads fitted each year. In buildings completely protected by fire sprinkler systems, over 96% of fires were controlled by fire sprinklers alone.

F. Body Detectors

A full-body scanner is a device that detects objects on a person's body for security screening purposes, without physically removing clothes or making physical contact. Depending on the technology used, the operator may see an alternate-wavelength image of the person's naked body, or merely a cartoon-like representation of the person with an indicator showing where any suspicious items were detected.

3. Safety And Security by Means of Architecture

A. High Rise Building

High-rise buildings present special security concerns, especially related to evacuation. An effective high-rise security strategy is a defend-in-place program, which protects occupants sufficiently inside the building to allow them time to exit safely. In designing high-rises, U.S. developers may look to Asia, where building codes are often more stringent – even if it means using approaches that sacrifice retail space. The 95-story shanghai world financial center, designed by Kohn Pederson Fox, provides a fireproof refuge floor every fifteen stories to buy time for evacuees in an emergency Special elevator in the core allows firefighters to haul equipment up without interfering with the exodus of evacuees.

B. Refuge Spaces

As a result of the Americans with Disabilities Act, areas of refuge are being identified to assist in building evacuation. Persons with disabilities can await assistance in this area, which is located in a fire-protected envelope. In a high-rise building, reinforced areas of refuge are often located every few floors so occupants do not have to go to the ground floor to reach safety. the importance of getting people out of a building quickly is obvious, so training and evacuation producers are important.

4. Case Study-I

A. Case Design (Reliance Foundry)

You might assume that the entrances to your building are where you need the most protection, and you might be right but if you limit security efforts to your front door, you would still be leaving your building vulnerable While security is important, it should and can be done without taking away from the aesthetics. Instead of solely focusing on the building, start by controlling who can walk or drive onto your property. Start at the building perimeter, or property lines, and move towards the building entrances. As an added incentive, installing outdoor security features is often simpler and cheaper than indoor or building envelope measures. What's on the outside counts especially when you're trying to protect what's on the inside.

B. Design Your Environment to Increase Security

Crime Prevention Through Environmental Design (CPTED) is a proactive design philosophy. The concept is simple: a multi-disciplinary approach is applied to buildings and properties to productively use the space to reduce exposure to crime the same way they are designed to prevent damage from daily weather and natural disasters. The benefits of CPTED aren't limited to crime prevention. Taking a proactive design approach can also create cost savings, improved quality of life for building users, and decreased loss and liability.

There are three main components of CPTED

- Surveillance
- Territorial Reinforcement
- Access Control

Surveillance: Surveillance doesn't just mean installing motion sensors and security cameras all over the property; it can be done naturally as well. At its most basic level, surveillance is visibility. Overgrown shrubs, dense trees, low-light conditions, and large window displays can all give criminals places to hide out of sight. Shrubs should be kept shorter than 3 feet tall, and trees should be no taller than 7 feet. Adequately lit parking lots, pathways, and entrances should be as safe at night as they are during the day. 14 If security is considered early enough in a building's design stage, driveways, paths, and walkways can all be placed in view of natural surveillance structures like building entrances and windows. Intruders outside the building aren't the only ones whom you'll want to make sure are visible. If passers-by can see the interior of the space from the sidewalk or street, that will also increase safety. Potential criminals can see that the building is occupied and be deterred, or passers-by may notice illegal activity going on indoors and can alert the authorities.

Territorial Reinforcement: Having a property perceived as a cared-for and secure space can protect it. This is called territorial reinforcement, and it is done through social and maintenance tools. The primary component of territorial reinforcement is maintaining the premises. The broken windows theory is a criminological theory that the little things matter. If properties are not steadfastly maintained, they are more likely to be targeted by vandalism and thieves, as they display a lack of owner care. By maintaining a clean, cared-for appearance, buildings can discourage crime. Second, encourage building users to take ownership of the space. Users who feel proprietary concern for a building are more likely to notice and challenge strangers or people who don't belong, and report them to security or police if necessary. When visitors enter buildings, they should be screened—this can be a more formal, intimidating security checkpoint, or simply a soft reminder by a greeter or receptionist that they are entering a private space. Ownership of the space can also be encouraged by placing amenities such as refreshments and seating in common areas and requiring guests to wear visitor tags.

