2015

STANDARDS FOR PHYSICAL SECURITY MANAGEMENT IN INDUSTRY

A RESEARCH PAPER ON BEHALF OF

NATIONAL POLICE ACADEMY
HYDERABAD

Undertaken by

K Nityanandam IPS (Retd.)

1977 Batch

STANDARDS

FOR PHYSICAL SECURITY MANAGEMENT

IN INDUSTRY

UNDERTAKEN

BY

K.NITYANANDAM IPS (RETD) 1977 BATCH

Contents

1. Acknowledgement

It was during the tenure of Mr. V. N. Rai, in 2012, the then Director of the National Police Academy that the idea of undertaking a project to prepare standards of security management in Industry germinated. Dr. S. Subramanian, former Director SPG and NPA also gave valuable suggestions on the proposed project. It was felt that Industrial security is vast ocean and CISF is not able to provide security to anyone except public sector undertakings. The vast industrial sector in the country was left to the proficiency of Private Security service providers without any standards for operation. A document was therefore proposed to provide some guidelines and standards to private security service operators and also to police forces in the country to adopt a standard operation procedure to handle industrial security.

I take this opportunity to thank successive Directors of NPA, Mr. Subash Goswami, and Ms. Aruna Bahuguna for facilitating this project. Dr. Anil Saxena of NPA was also very helpful in many ways.

I wish to thank Mr. Arvind Ranjan, Director CISF who directed all his CISF units to assist me in this project. I must make special mention of the help rendered by Ms. Shyamala Dinavahi Sr. Commandant of CISF who helped me in many ways.

I also am grateful to many serving and ex CISF officers especially some of them presently employed in the private sector who have provided valuable inputs. I would fail in my duty if I do not take this opportunity of thanking research scholars from Nirma University, Ahmedabad for analyzing the data collected.

Special thanks to Mr.A.N.S.P. Sastry former Director of Bureau of Indian Standards with his valuable inputs on Statistical Quality control and Analysis
I am thankful to Mr.Venkata Ramana and Mr.Kasi Vishwanath of GMR for providing valuable inputs on Technology in aid of Security.

K Nityanandam IPS (Retd.)
Jan 2015

2. Preface

The whole world is agog with standards in practically every field. It is felt that standards improve quality and lay down a benchmark for measuring the quality. Standards have generally been incorporated in the manufacturing sector where the quality of a particular product is laid down and once it is accepted it becomes a base for which other manufactures can produce the product with similar standards. However standards are not available in service sector and it becomes very difficult to provide standards for any service since it is impossible to lay a benchmark due to various factors which are beyond our control and also due to various factors which are not common. This exercise aims to identify and lay certain standards in the security field which when incorporated would enhance the quality of security and provide better security to the assets of the organisation. This exercise has been possible with the active support of the national Police Academy Hyderabad. I would therefore thank successive directors of the NPA who have been supportive in this project. In addition all the field officers including, public and private sector industries, captains of industries, security specialists have been very forthcoming in their views on the standards required for any establishment especially industrial establishment.

3. Introduction

Globally, billions of dollars are invested in security systems including manpower to protect the assets of an organisation especially in the industrial sector. The quality of the systems has improved over the years considering that trillions of dollars are invested globally in various forms of industries, some of them critical and some not so critical. But the fact remains that industry has a massive investment and there is a felt need to protect these assets with a certain percentage of investment. However most industries do not feel the need to invest in security since is not quantifiable and the return on investment is virtually zero.

One of the reasons for the apathy of the industry towards security (surprising since they are trying to protect their own assets) is the absence of a standard practises for protection of assets of an industry. The standards include practises which are uniform for a given asset and systems which are effective to protect the assets from unauthorised interference.

It is therefore important for the security managers to visualise a set of standards to protect the assets. In the absence of standards different industries have different practises while not following a common practise which is best suitable to the organisation.

4. Need and Importance of the Study

A security management system of an Industry involves security and protection of the assets of the industry which can be in the following form:

1. Physical assets
2. HR assets
3. IT Assets

Since management of IT assets has been taken care of in ISO 27001, it is felt necessary to prepare a management system for the security of Physical assets and Human Resource Assets. The Management system will provide a direction for the Security set-up in the enterprise.

a) A Plan for the Security Governance
b) Implementation of the Security system
c) Validation of the system. It will ensure that the system is competent to the security threats specific to the enterprise.
d) Periodically assess the effectiveness of the system through an Audit Process
e) Periodically Reviewed by the Chief Executive
f) It will ensure continuing competence to the changing security threats
It is therefore proposed to undertake a project for preparing a set of standards for security of the Industrial sector

<u>Objective of the Study</u>

The primary objective of the study is to prepare standards for protections of physical assets in any industry. The study will not only cover public sector industry both critical and non critical but also private sector industry which are both critical and non critical in its operations.

4.1 Research Methodology

Methodology will be in three forms

1) Through primary data available
2) Secondary research by interpreting primary sources
3) Undertaking original Quantitative and Qualitative study

<u>Sample</u>

Industries both in private and public sector including critical industries will be taken up for study.

Tools and Techniques for data collection including procedure and methodology for analysis of data: It is proposed to undertake data collection in the following forms:

1) Systematic review of available literature

2) Data collection through both questionnaire and survey
3) Field visits to both Public and Private sector industries including Critical industries
4) Study the best and worst practices
5) Meeting captains of major Industries
6) Exchange of ideas with security experts

4.2 Industrial Security – An Emerging Challenge

Having set the basic guidelines for security standards, it is proposed to start this project with formulating a set of standards for Management of Industrial Security.

Industrial Security, as everyone is aware, is throwing grave challenges to the economic security of the nation with incidents like the attack in Mumbai in 2008 still fresh in every one's mind. Attacks by extremists in the East and North East and incidents reported in 2013 in Regency Ceramics and Maruti plant are indicators of the state of things to come in the Industrial security sector. Never before in the history of independent India has Industrial security faced such grave danger as it is facing now. Vital installation and critical infrastructure are very vulnerable to terrorist attacks. Major Private Sector Industries like Reliance Industries and Infosys are using the services of CISF which is an indication of the growing threat to the industrial security.

Looking at the threat perception, it is felt necessary to prepare a set of standards and procedures to be followed by not only Public Sector Industry but also by the Private Sector Industry for management of their security systems.

A Security Management System of an Industry involves security and protection of the assets of the industry which can be in the following form:

1. Physical assets
2. HR assets
3. IT assets

It is therefore proposed to undertake a project for preparing a set of standards for security of the Industrial sector.

Security

<u>What Is Security?</u>

The word security is derived from '*cura*' a Latin word meaning 'care' or 'concern'.

- Freedom from danger, risk etc.
- Freedom from apprehension or doubt; well-founded confidence
- Something that secures or makes safe; protection, defense
- Freedom from financial cares or from want
- Precautions taken to guard against theft, sabotage, stealing of proprietary secrets etc.

- Something given or deposited as surety for the fulfillment of a promise or an obligation (Webster's Dictionary)

While these form a traditional perspective, today security involves protection from un-warranted interference of:

1) Physical assets
2) Human Resource Assets
3) IT assets

Security is the combination of measures and resources, human and material aimed at securing an asset or activity from unlawful intervention.

Security is the implementation of a set of logical and systematic procedures and processes that when taken as a whole have the effect of altering the ratio of undesirable events to total events and a realistic plan of action to deal with major occurrences when preventive measures fail due to variety of practical reasons.

Security, thus is both

1) A process of activity and
2) A condition resulting from such activity

Essential Ingredients

Security is thus a

- A continuous activity
- A vital input in the system
- Both preventive & protective
- Which is not completely fool proof
- With an acceptable level of residual risk
- Striking a balance between security & facilitation

Security can be graded in five levels depending on the threat

- Minimum Level – Simple applications to prevent unauthorized external activities against the organization
- Low Level – To impede, detect and assess unauthorized external and internal activity
- Medium Level – to forecast, Impede, detect, assess and neutralize external and internal threats
- High Level – To facilitate complete protection including contingency/disaster management plan

- Maximum Level – Complete and integrated system to protect national level security interest

Changing Trends / Threat perception

- Hi-tech transnational terrorism - Area threat from rocket launchers, mortars excuse of Aero plane as missile
- Bureaucratic monoliths giving way to lean & flat organizations - Paradigm shift from man power oriented security system
- Emergence of knowledge economy- protection of intangible values like IPRs, Patents etc. - Paradigm shift from physical security to Security of Information & Cyber-Security.
- New forms of terrorism like Bio-terrorism & Nuclear terrorism
- Changing ratio of white-collar and blue collar workers - Decline of militant trade unionism - threat from under privileged sections if their aspirations are not met
- Decline of the economic basis of National State & emergence of the supra-national economy. - Rise of MNCs, NGOs etc.

Business can have continuity and growth only when these areas are protected. Interference with any of these facets of business would constitute a serious danger to the interests of the organization.

4.3 Principles of Security

- Industry is a vital organ of the nation's economy
- Protection of industry from all types of risks is essential not only for business continuity but also for sustaining the economy of the nation as a whole.
- We have seen the tragic cases of Bhopal gas leak and the attack on the Mumbai Taj and Oberoi Hotel which have caused immense financial loss, damage and loss of innocent human lives. In the ceramic industry, we have seen the tragic case of Regency Ceramics in Yanam being completely burnt down and one of their senior executive killed. At Regency Ceramics, it was the inability of the management to address security issues which led to this tragic situation. We also have the tragic case of Industrial unrest in Maruti, Gurgaon in 2013, where HR assets were seriously jeopardised
- Industrial security is replete with cases of breaches of security of industry which has led to innumerable financial losses to the undertaking.
- A small step in securing the industry from all threats goes a long way in providing a security blanket to the industry such as
    - Protect it from all possible threats
    - Maintain business continuity
    - Facilitate growth of the industry
    - Minimize and eliminate losses

- Most management feel that security is a non-productive investment. Security of an undertaking is left to a few permanent staff with possible army/CISF/police background and some private security personnel who are generally outsourced. Their visions on security and their basic credentials are suspect.
- Top management is generally not involved in security management
- Returns on investments in security are not monetarily quantifiable

Essential Ingredients of Security

- Should have authority
- Responsibility of the management
- A continuous activity
- A vital input in the system
- Both preventive and protective
- With acceptable levels of residual risks
- Balance between security and facilitation
- Cost effective
- Should be independent
- Should have authority

Physical Security Controls

Providing an organization or site with effective security involves several factors, some relatively obvious, others less so. The intent of Physical Security is to control access and prevent the interruption of operations protecting the assets in the process. These goals are accomplished using tangible countermeasures ranging from fencing and lighting to electronic surveillance equipment and carefully defined policies and procedures. In short physical security is essentially a combination of access control and effective surveillance.

Keeping in mind the actual Physical Security "controls" — the materials, equipment, and procedures used in securing a site — are only one element of an in-depth program of protection. Indeed, an effective component of many security systems is the perception of security both on the part of authorized personnel on site and potential intruders. Similarly, the use of barriers and lighting systems provide two important deterrents to potential intrusion:

Physical Deterrence

Psychological deterrence is a consequence of perceived impediments to successful intrusion. While an essential component of a comprehensive approach to security, Physical Security programs are only one aspect. To maximize effectiveness, security designers must include communications, access control, surveillance, and event reporting systems.

The system control being proposed will ensure proper

- Access control
- Adequate surveillance
- Monitoring movement of men material and trucks
- Manpower deployment to keep a watch on all activities in the plant

4.4 Vulnerability Assessment

No security can commence without a vulnerability assessment. Vulnerability assessment enables the management of the organisation to examine the depth and extent of security required for an industrial undertaking.

Vulnerability assessment is a systematic approach used to assess a business establishment's security posture, analyze the effectiveness of the existing security program, and identify security weaknesses. The basic process of a vulnerability assessment includes determining what assets are in need of protection by the facility's security program, then identifying the protection measures already in place to secure those assets and finding gaps which exist. Finally, the assessment measures the security program's effectiveness against valid security metrics and provides recommendations to security decision makers for improvements. In essence, vulnerability assessment assists business establishments and security decision makers in determining the need for additional security systems, equipment upgrades, policy and procedure revisions, training opportunities, and manpower needs.

Vulnerability assessment identifies security weaknesses that can be exploited by an adversary to gain access to the industries assets. For example, a vulnerability assessment may reveal an egress path that could be exploited by an infant abductor or it may identify a lack of patrols by security personnel in sensitive areas of the industry. The goal of vulnerability assessment is to ensure life safety, protect assets, and ensure continuity of operations. The driving forces behind vulnerability assessments include new legislation or regulatory requirements, mandatory guidelines, revised threat assessments with new or emerging threats, increased criticality of assets, and the construction of new facilities at the existing plant.

The vulnerability of an asset is determined by the potential weaknesses in operational processes and procedures, physical security weaknesses, and technical gaps which can be exploited to attack an asset. Vulnerability assessments are used to identify these weaknesses by way of a security survey. A security survey is a fact-finding process whereby the assessment team gathers data that reflects the who, what, how, where, when, and why of existing security operations of CERA. The purpose of a security survey is to measure the vulnerabilities at a facility or to specific assets by determining what opportunities exist to exploit current security policies and procedures, physical security equipment, and security personnel.

Since many factors determine the vulnerability of a unit, it is important for the management to indentify the vulnerable areas of the plan and formulate their security policies.

In order to provide a total security cover, it is important for the management to examine the following:

Identification of Assets

In this context, the first step which an industry should undertake is an Asset Overview comprising of identification of assets by survey which should include among other things:

- **Property**: Infrastructure, stores, vital installations
- **Human Resources**: Employees, contract workforce, visitors/vendors
- **Information**: Blue prints, process documents, business data

Once assets are identified, it is important to classify them in terms of their importance to the industry/organization and prioritize them in terms of their value/importance - both tangible and intangible to the organization.

When once the assets are identified, the next step would be to identify the threat perception to these assets.

Threat Perception

Management should be able to understand and perceive the threat to the assets of the organisation.

Threats can be multifold and can be related to:

- **People**: Assault, murder, kidnapping
- **Material**: Theft, pilferage
- **Infrastructure**: Sabotage, accidental damages, natural calamities
- **Information**: Hacking of IT systems, stealing of information

Threat perception enables the management to identify areas of threat which would enable them to plan their security. Threat perception and vulnerability assessment are closely inter-related.

4.5 Standards and their Relevance

Why standards in police/security setup?

We in the police have seen a phenomenal growth in the role and responsibility over the last six decades. The original concept of policing has undergone a sea change with a large number of issues to be addressed which a few years back were beyond the realm of imagination of the police. Police duties and responsibilities have become more complex. Police is not just a law and order enforcing or a crime detecting agency. It has been entrusted with diverse duties and responsibilities. With increasing media, judicial and public activism, the accountability of the police has come under close scrutiny. Police action or the lack of it is being questioned and expectations for delivery are increasing day by day.

Though police operation procedures have undergone many changes, many core issues concerning the police have remained unaltered - both in the legal format and operational format. The Police Act is of 1861 origin and the IPC is of 1860 origin. The Criminal Procedure Code of 1898 has been amended in 1973. Thus archaic police laws are not keeping pace with the changing security scenario in the country. Hence we see a plethora of problems emerging every day which these archaic laws are unable to handle or tackle.

On the operational front, many practices of the colonial times continue to be in force even today without undergoing any transformation to meet the needs of the changing times and roles and responsibilities.

In a vast country like ours, with multifarious cultures and problems affecting the police, a uniform system of handling core police and security issues is found wanting. Each state has its own set of procedures and practices in police functioning. Though police is a state subject, a certain amount of federal control exists.

Our experience has shown that police efficiency has received a major beating due to varied factors and one of the main reasons is the lack of uniformity of practices in the absence of set code of standards applicable across the board all over the country. Policing in many areas is still a fire fighting operation without any set of standard operating procedures.

Need for Standards

Given the above situation, it is felt necessary to lay down a set of standards for police/security functioning (making allowance for regional variation) uniformly across the country and among all police and security agencies. It is now universally acknowledged that the standards as laid down in ISO 27001 in Information Security Management System have stood the test of time and are being used globally by everyone who want to secure their Information Management Systems.

What are Standards?

A standard is an agreed, repeatable way of doing something. It is a published document that contains a technical specification (when it comes to manufactured goods) or other precise criteria, designed to be used consistently as a rule, guideline or definition. Standards help to make life simpler and increase the reliability and effectiveness of goods or services. Standards are created by bringing together the experience and expertise of all interested parties aimed at achieving the optimum degree of order in a given context.

International standards such as those from IEC, ISO and ITU are crucial for increasing efficiency. This issue has come to the forefront as global challenges like sustainability and financial uncertainty mean that organizations are challenged to achieve better results with less waste.

Quite simply, efficiency indicates the ability to achieve objectives by implementing processes to develop products or services of optimal quality with minimal waste, expense or unnecessary effort. It helps organizations maximize profits and meet their goals, and is crucial for success in today's challenging and competitive economic environment. For example the British standards have the following criteria

Specification
Standard that sets out detailed requirements, to be satisfied by a product, material, process, service or system, and the procedures for checking conformity to these requirements.

Method
Standard that gives a complete account of the way in which an activity is performed (and, where appropriate, of the equipment or tools required to perform it) and conclusions are reached, to a degree of precision appropriate to the stated purpose.

Guide
Standard that gives broad and general information about a subject, with background information where appropriate.

Vocabulary
Standard listing definitions of terms used in a particular sector, field or discipline.

Codes of Practice
Standard comprising recommendations for accepted good practice as followed by competent and conscientious practitioners, and which brings together the results of practical experience and acquired knowledge for ease of access and use of the information.

Benefits of Standards
In view of different sets of procedures and practices used by different police/security organizations with sometimes conflicting results, it is felt that a set of standards for police operations would

- Improve efficiency of the police

- Reduce cost of operations
- Improve delivery
- Reduce monotony in repetitive activities
- Provide for standard operating procedures
- Provide easy access to data for all purposes including inspection
- Increase accountability
- Provide a proper frame work for command and control

Definition of 'Standardization'

- A framework of agreements to which all relevant parties in an industry or organization must adhere to ensure that all processes associated with the creation of a good or performance of a service are performed within set guidelines. This is done to ensure the end product has consistent quality, and that any conclusions made are comparable with all other equivalent items in the same class. (Investopedia)
- In standardization we look for consistent level of quality

Why do we need standards?

Standards can be found throughout our daily lives but why do we need them?

Rather than asking why we need standards, we might usefully ask ourselves what the world would be like without standards. Products might not work as expected. They may be of inferior quality and incompatible with other equipment, in fact they may not even connect with them, and in some cases; non-standardized products may even be dangerous.

Standardized products and services are valuable User 'confidence builders', being perceived as:

- Safe
- Healthy
- Secure
- High quality
- Flexible

As a result, standardized goods and services are widely accepted, commonly trusted and highly valued. Standards provide the foundation for many of the innovative communication features and options we have come to take for granted, and they contribute to the enhancement of our daily lives - often invisibly.

We need look no further for evidence than the GSM™ (Global System of Mobile Communication) standard which facilitates mobile communication the world over between (for example):

- Friends and relations
- Hospitals
- Business
- Schools
- Industry
- Emergency services
- Airports
- Governments

Are established and accepted the world over. ICT (Information and Communication Technology) standards are vital for efficient manufacturing:

- Contribute to better regulation
- Enable multi-market access
- Create active markets
- Encourage innovation
- Improve communication

Standardization brings important benefits to business including a solid foundation upon which to develop new technologies and an opportunity to share and enhance existing practices.

Standardization also plays a vital role in assisting Governments, Administrations, Regulators and the legal profession as legislation, regulation and policy initiatives are all supported by standardization.

Challenges

There is no doubt that a huge wave of privatisation is sweeping across nearly all aspects of the international security sector bringing a number of important challenges

Lack of Coordination among Different Security Providers

With private or individual interests purchasing security services to protect their particular interests, the model is moving away from a state-monopolistic, state coordinated security provision to one in which many different unrelated actors provide security on an *ad hoc* basis. This decentralisation of security can create situations in which security coverage is patchy, resulting in both gaps and overlaps. In the area of SSR,(Security Sector Reform) the lack of a holistic approach among the different actors of the larger security sector (such as, police, armed forces, border guards, judiciary and prisons, parliaments and civil society) can undermine the long-term sustainability of reform efforts, such as the training by PMSCs of police forces.

Lack of Effective Oversight and Accountability

Related to the decline of traditional state-centric security systems is the breakdown of effective oversight and accountability mechanisms. Where the state has less control of private security forces, it also has less ability to hold such actors accountable when violations occur. As most "hard law" depends upon a state's ability to enforce it within its territory, the ease with which private actors cross borders and can escape territorial reach undermines the enforcement of both national and international law.

Asymmetry in Security Provision

The private contractual nature of these services means that Private Maritime Security Companies (PMSC) contracted security obligations run to their clients, but not to the public at large. This can create an asymmetric situation in which some are provided with more security than others. Furthermore, the security measures employed to protect paying clients may negatively impact on those not-paying. This shift in obligation from providing security for the "common good" to that of the paying client has huge implications for how security is provided generally. It stands to reason that in this new paradigm, decisions on how security should be provided would begin with the client's needs, followed by those of the wider community. At the same time, it may not always be the client's best interest that guides decision-making. For example, it has been suggested by one journalist that the scope and duration of training programmes were extended beyond what was appropriate in order to secure the greatest possible return on investments.

The International Code of Conduct for Private Security Service Providers (Detailed code at the end of the research paper)

In response to industry demands to develop international standards for private security service providers, the Swiss government launched another initiative to develop an *International Code of Conduct for Private Security Service Providers* (ICoC) which would articulate clear standards for private security providers based on international human rights law, as well as develop an independent oversight and compliance mechanism to provide effective sanctions when the ICoC is breached, as well as remedies to victims. Once again developed through a multi-stakeholder approach, including private security companies, states and civil society, the ICoC was finalised and signed by participating companies in November 2010. The ICoC uses contractual mechanisms to impose human-rights compliant standards *directly on the companies themselves, regardless of where they are operating*. Currently, the ICoC is in an institution-building phase led by a multi-stakeholder Steering Committee to develop the operational framework for the oversight institution. It is expected that this framework will be completed by the end of 2011, and the institution should be functioning shortly after that.

In a time of increasing security threats—both public and private-- which affect states and a multitude of private actors, as well as decreasing state capacity to meet those threats, the trend to use private military and security companies will likely continue to increase and shape international security. In defiance of the traditional paradigm of state-centric security, these private security actors pose real challenges to effective regulation of their services, particularly accountability for violations of human rights and remedies to victims. However, these actors can also challenge security provision in a positive manner, through innovations and the possibility of cost-effectiveness that may be welcome in diffi cult economic times. The recent trends towards privatisation of security and the impact of international business on the enjoyment of human rights have also served as the impetus to forge surprising alliances among states, industry and civil society groups. These multi-stakeholder efforts may be able to find real solutions to some of these challenges, building innovative and flexible frameworks that can respond to the confluence of global, economic and human security that characterises today's 21st century world.

How Security Standards have Evolved

Standards in security are unheard of even today. But with the explosion in the Information Management system and with trillions of US dollars at stake and breaches of eh Information Management system increasing manifold with huge losses of data to companies, it dawned on security manages that some standards should be evolved to protect the Information Assets and thus the Information Management System Security evolved in 2005.

ISO/IEC 27001 - Information Security Management

Security management system today incorporates standards which so far have been alien to security managers all over the world; both in the private and public sector. It was only in 1995 that an Information Security Management System was incorporated which ultimately crystallized into the ISO 27001 standard IN 2005.

The Information Security Management System is a set of policies concerned with Information Security Management on IT related risks. The need for this arose since IT was being extensively used globally for all transactions going beyond geographical boundaries

ISO 27001 is essentially an Information Security Management System that is intended to bring Information Security under explicit management control.

All security and police organizations have a number of controls but without a management system, the controls tend to be disorganized and disjointed having been implemented as a point solution to specific situations or simply as a matter of convention.

Security controls typically address certain aspects of IT or data related security leaving non IT information assets, (public work or proprietary knowledge) less protected on the whole. Business security and physical security planning need to be managed independently. The ISO 27000 family of standards helps organizations keep information assets secure.

Using this family of standards will help any organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

4.6 ISMS

ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. It can help small, medium and large businesses in any sector keep information assets secure.

The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)". Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization" - ISO 27001 Directory.

Security managers all over the world seem to be satisfied with formulating ISMS. However it should be realised that physical security and HR security are equally important. Unfortunately no systematic effort has been made in any part of the world to evolve a set of standards for physical security management. It is now the need of the hour to lay down some physical security standards so that there is a direction to security management of this essential and vital input of industry.

Physical Security Management Systems

5. Physical Security Management Systems

Physical security comprises of methods and devices which are designed to prevent losses through theft, espionage, sabotage or any other kind of intentional damage of any industrial establishment. There are various aspects of physical security which when studied and implemented and incorporated in the security policy of the organisation go a long way in providing fool proof security to the organisation. The major physical security components include:

1. Perimeter and fences
2. Gates and their management
3. Watch towers
4. Access control systems
5. Surveillance systems
6. Manpower management
7. Control room and its management
8. Patrolling
9. Protective lighting
10. Fire alarm systems

The research paper attempts to examine all the above systems by providing various requirements for effective installation of these systems and the need to have specific standards which when applied and practised would go a long way in ensuring a near fool proof security for the organisation. The level of security may vary from industry to industry depending on the volume of assets being protected and the criticality of the industry or the manufacturing process. All industries may not face the same physical security requirement and thus the equipment, manpower deployed may vary from place to place. Additionally all industries may not require the various technological devices enumerated here. But the specific industry may implement those which are required for specific threat perception of an industry

Manpower is the core of physical security and this paper tries to examine the standard manpower requirement and their strengths and weaknesses in various industries. But manpower alone cannot provide security. It has to be complemented by systems and both these together can provide effective security.

Physical security essentially involves effective access control and surveillance through a proper mix of manpower and technology

5.1 Perimeter Security System

The first defined boundary of the premises is the perimeter wall. This not only defines the boundary of the organisation, it also acts as the first line of defence to any organisation from any unauthorised intrusion. It is therefore important that a well designed boundary would ward off any potential threats from unauthorised intrusion. Perimeter acts as a barrier which can be both natural and artificial.

Physical Barriers

Natural Barriers

Mountains, cliffs, sea, marsh, desert & other geographical features near around the protected premises. Though these may look quite formidable, a determined intruder can surmount them. Therefore, even if there appears to be a seemingly impenetrable Natural barrier, it should be constantly kept under watch by security personnel. There is no such thing as a Natural barrier that cannot be penetrated by the miscreants. Their presence should not make security authorities complacent.

Man-made Physical Barriers

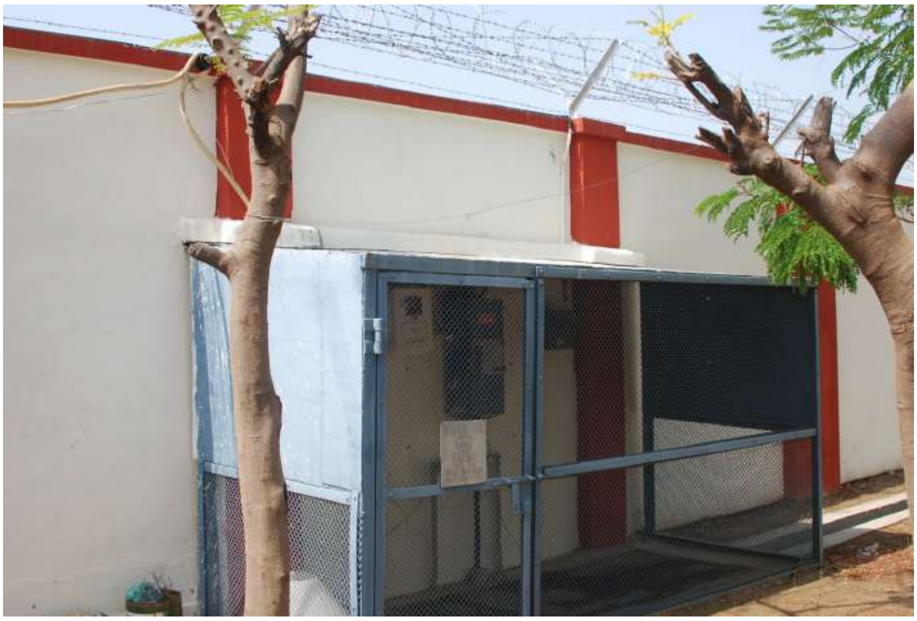
Perimeter Wall and Fencing

- First obstacle the miscreant ill encounter, this not only deters the miscreants from getting access into the complex but also prevents employee theft, pilferage and unauthorised removal of materials.
- An ideal arrangement of protection, which is cost effective in the long run, it is intrusion proof and of masonry and concrete constructions built to a height of 8 feet from the ground level.
- A perimeter wall is a physical security measure which is designed to prevent unauthorised entry and access into the physical limits of the industry by unauthorised persons.
    a. An ideal arrangement for protection
    b. Cost effective in the long run
    c. Intrusion proof
    d. Perimeter wall should be of masonry or concrete construction
    e. Height of wall should be 8 feet from ground level
    f. If ground is undulating, at any given point the effective height of parameter wall should be 8 feet
    g. On the top of the wall, an overhang of barbed wire/concertina coil to a height of 2-4 feet should be fixed
    h. This overhang should be fixed on the wall at an interval of 8 to 10 feet

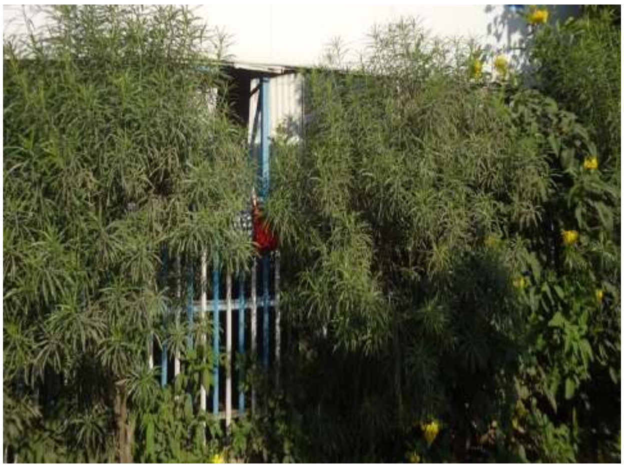
i. Cast iron angles of the shape of 'Y' should also be fixed at the same gap
j. The base rod will be 3 feet long & angles will be 18 inches long
k. Three strands of barbed wire should be fixed on the arms of the angle and 4 strands fixed on the base rod
l. Thus effective height of parameter wall will be 12 feet
m. As an added measure, instead of the overhang, infrared beams can be fixed at effective intervals keeping in mind the requirements of "Line of Sight"
n. Electric and telephone poles and fully grown trees should not be allowed near boundary wall
o. If it is not possible to remove them, anti climbing devices like spikes, barbed wire rods should be provided
p. On either side of the wall the ground should be clear of wild growth and bushes
q. Motorable road should be created all around the wall outside
r. Inside, a pathway for the security personnel to patrol the parameter wall should be provided
s. Slums should not be permitted alongside parameter wall
t. Creates legal liability against the intruder
u. Delays intrusion

An ideal perimeter wall with overhang fencing

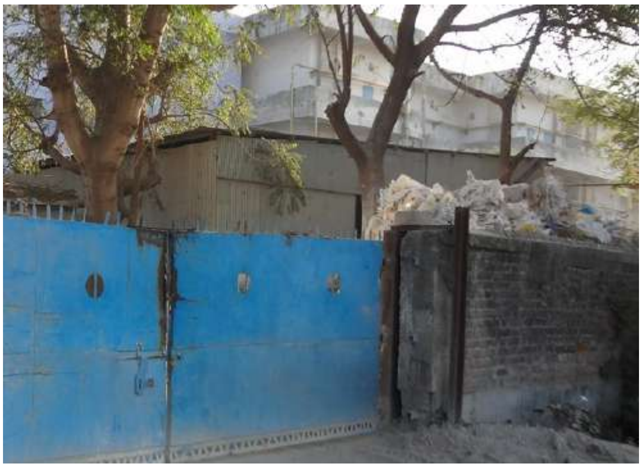
Deficient perimeter walls



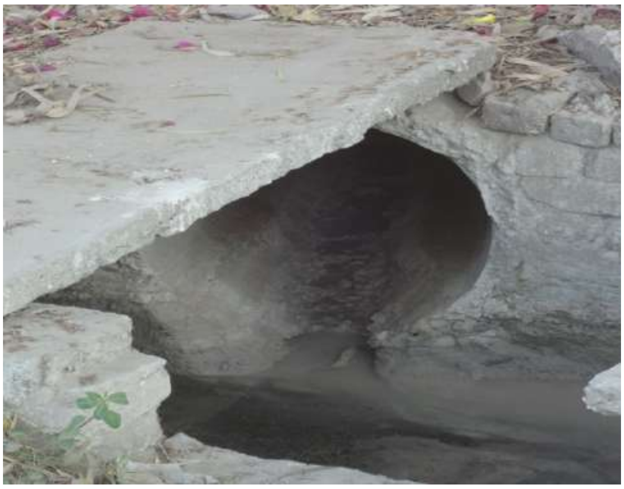
Wild growth at the fence



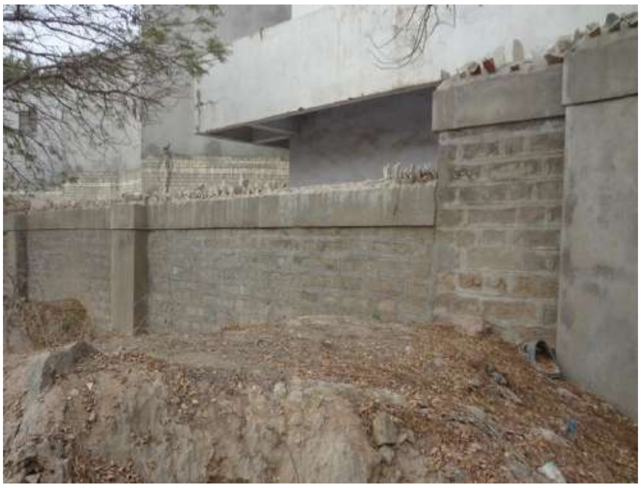
Waste material stacked at the perimeter wall



Open drain without iron grill



Mound near the perimeter wall



Perimeter lighting:

a) Whether a wall is constructed or a chain link fence is erected, the perimeter should be clearly lit during the night
b) Ideally, the light should illuminate a total area of 25 feet on either side of the wall.
c) The cone of light should point outwards & downwards
d) There should be no glare affecting the patrolling security personnel
e) Sodium vapour or halogen lamps have been found effective
f) The perimeter lighting arrangements should be linked to the emergency power supply so that it can function even during power failure
g) The overhang and fence can be energized using solar panels which give non lethal shock when contacted by an animal or a human being
h) Under no circumstances, high voltage industrial or domestic current should be directly connected to the fence

Existing practices in the Industry

The perimeter wall is generally a brick & mortar or concrete wall about 10 or 12 feet high running along the boundary of the property owned by two industrial undertaking. Sometimes it may not include the entire area if the area is very large and may only be built around the plant & machinery which require protection. In order to make the perimeter wall more effective against intrusion an overhang is provided at the top of a wall comprising angle irons and barbed wire. An overhang is sometimes also called a top guard. The overhang comprised of a series of angle irons projecting out of the top of the wall for about two feet at intervals of 8 to 10 feet all along the wall. Strands of barbed wire are strung along these angles irons spaced six inches apart.

Deficiency of the System

(a) It is costly
(b) Restricts the vision of the security personnel outside the perimeter wall
(c) It has to be kept under constant observation

What should be an ideal situation?

The perimeter wall by itself cannot prevent intrusion by a determined intruder. In order to make it ideal of effective barrier the following measures have also be taken:

(a) The entire perimeter wall should be lit up during hours of darkness to prevent entry by scaling over or breaking the wall.
(b) The entire lengths of perimeter wall should be kept under observation by security patrols or security personnel.
(c) Both the inner and outsides of wall should be kept clear of vegetation or any type of construction for a distance of 20 to 50 feet on either side depending on the area and the height of the wall. Electric or telephone poles should not be erected closer than 5 yards from the perimeter wall.
(d) Sometimes it becomes necessary to provide small openings in the wall for the purpose of drainage etc. These openings must be provided with strong iron grills.
(e) Quite often loose earth, waste material, scrap etc., is dumped just outside the perimeter wall. As a result the ground level outside the perimeter wall keeps rising and after sometimes the perimeter wall is only a few feet high from the outside and becomes easily crossable. Therefore, no such dumping as earth etc., should be permitted next to the perimeter wall.
(f) As an added measure, instead of the overhang, infrared beams can be fixed at effective intervals keeping in mind the requirements of “Line of Sight”.

Standard Norms

The perimeter wall should be of masonry or concrete construction built to a height of 8 feet from the ground level. If the ground is undulating, at any given point, the effective height of the wall should be 8 feet.

On the top of the wall, an overhang of barbed wire to a height of 4 feet should be fixed. This is done by fixing on the wall at an interval of 8 to 10 feet, cast iron angles of 'Y' shape. The base rod will be 3 feet long and angles will be 18 inches long. Three strands of barbed wire should be fixed on the arms of the angle and 4 strands to be fixed on the base rod. Thus the effective height of the perimeter protection system will be 12 feet. As an added measure instead of the overhang, infrared beams can be fixed at effective interval keeping in mind the requirements of 'Line of Sight'.

Electric and telephone poles and fully grown trees near the perimeter wall enable people to jump over the wall. To prevent this, if it is not possible to remove them, anti-climbing devices like spikes, barbed wire rolls etc. should be provided. On either side of the wall, the ground should be cleared of wild growths and bushes and a motorable road should be created all around the wall outside. Inside, a pathway for the security personnel to patrol the perimeter should be provided.

It is often seen that around industrial complexes slums develop and people use the perimeter wall as a support for construction of their huts. This should not e allowed as it defeats the very purpose for which the wall has been constructed. These huts will enable the criminals to hide and attack premises whenever suitable. These huts will also enable stolen items to be stored.
The perimeter barrier standard for India is a concrete composite wall with allowable soil bearing 1000 PSF, foundation concrete 2000 PSI, hollow concrete masonry 675 PSI, reinforced steel 20,000 PSI and joint reinforcing 30,000 PSI.

PSF – Pounds per square feet
PSI – Pounds per square inch
PCF – Pounds per cubic feet

Importance of Perimeter Wall

- It defines the limits of the property of the undertaking
- It physically prevents entry into the productive area of the property owned by the industry
- It creates a legal liability against the intruder
- It delays intrusion and help in detection of any intrusion if it takes place

- It channelized the entry & exit of men and materials
- It helps in the economy of manpower and effective utilisation of security personnel
- It acts as a psychological barrier to potential criminals
- Walls define the outer most boundary of a protected area to deter accidental or casual intruders from entering
- Fences define the surveillance region of an exterior intrusion detection system (PIDS or guards) an assessment system (CCTV or guards) and associated exterior security lights
- Fences and walls are used to channel and control the flow of personnel and vehicles through designated entries into the site and need to have the same level of protection and vehicle resistance and the entry control facility

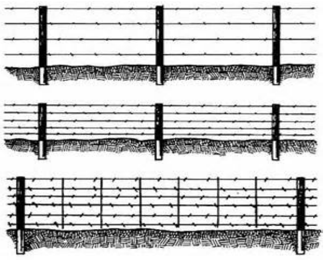
Fences

In some industries which occupy a very large are it may not be economically feasible to build a perimeter wall for the entire length of the boundary and yet it may be felt necessary to prevent the entry of unauthorised persons for security reasons. In such cases fences are erected to achieve the objective of access denial/delay.

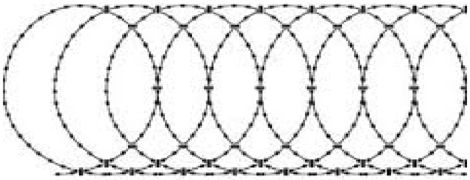
Types of Fences

1. Chain link fence : It is made up of thick wire mesh (8 gauge or heavier)
    - The bottom of wire mesh should not be more than 2 inches above the ground if the soil is hard
    - If the soil is soft, it should be embedded in the ground to prevent intruder from digging under the fence.
    - The metal/concrete post and the fence should be at least 8 feet height
    - The post should be provided with 2 feet overhang with barbed wire strands at intervals of 8 inches
    - The wire mesh fence should be firmly fastened to the posts by means of welded hooks or shaped bolts

2. Barbed Wire Fence:
    - It is made up of rods of barbed wire fixed horizontally on to a rod of metal, concrete or wooden posts forming a barrier.
    - This fence can also be fitted with and overhang to make it more difficult to scale over.
    - The posts are made of strong angle irons upto 7 feet above the ground level with a 2 feet overhang projecting outwards.



3. Concertina Coil Fencing:
    - It is erected by using coils or barbed wire.
    - The coils are 3 feet in diameter and are fixed between parallel posts stretching them out like a coil spring.
    - The bottom coil should be fixed to the ground by means of steel pickets driven into the soil.
    - The stretched coils are placed one above the other to make a 6 feet high barrier.



4. CGI (Corrugated Galvanised Iron) Sheet Fence:
    - It is made up of corrugated galvanised iron sheets.
    - The CGI sheets are nailed into sturdy wooden posts or fixed on metal pots by means of nuts and bolts.
    - The height of this barrier should be at least 8 feet.

Ideal Situation

All types of fences may be mounted with security gadgets, vibration detector, power fence and erection of different fences concerting & barbed.

Advantages

- Cheaper than perimeter wall
- Quickly erected
- Clear visibility
- Can be used when permanent barrier is damaged
- Beatification

Disadvantages

- To be kept under constant observation
- Easy to damage or cut
- Security problem can be raised due to clear visibility

Power Fence

Objective

The power fence system is a pulsating current system capable of active perimeter protection and zone wise intruder/alarm monitoring and detection. It not only deters would be intruders by regulating pulsating high voltage electrical energy but also delays an intruder's entry to and exit from the protected area. Ultimately, the Power Fence system effectively denies entry.

Application

Power fence systems have varied application in Agricultural, industrial and forestry/plantation sectors. With increasing crime in urban areas, this proven technology has now been adapted for domestic security application too.

Specification

- A power fence is an active fence which not only stops intruders but also detects tampering of the system. The energiser which powers the fence emits high voltage pulses every 1.2 seconds. Any person who attempts to trespass receives a painful but a safe shock. The shock is completely safe as it lasts only 300 millionth of a second.
- For example our system is solar powered with built in battery to last for one week on full charge. Its length is 100m. The required DC voltage of about 8 KV which is pulsating

with the current range of few milli lamps, is generated using from 12 V batteries and associated electronics.

- It gives an alarm when cutting or shorting the terminals is done with a view to disable the system.
- Power Consumption (AC) : 40 Watts
- Aux. DC output : 13.8 VDC 100
- MA. Power break up: 12 v @ 90 AH Maintenance free battery
- Typical HV Output : 4.5 KV to 8 KV on the fence
- Alarm inputs: Reconfigurable fence channels. Panic/alarm

Taut Wire Fence System

A physical barrier fence with integrated intrusion detection capabilities, typically installed along the perimeter. Taut wire should be a deterrent and detection fence with very high probability of detection while maintaining extremely low nuisance alarm rates. The system should reliably detect attempts to climb, cut or spread the fence wires. Taut wire, in conjunction with magnetic switches, may be considered for perimeter gates, either in sliding or double swing configurations.

Specifications

The Taut Wire fence should comprise of wires that are tensioned to a specific force and anchored to anchor posts. The Taut Wire fence is to be divided into zones/sections (the length of each section is determined according to the requirements of the complex, but cannot exceed 50 meters) allowing the control centre to receive an accurate zone of the intrusion attempt. Intrusion attempts carried out simultaneously at a number of sections will be reported to control centre as independent events. An inoperable section will not interrupt the operation of other sections. A detector post installed in the middle of each zone responds to characteristic forces that represent an intrusion attempt. Communication between all detector posts and the Control Centre is accomplished via a communication cable that is routed along the fence. In case of an intrusion, the detector post responds by generating an alarm which is transferred to the Command and Control centre and is annunciated both audibly and visually, displaying the exact location of the intrusion attempt. The typical Taut Wire fence will be installed on a concrete belt, anti-tunnelling strip that adds to the fence’s stability and longevity while creating a sub-terrain barrier as well.

The Taut Wire fence consists of the main following components:

- Anchor posts
- Detector posts and detectors
- Barbed wire
- Communication system

- Field Analyzers

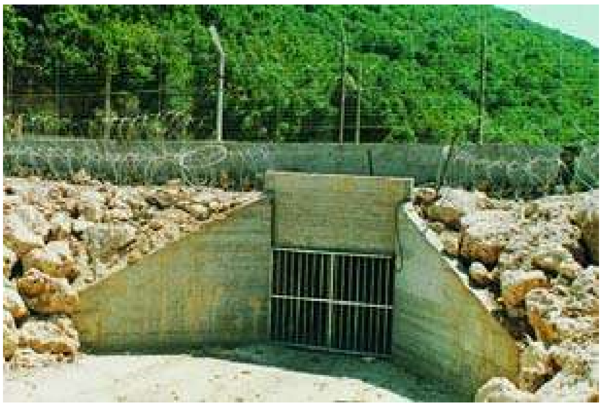
The system shall generate an audio and visual indication for each section separately, indicating the section number. Each gate (main, vehicles, pedestrians, etc.) shall be identified as a separate zone in the system.

System Description

The system shall be a taut wire outdoor intrusion detection sensor system based on the technology of the detection field and formed by a grid of taut wires connected to the sensor switches. Any change in the tension of the taut wires is transferred to the sensor switch which transfers this data along a communication cable to a computer for indication. The taut wire system shall be configured in an in-trigger configuration on perimeter wall with a total length of one (1) meter with concertina coil.

Intrusion Detection Grid

Intrusion detection grids provide detection for water passageways around the perimeter. Installed on the internal side of the perimeter; the grid is mounted on rails, which provides unrestricted access for maintenance. A non detection grid can be installed on the public side of the passageway to deter intrusions.



Intrusion detection grids will be installed along the perimeter to protect from intruders passing through waterways and other openings that exist along the perimeter. The grid will be of an epoxy cast type with a copper sensor cable interwoven among the grid rods and frame. It will be strong enough to prevent sawing and dense enough so that a man cannot penetrate but at the same time will allow the water and waste to flow. Any attempt to enter the complex through the grid will be detected and an alarm will be sent to the control room. This connection is based on Dry Contacts and does not require any power supply. It shall be possible to remove the grid for cleaning the waterway for any waste that has accumulated. The grid should be raised manually or electromechanically. A high security lock + a magnetic switch of a heavy-duty high security type will be installed on the grid as well. Each grid will be connected to the system computer according to an agreed-upon selection to enable the immediate identification of the location of the alarm, so that intrusions through the waterway can be detected immediately

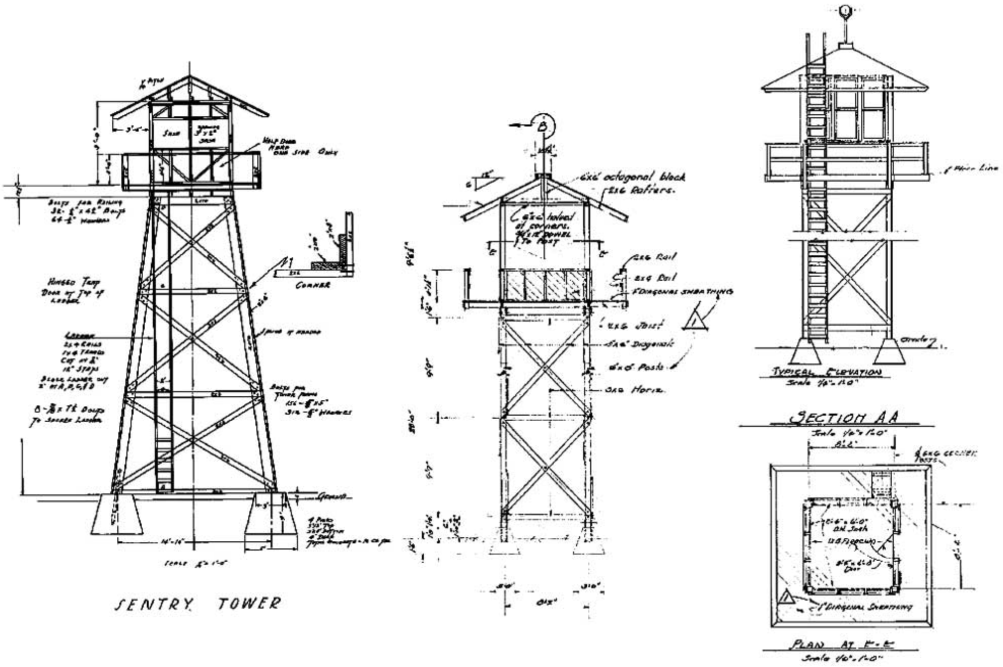
5.2 Watch Towers

- A watch tower (observation post) is an elevated platform from which security personnel can watch/observe certain areas
- To provide security cover to a larger area
- To watch the area in and outside of the perimeter wall and fencing
    - To prevent any criminal activities (such as sabotage, intrusion etc.)
    - The height of the watch tower should be between 5-10 meters depending on the area it is covering
    - From perimeter wall it should be at least 3 to 5 meters, adjoining the patrolling roads
- The cabin of watch tower should have unbreakable glass windows or iron grills.
- Should have revolving lights
- Should have modern communication devices & gadgets (walkie-talkie ,binocular etc.,)
- Should have log book
- Should have ladder
- Should have long range search lights
- Can be fitted with a siren also

<u>Duties of Sentry at Watch Tower</u>

- Sentry should not leave the watch tower without reliever
- Record the events in log book
- Convey situation report to the control room every hour about his area
- He should know how to operate the security equipments
- Familiar with whistle code, hand and light signals

The sentry guarding the watch tower should have easy view of both the perimeter wall and beyond


Sash
3'x 5' Sash
Half Door Hand One Side Only
Bolts for Railing 32- ½" x 4½" Bolts 64-½" Washers
Hinged Trap Door at Top of Ladder
Corner
Ladder
2x4 Rails
Cut at 8"
12" Steps
8 - ⅝ x 7½ Bolts To Secure Ladder
Bolts for Tower Frame 156 - ⅝" x 5" 312 - ⅝" Washers
Ground
14'-10"
Scale ⅛" = 1'-0"
SENTRY TOWER
B
6x6' octagonal block
2x6 Rafters.
4x4 halved at corners. ¾"x12" DOWEL To POST
2x6 Rail
2x6 Rail
1" DIAGONAL SHEATHING
2x6 Joist
4x4" Diagonals
6x6 Posts
2x6 Horiz.
Floor Line
Grade
TYPICAL ELEVATION
Scale ⅛" = 1'-0"
SECTION AA
Scale ⅛" = 1'-0"
6x6 Corner Posts
2'-6" x 6'-0" D.H. Sash
1x8 Flooring
2'-6" x 6'-8" Door
1" Diagonal Sheathing
PLAN AT E-E
Scale ⅛" = 1'-0"

5.3 Gates

What is a Gate?

It is the entry/exit point for

- ✓ Men
- ✓ Material
- ✓ Vehicles

Into any premises

Purpose of Gates

- ✓ Regulate the entry/exit of unauthorized persons
- ✓ Regulate the entry /exit of an authorized vehicle
- ✓ Helps to detect crime and criminal
- ✓ Helps to protect the undertaking during strike
- ✓ Helps to stop the unauthorized entry
- ✓ Helps for smooth functioning of undertaking

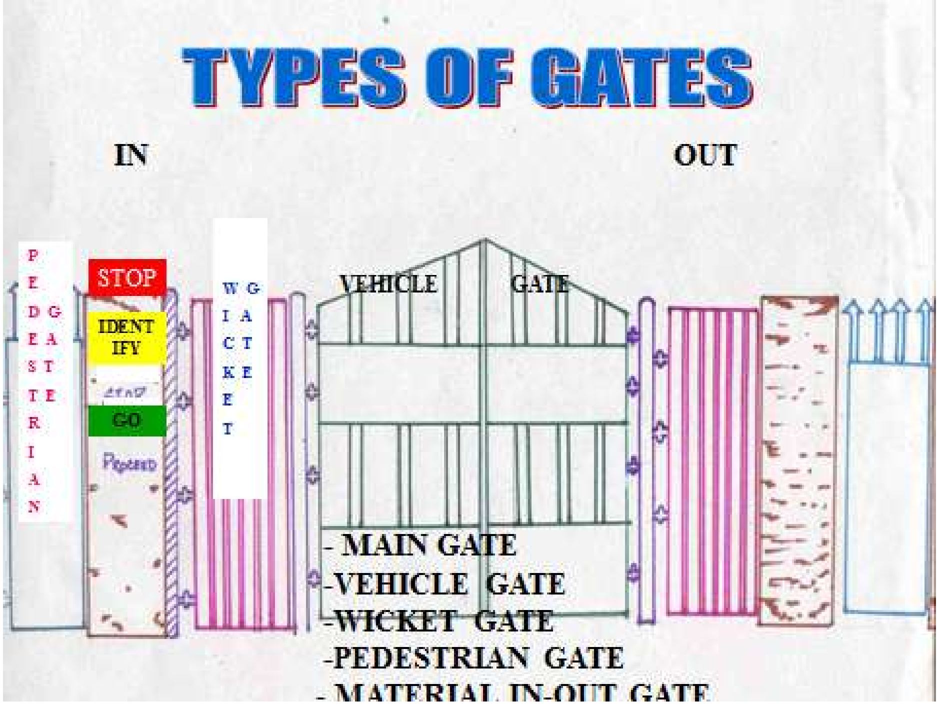
How the gate should be

- ✓ Since the gate will be the outlook of the Industry it should be constructed beautifully
- ✓ There should be sufficient parking place inside as well as outside the gate
- ✓ There should be a road barrier operated mechanically and manually
- ✓ There should be a railing at cyclist as well as pedestrian gate
- ✓ There should be a visitor's room
- ✓ There should be a control room

- ✓ Adequate lighting arrangement must be there
- ✓ Adequate security staff
- ✓ CCTV

Types of Gates

- ✓ Vehicle gate
- ✓ Employees’ gate
- ✓ Railway gate
- ✓ Material Gate



Ideal Features of Gates

- Adequate numbers of gates should to be provided in the perimeter security systems for people & material to get into the compound
- Gates should be sturdy & strap & firmly anchored to the ground
- Gates are to be sited with forethought & imagination
- It is advisable to earmark a gate exclusively for employees to enter & exit and one for movement of vehicles
- For visitors the entry should be through the gate office
- Adequate arrangements should be made at the gates to check the credentials of the people & material entering & exiting the premises
- To prevent vehicles from making a forced entry, drop barriers, spike stoppers, zigzag pathway, etc can be made at a distance of 30 feet from the gate
- A speed barrier should be constructed to slow down speed
- Zigzag approach roads also serve the same purpose of reducing the speed of vehicles entering the compound
- For the vehicle gate, at a distance of 100 feet inside the complex a drop barrier should be erected

Other requirements at all gates

- Denial lane for sending back the vehicle, if entry is denied
- 1mtr median between lanes – in case of more than one lane
- Minimum lux level – 100 Lux for enable checking – white light
- Sufficient light at-least 50mtrs approach road of gate
- Electronic cantilever gate(s)

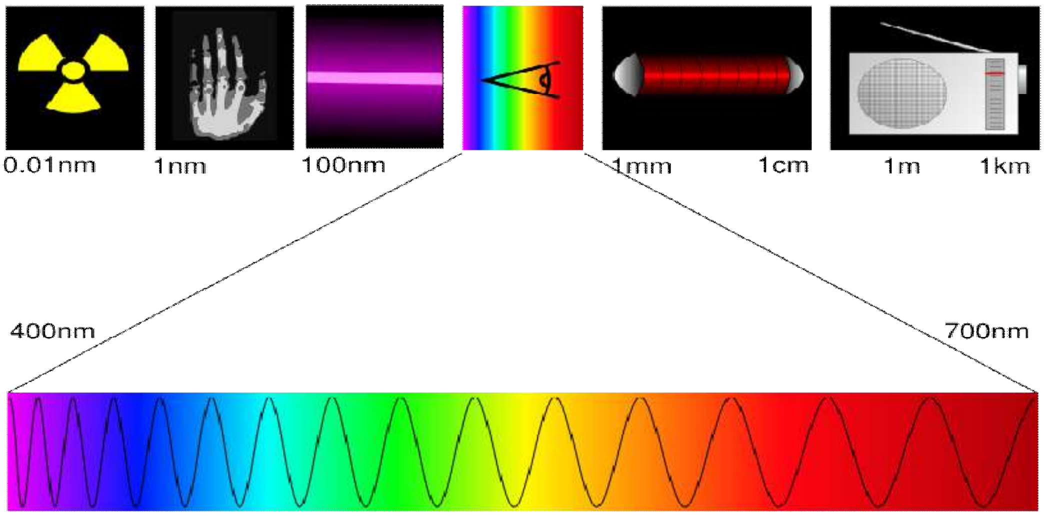
- Boom barrier(s) – high-crash rated as per site criticality
- Tyre killers integrated with boom barriers / control room
- Minimum 5 metres lane road width foe safety of Security Guards to stand and operate
- Stabilized power and IT network to support automation gadgets
- Communication system - Telephone connectivity, PA system cum duress alert system connected with the Security control room
- Video coverage for all incoming / outgoing lanes – vehicular / pedestrian
- Preferred Shed for Security guard at vehicle / pedestrian checking lanes
- Funnel type entry (wherein distance from outer side will depend upon the volume)
- Preferred Morchas (at all critical gates), in case of deployment of armed guards
- Sufficient standard display boards (as informatory, mandatory rules etc.)
- Bomb pit outside gate house for disposal of suspected object.

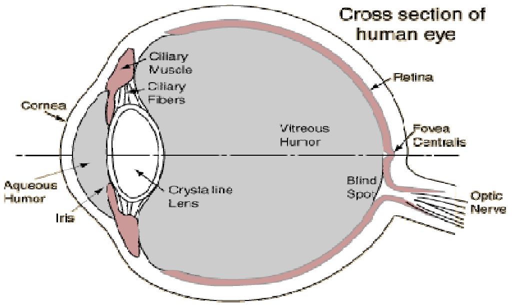
5.4 Security Lighting System

Lighting and that too proper lighting plays an important role in the security of any undertaking. Lighting management should include, proper lighting, with its various facets. The following narration includes, the concept of light, its impact on the eye, the need to have proper lighting and other related issues which would ensure that the area protected is properly illuminated so that there is no possibility of any interference from unauthorised elements so that the industries activities and the assets of the industry are protected properly.

- Light is that part of the electromagnetic spectrum which produces a sense of sight when it falls upon our "eyes"
- The electromagnetic spectrum is much larger than the visible spectrum

Electro Magnetic Spectrum





Purpose

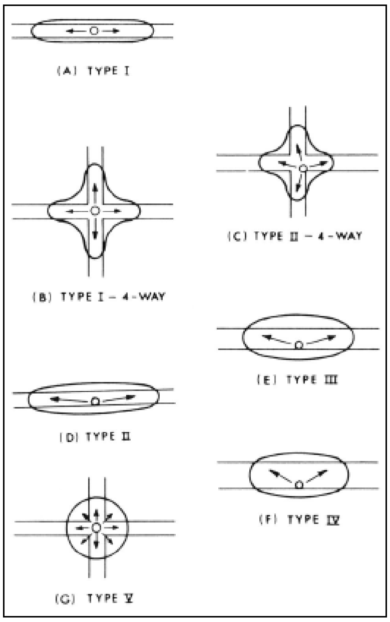
Security lighting is installed to help protect people and property from criminal activities, and to create a perception of security. To better understand the principles of security lighting, it is first appropriate to look at several key security tenets.

Lighting can affect crime by two indirect mechanisms. The first is the obvious one of facilitating surveillance by the authorities and the community after dark. If such increased surveillance is perceived by criminals as increasing the effort and risk and decreasing the reward for a criminal activity, then the level of crime is likely to be reduced. Where increased surveillance is perceived by the criminally inclined not to matter, then better lighting will not be effective. The second mechanism by which an investment in better lighting might affect the level of crime is by enhancing community confidence and hence increasing the degree of informal social control. This mechanism can be effective both day and night but is subject to many influences other than lighting.

Recommendation

Security lighting, as part of a well-balanced security plan, should have the following objectives:

- Provide a clear view of an area from a distance and enable anyone moving in or immediately around it to be easily seen
- Deny potential hiding spaces adjacent to frequently traveled foot routes
- Permit facial identification at distance of at least 9 m (30 ft), and create the perception of being identifiable
- Facilitate the proper use of other security devices available on the property
- Deter crime against persons or property
- Enhance the public's feeling of comfort in accessing spaces and increase night-time pedestrian traffic



Principles in Security Lighting

- Integration of illumination into the total security system, thereby facilitating the effectiveness of other security devices or procedures
- Illumination of objects, people, and places to allow observation and identification, thereby reducing criminal concealment
- Illumination to deter criminal acts by increasing fear of detection, identification, and apprehension
- Lessening the fear of crime by enhancing a perception of security
- Illumination that allows persons to more easily avoid threats, and to take defensive action when threats are perceived

Different Light Distribution Patterns

Recommended Lighting Standards

Area lighting is typically accomplished with floodlighting or luminaires mounted on poles 9 m (30 ft) or more in height. The recommended average illumination on the surface of large open areas is 5 to 20 lux (0.5 to 2 fc) with an average-to-minimum illumination uniformity ratio not greater than 8:1.

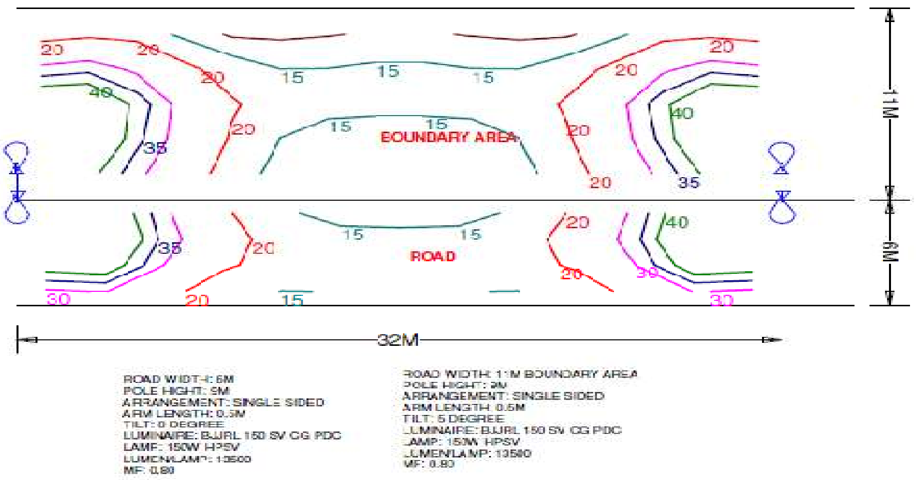
The greater the brightness of the surrounding area, the higher the luminance required to balance the brightness in the space, while exercising caution to avoid light trespass and glare. Luminaire spacing will depend on the output, mounting height, and distribution of the luminaires. In storage areas where unacceptable material losses have been sustained or security is an issue, the average maintained luminance levels should be at least 10 lux (1fc), with an average-to-minimum uniformity ratio not greater than 6:1.

If the area contains a large number of obstructions to visibility, (as in Power station or Storage tank area) a design utilizing additional multiple source locations and higher mounting heights will reduce shadows.

It will be helpful if the luminaires are positioned within the site, between obstructions, and with overlapping light patterns. The reflectance of site materials can also be used to advantage. Light, reflective colours on buildings and in concrete paving will enhance the efficiency and uniformity of the lighting system.

At the perimeter walls, it may be good to designing lighting systems with disability glare, because the technique is sometimes used in special security lighting applications to protect a secure area. The glare renders would-be intruders outside the protected area highly visible to guards inside the perimeter, while masking the guards and other features from the casual outside observer.

ILLUMINATION DESIGN FOR 6M WIDE ROAD WITH 9M POLE



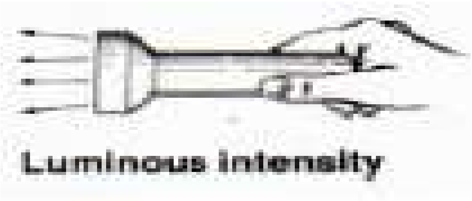
ROAD WIDTH: 6M
POLE HIGHT: 9M
ARRANGEMENT: SINGLE SIDED
ARM LENGTH: 0.5M
TILT: 0 DEGREE
LUMINAIRE: BJURL 150 SV CG PDC
LAMP: 150W HPSV
LUMEN/LAMP: 13500
MF: 0.80

ROAD WIDTH: 11M BOUNDARY AREA
POLE HIGHT: 9M
ARRANGEMENT: SINGLE SIDED
ARM LENGTH: 0.5M
TILT: 5 DEGREE
LUMINAIRE: BJURL 150 SV CG PDC
LAMP: 150W HPSV
LUMEN/LAMP: 13500
MF: 0.80

- Lighting Load of 20KW for 240Nos, 150W Fittings with 120Poles shall cover around 3.75KM stretch from 100KVA Voltage Regulating Lighting Transformer (composite panel) along with 4Nos, 63Amp outgoing feeders. One spare feeder of 63Amp shall be provided. This main panel shall be installed near the boundary wall.
- Lighting transformer shall be of oil cooled type, Voltage regulation from 382-415V, outdoor type, Insulation Class with Aluminum windings.
- For auto switching of lighting system, timer/contactor circuit shall be provided in the composite panel
- Composite panel shall have 200Amp, MCCB incoming facility and 5Nos, 63Amp, TPN MCB as outgoing with 100KVA inbuilt Voltage regulating transformer. The panel shall be outdoor type with IP-55 protection. Transformer Make shall be of reputed. Necessary drawing approval shall be obtained after order placement
- From outgoing of each Composite Panel (MLDB), SLDB shall be placed with Minimum qty of 2Nos to distribute and cover entire 3.75KM stretch. Hence from total of 2Nos of MLDBs shall cover entire stretch of 3.0KM. SLDB shall be outdoor type and having incomer 63A, TPN MCB & outgoing with 2Nos, 32Amp, TPN MCB with suitable terminal block & bus bar arrangement.
- Panel manufacturer should be CPRI approved.
- Switchgear components shall be of following approved make – ABB/Siemens/Schneider/L&T. All other accessories of the panel like bus bar, terminal blocks, wirings etc shall be of reputed make. Drawing approval shall be obtained prior to manufacturing the panel.
- Make of cable shall be of approved make

<u>Basic Lighting Quantities</u>

- Luminous Flux
    a. It is the amount of light energy given out per second by a light source
    b. Measured in Lumens
    c. A 100 watt bulb will give between 1200 and 1600 lumens
- Wattage
    a. It is the electrical power consumed by the light
    b. Used to calculate the cost of lighting
    c. Used to calculate efficiency of the bulb in lumens per watt or LPW
- Luminous Intensity
    a. The luminous flux produced in a *particular direction*
    b. Measured in candela
    c. Typical Values



i. LED : 0.005 cd
ii. Candle : 1 Cd
iii. 100 W bulb : 150 cd
iv. Headlights : 100,000 cd

- Luminance
  - Measurement of “Brightness”
  - Depends on:
    - Illuminance and
    - Reflective nature of surface
  - Measured as Cd per sq m
  - Typical values
    - Clear sky : 9000 cd/m^2
    - Candle: 10,000 cd/m^2

Types of light sources

- Incandescent
- Fluorescent
- High Intensity Discharge
- Low Pressure Sodium
- Outdoor Solar Lighting

Terms of Comparison

Efficacy

- Measured in Lumen per watt
- Determines the brightness at the source for a given wattage

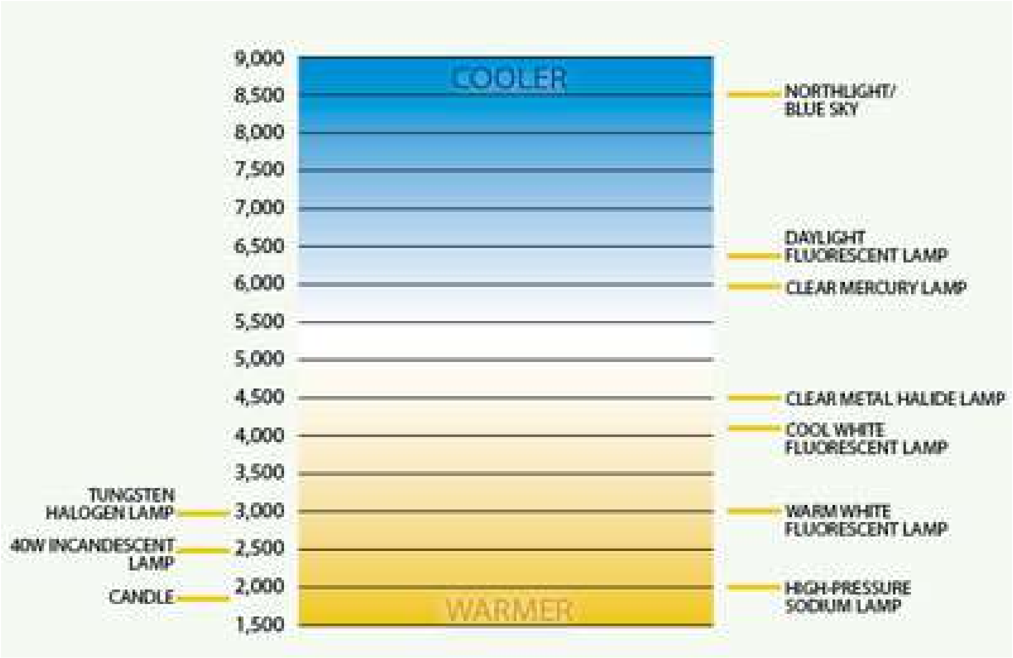
Life Time

- The number of hours before replacement is required

Colour Rendition Index (CRI)

- A number from 0 to 100 denoting the ability to show all colours in their true form.
- CRI below 80 distorts the colour perception

COLOUR TEMPERATURE



2800K

3100K

4100K

4700K

Principles of Good Lighting

- Adequate lighting – “More is not Good”
- “Shielded” Lamps to direct light to the target area (s)
- High efficiency lamps with adequate thought for colour and quality

Reasons for Ineffective Lighting

- Excessive Illumination
- Unnecessary Illumination
- Unshielded Light Fixtures
- Misaligned Light Fixtures
- Glare and Clutter
- Inefficient Light Sources

Side Effects of Glare and Lighting

- Is the result of excessive contrast between bright and dark areas
- Direct light into the eyes can obscure night vision for up to an hour after exposure.
- Glare can also make it difficult for the human eye to adjust to the differences in brightness

Types of Glare

- Blinding Glare
    - It is completely blinding and leaves temporary vision deficiencies. E.g. caused by staring into the sun
- Disability Glare
    - Describes effects with significant reduction in sight capabilities. E.g. caused by oncoming vehicle lights
- Discomfort Glare
    - Does not typically cause a dangerous situation in itself, and is annoying and irritating at best.
    - It can potentially cause fatigue if experienced over extended periods
- Clutter
    - Refers to excessive groupings of lights.
    - May generate confusion, distract from obstacles, including those that they may be intended to illuminate.

Desired Capability of Security Lighting

- Deterring the intending intruder
- Revealing the intruder before, during and after
- Providing some degree of concealment to the security personnel

- Perimeter lighting
- Security lighting deployment
- Checkpoint Lighting
- Defensive area lighting
- Defensive building floodlighting
- Topping up

Security Lighting Techniques

- Continuous Lighting
- Controlled Lighting: When lighting is used to uniformly light a given area
- Glare Lighting: When the intention is to disable visual capabilities of the intruder
- Trip Lighting: Lighting which is triggered through some alarm mechanism
- Emergency or backup lighting
- Portable and moveable lights

Perimeter Lighting

- Defended Area : All area within the perimeter
- Surveillance Zone: Extending from 20m to 50m outside the fence
- Sterile Strip : Around 6m wide from the perimeter to the lights
- Patrol path : About 1 m behind the lights
- Watch out for the Sleeping Sentry Syndrome

Defensive Area Lighting

- Areas near the perimeter may be lit or unlit depending on the use
- In case area is not in use then perimeter lighting is sufficient
- Else area may be lit sacrificing concealment strategy of the perimeter light
- Avoid mounting lighting on buildings as it will keep entrances, recesses in darkness
- If CCTV is deployed then lighting level should correspond to that required for CCTV

Defensive Building Floodlighting

- Purpose: To reveal an intruder by positioning him in front of a brightly lit background
- Technique: Putting lights aimed at lower parts of the building in front of the building.
- Light paint used in the building exterior
- Floodlighting from outside in case of isolated area

Topping Up

Refers to addition of light sources to cover

- Shaded areas
- Areas where normal security lights cannot penetrate due to obstructions etc.

5.5 Alarm Systems

Alarm systems can provide early warning of unauthorized access to agencies' facilities. An alarm system is only of value in conjunction with other measures designed to detect, delay and respond. All alarm systems are to be monitored and linked to a pre-determined response.

Alarm systems may be single sector or sectionalized to give coverage to specific areas of risk. Sectionalized alarm systems allow greater flexibility as highly sensitive areas can remain secured when not in use and other parts of the facility are open.

Agencies should, where possible, configure alarm systems to continuously monitor detection devices in high risk areas, for example irregularly accessed areas, roof spaces, inspection hatches and under floor cavities.

Each agency is to have direct management and control of alarm systems. Agencies should have direct management and administration of other alarm systems.

Each agency is to use appropriately cleared and trained agency staff as privileged alarm system operators and users. Agencies should only use appropriately cleared and trained agency staff as privileged operators and users of other alarm systems.

However, operation functions, such as monitoring and maintenance, may be outsourced. Agencies are to ensure all alarm system arming and disarming personal identification numbers (PINs) are:

- Uniquely identifiable to an individual
- Not recorded by the individual
- Regularly changed in accordance with the agency's risk assessment

Agencies should have the default/engineering user codes removed from alarm systems at commissioning. Agencies should develop appropriate testing and maintenance procedures to ensure the alarm system is continually operational. Alarm systems can be broadly divided into two types:

- Perimeter (or external) intrusion detection systems (PIDS) or alarms
- Internal security alarm systems (SAS)

Agencies may use out-of-hours guard patrols instead of an alarm system in all areas. PIDS may be of value to agencies that have facilities enclosed in a perimeter fence. They provide early warning of unauthorized breaches of a facility perimeter.

Individual Alarm Options

The use of building alarm systems, EACS or other facility-wide measures may not be ideal in some situations. This includes, but is not limited to, working away from the office, areas with a high potential for personal violence and protection from the compromise of physical assets in public areas. There are a number of individual alarm options that may be suitable in some situations, including duress alarms, individual item alarms, or alarm circuits, and vehicle alarms.

Duress Alarms

Duress alarms enable employees to call for assistance in response to a threatening incident. Agencies may be required to use duress alarms activated by dual action duress buttons—that is, depressing two separate buttons to trigger the alarm to reduce the occurrence of false alarms—when a police response is required in some jurisdictions.

Individual Duress Alarm

Individual or mobile duress alarms provide some deterrence to violence when employees are outside the office or circulating in public areas. Personal duress alarms fall into two broad categories:

- Remotely monitored duress alarms
- Alarms that produce loud noise on activation

Remotely monitored alarms are suitable for use within facilities where there is a dedicated monitoring and response force. The alarms consist of a personal alarm transmitter linked to the facility, or a separate alarm system.

Noise producing duress alarms rely on response by bystanders. They are more suited for applications external to the agency facilities than monitored duress alarms where there could be considerable delay in response to the alarm. Agencies may use these alarms within a facility where they desire immediate notice of an incident by the people in the immediate area.

Hidden/Fixed Duress Alarm

Fixed duress alarms are a type of remotely monitored individual duress alarm. They are normally hard wired and fixed to a location. Agencies should consider equipping public contact areas, including the reception area, counters and interview rooms, with duress alarms where the risk assessment has identified a potential problem. Hidden duress alarms should**:**

- Enable employees to raise an alarm discreetly
- Be augmented by procedures that provide an appropriate response.

Agencies should ensure that:

- All relevant staff are aware of and have regular training and trials with the duress alarm
- The duress alarm is configured as part of an intruder alarm system
- The alarm panel is located within the protection zones of the alarm

Individual Item Alarm/Alarm Circuit

Valuable items, particularly when in public areas such as exhibitions, may not be able to be protected by normal alarm systems. An option is to install individual item alarm circuits or a separate alarm system to monitor individual items. Some possible alarm sensor types that may be suitable are:

- Pressure switches
- Motion sensors
- CCTV activated alarms
- Radio frequency identification (RFID) tag systems

Agencies should seek specialist advice when designing alarm systems for individual items.

Vehicle Alarm

Agencies that have field workers often require these employees to work from vehicles that can contain large quantities of valuable equipment. Most vehicle alarms rely on noise and have similar deterrent value to noise producing personal duress alarms. However, they rely on a response by bystanders if the employee is outside hearing range.

Agencies may consider fitting remotely monitored vehicle alarms where the business impact level of loss of the information or physical assets in the vehicle, or the vehicle itself, is high or above. Remote vehicle alarms may also be linked to remote vehicle tracking and immobilization systems.

Fire Alarm Systems

The Fire Alarm System consists of the following parts:

a. Control Panel
b. Smoke Detector
c. Flame Detector
d. Thermal Detector
e. Power Supply Unit (Back up Battery)
f. Audio Alarm Unit

Automatic Fire Alarm system is meant for detecting fire in its early stage and gives out audio/visual alarm for initiating appropriate counter measures to avoid or at least minimise the loss of human life and property.

Automatic fire alarm system consists of a Central Control Unit connected by a number of fire detectors located at different risk areas. These sensing devices use one of the physical parameters of fire for detection. On detection of these, fire detectors transmit an electrical signal to the control panel to initiate audio and visual signal. The control panel displays the exact location of affected area to take quick counter actions. The fire signal can also be transmitted to the nearest fire brigade.

5.6 Patrolling

It is a method of providing :

- Security for men & materials
- Covering vast area on foot or vehicle
- With minimum security personnel

One of the most effective means of providing security is through patrolling by security personnel. The greatest deterrent to a criminal is the presence of a Security Guard in the area in which he intends to operate. Patrolling is done in those areas where it is not possible to provide a static sentry post because of reasons of economy or otherwise. Those areas which are not so vital as to merit a static guard are also covered by patrolling.

Objectives of Patrolling

The main objectives of patrolling are :

1. Prevention and detection of offences against the property of the undertaking.
2. To ensure that proper security measures are being taken by all those who are responsible for the security of plant property
3. To locate any damage to physical security measures like walls, fences, lighting, doors, locking devices, alarms etc.
4. To obtain information about activities of workers detrimental to the interests of the industry
5. To ensure that safety measures are being taken and safety rules are being followed to prevent fires, accidents etc.
6. To create an atmosphere of alertness to show that the security force is vigilant and effective thereby acting as a deterrent to potential criminals
7. To prevent the outbreak of fire by maintaining a constant look out in areas vulnerable to fire

Foot Patrols

Patrolling can be done on foot or on vehicles. Foot patrols are more effective because the security personnel move slowly and can observe the area in much greater detail than if they were to ride fast on bicycle or on a jeep. Secondly, patrolling on foot enables the security personnel to develop contacts and greater rapport with the workers in the plant with the result that they acquire more detailed knowledge about the Plant and about the activities of the workers, Unions, pilferers etc. Patrolling on foot enables them to check the locks on the doors as well as to observe any security risks like broken windows or doors or gaps or breaches in the physical security measures. Foot patrols are silent and on many occasions they have been able to surprise criminals and catch them in the act of stealing. The only disadvantage of foot patrol is that they can cover a small area.

Mobile Patrols

Mobile patrols can move on slow moving vehicles like cycles or fast moving vehicles like motor cycles and jeeps. They can cover a much larger area than foot patrols in a much shorter time. They have also the advantage of being able to chase criminals who are mobile. If there is need for quick reinforcements a mobile patrol in a jeep can drop a few guards to handle a situation and rush off and get reinforcement without delay. A patrol jeep could also be fitted with a wireless set and remain in contact with the control room or security headquarters.

Armed Patrols

Some industries located in crime prone areas are sometimes attacked by armed gangs of criminals. Where such conditions prevail it becomes necessary to arm the security patrol to enable them to perform their duties effectively. In order to organise patrolling in the most effective manner the following points should be borne in mind:

a) Areas requiring intensive security cover, i.e. areas like vital installations, stores with expensive material, areas vulnerable to theft and pilferage or sabotage must be covered by foot patrols
b) Perimeter barriers, if they are very long, should be covered by mobile patrols
c) The open area between the perimeter barrier and the plant could be covered, by mobile patrols
d) During the day a single guard may be detailed on patrolling duty but at night at least two guards should be sent together
e) All patrols should be equipped with some means to call for reinforcements in an emergency. They could be given whistles or walkie-talkies sets. Pre-arranged signals by whistles could be used
f) All patrols must be given a specific area to guard and should be briefed about their duties

g) All patrols must know what action they should take in an emergency, where they are to look for assistance or reinforcements etc.

h) On completion of duty the patrols must report back at a pre-determined point and report any unusual occurrence of breaches in security arrangements or other important information pertaining to the security of the Plant which they might have observed during the duty period.

i) Patrolling must never be done at fixed times and at fixed places as this enables the criminal to avoid the patrol easily. Timings and routes of patrols must be changed daily.

j) Officers must be detailed to supervise the patrols and to ensure that the patrols carry out their duties according to the given programme.

k) After the patrol completes its duty it should report back to the starting point and the officer to whom they report back must debrief them to obtain all the information collected during their patrolling. This formal debriefing is very useful as quite often the members of the patrol tend to forget to report many important things they might have noticed during their duty.

l) Once patrols are sent out they must also be checked to see that they perform the duties assigned to them correctly and in time. Many methods have been devised for this kind of checking. One is the token system where the patrol has to deposit metal tokens at predetermined places. Another system is by maintaining registers at suitable points which require filling up at fixed timings. The tell tale clock is also a useful device which registers the time at which the patrol reaches it. Such clocks are placed at suitable points and the patrol has to visit each clock and register its arrival.

Duties While on Patrol

- Check all physical security measures for the damages / breaches if any (perimeter wall, fencing etc.)
- To inspect the locks and seals of the stores &important buildings

- Check for suspected persons who are loitering about inside the plant
- To inspect the parked vehicles and railway wagons
- Collect information
- To look for any property lying around in an in secured place
- Look for any security hazard or safety breaches and inform the concerned
- To investigate any thing which does not appear to be normal

How to make Patrolling more Effective

- Important areas such as vital installations, stores etc., to be covered by foot patrolling
- Perimeter barriers if longer to be covered by vehicle patrols
- All patrols should be equipped with communication facilities if during night torches, night vision equipment.
- Patrolling should never be done at fixed time and in fixed route
- All patrols should be given specific area to guard
- Patrol parties should be briefed and debriefed before and after duty

Conduct while on patrol

- Smart appearance
- Professional knowledge
- Dutiful attitude
- Always watchful
- Safe distance
- Observation discipline
- Noise discipline
- Light discipline
- Cover and retreat

5.7 Identity Cards

Identity (ID) cards allow for speedy recognition of employees in agency facilities. They should be used in all facilities. Users should issue ID cards to all people who have regular access to their facilities, subject to meeting any personnel security requirements. Users are to verify the identity of all people who are issued with identity cards.

ID cards should be:

- Worn by employees and clearly displayed at all times in agency premises
- Uniquely identifiable
- Audited regularly in accordance with the agency's risk assessment

Users should discourage employees from wearing ID cards outside premises. ID cards should include a return address for lost cards; it should not identify the facility to which the card gives access. Users may include other information on ID cards to improve control of access, such as names, photographs and colours. EACS access cards can be used as ID cards. Users are to secure all card making equipment, and spare, blank or returned cards

Security policies regarding entry

Before establishing a Security Policy, the management has to enunciate security policy and communicate the same to the security manager to work out the details. Such as

- Who should be permitted to enter?
- Where, when and how should they enter?
- What types of restrictions on their movements within the facility, if any, to be imposed and by whom?
- Will the visitors be required to be escorted into/out of the facility?
- What types of controls are to be prescribed to authorise removal of property from the facility?
- Should observance of security policy be made mandatory for all employees and should their failure to do so, result in disciplinary measures?

Employee Identification Card

To establish their identity, all employees are to be issued Identity Cards containing the Name of the Employee, employee number and identifying marks division/department where he works, name of the organisation, etc. It should also contain the latest colour photograph of the employee. The validity should not more than 3 years and I.D. cards should be changed at least once in 3 years. To make duplication difficult, the insignia of the organisation with a complex geometrical design should be printed as the background. The signature and seal of the issuing authority should be on the side containing the photograph. On the reverse side, there should be a request to the finder to return the card to the organisation, offering him a monetary reward. The card should be enclosed in a transparent clear plastic material and laminated with heat process.

Authority to issue ID card

In all organisations, there is a debate as to which department should issue the identity card. In our opinion, the Personnel Department should be the authority to issue Employees ID cards and it should maintain a permanent record of all cards issued with their particulars. A copy of these records should be available to the Security Manager for ready reference. On retirement or resignation, an employee should deposit his I.D. card in the Personnel Department and the card should be cancelled at the earliest and the fact notified to the Security Department.

Temporary I.D. cards

It may so happen that an employee leaves his card behind at home and reports for duty. Provision should be made to issue him a temporary ID card valid for a day only on payment of a prescribed fee. These temporary cards are to be issued by the Security Department, which should report details of such cards issued to the Personnel Department on a daily basis.

Loss of I.D. Cards

Employees should be advised to report the loss of their I.D. Card to the nearest Police station, to the Security Department and the Personnel Department without any loss of time. Duplicate I.D. Cards should be issued after collecting a prescribed fee.

Visitor's Card

It is also necessary to design identification cards to accurately identify the various types of visitors. Visitors should be courteously received and the reason for their visit should be established. After verification, a visitor's card should be issued to them and they should be escorted inside the facility by security personnel and handed over to the executive with whom he has business.

Contractor's Labour, Casual Labour and Service Personnel

Casual labour and service personnel can be issued temporary I.D. card for a day after verifying their bona fides and the requirement for them to enter the premises.

Types of Identity Cards

- Computerised I.D. Cards
- Exchange System Card
- Optically Coded Card

- Magnetic Coded Card
- Magnetic Strip Coded Card
- Passive Electronic Coded Card
- Active Electronic Card
- Bar Code Card

Identity Verification Systems

- Finger Print Verification System
- Hand Geometry Verification System
- Face Identification System
- Iris Comparison System
- Speech Verification
- Signature Comparison

The security policies can be categorised into two namely; (a) Technical Policy to be carried out by hardware or software and (b) Administrative Policy to be carried out by people using and managing the system.

- Identification and Authentication
- Applying identification and authorization Policies
- Password management Policies
- Robust Authentication Policy
- Digital Signatures and Certificates
- Software Import Control
- Local Area Network (LAN)
- Access Control Mechanisms
- Future of LANs / WANs
- Risk Assessment

5.8 Visitor Control

Visitor control is normally an administrative process; however, this can be augmented by use of EACS. Visitors can be issued with EACS access cards specifically enabled for the areas they may access. In more advanced EACS it is possible to require validation at all EACS access points from the escorting officer.

Regardless of the entry control method used, people should only be given unescorted entry if they:

- Are able to show a suitable form of identification
- Have a legitimate need for unescorted entry to the area, and
- Have the appropriate security clearance;.

Agencies should consider anyone who is not an employee in a facility or area, or has otherwise been granted normal access to the facility or area, as a visitor. This may include employees from other areas of the agency.

Agencies are to issue visitors accessing Zones Three to Five areas with visitor passes. Agencies should also issue visitors to Zone Two with visitor passes when other controls to limit access are not in place. Passes are to be:

- Worn at all times
- Collected at the end of the visit
- Disabled on return if the passes give access to any agency access control systems
- Checked at the end of the day and, where the passes are reusable, action taken to disable and recover any not returned

Agencies are to record details of all visitors to Zone. Agencies should also record visitor access to areas if other control measures are not in place. An agency employee or authorized person should escort visitors. Agencies may, based on their risk assessment, record visitor details at the facility reception areas, or entry to individual security zones.

Visitor Registers

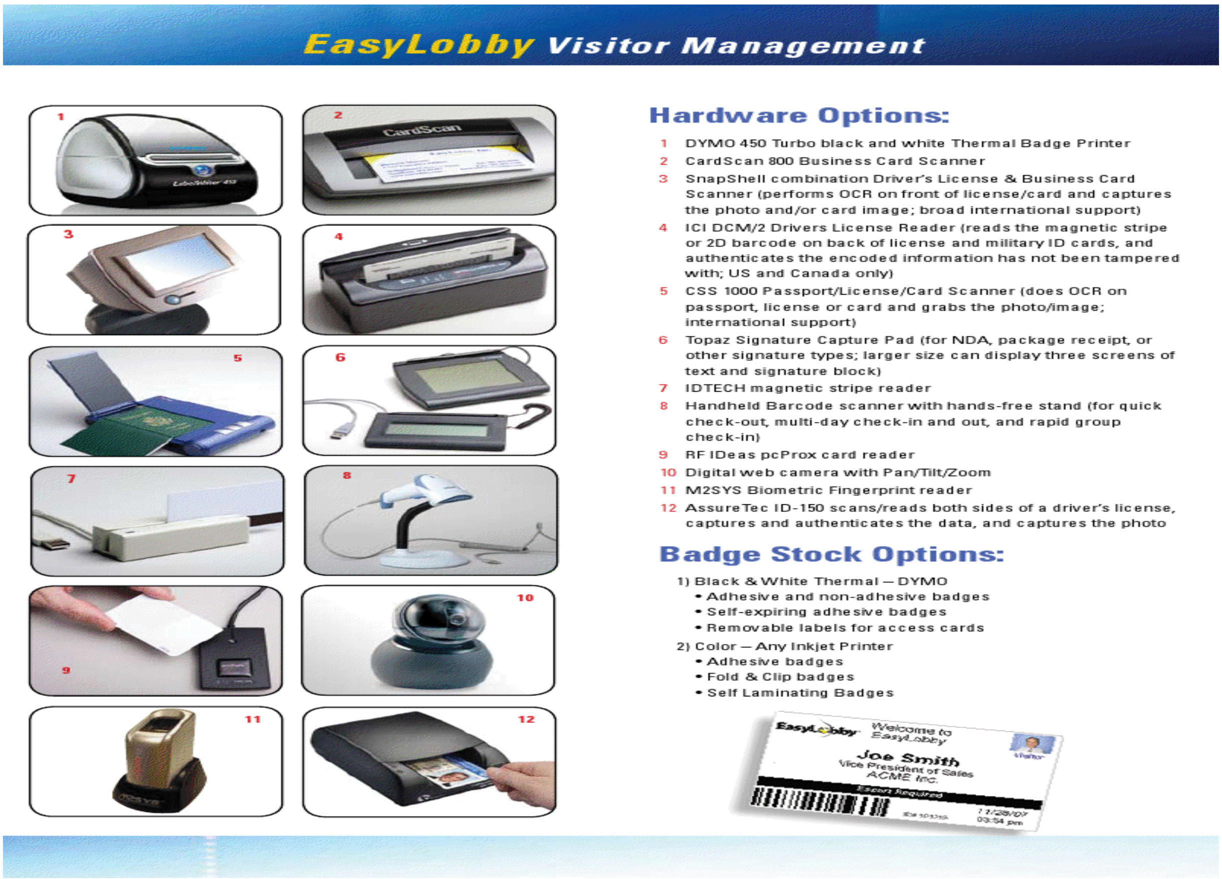
Users should use visitor registers signed by each visitor and the agency employee authorizing the visit. The register may include:

- The name of the visitor
- The visitor’s agency or firm or, in the case of private individuals, their private address
- The name of the employee to be visited
- The times of the visitor’s arrival and departure
- The reason for visit

The visitor register would normally be located at the facility reception desk unless the desk is unmanned, in which case it should be held by a designated employee within the facility. Where agencies manage the control of access to specific areas at the entry to the area then those areas should have their own visitor registers.

Visitor Management

- Greet visitors with smile
- Show a sincere desire to be helpful
- Answer the visitor's questions in a polite manner
- Be attentive and don't interrupt when the visitor is talking
- Use patience and tact
- Visitors carrying laptop computers must register the information like make & serial number of the laptop into the log book. A laptop pass shall be issued. Security personnel to verify the existence of the computer upon entry and exit by the visitor.
- On departure by the visitor, security must collect the pass and record the appropriate details in the visitor's profile
- Visitors are not permitted into the facility with weapons, chemicals, or any dangerous goods/items. Items being carried by visitors must be scrutinised by security
- Security shall guide the visitors to facility centre lobby. The front office executive in the reception shall request the particulars of the visitor and the host being visited. The visitor will be guided to wait in the visitor lounge and the host contacted.
- The host must personally escort the visitors into the office area. Visitors are never to be allowed to proceed into the building without being escorted by the host.
- Visitors in general think of you and all security professional in general, as capable, skilled, intelligent professional, you must impress upon them those very things. Your endeavour to make this kind of impression on visitors will be undermined if you:
- Sleep on the job
- Exhibit poor grooming
- Fail to act quickly and efficiently when such action is necessary
- Make derogatory statements then others may hear or pass along
- Have a bad attitude.
- Above all very important to watch your language. Discourteous, obscene remarks can cause irreparable damage to the company and security in general.



EasyLobby Visitor Management

Hardware Options:

1 DYMO 450 Turbo black and white Thermal Badge Printer

2 CardScan 800 Business Card Scanner

3 SnapShell combination Driver's License & Business Card Scanner (performs OCR on front of license/card and captures the photo and/or card image; broad international support)

4 ICI DCM/2 Drivers License Reader (reads the magnetic stripe or 2D barcode on back of license and military ID cards, and authenticates the encoded information has not been tampered with; US and Canada only)

5 CSS 1000 Passport/License/Card Scanner (does OCR on passport, license or card and grabs the photo/image; international support)

6 Topaz Signature Capture Pad (for NDA, package receipt, or other signature types; larger size can display three screens of text and signature block)

7 IDTECH magnetic stripe reader

8 Handheld Barcode scanner with hands-free stand (for quick check-out, multi-day check-in and out, and rapid group check-in)

9 RF IDeas pcProx card reader

10 Digital web camera with Pan/Tilt/Zoom

11 M2SYS Biometric Fingerprint reader

12 AssureTec ID-150 scans/reads both sides of a driver's license, captures and authenticates the data, and captures the photo

Badge Stock Options:

1) Black & White Thermal — DYMO
- Adhesive and non-adhesive badges
- Self-expiring adhesive badges
- Removable labels for access cards

2) Color — Any Inkjet Printer
- Adhesive badges
- Fold & Clip badges
- Self Laminating Badges

5.9 Key Management

Key systems are a crucial part of a physical security program, and must be properly designed and managed in order to provide the necessary controls and a solid foundation to an overall security program. Left alone and unmanaged, a key system opens an organization to the potential for loss and liability.

An electronic physical access control system verifies individuals' identities and provides access based on a company's security policies and procedures, which govern how access privileges are granted within an organization. The management (or enrollment), issuance and termination of these credentials is a critical component in providing the right individual with the right level of access and in making sure that no individual has unauthorized access to any part of a facility.

In order for access control systems to properly function, some manner of restraint must be employed to prevent an unauthorized individual from gaining access to a restricted area. In most cases, this restraint is a locking mechanism (i.e., lock) that can be opened by using a mechanical key. The management of this secondary credential (the key) is critically important because it provides any individual with access to restricted areas. Many times, security personnel are unable to verify the identity of the individual key holder.

Your security starts with locks and keys, and your key system is your first line of defense. It is a critical component in protecting your facility against loss while increasing accountability and limiting risk. With mechanical key systems, security is derived from the management and protection of physical keys and the key system policies you create to enable that management and protection.

A well-documented key system policy will seek to address the following:

- Taking action when a key or master key is lost or stolen
- Distributing, replacing, tracking or returning keys
- Handling requests for additional, new and replacement keys
- Managing temporary and contract employees
- Identifying the key control authority and the authority's responsibilities
- Keeping records
- Creating an authorization process to obtain keys
- Taking steps to re-key the facility ° Enacting disciplinary actions for individuals that violate the policy

Locking Hardware

Locks are the most widely employed security devices. They are found on anything to which access must be controlled, such as vehicles, storage containers, doors, gates, and windows. The security of any property or facility relies heavily upon locking devices. Locks merely deter or delay entry and should be supplemented with other protection devices when a proper balance of physical security is needed. An assessment of all hardware, including doorframes and jambs, should be included in any physical security survey. Locking devices vary greatly in appearance as well as function and application.

Types of Locks

Locks can be divided into three very general classes: (1) those that operate on purely mechanical principles; (2) those that are electro-mechanical and combine electrical energy with mechanical operations; and (3) electronic locks, which add to electro-mechanical lock devices various logic operations associated with integrated circuits.

Mechanical Locks

Key Locks: Key locks are the most common mechanical locks. They include warded, lever, and pin tumbler locks. Although most key locks can be opened by a determined individual in a few minutes, they are used primarily to delay, discourage, or deter theft or unauthorized access.

Warded Lock: The mechanical lock longest in use and first developed is the warded lock. The lock is exemplified by the open, see-through keyway and the long, barrel-like key. Still found in older facilities, the warded lock is a very simple device. A modern locking program does not include warded locks. In any installation where warded locks are already present, phased replacement or augmentation with other locks is recommended.

Lever Lock: A significant lock improvement after the warded lock came in the eighteenth century with the perfection of the lever principle. The lever lock finds continued application today in such varying situations as desk, cabinet, and locker installations. The lever lock offers more security than the warded lock, but is inherently susceptible to picking.

Pin Tumbler Lock: The pin tumbler is probably the most widely used lock for applications such as exterior and interior building doors. A number of very useful refinements have been added to the basic pin tumbler in recent years, so that now a very high level of lock security can be achieved with many models. A pin tumbler lock with at least 6 pins is considered a high-security lock according to the FPS.

Combination Locks*:* A manipulation-resistant combination lock provides a high degree of protection. It is used primarily for safeguarding classified or sensitive material. Its technical design is to prevent the opening lever from coming in contact with the tumblers until the combination has been dialed.

Built-in Combination Locks: When a security container or vault door is used to safeguard classified information, it must be equipped with a changeable 3-position, dial-type combination lock that has been approved by GSA. These locks can be purchased from companies listed on the GSA FSS.

Combination Padlocks: Combination padlocks are locks designed for attachment to a mounted hasp. They are not approved for the protection of classified National Security Information and are not rated for resistance to physical attack. Combination padlocks can be used either as a removable padlock in conjunction with bar-lock cabinets and other conventional hasp-type locks, or by fastening the security cover of the padlock to the surface of a container. It can be used on desks, storage cabinets, filing cabinets, sliding door cabinets, and virtually any type of container through the use of an eyelet or loop designed to fit the tolerances of the opening of the padlock.

Electro-Mechanical Locks: Electro-mechanical door locks are primarily used to control entry into an area. Rather than using a key, they open by pushing a series of numbered buttons. The locks can be either electrically or mechanically activated. Some of the advantages of using these locks are low cost, easy installation, easy combination changing, and simple operation. These devices are used for access control and do not provide a high degree of security when used alone. Some models have "time penalty" and error alarm features and can be tied to an existing alarm system. When used in a controlled or restricted area that is not continually manned, these locks should be supplemented by a built-in combination lock. The combination or code used to activate an electro-mechanical door lock should be changed at least annually and when any person having knowledge of the combination no longer requires access to the area.

Electronic Locks

An electronic lock system uses a card key programmed with a particular code, which is read by a card reader that communicates with an automated central or local processor for access control. An electronic lock is considered a high-security lock according to the FPS. The card reader obtains data from the card by reading punched holes, magnetic strips or spots, imbedded wires, or any of several other methods. To open a door or activate a turnstile or lock, the card is typically inserted into a slot or groove and the coded area is read by the reader. If the code is an authorized one, the processor will direct the lock to open. Key cards should be voided in the system when lost, stolen, or when access is no longer required and the card recovered.

Card readers fall into two basic categories: on-line and intelligent.

- On-line readers must communicate with a central processor that makes the entry/exit decision.

- The intelligent card reader compares the data on the card with preprogrammed data, and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or off-line readers.

Multiple card readers can be used to control access to numerous buildings and rooms from one central processor. Most processors are capable of discriminating between time zones and levels of status for multiple readers and recording the time, date, location, and frequency of transactions. Many have additional features and capabilities such as monitoring alarms, keeping time and attendance records, and communicating with emergency or security personnel.

Biometric Systems

Other locking systems are available that use neither keys nor combinations. These include locks which open by using one of six primary categories of biometrics technology: fingerprints, hand geometry, retinal scan, signature dynamics, voice verification, or keystroke dynamics. These biometric systems are considered high-security locks and are designed primarily to control access to extremely sensitive, special-use areas where positive personal identification is an operational necessity.

Keys

Keys to locks are often the first and only level of physical security control for many organizational assets. Consequently, key control or the lack of it can mean the difference between a relatively secure activity and extraordinary loss. Almost all organizations utilize some type of key access in everyday operations. Each day offers an opportunity of key mismanagement, which can lead to mild annoyances such as the replacement and cost for lost keys, or to more serious losses, such as theft or personal injury. A good key control system will maintain a strict accountability for keys and limit both key duplication and distribution.

<u>Types of Keys</u>

- Operating or "change" keys are keys that are used to open locks.
- Duplicate keys are copies of operating keys and are usually stored for use in an emergency or to replace a lost key. Duplicate keys must be kept to a minimum and be protected to avoid proliferation and loss of accountability.
- Master keys are designed to open all locks of a particular series. Key systems can have one grandmaster key for the overall system and several sub-master keys for each subsystem. Master keys can be used as a convenience, e.g., carrying one key instead of numerous keys, but must be carefully controlled.
- Construction keys open removable lock cylinders installed on the doors during construction of a facility. These cylinders are replaced at the end of construction with cylinders using the facility's key system.

- Control keys are used to remove the cylinder of locks for changing keys. These keys are used only in interchangeable cylinder systems.

Accountability Procedures

- The integrity of a key system is important to safeguarding property and controlling access. Lost keys minimize a lock's effectiveness. The security officer should ensure that responsible individuals maintain control over the facility's key system by storing, issuing, and accounting for all keys under the facility's control. Issuance of keys must be kept to a minimum. Keys should be issued only to persons who have an official need.
- Accurate accountability records must be kept and should contain the information listed below. Keys not issued should be destroyed if no longer needed or stored in a locked container.
    - Number assigned to each key and lock
    - Location of each lock (room number)
    - Person to whom keys have been issued
    - Date of issuance
    - Recipient's signature for keys issued
- When a key to a designated controlled or restricted area is lost, the locks to the area must be changed
- Access lists for persons authorized to use master keys should be maintained
- The key storage container should be kept locked and checked at least monthly
- All keys should be inventoried at least annually
- Requests for issuance of new, duplicate, or replacement keys should be approved or monitored by the security officer

Protection of Keys

- Do not place identifying key tags on rings; if lost, it's an open invitation for misuse.
- Ensure keys are not left on desks, in unlocked drawers, or where they can be easily taken and copied. Remind employees to keep official keys on their person or securely locked in a desk or cabinet, and that they are not to lend them to individuals not specifically authorized.
- Ensure employees promptly return official keys checked out on a temporary basis.
- Ensure lost keys are immediately reported to the appropriate official. Locks should be rekeyed immediately and new keys issued when keys are lost or stolen.

Source: www.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h-ch6.html
Anixter.com

5.10 Public Address System

Public Address System provides all / selective announcements through speakers connected to it from security control room. It is used usually to make announcements in times of emergencies and in normal conditions is used to play music. And also connected with common siren for outdoors and be integrated with Fire alarm system wherever necessary. In addition to above Day/night vision binoculars recommended.

5.11 Control Room and Security Management

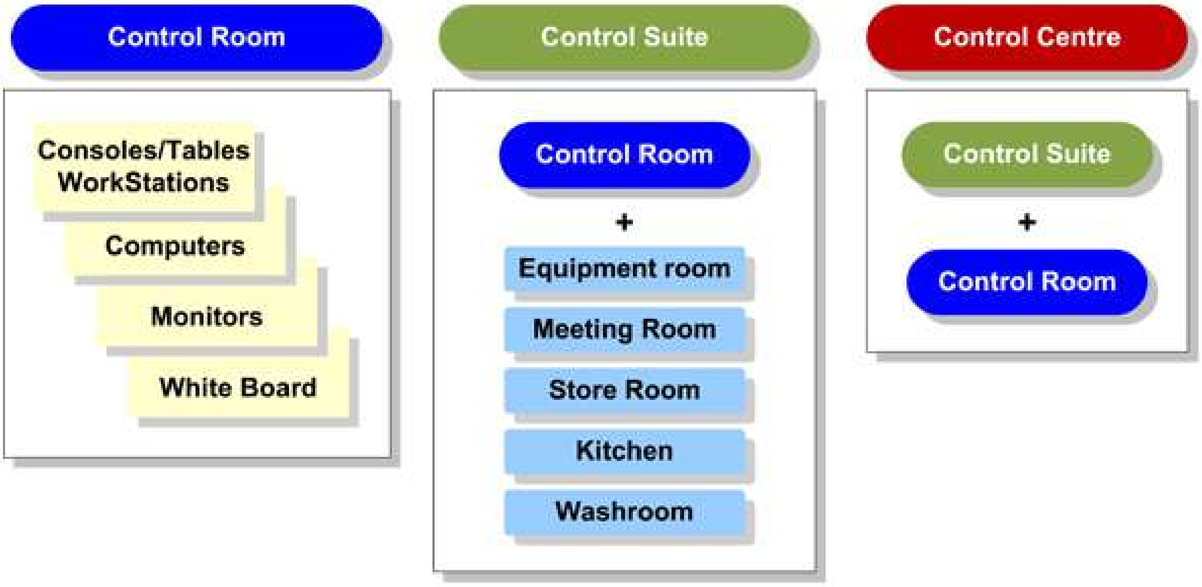
Over the past few years, significant progress has been made in the concept of security and CCTV control rooms. Control rooms are complex networked environments handling an ever increasing number of video and data sources. Efficient collaboration and decision-making is only possible if operators and decision-makers have easy and timely access to this information. In many cases, information even needs to be accessible to multiple users sat the same time.

A control room should consist of high-quality displays, rear-projection video walls, graphic controllers and web-based operating software, where operators get a complete overview of all surveillance systems and cameras. Operations management software including advanced warning capabilities designed to facilitate decision-making, draws operators' attention to the most critical images. Networked solutions distribute video and data over the standard IP network to provide you with accurate and real-time information, no matter where you are.

Few Definitions

- Control Room - core functional entity, and its associated physical structure, where control room operators are stationed to carry out centralized control, monitoring and administrative responsibilities [source: ISO 11064-3].
- Control Suite - group of functionally related rooms, co-located with the control room, and including it, which house the supporting functions to the control room, such as related offices, equipment rooms, rest areas and training rooms [source: ISO 11064-3].
- Control Centre - combination of control rooms, control suites and local control stations which are functionally related and all on the same site [source: ISO 11064-3].
- Control Room Operator - an individual whose primary duties relate to the conduct of monitoring and control functions, usually at a control workstation, either on their own or in conjunction with other personnel both within the control room or outside [source: ISO 11064-3].

- Control Workstation - single or multiple working position, including all equipment such as computers and communication terminals and furniture at which control and monitoring functions are conducted [source: ISO 11064-3].
- Local Control Station - operator interface that is located near the equipment or system being monitored and/or controlled [source: ISO 11064-3].



In normal routine days Control room functions as

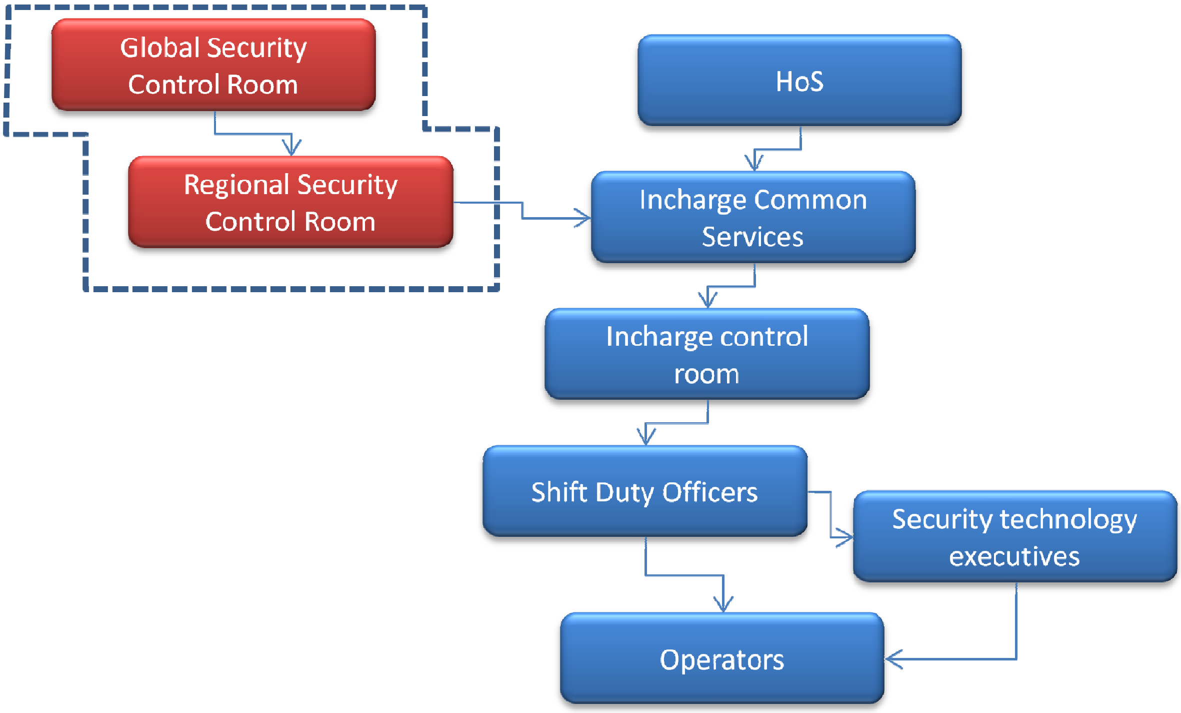
- Overall situation monitoring
- Oversee deployment of Security manpower
- Overall monitoring of access control personnel
- Overall monitoring of access control material & vehicles
- Compilation / logging of events and relevant data.
- Coordination and monitoring of important visits / events
- Maintain data related to road closures and non-availability of Security resources due to maintenance activity or otherwise.
- Ensure photography and other such activities with due approval and keep log of the same.
- Maintenance of arms and ammunitions and ensure kept Secured and issued on authorization only with proper logging, if available under SCR
- Anchor between security, operations (at manufacturing sites it is SSM) and other departments
- To act as focal point for reference

In emergency situations control room should act as

- Ready to receive information
- Ensure timely flow of information to the responders.
- Guiding the responders to the incident sites
- Ensure re-enforcement to incident site as per requirement.
- Situation monitoring and identifying additional requirement.
- Coordination of resource fulfilment – logistics, admin and responding
- Regular updation to SENIORS and concerned officials
- Percolate the instructions from apex members down the level for implementation
- Event logging with time-stamping for post incident investigation

Resource Requirement

- The control room should be planned to manned on 24/7 basis. Even in case no operations are performed during silent hours (like office complex), but Security deployment at multiple points remains, manning of control room still is important.
- Manning plan may be divided into two parts - routine and special / emergency operations.


Global Security Control Room
Regional Security Control Room
HoS
Incharge Common Services
Incharge control room
Shift Duty Officers
Security technology executives
Operators

Routine Operations

- As mentioned in the previous slides, manning during the routine operations depends upon the volume to be handled in terms of monitoring of physical Security operations, alarms points and surveillance system.
- In case the alarm points / surveillance system monitoring requirement is more than defined limit as per individual handling capability, dedicated Security technology executive may be deployed along with the control room shift duty officer.
- This will not only enables the fast response to any requirement like extraction of archived video & access data & analysis over-it or coordination with IT team etc. but also will assist in first hand trouble shooting of systems, if required.

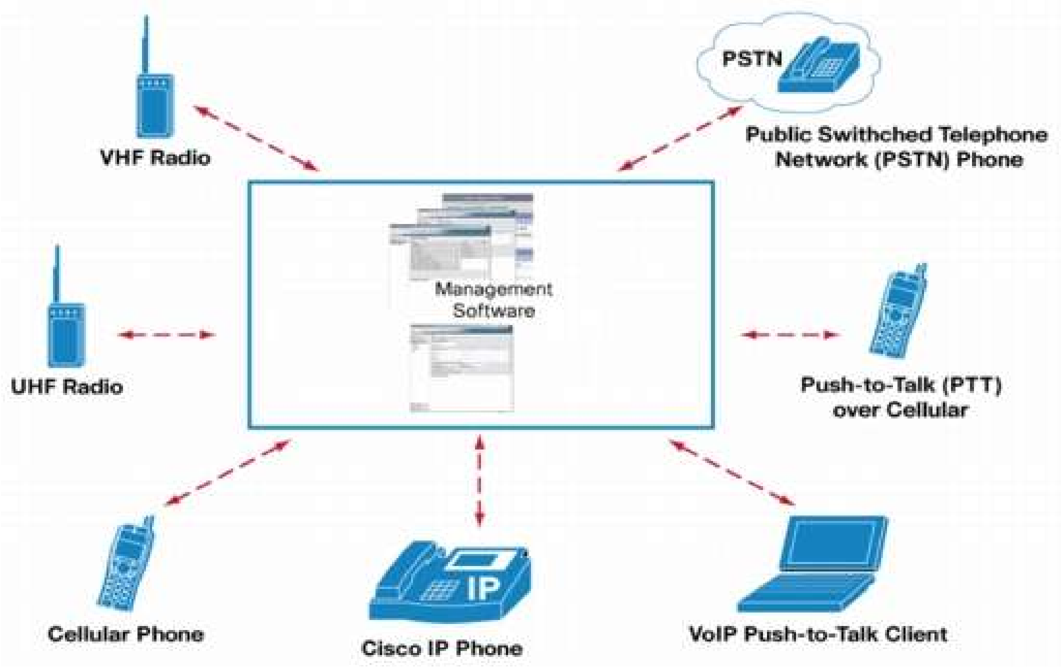
Key skills of Control Room Officers

- Strong communication skill - communicate only what want to
- Strong visualization
- Open mind & attentive
- Good field knowledge / topography
- Good procedural knowledge
- Presentable behaviour with diplomacy
- Commanding skills
- Remain calm for effective emergency management
- Knows who's who

Infrastructure Requirement

- Following systems / infrastructure may be installed as per need:
  - ✓ Phone - multi-line / analog or digital / mobile / hotline-connectivity
  - ✓ Fax
  - ✓ E-Mail
  - ✓ Wireless radio communication - UHF / VHF / Tetra
  - ✓ Bulk sms-ing system / Voice message or mail
  - ✓ Public Address (PA) system
  - ✓ PC based notification / Pop-ups
  - ✓ VoIP
- For large area / complex, interoperate-able communication is important

Infrastructure Requirement (Interoperability)



Following systems / infrastructure may be installed as per need:

- Display system
  - Video wall / large displays
  - Plasma / LCDs
  - PCs / Workstations
- Alarm panel / Hooters
- Resource deployment system
- Dash-board

5.12 Manpower Management

Traditionally, manpower was the only source of security for any organisation. A watchman watching over the security of an organization is familiar sight anywhere in the country. Quite often they are in uniform or in civil dress. Some of these security guards belonged to a particular community which was known to be traditional warriors or guards by inheritance as a family business. They did perform an important duty of protecting the physical assets by acting as a deterrent to potential thieves who pilfer or steal the property of the organisation. In addition most organizations were not seriously concerned about small thefts since it formed a very miniscule part of their assets and the untrained and un uniformed guard generally accomplished the task assigned to him of preventing thefts.

Manpower is critical for the protection of assets and properly trained and disciplined manpower is more critical. If here is a deficiency in the protection of the assets of the industry, the blame will squarely lay in the manpower and its management.

Times have changed and certain automation started taking over the security of the organisation, like access control and surveillance systems. This was followed by gate management and observation posts to protect the vital interests of the organisation. Gate was not the only place where surveillance was introduced, but the perimeter and inside of the premises was also covered by a watch and ward staff. With the value of the goods being manufactured or transported increased in volume and cost, more sophisticated methods of monitoring the movement of products was put in force. The evolution was slow but steady with emphasis still on protecting physical assets.

It was only over the last two decades that security of undertakings was given some push, more so after the effective functioning of the Central Industrial Security Force which emerged as the leading security provider of the Government for major Industrial Undertakings of the country. The CISF which was formed in 1967 is an armed force of the Union with the primary objective of providing security to major Public sector undertakings in the country, some critical and some non critical. CISF evolved a plan of security with emphasis both on manpower and technology which has been replicated in many undertakings in the private sector.

However most of the private security service providers are a disorganised lot. Except for some multinationals and big players, most of the providers are very poor in their output and performance. Private security service has become a lucrative business with very little and no concern for providing the basic minimum service. Most of them do not have any set standards and seem to have emerged only as a commercial business proposition without much security inputs. The performance of the private security providers, prompted the Switzerland Government to evolve International Code of Conduct for Private Security Service Providers.

If one goes into the history of security agencies it can be seen that they were just watch and ward staff providing chowkidari duties in factories or business or commercial establishment. They still perform similar tasks in many undertaking but with improved perception of the need to provide security to the undertaking.

Till the PASARA (Private Security Agencies Regulations Act) act was passed in 2005, the whole private security service was un-monitored/unregulated sector, where the recruitment process, background check of the guards, quality of the guards, training, wages and review of their performance was mostly arbitrary since no external monitoring agency was available to audit their work. Hence, the conditions of service were determined by the owner of the agency and it was essentially a business venture with no periodic review. The hiring companies were also not very adept at examining the quality of the services provided as security is a more refined subject. Presence of uniformed guards at the gate was presumed to be an effective deterrent for potential mischief mongers .As long as no loss was reported, everything was hanky dory. While hiring man power the managements failed to give adequate attention to the quality of the services being provided. Background check of the guards was never undertaken. Some of them were even deployed in critical areas including executive protection. Wages paid both by the management to the security agencies as also the security agencies to the guards and were also well below the minimum wages. Some of the agencies were also exploiting the guards by taking a 12 hour duty, instead of 8 hour duty and not paying minimum wages and not fulfilling the statutory requirements of ESIS, PPF deductions. Of course, welfare measures were out of question. All these led to severe frustration and attrition affecting the quality of services provided and lack of commitment. In fact cases are not wanting where some of the guards have been conniving in pilfering the assets of the company either themselves or in association with professional criminals.

Realising the inherent danger in the functioning of mushrooming security service providers in the country and with many reported cases of violations of many statutory requirements , the Government of India promulgated the Private Security Agencies(Regulation) Act of 2005..The main provisions of the acts include

1) Persons or private security agencies not to engage or provide security guards without license
2) Appointment of a controlling Authority
3) Application for license can be considered only from persons whose antecedents are verified.
4) Certain categories of persons (convicted in an offence or dismissed from government service etc.) are not eligible.
5) Private security agencies to impart training and skills as required to the guards.

6) Preference for ex servicemen, police or home guards for appointment
7) Only those persons who fulfil basic criteria like undergoing training, fulfils certain physical standards, and within a particular age group are eligible for appointment as security guards
8) State government may frame rules
9) Conditions for cancellation of license have also been provided
10) Uniform of military and police not be used

While the above are the broad conditions of grant of license, some states have also incorporated rules as provided in the act. For example the Gujarat Government has framed rules on 18th July 2007.

The main provisions of the rules is the framing of training schedule where the private security agencies are required to impart a minimum of 21 days training to all the security guards. The subjects of training have also been identified. Minimum physical standards have also been prescribed as also a compulsory ID card to be worn by all guards.

Are the security agencies fulfilling the provisions as enumerated in the act and rules and are all the companies hiring these agencies for providing security ensuring that the service provider is fulfilling all the conditions laid down in the act? Unfortunately the answer is the negative for most.