Access Control: Well-designed buildings take the proverbial high ground. They don't give criminals an advantage or an easy approach. The easiest way to accomplish that is to clearly delineate public versus private space, and control all paths to the building. Visitors should be guided—both visually and physically—to where they need to enter the building. Entrances and exits, fencing, lighting, landscaping, and other site furnishings can be placed to control pedestrian and traffic flow. For example, small shrubs can be placed between a sidewalk and driveway to deter pedestrians from walking into a traffic area outside of a crosswalk. Physical guides like architectural bollards and light posts force visitors to slow and navigate around them. Recent terrorist attacks have increased the prevalence of crash- and attack-resistant security bollards at military, governmental, and other buildings or spaces requiring higher security levels. Security bollards are more than a visual marker; they can be used to protect property and occupants from vehicle ramming attacks. Pedestrians can easily walk around them, but a well-placed bollard can greatly increase the building's physical barrier to cars, to remind them where they should and shouldn't go. Flexible bollards can instruct drivers where not to go but will bend and decrease damage both to the vehicle and the bollard itself in the case of impact. For paths where certain vehicles need to enter, but most visitor access must be restricted, removable bollards are also an option left standing, they will block vehicles from entering the driveway, but they can easily be removed or locked in a prone position to enable maintenance vehicles, for example. Access control should also take into account other, non-vehicle modes of getting into a building. Doors and windows should always be locked during non-business hours, and key control maintained. Access to ladders should be secured, and trees should not be placed within reach of windows.

I. Case Study-II

A. *Case Study: Cisco IT*

Cisco's global security network is a leading-edge enterprise environment and one of the largest and most complex in the world. Cisco customers can draw on Our real-world experience in this area to help support similar enterprise needs.

Enterprise Access Control: At Cisco Systems@, the corporate Security, Technology Systems (STS) team manages physical security for more than271 Cisco@ facilities in 50 countries worldwide. Their job is to make sure that only people authorized to have access to these Cisco facilities gain entry and to detect and respond to all unauthorized entries. Securely and cost-effectively controlling this access across the global enterprise is one of the primary challenges for Cisco. Based on the size and risk level of a facility, Cisco deploys security technologies such as intrusion detection and physical electronic security-access-control systems, including closed-circuit TV (CCTV), for surveillance. These technologies include Lock and key systems for doors, offices, desks, and cabinets Badge readers in front of doors or labs or locked storage rooms, and sometimes even elevators Video cameras in front of the entry and perimeter exit doors, elevators, and other strategic locations. Door-latch sensors and controls, motion detectors, glass-break detectors, and other sensors (including fire and smoke detectors) Together, these technologies help Cisco provide intrusion detection and physical access control. The information they gather is transmitted to centralized security operations centers, where it is reviewed and responded to by the STS department.

Challenge: The Cisco STS department faced the following challenges: Defining and developing a corporate physical-security philosophy. After meeting with executive staff members, philosophy was defined, which included a primary goal of providing 24-hour access to all Cisco employees. This enabled mobility and higher levels of employee productivity, making it easier for employees to work any time of the day or night while still maintaining physical security. Contractors, vendors, and other temporary workers were restricted depending on location or time of day. Defining and developing a corporate physical-security design standard. This standard was to be developed based on the corporate culture and, as always, a balance between culture, practical security applications, and costs.

Solution: Centralized Server Architecture and WAN Cisco STS developed centralized server architecture based on a single set of equipment standards, supported by regional security servers worldwide. These centralized servers were located in data centers that Cisco IT supports and connected to the Cisco human resources servers. Using the existing Cisco IP WAN, the centralized servers are linked to each other and to each access control system at each almost 300 Cisco sites worldwide.

Cisco IT required that the servers meet server and OS standards, which initially create extra work for the STS team. The advantage to IT is that it is easier to manage a limited set of standard servers. The advantage to the security and safety department is that it is no longer responsible for managing and maintaining its servers and software patches and updates.