During Security Audit of Industries, it is noticed that though agencies are holding licenses for providing security services, the conditions of the license are rarely fulfilled. The company hiring the agencies are all looking only at the license but not at the conditions required in the license. The most common deficiencies noticed are:

1) Total lack of training or in fact no training is being imparted
2) Physical standards are rarely fulfilled
3) No identifiable uniform or uniforms similar to the police or military are being used.
4) Back ground check of guards not being done
5) Guards are providing 12 hour duties instead of the statutory 8 hour duties
6) Minimum wages are not being paid
7) Supervisors or owners of the security providers have no police or military background
8) The guards sometimes provide day service and continue to provide night service by shifting to a new location and sleeping at the place of duty. This practise would come to the notice of the hirer only when there is a theft and the guard is found sleeping or not alert.

Important Provisions of the Private Security Agencies (Regulations) Act 2005

In order to regulate the functioning of the Private Security Agencies, the Government of India passed the PRIVATE SECURITY AGENCIES REGULATION ACT 2005.

The act provides for the following:

1) Appointment of a controlling authority (Section 3)
2) Private Security Agencies should have a license to operate (Section4)
3) Eligibility and non eligibility for license (Section 5 and 6)
4) Application for grant of a license (Section 7)
5) Conditions for commencement of operations an engagement of supervisors (Section9)
6) Eligibility to be a private security guard (Section 10)
    - Should be a citizen of India
    - Between 18 and 65 years of age
    - Character and Antecedents should have been verified
    - Has completed the prescribed security training successfully
    - Fulfils such physical standards as prescribed
    - Preference to Armed Forces, Police, Home Guards, Para Military Police etc.
7) Cancellation and suspension of license (Section 10)

Important Provisions of the Gujarat Private Security Agencies Rules 2007

1) Verification of the antecedents of the applicant (Rule 3)
2) Verification of the character and antecedents of the private security guard and supervisor (Rule 4)
3) Security training. 100 hours of class room and sixty hours of field training spread over at least twenty working days(Rule 5)
    - Sub rule (2) provides for the subjects which have to covered in the training
    - Sub rule (3) provides for a certificate of having undergone training.
    - Sub rule (4) provides for the competent authority to inspect the training facility.
4) Standards of Physical fitness for security guards (Rule 6)
5) Controlling authority to grant license and conditions thereof (Rule 9 and 10)
6) Photo ID card compulsory (Rule 15)

Most industries are putting the security of their asses at great peril by hiring such untrained personnel for cost cutting. While a qualified guard would cost anything between 15000-20000 rupees, quite a few industries are hiring the personnel at half the cost compromising on security quality.

Additionally most industries do not have an exclusive security department and security is generally handled by the HR department. The coordination required between the management and security personnel is lacking. Management is still looking at the costing of hiring a security guard and are willing to compromise on quality for the sake of cost cutting.

It is not understood why managements do not hire trained manpower especially after the Knowledge and Skill Development Council has provided for skill up-gradation programmes in various skills including Security Guards. The Government of India pays established agencies Rs 9,000/- towards training a security guard and such trained guards can be taken on duty.

Major initiatives have been undertaken by the Government of India through security knowledge and skill development council through a policy formulated in 2009.

What is Security Sector Skill Development Council (SKSDC)?
The National Skill Development Policy 2009 mandates that NSDC would constitute Sector Skill Councils (SSCs) with following functions:

Setting up LMIS to assist planning and delivery of training:

- ✓ Identification of skill development needs and preparing a catalogue of skill types
- ✓ Develop a sector skill development plan and maintain skill inventory
- ✓ Developing skill competency standards and qualifications
- ✓ Standardization of affiliation and accreditation process
- ✓ Participation in affiliation, accreditation, standardization
- ✓ Participation in affiliation, accreditation, standardization
- ✓ Plan and execute training of trainers

Promotion of academies of excellence SKSDC has been formed to transform the Private Security Sector (PSS) from an unorganized industry to an organized one and for addressing issues related to PSS.

Objectives of SKSDC
The objectives of SKSDC are:

- ✓ Promote skill development of the manpower in the PSS and narrow existing gaps between demand and supply
- ✓ Develop framework for upgrading skills of Security Guards to international standards.
- ✓ Undertake research to identify future requirements in training and skill enhancement.
- ✓ Initiate, carry out, execute, implement, aid and assist activities towards skill development in the PSS
- ✓ Develop skill development plan for the PSS
- ✓ Determine skill/competency standards and qualifications
- ✓ Plan and execute Training of Trainers
- ✓ Promote academies of excellence

- ✓ Establish well structured 'Labour Market Information System' to assist planning and delivery of training
- ✓ Facilitate in standardizing the affiliation and accreditation process for the PSS.
- ✓ Identify skill development needs, review international trends and identify sector skill gaps and technology
- ✓ Undertake task of education and vocational skill upgrades
- ✓ Facilitate in setting up robust and stringent certification and accreditation process to ensure acceptability of standards

Why is there a need for an organization like SKSDC?

Today the Private Security Sector (PSS), which is the second largest employer of manpower after the Agriculture Sector, lies in the unorganised sector of our economy and is perhaps not optimally motivated, trained or equipped to successfully take on the challenges that confront it. This sector employing approximately seven million people and growing at an annual rate of 25 per cent comprises youth lacking in education and hailing from the weaker sections of our society. Honing their skills therefore, falls within the ambit of our Prime Minister's vision of up skilling the youth of our country in preparing them to take their rightful place in India's growing economy. SKSDC is therefore mandated to up skill the PSS.

Manpower is the backbone for any security. Despite the advances in Technology and the desire to wish away with manpower since they are bereft with inherent human weaknesses, no organisation can provide fool proof security without a trained and adequate manpower, The quantum of manpower may vary from organisation to organisation, but manpower is a must and we cannot depend only on technology since we need manpower to drive the technology. An ideal situation would be to have a proper mix of man and machine and train all personnel in skill enhancement especially in the security sector.

Technology in Aid of Security

6. Technology in Aid of Security

While manpower plays an important role in the overall security scenario, in today's world it is impossible to visualise a situation where technology in aid of manpower is not considered collaterally for any effective security.

The last quarter century has seen tremendous strides in the concept of technology for security and more and more emphasis is being laid on technology and reduce the requirement of manpower. Tough technology cannot replace manpower fully, it is important to have a proper mix of technology and manpower, since both have their inherent weaknesses and also strengths.

This chapter attempts to portray the available technology both essential and specialised for any industry. Though some technology inputs are fundamental, choice of specialised technology depends on the threat perception, type of product being manufactured and the value of the asset being manufactured. A lot also depends on the inclination of the management to invest in security, especially when one visualises that there is no return on investment in security and returns cannot be quantified The equipment mentioned here cover a wide range of products and their needs arises on the type of product or industry one is guarding especially in terms of its criticality.

While access control and surveillance are fundamental, other equipments which are probably required in any situation have also been disclosed. These are equipments which are essential where there is a likely attempt at sabotage or an external attack .These equipments are required to prevent or minimise loss in critical situations.

There are two fundamental elements in technology support in aid of security. They are access control and surveillance. If these two elements are taken care of security can be near perfect. Most systems are effectively extensions of these two fundamental tenets of technology.

6.1 Access Control Systems

Access control is the process used to identify and verify the credentials of men, material and transport that may pass through an authorised entry or exit point of a protected area. Access control regulates and controls authorised entry and denies unauthorised entry to specific locations. It also ensures that movement within the premises conforms to the level of authorisation. Access control systems ensure that the authorised entry is regulated and unauthorised people / material are kept away.

The objectives of an Access Control Systems are:

- ✓ It should facilitate quick recognition, search and grant of access to authorised people, vehicle and material.
- ✓ It should detect, deny and warn about unauthorised access.
- ✓ It should have the capability to stop and respond to unauthorised or forcible attempts of access.

To achieve this objectives on access control system requires following capabilities :

- ✓ A system to authenticate and identify bonafide men, material and vehicles.
- ✓ A system if effective physical search/check of men material and vehicles to preclude any chances of prohibited items being smuggled in or / or any items being stolen and taken out.
- ✓ A mechanism to react in case of breach of system which may range from local reporting, to initiating legal action, to an effective response to an organised armed attack, depending upon the vulnerability of the installation being protected.

Identification

The biggest challenge before security agencies today is the correct, reliable and positive identification of persons gaining access to a protect area.

The access control system for individuals are primarily based on one of three factors or a combination of them as enumerated below:

- ✓ On the basis of something a person has-such as an ID card or Smart Card etc.
- ✓ On the basis of something an individual knows-such as a password, PIN etc.
- ✓ On the basis of something an individual is-such as finger prints, voice, face, iris, retina etc.

Hence it becomes apparent that the components of a modern access control system could include the following:

1. Authentication Key / Credentials

2. Authentication Device / Readers
3. Access Denial Mechanism (Door and Gates)
4. Controllers
5. PC based software

Authentication Keys/Credentials

Access control systems have evolved through the years and there are different types of Authentication. Keys/Credentials that can all be used to solve enterprise access solutions. Tokens, smart cards, encrypted keys, passwords and biometric features present a range of choices for the system designer. Each such key needs to go through the following cycle to be used effectively by the system.

Enrolment

Key is matched to the personal details of the person in a database to serve as an access control list.

Storage

The information about the person, the key and the access control list need to be stored on the appropriate controller for making decision on allowing/disallowing access at different access points.

Comparison

When presented to the reader, the reader compares the trait presented to the information stored. Then, it either accepts or rejects according to the match, you are who you claim to be.

Biometrics

In biometric systems personal identity is confirmed through unique physiological or behaviour features of humans. Biometrics systems identify humans directly; no codes or passwords are required. Biometrics can be use physical characteristics, like face, fingerprints, iris or veins, or behavioural characteristics like voice, handwriting or typing rhythm. Unlike keys and passwords, personal traits are extremely difficult to lose or forget. These are difficult to copy and for this reason biometrics is considered to be safer and more secure than keys or passwords.

Authentication Device/Readers

Access control readers may be classified by functions they are able to perform. Sometimes readers may have additional features such as LCD and function button for data collection purposes (i.e. clock-in/clock-out events for attendance reports), camera/speaker/ microphone for intercom, and smart card read/write support. Access control readers may also be classified by the type of identification technology and read range. This category has been described along with the credential details.

Access Denial Mechanism (Door and Gates)

These can come in to play for regulating the access of personnel and vehicles. Depending on the security level, aesthetics, space available, presence of security personnel, integration with cameras, authentication key etc., we may choose from a range of options available.

Controllers

Access Control System for Material and Vehicles

Managing access control for materials and vehicles are yet another challenge for security administrator. Firstly, movement of material and vehicles are always linked with movement of people as well, and as such requires all systems / infrastructure required for access control of people too. Secondly, material and vehicles unlike human beings do not possess biometric qualities and as such cannot be identified with the same level of accuracy which is possible in case of humans. In most of the industrial or business establishments, therefore, the access regulations of the material and vehicles is primarily procedural and has to be business specific.

In context of vehicles certain technologies such as RFID and CCTV based number plate recognition systems are being used which can identify the bonafides of a vehicle from a distance thereby giving sufficient reaction time to security agencies. None of the systems, however, are fool proof as both the RFID as well as number plates can be switched over from one vehicle to other.

Scanning Systems

The second important aspect of an access control mechanism is the security check of men, material and vehicles. The security check in an access control system is done from two different perspectives:

- ✓ Security checks when entering a protected area it is done from the point of view of terrorist attack, sabotage, espionage etc. Such a check is based on two basic presumptions. Firstly the access identification system may not be fool proof and it is likely that threat elements may breach the system and gain access to endanger the safety and security of the protected place, and secondly that bonafide people may also become a source of threat.
- ✓ Security check while leaving a protected place is done from the point of view to check theft, pilferage, espionage etc. in this kind of check the employees working in the establishment are main target group for checks.

As discussed earlier, it is also important that such security checks needs to be performed within a defined limit. Manual security checks are manpower oriented and time consuming and yet fail to give desired results. For example, it is difficult to detect explosives by manual checks. It is, therefore, imperative that depending upon the requirement the access control should be designed in a manner which suits the needs of the security agencies. While a detailed list of various scanning equipment is being provided, a security administrator must know his objectives, targets and also his limitations.

Broadly speaking the purpose of a security check is to find out following kind of materials:

- ✓ Weapons (modified weapon and weapons in concealment)
- ✓ Explosives, Bombs, IEDs, Detonators, Plungers, Wires, Batteries or any other kind of power sources etc.
- ✓ RCB materials.
- ✓ Digital data, CD, Pen Drive, Hard Disc etc.
- ✓ Information in hard copy such as files, maps, etc.
- ✓ Any other items being stolen for pecuniary gains or for creating subversion or sabotage.

The above mentioned list is generic and it is obvious that every protected place may or may not have all the threat perceptions but it is logical to presume that it will be a combination of items mentioned above. Architects of the access control systems need to set his objectives and targets first and then decide the design of a check /search matrix.

Physical Search of an Individual

The most popular equipment for carrying out a security check of an individual is a metal detector DFMD & HHMD. Though substantial improvement has been made in the quality of the metal detectors, as the name suggests, it can detect only metals. Further even the best of the DFMDs have a threshold level and they cannot detect metal objects below a defined weight. Thus, if a security check point requires detecting explosives, then use of metal detectors are of no use. Even the most advance kind of DFMDs is not able to detect ammunitions, detonators etc. if carried on person. Further, HHMD or DFMD cannot detect non-metallic weapons or material.

Equipments are available which can scan a human body and can reveal if anything has been concealed below the cloths or even inside the body. Such scanners however are not in common use because of privacy issues. Two kinds of body scanners using different technologies are available in market. One uses X-Ray back scatter technology and the second uses terra Hertz waves, popularly known as millimetre wave technology. Both are extremely good in detecting concealment on or within the body. The X-ray back scatter, however, gives an extremely revealing image of human body which raises moral and ethical issues. Further, though it can reveal the concealment with a greater degree of success, its ability in actually identifying the explosives, drugs etc. is suspect. The body scanner using millimetre wave technology is less revealing, but it suffers from two limitations, first it works on the principle of temperature difference and if something is concealed on body for some time and obtain the same temperature, it may not be detected. Second, ability to identify the material is again suspect. To overcome these problems equipments have been developed which can sniff presence of explosives on human body. These equipment work on the principle of normal explosive detectors and there is no image involved. Such scanners however cannot detect metals and has to be used in conjunction with DFMD. Even, if both the equipments are used still it will not be possible to detect RCB material which will require a completely different set of equipment for its detection.

Similarly, separate equipments are available for checking of shoes, liquids, etc. it is like being treated for symptoms and not for disease. Practically, it is not possible to check everyone with each equipment especially when time available for such checks is limited. The complexities involved in physical search of an individual raises a very significant question whether everyone should be subjected to similar level of check, or some category of people may be subjected to more intensive check. The second principal is followed at most of the Airports in USA. While everyone is subjected to a minimum security check, based on predesigned parameter, some people have to undergo more intensive and through check. Profiling and computer generated random through check methods can be used for this purpose. This need again arises because it is not feasible to subject everyone to similar level of through checks as it is time consuming.

Scanning of Material & Vehicle

The scanning of material and vehicles possess a challenge entirely different from scanning of an individual. In checking an individual, if concealment is detected, that gives enough suspicious to subject the individual to a detailed security check. In case of material scan, this advantage is not available. The security personnel are required to know, the actual nature of material in every case.

Expect CTS (computer tomography X-ray) scanners, other scanners are not able to detect explosives with any degree of success. The back scatter or millimetre wave based scanning technology is useful for scanning humans but not very practical when it comes to scanning materials, as their ability to identify the material is in suspect. Even a CTX scanner cannot detect explosive with the 100% accuracy. It however, narrows down the area of search. A most accurate identification of explosives can be done only by dogs or explosive detectors.

The checking of vehicles is only slightly different from checking of materials. Vehicle checks have two dimensions. One, the vehicle itself is being checked. Two, apart from the vehicle the material loaded in a vehicle such as cargo, etc. is subjected to check. There are scanners which can subject the entire vehicle along with cargo, to check. All these scanners work on the same principle on which a normal X-BIS operates which has limitations in detecting explosives, drugs, etc. under vehicle surveillance system is a useful system for subjecting the chases of the vehicle to security checks. But such checks are relevant to the known vehicle.

Types of Biometric Access Controls

What are Biometrics

- Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioural characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odours.
- Among the many reactions to the September 11 tragedy has been a renewed attention to biometrics

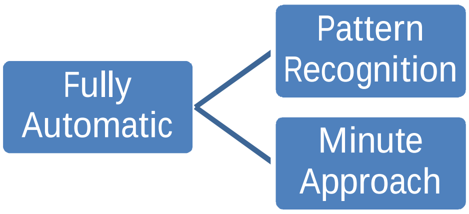
Fingerprint

Your finger is the key that unlocks your car and starts the ignition. Your eyes are your bankcard to withdraw cash. Your hand is the security software that protects your network from intrusions and fraud. Your face opens the door to your workplace. Transcending mere technology, biometrics combines high-tech gadgetry and no-tech biology to create a viable solution to the problem of personal and corporate security.

Fingerprint Comparison

- Fingerprinting is a highly familiar and well-established biometric science.
- The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators by the fingerprints they leave behind them at crime scenes.

- Scientists compare a latent sample left at a crime scene against a known sample taken from a suspect.
- This comparison uses the unique features of any given fingerprint, including its overall shape, and the pattern of ridges, valleys, and their bifurcations and terminations, to establish the identity of the perpetrator.
- In the context of modern biometrics, these features, called fingerprint minutiae, can be captured, analysed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies.
- Fingerprints offer tremendous invariability, changing only in size with age, is highly resistant to modification or injury, and very difficult to "forge" in any useful way.
- Although the development of some sort of surreptitious sensor is not inconceivable, the reality is that sensors remain obtrusive, requiring a wilful finger pressure to gather a useful sample.
- Unlike other systems, based on cameras and high-tech sensors, fingerprint sampling units are compact, rugged, and inexpensive, with commercially available systems from multiple vendors offering very good accuracy.
- Next-generation scanners can analyse below the surface of the skin, and can add pore pattern recognition in addition to the more obvious minutia of the fingerprint.



- Mathematical characterization of the fingerprint or template is created for each individual
- Ideal for applications where identity of an individual must be positively confirmed
- Fast, easy access in less than half a second
- Any one or two fingers can be enrolled
- Controlled access to protected data, service or funds

<u>Signature Comparison</u>

- The biometric most familiar to us is the signature. Our ability to judge by sight if one signature matches another has made this a time-proven and legally-binding biometric.
- However, by sight alone, most of us cannot recognize the pressure of the pen on the paper or the speed and rhythms of its traverse of the page.

- Computers can do all these things, and quantify, analyse and compare each of these properties to make signature recognition a viable biometric technology.
- Being based on things that are not visible (pen pressure and velocity, for example), signature-based biometric technology, offers a distinct advantage over regular signature verification -- in addition to mimicking the letter forms, any potential forger has to fabricate a signature at the same speed, and with the same pen weight, as his victim.

Keystroke Dynamics

- The rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics.
- While distinct, keystroke dynamics are not sufficiently unique to provide identification, but can be used to confirm a user's identity.
- Keystroke dynamics, unlike other biometric technologies, is 100% software-based, requiring no sensor more sophisticated than a home computer.
- Because of this, deployment is occurring in fairly low-stakes, computer-centric applications, such as content filtering and digital rights management, in which passwords to download music are bolstered with by keystroke dynamic verification, to prevent password-sharing.

Facial Recognition

- Effective for surveillance applications
  - First level scan for large low-security situations
  - Passive – does not require user cooperation
- Not a baseline identifier
  - Easy to fool
  - Error enhanced by factors such as lighting, age, glasses, facial hair, head coverings, masks, etc
- Semi-automatic systems more preferred
  - Automatic storage & presentation of picture
  - Manual comparison

Hand Geometry

- Perhaps the most ubiquitous electronic biometric systems are hand geometry based.
- Hand-geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured.
- Made of 27 bones and a complex web of interconnected joints, muscles, and tendons, the human hand presents a sufficiently peculiar conformation of anatomical features to

enable authentication, but is not considered sufficiently unique to provide full identification.

- Further, the geometry of the hand is variable over time, as hand shape may be altered due to injury, disease, aging, or dramatic weight swings.
- A simple hand-geometry system will measure length and thickness of digits, width of the palm at various points, and the radius of the palm.
- This results in a relatively simple identification that can be expressed in a very simple, compact string of data.

<ins>Features</ins>

- Easy to use – high acceptance among users
- Effective identification tool
- Weather, temperature & medical conditions affect hand size
- Hand size & geometry changes with age
- Hygiene issue
- Expensive & bulky equipment

<ins>Deployment of Hand – Geometry</ins>

- In deployment, traditional hand geometry systems have found acceptance in applications requiring verification of an identity, rather than a full proof or establishment of an identity.
- Airports, factories etc. have successfully employed hand-geometry-based systems to restrict access to runways, and to ensure that time cards are being punched only by the worker, and not by that worker's pal on his or her behalf.
- In these instances, the subject is attempting to prove or disprove his or her membership in a relatively small group of people (authorized runway personnel, factory workers).
- When stakes are high, these systems are not relied on exclusively to confirm identity; rather, they are used to provide an additional layer of security above and beyond that provided by existing security systems.

Retinal Pattern of Eye

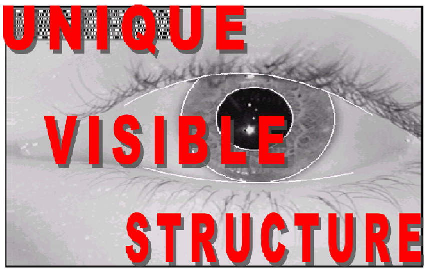
- The veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual.
- Retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target while the scan is completed.
- It's definitely one of the more intrusive biometric technologies, with some subjects reporting discomfort at the scanning method.

Features

- Pattern of blood vessels on retina
- Binocular eyepiece
- Low intensity IR beam used
- Photo Sensor
- Digitized database comparison

Iris Recognition

The iris is the colourful part of the eye between the white (sclera) and the pupil. Its uniqueness in every person stems from variations in features such as furrows, striations, pits, collagenous fibres, filaments, crypts (darkened areas), serpentine vasculature, and freckles. Human iris is more distinct than DNA as identical twins can have the same DNA yet different Iris patterns



- Multiple Contraction Furrows
- Caliginous Fibres
- Crypts
- Coronas
- Striations
- Serpentine Vasculature
- Freckles
- Rifts
- Pits

Advanced Multifactor Biometric Iris Reader

Advantages:

- The iris is more unique than the fingerprint (but less so than the retina)
- Input is stable. Iris patterns do not change over a person's lifetime
- Non-intrusive. The subject can be at a comfortable range from the scanner (but not too far away)

Disadvantages:

- Iris scan device generates a fairly large template, 256 bytes. With the dramatic drop in computer memory cost, however, this does not seen to be much of a problem.
- Tests conducted by independent third parties suggest that iris recognition may yield a FRR performance of 12%, because of various practical (e.g. field) conditions such as the inability of the automated image segmentation routines to distinguish between the straight-line features found in images such as eyebrows or eyelashes and the iris, resulting in an improperly focused image. At this level of performance, users are likely to become frustrated with repeated denials of their legitimate identity claims.
- Single-source. Iris can hold patents to the key elements of iris identification
- High cost
- The iris biometric has not been proven a 1:N match capability
- Advanced Fingerprint based Attendance System enabled with Access Control

Facial Thermogram

Thermal imaging cameras detect radiation in the infrared range of the electromagnetic spectrum (roughly 9000-14,000 nanometers or 9-14 m) and produce images of that radiation, called thermograms.

The variation of branching blood vessels throughout one's face creates a different 'thermal' image from person to person; even identical twins have different facial thermograms. Facial thermograms apparently do not change during a person's lifetime and are not affected by surface or cosmetic changes to the face; even plastic surgery won't change the thermogram unless it goes so deep as to redirect the flow of blood.

Advantages:

- Non-intrusive. The user need not insert a hand or a finger into a reading device
- Input is stable
- Subject can be evaluated covertly, without the subject's knowledge

Disadvantages:

- High cost. Current prices for infrared cameras are high, but are expected to drop dramatically in the next few years
- Large template size; between 2,000 and 3,000 bytes. This can make for slow searching in large database. Further development and video compression techniques may solve this problem in the future.

Signature Recognition

Signature is not new; it has long been the means by which validate all our legal documents. However, absolute validation of signatures is a different matter, one that is much more difficult.

Advantages:

- Each person's signature is very unique, to include the actual letters and the writing style.
- Very little special hardware is needed to implement a signature recognition system.
- Low cost.
- In the latest technology for this biometric, the actual, visible signature (that is seen on the document) is not recorded or stored; only the "dynamics" of the construction (writing) if the signature are actually recorded in digital format. This record can, in turn, be encrypted to prevent tampering and/or copying. Since the actual signature itself is not recorded, most, if not all, of the ever-important privacy concerns are avoided.

Disadvantages:

A person's signature may vary so much that the machine may not always recognize it. In which case, further attempts must be made. However, the latest developments in signature recognition technology (yr.2002) seem to have overcome most, if not all, of the "enrolment" or capture, of the signature biometric.

Voice Recognition

One of the simplest systems is voice recognition. The changes in a person's voice are somewhat due to physical attributes, but mostly due to behaviour patterns. Vocal cords vibrate at about 80 times per second for men, 400 times per second for women. These vibrations are modified by the size of the jaw opening and by tongue and lip shape and position factors that make each person's voice unique.

Advantages:

- Easy to use
- Non-intrusive. A person need only speak into microphone
- Can be used with existing phone systems
- Utilizes existing speech processing software

Disadvantages:

- Computers have difficulty with background noise
- A person's voice will vary with their mood; depression, excitement, anger, etc.
- A person's voice changes when they have a cold or flu
- They can easily be deceived. All it takes a simple tape recorder to capture a person speaking their password

Hand Recognition

Hand geometry as the name suggests uses the shape of the hand to verify the person. Unlike iris, face or fingerprints, the human hand isn't unique.

Advantages:

- A very small template size, easy to maintain and store large database
- High reliability and accuracy
- Robust, user friendly and easy to integrate into existing and third party systems
- Ideal for rough outdoor environments like construction industry and can handle high throughput of people
- Relatively inexpensive offers excellent return on investment

RFID – Radio Frequency Identification

Current RFIDs fall into three categories; active, semi-active, and passive RFID tags. Composed of microchip, antenna, and, in the case of active and semi-passive tags, a battery they are usually enclosed within plastic, silicon or sometimes glass.

Main uses:

- Asset management and retail assets
- Payment by mobile phones
- Transportation payments like toll roads, public transport and season tickets.
- Product tracking
- Transportation and logistics
- Animal identification
- Inventory systems

Advantages:

- RFID offers read and write memory capabilities.
- It can communicate without contact or line of sight.

Anti-intrusion Devices

Barriers

Barriers in principle prevent action or slow progress. It can be defined as a structure or a fence built to bar the passage. Something immaterial that obstructs or impedes entry to a boundary or limit.

- Boom Barriers
- Flap Barriers
- Wedge/Plate barrier
- Drop Arm Barriers
- Crash Resistant Barrier
- Net based, Energy Absorbing, Active Vehicle Barrier
- Quick Connect Barrier

Control of Entry of Packages, Material etc:

All packages and materials entering the premises will have to be examined by security personnel to preclude any harmful substance getting into the premises. Letters are to be screened with Letter Bomb Detectors; other packages are to be subjected to X-Ray scanning and bulky material like construction material by visual and physical examination etc. All items going in are to be accounted for, their weight and other particulars are to be entered and a proper “Inward Voucher” should be prepared. Their acceptance by the concerned should be confirmed in writing.

Similarly, all items being taken out of the premises are to be issued with an “Out Pass” signed by an authorised person. The out pass should contain the description of the item, its weight and other particulars.

Product Vehicle Control

The number of vehicles entering the complex should be properly controlled and checked thoroughly from the point of view of sabotage and also to tally the goods that they are supposed to bring in. Vehicles can be unwitting carriers of explosives with timer devices. For this reason, all vehicles should be parked far away from sensitive areas.

Controlling Access to hazardous substances

To prevent the ingress of explosives, arson-inducing materials, time devices and hazardous substances into the complex, through screening of all mail, packages, parcels, etc. is to be carried out. The under carriage of vehicles should also be thoroughly checked.

Technology Driven Gates

Adequate number of gates should be provided in the perimeter security system for people and material to get into the complex. Gates should be of strong and sturdy material and firmly anchored to the ground. Gates are to be sited with forethought and imagination. If they are located in inconvenient places, workers will attempt to make openings in the wall or the fence and weaken the system. It is advisable to earmark a gate exclusively for employees to enter and exit and one for the movement of vehicles. For visitors, the entry should be through Gate Office. Where large number of contract and casual labour is employed, a separate temporary gate should be provided for them. Adequate arrangements should be made at the gates to check the credentials of the people and materials entering and exiting the premises.

An automatic gate works on the principle of positive identification and provides access, based on an information source, which may be a smart card or combination of smart card with biometric identification. The objective is to restrict unauthorised access.

Swing Gate

Swing gates are operated through communicating with optional devices such as photo sensors and card readers used for gate operation. Sensing request the gates are operated by electro/mechanical devices. Microprocessor based control systems are incorporated in these gate systems.

Features include convenience to open and close gates using a remote control or from guard room or inside the house using a push button or optional devices such as photo sensors, card readers etc. associated with the gate system. These gates can easily be operated by means of a remote control from inside a car or push button from inside the guard room. The Rotary Drive units are silent, reliable and maintenance free. The inbuilt clutch system suspends the motion of the gate, should it come in contact with child or car. A special electrical lock offers the convenience of automatic locking of gate. In case of power failure, the lock may be manually opened with the help of a special pass key. These systems can be installed in existing Swing Gates.

Sliding Gate

These gates systems are operated through communicating with external devices such as photo sensors and card readers used for gate operation. These gates work on an adjustable mechanical clutch which delivers required thrust and provides quiet operation to the gate. The irreversible electromechanical unit keeps the gate securely locked while a special passkey provides release for manual operation during power failure.

The features include timed electrical system plus built in switches offer precise adjustment and added safety to electrical motor. Electronic control panel is designed to accept various controls and safety accessories such as Optical Beam Sensors, Magnetic Card Remote Control etc. which are optional. Suited for industrial gates and heavy duty applications. The options available are Telescopic Sliding gate and Tracked sliding gates

Automatic Telescopic Sliding Gate

Automatic telescopic sliding gates are suitable for sites where there is limited opening space due to structural conditions for the gate to slide. Motorized sliding gates are also available in the markets.

Turnstile Gate

A turnstile is a type of gate that consists of 3 or 4 arms / doors that rotate to allow only one person to pass per rotation. There are two types of turnstiles, half height (waist height) and full height (full body height). It may be totally mechanical device to one that may be integrated with a fully computerised access control. Turnstiles offer better security and better manpower utilization, as they provide only a small passageway and allow only one person to pass at a time. On presenting the valid card the gate will automatically opens/unlocks/rotates and allows the users to pass through the direction requested. The turnstile can also work with push button, finger print and face recognition access control systems.

Waist High Turnstile

Certain models operate on lithium battery. LCD seven digit counters is installed in the turnstile. Each rotation of the turnstile arm generates a count. One counter is required per direction of travel. Counters can be ordered as resettable or non resettable. Resettable counters can be reset to “0” using a provided key. Non resettable counters cannot be reset.

Waist height tripod turnstile for reception areas and full height full security turnstile for unsupervised installations and highly secured areas. Applicable at Airports and metros.

Road Blocker

Road blockers are based on hydraulic drive which is operated by an energy accumulator that can be positioned as far away as 4 m. The hydraulic road blocker is the vehicle control device which can be either integrated with various parking systems or installed as single unit, designed as an effective means of controlling access to high security areas. The hydraulic road blocker is designed to guarantee the full level of security. This facilitates placing several barriers end to end to control exceptionally wide access points. Applicable at Airports, Sea Ports, Governmental buildings, Banks, Prisons, Power Stations, Military sites, Stores, Embassies and Warehouses. The options available is Hump Type – also act as mild speed breaker, do not require digging of road and Flat Type – as the name suggests offers flat surface on the road but requires digging trench across the road. Automatic Spike road blocker Automatic Hump Road Blocker.

Magnum Spike allows the spikes to be field replaced, deployment does not destroy the unit, and post deployment involves moving the used spikes o the side of the road as with any other spikes strip. Portability and ease of deployment are the key features.

Bollards

Bollards works on the principle of the pneumatic jack and solenoid locking device provides the strongest, fastest and most reliable method of operation. These gate systems are operated through communicating with external devices and engaged automatically to avoid entry of unauthorised vehicles. Special passkey provides release for manual operation during power failure. Bollards are used for traffic control and to stop the vehicle like Airports, Seaports and Industries. The options available are Automatic bollards, Semi automatic bollards, fixed and removable bollards.

These are available in various raising heights, diameters and raising speeds. Usually constructed with galvanized steel or stainless steel. Comes with failsafe protection around the installed bollards. Additional safety such as photocells, interactive IR detectors or magnetic loops can also be availed. Drive unit is an underground hydraulic system. Microprocessor controlled drive unit is available which can be interfaced with any standard control system. Operates at a temperature -20 to 80 degree centigrade.

Documents Required at Gates

- General diary (Roznamcha)
- Message register
- Vehicle In/Out register
- Standing orders
- Visitor register
- Foreigners register
- Key issue and deposit register
- Incoming/ outgoing returnable material register
- Material incoming register
- Material outgoing register
- Contractor’s material registers
- Specimen signatures of pass issuing authorities of the plant
- Registers containing important telephone numbers
- Short leave pass register.

Types of Gates

- Main Gate
- Material Gate
- Wicket Gate
- Railway Gate
- ADM Building Gate

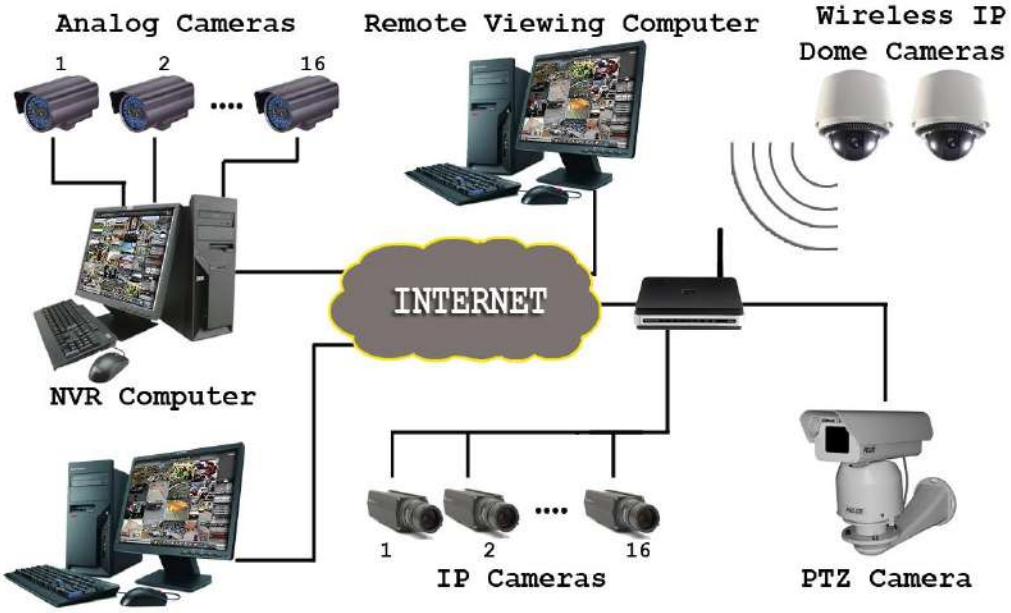
6.2 Video Surveillance System

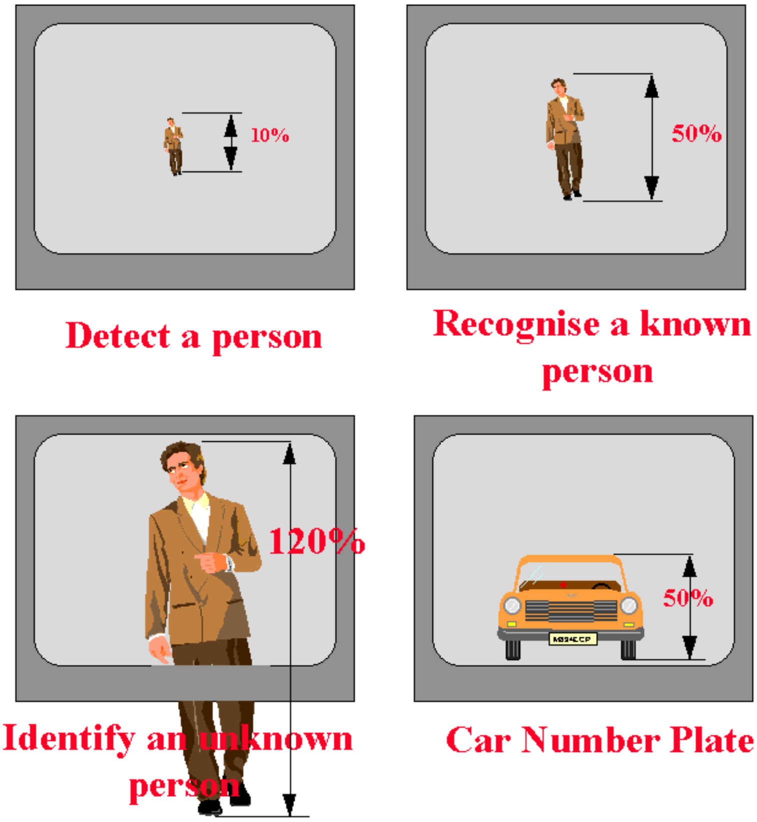
The second most important feature of security is surveillance (the first being access control). While access control ensures that only authorised personnel are allowed access in various parts of the plant, surveillance is required to ensure that the personnel in the plant are performing their legitimate duties and there is no attempt by anyone to indulge in activities prejudicial to the interest of the organisation. Hence movement and activities need to be watched, not only for keeping a track but also to record events which my provide insight into events /incidents

Thus surveillance CCTV system is required to ensure effective surveillance of an area as well as create a tamperproof record for post event analysis. The system shall provide an online display of video images on LCD/LED monitors located in Central control room. System should facilitate viewing of live and recorded images and controlling of all cameras by the authorized users present in the LAN .The network considerations should take into account other systems beyond the CCTV. System should provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. System expansion should not be limited.

Closed Circuit Television systems are used for surveillance covert or overt and they are suitable for monitoring movements in real time to reinforce the access control system with personal identification, in true/false verification of intruder detection, as a part of video motion detection and also can be integrated with a perimeter protection system.

CCTV system comprises of camera, lens, sensor, monitor, housing, pan, tilt & zoom unit, network switches, encoder/decoder, time/date generator, camera identify generator, network video recorder/server, control console etc.




10%
Detect a person
50%
Recognise a known person
120%
Identify an unknown person
50%
Car Number Plate

CCTV

General Specifications

- CCTV system shall be an open standard based integrated system with IP network centric functional and management architecture aimed at providing high-speed manual/automatic operation for best performance.
- System shall use video signals from various types of outdoor CCD/CMOS colour cameras installed at different locations, process them for viewing on workstations/monitors at Central Control Room/local control rooms and simultaneously record all the cameras after compression using H.264. Joystick or Mouse-Keyboard controllers shall be used for Pan, Tilt, Zoom, and other functions of desired cameras.
- System shall have in-built IP or combination of analogue CCD Colour Video Cameras with Fixed or P/T/Z Lens, encoders / decoders, Network Video recorders (NVR), NAS / Raid for back up, Application software, Colour Video Monitors, Keyboards with Joystick controllers / Mouse-Keyboard, workstation for System Administration / Management / Maintenance etc.
- The NVR can be embedded type or server based. However the NVR software shall run on common servers (Camera server & Database server).
- Network Video Recorder shall offer both video stream management and video stream storage management. Recording frame rate & resolution in respect of individual channel shall be programmable.
- System should ensure that once recorded, the video cannot be altered; ensuring the audit trail is intact for evidential purposes.
- System shall provide sufficient storage of all the camera recordings for a period of min 21 days @ 20-30 FPS, at 4 CIF or as per requirement using necessary compression techniques for all cameras
- The video shall be compressed using H.264 and streamed over the IP network.
- The recording resolution and frame rate for each camera shall be user programmable.
- The Area under surveillance shall be monitored and controlled from Central Control Room through workstations.
- Power for all the equipment will be conditioned using on-line UPS with minimum one hour or more back up. If any equipment operates on any voltage other than the supply voltage and supply frequency, necessary conversion/correction device for supply shall be supplied along with the equipment.

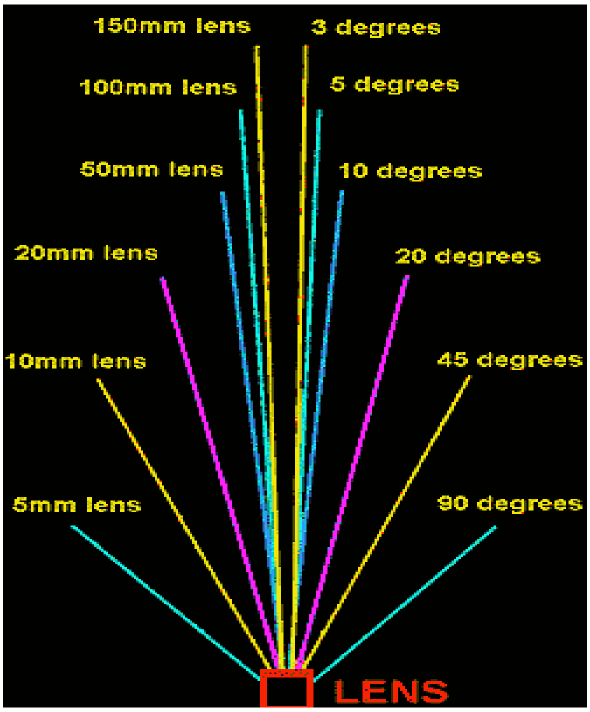
System Requirements

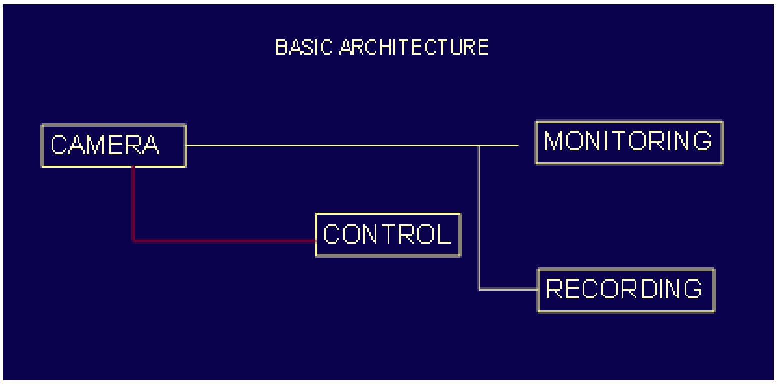
- IP cameras or analogue cameras with external encoder shall be used for image capture.
- All outdoor/indoor Cameras shall be Day/Night cameras.

- Housing of cameras meant for outdoor camera housing shall be of IP 66 or better rating. These must be integrated by the camera manufacturer.
- System must provide built-in facility of watermarking or Digital certificate to ensure tamperproof recording so that these can be used as evidence at a later date, if so desired. The recording shall support audit trail feature.
- All camera recordings shall have Camera ID & location/area of recording as well as date/time stamp. Camera ID, Location/Area of recording & date/time shall be programmable by the system administrator with User ID & Password.
- Facility of camera recording in real-time mode (30/25 FPS)/15/12.5/10 or lower FPS as well as in any desired combination must be available in the system.
- Facility of Camera recording in CIF, 2CIF, 4 CIF as well as in any combination i.e. any camera can be recorded in any quality – Selective or Group of cameras must be available in the system.
- System to have facility of additional camera installation beyond the originally planned capacity.

In order to optimize the memory, while recording, video shall be compressed using MPEG-4 and streamed over the IP network. Once on the network, video can be viewed on a Control room workstation or on analogue monitor using a hardware decoder (MPEG-4/compatible standard Receiver) and shall be recorded on NVR or NAS / Raid and shall be backed up on Backup device.

- System shall be triplex i.e. it should provide facility of Viewing, Recording & Replay simultaneously.
- PTZ Cameras shall have 128 or more pre-defined positions, to be selected through suitable input alarm.
- Redundancy/Fail-over feature is required i.e. in case of failure of an NVR the relevant cameras shall automatically switch over to the redundant NVR.





System Design

- Each camera should have inbuilt Hardware Encoder which shall support minimum dual streams. The encoders should be capable of producing streams @ 25-30 fps for each camera for viewing on LAN and on monitors and also recording into the NVR @ 30 fps or lower frame rate, user selectable as per requirement, for each individual camera.
- At any stage the operator shall be able to see any camera at full resolution and full rate with no quality degrading.
- Central/Local Control Room will have workstations along with controllers for Camera operation. For monitoring purposes, Video monitors shall be setup with suitable mounting arrangements, as per user requirements. Facility for viewing and controlling all the cameras at various other locations, as required, shall be provided.
- Monitoring at Local control rooms may be restricted to operation of certain cameras only & system administrator should be able to configure the system, accordingly.
- There shall be a Control System with Video Control Software to manage all the video surveillance devices.
- Database Server shall keep track of all configurations & events. This will help in proper System administration & management of redundancies etc.
- System shall have provision to automatically over-write the new information after the period of 21 days & necessary script/algorithm must be available in the Application.

- All the workstations in LAN should be provided with software to view and control the cameras, encoders and retrieve the recorded video images from the NVR and backup device seamlessly.

PTZ Camera

PTZ is an abbreviation for pan, tilt and zoom and reflects the movement options of the camera. Surveillance cameras of this type are often connected to a digital video recorder which records the full field of view in full quality.

The following are recommended specifications for a PTZ camera

Key Features

SNP-5430H/5430
1.3Megapixel HD 43x Network PTZ Dome Camera
REVISED 10-2014 58

- Max. 1.3M (1280 x 1024) resolution
- 16 : 9 HD (720p) resolution support
- 3.5 ~ 150.5mm (43x) optical zoom, 16x digital zoom
- H.264, MJPEG dual codec, Multiple streaming
- Day & Night (ICR), WDR (120dB)
- Auto tracking, Intelligent video analytics
- PoE+, SD/SDHC/SDXC memory slot, Bi-directional audio support
- IP66 (SNP-5430H) / IK10 (SNP-5430H, SNP-5430 + SHP-3701H only)

Video

- Imaging Device 1/4" 1.3M CMOS
- Total / Effective Pixels 1,392(H) x 1,076(V), 1.49M pixels / 1,368(H) x 1,049(V), 1.43M pixels
- Scanning System Progressive
- Min. Illumination Color : 0.5Lux (F1.4, 50IRE), 0.3Lux (F1.4, 30IRE)
- B/W : 0.01Lux (F1.4, 50IRE), 0.006Lux (F1.4, 30IRE)
- S / N Ratio 50dB
- Video Output CVBS : 1.0 Vpp / 75Ω composite, 720 x 480(N), 720 x 576(P), for installation

Lens

- Focal Length (Zoom Ratio) 3.5 ~ 150.5mm (Optical 43x)
- Max. Aperture Ratio F1.4(Wide) / F4.9(Tele)
- Angular Field of View H : 53.92˚(Wide) ~ 1.396˚(Tele) / V : 44.08˚(Wide) ~ 1.12˚(Tele)

- Min. Object Distance Wide : 1.4m (4.59ft), Tele : 1.9m (6.23ft) Wide : 1.5m (4.92ft), Tele : 2m (6.56ft)
- Focus Control Auto / Manual / One push
- Lens / Mount Type DC auto iris / Board-in type
- Pan / Tilt / Rotate
- Pan / Tilt Range 360˚ Endless / 210˚ (-15˚ ~195˚)
- Pan / Tilt Speed Preset : 700˚/sec, Manual : 0.024˚/sec ~ 120˚/sec
- Preset / Preset Accuracy 255ea / ±0.2˚
- Auto Tracking Off / On

Operational

- Camera Title Off / On (Displayed up to 15 characters)
- Day & Night Auto (ICR) / Color / B/W
- Backlight Compensation Off / BLC / HLC / WDR
- Wide Dynamic Range 120dB
- Contrast Enhancement SSDR (Samsung Super Dynamic Range) (Off / On)
- Digital Noise Reduction SSNRIII (2D+3D noise filter) (Off / On)
- Digital Image Stabilization Off / On
- Defog Off / Auto / Manual
- Motion Detection Off / On (4ea rectangle zone)
- Privacy Masking Off / On (32 zones of rectangle zone)
- Gain Control Off / Low / Middle / High
- White Balance ATW / AWC / Manual / Indoor / Outdoor / Mercury / Sodium
- Electronic Shutter Speed Minimum / Maximum / Anti flicker (2 ~ 1/12,000sec)
- Digital Zoom 16x
- Flip / Mirror Off / On
- Intelligent Video Analytics Tampering, Virtual line, Enter / Exit, (Dis)Appear, Audio detection, Face detection
- Alarm I/O Input 4ea / Output 2ea (Relay)
- Remote Control Interface RS-485
- RS-485 Protocol Samsung-T/E, Pelco-P/D, Panasonic, Honeywell, AD, Vicon, Bosch, GE
- Alarm Triggers Motion detection, Tampering, Audio detection, Face detection,
- Video analytics, Alarm input, Network disconnection
- Alarm Events
- File upload via FTP and E-mail, Notification via E-mail, TCP and HTTP,
- Local storage (SD/SDHC/SDXC) or NAS recording at network disconnected & event (Alarm
- triggers), External output

Network

- Ethernet RJ-45 (10/100BASE-T)
- Video Compression Format H.264 (MPEG-4 part 10 / AVC), MJPEG
- Resolution 1280 x 1024, 1280 x 720, 1024 x 768, 800 x 600, 640 x 480, 320 x 240
- Max. Framerate
- H.264 : Max. 60fps at all resolutions
- MJPEG : 1280 x 1024, 1280 x 720, 1024 x 768 : Max. 15fps
- 800 x 600, 640 x 480, 320 x 240 : Max. 30fps
- Smart Codec Manual mode (Area-based : 5ea), Face detection mode
- Video Quality Adjustment H.264 : Compression level, Target bitrate level control, MJPEG: Quality level control
- Bitrate Control Method H.264 : CBR or VBR, MJPEG : VBR
- Streaming Capability Multiple streaming (Up to 10 profiles)
- Audio In Selectable (Mic in / Line in), Supply voltage : 2.5V DC (4mA), Input impedance : approx. 2K Ohm
- Audio Out Line out (3.5mm mono jack), Max output level : 1 Vrms
- Audio Compression Format G.711 u-law/G.726 selectable, G.726 (ADPCM) 8KHz,
- G.711 8KHz, G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps
- Audio Communication Bi-directional audio
- IP IPv4, IPv6
- Protocol TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTSP, RTCP, NTP, HTTP, HTTPS, SSL, DHCP, PPPoE, FTP,
- SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour
- Security HTTPS(SSL) login authentication, Digest login authentication
- IP address filtering, User access log, 802.1x authentication
- Streaming Method Unicast / Multicast
- Max. User Access 15 users at unicast mode
- Edge Storage
- SD/SDHC/SDXC (SNP-5340 : micro SD type, SNP-5340H : SD type)
- Motion Images recorded in the SD/SDHC/SDXC memory card can be downloaded
- NAS (Network Attached Storage)
- Application Programming Interface ONVIF profile S, SUNAPI (HTTP API), SVNP 1.2
- Webpage Language English, French, German, Spanish, Italian, Chinese, Korean, Russian, Japanese, Swedish, Danish, Portuguese,
- Turkish, Polish, Czech, Rumanian, Serbian, Dutch, Croatian,

Hungarian, Greek, Finnish, Norwegian

- Web Viewer
- Supported OS : Windows XP / VISTA / 7 / 8 / 8.1, MAC OS X 10.7 / 10.8
- Supported Browser : Microsoft Internet Explorer (Ver. 8 ~ 11), Mozilla Firefox (Ver. 9 ~ 19),
- Google Chrome (Ver. 15 ~ 32), Apple Safari (Ver. 6.0.2(Mac OS X 10.8, 10.7 Only), 5.1.7)
- * Mac OS X only
- Central Management Software SmartViewer, SSM

Environmental

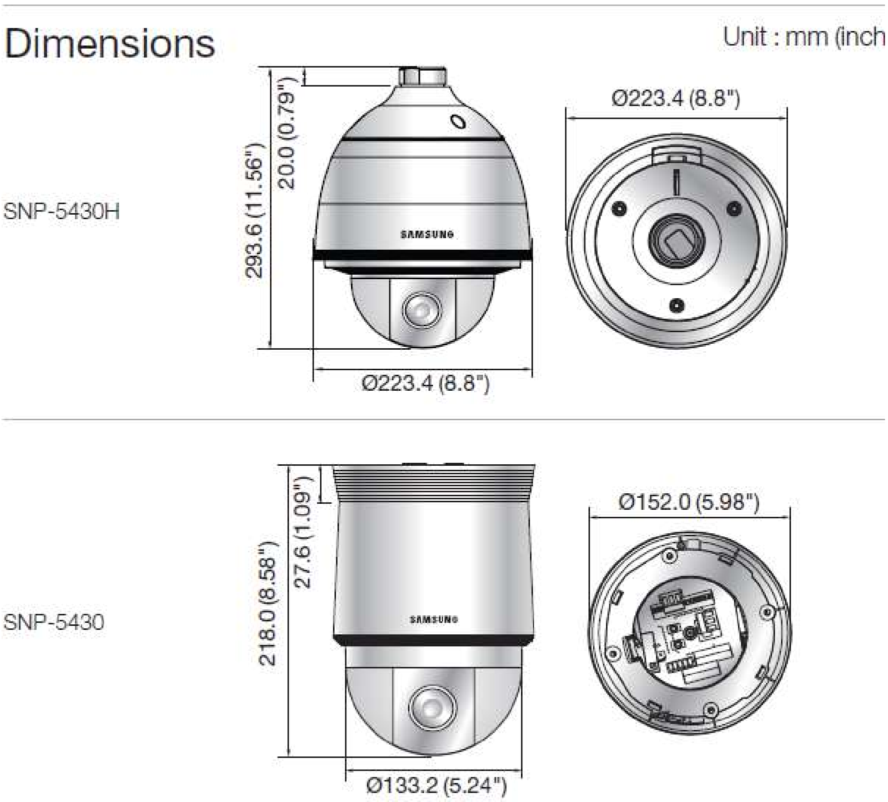
- Operating Temperature / Humidity
- 24V AC : -50°C ~ +55°C (-58°F ~ +131°F) / Less than ~ 90% RH
- PoE+ : -30°C ~ +55°C (-22°F ~ +131°F) / Less than 90% RH
- -10°C ~ +55°C (+14°F ~ +131°F) / Less than 90% RH
- Storage Temperature / Humidity -30°C ~ +60°C (-22°F ~ +140°F) / Less than 90% RH
- Ingress Protection / Vandal Resistance IP66 / IK10 N/A / IK10 (With SHP-3701H)

Electrical

- Input Voltage / Current 24V AC ±10%, PoE+ (IEEE802.3at class3)
- Power Consumption
- Max. 24W (Heater off),
- Max. 65W (Heater on, 24V AC)
- Max. 20W

Mechanical

- Color / Material Ivory / Plastic + Metal
- Dimensions (WxH)
  - 23.4 x 293.6mm (Ø8.8" x 11.56")
  - 52.0 x 218.0mm (Ø5.98" x 8.58")
- Weight 3.4Kg (7.5 lb) 2.2Kg (4.85 lb)



Source: SNP – 5430H Datasheet by Samsung

Fixed Video Camera

Video

- Imaging Device 1/2.8" PS Exmor 2.38M CMOS
- Total Pixels 1,952(H) x 1,116(V)
- Effective Pixels 1,944(H) x 1,104(V)

- Scanning System Progressive
- Min. Illumination Color: 0.1Lux (1/30sec, F1.2, 50IRE), 0.0017Lux (2sec, F1.2, 50IRE), B/W: 0Lux (IR LED on)
- S / N Ratio 50dB
- Video Output CVBS: 1.0 Vp-p / 75Ω composite, 704 x 480(N), 704 x 576(P), for installation, DIP connector type

Lens

- Focal Length (Zoom Ratio) 3 ~ 8.5mm (2.8x) motorized varifocal
- Max. Aperture Ratio F1.2
- Angular Field of View H : 105.5°(Wide) ~ 37.1°(Tele) / V : 57.5°(Wide) ~ 21.0°(Tele)
- Min. Object Distance 0.5m (1.64ft)
- Focus Control Simple focus (Motorized V/F) / Manual, Remote control via network (Manual, Simple focus)
- Lens Type DC auto iris
- Mount Type Board-in type

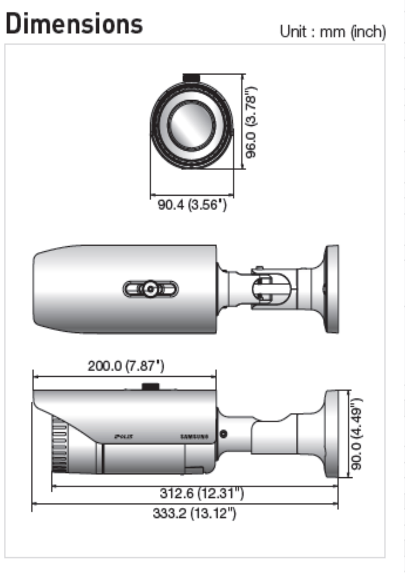
Operational

- IR LED 20ea
- Viewable Length 30m (98.43ft)
- Camera Title Off / On (Displayed up to 45 characters)
- Day & Night Auto (ICR) / Color / B/W / External / Schedule
- Backlight Compensation Off / BLC
- Wide Dynamic Range 100dB
- Contrast Enhancement SSDR (Samsung Super Dynamic Range) (Off / On)
- Digital Noise Reduction SSNRIII (2D+3D noise filter) (Off / On)
- Digital Image Stabilization Off / On
- Defog Off / Auto / Manual
- Motion Detection Off / On (4ea 4points polygonal zones)
- Privacy Masking Off / On (32zones with 4points of polygonal)
- Gain Control Off / Low / Middle / High
- White Balance ATW / AWC / Manual / Indoor / Outdoor
- Electronic Shutter Speed Minimum / Maximum / Anti flicker
- Flip / Mirror Off / On
- Intelligent Video Analytics Tampering, Virtual line, Enter/Exit, Appear / Disappear, Audio detection, Face detection
- Alarm I/O Input 1ea / Output 1ea
- Alarm Triggers Motion detection, Tempering, Audio detection, Face detection,
- Video analytics, Network disconnection, Alarm input

- Alarm Events File upload via FTP and E-mail, Notification via E-mail, TCP,
- Local storage (SD/SDHC/SDXC) recording at Network disconnected & Event (Alarm triggers), External output

Network

- Ethernet RJ-45 (10/100BASE-T)
- Video Compression Format H.264 (MPEG-4 part 10/AVC), MJPEG
- Resolution 1920 x 1080, 1280 x 1024, 1280 x 960, 1280 x 720, 1024 x 768,
- 800 x 600, 800 x 450, 640 x 480, 640 x 360, 320 x 240, 320 x 180
- Max. Framerate
- H.264: Max. 60fps at all resolutions
- MJPEG: 1920 x 1080, 1280 x 1024, 1280 x 960, 1280 x 720, 1024 x 768: Max. 15fps
- 800 x 600, 800 x 450, 640 x 480, 640 x 360, 320 x 240, 320 x 180 : Max.30fps
- Video Quality Adjustment H.264: Compression level, Target bitrate level control, MJPEG : Quality level control
- Bitrate Control Method H.264: CBR or VBR, MJPEG : VBR
- Streaming Capability Multiple streaming (Up to 10 profiles)
- Audio In Selectable (Mic in / Line in), Max output level : 1 Vrms
- Supply voltage: 2.5V DC (4mA), Input impedance : approx. 2K Ohm
- Audio Out Line out (3.5mm stereo mini jack)
- Audio Compression Format G.711 u-law /G.726 selectable, G.726 (ADPCM) 8KHz, G.711 8KHz
- G.726: 16Kbps, 24Kbps, 32Kbps, 40Kbps
- Audio Communication Bi-directional audio
- IP IPv4, IPv6
- Protocol TCP/IP, UDP/IP, RTP (UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL, DHCP, PPPoE, FTP, SMTP, ICMP, IGMP,
- SNMPv1/v2c/v3 (MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour
- Security HTTPS (SSL) login authentication, Digest login authentication
- IP address filtering, User access log, 802.1x authentication
- Streaming Method Unicast / Multicast
- Max. User Access 15 users at unicast mode
- Memory Slot Micro SD/SDHC/SDXC
- Motion images recorded in the SDXC/SDHC/SD memory card can be downloaded



- Application Programming Interface ONVIF profile S, HTTP API v2.0, SVNP 1.2
- Webpage Language
- English, French, German, Spanish, Italian, Chinese, Korean, Russian, Japanese,
- Swedish, Danish, Portuguese, Turkish, Polish, Czech, Rumanian, Serbian, Dutch,
- Croatian, Hungarian, Greek, Norwegian, Finnish
- Web Viewer
- Supported OS: Windows XP / VISTA / 7 / 8, MAC OS X 10.7
- Supported Browser: Microsoft Internet Explorer (Ver. 10, 9, 8, 7),
- Mozilla Firefox (Ver. 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9),
- Google Chrome (Ver. 25, 24, 23, 22, 21, 20, 19, 18, 17, 16, 15),
- Apple Safari (Ver. 6.0.2(Mac OS X 10.8, 10.7 only), 5.1.7) * Mac OS X only
- Central Management Software Smart Viewer 4.0

Environmental

- Operating Temperature / Humidity 24V AC: -50°C ~ +55°C (-58°F ~ +131°F) / Less than 90% RH
- 12V DC, PoE : -10°C ~ +55°C (+14°F ~ +131°F) / Less than 90% RH
- Storage Temperature / Humidity -30°C ~ +60°C (-22°F ~ +140°F) / Less than 90% RH
- Ingress Protection IP66 grade
- Vandal Resistance IK10

Electrical

- Input Voltage / Current 12V DC, 24V AC, PoE (IEEE802.3af)
- Power Consumption Max. 11W (Heater off), Max. 17W (24V AC - Heater on)

Mechanical

- Color / Material Dark gray / Metal
- Dimensions (WxHxD) 90.4 x 96.0 x 333.2mm (3.56" x 3.78" x 13.12")
- Weight 1.19Kg (2.62 lb)

Source: SN0 – 6084R Datasheet by Samsung

6.3 Intrusion Detection Systems

Active Infra-Red Barrier

It is a perimeter protection system generally installed for outdoor application. They can be single beam or multi beam barriers which minimises the evasion of detection of an intruder. The maximum range recommended is 150 metres, but as it works on line of sight condition for undulated land or zigzag perimeter range may become lesser.

The system consists of a transmitter column and a receiver column spaced apart by about some distance (150 metres). Transmitter generates modulated light beam using infra red source and mirrors to form a beam which are received by the receiver column consisting of photocell detectors. Thus it constitutes invisible & continuous beams between transmitter and receiver which are connected to control panel. When an intrusion takes place cutting across the beam, it disturbs the beam path and a visual alarm showing the zone of intrusion associated with an aural alarm notifies the detection. To increase the degree of detection and to compensate for the failure of any single Tx-Rx pair in the four beam system, 16 beams, four from each transmitter are used.

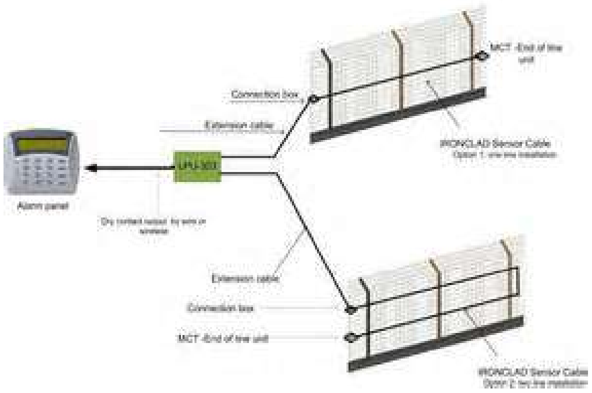
The system is prone to produce false alarms, in the event of heavy downpour and vegetation and less effective in detection in fog and mist.

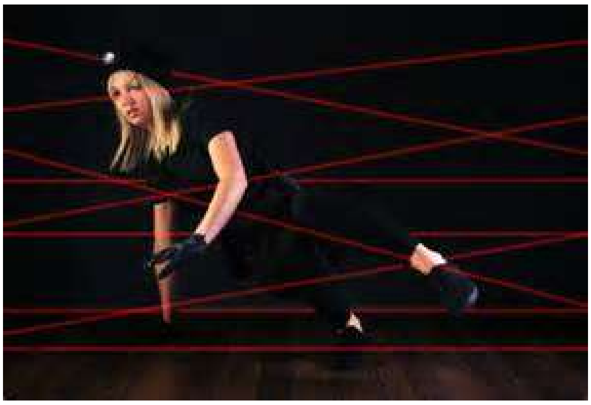
Microwave Barrier

It consists of a pair of free standing structures - one is a transmitter and the other a receiver. Microwave transmitter transmits energy in the form of electromagnetic energy in the range of 10 GHz, which is received by the receiver, spaced at a distance of about 150 Metres. It is an active and visible perimeter protection system and works on line of sight condition. It detects the intrusion when the Microwave beam is disturbed. Transmitter Power is of the order of 6 Watts.

Microwave barrier are generally used between the external perimeter and inner perimeter and on detection it sends a visual alarm in the zone associated with audio alarm in the control panel. As the frequency is very high, it is not affected by wide range environmental conditions and thus false alarm rate is very low.

Laser Detection System





It is an invisible and active perimeter protection system. It can be used for indoor applications also. A transmitter consisting of an infra red source emits an invisible beam and that is made into a sharp pencil beam for rectilinear propagation by using a lens arrangement and the pencil beam is received by a photo electric detector after being focussed by lens arrangement at the receiver placed at about 70 - 100 ft. outdoor or 20-30 ft in indoor application. Transmitter and receiver are to be perfectly aligned. There are in fact, two pencil beams, one above the other with a spacing of a few inches and when both the beams are interrupted by intrusion, only then the alarm is activated. The beam has 700 pulse per second at 8800 A^0 with a designable interruption period ranging from 50 to 500 m/sec. It requires a power input of 10 to 30 V DC and draws a current of 35 mA.

Magnetic Contacts (Door Switches)

This device is utilised in detecting unauthorised entry to any secure room when the door is closed during non-working hours. It works on a device consisting of two small magnetic contacts. One is fitted in the Door Frame connected through an electrical wire and the other terminal being connected to the Main Process Control. The other magnet is fitted in the door sidings exactly at the opposite part. Once the door is kept closed, the magnets will have closed contact. When the door is opened the magnets get displaced. This disconnection of two magnets will trigger the main process which in turn raises an alarm as well as glow of red LED, indicating alarm condition.

Pressure Mat

This device is helpful in detecting any unauthorised entry into a secure/ vital installation at the entry point. Two layers of metal foils are separated by a layer of perforated foam plastic. When the pressure is applied to the mat, the foil sheets make contact through the foam perforations and give alarm. Alternately, a push switch/or a combination of push switches / pressure switches placed under a door mat, makes contact and thus an alarm is activated. The pressure switch can be designed for a specific minimum pressure so as to minimise false alarm rate due to movements of small animals.

Vibration Detector

This equipment is helpful in detecting any person who gains access into protected area either by scaling over or cutting the fencing. This equipment is fitted on chain-link fencing/taut wire. The equipment control is connected to the main process controller kept in the Control Room. When any person tried to climb or scale or cut the fence, the vibrations caused by the action are processed and detected after a level of adjusted sensitivity one activates a alarm in the control panel.

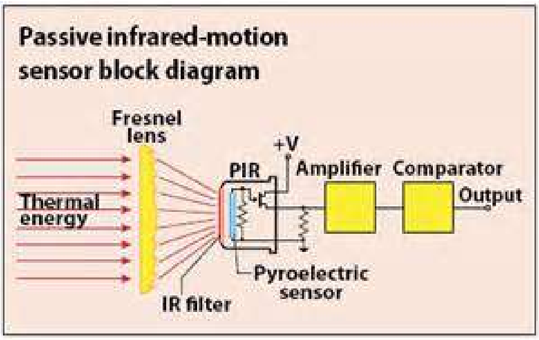
Features

- ✓ Instantaneous intrusion detection.
- ✓ Adjustable sensitivity
- ✓ Facility for individual zone selection
- ✓ Incorporates tamper protection circuits.

Passive Infra Red Detector

This device encapsulated in an inert gas chamber and detects the infra red component of thermal radiation of the human body against the ambient conditions when a person passes in front of the device in a volumetric space of radius (optical field of view) of 15-25 ft.

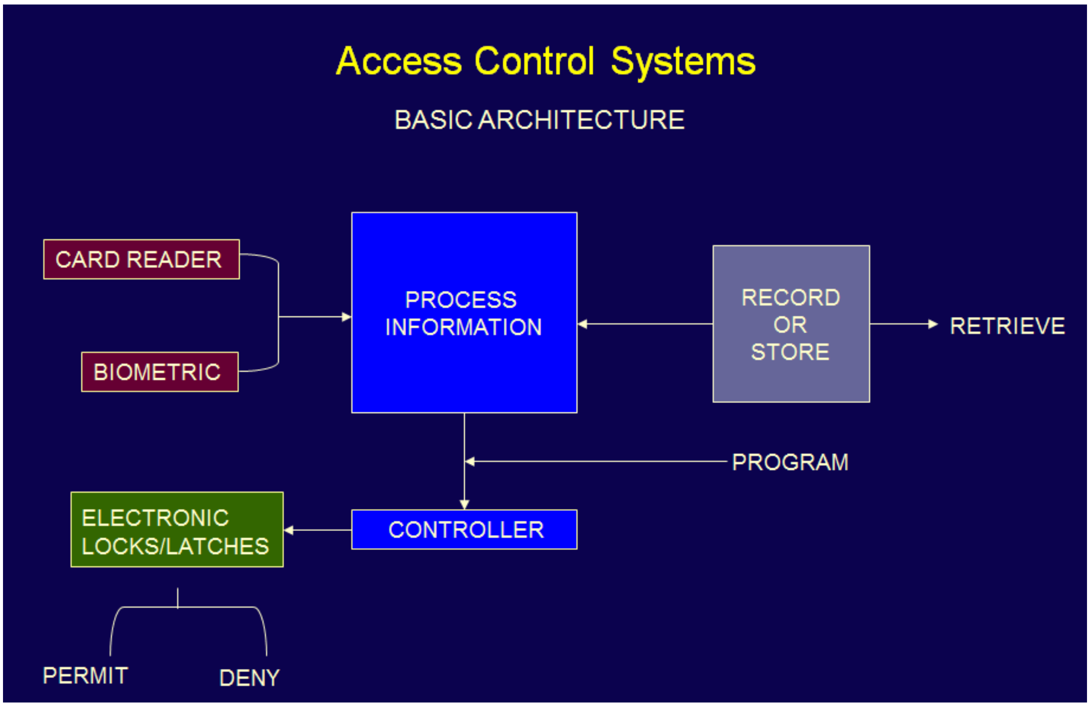
1. Miniature wall mounted intruder sensor
2. Heat sensitive
3. The detection pattern can be varied for long range or short range with varying zone adjustment.
4. Power consumption very low.



Glass Break Detector

This is an Indoor intrusion detection system where the breaking of glass of windows to gain entry into a premise by sensor fitted on glass panes of the window of any building. If someone breaks the glass, it generates a specific range of frequencies that is different from vibrations caused by other disturbances and it is precisely detected using a Band Pass Filter which will filter out other frequencies except that of glass break only and activates an alarm on positive detection. Thus false alarms are minimised.

Configuration and Architecture



Access Control Systems

BASIC ARCHITECTURE

CARD READER

BIOMETRIC

PROCESS INFORMATION

RECORD OR STORE

RETRIEVE

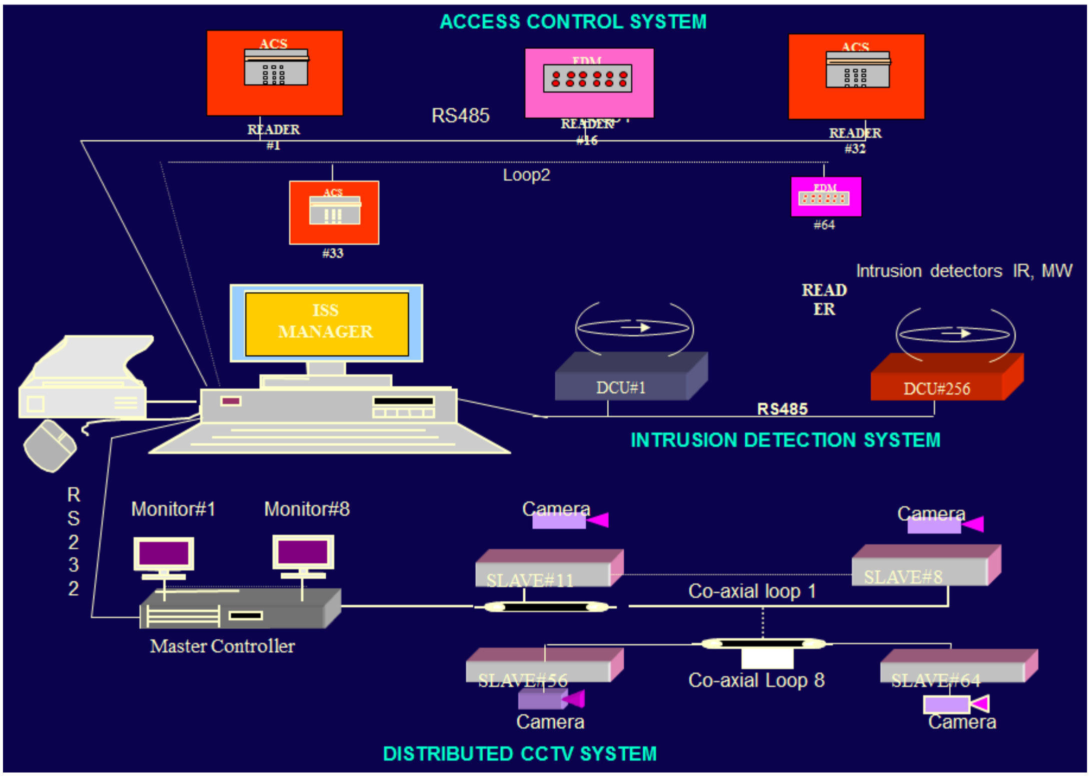
PROGRAM

ELECTRONIC LOCKS/LATCHES

CONTROLLER

PERMIT

DENY



ACCESS CONTROL SYSTEM

ACS

READER #1

RS485

FDM

READER #16

ACS

READER #32

Loop2

ACS

#33

FDM

#64

Intrusion detectors IR, MW

READ ER

ISS MANAGER

DCU#1

DCU#256

RS485

INTRUSION DETECTION SYSTEM

R S 2 3 2

Monitor#1

Monitor#8

Master Controller

Camera

SLAVE#11

Camera

SLAVE#8

Co-axial loop 1

SLAVE#56

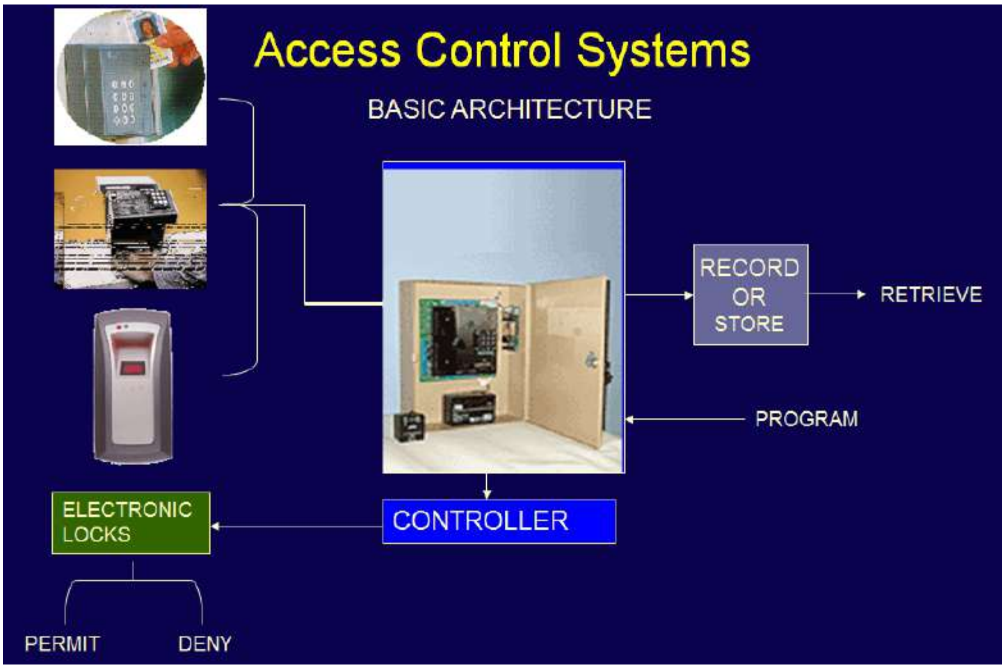
Co-axial Loop 8

SLAVE#64

Camera

Camera

DISTRIBUTED CCTV SYSTEM



Access Control Systems

BASIC ARCHITECTURE

RECORD OR STORE

RETRIEVE

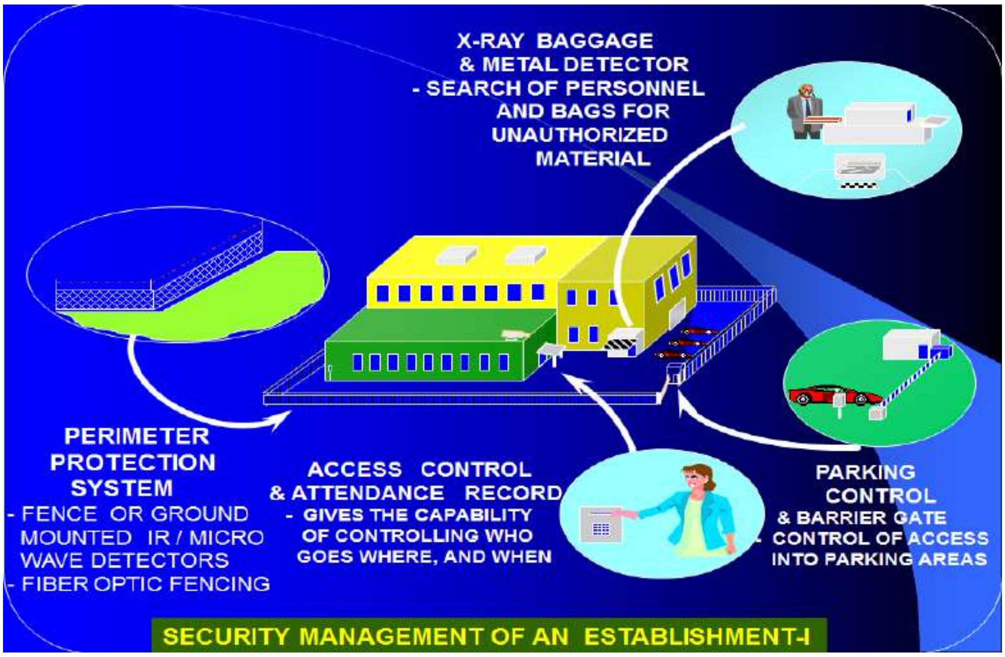
PROGRAM

CONTROLLER

ELECTRONIC LOCKS

PERMIT

DENY



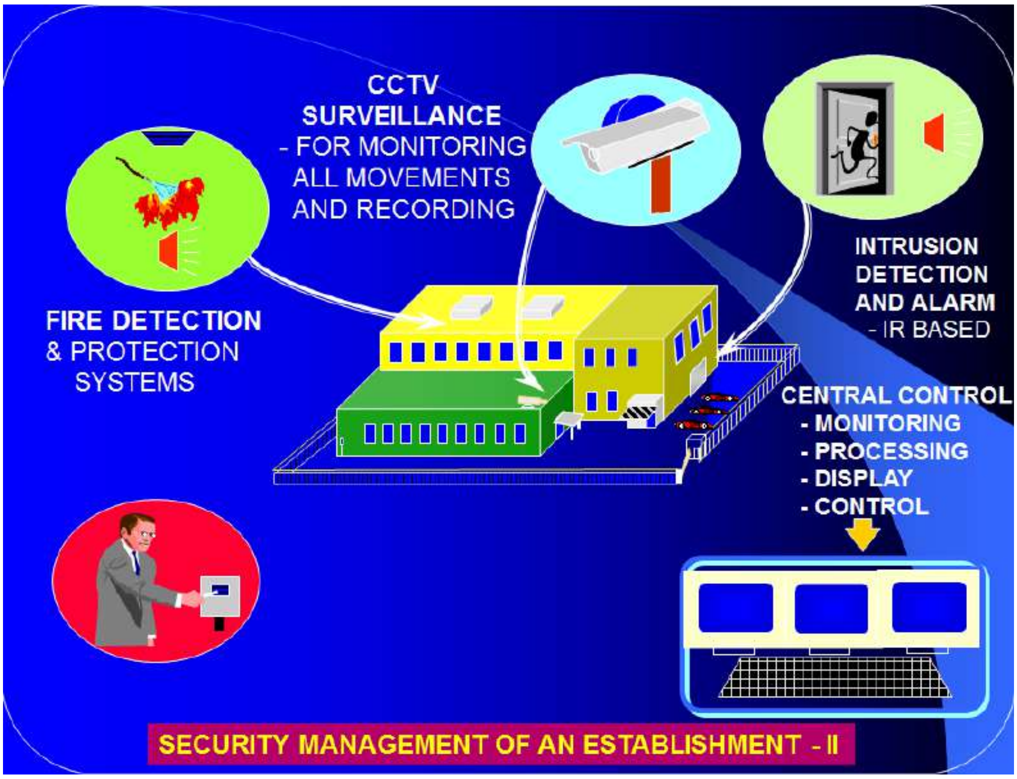
X-RAY BAGGAGE & METAL DETECTOR
- SEARCH OF PERSONNEL AND BAGS FOR UNAUTHORIZED MATERIAL

PERIMETER PROTECTION SYSTEM
- FENCE OR GROUND MOUNTED IR / MICRO WAVE DETECTORS
- FIBER OPTIC FENCING

ACCESS CONTROL & ATTENDANCE RECORD
- GIVES THE CAPABILITY OF CONTROLLING WHO GOES WHERE, AND WHEN

PARKING CONTROL & BARRIER GATE
CONTROL OF ACCESS INTO PARKING AREAS

SECURITY MANAGEMENT OF AN ESTABLISHMENT-I



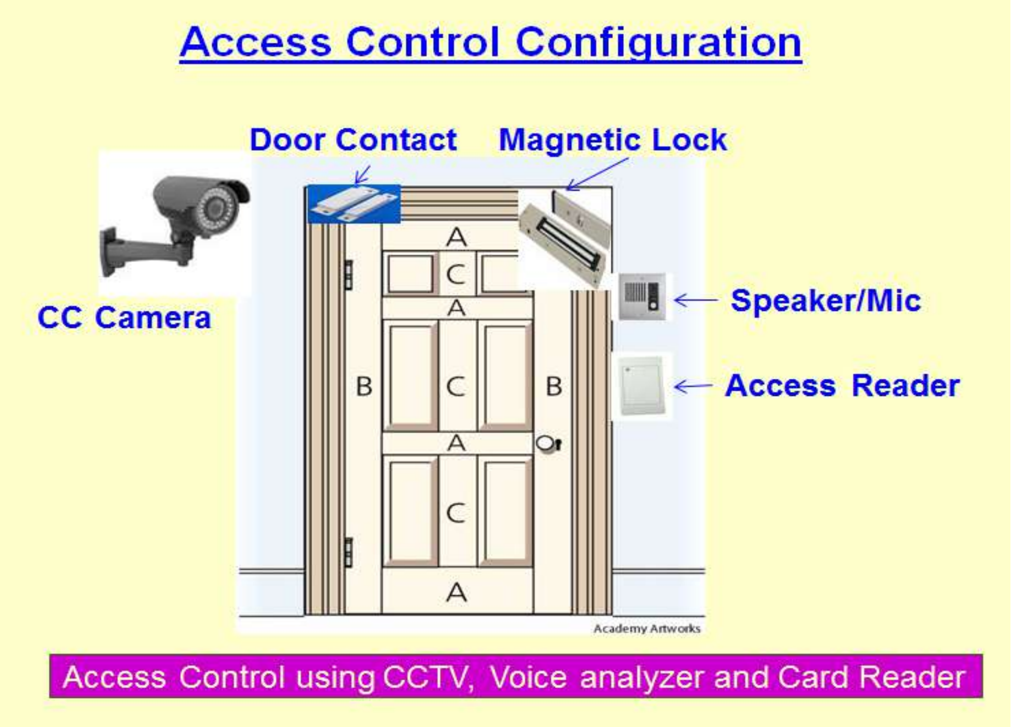
CCTV SURVEILLANCE
- FOR MONITORING ALL MOVEMENTS AND RECORDING

FIRE DETECTION & PROTECTION SYSTEMS

INTRUSION DETECTION AND ALARM
- IR BASED

CENTRAL CONTROL
- MONITORING
- PROCESSING
- DISPLAY
- CONTROL

SECURITY MANAGEMENT OF AN ESTABLISHMENT - II



Access Control Configuration

Door Contact

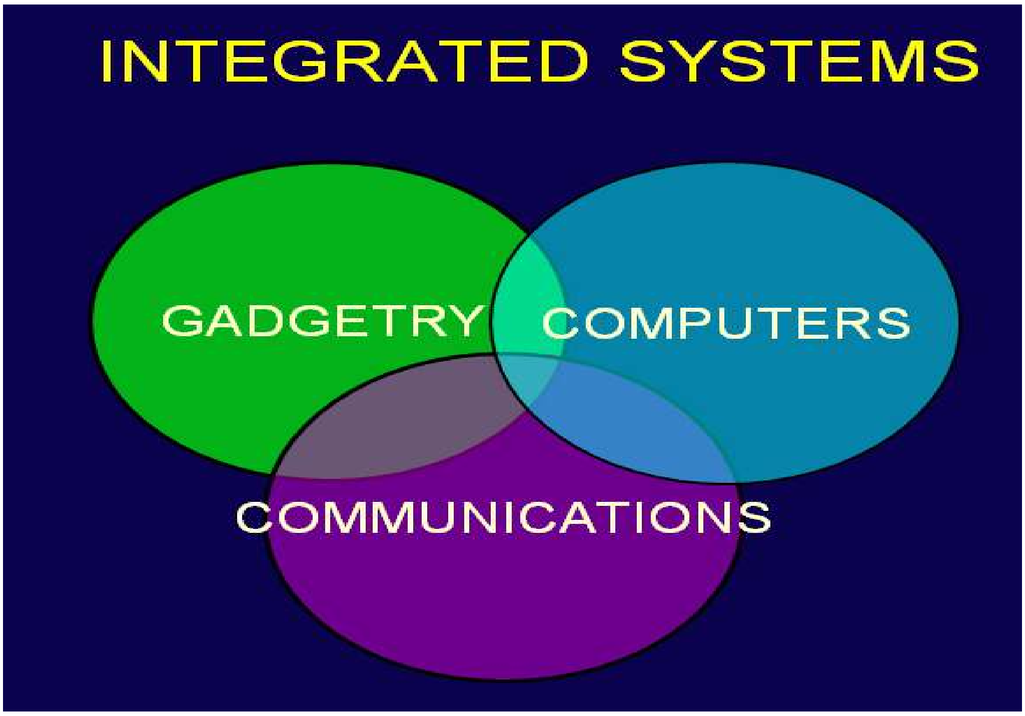
Magnetic Lock

CC Camera

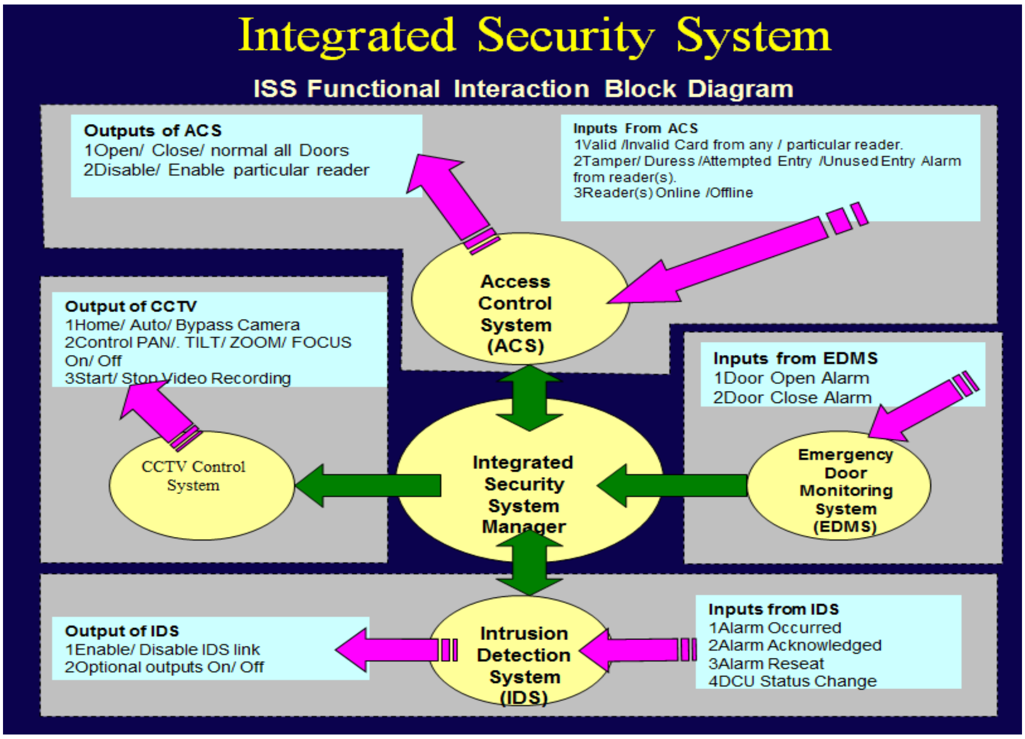
Speaker/Mic

Access Reader

Access Control using CCTV, Voice analyzer and Card Reader



INTEGRATED SYSTEMS



Integrated Security System

ISS Functional Interaction Block Diagram

Outputs of ACS
1Open/ Close/ normal all Doors
2Disable/ Enable particular reader

Inputs From ACS
1Valid /Invalid Card from any / particular reader.
2Tamper/ Duress /Attempted Entry /Unused Entry Alarm from reader(s).
3Reader(s) Online /Offline

Access Control System (ACS)

Output of CCTV
1Home/ Auto/ Bypass Camera
2Control PAN/. TILT/ ZOOM/ FOCUS On/ Off
3Start/ Stop Video Recording

Inputs from EDMS
1Door Open Alarm
2Door Close Alarm

CCTV Control System

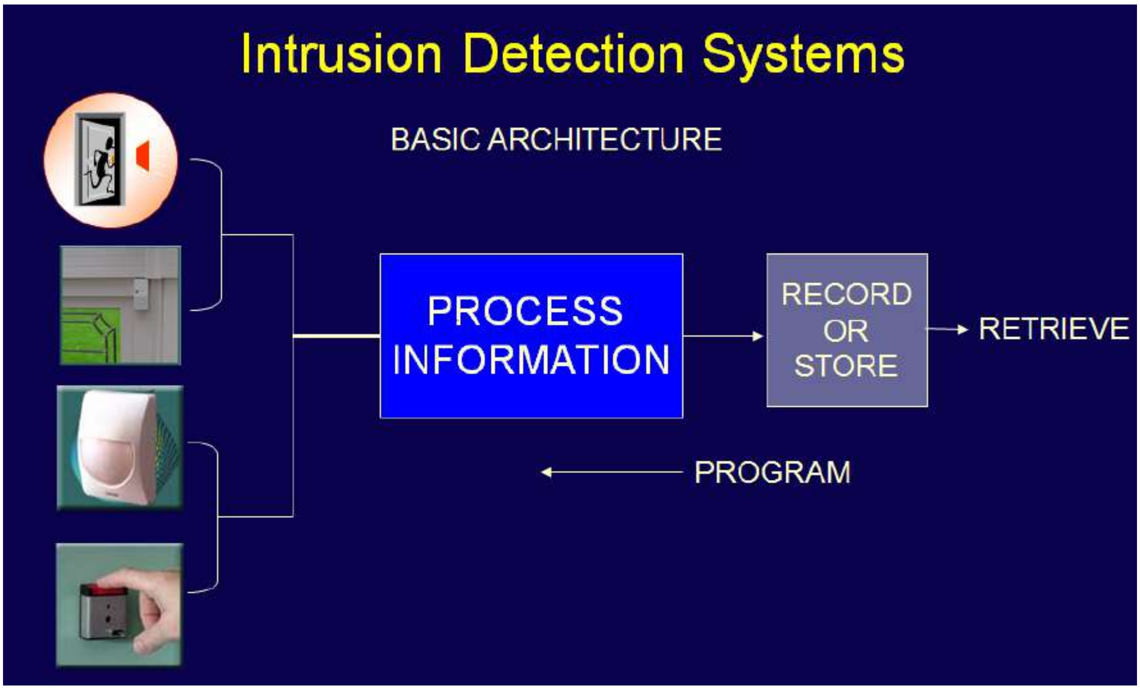
Integrated Security System Manager

Emergency Door Monitoring System (EDMS)

Output of IDS
1Enable/ Disable IDS link
2Optional outputs On/ Off

Intrusion Detection System (IDS)

Inputs from IDS
1Alarm Occurred
2Alarm Acknowledged
3Alarm Reseat
4DCU Status Change



Intrusion Detection Systems

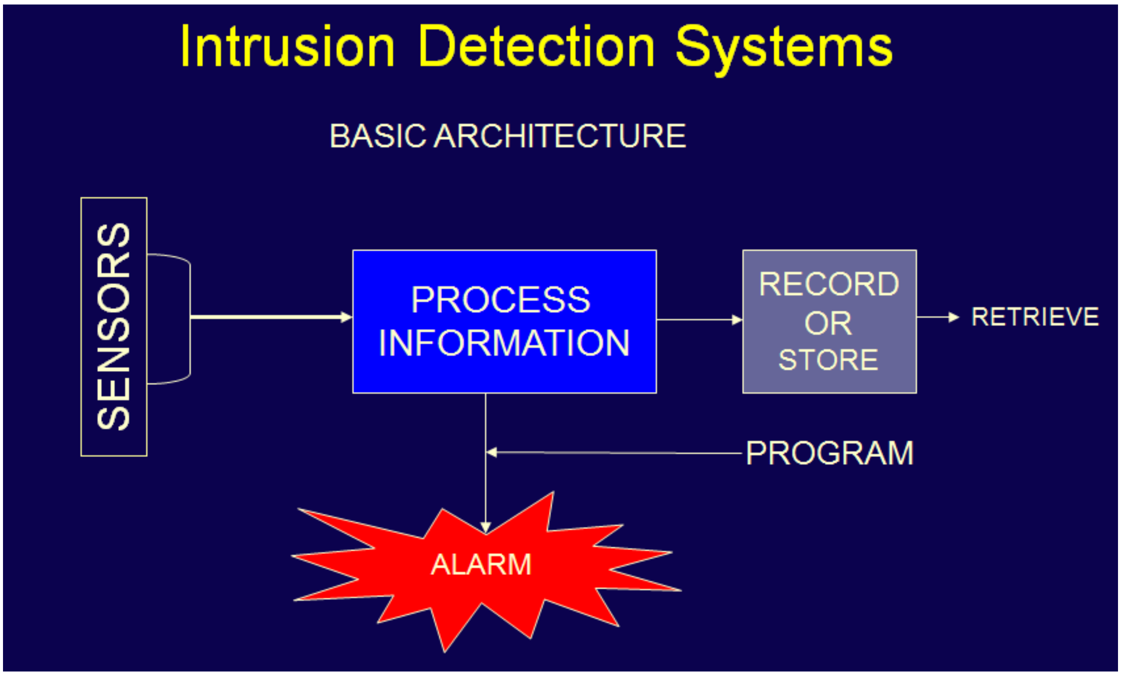
BASIC ARCHITECTURE

PROCESS INFORMATION

RECORD OR STORE

RETRIEVE

PROGRAM



Intrusion Detection Systems

BASIC ARCHITECTURE

SENSORS

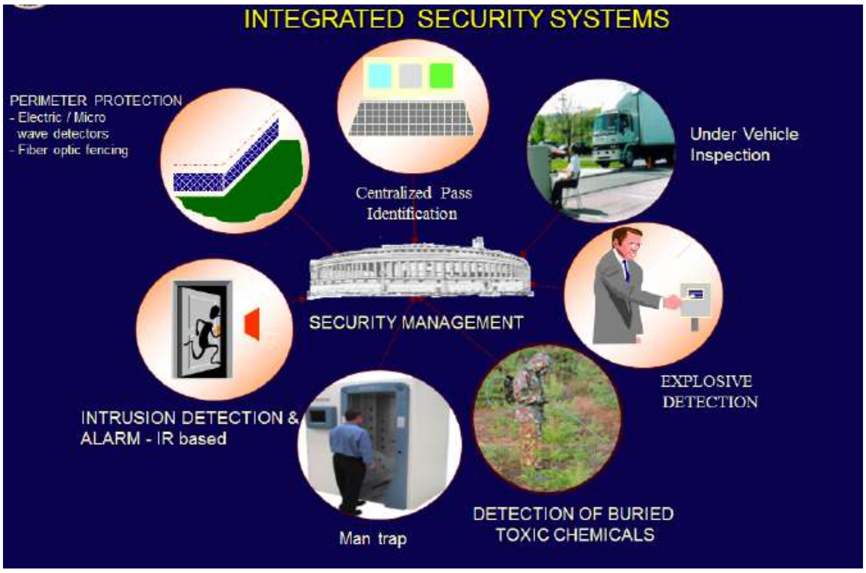
PROCESS INFORMATION

RECORD OR STORE

RETRIEVE

PROGRAM

ALARM



INTEGRATED SECURITY SYSTEMS

PERIMETER PROTECTION
- Electric / Micro wave detectors
- Fiber optic fencing

Centralized Pass Identification

Under Vehicle Inspection

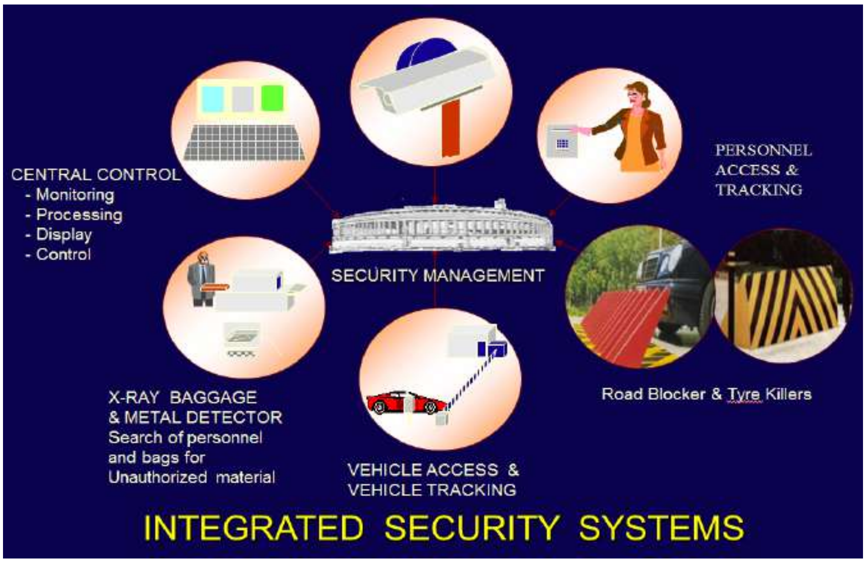
SECURITY MANAGEMENT

INTRUSION DETECTION & ALARM - IR based

EXPLOSIVE DETECTION

Man trap

DETECTION OF BURIED TOXIC CHEMICALS



CENTRAL CONTROL
- Monitoring
- Processing
- Display
- Control

PERSONNEL ACCESS & TRACKING

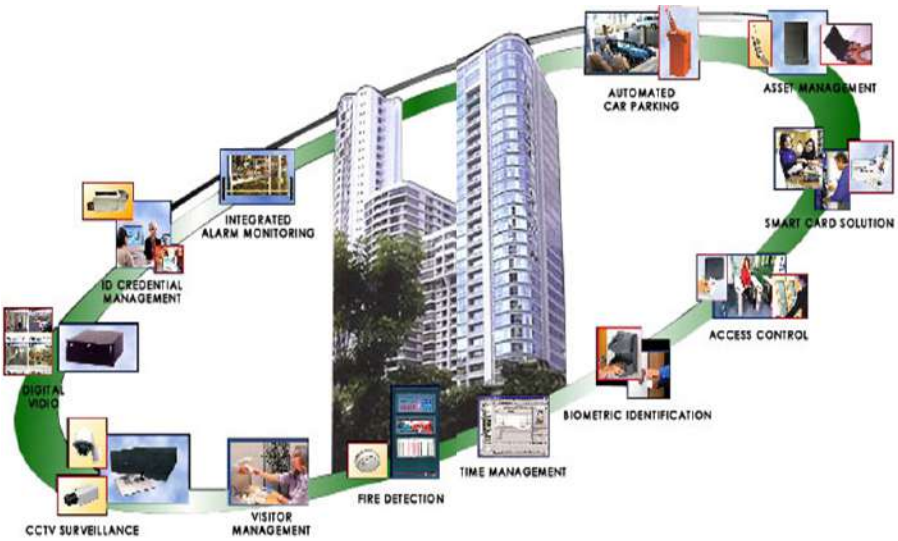
SECURITY MANAGEMENT

Road Blocker & Tyre Killers

X-RAY BAGGAGE & METAL DETECTOR Search of personnel and bags for Unauthorized material

VEHICLE ACCESS & VEHICLE TRACKING

INTEGRATED SECURITY SYSTEMS



Technical Specifications of Road Barriers

Barriers are required to prevent forceful entry through vehicles. The following are the specifications for such equipment.

Crash Rated Electro-hydraulic Bollards

Normal Operation: Bollard(s) shall provide excellent security and positive control of normal traffic in both directions by providing an almost insurmountable obstacle to non-armoured or non-tracked vehicles. The Bollard system shall be designed to stop a vehicle attacking from either direction and continue to operate when the vehicle is within the defined weight and velocity characteristics, minor repairs accepted.

Electro-hydraulic Bollard, consisting of (one, two, three or four) vertical lift retractable Bollards operating (independently or in sets of two, three or four), a Hydraulic Power Unit, the Controls and Logic Circuits and Related Features.

System Configuration

Bollard Construction: Bollard shall be a below ground assembly containing a heavy steel cylindrical weldment capable of being raised to an above ground guard position. The guard position shall present a formidable obstacle to an approaching vehicle.

- Bollard Arrangement: The system shall have a total four numbers of Bollards arranged in multi bollards operating in sets
- Design:
  - Blocking bollards in compact design with drive unit in underground casing attached to base bollard. Available as single, double and triple unit
  - Blocking Element Cylindrical**:** Diameter: 275 mm, blocking height 900 mm above ground level
- Blocking Element Material: S355 – with multi-level zinc based plastic coating.
- Operating Time: (For single system)- Raising: approx. 5 seconds **-** Lowering: approx. 3 seconds
- Impact Load: 1220 kJ (7.5 t at a speed of 65 km/h) Test–certified according to British Standard PAS 68 and DOS SD-STD-02.01 Rev. A
- Power: 1.1 kW, 400 V
- Hydraulic Fluid:
  - Biodegradable hydraulic oil plan to hydraulic 22 S-NWG, water protection class 1 or mineral oil HLP 22
- Control: Control board in separate control box for wall mounting inside a building (optional: in separate control cabinet for outdoor installation), raising in deadman function, control voltage 24 V

- Emergency Operation: The bollards remain in the raised position in case of power failure and can be lowered manually by operating the ball cock on the solenoid valve in the underground casing.

Optional: bollards lower automatically upon power failure
Optional: hand pump for manual raising

- Lighting (Optional): Bollard top lighting red or yellow, i.e. LED lighting on top plate (UFO-shape)
- Weight: Base bollard with drive 400 – 450 kg, each additional bollard approx. 380 kg
- Colour: Standard
- Blocking element: RAL 6005, 7030, 7016 or 9010 drive housing: hot-dip galvanised, cover plate of underground casing and stand pipe: RAL 7016 (optional stainless steel)
- Optional: RAL colours or DB colour tones

Boom Barriers

- Blocking width: Up to 4000 mm
- Casing dimensions: Width: 350 mm, Height: 1100 mm, Depth: 365 mm
- For blocking width greater than 300 m it is necessary to install an impact post or a pendulum support for functional function.
- Drive: 230/400 V three-phase motor
- Gearing: worm gear motor
- Auto-stop: by magnetic switch, contact free, freeze proof
- Drive control: microprocessor-control
- Casing: stainless-steel 1.4301, grinding 340, cover rounded, red 3002, optional powder coated
- Barrier pole: aluminum-round-pole, diameter 80 mm powder coated, colour white (RAL 9016) with red strips
- Control: optional with key switch, desk-top console, radio control, code-card reader, induction loop,
- Photo-electric barrier
- Options: pendulum support, impact post, crawl-under protection, safety pressure strips, traffic-light,
- Intercom system, boom breaking point,

Multi Zone Door Frame Metal Detector

Sensitivity

- DFMD should have uniform sensitivity across the aperture. Metal object exceeding threshold mass should produce identical alarm when passed through any portion within frame.
- The DFMD should have multi-zone capability(6 zones) with uniform sensitivity in all Zones
- The system should be capable of detecting ferrous/non ferrous & alloys metals of 30 gms or more when passed through the archway concealed on the body of the person.

Note

It is expected that person before passing through the DFMD will take out all removable metal articles from body of the person and deposit in a bowl and will pass through DFMD. Presence of metal will have to be reconciled to the satisfaction of the security personnel.

Aperture Size

The aperture of the DFMD should be 2 metres high and .75 metres to .85 metres wide.

Speed of Passage

The performance of the DFMD should be independent of the speed of the person passing through. This is particularly important as a person's foot may swing through the archway without touching the ground, or may come to rest on the ground between the archway pillars.

Interference Rejection

Interference, which is `**mains-borne**' or radiated by an external source, should not cause the DFMD to raise the alarm spuriously. It should be possible to use equipment such s radio, portable telephone, walkie-talkie sets X-ray monitors etc. at a distance of one metre from the archway without causing spurious alarms.

Moving metal beyond one metre from DFMD should not affect performance of the DFMD. It should be possible to move metallic items like trolleys one metre away from the DFMD without the generation of false alarm.

Alarm Indication

- There should be both visual and audible alarms. It should be possible to adjust volume of the audible alarm. At its loudest setting the volume should be adequate to overcome ambient noise present at airport search facilities.
- Detection circuit shall be continuously active for detection of metals and alloys. The equipment shall have comprehensive self diagnostic that shall be able to pin point the defects by constantly monitoring the internal circuitry external connections and environment.
- The unit shall be able to work without any manual adjustment for power variations over voltage range from 160 V to 260 AC.
- The unit shall conform to international and national standards for electrical safety.

Stability

The design of the DFMD should be such that its level of performance is constant over long periods of time. The DFMD shall be manufactured by firms having ISO 9000 certification.

Security

- Adjustable controls should be activated only on the insertion of a removable key.
- DFMD resets itself within three sec after an alarm condition.
- The unit should have traffic and alarm counter. The system should also be functional bi-directional.

Health and Safety

- DFMD shall be Cardiac pacemaker, Magnetic tape & Film safe, Supplier shall submit certification to this effect with supporting documents.
- Operation of DFMD shall not be affected by infrared, ultraviolet, electromagnetic or RF radiation. Offered equipment shall comply with CE or equivalent safety / immunity standard.

Static Metal Compensation

It may be necessary to install DFMD close to fixed sheets or pieces of metal, which form part of the building or its fittings. The DFMD should compensate for the presence of such metal and its performance should not be degraded by the presence of metal as stated above.

Operating Temperature

DFMD shall work satisfactorily without any deterioration in performance within the temperature range of 0 to +45 C with RH up to 95 % non-condensing.

Calibration

DFMD shall have in built feature of auto calibration.

Hand Held Metal Detector

- Dimensions
    - Length 200 to 400 mm
    - Probe width 50 to 100 mm
    - Body width Maximum 40 mm
- Weight: Not more than 500 gms
- Power Source Alkaline battery 3/6/9 volt, should run minimum 200 hrs or more
- Battery protection To be provided against damage due to reverse polarity
- Indication (a) Single LED based audio and visual multiple indication for:-
    - Switch on
    - Metal detection
    - Low battery indication
    - Operation Single push button operation.
    - Construction should be rugged and impact resistant ABS moulded casing.
- Scan rate Minimum 3” to 24”/sec.
- Detection should be able to detect Ferrous and Non Ferrous metals.
- Pistol .22 at min 6 “
- Cartridge .22 at min 2”
- Razor Blade at min 1”
- Tuning Automatic to ensure equal results on wide range of metal sand alloys.

Hand Held Search Light

Hand held search light Basic Model in one-piece moulded casing with integral Handle.

Technical Particulars for Hand held Search Light Basic Model

Construction
The light shall have integral handle and the front cover shall be screwed on the Body for easy replacement of lamp. The battery can be replaced by unscrewing the Rear cover without disturbing the electronic circuits. Fuses shall also be Accessible for easy replacement. All casings shall be water resistant in super tough glass filled nylon or ABS or Polycarbonate in olive green or gray or black color with minimum thickness of 2mm.

Light Beam
The lamp shall be halogen type and lamp mounting shall be adjusted to give parallel beam. Parabolic reflector shall be mounted on shock resistance cap and shall be housed securely in the casing. The front glass should be heat and shock resistance it shall not crack when water droplets fall on it while searchlight is on. The light shall give minimum illumination of 6000 Lux for 55W lights and 9000 Lux for

100W lights at an axial distance of 5m from the front glass. The searchlight should be able to detect a group of persons at a distance of 350 meter.

Physical Dimensions
Beam Diameter: 13cm +/-5%
Total weight: 4.0 Kg (max.) for item 1, 6.5 Kg (max) for item 2.

Operation
The light can be switched on either by a membrane switch, a push button type micro switch or a toggle switch. The switch shall be located near the handle for easy access in dark.

Controls
Following controls shall be provided:

- Membrane type/push button type/toggle switch for system ON/OFF.
- LEDs for Battery charging/Low Battery/DC fuse blown.

Batteries and Current Consumption
Rechargeable sealed maintenance free batteries of specified capacity (12V7AH or 12V 12AH) shall be suitable for being housed in the casing. Bidders shall furnish complete details of the battery including name of the make, model and capacity etc. along with the offer.

In-built Battery Charger
It shall be suitable for charging 12V 7AH or 12V 12AH sealed maintenance free battery as applicable with following parameters and supplied with power cord 3 meter long fitted with suitable connector:

- Input voltage: 100V to 270V, 50 Hz single phase AC.
- Charging current: 0.1 C with maximum current of 1.5A for 12V7AH battery, 2.6A for 12V 12AH battery.
- Protection for Battery charger- Adequate protection shall be provided against short circuit, battery over charge, battery deep discharge and reverse polarity.

Shoulder Strap

Shoulder strap shall be 150cm long 3cm wide made of nylon duly fitted with suitable rings and brackets. The bracket may be integral or fixed firmly to the body/handle. Shoulder strap shall also have a strap for shoulder support 20cm long 5cm wide and 3mm thick.

Operating conditions

Equipment should be able to operate satisfactorily in a temperature range of at least -10 degree C to 50 degree C and 95% RH at 40 degree C

General Technical requirements

Each rating of HHSL shall be type tested for following environmental tests. At the end of each of these tests, HHSL shall be switched ON for half an hour. After completion of each test, equipment shall function normally.

Cold test

Test Temperature shall be -10 degree C and test duration shall be 16 hour.

Dry Heat test

Test Temperature shall be 50 degree C and test duration shall be 16 hour.

Damp heat test

Test temperature shall be 40 degree C & relative humidity (RH) 95% and test duration shall be two cycles.

X-Ray Baggage inspection system

Specifications

General

Resolution	42 SWG (38 AWG) Guaranteed
Penetration	Steel - 28 mm. Guaranteed 30 mm. Typical
Power	170 - 260 VAC, 50Hz., single phase 3.45 Amp. (Max.)
Carrying Capacity	175 kg. distributed
Conveyor Speed	Approx. 0.2 m/sec

X-Ray Generator

Cooling	Sealed oil bath
Anode Voltage	160 KV rated, 140 KV operating
Tube Current	1 mA rated, 0.7 mA operating
Beam Divergence	60 degree

Computer Configuration

Processor	Pentium IV Processor 2.8 GHZ minimum
Hard Disk	80 GB minimum
Floppy Drive	1.44 MB (3.5 in)
CD-ROM Drive R/W	52X Minimum
DDR RAM	512 MB minimum
Video Memory	16 MB minimum or better

Image Processing

Sensor	Folded Array
Grey Levels	4096 Stored
Display	High resolution SVGA 17" color monitor with minimum 1024 x 768 pixels or better

Environmental Requirements

Storage	-20 Degree Celsius to 60 Degree Celsius
Operating Temp.	0 Degree Celsius to 50 Degree Celsius
Relative Humidity	5 to 95% Non-Condensing

Standard Features

- Crystal Clear™
- EPX
- Multi Energy Imaging with four colour palette for material discrimination
- Organic / Inorganic stripping
- High, Low penetration
- Variable colour stripping with save function
- Variable gamma with save function
- Variable density zoom
- Edge Enhancement
- Variable edge enhancement with save function
- Variable zoom X8
- Inverse Video
- Black & White Image
- Pseudo Colour
- Bi-directional scanning
- Manual Image Archiving
- Image recall
- Density Threat Alert (Audio & Visual)
- Date & Time display
- Baggage Counter
- Search Indicator

- Full diagnostic built-in test facility
- Rodent protected
- Input / Output frames with SS Rollers / Drop Chute
- Lockable console cabinet
- Voltage Stabilizer with Isolation Transformer

Optional Features

- Target Software
- Threat Image Projection (TIP)
- Operator Training Program
- TIP Network
- Remote Image Testing (RIT)
- Automatic Image Archiving-Standard
- Manual Image Archiving-Standard
- Operational Hour Counter

Health & Safety

- Approved by A.E.R.B.
- Maximum leakage radiation less than 0.1 mR/hr. (1 μ SV/hr) at a distance of 5 cm. from external housing
- Complies with all applicable international Health & Radiation Safety regulations including USA FDA for cabinet X-Ray Systems
- Film safety for ISO 1600/33 DIN, guaranteed up to 10 times exposure to radiation

Under Vehicle Scanning System (UVSS)

Supply & installation of Under Vehicle Scanning System, to enable inspection of any vehicle's underside through a composite image of the vehicle, as per the details given below:

- The UVSS offered must preferably be of Indian origin, with respect to its design & development.
- The bidder to be either the original equipment manufacturer (OEM) or its authorized business dealer only, and should be an ISO-9001 certified company. The quoted UVSS type and make should have at least twenty (20) or more such installations anywhere within India. A list of such references may be furnished.
- The UVSS should be able to capture very high resolution & complete composite under body image of any vehicle passing over it, without the vehicle being required to be fully stopped, by using a high quality colour Line-Scan CCD camera, with resolution not less than 4,000 pixels.
- The UVSS should be able to handle vehicles moving at different speeds ranging from 5–30 Km/hr, while the composite image so captured by the system should be automatically and dynamically adjusted according to the speed of the vehicle using multiple loop based sensors.
- The system should have a feature of dynamically and automatically adjusting the brightness and contrast of the system to ensure good quality images, irrespective of the different external lighting conditions.
- The UVSS should also provide a feature to capture the image of the driver of all RHS driven vehicles, captured through a suitable driver view camera.
- The system should have an Automated Number Plate Reading System (ANPRS) tuned to the Indian license plates, i.e. it should be able to automatically read and record a wide range of vehicle registration number plates' alpha-numeric characters, written in English. Also, the frontal image view of the vehicle to be provided in the GUI, to facilitate manual viewing of the license plate image.
- The system should have capability to automatically detect foreign objects or additional attachments on the underside by comparison with a reference image stored on the basis of the license plate. The system should detect all objects of size 6" x 6" inches and larger.
- There should be 3 or more additional view cameras for capturing motion video images of the deeper *hard-to-view* areas of the underside, e.g. areas around suspensions, below the engine areas, side wall of fuel tanks & exhaust pipes etc.
- The UVSS should give a real-time output of all the data simultaneously i.e. the composite image, additional videos of hard-viewing cameras, driver photos, vehicle's frontal image and its number display – all should be displayed on the monitor almost instantaneously. Also, the system should have a facility to view the composite image and video images, off-line also, for all vehicles.
- The UVSS should be capable of displaying a pre-stored image of the underside of the vehicle, for visual comparison purpose – identified either by its License plate number

automatically read by the system or by choosing the class/type of the vehicle by the operator. Also, the UVSS should be capable of adding standard templates/images of different makes/models of vehicles, for ease of such visual comparison.

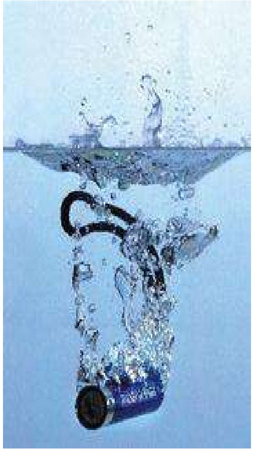
- The system applications & operating software should preferably be based on open architecture / Linux platform. It should also have a user friendly Graphical User Interface (GUI) with provision for multiple users logging of events and search facility.
- The UVSS must essentially have a feature to magnify the composite images (current and past), so as to facilitate a closer and zoom-up view of it.
- The UVSS system must have a facility to take back-up of all the transactions to any usual backup / storage media and also should be able to print out reports.
- The UVSS components should be enclosed in a suitable all-weather-proof housing of IP67 equivalent or higher standard. A certificate of such standards being tested by a competent government certifying agency shall be submitted. The complete civil installation structure should be suitably designed to withstand a total vehicle load up to 40-Tons, so as not to cause any accidental or physical damage to the unit.
- The UVSS should have open protocol for integration with other security systems and also networking for any remote monitoring requirements. The UVSS should have an option of a local language graphical interface (GUI) in addition to English

Guard Monitoring System

The TRACKER Guard Patrol Clocking system is new and unique. It enables your security guards to be alert and register their visits to each checkpoint much more quickly and easily than ever before. What's more, the TRACKER provides you with fool-proof records of guarding performance, showing clearly if any checkpoint has been missed out. Now with TRACKER there's no need to worry that your guards aren't doing the job you pay them to do. The paper print-out tells you everything in exact detail. And the TRACKER has proved immensely popular with the guards themselves, because the unit they carry is lightweight (just 49 gms) and easy to use as a small pocket torch. What more? Guards who perform well get noticed

How the tracker system works?

At the start of a shift or before beginning a patrol, the guard uses the tracker to read his or her unique guard 'I Button'. This ensures that all subsequent tour activity is associated with that guard. The guard is now ready to start his patrol and visit each of the location/buttons in the route, touching the tracker to each button to confirm the visit. The tracker (data acquisition reader) is the core of our security Guard Patrol Clocking System. It has a unique serial number and is carried by the patrolling security guard. This records data contained in tamper and weather resistant touch memory buttons called I Buttons. Each button contains a microchip and a unique ID number. This number is pre-programmed and is virtually impossible to alter. It is maintenance-free and not affected by dirt, grease or weather. It requires no power to work.



iButtons can represent locations, incidents or guards — as determined by the guard patrol clocking software. When a guard reaches a checkpoint he simply touches the tracker to the I Button. The iButtons are physically mounted at these checkpoints — on walls, floors, in closets, inside or outside of a facility, or adjacent to fire extinguishers to facilitate periodic extinguisher checks. When contact is made with these I Buttons the tracker beeps and flashes its LED, automatically recording the exact time, date and location of the guard. The tracker itself is the most rugged employee-monitoring device in the world! It is equipped with unique anti-vandal Technology, a self-protective system that can even recognize and record who tried to damage it and how! The tracker has an internal lithium-ion battery that requires no recharging and lasts upto 10 years! The acquired time stamped data resides in the internal non-volatile memory of the tracker, till downloaded. It's almost impossible to circumvent or defeat the system.