The department can now concentrate on its primary security issues. Cisco also standardized the access control and alarm systems at every site and supports them with a single set of software tools. These standard systems are maintained by a global software and services vendor that provides technology compatible with the current security database system, and installs and supports the systems globally at a competitive price. Together, Cisco STS and the vendor developed the first true enterprise system solution. Database administration occurs at region-centric administration points and data records are reconciled and updated between all the servers on a present schedule. Cisco has a database of all its employee records that is updated when an employee joins or leaves Cisco. After a background check, new employees are added to the database and go to the local Cisco security office to obtain a badge with their pictures on it. Badges are unique to each employee and can be used only at Cisco locations. Not only is the employee's picture on the badge, but the embedded badge number is used to identify the employee every time the badge is used to open a door. The picture is copied from the regional security server to the global enterprise system and also copied to the employee directory where it is available to all employees. Access to company resources is determined by an employee profile, which is assigned automatically based on the person's employment status and geography and then customized according to individual job needs. Some engineers, for example, need access to special labs, whereas IT personnel need access to wiring closets. Because everyone has access to the employee database, building staff can compare the picture in the database with the employee in front of them if the employee has a lost or misplaced badge and needs building access. And because security personnel has access to this database and to IP video streams, they can view a video stream and compare a person on camera to the pictures of people who are authorized to be at that location.

Security Operations Centers: Security operations centers are the focal points for alarm management and response programs. All incident or event information is sent automatically from each office to the regional server and from there to the central server. All fire alarms, glass-break alarms, and door-opening alerts, in all about 60 to 80 monitor points per Cisco building, are sent to the regional and global Security Operations Centre (SOC). The SOC security personnel can log on to the closed-circuit video camera near an area in question and determine whether they should call the local private security patrol or the local police to manage an incident. Many alarms are "false alarms, for example, a secure door being held open by an employee, the wind, or a faulty door latch. Because the SOC can view each event in real-time using CCTV cameras over the corporate IP network, the number of false alarms that Cisco and the local police have had to respond to has significantly reduced. This benefit, coupled with the professionalism and skill of the SOC personnel, has helped to maintain credibility and good relationships with local police departments worldwide. The SOC also acts as a central emergency call center for Cisco employees. All emergency calls are routed to the nearest SOC personnel, who know where the call is coming from and are trained to respond immediately in an emergency. They alert the appropriate local emergency-response team and direct these teams to the emergency.

II. Results

From 1997 to 2004, Cisco has tripled in size, growing from 10,700 to more than 35,000 employees, and more than doubled the number of locations. During that time the STS team has remained about the same size mostly because of the efficiencies gained from automating many of its access-control systems and centralizing its management.

In the ongoing construction, the principle is meeting the strength requirements they have provided by securing a total designed solution environmentally which will result in expanding life expectancy for the building structure, design safety, and energy conservation.

III. Conclusions

- Studied the difference between safety and security.
- Safety is the condition of being protected from harm or other non-desirable outcomes. Safety can also refer to the control of recognized hazards in order to achieve an acceptable level of risk.
- Security is active measures any of device designed to guard persons and property against a broad range of hazards, including crime, fire, accidents, and attacks.
- Various types of safety and security measures were studied. Safety can be achieved only by means of architecture and security is achieved by means of mechanical applications.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING SUPPORT

The author declares that they have no funding support for this study.

REFERENCES

[1] Garold D. Oberiender, (2014); Project Management for Engineering and Construction, MHHD 0-07-18821-3

[2] Mredith, Mantl, Shaffer, Sutton, (2014), Project Management in Practice 5th Ed, John Wiley

[3] Jack R. Meredith, Samuel J. Mantel Jr, (2011), Project Management: A Managerial Approach, 8th Ed, John Wiley & Sons.

[4] Ofori, George; (2015); "Nature of the Construction Industry, Its Needs and Its Development: A Review of Four Decades of Research"; Journal of Construction in Developing Countries, 20(2), 115–135, 2015

[5] Yevseiev, Serhii & Aleksiyev, Volodymyr & Balakireva, Svitlana & Peleshok, Yevhen & Milov, Oleksandr & Petrov, Oleksii & Rayevnyeva, Olena & Tomashevsky, Bogdan & Shmatko, Olexander. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. Eastern-European Journal of Enterprise Technologies. 3. 49-63. 10.15587/1729-4061.2019.169527.

[6] Gomeseria, Ronald. (2019). "Planning, Design & Construction - Safety & Security Policy;" CEAI ViewPoint Journal; September 2019 Edition; Consulting Engineers Association of India. 10.17605/OSF.IO/4MPD2.

[7] Dennis Challinger, "From the Ground Up: Security for Tall Building", From the Ground Up: Security for Tall Building, ISBN-978-1-887056-90-8