Data Processing

The data from the tracker may be downloaded to a PC for processing of the reports via the specially supplied software. The data can be downloaded in two different ways: Directly – by placing the tracker into the TMD USB download adapter or indirectly – all data from the tracker is downloaded to a data chip held by a supervisor. The data is then transferred from the data chip through the USB adapter to the PC. The evaluation software represents a useful tool for analysing the collected data and generating different kinds of reports.

Getting the information to you

The information contained in the tracker is downloaded to the application software to generate reports and data analysis. The guard tour administration becomes a whole lot simpler and authentic with the tracker system. There are more than twenty reports offered to the user, ranging from simple tour information to individual employee reports: report for a sensor/group of sensors; report for an employee/group of employees; report for a checkpoint; report for a tour and many others. The users can also define and modify the preset reports according to individual needs. The reports can be printed or exported to other software programmes in HTML or CSV format. Now your guards will always stay alert!

Computerized Visitor Management System

Security has become a paramount concern for any organization in the modern world. Physical security of the assets and the intellectual property protection has become a major challenge of any security department of an organization. Proper vigilance over the visitors is the first step towards achieving effective security to the organization.

Limitations of a Manual System

Normally the manual systems followed by most of the organization are inefficient because of certain basic lapses in the security system. Some of problems with the manual system are as follows:

- Since the badge given to the visitor does not have any photo identification, it is very difficult to identify the person.
- Stealing and reusing a badge is possible because the badges are not changed for a considerable period.
- The time taken by a visitor for a specific visit is very cumbersome to calculate and hence very difficult to generate the alerts based on the same.
- Any lapse in the system would be available as compared to a computerized system. In fact an alert can be generated far latter than lapse occurs.
- Generating any archival data is very difficult and time consuming.
- It is very easy for a security guard to by-pass the manual system (e.g. He can sign a register for one month in one day)

Advantages

- In this system, all these problems are handled using the latest technological developments in the field of Information Technology.
- Basically this system takes advantage of Data Warehousing and Data mining facilities. It maintains a database of all Employees, Contractors, Consultants, and Vendors etc. It offers many workflow control utilities using which one can get control over visitors' movement within the organization.
- It also offers many access points and restricting the movement of the visitor within the premise.
- It makes use of Bar Code Technology, which automatically avoids errors in typing etc. and also reduces the speed of access drastically. The Bar Code system is absolutely tamperproof to an extend that unique barcodes can be generated for a specific period.

- It helps the organization in controlling managing the security needs of the organization efficiently with modern technology
- Appointment System: Employees within the organization can send a mail to the reception machine specifying the details. The reception machine can accept these mails and interpret the same and then populate the details into the appointment database. Appointments will be accepted only from the email Ids of the existing employees.
- Gate Pass Creation: This allows you to create the gate pass either through prior appointments or without appointments (Workflow settable by the user). This option will fetch the information from the archival data and give a chance to take the photograph of that person. This system offers you the option of storing the archival photographs and does not require taking a new photograph every time you create the gate pass.
- Check out Terminal: Check out terminal is placed at the exit gate of an organization. It is used for recording the exit time of a visitor. In case the gate pass of a person is not checked out an alert is generated and the security department is informed about presence of a visitor within the organization after office hours.
- Restrict Visitor: There can be many visitors which the security department may not like to visit the organization e.g. certain vendors or certain individuals during the industrial unrest.

Salient Features

- Facility to create appointment for Visitors. In case the visitor is not approved by the security then an alert is generated at the control console.
- Appointment can be created only for a set period of time
- Security has a right to approve or reject an appointment
- Gate pass can be made only before stipulated time of the appointment.
- Visitor Gate Pass with Photo ID
- No need to take photograph every time the user visits , the photograph is stored in the database for further usage
- Facility to give an expected time to travel from security gate to a location in the organization and the same is printed on the card
- Facility to directions to travel to the department including a map is possible
- You can create gate for multiple users in the same pass
- It has comprehensive features for data ware housing and data mining. The data collected during the operation of the system can be analyzed on various parameters.
- Powerful Data Snuffer Algorithms to control suspicious patterns
- Report mails would be sent directly via email
- Management software integrated, single machine based and in built barcode reader
- Good resolution Web-camera
- Visitor card scanner

Material Management System

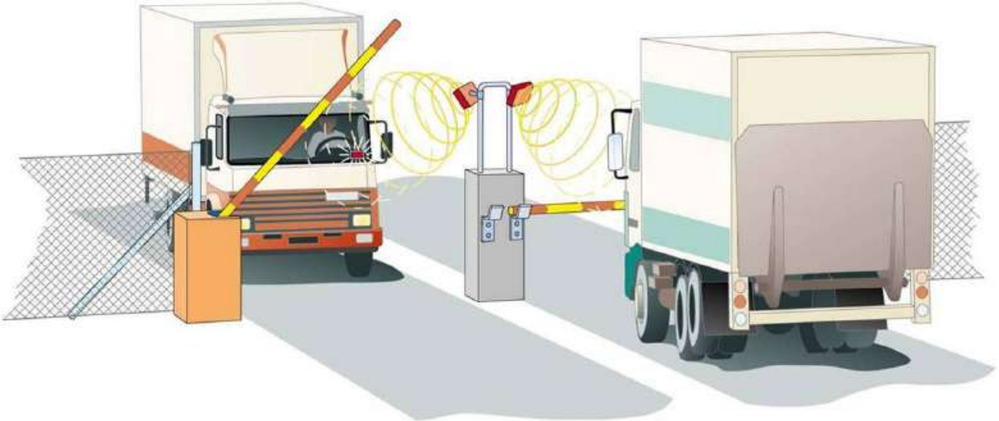
Material management, movement and control is a major function in industrial and business establishments. It has been traditionally handled by books, registers; gate passes etc. and is a cumbersome process as it goes through various levels of permissions, checks and verifications over time and space fronts. Issues like Inventory control, tracking, retrieval of data, responsibility of process owners, huge stationery and database- all pose challenge. In addition, visitor management, mail/courier movement etc. are also separate tasks.

In order to simplify and integrate all the processes in an user friendly manner, material management software for inward/outward/returnable/non-returnable materials coupled with visitor management and courier/mail movement modules may be used. Customized software suiting to the needs of the complex may be developed to make it effective

RFID

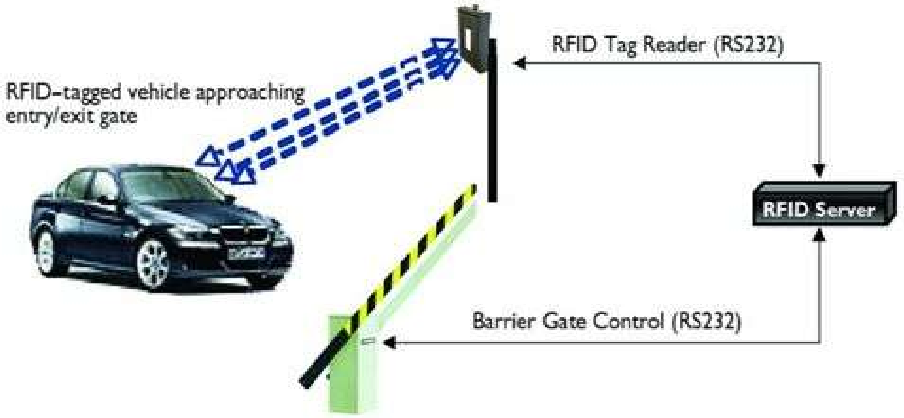
The automatic vehicle tracking facility delivers the flexibility, scalability, and responsiveness that today's organizations need. It provides accurate, up-to-minute information, high- speed communication, and powerful analysis features required to make better decisions faster. The major potential comes from the much acclaimed no line of sight and simultaneous reading properties of RFID. It is now widely recognized that real – time vehicle information will revolutionize the control and logistical organization with significant vehicle fleets. In a global marketplace where productivity is crucial to success, vehicle fleet operators use vehicle management systems as a formidable tool to drive down costs and increase the value of their service.

<u>Technology</u>



Radio Frequency Identification (RFID) devices consist of tags and readers that assist in the tracking of goods and vehicles. Tags are the devices that give identity to the vehicle and work like a wireless name plate. It transmits it identity to readers which are placed at strategic locations like entry/exit of a premise, highway, weighing bridge, parking lots and others.

Readers pick up these signals and transmit them to the centralized data servers from where the information can be viewed or utilized any where these readers can also trigger the other peripheral devices like an access control mechanism- boom barrier to operate as per the business logic. For e.g. on identifying a known vehicle, a reader can signal the boom barrier to open and allow the vehicle automatically. The read-range of the reader varies from 5m to 30 m depending upon the technology (Passive Vs Active) in place. The use of RFID technology also necessitates the purchase and utilization of either fixed or hand held readers which can help the guard to quickly access the vehicle information by bringing the device near the Vehicle.


RFID Tag Reader (RS232)
RFID-tagged vehicle approaching entry/exit gate
RFID Server
Barrier Gate Control (RS232)

Explosive Detectors

It must be understood that explosives and bombs are two different things. And as such their detection requires different methods. Explosive in its raw forms is not a bomb. A bomb, in addition to explosives, requires a power source and detonating mechanism. An explosive detector does not detect a bomb. It detect explosive material only which may or may not be part of the bomb or IED. The scanning equipment, whereas, can detect both the bomb as well as explosives. Scanning equipment, using X-Ray or millimetre waves, throws a beam of ray on target and analysis the reflected beam which can broadly tell about the nature of the material.

The problem is that such identification is primarily based on the density of the target object and presence of carbon, it cannot detect a material with pinpoint accuracy. A normal X-ray scanner will, therefore, classify all objects with high level of organic presence. As explosives and as such is not user friendly. Our experience at Airports has shown that food items, cloths, books etc. all are classified as explosive in an X-BIS.

A scanner, however, also gives an image of the target which is useful in identifying a bomb and not the explosive. Such identification will primarily depend upon the expertise and experience of the screener. It can also be made automated identification by the scanner, if the image matches the pre-stored threat image maintained in the library of scanning equipment. While the normal scanners look at the target object from one direction only the CTX scanners give the multi-dimensional image and are more effective in detecting a bomb.

The explosive detectors identify the explosive materials and not the bomb. Explosive detectors need a microscopic sample from the suspect object which can be in form of either a trace or vapour. In efficient use of an explosive detector collection of sample is of prime importance. It is possible that a hand bag may contain explosives but the detector does not identify it because the sample itself was negative. Since traces are not visible the security personnel must have the experience and expertise in collecting the sample. Similarly it is also possible that a particular bag may give positive signal and yet no explosives are found. It may happen, if explosives were kept in the bag at an earlier occasion and removed later but invisible traces of explosive are still present.

List of Various Scanning Equipment

Various devices are available which can detect unauthorised entry of people or explosives. Depending on the vulnerability and threat perception and type of assets being protected these equipment can be used depending on the industry. It is not necessary for everyone to have this equipment but an idea of the availability of these equipment goes a long way in insulating the organisation from any potential threat

1. Remote Explosive Detector
   Remote explosive detector is the next generation of long range detector and is able to detect substances at long distances safely and without the need to have actual physical contact with the substance. It is easy to operate and delivers fast detection of the substances in a small light weight package. The features include reduced ‘false positive’ readings on contaminated targets.
2. Hand Held Explosive Detector
   Hand held explosive detector is a portable detector. Quick in detection with accurate results. Very high selectivity for explosives and immunity to humidity problems. Hand held explosive detectors or explosive trace detector detects traces of particulates and vapours of explosives, non sensitive in language, mail, cars, trucks, clothing, electronic articles, bag packs, documents and containers.
3. Automatic Explosive Detection System
   Automatic explosive detection system represents the second generation of proven energy dispersive X-ray spectrometry technology. The abilities of the EDS to meet all the requirements existing within the 100% screening environment offers the most sophisticated and comprehensive solution to date.

4. Improvised detonator finder

Improvised detonator finder is designed to detect mines and improvised explosive systems within explosive ordnance disposal and counter terrorists' applications.

5. Liquid Explosive Detection

LED is based on the unique patented Magneto-electrostatic Detection (MED) method, as it forms modulated Magnetic Field (MMF) that allows immediate detection of all types of commercial and military explosives including liquid explosives within a distance between 2-100 m behind and through all types of barriers.

With LED the classification of people, objects, areas and cargo can be achieved on the spot, as the device is immediately ready for use without any warm-up time. LED is maintenance free and designed for continuous use under all climatic conditions. Due to its sort medium and long range detection capabilities, LEDs is the perfect complementary tool for all explosive detection methods, as strategic classification and proactive measures become possible. Even weapons and ammunition will be detected.

6. Bottle Scanning Device

Bottle scanning device can detect dangerous substances in bottles. The model uses light wavelength to read contents while the general dielectric machine uses microwaves.

The operation:

- ✓ A bottle is placed in special compartment or area.
- ✓ A fibre optic probe scan the contents
- ✓ The results appear on a video screen. In some cases, name of the contravent is displayed.

7. Hand held / flammable liquid detector

The hand held device for contact less detection of flammable or explosive liquids inside sealed containers (bottle screening). The devices enables checking of the contents of various vessels such as plastic and glass bottles, cardboard packages and other non metallic containers. It provides detection of flammable and explosive liquids without violation of containers sealing. It can be used by security and law enforcement services at the Airports, Checkpoints, places of mass congestion of people (stadium, discos, etc.). The device allows contact less distinguishing of such substances as gasoline, incendiary mixtures, acetone, nitro glycerine, various spirits, ethers, and other dangerous liquids from water, non alcoholic and alcoholic drinks, dairy products, etc. The latest version of software allows testing more 800 different liquids, the parameters of which are used as a database to compare with the measured values.

8. Suicide Bomber Detection Radar System

The new radar system promises to detect suicide bombers from 100 yards away. The rardar uses a complex algorithm to detect possible explosive materials hidden beneath a person’s clothing. Once a suicide bomber is detected, security personnel will receive advanced warning hand held mobile device much like a Smartphone.

9. Through Wall Radar

   Through wall radar provides quick and covered intelligence on the movement and location of people in a room or building without the need for invasive sensors. It has been designed for situations where a high degree of insight is essential. Through wall radar is compact and portable equipment which uses advanced signal processing to highlight moving people and objects in cluttered environments, through door or brick, block and concrete walls. It is easy to use and with the press of the button, operator can switch between front, plan or profile views for a complete picture. The user can also observe the scenario in a 3D view, where the perspective can be rotate to look at the room or building from various vantage points.

10. Chemical identifier and Mixture Analysis System

    It utilises the new technology to identify volatile or semi volatile organic compounds. Start up and ready to operate in 5 minutes or less and analysis in 3 minutes or less allows for up to 30 samples runs on a single battery charge. Light weight, compact and ruggedized for field operations. Universal, broad based sample collection and injection technique accommodates gas, liquid and solid sampling.

11. Mobile Check

    This remotely operated non intrusive baggage and people screening solution is housed in a standard 20feet container with state of the art system to detect threats, explosives, nuclear material and weapons. It has superior X-ray image quality is utilised for baggage and a small parcel screening. It is an advanced back scatter X-ray whole body imaging system for identification of weapon and contravenes on and under the persons clothing regardless of the material composition of threat.

12. Computed Tomography

    CT scanning provides information not only on gross structure but on material density. In medical applications this enables it to image soft tissues far better than conventional X-ray systems. In some security city systems, the scanners computer can automatically colour code densities characteristics of explosives or other special substances. Built on computed tomography technology platform, the features expanded imaging capabilities and meets the latest, rigorous standards for explosives detection within a lighter, smaller framed system. Suitable for Airport lobbies, baggage makeup areas and full integration with baggage handling systems, the adaptable, streamlined SX delivers operational throughput rates up to 360 bags per hour in line and up to 300 bags per hour in a standalone configuration. The system automatically clears non threat bags for flight at the lowest false alarm rates in the industry, resulting in fewer bags sent to costly secondary search areas.

13. Checked Baggage EDS System

The explosive detection system (EDS), the highest capacity airport security system in the industry, is designed to expertly handle the checked-baggage needs of very large, high traffic airports.

The EDS provides the most comprehensive explosives and threat detection with the highest level of accuracy and lowest false-alarm rates currently available in the industry.

14. X-Ray Inspection System

Automatic detection of explosive in carry-on baggage and analysis if Zeff and density using independent views. Maximum baggage throughput / real time evaluation. The ergonomic operating concept is retained, two high resolution and detailed views (Dual View).

15. Advanced Multiview X-Ray

Advanced Multiview X-ray introduces multiview technology for hand baggage check. With a small footprint and excellent image quality it is the ideal checkpoint solution, its compact design makes checkpoint redesign unnecessary. It displays two orthogonal views for a more accurate and detailed inspection independent of bag placement on the belt, dramatically reducing the need for re-scans. High quality images featuring the greatest penetration and resolution on the market show the object under examination with superior detail.

Detection characteristics :

Resolution: 38 AWG guaranteed, 41 AWG typical in each view/Penetration: 27mm steel guaranteed, 30mm steel typical/Multiview detection system is L-shaped rows of photodiodes.

16. Baggage Inspection System

It provides proven CT-based explosives-detection and dual energy 3D imaging for large baggage – at 1,000 bags per hour. It combines outstanding threat detection capabilities with a low false-alarm rate, at the high throughput needed for large baggage-handling operations. With these features, it is a highly effective security solution for airports and other passenger facilities.

17. Coherent Scattering

The atomic orderliness of a substance affects the way in which X-rays are diffracted (i.e., forced to mutually interfere) when passed through it and by recording the scattering patterns characteristics of specific compounds (e.g. drugs, explosives) and comparing these templates to patterns observed when scanning objects, a substance specific detection system can be devised. This technique is now in the early development stage, and is not ready for deployment.

18. Dual-Energy Transmission X-ray with backscatter

Dual-energy transmission X-ray generates a colorized, high resolution image, easily detecting metallic threats such as guns & knives and fine details including tiny wires which could indicate and IED. Dual-energy also provides organic and metallic discrimination in uncluttered environments.

19. Comprehensive Multi-Technology Baggage Inspection

Multi-technology inspection systems with simultaneous Z backscatter and dual-energy transmission X-rays provide the most information about the object under examination.

Innovative Z backscatter technology highlights organic threats and contraband that other systems miss-explosives, plastic weapons and drugs. Available with a variety of tunnel sizes, to accommodate mail, baggage, or small cargo.

Mail, parcel and baggage inspection systems use complementary technologies, Z backscatter plus dual-energy transmission X-rays, to provide safe, effective and non-intrusive security solutions. Photo-like Z backscatter images, in addition to dual-energy transmission X-rays, reveal organic material and add clarity to expedite inspection. Parcel and baggage inspection systems are designed to quickly detect even the most elusive threats or contraband in parcels of all sizes.

20. Parcel inspection systems

With a tunnel size of 64 cm x 44 cm for checkpoint, mailroom and lobby applications.

With a tunnel size of 78 cm x 58 cm to accommodate large package for checkpoint, mailroom and lobby applications.

With a tunnel size of 105 cm x 102.5 cm for break bulk cargo and large packages for high threat facilities, airports, mailrooms and customs checkpoints and lobby applications.

21. Explosive detection Systems (EDS)

It focuses on detection of chemicals that can be used in explosives. EDS devices are generally based on vapour detection methods. These come in a range of forms, from hand held devices to walk-through devices. Handheld devices used at certain airports are known to require about 20 seconds to inspect the average bag. These devices are useful in inspecting a selected number of bags rather than the complete flow of bags.

22. High Current X-Ray

The system comes standard with latest high-current X-ray source. It is the combination of vertical geometry and high-powered tank deliver the ultimate in penetration, image resolution and quality. It also features patented user friendly touchpad operator interface with heads-up display allowing operators to efficiently and accurately screen items. Transparent colour imaging with Operator Assist detection (OA) capabilities facilities the rapid detection of threats including weapons, narcotics, explosives and other contraband. With multi-language support capability, operators can interact with a system that speaks their native language.

23. Multi Check Scanner

Single point Multi Check Scanner is being configured to present the fullest possible array of threat detection information in any application where checkpoint inspection is required. The five checks at one point it does are Automated Checkpoint X-ray System, Bin Return System, Walk-through Explosive Trace Detection, Whole Body Imager, and Zoned Metal Detection.

24. Body Scanning System (BSS)

The whole body imager screens people for concealed threats without exposure to harmful electromagnetic radiation. The active millimetre wave imaging technology penetrates clothing and packaging to reveal and pinpoint hidden weapons, explosives, drugs and other contrabands. With potential peak throughput levels of over 400 people and hour, Micro Sec. BSS far outpaces alternative screening methods.

25. IRIS Recognition

IRIS recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irises of an individual's eye, whose complex random pattern are unique and can be seen from some distance.

Not to be confused with retina scanning, iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail rich, intricate structures of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow unambiguous positive identification of an individual.

26. Shoe Scanner

Shoe scanner will “enhance the flow” of passengers through checkpoints. Instead of removing shoes, passengers would stand on a machine for a few seconds while a highly sensitive radio-frequency coil looks for explosives but a key challenge is whether machines can withstand the rigors of airports.

27. Scanners of Security Applications

Displays thoroughly explosive, detonator, lighter, printing ink and jewellery concealed in human body. It also effectively detects metal, non-metal (paper money), liquid and powder inside and outside of human body.

Non-stop inspection, high efficiency, people unblocked.

The dosage of single scan is equivalent to natural radiation dosage, without any harm to human body and respect privacy and displays no image of body surface.

Bomb Detection and Isolation Equipment

A set of bomb detection isolation equipment is required to be available with QRT9(Quick Reaction Team) at control room for action before the police teams arrive for disposal. Following equipment is recommended:

- Handheld Explosive detector
- Portable X-ray viewing system
- Deep search metal detector
- Hand held Search light
- Telescopic inspection mirror
- Telescopic prodders
- Search kit with Endoscope
- Handheld metal detector
- Electronic stethoscope
- Non linear junction detector
- RSP Tool kit
- Hook and line set
- Safety circle & Bomb suppression blanket
- Megaphones

Bomb Blanket

- The Bomb Blanket should offer protection against blast and fragments (V50 @ not less than 550 m/s). The firm will have to produce certificate from a national /International accredited lab.
- The Bomb Blanket should be made with multiple layers of treated KEVLAR, Ballistic fabric and should confirm to the protection level required and then sewn into a Fire retardant and Water repellent nylon cover.
- The Bomb Blanket should consist of a nylon web loop near the 4 corners.
- Size of Bomb Blanket should be minimum 1.5 m x 1.5 m.
- Minimum weight of the Bomb Blanket should be 9 kgs.
- Should be able to contain a blast of minimum 100 gms of high explosives.
- Miscellaneous. The firm should be able to provide the following, as applicable, Along with the equipment:
  - Cleaning kit, if any
  - User’s Hand Book and Technical Manual giving full description of the item

- o Literature on preservation technique as applicable

Mail Bomb Detector

It also functions similar to a metal detector with a search coil, but for smaller quantities of metal. It does not require tuning/adjustments and device automatically resets after detection.

Features

- Screening packets of various sizes up to 2.5 in.
- Detects all detonating devices, knives, weapons, and small metal objects in mail
- Visual and audio alarm

Deep Search Metal Detector

It detects both ferrous and non-ferrous metals buried in the ground. Penetration range upto 1 mtr. For large objects (one rupee coin upto 30 cms and 6 inch nail upto 40 cm) meant for underground search for mines.

Features

- Pulse-induction technology
- Audio alarm proportional to the size of the metal
- Detects metal and its alloys
- Double coil
- Telescopic handle for easy manoeuvring along with grip and handset
- Rechargeable battery within built SMPs charger from 90V – 270V
- Coils are waterproof
- Sensitivity is adjustable from 0 to 9
- Bar graph display
- Head phone facility
- Volume control

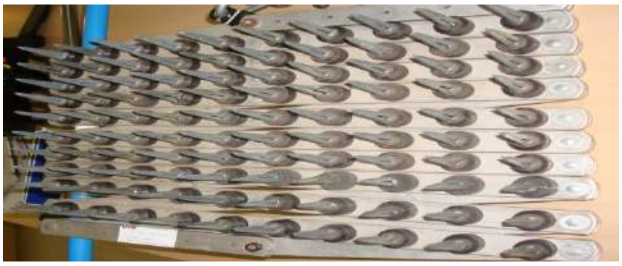
Under Vehicle Search System

It consists of colour Camera with IR. The camera adapts to low light conditions. It's able to change from colour to black and white in low light. Manual swivel and tilt function make it easy for the operator to point the camera in any direction off the end of the pole.

Features

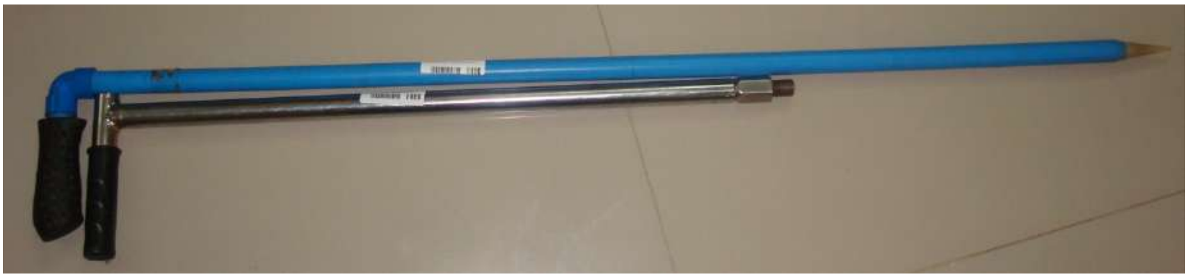
- Camera can be manually moved for 360o with tilt
- High resolution LCD screen with 12 VDC with charger
- The charger is made to with stand fluctuation from 90V to 270V with adequate battery protection.
- Telescopic extension extending up to 180 cm, with non-rotational, lightweight, aluminum pole with rubber grip and arm rest.

Portable Tyre Killer



It is made of alloy steel and can be very effectively used for stopping the vehicle of any insurgent while making an attempt to crash in the high security area. It can withstand load up to 24 tons.

Prodders



- It's made up of heavy steel with nickel coating
- It's one meter length
- It can be folded with thread system
- It has sharp pointed end at one side and shock proof rubber grip at another end
- It is light weight
- It's strong enough to dig all kinds of soil for suspected items
- Hand grip is made of non-conducting material

(Remote Operated) Wire Cutter

- It cut all types of wires from a minimum of 100 metres. distance
- It has minimum 1 metre pole stand to fix the motor with wire cutter
- The wire cutter have shock proof grip
- Adjustable clamp to fix the system at required height
- Standard 12 v battery for motor operation
- Standard connecting wires

Under Vehicle Search Mirror

It consists of a flat platform mounted on castor wheels, a mirror placed on the top, with a light for illuminating the undercarriage. It has a telescopic handle bar fitted on the movement of trolley mirror.

Features

- An excellent tool for security personnel / bomb disposal squad
- An excellent under vehicle / table search operation
- Locate explosives hideouts without physically approaching light weight, distinct vision.

Un-manned Aerial Vehicles/Drones

The last few years have seen a revolution in the use of UAVs for many operations especially offensive actions. UAV is essentially an unmanned vehicle fitted with cameras which can record aerial images, a concept which cannot be visualised with existing technology. Controlled from the ground a UAV is very useful in capturing aerial images. Their counterparts called the Drones have been effectively used in many war situations as bombers/attack mode.

UAVs have immense potential in defensive security. They can be used to aerially patrol area and capture images and transmit them to the ground. They can be used extensively to monitor pipeline transporting gas/oil or can be used for any situation which cannot be accessed by human or with the present technology. UAVs as a defensive piece of security aid have immense potential in any security situation.

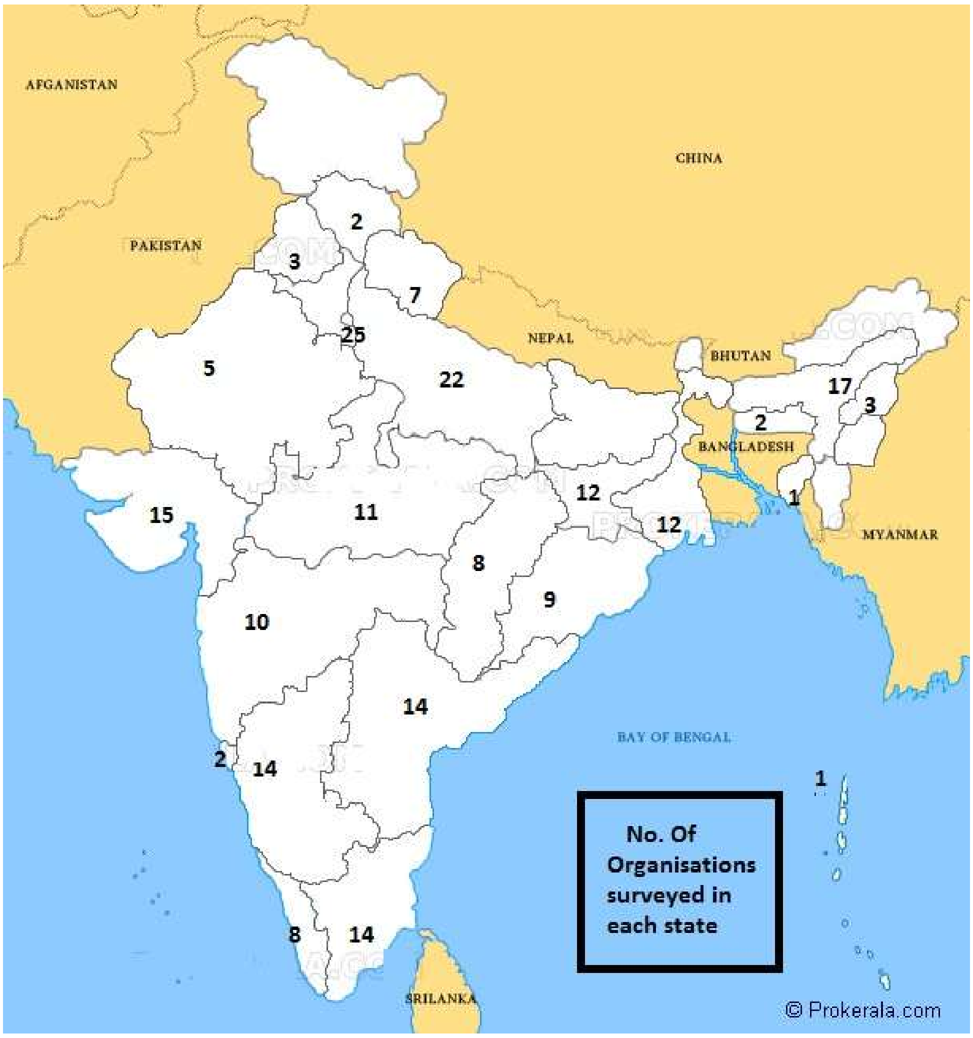
Unfortunately, UAVs also have a grave security risk since they can be used for offensive and illegal operations or attacks on any object or human being. Their remote control and remote operation can pose grave security risk. Hence a serious debate is going on globally on the utility and use of UAVs for security. Since UAVs can be dangerous weapon in the hands of terrorists or anti national elements, their use can be limited. Of course they can be used with some control and regulations but as one has seen in the modern days, there is nothing which a crooked mind cannot circumvent

Data Analysis

7. Data Analysis

No research paper is complete without collection data from field units. In pursuance of this objective and as also enumerated in our original proposal, an attempt was made to collect date from field units across the country by providing a questionnaire. The questionnaire was based on 10 heads each head having at least ten sub heads. This questionnaire was distributed among nearly 250 industrial undertaking across the country of which 208 responded. The data collected provides and insight into the existing physical security management system in major industrial undertakings and gives us an idea as to where the industries are failing/succeeding to protect their assets in some critical areas

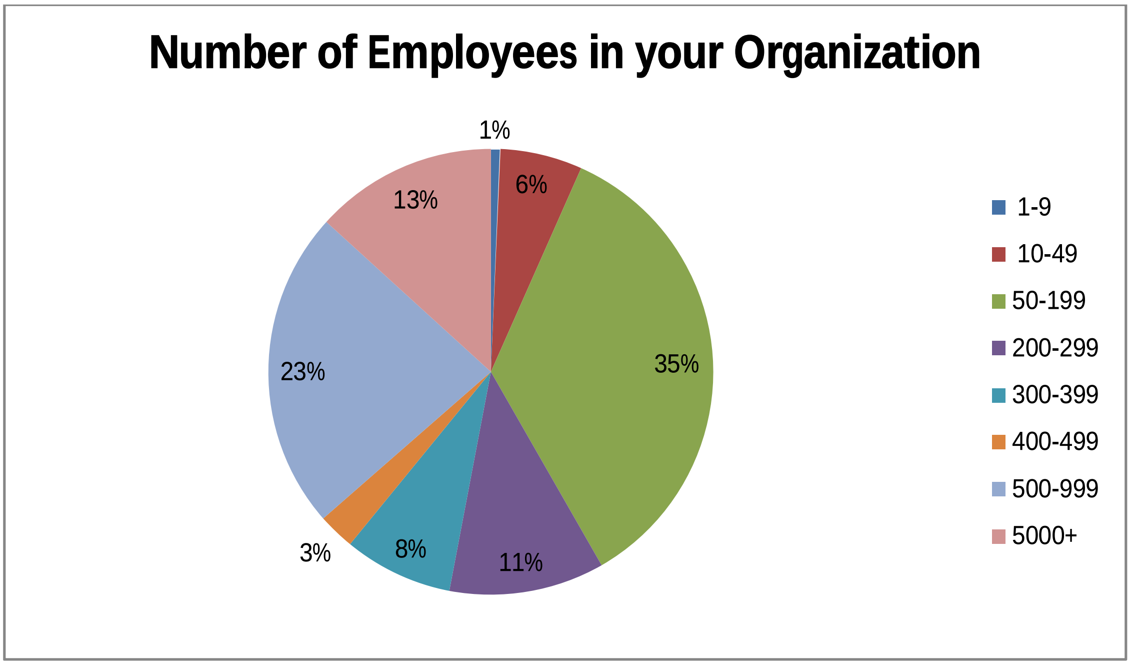
Analysis of Collected Data



It can be seen from the below mentioned data that organisations a large number of employees have been selected more than half the companies selected for had employees ranging from 50 to 999 and nearly 35 % had employees ranging from 500 to 999 and nearly 20 % had employees had employees of 500 or more. The number of the employees is a direct indication of the size of the organisation.

No of employees in the Organization:

Employee Range	Percentage
1-9	1
10-49	9
50-199	53
200-299	17
300-399	12
400-499	4
500-999	35
5000+	20

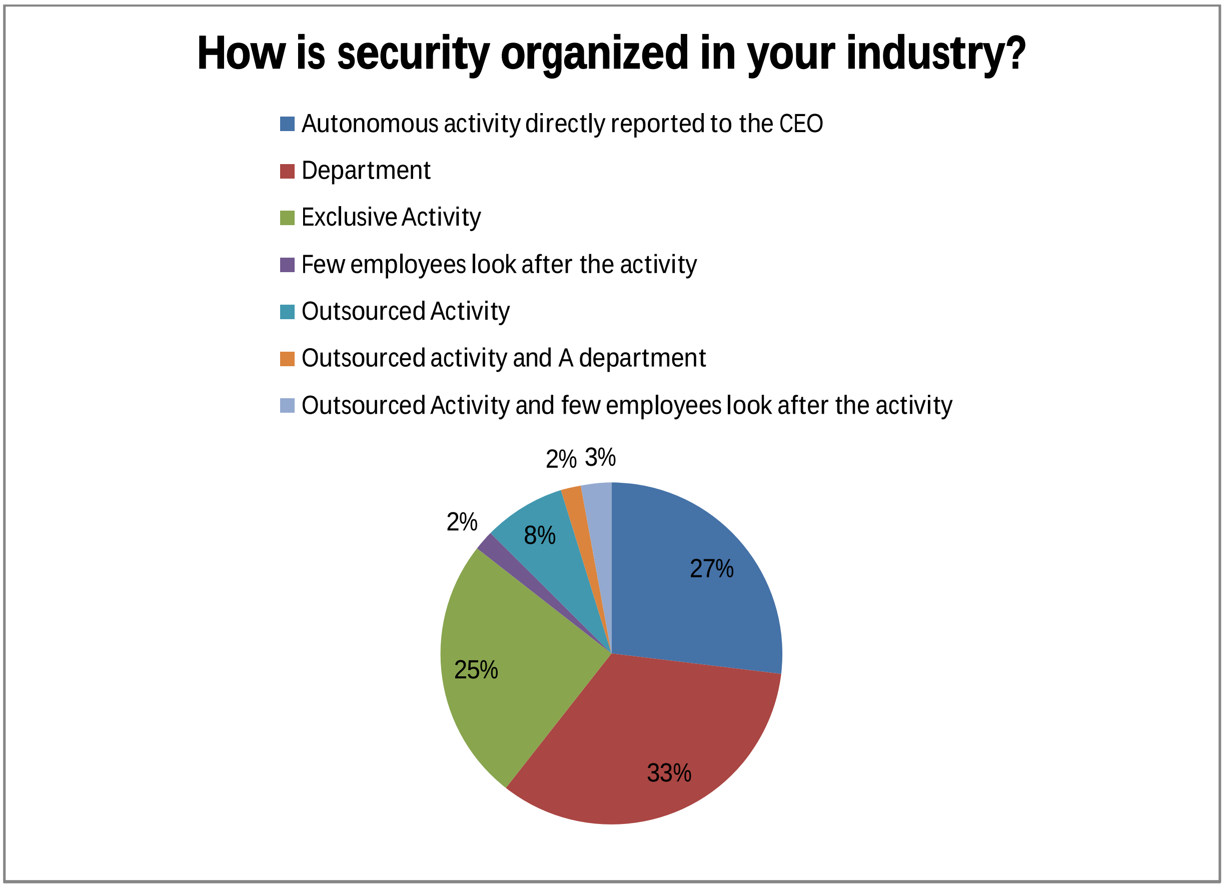


About Security in your Industry

The industries selected for the survey included many public sector undertakings where in security is an independent activity reporting directly to the CEO. However in many private sector organisations security is a part of the HR department. Also except for a handful employees in the security department most of the security activity is in the hands of out sourced security personnel. The purpose behind this is obviously to avoid commitment to the organisation by employing full time staff.

How is security organised in your industry?

Autonomous activity directly reported to the CEO	28
Department	35
Exclusive Activity	26
Few employees look after the activity	2
Outsourced Activity	8
Outsourced activity and A department	2
Outsourced Activity and few employees look after the activity	3



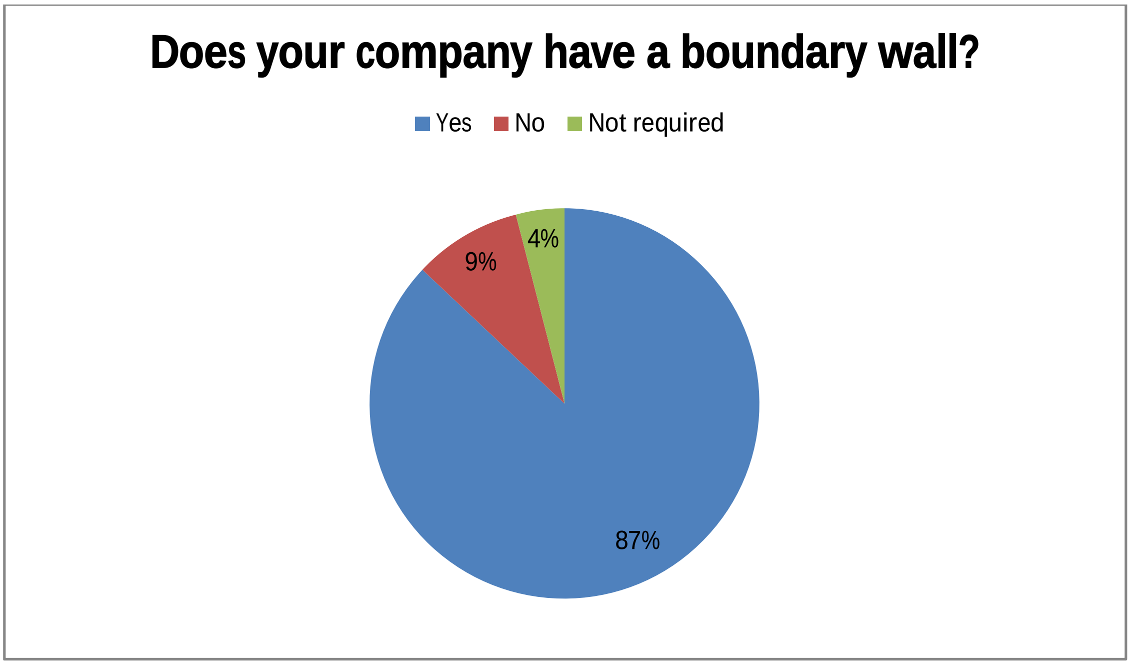
A.Physical Security

Perimeter Wall

Does your company have boundary wall?

Most companies have perimeter walls

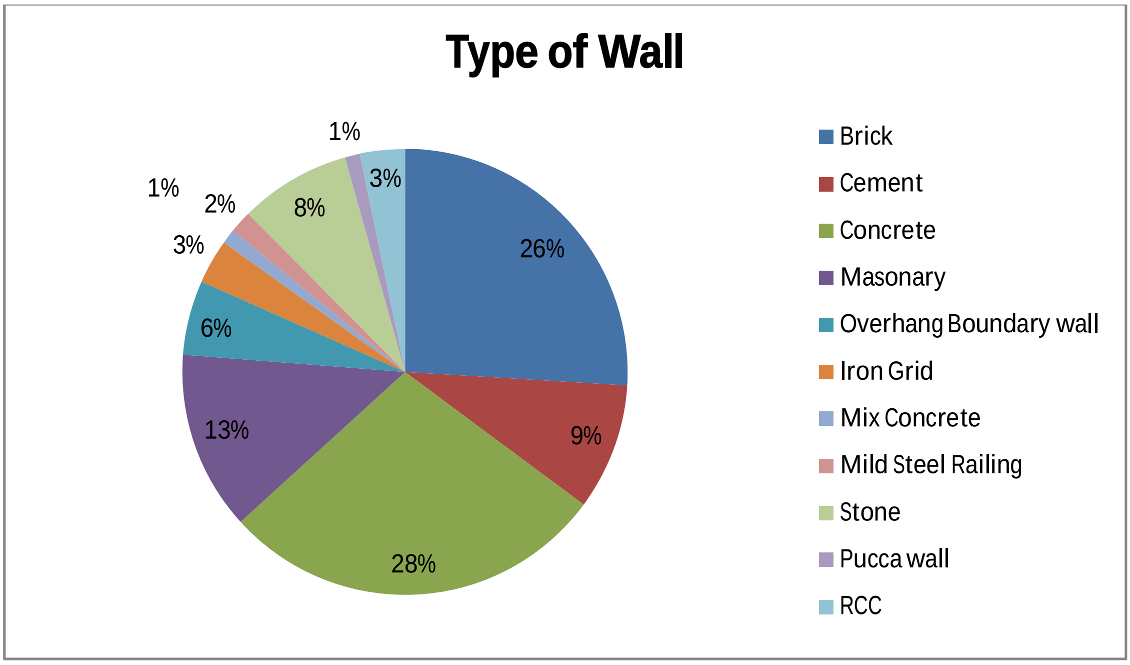
Response	Percentage
Yes	87%
No	9%
Not Required	4%



What type of wall does your company have?

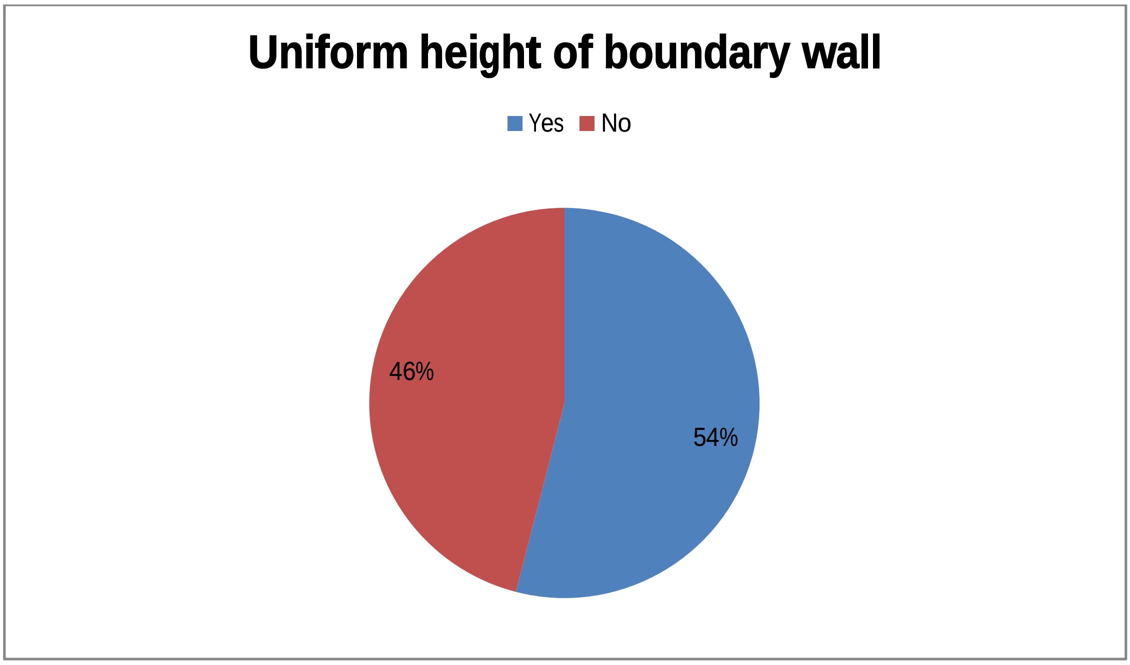
The type of wall is permanent in most companies

Brick	48
Cement	17
Concrete	52
Masonary	24
Overhang Boundary wall	10
Iron Grid	6
Mix Concrete	2
Mild Steel Railing	3
Stone	15
Pucca wall	2
RCC	6



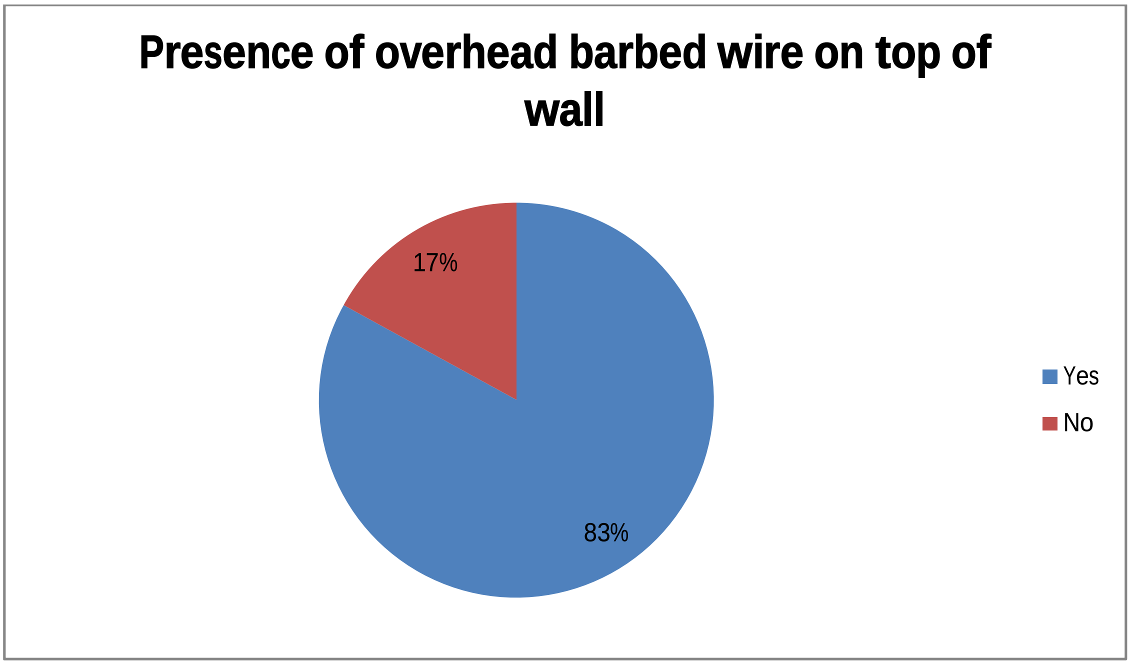
Is the height of boundary wall uniform at every point?

Response	Percentage
Yes	67
No	57



Is there any overhead barbed wire on top of the wall?

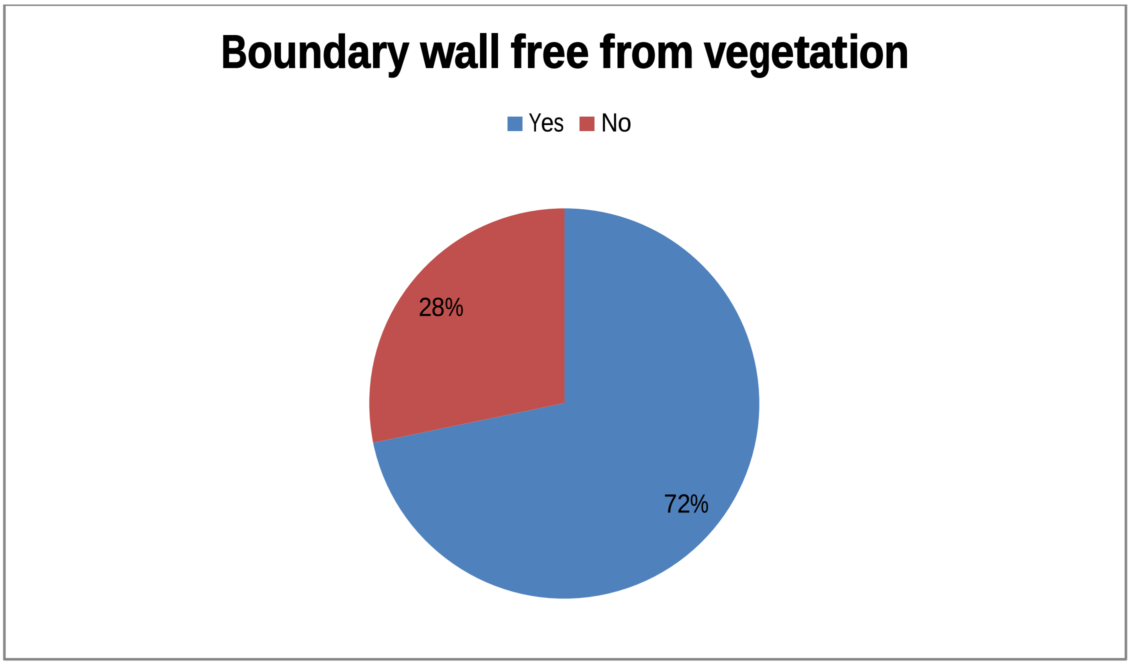
Response	Percentage
Yes	83
No	17



Is the area around your boundary wall free from vegetation?

The finding of this is not very encouraging. Vegetation around the perimeter wall provides access for unauthorised entry.

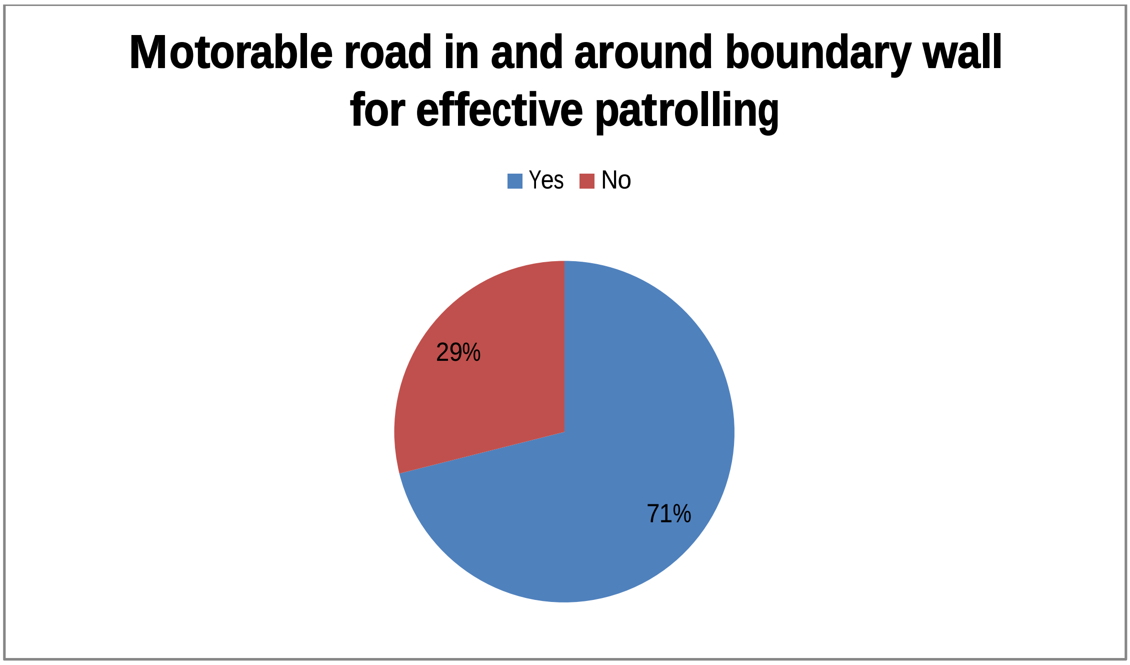
Yes	145
No	57



Is there a motor-able road in and around boundary wall for effective patrolling?

A motorable road around the compound wall provides for effective patrolling.64 of the 221 industries that is nearly 35 % of the industries do not have effective motorable road.

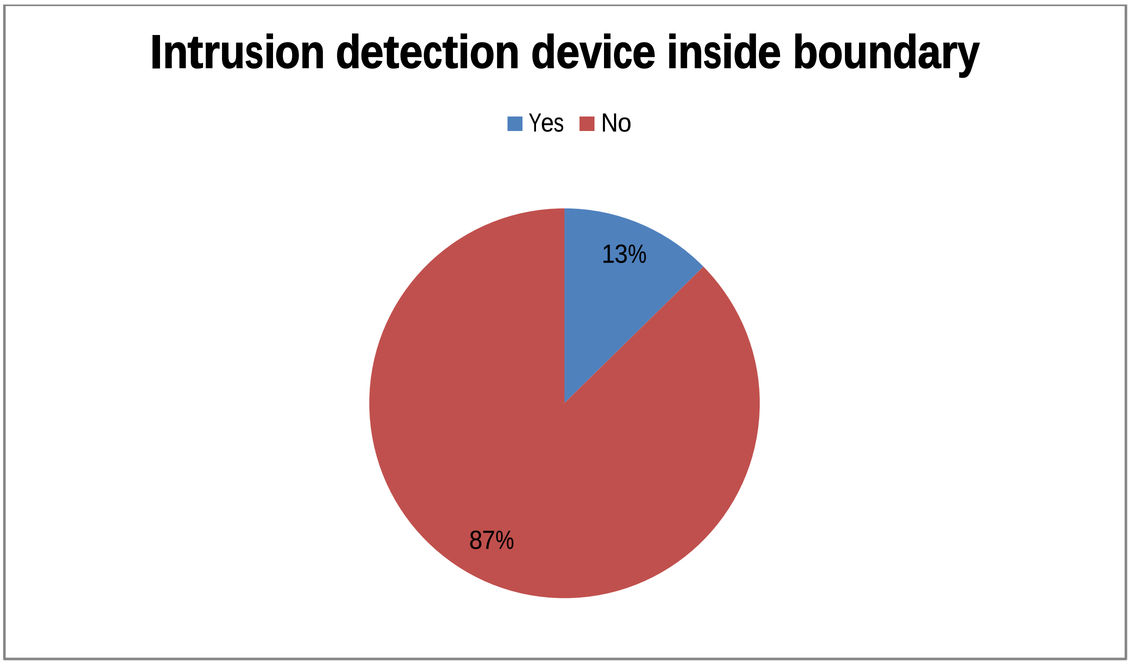
Yes	157
No	64



Is there any intrusion detection device anywhere in the boundary?

Absence of intrusion detection device hampers second line of defence and it is noticed that most of the industries do not have this as they are not aware of its requirement and it also involves cost

Yes	25
No	173

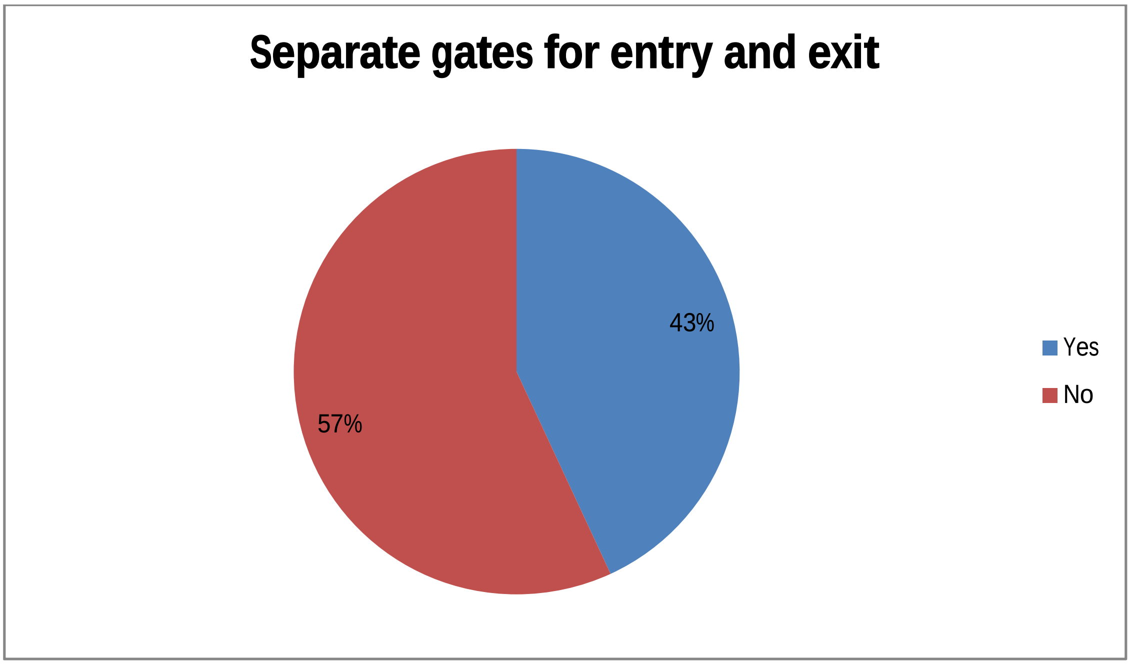


B.Gates

Are there separate gates for entry and exit?

Separate gates for entry and exit provide easy access and enhanced security. Nearly 57% of the industries do not have separate gates for entry and exit

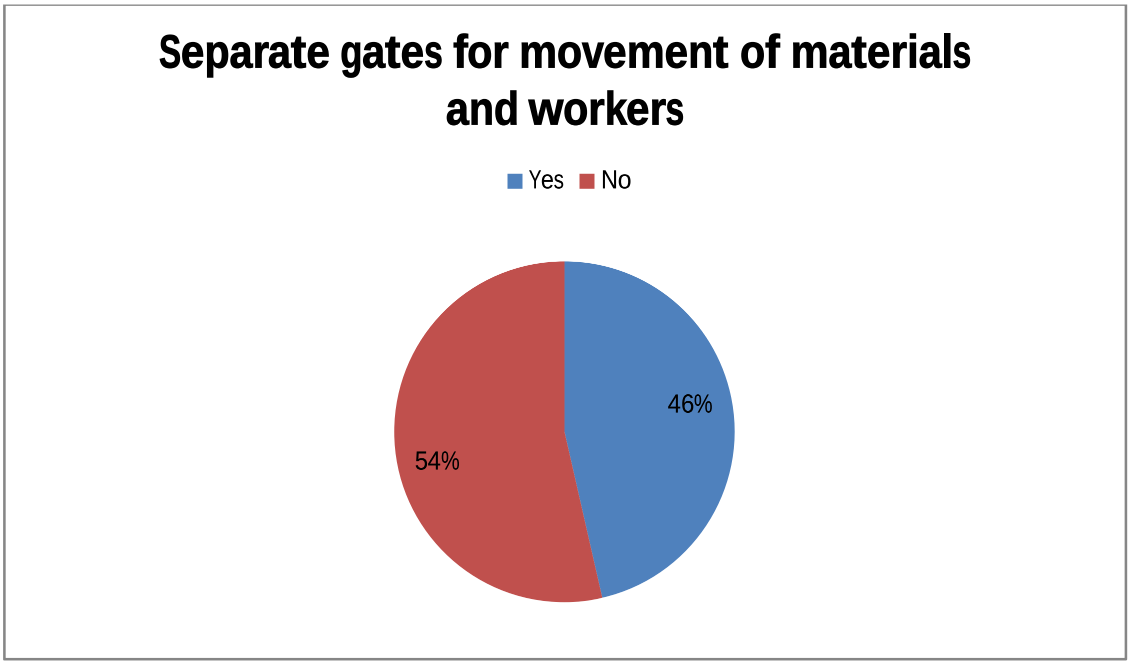
Yes	90
No	119



Are there separate gates for movement of materials and workers?

This also is a sore point from the security perspective. Separate entries provide for easy checking of both workers and material

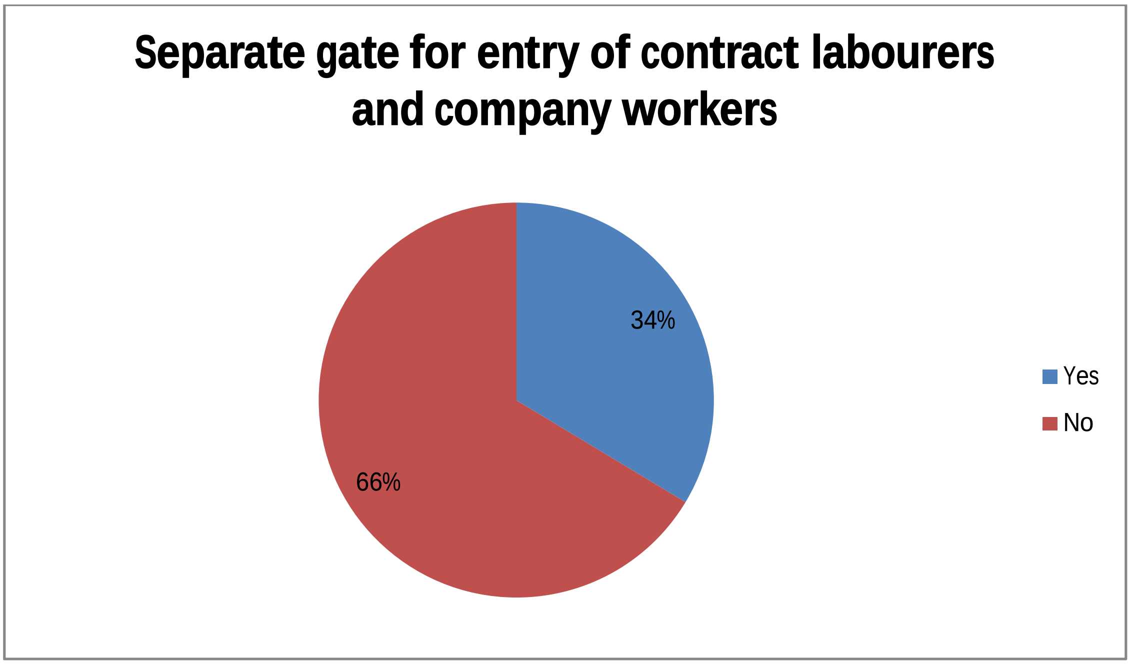
Yes	97
No	112



Is there any separate gate for entry of contract labourers/company workers?

The same applies to employees and casual labourers. Casual labourers are not committed to the organisation and hence need to be checked more as their liability is limited. Nearly 66% of the industries do not have separate entries for contract labourers.

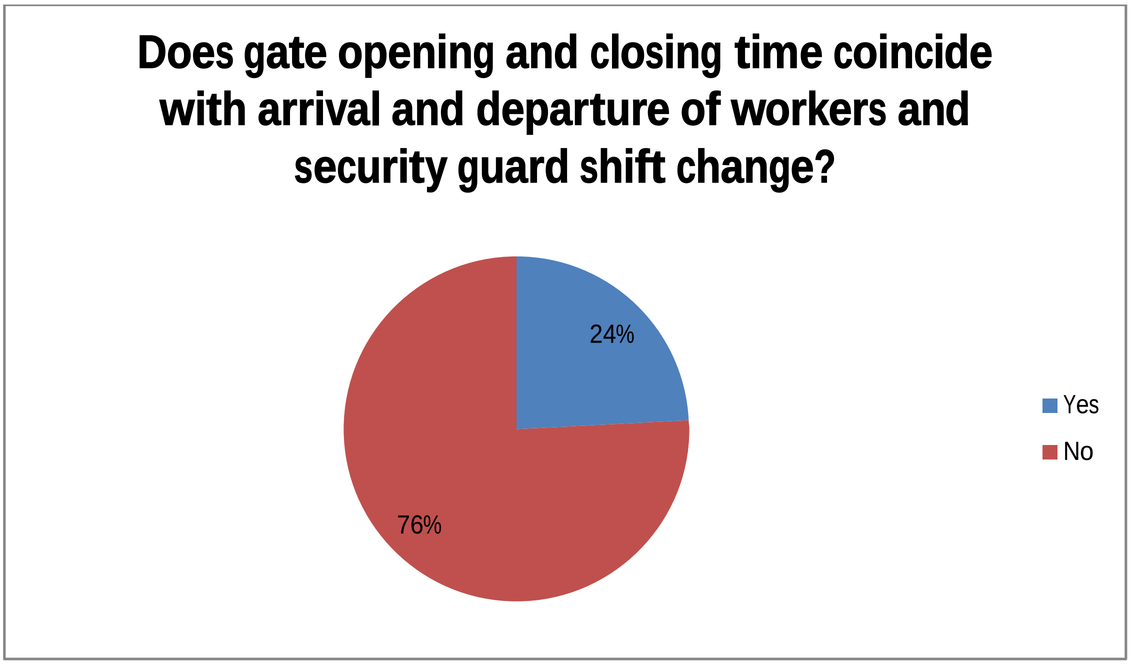
Yes	71
No	140



Does the gate opening and closing time coincide with arrival and departure of worker and security guard shift change?

This is a major lacuna in security. Change of guard should not coincide with the factory timings. The security personnel should not be changed at the same time as the workers come and go after a particular shift

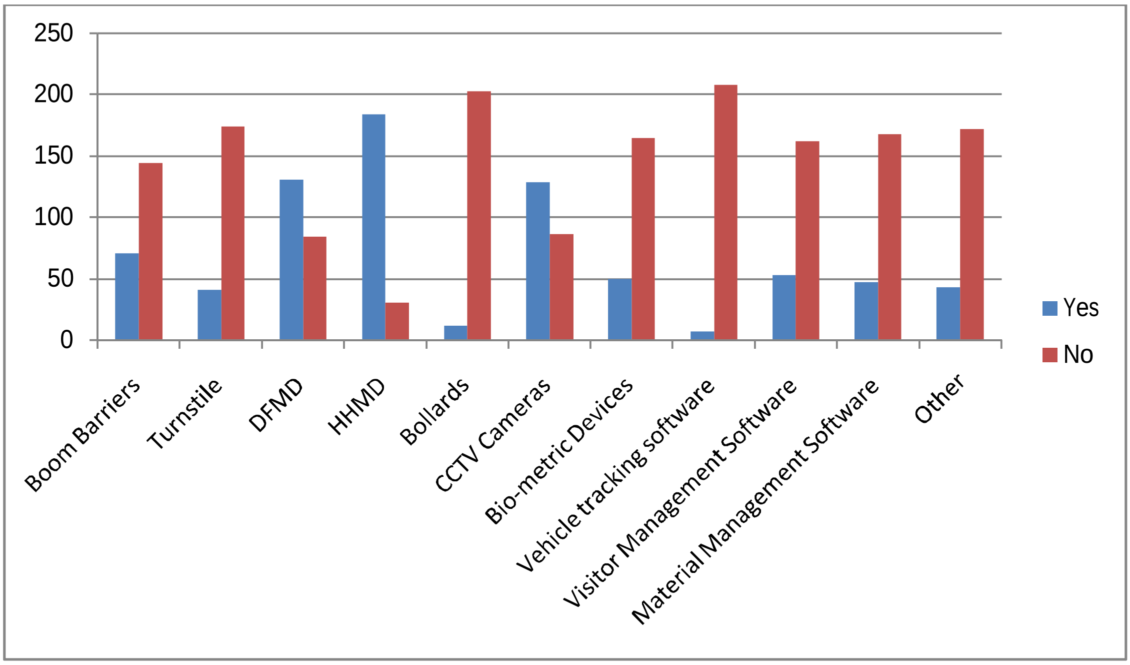
Yes	47
No	147



Are the following electronic gadgets available at the gate?

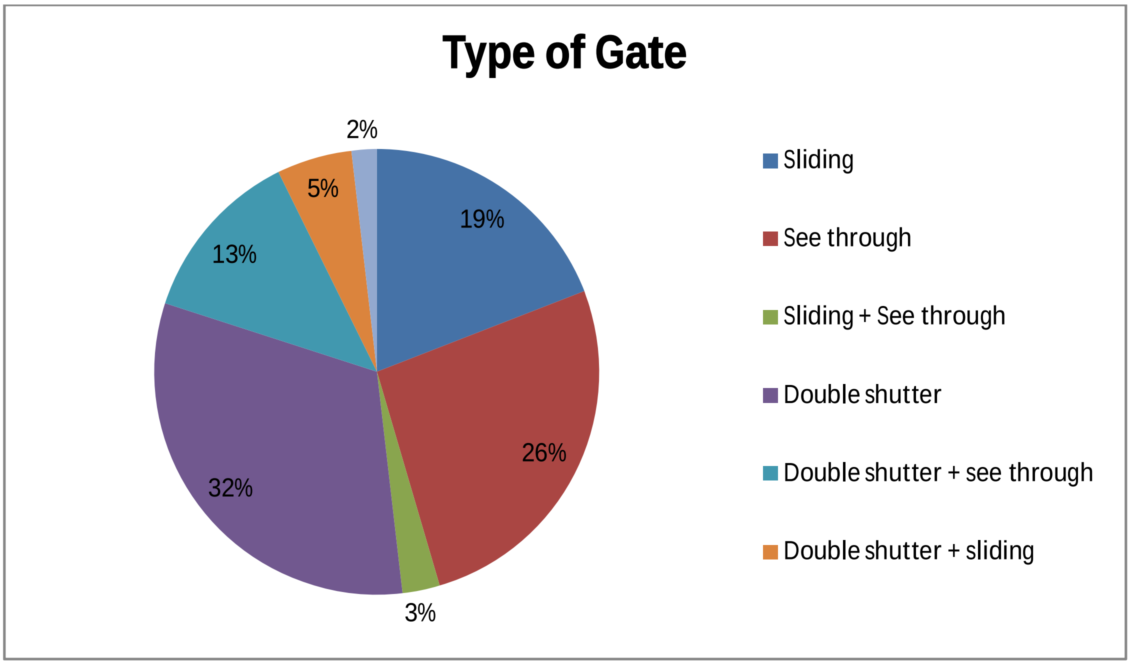
Except HHMD, CCTV and DFMD most of the essential gadgets required at gates are not available in most units

S. No.	Gadgets	Yes	No	%
1	Boom Barriers	71	144	33.02
2	Turnstile	41	174	19.07
3	DFMD	131	84	60.93
4	HHMD	184	31	85.58
5	Bollards	12	203	5.58
6	CCTV Cameras	129	86	60.00
7	Bio-metric Devices	50	165	23.26
8	Vehicle tracking software	7	208	3.26
9	Visitor Management Software	53	162	24.65
10	Material Management Software	47	168	21.86
11	Other	43	172	20.00



What is the type of gate?

Sliding	21
See through	29
Sliding + See through	3
Double shutter	35
Double shutter + see through	14
Double shutter + sliding	6
Sliding + See through + Single shutter + Double shutter	2



C.Watch Tower

While planning watch towers in the plant it is important to establish their distance from each other, height number and available of communication facilities in each watch tower

How many watch-towers are there in your company?

Min	0
Max	50
Average	7.85

What is the height of the watch-towers?

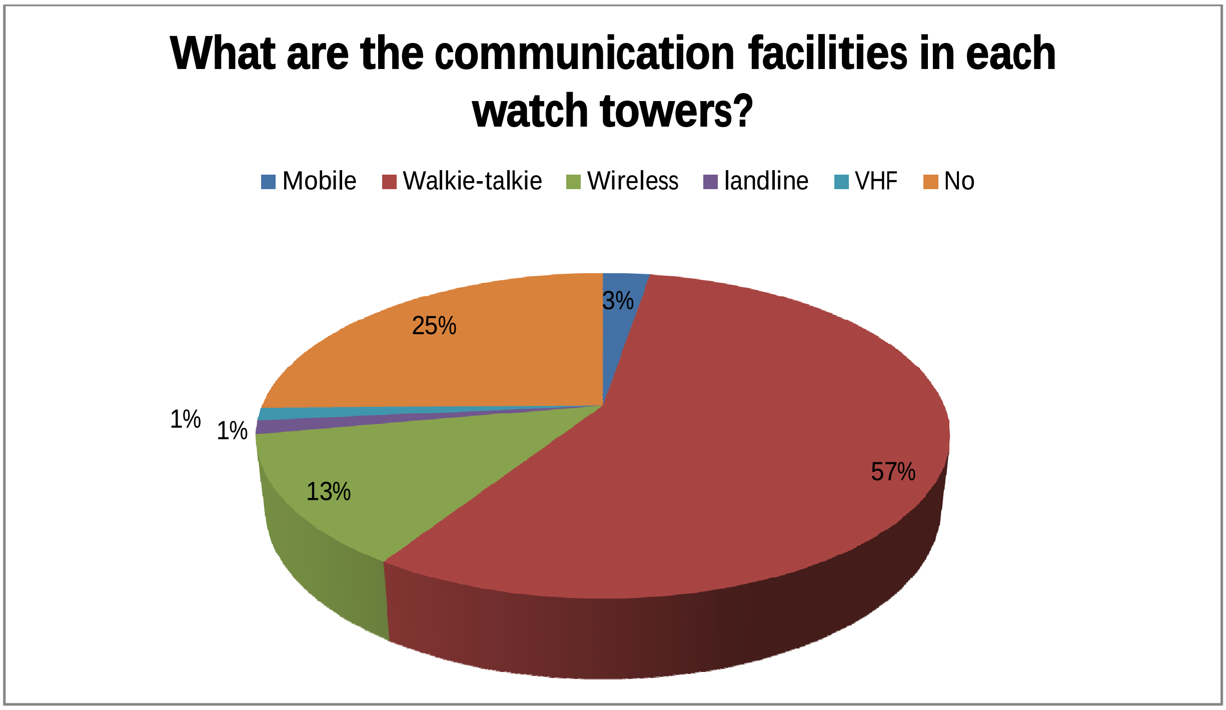
Min	8 Feet
Max	250 Feet
Average	24.27 Feet

What is the distance of one watch tower from the other?

Min	1 Feet	
Max	3000 Feet	(10 km)
Average	570 Feet	

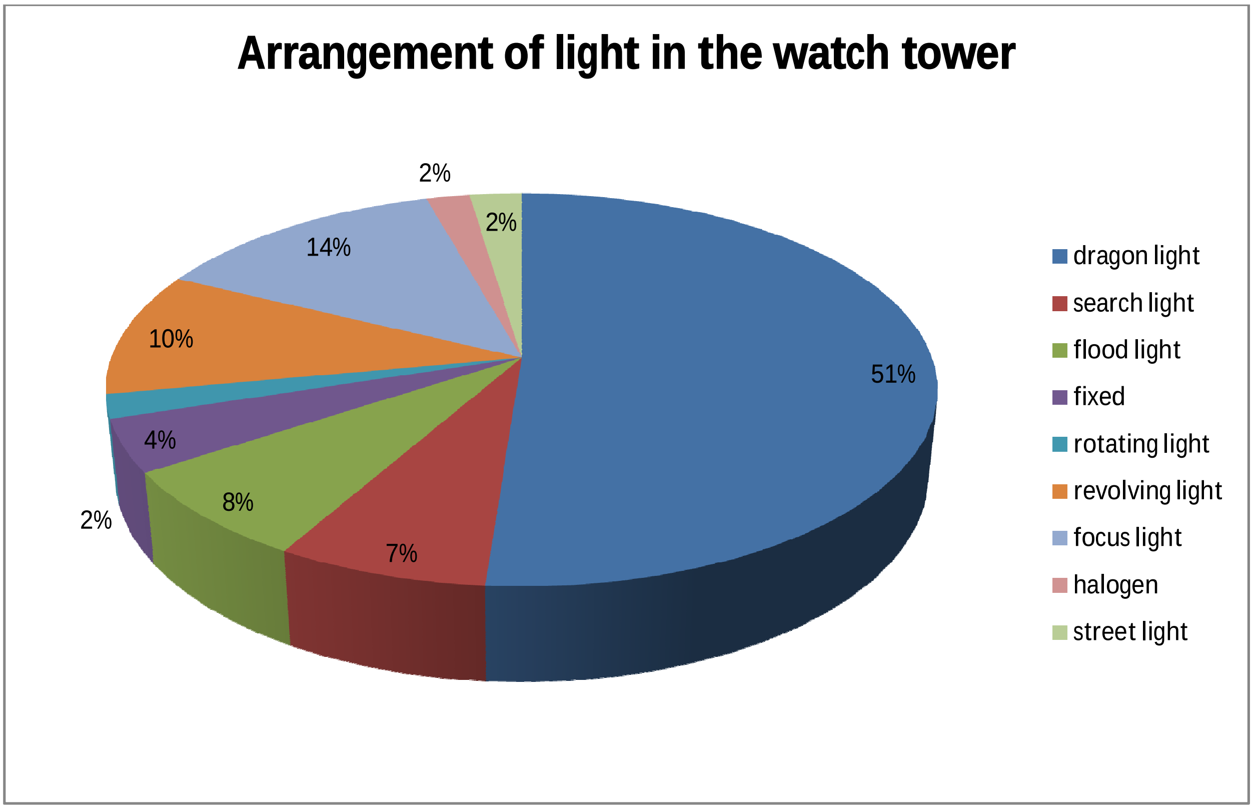
What are the communication facilities in each watch towers?

Mobile	6
Walkie-talkie	130
Wireless	30
landline	3
VHF	3
No	58



What is the arrangement of light in the watch tower?

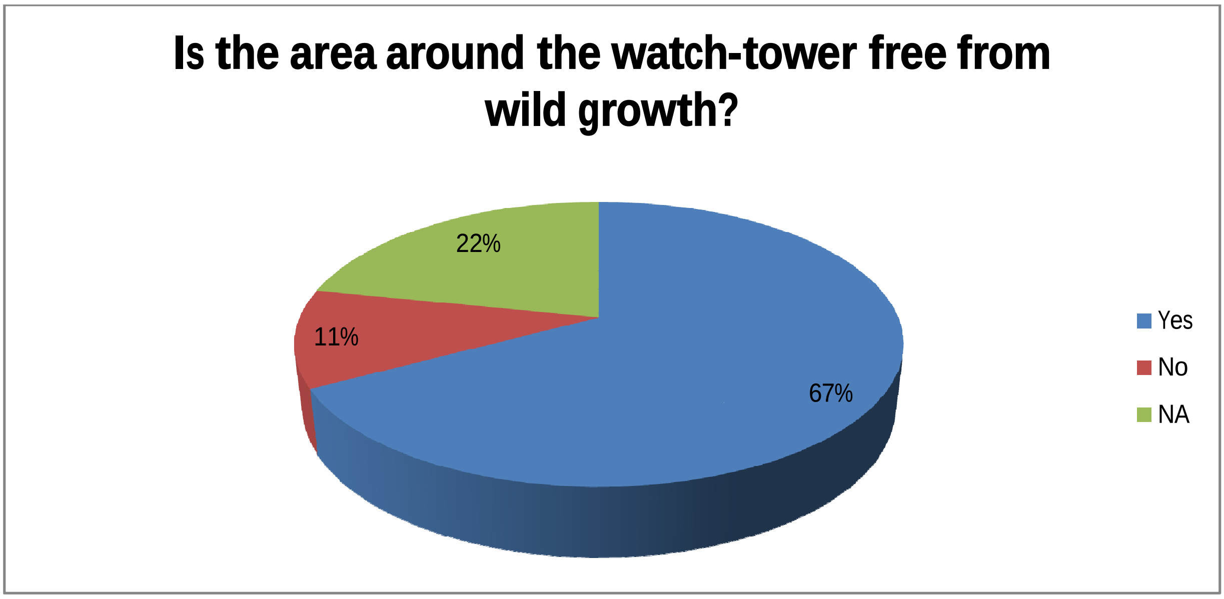
Dragon Light	130
Search Light	18
Flood Light	19
Fixed	11
Rotating Light	5
Revolving Light	26
Focus Light	34
Halogen	5
Street Light	6



Arrangement of light in the watch tower

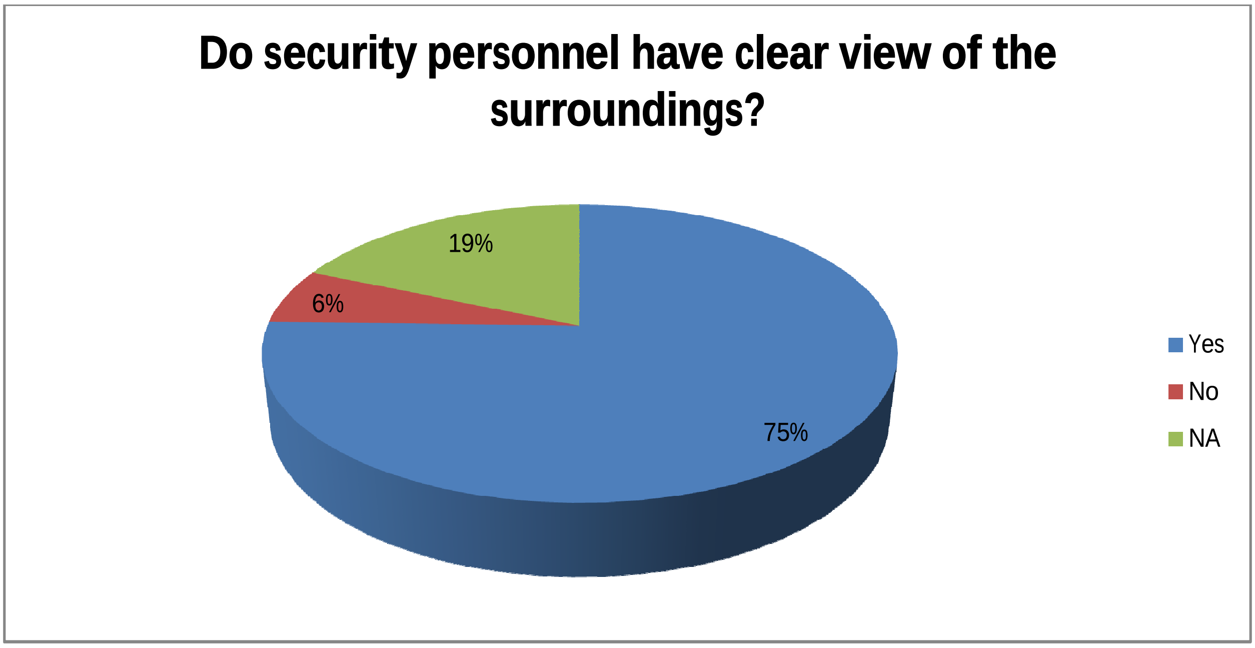
Is the area around the watch-tower free from wild growth?

Yes	145
No	24
NA	47



Do security personnel have clear view of the surroundings?

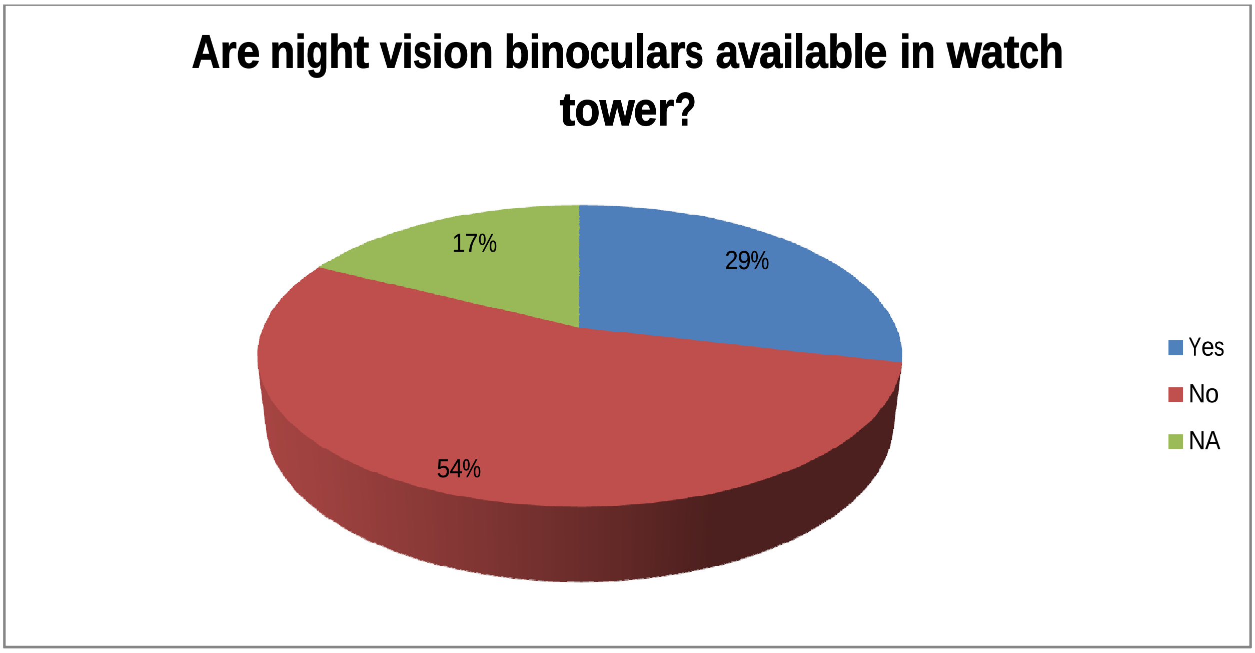
Yes	163
No	13
NA	40



Are night vision binoculars available in watch tower?

Night vision binoculars are essential for watching on intrudes during night time. 54% of the units don’t have them

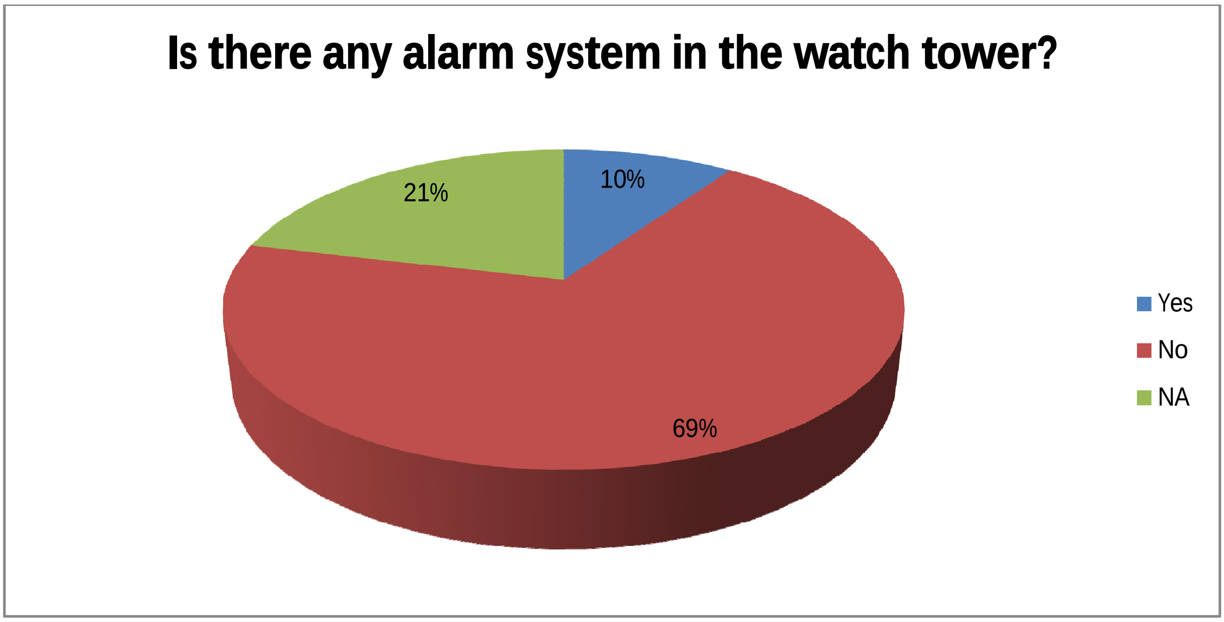
Yes	62
No	116
NA	38



Is there any alarm system in the watch tower?

Alarm systems in the watch towers provide for general alarms in eh event of any incident which requires everyone to be aware of the incident. However 69 % of the units are not provided with alarm systems

Yes	21
No	149
NA	46



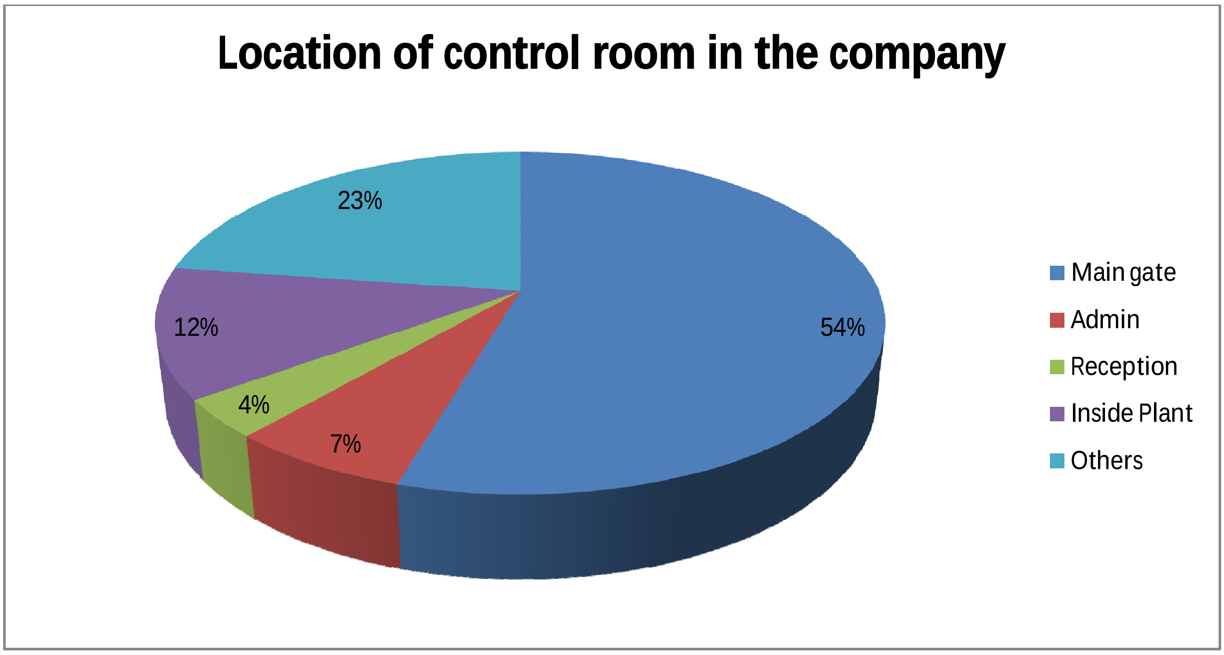
What is the distance of watch tower from the boundary wall?

Min	0 Feet	
Max	3000 Feet	(10 km)
Average	77 Feet	

D. Control Room

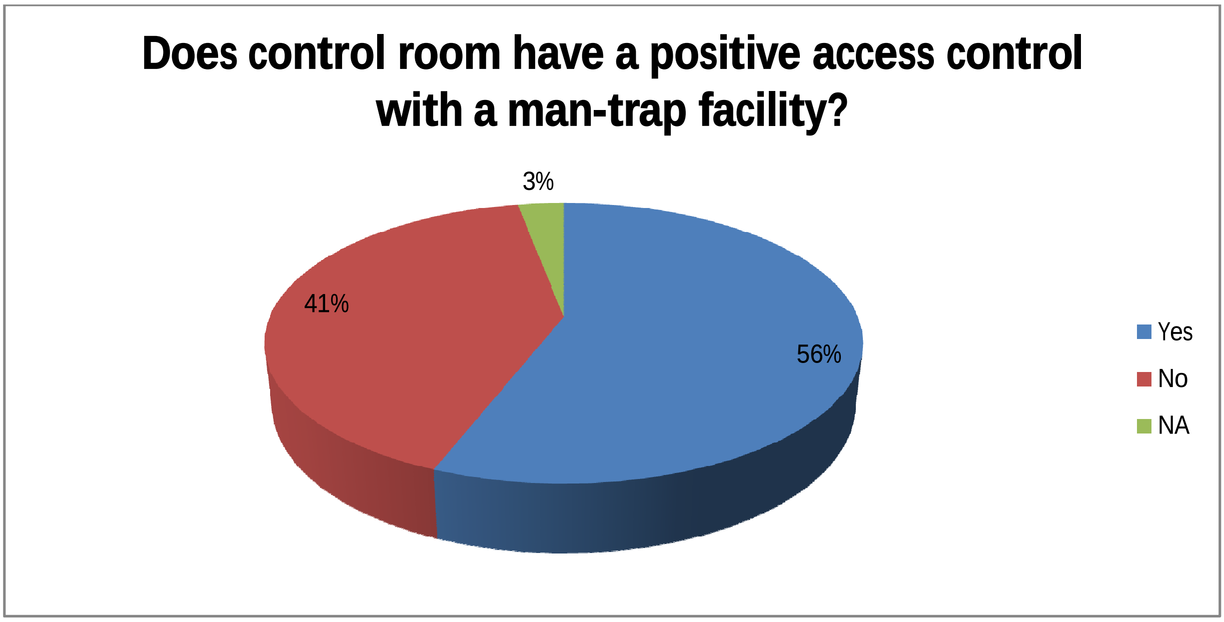
What is the location of control room in your company?

Main gate	120
Admin	15
Reception	8
Inside Plant	27
Others	50



Does it have a positive access control with a man-trap facility?

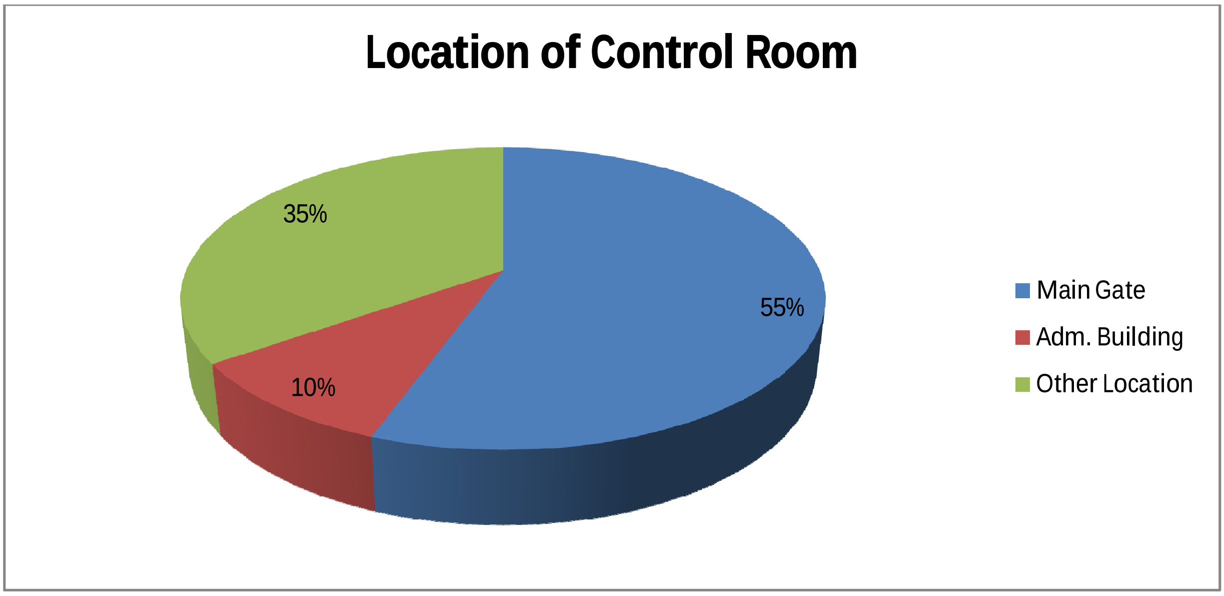
Yes	113
No	83
NA	6



Is it on the gate or at Admin building?

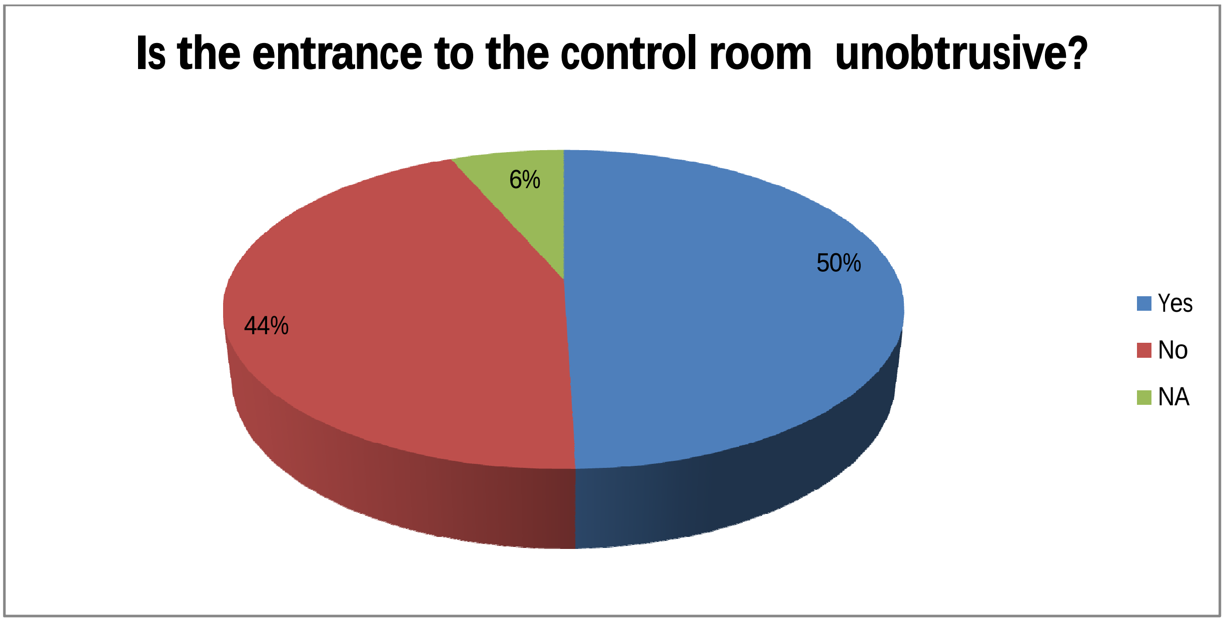
Control room should generally be located at the main gate. That is where access is controlled. Only 55% of the units have control rooms located at the main gate

Main Gate	120
Adm. Building	21
Other Location	75



Is the entrance to the control room unobtrusive?

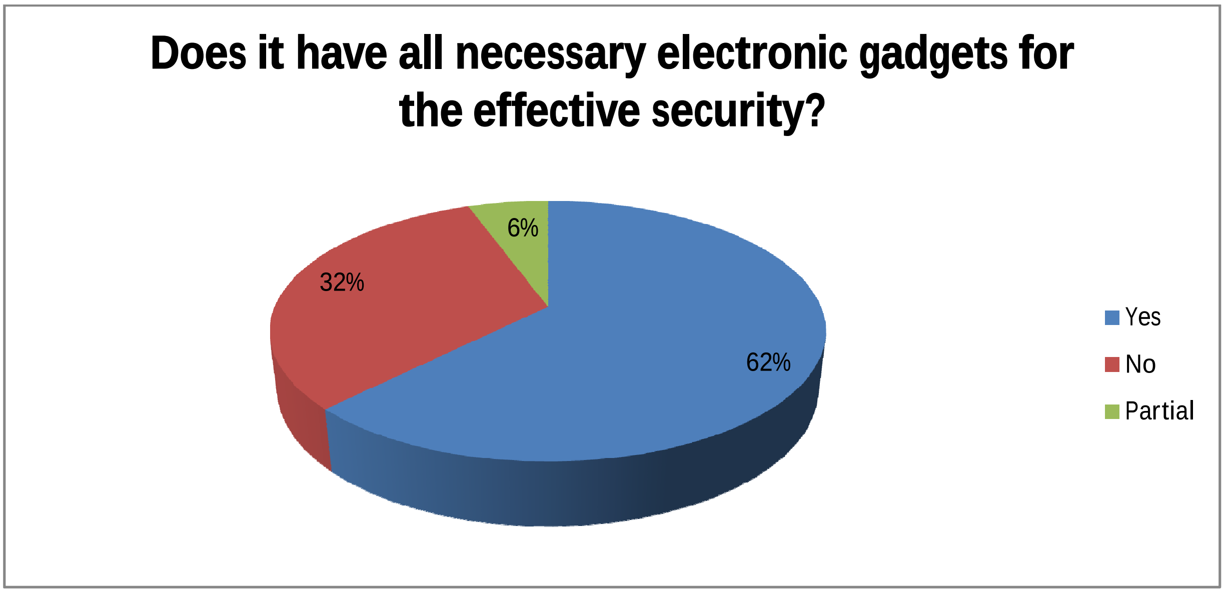
Yes	107
No	95
NA	14



Does it have all necessary electronic gadgets for effective security?

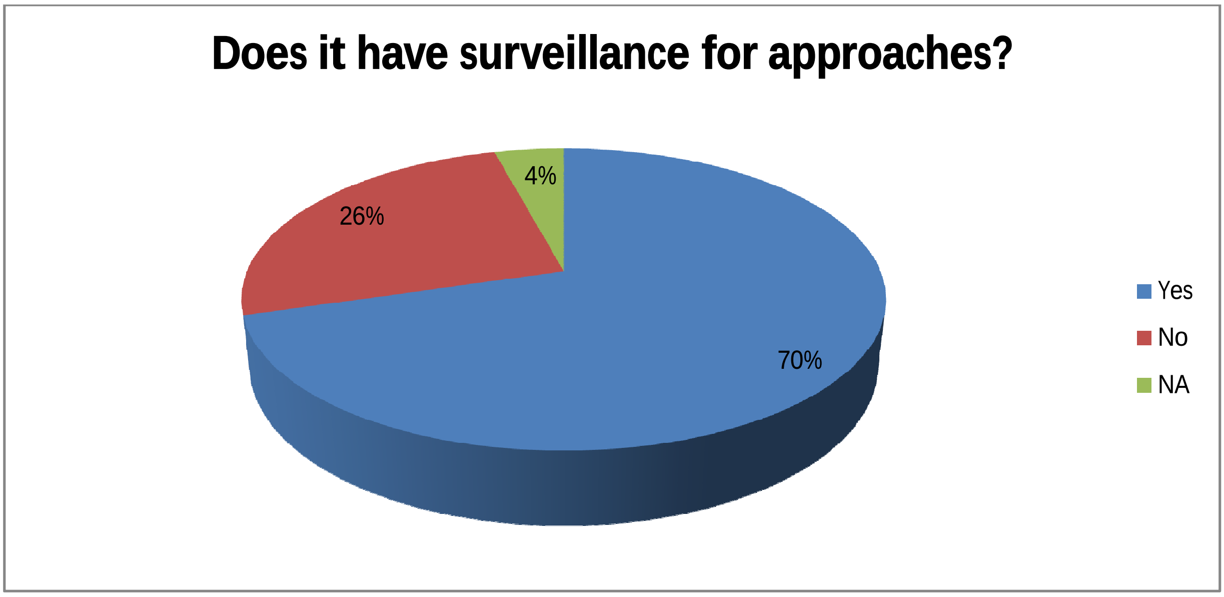
32% of the control rooms do not necessary electronic gadgets which are essential for manning the control room as control room is the nerve centre of all activity and if one wants to disrupt the activity, it can be done by targeting the control room

Yes	135
No	69
Partial	12



Does it have surveillance for approaches?

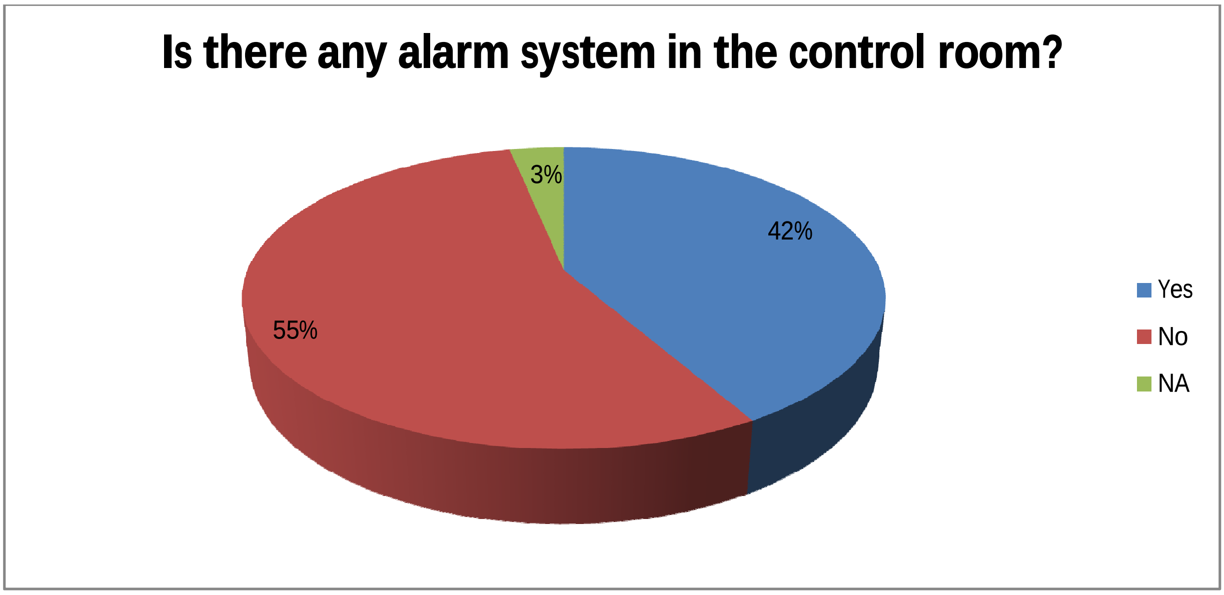
Yes	152
No	55
NA	9



Is there any alarm system in the control room?

Alarm system in the control room is essential to warn others of any unauthorised intrusion. 55% of the units do not have alarms systems in the control room

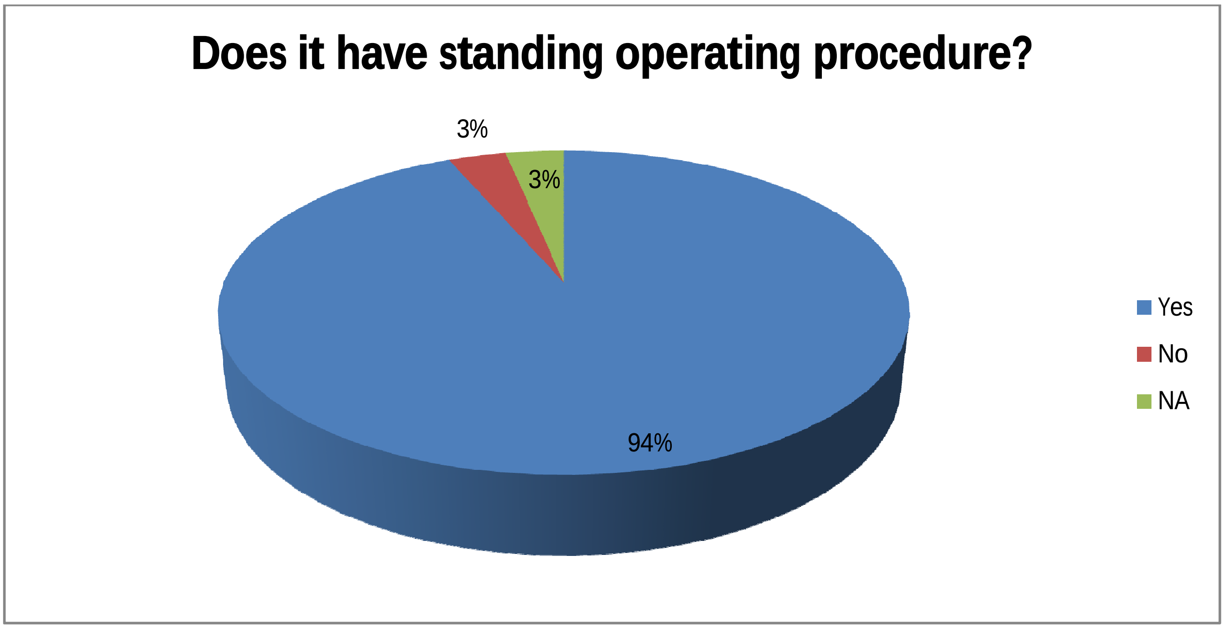
Yes	90
No	119
NA	7



Does it have standing operating procedure?

SOP is essential in any unit. Most control rooms surveyed have SOPs

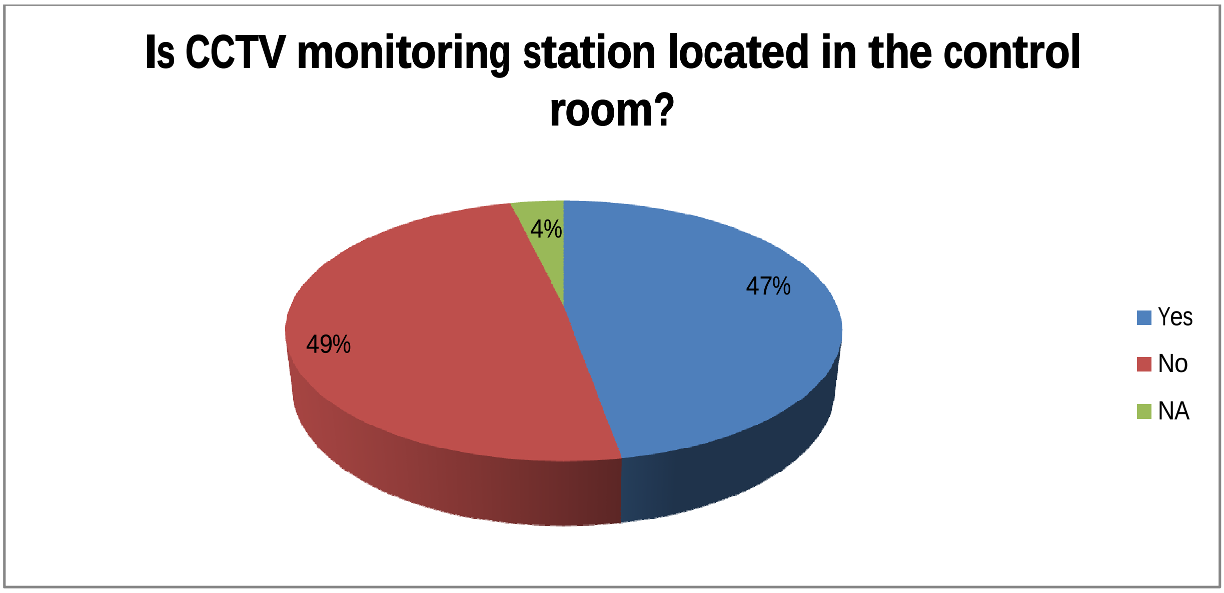
Yes	202
No	7
NA	7



Is CCTV monitoring station located in the control room?

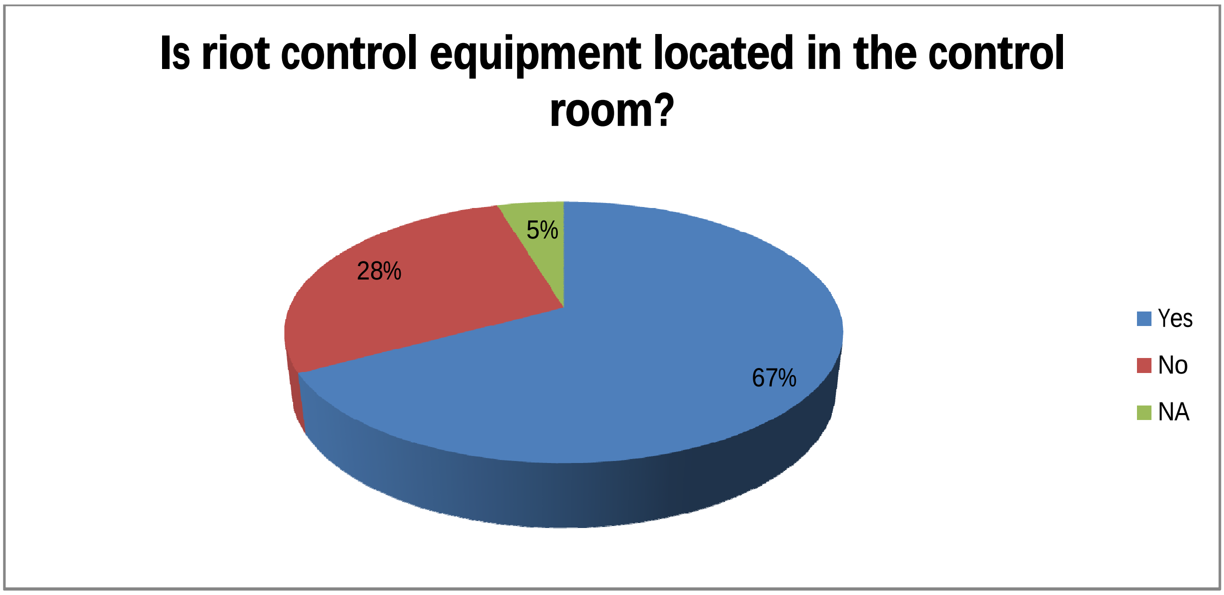
CCTV monitoring is a debatable issue depending on the felt need of the management and hence it is noticed that half of the units do not have in the control room

Yes	102
No	106
NA	8



Is the riot control equipment located in the control room?

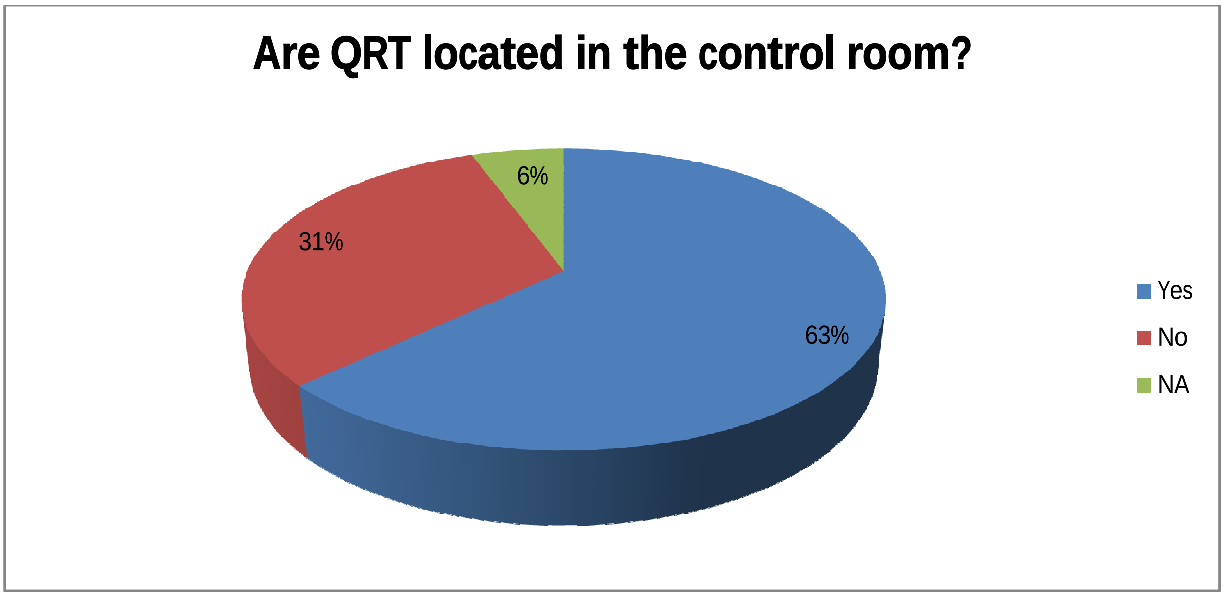
Yes	145
No	61
NA	10



Is riot control equipment located in the control room?

Are QRT located in the control room?

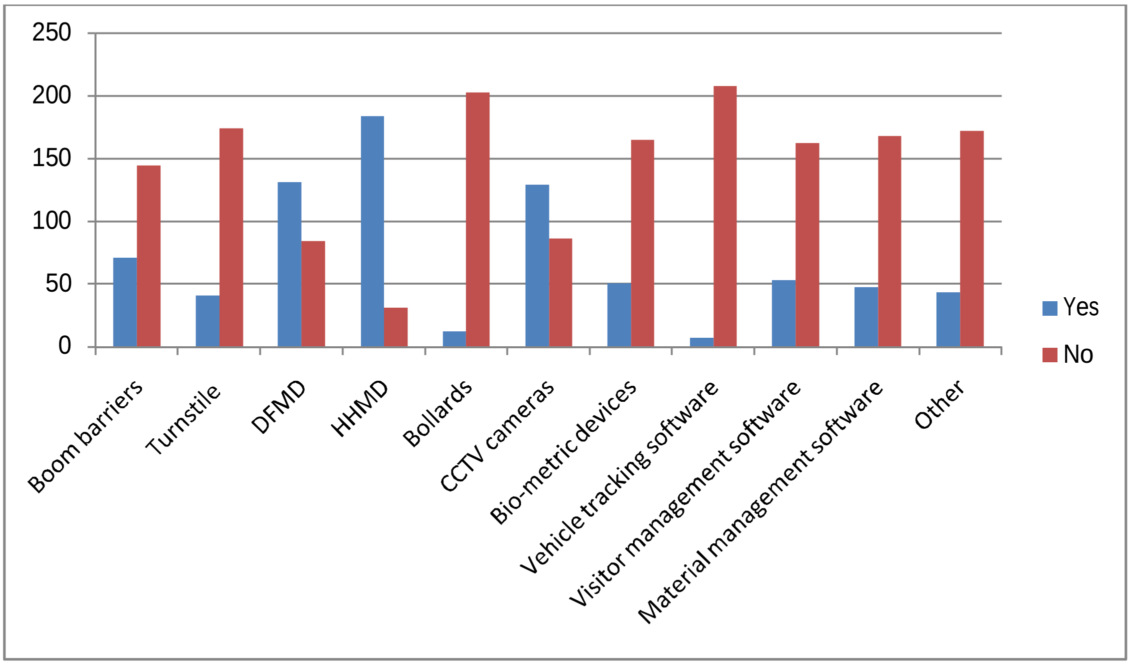
Yes	136
No	68
NA	12



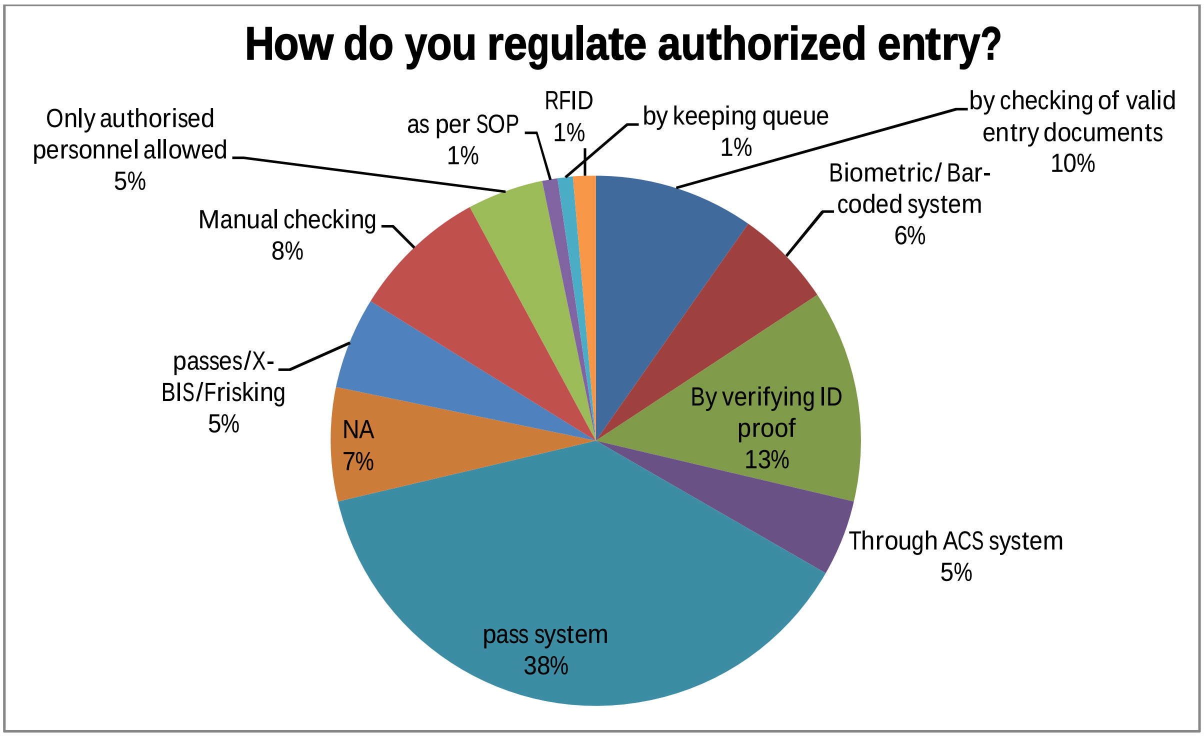
E. Access Control

What are the measures for ensuring access control in your company?

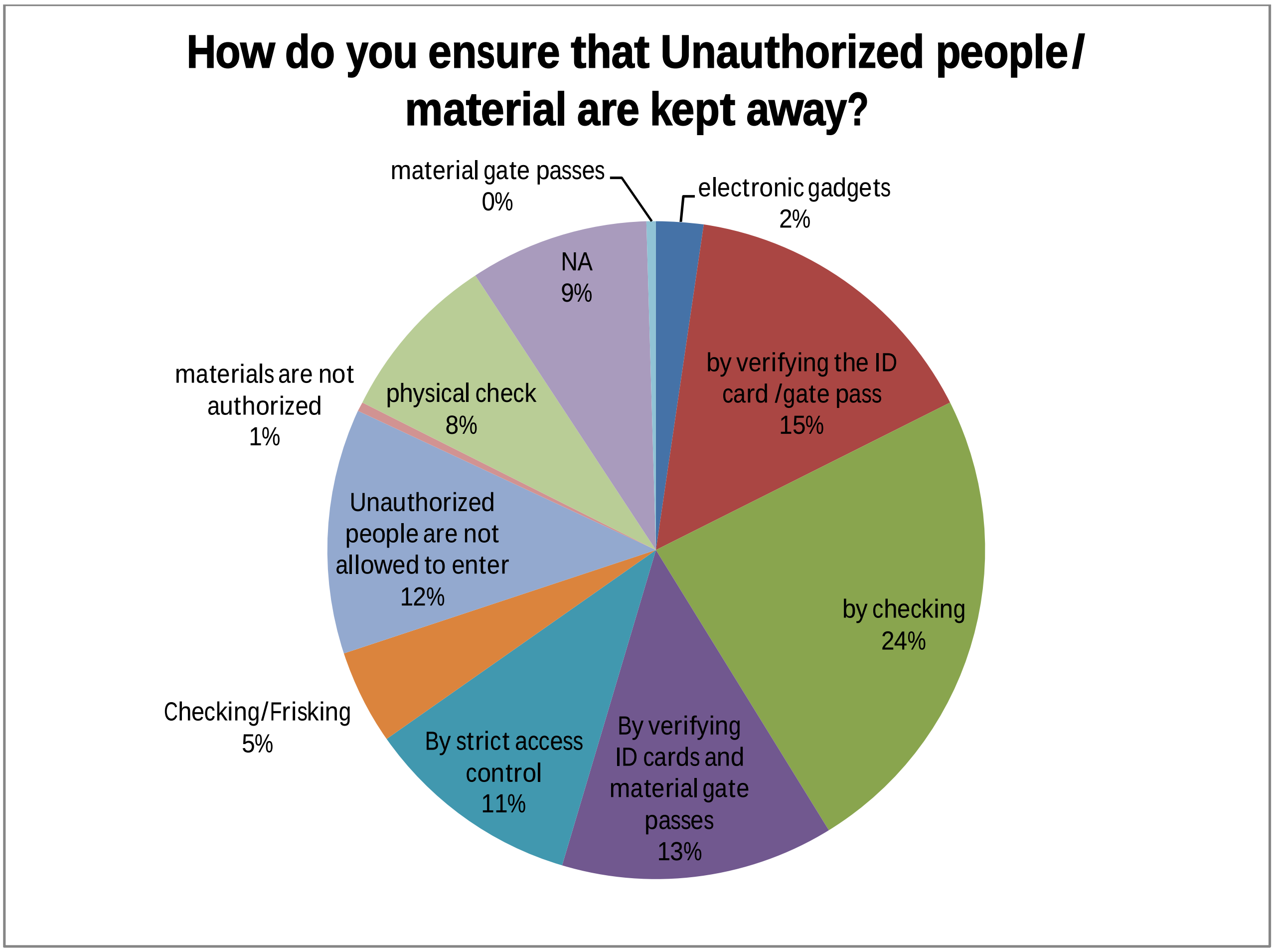
Measures	Yes	No	Percentage
Boom barriers	71	144	33.02
Turnstile	41	174	19.07
DFMD	131	84	60.93
HHMD	184	31	85.58
Bollards	12	203	5.58
CCTV cameras	129	86	60
Bio-metric devices	50	165	23.26
Vehicle tracking software	7	208	3.26
Visitor management software	53	162	24.65
Material management software	47	168	21.86
Other	43	172	20



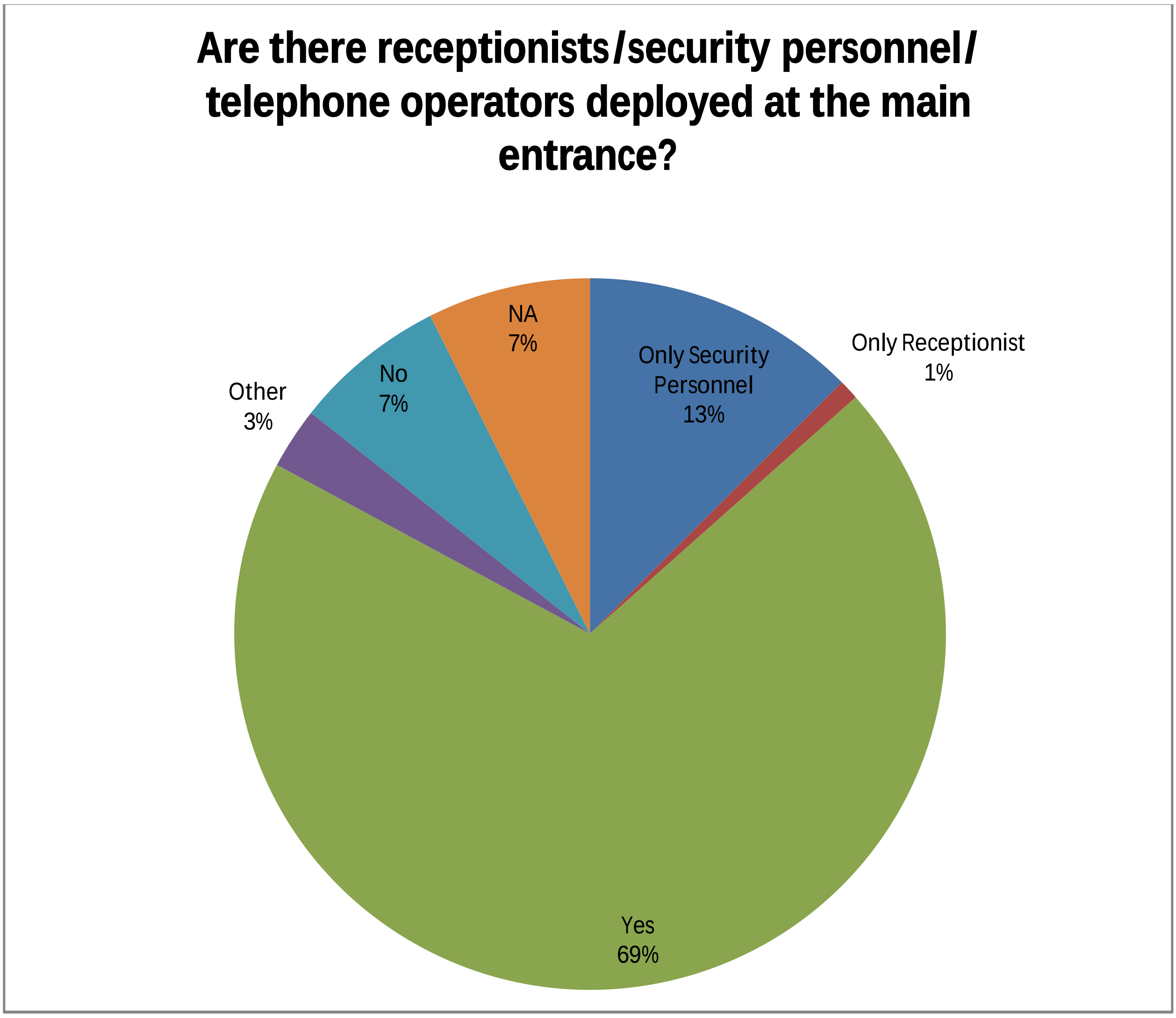
How do you regulate authorized entry?



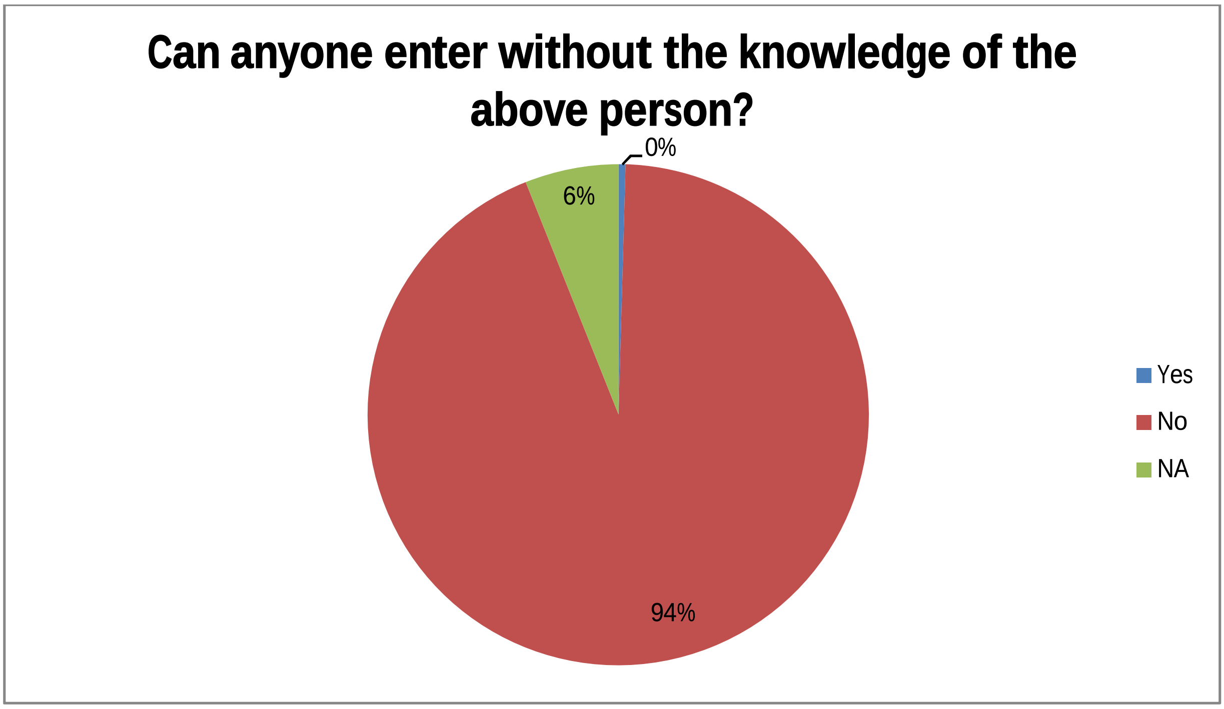
How do you ensure that unauthorized people/ material are kept away?



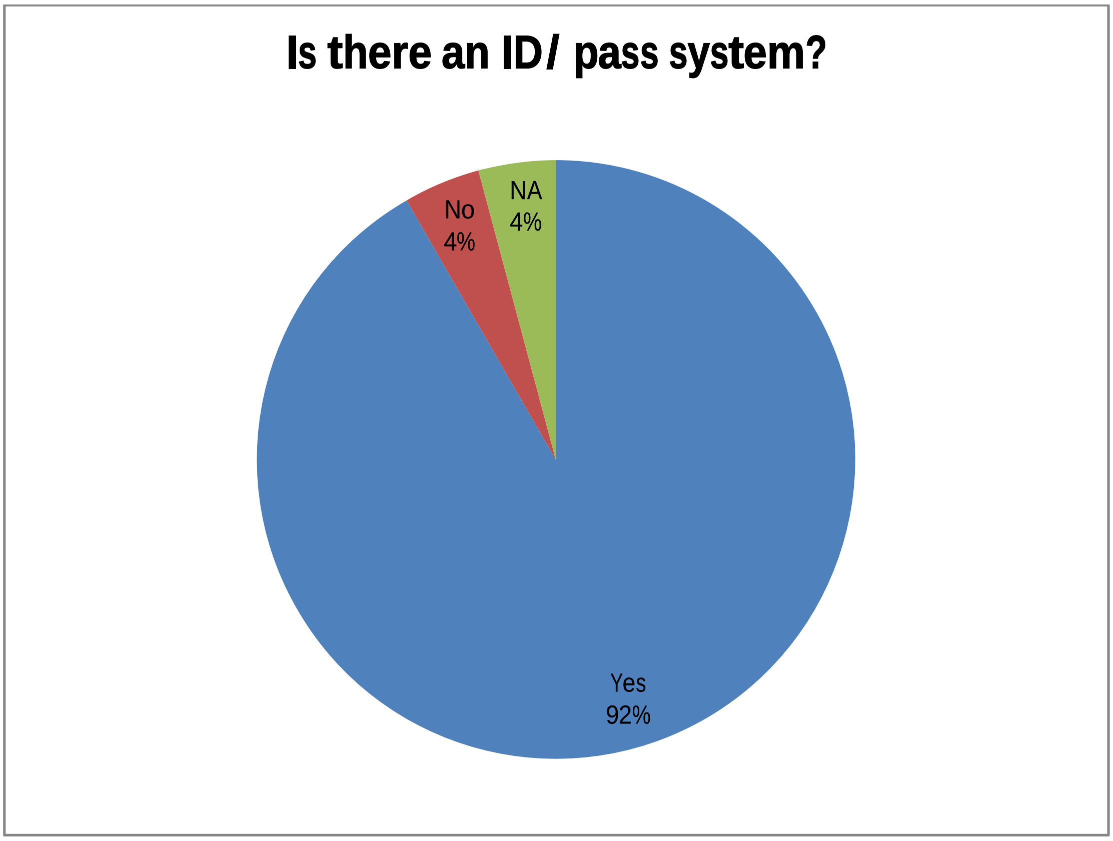
Are there receptionist/ security personnel/ telephone operator deployed at the main entrance?

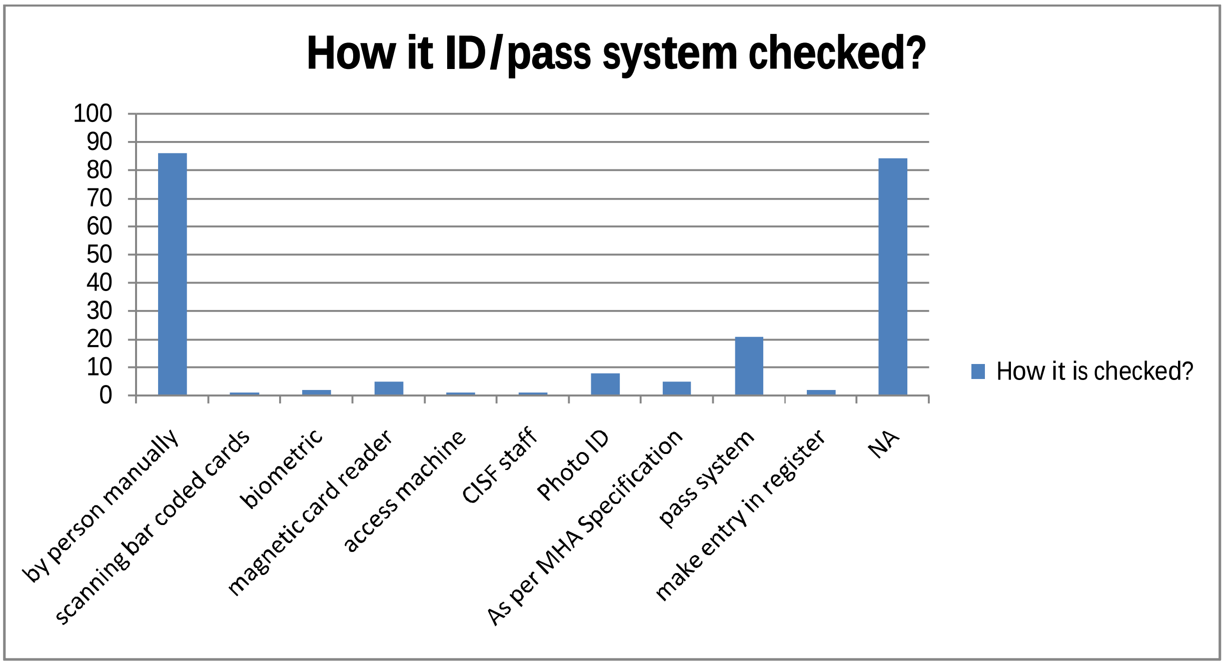


Can anyone enter without the knowledge of the above person?

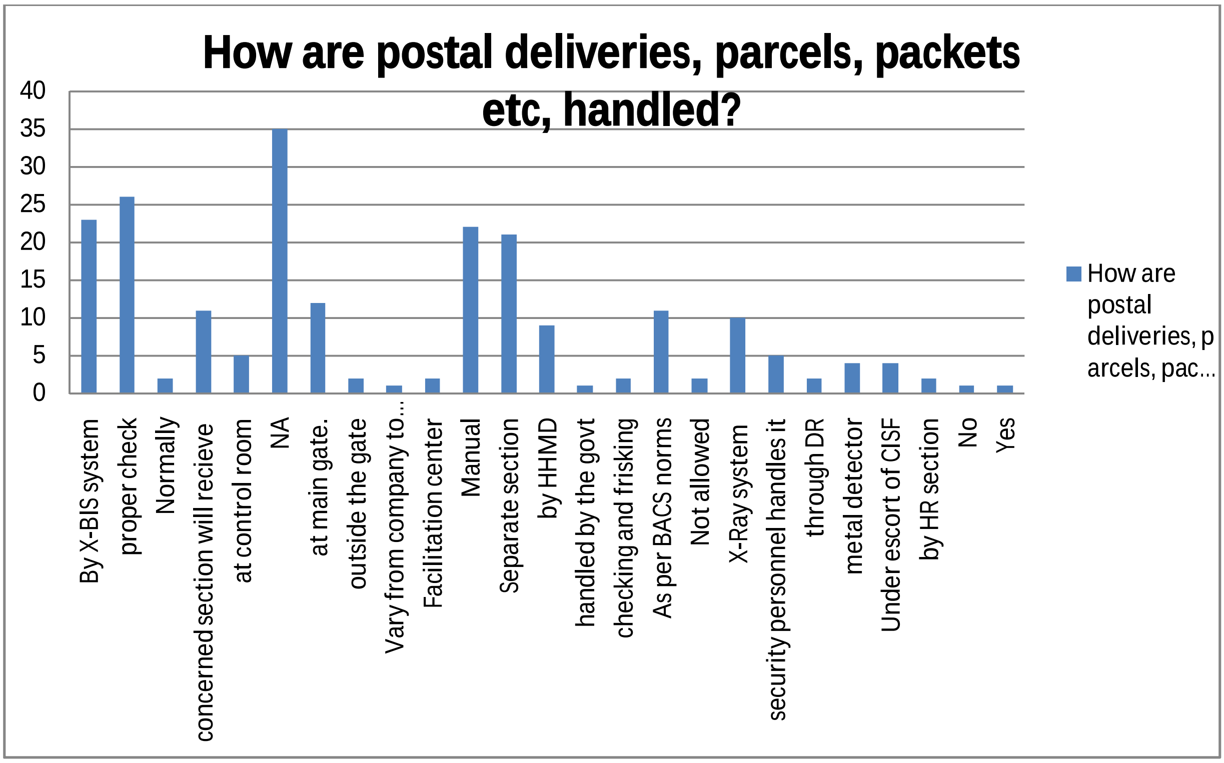


Is there an ID/ pass system?

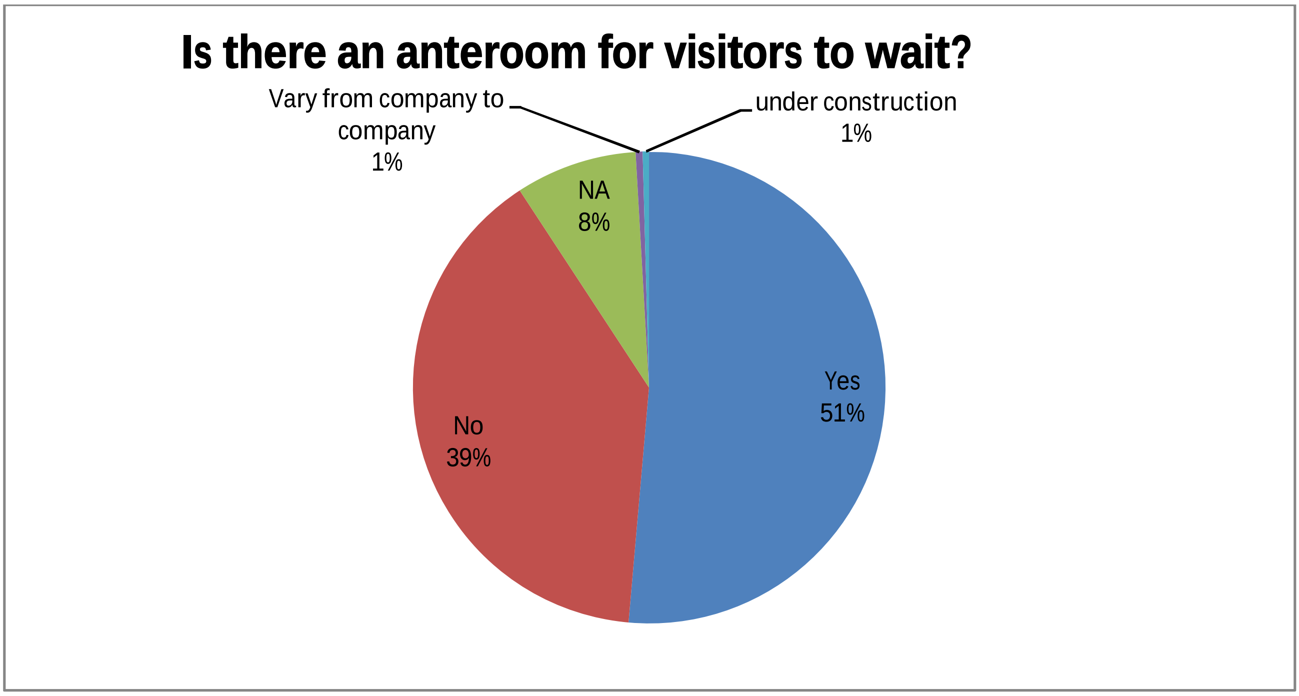




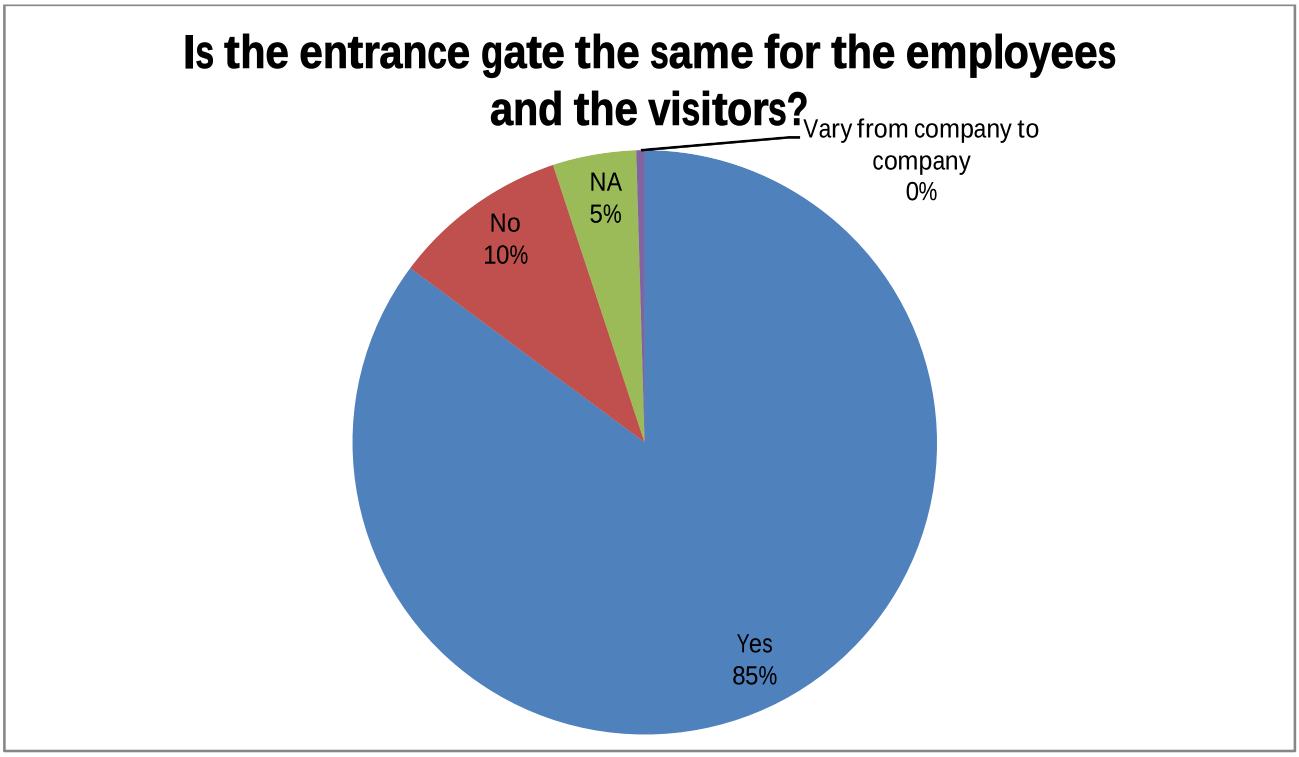
How are postal deliveries, parcels, packets etc, handled?



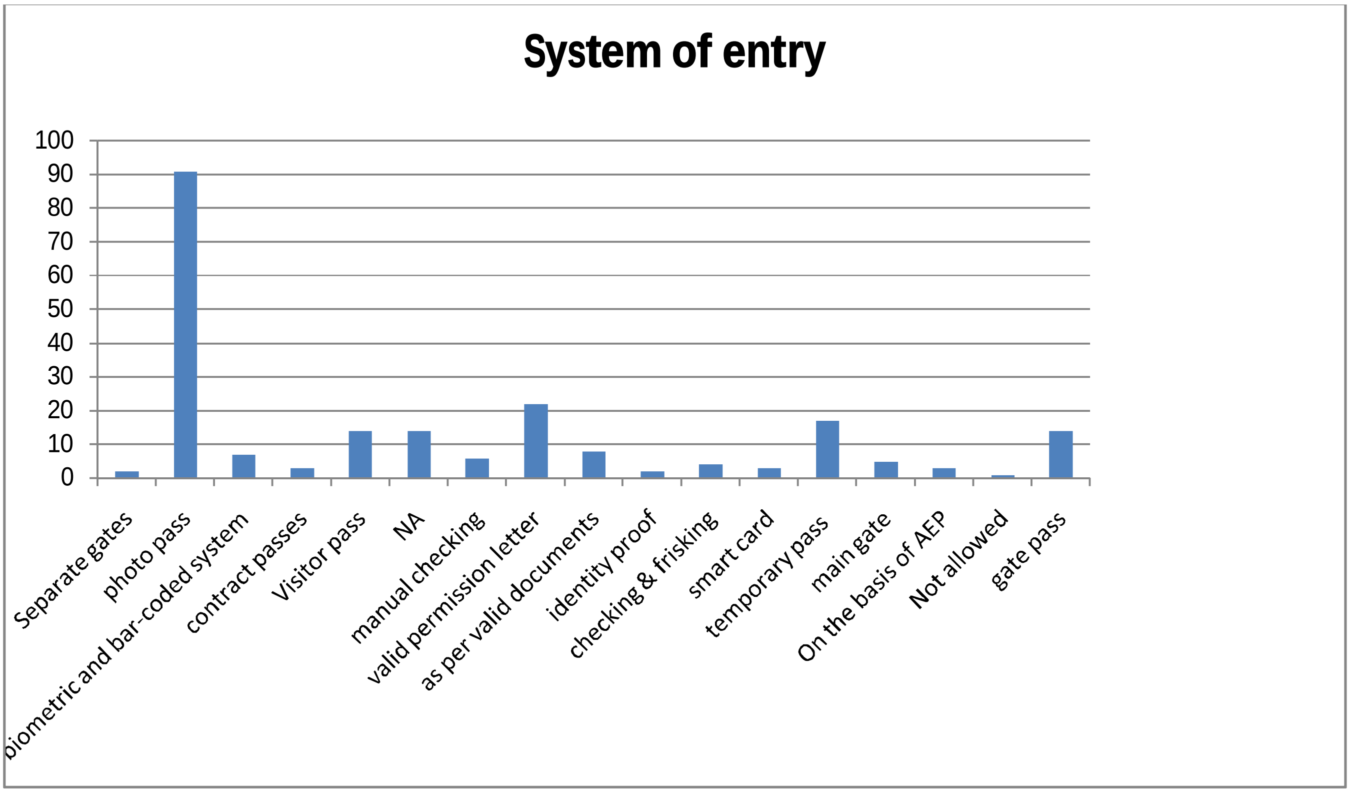
Is there an anteroom for visitors to wait?



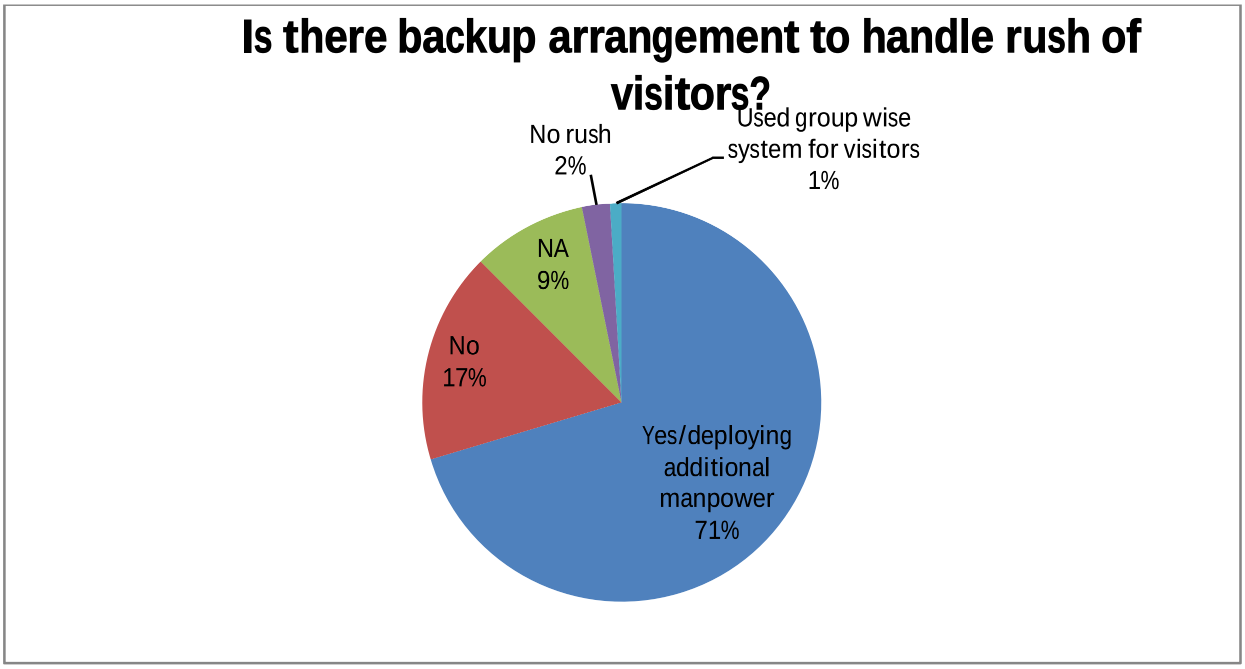
Is the entrance gate the same for the employees and the visitors?



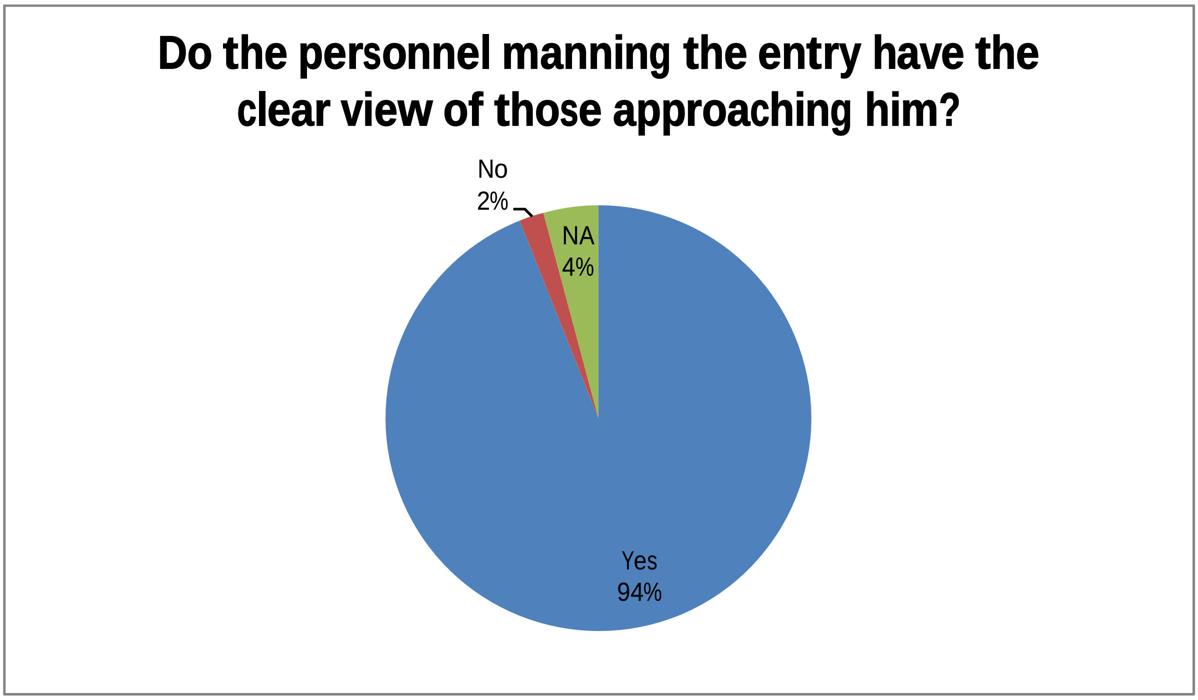
What is the system of entry (for maintenance people, telephone mechanics, cleaners and casual maintained personnel)?



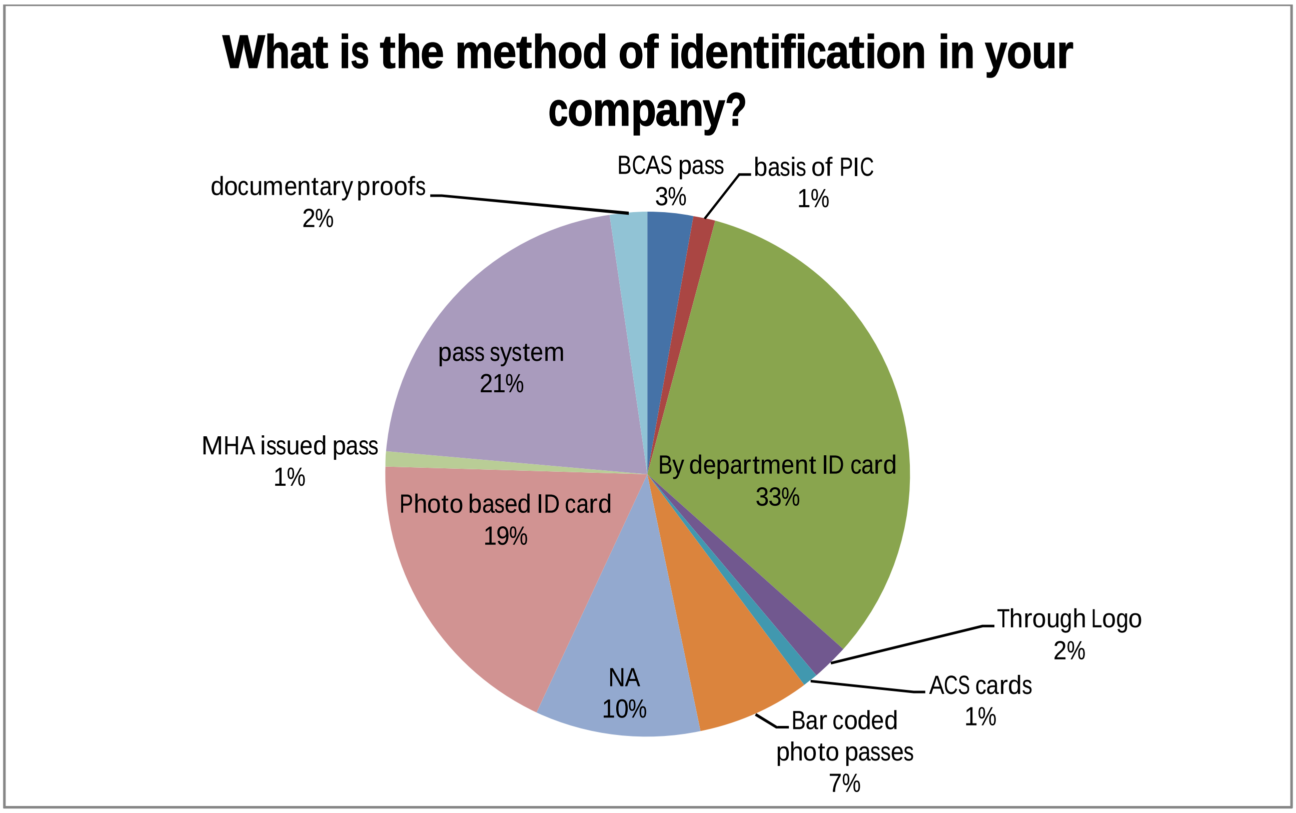
Is there backup arrangement to handle rush of visitors?



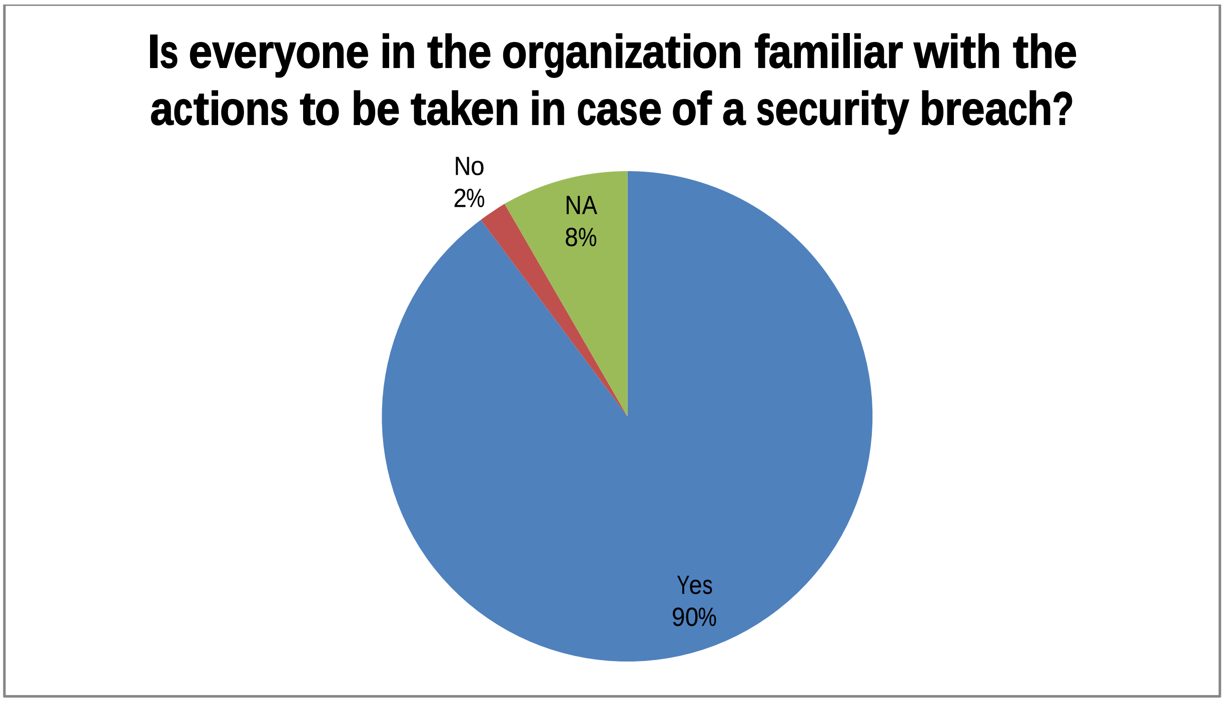
Do the personnel manning the entry have the clear view of those approaching him?



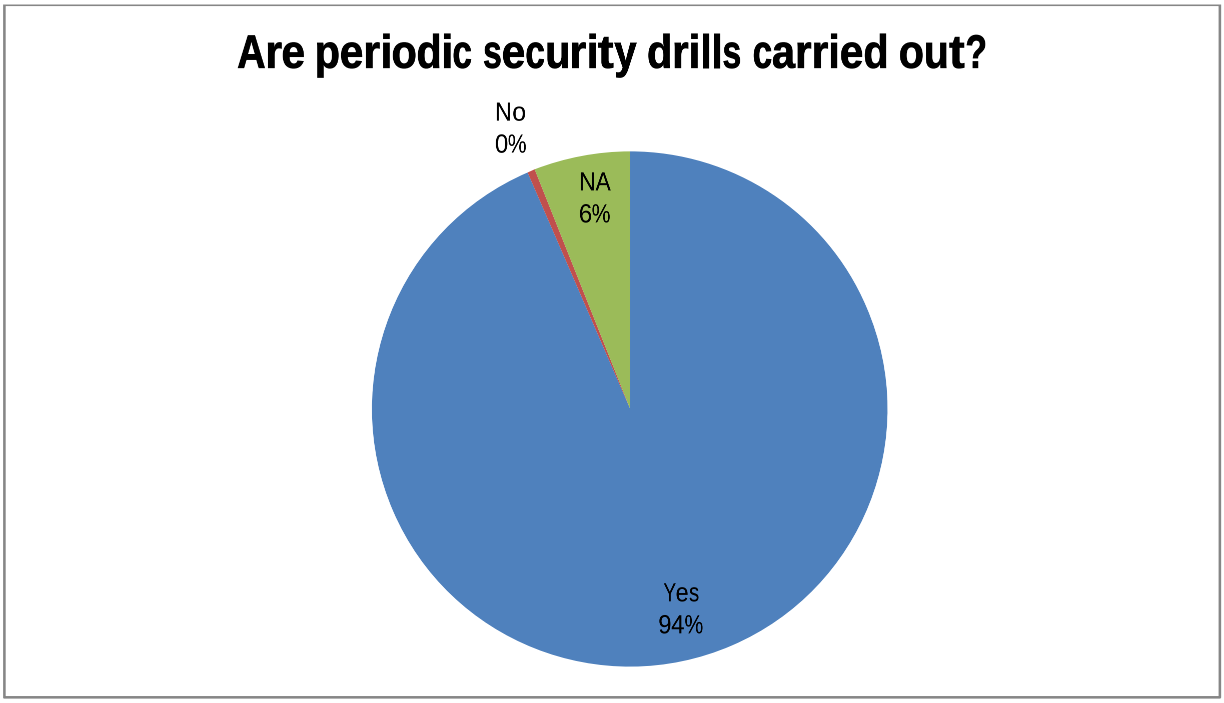
What is the method of identification in your company?



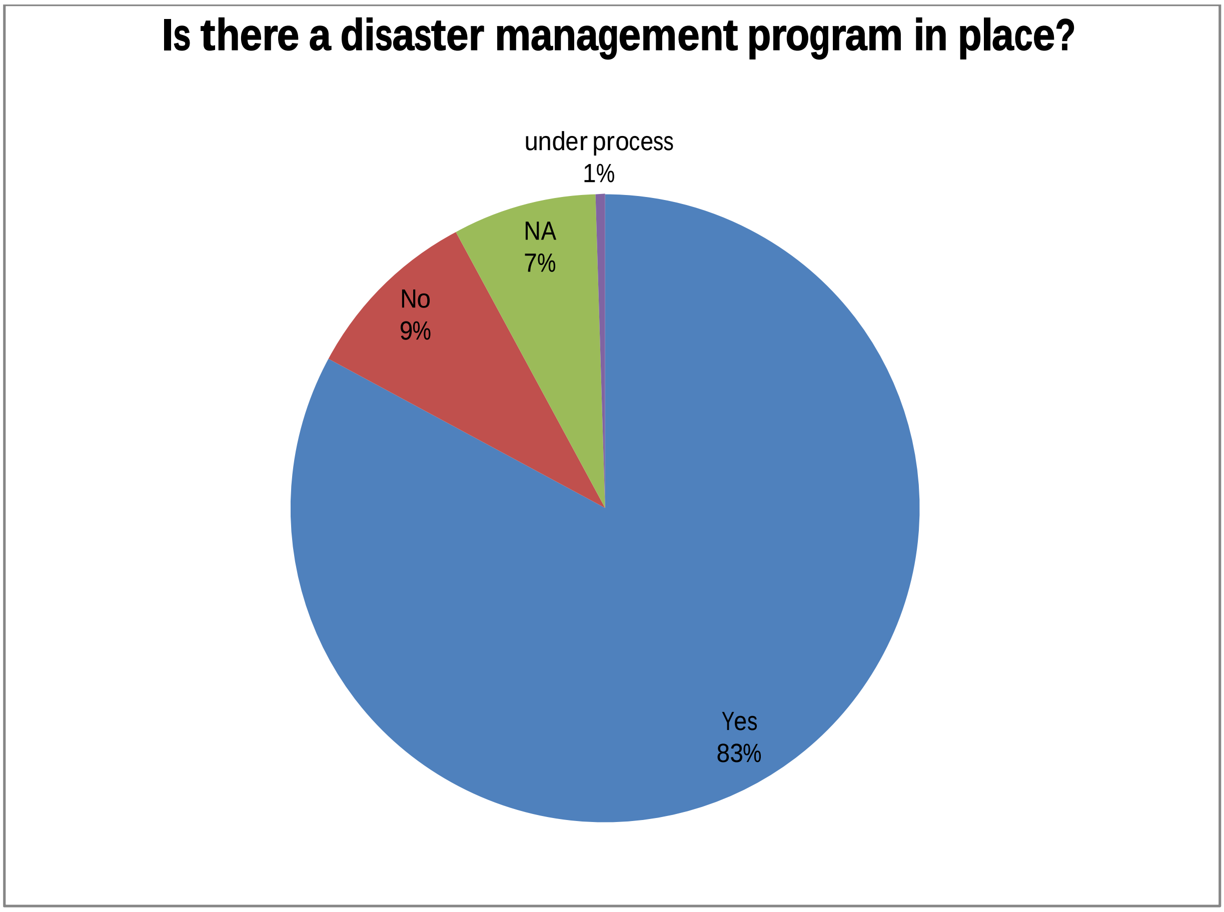
Is everyone in the organization familiar with the actions to be taken in case of a security breach?



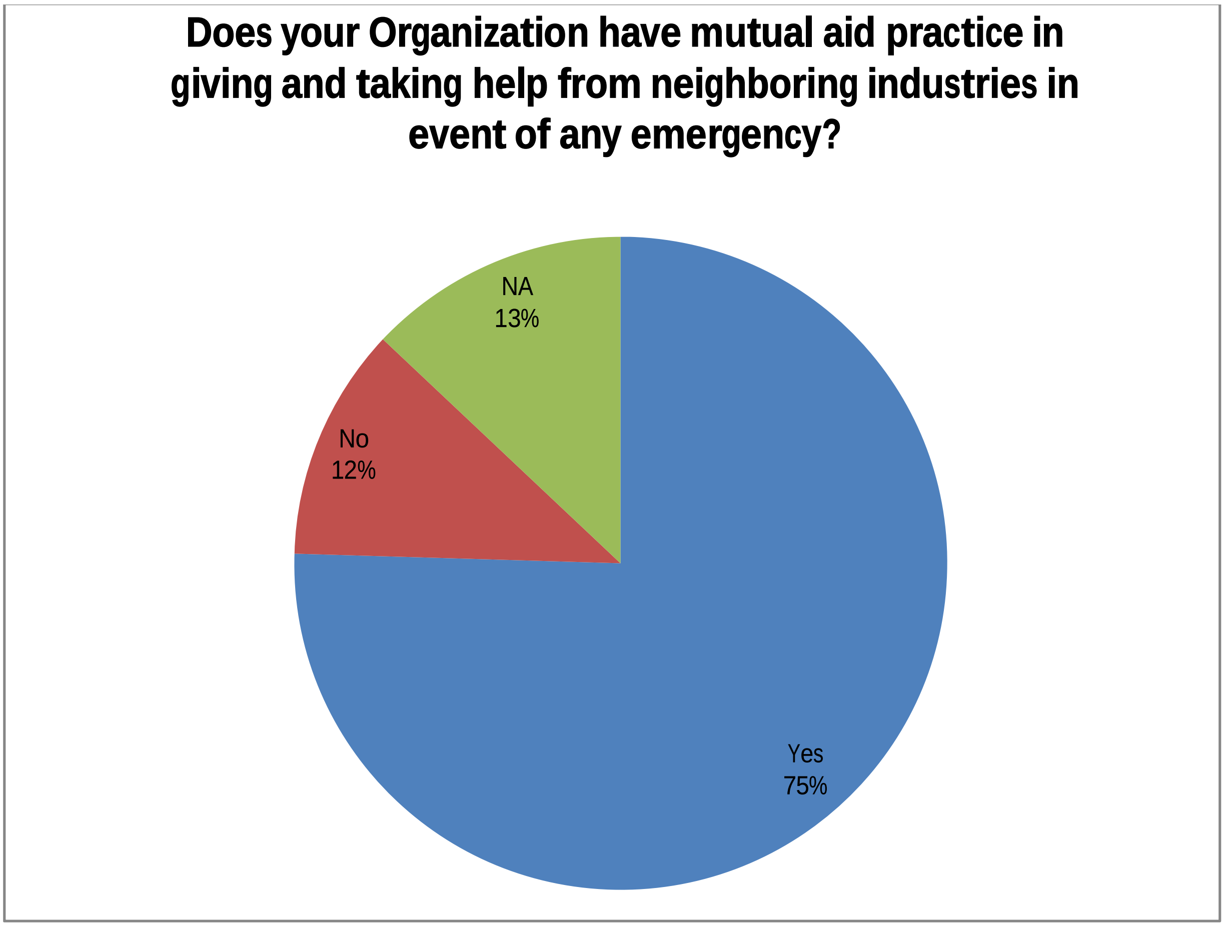
Are periodic security drills carried out?



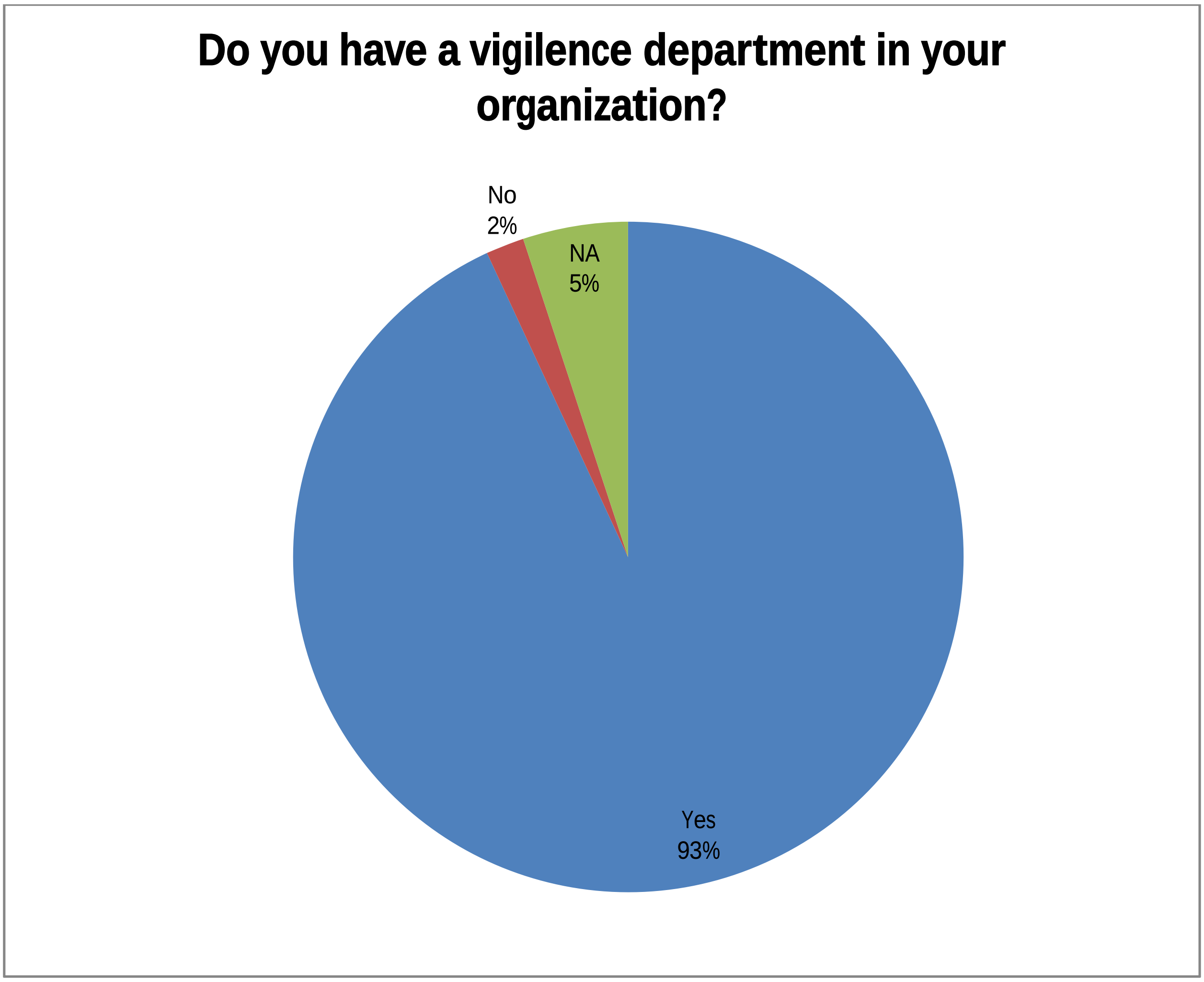
Is there a disaster management program in place?



Does your Organization have mutual aid practice in giving and taking help from neighbouring industries in event of any emergency?



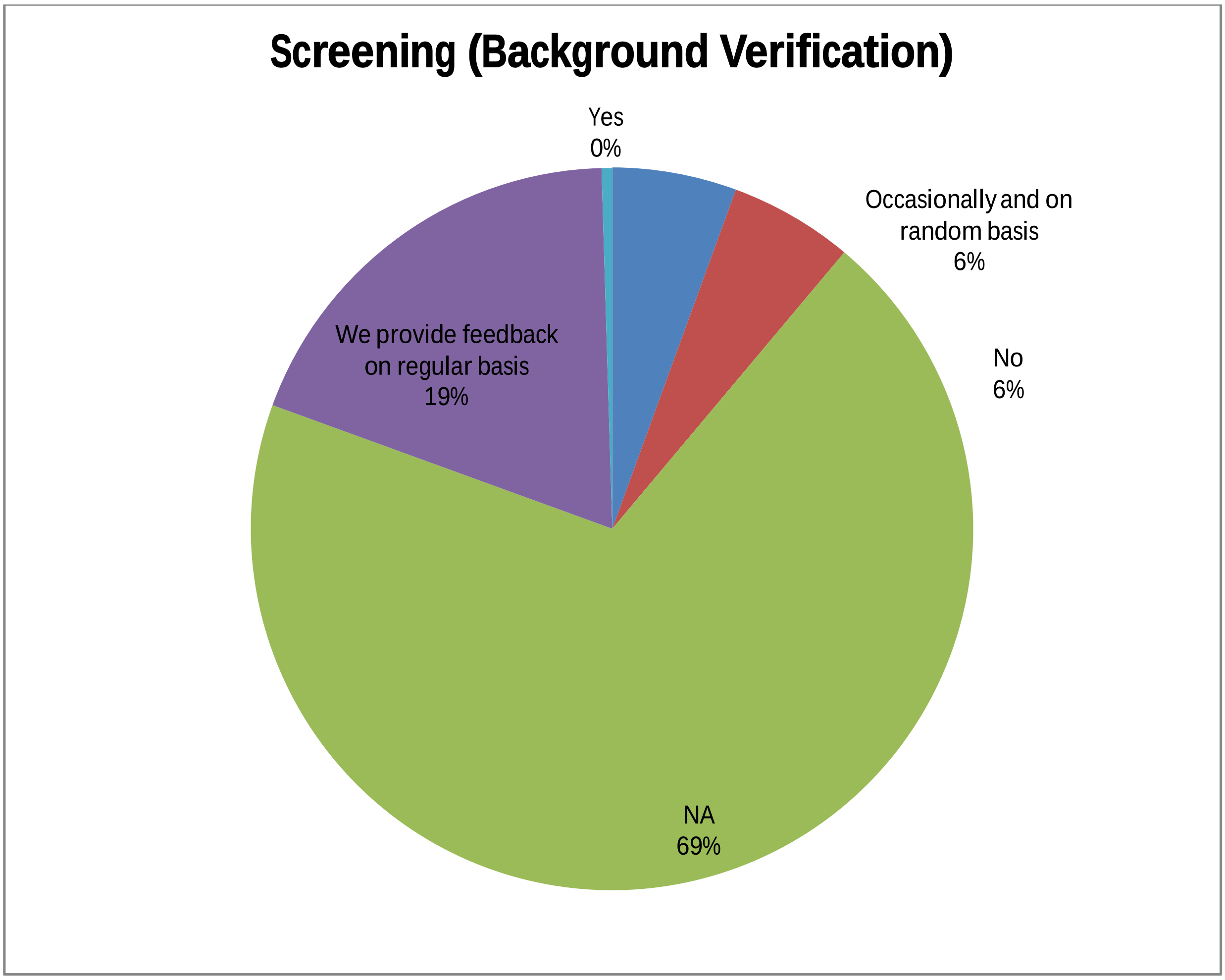
Do you have a vigilance department in your organization?

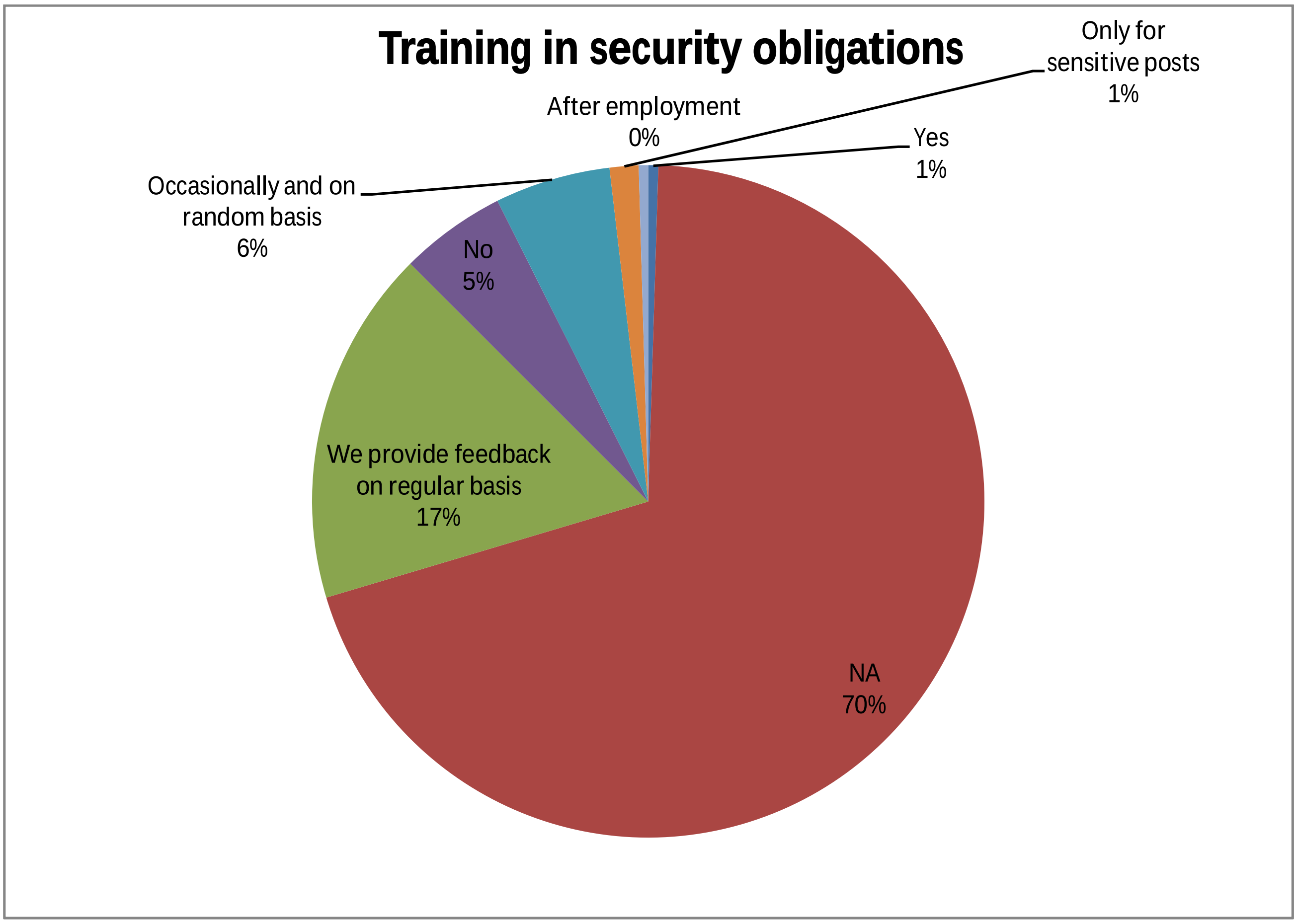


F. Security of the Human Resources

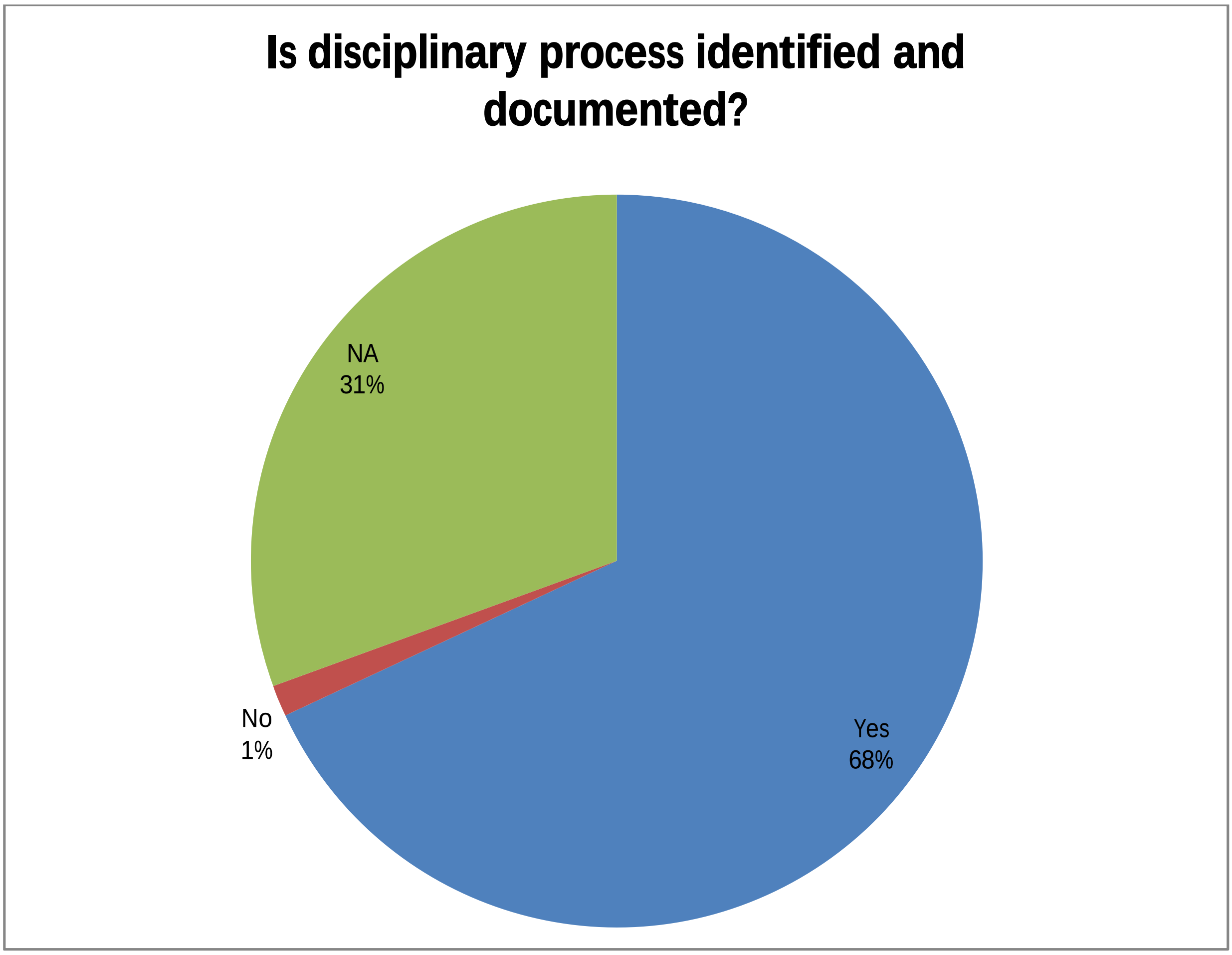
Before Recruitment

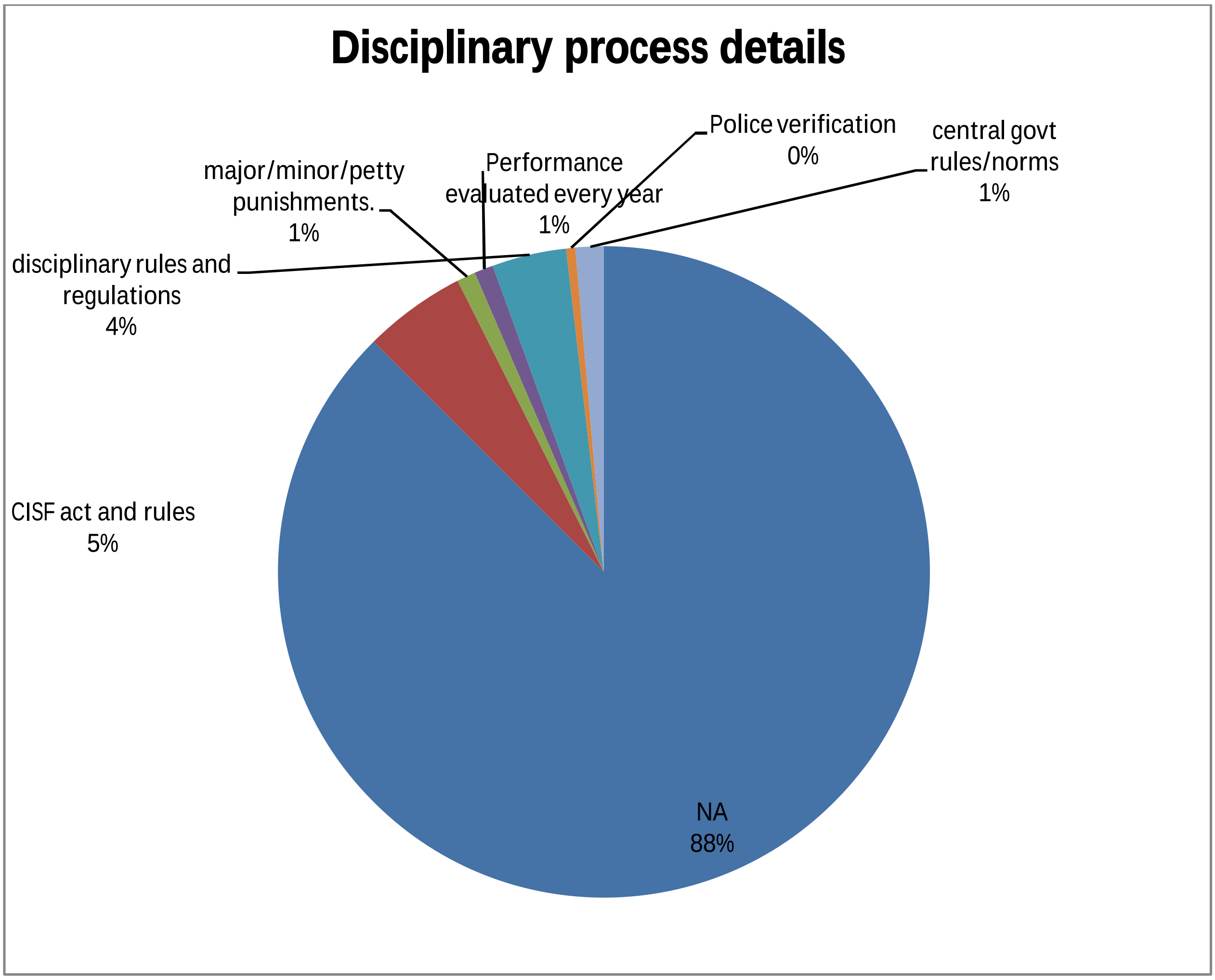
(Most of the respondents didn't answer this section of the questionnaire)



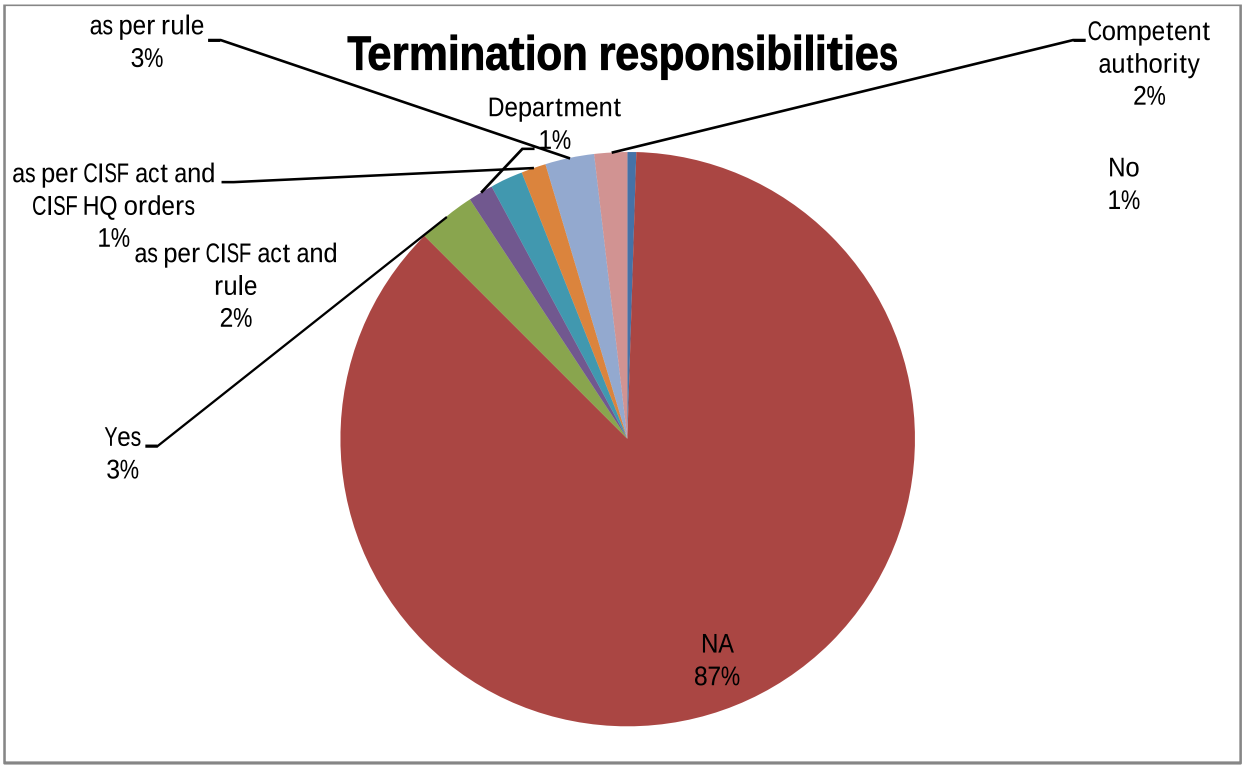

Training in security obligations
Only for sensitive posts 1%
After employment 0%
Yes 1%
Occasionally and on random basis 6%
No 5%
We provide feedback on regular basis 17%
NA 70%

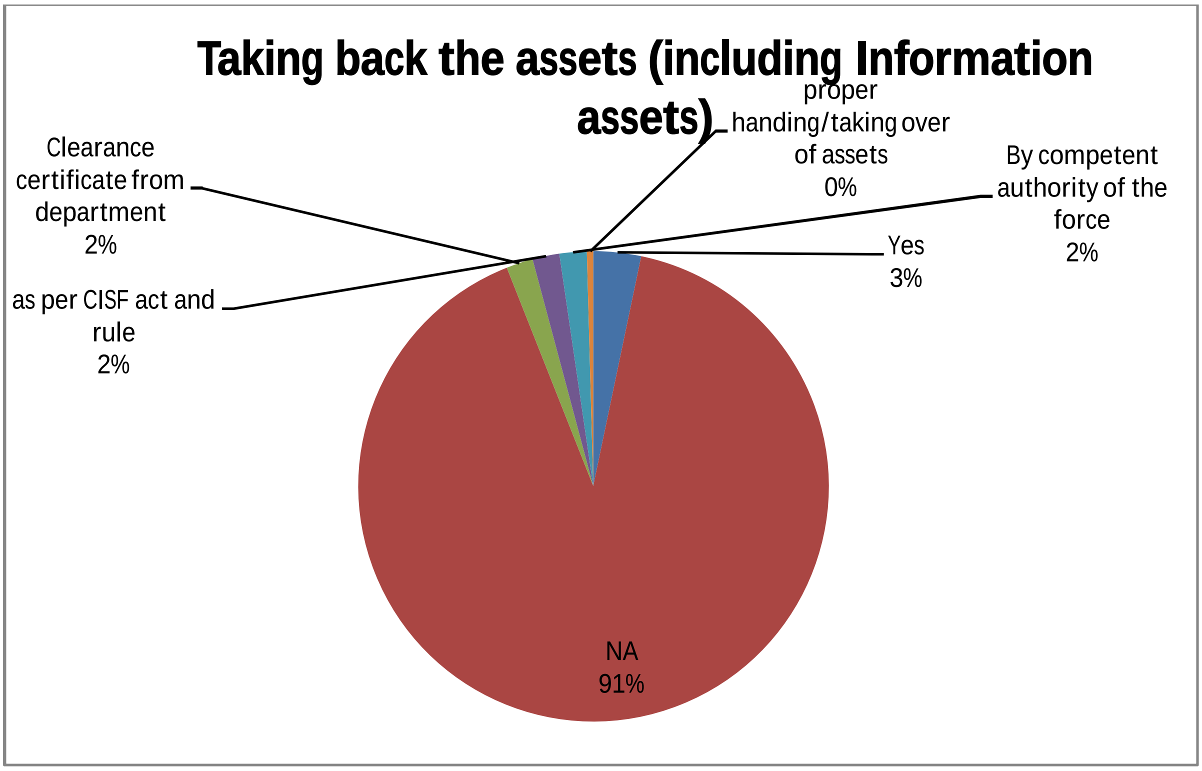
During Employment

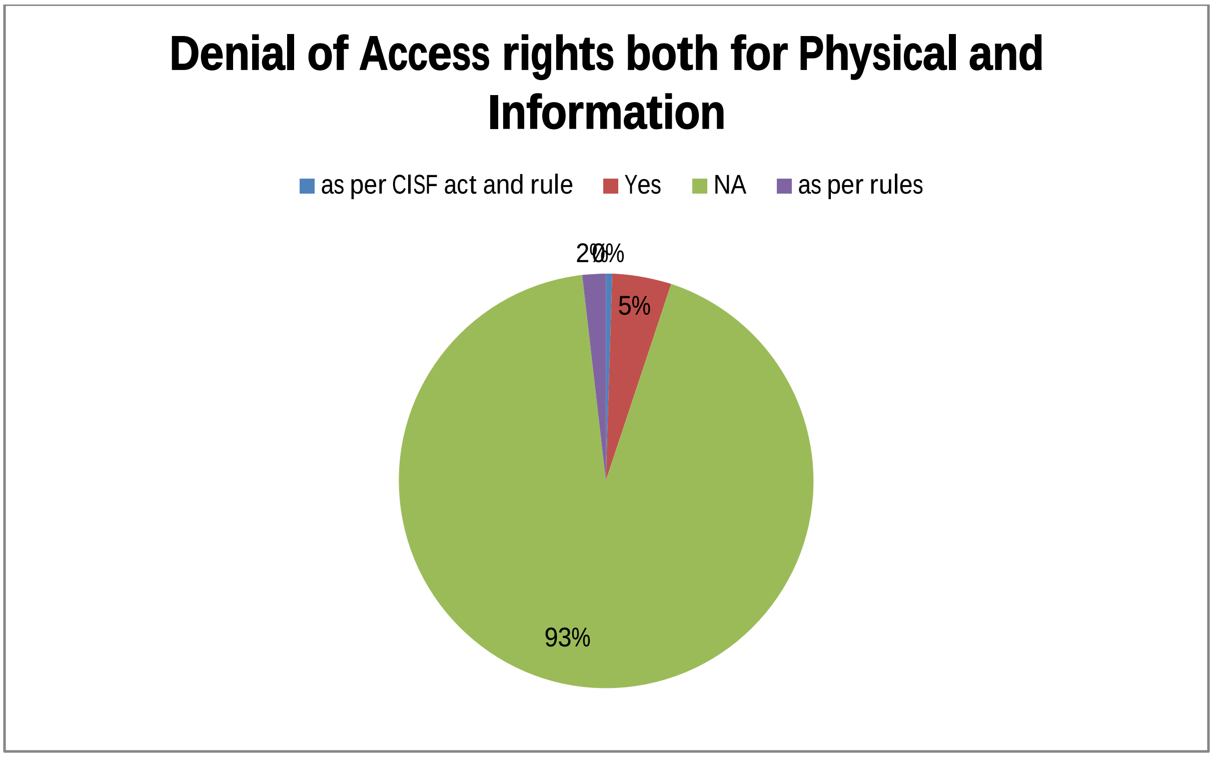


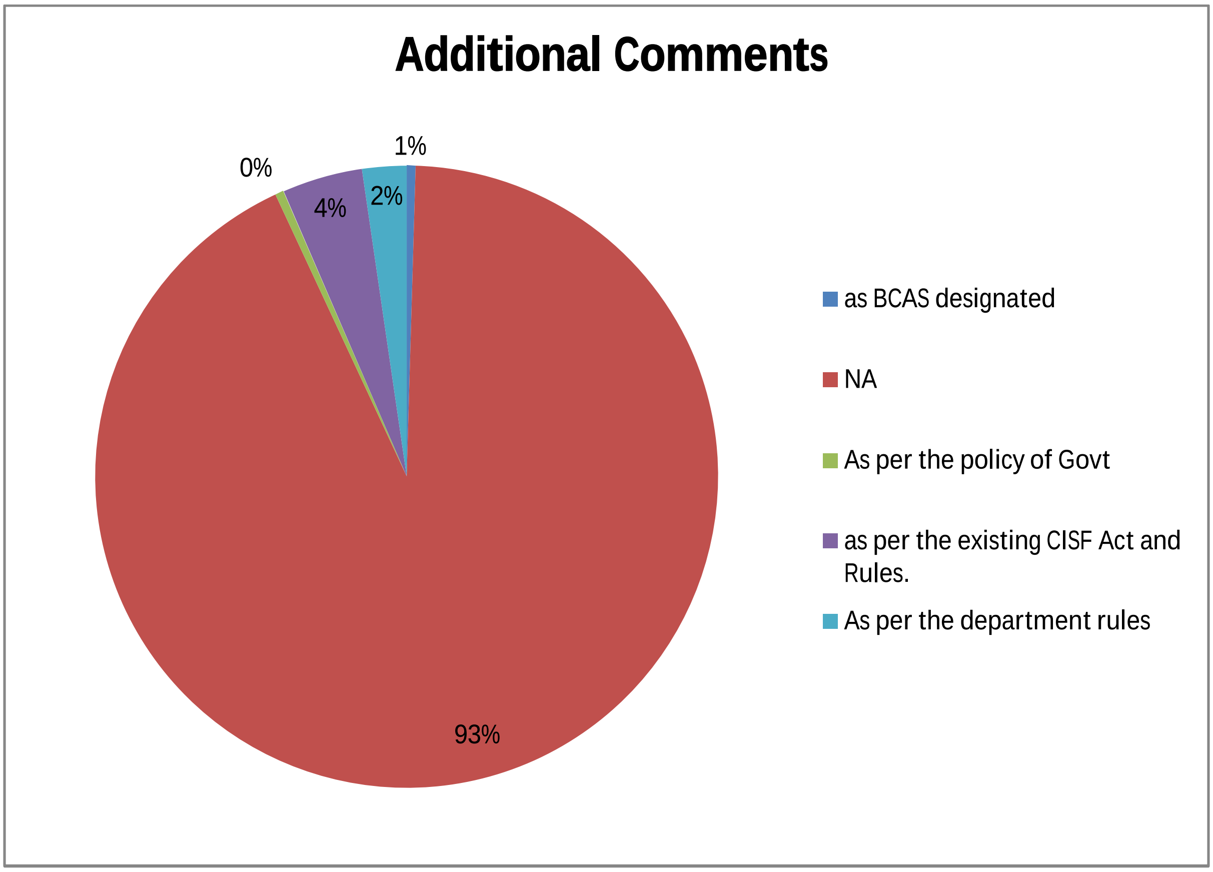

Disciplinary process details
Police verification 0%
central govt rules/norms 1%
major/minor/petty punishments. 1%
Performance evaluated every year 1%
disciplinary rules and regulations 4%
CISF act and rules 5%
NA 88%

Change of Employment or Termination




Taking back the assets (including Information assets)
proper handing/taking over of assets 0%
By competent authority of the force 2%
Yes 3%
Clearance certificate from department 2%
as per CISF act and rule 2%
NA 91%


Denial of Access rights both for Physical and Information
as per CISF act and rule
Yes
NA
as per rules
2%
0%
5%
93%


Additional Comments
1%
0%
4%
2%
93%
as BCAS designated
NA
As per the policy of Govt
as per the existing CISF Act and Rules.
As per the department rules

8. The Private Security Agencies (Regulation) Act, 2005

No. 29 OF 2005, [23rd June, 2005.]

An Act to provide for the regulation of private security agencies and for matters connected therewith or incidental thereto. BE it enacted by Parliament in the Fifty-sixth Year of the Republic of India as follows:-

Short title, extent and commencement

- Short title, extent and commencement.-(1) This Act may be called the Private Security Agencies (Regulation) Act, 2005.
- It extends to the whole of India except the State of Jammu and Kashmir
- It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

Definitions

In this Act, unless the context otherwise requires,

- "Armoured car service" means the service provided by deployment of armed guards along with armoured car and such other related services which may be notified by the Central Government or as the case may be, the State Government from time to time
- "Controlling Authority" means the Controlling Authority appointed under sub-section (1) of section 3
- "Licence" means a licence granted under sub-section (5) of section 7
- "Notification" means a notification published in the Official Gazette
- "Prescribed" means prescribed by rules made under this Act
- "Private security" means security provided by a person, other than a public servant, to protect or guard any person or property or both and includes provision of armoured car service
- "Private security agency" means a person or body of persons other than a government agency, department or organisation engaged in the business of providing private security services including training to private security guards or their supervisor or providing private security guards to any industrial or business undertaking or a company or any other person or property
- "Private security guard" means a person providing private security with or without arms to another person or property or both and includes a supervisor
- "State Government", in relation to a Union territory, includes the Administrator of that Union territory appointed by the President under article 239 of the Constitution.

Appointment of Controlling Authority

The State Government shall, by notification, designate an officer not below the rank of a Joint Secretary in the Home Department of the State or an equivalent officer to be the Controlling Authority for the purposes of this Act.

The State Government may, for efficient discharge of functions by the Controlling Authority, provide it with such other officers and staff as that Government considers necessary.

Persons or Private Security Agency not to engage or provide private security guard without licence

Persons or Private Security Agency not to engage or provide private security guard without licence.-No person shall carry on or commence the business of private security agency, unless he holds a licence issued under this Act:

Provided that the person carrying on the business of private security agency, immediately before the commencement of this Act, may continue to do so for a period of one year from the date of such commencement and if he has made an application for such licence within the said period of one year, till the disposal of such application: Provided further that no private security agency shall provide private security abroad without obtaining permission of the Controlling Authority, which shall consult the Central Government before according such permission.

Eligibility for Licence

Eligibility for licence.-An application for issue of a licence under this Act shall only be considered from a person after due verification of his antecedents..

Persons not Eligible for Licence

A person shall not be considered for issue of a licence under this Act, if he has been

- Convicted of an offence in connection with promotion, formation or management of a company (any fraud or misfeasance committed by him in relation to the company), including an undischarged insolvent
- Convicted by a competent court for an offence, the prescribed punishment for which is imprisonment of not less than two years
- Keeping links with any organisation or association which is banned under any law on account of their activities which pose threat to national security or public order or there is information about such a person indulging in activities which are prejudicial to national security or public order
- Dismissed or removed from Government service on grounds of misconduct or moral turpitude.

A company, firm or an association of persons shall not be considered for issue of a licence under this Act, if, it is not registered in India, or having a proprietor or a majority shareholder, partner or director, who is not a citizen of India.

Application for Grant of Licence

An application for grant of licence to a private security agency shall be made to the Controlling Authority in such form as may be prescribed.

The applicant shall submit an affidavit incorporating the details in relation to the provisions contained in section 6, ensure the availability of the training for its private security guards and supervisors required under sub-section (2) of section 9, fulfilment of conditions under section 11 and of cases registered with police or pending in a court of law involving the applicant.

Every application under sub-section (1) shall be accompanied by a fee of

- Rupees five thousand if the private security agency is operating in one district of a State
- Rupees ten thousand if the agency is operating in more than one but up to five districts of a State
- Rupees twenty-five thousand if it is operating in the whole State

On receipt of an application under sub-section (1), the Controlling Authority may, after making such inquiries as it considers necessary and obtaining no objection certificate from the concerned police authority, by order in writing, either grant a licence or refuse to grant the same within a period of sixty days from the date of receipt of application with complete particulars and the prescribed fee: Provided that no order of refusal shall be made unless

- The applicant has been given a reasonable opportunity of being heard
- The grounds on which licence is refused is mentioned in the order

A licence granted under this section

- Shall be valid for a period of five years unless the same is cancelled under sub-section (1) of section 13
- May be renewed from time to time after the expiry of five years, for a further period of five years on payment of such fee as may be prescribed
- Shall be subject to such conditions as may be prescribed

Renewal of Licence

(1) An application for renewal of licence shall be made to the Controlling Authority, not less than forty-five days before the date of expiry of the period of validity thereof, in such form as may be prescribed and shall be accompanied by the requisite fee and other documents required under sections 6, 7 and 11 of this Act.

(2) The Controlling Authority shall pass an order on application for renewal of licence within thirty days from the date of receipt of application complete in all respects.

(3) On receipt of an application under sub-section (1), the Controlling Authority may, after making such inquiries as he considers necessary and by order in writing, renew the licence or refuse to renew the same: Provided that no order of refusal shall be made except after giving the applicant a reasonable opportunity of being heard.

Conditions for commencement of operation and engagement of supervisors

1) Every private security agency shall, within six months of obtaining the licence, commence its activities.

(2) Every private security agency shall ensure imparting of such training and skills to its private security guards and supervisors as may be prescribed: Provided that the person carrying on the business of private security agency, before the commencement of this Act, shall ensure the required training to its security guards and supervisors within a period of one year from the date of such commencement.

(3) Every private security agency shall, within sixty days from the date of issue of the licence, employ such number of supervisors, as may be prescribed.

(4) A private security agency shall not employ or engage a person as a supervisor unless he fulfils the conditions specified in sub-section (1) of section 10.

(5) While engaging a supervisor of private security guards, every private security agency shall give preference to a person who has experience of serving in the Army, Navy, Air Force or any other Armed forces of the Union or State Police including armed constabularies and Home Guards for a period of not less than three years.

Eligibility to be a Private Security Guard

(1) A private security agency shall not employ or engage any person as a private security guard unless he

a) Is a citizen of India or a citizen of such other country as the Central Government may, by notification in the Official Gazette, specify
b) Has completed eighteen years of age but has not attained the age of sixty-five years
c) Satisfies the agency about his character and antecedents in such manner as may be prescribed
d) Has completed the prescribed security training successfully
e) Fulfils such physical standards as may be prescribed
f) Satisfies such other conditions as may be prescribed

(2) No person who has been convicted by a competent court or who has been dismissed or removed on grounds of misconduct or moral turpitude while serving in any of the armed forces of the Union, State Police Organisations, Central or State Governments or in any private security agency shall be employed or engaged as a private security guard or a supervisor.

(3) Every private security agency may, while employing a person as a private security guard, give preference to a person who has served as a member in one or more of the following, namely:

a) Army
b) Navy
c) Air Force
d) Any other armed forces of the Union
e) Police, including armed constabularies of States
f) Home Guards

Conditions of Licence

(1) The State Government may frame rules to prescribe the conditions on which licence shall be granted under this Act and such conditions shall include requirements as to the training which the licensee is to undergo, details of the person or persons forming the agency, obligation as to the information to be provided from time to time to the Controlling Authority regarding any change in their address, change of management and also about any criminal charge made against them in the course of their performance of duties of the private security agency or as the case may be, a private security guard employed or engaged by them.

(2) The State Government may make provision in the rules to verify about imparting of required training by the private security agency under sub-section (2) of section 9 and to review continuation or otherwise of licence of such private security agency which may not have adhered to the condition of ensuring the required training.

Licence to be Exhibited

12. Licence to be exhibited.-Every private security agency shall exhibit its licence or copy thereof in a conspicuous place of its business.

Cancellation and Suspension of Licence

(1) The Controlling Authority may cancel any licence on any one or more of the following grounds, namely:

a) That the licence has been obtained on misrepresentation or suppression of material facts
b) That the licence holder has used false documents or photographs
c) That the licence holder has violated the provisions of this Act or the rules made there under or any of the conditions of the licence
d) That the licence holder has misused information obtained by him during the discharge of his duties as the private security agency to any industrial or business undertaking or a company or any other person
e) That the licence holder by using any letter-head, advertisement or any other printed matter or in any other manner represented that the private security agency is an

instrumentality of the Government or such agency is or has been using a name different from that for which licence has been granted

f) That the licence holder is or has been impersonating or permitting or aiding or abetting anybody to impersonate as a public servant

g) That the private security agency had failed to commence its activities or to engage a supervisor within the specified time period

h) That the licence holder is or has wilfully failed or refused to render the services agreed to any person

i) That the licence holder has done any act which is in violation of a court order or an order of a lawful authority or is or has been advising, encouraging or assisting any person to violate any such order

j) That the licence holder has violated the provisions of the Acts given in the Schedule which may be modified by the Central Government, by notification in the Official Gazette

k) That there have been repeated instances when the private security guard or guards provided by the private security agency

   i. Failed to provide private security or were guilty of gross negligence in not providing such security

   ii. Committed a breach of trust or misappropriated the property or a part thereof which they were supposed to protect

   iii. Were found habitually drunk or indisciplined

   iv. Were found to be involved in committing crimes

   v. Had connived or abetted a crime against the person or property placed under their charge

   vi. The licence holder has done any act which poses a threat to national security, or did not provide assistance to the police or other authority in the discharge of its duties or acted in a manner prejudicial to national security or public order or law and order.

(2) Where the Controlling Authority, for reasons to be recorded in writing, is satisfied that pending the question of cancelling of licence on any of the grounds mentioned in sub-section (1), it is necessary to do so, that Controlling Authority may, by order in writing, suspend the operation of the licence for such period not exceeding thirty days as may be specified in the order and require the licence holder to show cause, within fifteen days from the date of issue of such order, as to why the suspension of the licence should not be extended till the determination of the question of cancellation.

(3) Every order of suspending or cancelling of a licence shall be in writing and shall specify the reasons for such suspension or cancellation and a copy thereof shall be communicated to the person affected.

(4) No order of cancellation of licence under sub-section (1) shall be made unless the person concerned has been given a reasonable opportunity of being heard.

Appeals

(1) Any person aggrieved by an order of the Controlling Authority refusing the licence under sub-section (4) of section 7 or renewal under sub-section (3) of section 8 or order of suspension of licence under sub-section (2) of section 13 or cancellation of licence under sub-section (1) of that section, may prefer an appeal against that order to the Home Secretary of the State Government within a period of sixty days of the date of such order: Provided that an appeal may be admitted after the expiry of the said period of sixty days if the appellant satisfies the State Government that he has sufficient cause for not preferring the appeal within that period.

(2) Every appeal under sub-section (1) shall be made in such form as may be prescribed and shall be accompanied by a copy of the order appealed against.

(3) Before disposing of an appeal, the State Government shall give the appellant a reasonable opportunity of being heard.

Register to be maintained by a Private Security Agency

(1) Every private security agency shall maintain a register containing- (a) the names and addresses of the persons managing the private security agency; (b) the names, addresses, photographs and salaries of the private security guards and supervisors under its control; (c) the names and addresses of the persons whom it had provided private security guards or services; and (d) such other particulars as may be prescribed.

(2) The Controlling Authority may call for such information as it considers necessary from any private security agency, supervisor or private security guard to ensure due compliance of the Act.

Inspection of Licence

The Controlling Authority or any other officer authorised by it in this behalf may at any reasonable time, enter the premises of the private security agency and inspect and examine the place of business, the records, accounts and other documents connected with the licence and may take copy of any document.

Issue of Photo Identity Card

(1) Every private security guard shall be issued a photo identity card, by the private security agency employing or engaging the guard.

(2) The photo identity card under sub-section (1) shall be issued in such form as may be prescribed. (3) Every private security guard or supervisor shall carry on his person the photo identity card issued under sub-section (1) and shall produce it on demand for inspection by the Controlling Authority or any other officer authorised by it in this behalf.

Disclosure of Information to Unauthorized Person

(1) Any person who may be or has been employed or engaged as a private security guard by the private security agency shall not divulge to anyone other than the employer, or in such manner and to such person as the employer directs, any information acquired by him during such employment with respect to the work which he has been assigned by such employer, except such disclosure as may be required under this Act or in connection with any inquiry or investigation by the police or as may be required by an authority or process of law.

(2) All private security guards of a private security agency shall render necessary assistance to the police or to such authority in the process of any investigation pertaining to the activities of that agency.

(3) If violation of any law is noticed by any private security guard during the course of discharge of his duties, he shall bring it to the notice of his superior, who in turn shall inform the police either through his employer or agency or on his own.

Delegation

The State Government may, by notification, direct that any power or function (except the powers to make rules under section 25 (a) which may be exercised or performed by it, or (b) which may be exercised or performed by the Controlling Authority, under this Act, may, in relation to such matter and subject to such conditions, if any, as may be specified in the notification, be also exercised or performed by such officer or authority subordinate to the Government or officer subordinate to the Controlling Authority, as may be specified in such notification.

Punishment for Contravention of Certain Provisions

(1) Any person who contravenes the provisions of section 4 shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to twenty-five thousand rupees, or with both.

(2) Any person or private security agency who contravenes the provisions of sections 9, 10 and 12 of the Act, shall be punishable with a fine which may extend to twenty-five thousand rupees, in addition to suspension or cancellation of the licence.

Penalty for unauthorized use of certain uniforms

If any private security guard or supervisor wears the uniform of the Army, Air force, Navy or any other armed forces of the Union or Police or any dress having the appearance or bearing any of the distinctive marks of that uniform, he and the proprietor of the private security agency shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to five thousand rupees, or with both.

Offences by Companies

(1) Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the

company for the conduct of the business of the company as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to, any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly. Explanation.-For the purposes of this section- (a) "company" means anybody corporate and includes a firm or other association of individuals; and (b) "director", in relation to a firm, means a partner in the firm.

Indemnity

No suit, prosecution or other legal proceeding shall lie against the Controlling authority or any other officer authorised by it in respect of anything in good faith done or intended to be done under this Act.

Framing of model rules for adoption by States

The Central Government may frame model rules in respect of all or any of the matters with respect to which the State Government may make rules under this Act, and where any such model rules have been framed the State Government shall, while making any rules in respect of that matter under section 25, so far as is practicable, conform to such model rules.

Power of State Government to make rules

(1) The State Government may, by notification, make rules for carrying out the provisions of this Act. (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

a) The procedure for verification of character and antecedents under clause (c) of sub-section (1) of section 10; the type of training under clause (d) of sub-section (1) of section 10; the physical standard under clause (e) of sub-section (1) of section 10; and other conditions under clause (f) of sub-section (1) of section 10
b) The number of supervisors to be employed under sub-section (3) of section 9
c) The form of an application for grant of licence under sub-section (1) of section 7;
d) The form in which the licence to be granted under sub-section (4) of section 7 and conditions subject to which such licence to be granted under section 11
e) The form of an application for renewal of licence under sub-section (1) of section 8
f) The form under sub-section (2) of section 14 for preferring an appeal

g) Particulars to be maintained in a register under sub-section (1) of section 15
h) The form in which photo identity card under sub-section (2) of section 17 be issued
i) Any other matter which is required to be, or may be, prescribed

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such
Legislature consists of one House, before that House.

(4) In respect of Union territories, every rule made to carry out the provisions of the Act shall be laid before each House of Parliament and where there exists a Legislative Assembly, before that Assembly.

9. Model Rules of Gujarat under the PASARA Act 2005

These rules were framed in the year 2007 and are in force. Only 9 states in the country have formulated rules.

Some of the provisions of the rules are as follows:

- Private Security Agencies Regulation rules 2007
- Verification of the antecedents of the applicant (Rule 3)
- Verification of character and antecedents of security guard and supervisor (Rule 4)
- All security guards to undergo training
- Minimum of 160 hours spread over 20 working days
- 100 hours of classroom and 60 hours of outdoor training
- Syllabus to be drafted which should include PT, security, fire fighting, crowd control, identification of papers, first-aid, defensive driving, law, badges of rank, use of security equipment and devices
- One supervisor for every fifteen guards (Rule 7)
- Manner of making application for grant of license (Rule 8)
- Grant of license by the controlling authority (Rule 9)
- Conditions for grant of license and renewal (Rule 10,11,12)
- Photo ID card must for Security Guards
- Other conditions (Rule 16)

10. International Code of Conduct for Private Security Service Providers

9 November 2010

A. Preamble

Private Security Companies and other Private Security Service Providers (collectively "PSCs") play an important role in protecting state and non-state clients engaged in relief, recovery, and reconstruction efforts, commercial business operations, diplomacy and military activity. In providing these services, the activities of PSCs can have potentially positive and negative consequences for their clients, the local population in the area of operation, the general security environment, the enjoyment of human rights and the rule of law.

The *Montreux Document On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict* recognizes that well-established rules of international law apply to States in their relations with private security service providers and provides for good practices relating to PSCs. The "Respect, Protect, Remedy" framework developed by the Special Representative of the United Nations (UN) Secretary- General on Business and Human Rights, and welcomed by the UN Human Rights Council, entails acting with due diligence to avoid infringing the rights of others.

Building on these foundations, the Signatory Companies to this International Code of Conduct for Private Security Service Providers (the "Code") endorse the principles of the Montreux Document and the aforementioned "Respect, Protect, Remedy" framework as they apply to PSCs. In so doing, the Signatory Companies commit to the responsible provision of Security Services so as to support the rule of law, respect the human rights of all persons, and protect the interests of their clients.

The Signatory Companies affirm that they have a responsibility to respect the human rights of, and fulfill humanitarian responsibilities towards, all those affected by their business activities, including Personnel, Clients, suppliers, shareholders, and the population of the area in which services are provided. The Signatory Companies also recognize the importance of respecting the various cultures encountered in their work, as well as the individuals they come into contact with as a result of those activities.

The purpose of this Code is to set forth a commonly-agreed set of principles for PSCs and to establish a foundation to translate those principles into related standards as well as governance and oversight mechanisms.

Signatory Companies commit to the following, as set forth in this Code:

- To operate in accordance with this Code
- To operate in accordance with applicable laws and regulations, and in accordance with relevant corporate standards of business conduct
- To operate in a manner that recognizes and supports the rule of law; respects human rights, and protects the interests of their clients
- To take steps to establish and maintain an effective internal governance framework in order to deter, monitor, report, and effectively address adverse impacts on human rights
- To provide a means for responding to and resolving allegations of activity that violates any applicable national or international law or this Code
- To cooperate in good faith with national and international authorities exercising proper jurisdiction, in particular with regard to national and international investigations of violations of national and international criminal law, of violations of international humanitarian law, or of human rights abuses.

Those establishing this Code recognize that this Code acts as a founding instrument for a broader initiative to create better governance, compliance and accountability. Recognizing that further effort is necessary to implement effectively the principles of this Code, Signatory Companies accordingly commit to work with states, other Signatory Companies, Clients and other relevant stakeholders after initial endorsement of this Code to, within 18 months:

- Establish objective and measurable standards for providing Security Services based upon this Code, with the objective of realizing common and internationally-recognized operational and business practice standards
- Establish external independent mechanisms for effective governance and oversight, which will include Certification of Signatory Companies' compliance with the Code's principles and the standards derived from the Code, beginning with adequate policies and procedures, Auditing and Monitoring of their work in the field, including Reporting, and execution of a mechanism to address alleged violations of the Code's principles or the standards derived from the Code; and thereafter to consider the development of additional principles and standards for related services, such as training of external forces, the provision of maritime security services and the participation in operations related to detainees and other protected persons.

Signature of this Code is the first step in a process towards full compliance. Signatory Companies need to: (1) establish and/or demonstrate internal processes to meet the requirements of the Code's principles and the standards derived from the Code; and (2) once the governance and oversight mechanism is established, become certified by and submit to ongoing independent Auditing and verification by that mechanism. Signatory Companies undertake to be transparent regarding their progress towards implementing the

Code's principles and the standards derived from the Code. Companies will not claim they are certified under this Code until Certification has been granted by the governance and oversight mechanism as outlined below.

B. Definitions

These definitions are only intended to apply exclusively in the context of this Code.

Auditing – a process through which independent auditors, accredited by the governance and oversight mechanism, conduct on-site audits, including in the field, on a periodic basis, gathering data to be reported to the governance and oversight mechanism which will in turn verify whether a Company is meeting requirements and if not, what remediation may be required.

Certification – a process through which the governance and oversight mechanism will certify that a Company's systems and policies meet the Code's principles and the standards derived from the Code and that a Company is undergoing Monitoring, Auditing, and verification, including in the field, by the governance and oversight mechanism. Certification is one element of a larger effort needed to ensure the credibility of any Implementation and oversight initiative.

Client – an entity that hires, has formerly hired, or intends to hire a PSC to perform Security Services on its behalf, including, as appropriate, where such a PSC subcontracts with another Company.

Company – any kind of business entity or form, such as a sole proprietorship, partnership, company (whether public or private), or corporation, and "Companies" shall be interpreted accordingly.

Competent Authority – any state or intergovernmental organization which has jurisdiction over the activities and/or persons in question and "Competent Authorities" shall be interpreted accordingly.

Complex Environments – any areas experiencing or recovering from unrest or instability, whether due to natural disasters or armed conflicts, where the rule of law has been substantially undermined, and in which the capacity of the state authority to handle the situation is diminished, limited, or non-existent. Implementation – the introduction of policy, governance and oversight mechanisms and training of Personnel and/or subcontractors by Signatory Companies, necessary to demonstrate compliance with the Code's principles and the standards derived from this Code.

Monitoring – a process for gathering data on whether Company Personnel, or subcontractors, are operating in compliance with the Code's principles and standards derived from this Code.

Personnel – persons working for a PSC, whether as employees or under a contract, including its staff, managers and directors. For the avoidance of doubt, persons are considered to be personnel if they are connected to a PSC through an employment contract (fixed term, permanent or open-ended) or a contract of assignment (whether renewable or not), or if they are independent contractors, or temporary workers and/or interns (whether paid or unpaid), regardless of the specific designation used by the Company concerned.

Private Security Companies and Private Security Service Providers (collectively "PSCs") – any Company (as defined in this Code) whose business activities include the provision of Security Services either on its own behalf or on behalf of another, irrespective of how such Company describes itself.

Reporting – a process covered by necessary confidentiality and nondisclosure arrangements through which companies will submit to a governance and oversight mechanism a written assessment of their performance pursuant to a transparent set of criteria established by the mechanism.

Security Services – guarding and protection of persons and objects, such as convoys, facilities, designated sites, property or other places (whether armed or unarmed), or any other activity for which the Personnel of Companies are required to carry or operate a weapon in the performance of their duties.

Signatory Companies – are PSCs that have signed and agreed to operate in compliance with the Code's principles and the standards derived from the Code and "Signatory Company" shall be interpreted accordingly.

C. Implementation

In recognition of the additional steps to be taken to support the Implementation of this Code – in particular the development of standards based on the Code ("standards") and an independent governance and oversight mechanism ("the mechanism") as outlined in the Preamble – Signatory Companies intend to, along with other interested stakeholders, convene regularly to review progress toward those steps.

Upon signature of the Code, Signatory Companies and other stakeholders will undertake to work with national standards bodies as appropriate to develop standards, with the intent that any national standards would eventually be harmonized in an international set of standards based on the Code.

Upon signature of the Code, Signatory Companies and other stakeholders will appoint a multi-stakeholder steering committee of 6-9 members who will function as a "temporary board". This steering committee will be responsible for developing and documenting the initial arrangements for the independent governance and oversight mechanism, including by-laws or a charter which will outline mandate and governing policies for the mechanism. The Steering Committee will endeavour to complete a work plan for constituting the mechanism before the end of March 2011, and further to develop the bylaws/charter by the end of July 2011 and an operational plan before the end of November 2011.

After the independent governance and oversight mechanism has been constituted (by the adoption of bylaws/charter), the governance and oversight mechanism shall accept responsibility for maintenance and administration of the Code, and shall determine whether and how it is appropriate for the mechanism and standards to be reflected in the text of the Code itself.

D. General Provisions

This Code articulates principles applicable to the actions of Signatory Companies while performing Security Services in Complex Environments.

This Code complements and does not replace the control exercised by Competent Authorities, and does not limit or alter applicable international law or relevant national law. The Code itself creates no legal obligations and no legal liabilities on the Signatory Companies, beyond those which already exist under national or international law. Nothing in this Code shall be interpreted as limiting or prejudicing in any way existing or developing rules of international law.

This Code may be modified in accordance with procedures to be established by the governance and oversight mechanism.

E. General Commitments

Signatory Companies agree to operate in accordance with the principles contained in this Code. Signatory Companies will require that their Personnel, and all subcontractors or other parties carrying out Security Services under Signatory Company contracts, operate in accordance with the principles contained in this Code.

Signatory Companies will implement appropriate policies and oversight with the intent that the actions of their Personnel comply at all times with the principles contained herein.

Signatory Companies will make compliance with this Code an integral part of contractual agreements with Personnel and subcontractors or other parties carrying out Security Services under their contracts.

Signatory Companies will adhere to this Code, even when the Code is not included in a contractual agreement with a Client.

Signatory Companies will not knowingly enter into contracts where performance would directly and materially conflict with the principles of this Code, applicable national or international law, or applicable local, regional and international human rights law, and are not excused by any contractual obligation from complying with this Code. To the maximum extent possible, Signatory Companies will interpret and perform contracts in a manner that is consistent with this Code.

Signatory Companies will comply, and will require their Personnel to comply, with applicable law which may include international humanitarian law, and human rights law as imposed upon them by applicable national law, as well as all other applicable international and national law. Signatory Companies will exercise due diligence to ensure compliance with the law and with the principles contained in this Code, and will respect the human rights of persons they come into contact with, including, the rights to freedom of expression, association, and peaceful assembly and against arbitrary or unlawful interference with privacy or deprivation of property.

Signatory Companies agree not to contract with, support or service any government, person, or entity in a manner that would be contrary to United Nations Security Council sanctions. Signatory Companies will not, and will require that their Personnel do not, participate in, encourage, or seek to benefit from any national or international crimes including but not limited to war crimes, crimes against humanity, genocide, torture, enforced disappearance, forced or compulsory labour, hostage-taking, sexual or gender-based violence, human trafficking, the trafficking of weapons or drugs, child labour or extrajudicial, summary or arbitrary executions.

Signatory Companies will not, and will require that their Personnel do not, invoke contractual obligations, superior orders or exceptional circumstances such as an armed conflict or an imminent armed conflict, a threat to national or international security, internal political instability, or any other public emergency, as a justification for engaging in any of the conduct identified in paragraph 22 of this Code.

Signatory Companies will report, and will require their Personnel to report, known or reasonable suspicion of the commission of any of the acts identified in paragraph 22 of this Code to the Client and one or more of the following: the Competent Authorities in the country where the act took place, the country of nationality of the victim, or the country of nationality of the perpetrator.

Signatory Companies will take reasonable steps to ensure that the goods and services they provide are not used to violate human rights law or international humanitarian law, and such goods and services are not derived from such violations.

Signatory Companies will not, and will require that their Personnel do not, consistent with applicable national and international law, promise, offer, or give to any public official, directly or indirectly, anything of value for the public official himself or herself or another person or entity, in order that the public official act or refrain from acting in the exercise of his or her official duties if such inducement is illegal. Signatory Companies will not, and will require their Personnel do not, solicit or accept, directly or indirectly, anything of value in exchange for not complying with national and international law and/or standards, or with the principles contained within this Code.

Signatory Companies are responsible for establishing a corporate culture that promotes awareness of and adherence by all Personnel to the principles of this Code. Signatory Companies will require their Personnel to comply with this Code, which will include providing sufficient training to ensure Personnel are capable of doing so.

F. Specific Principles Regarding the Conduct of Personnel

General Conduct

Signatory Companies will, and will require their Personnel to, treat all persons humanely and with respect for their dignity and privacy and will report any breach of this Code.

Rules for the Use of Force

Signatory Companies will adopt Rules for the Use of Force consistent with applicable law and the minimum requirements contained in the section on Use of Force in this Code and agree those rules with the Client.

Use of Force

Signatory Companies will require their Personnel to take all reasonable steps to avoid the use of force. If force is used, it shall be in a manner consistent with applicable law. In no case shall the use of force exceed what is strictly necessary, and should be proportionate to the threat and appropriate to the situation.

Signatory Companies will require that their Personnel not use firearms against persons except in self-defense or defense of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life.

To the extent that Personnel are formally authorized to assist in the exercise of a state's law enforcement authority, Signatory Companies will require that their use of force or weapons will comply with all national and international obligations applicable to regular law enforcement officials of that state and, as a minimum, with the standards expressed in the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990).

Detention

Signatory Companies will only, and will require their Personnel will only, guard, transport, or question detainees if: (a) the Company has been specifically contracted to do so by a state; and (b) its Personnel are trained in the applicable national and international law. Signatory Companies will, and will require that their Personnel, treat all detained persons humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Apprehending Persons

Signatory Companies will, and will require their Personnel to, not take or hold any persons except when apprehending persons to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity. Any such apprehension must be consistent with applicable national or international law and be reported to the Client without delay. Signatory Companies will, and will require that their Personnel to, treat all apprehended persons humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Prohibition of Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment

Signatory Companies will not, and will require that their Personnel not, engage in torture or other cruel, inhuman or degrading treatment or punishment. For the avoidance of doubt, torture and other cruel, inhuman or degrading treatment or punishment, as referred to here, includes conduct by a private entity which would constitute torture or other cruel, inhuman or degrading treatment or punishment if committed by a public official.

Contractual obligations, superior orders or exceptional circumstances such as an armed conflict or an imminent armed conflict, a threat to national or international security, internal political instability, or any other public emergency, can never be a justification for engaging in torture or other cruel, inhuman or degrading treatment or punishment.

Signatory Companies will, and will require that their Personnel, report any acts of torture or other cruel, inhuman or degrading treatment or punishment, known to them, or of which they have reasonable suspicion. Such reports will be made to the Client and one or more of the following: the competent authorities in the country where the acts took place, the country of nationality of the victim, or the country of nationality of the perpetrator.

Sexual Exploitation and Abuse or Gender-Based Violence

Signatory Companies will not benefit from, nor allow their Personnel to engage in or benefit from, sexual exploitation (including, for these purposes, prostitution) and abuse or gender-based violence or crimes, either within the Company or externally, including rape, sexual harassment, or any other form of sexual abuse or violence. Signatory Companies will, and will require their Personnel to, remain vigilant for all instances of sexual or gender-based violence and, where discovered, report such instances to competent authorities.

Human Trafficking

Signatory Companies will not, and will require their Personnel not to, engage in trafficking in persons. Signatory Companies will, and will require their Personnel to, remain vigilant for all instances of trafficking in persons and, where discovered, report such instances to Competent Authorities. For the purposes of this Code, human trafficking is the recruitment, harbouring, transportation, provision, or obtaining of a person for (1) a commercial sex act induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or (2) labour or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, debt bondage, or slavery.

Prohibition of Slavery and Forced Labour

Signatory Companies will not use slavery, forced or compulsory labour, or be complicit in any other entity's use of such labour.

Prohibition on the Worst Forms of Child Labour

Signatory Companies will respect the rights of children (anyone under the age of 18) to be protected from the worst forms of child labour, including: a) all forms of slavery or practices similar to slavery, such as the sale and trafficking of children, debt bondage and serfdom and forced or compulsory labour, including forced or compulsory recruitment of children for use in provision of armed services; b) the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances; c) the use, procuring or offering of a child for illicit activities, in particular for the production and trafficking of drugs; d) work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children. Signatory Companies will, and will require their Personnel to, report any instances of the activities referenced above that they know of, or have reasonable suspicion of, to Competent Authorities.

Discrimination

Signatory Companies will not, and will require that their Personnel do not, discriminate on grounds of race, colour, sex, religion, social origin, social status, indigenous status, disability, or sexual orientation when hiring Personnel and will select Personnel on the basis of the inherent requirements of the contract.

Identification and Registering

Signatory Companies, to the extent consistent with reasonable security requirements and the safety of civilians, their Personnel and Clients, will: a) require all Personnel to be individually identifiable whenever they are carrying out activities in discharge of their contractual responsibilities; b) ensure that their vehicles are registered and licensed with the relevant national authorities whenever they are carrying out activities in discharge of their contractual responsibilities; and c) will ensure that all hazardous materials are registered and licensed with the relevant national authorities.

G. Specific Commitments Regarding Management and Governance

Incorporation of the Code into Company Policies

Signatory Companies will incorporate this Code into Company policies and internal control and compliance systems and integrate it into all relevant elements of their operations.

Selection and Vetting of Personnel

Signatory Companies will exercise due diligence in the selection of Personnel, including verifiable vetting and ongoing performance review of their Personnel. Signatory Companies will only hire individuals with the requisite qualifications as defined by the applicable contract, applicable national law and industry standards, and the principles contained in this Code.

Signatory Companies will not hire individuals under the age of 18 years to carry out Security Services.

Signatory Companies will assess and ensure the continued ability of Personnel to perform their duties in accordance with the principles of this Code and will regularly evaluate Personnel to ensure that they meet appropriate physical and mental fitness standards to perform their contracted duties.

Signatory Companies will establish and maintain internal policies and procedures to determine the suitability of applicants, or Personnel, to carry weapons as part of their duties. At a minimum, this will include checks that they have not: a) been convicted of a crime that would indicate that the individual lacks the character and fitness to perform security services pursuant to the principles of

this Code; b) been dishonorably discharged; c) had other employment or engagement contracts terminated for documented violations of one or more of the principles contained in this Code; or d) had a history of other conduct that, according to an objectively reasonable standard, brings into question their fitness to carry a weapon. For the purposes of this paragraph, disqualifying crimes may include, but are not limited to, battery, murder, arson, fraud, rape, sexual abuse, organized crime, bribery, corruption, perjury, torture, kidnapping, drug trafficking or trafficking in persons. This provision shall not override any law restricting whether a crime may be considered in evaluating an applicant. Nothing in this section would prohibit a Company from utilizing more stringent criteria.

Signatory Companies will require all applicants to authorize access to prior employment records and available Government records as a condition for employment or engagement. This includes records relating to posts held with military, police or public or Private Security Providers. Moreover, Signatory Companies will, consistent with applicable national law, require all Personnel to agree to participate in internal investigations and disciplinary procedures as well as in any public investigations conducted by competent authorities, except where prohibited by law.

Selection and Vetting of Subcontractors

Signatory Companies will exercise due diligence in the selection, vetting and ongoing performance review of all subcontractors performing Security Services.

In accordance with principle 13 of this Code, Signatory Companies will require that their Personnel and all subcontractors and other parties carrying out Security Services under the contract, operate in accordance with the principles contained in this Code and the standards derived from the Code. If a Company contracts with an individual or any other group or entity to perform Security Services, and that individual or group is not able to fulfil the selection, vetting and training principles contained in this Code and the standards derived from the Code, the contracting Company will take reasonable and appropriate steps to ensure that all selection, vetting and training of subcontractor’s Personnel is conducted in accordance with the principles contained in this Code and the standards derived from the Code.

Company Policies and Personnel Contracts

Signatory Companies will ensure that their policies on the nature and scope of services they provide, on hiring of Personnel and other relevant Personnel reference materials such as Personnel contracts include appropriate incorporation of this Code and relevant and applicable labour laws. Contract terms and conditions will be clearly communicated and available in a written form to all Personnel in a format and language that is accessible to them.

Signatory Companies will keep employment and service records and reports on all past and present personnel for a period of 7 (seven) years. Signatory Companies will require all

Personnel to authorize the access to, and retention of, employment records and available Government records, except where prohibited by law. Such records will be made available to any compliance mechanism established pursuant to this Code or Competent Authority on request, except where prohibited by law.

Signatory Companies will only hold passports, other travel documents, or other identification documents of their Personnel for the shortest period of time reasonable for administrative processing or other legitimate purposes. This paragraph does not prevent a Company from co-operating with law enforcement authorities in the event that a member of their Personnel is under investigation.

Training of Personnel

Signatory Companies will ensure that all Personnel performing Security Services receive initial and recurrent professional training and are also fully aware of this Code and all applicable international and relevant national laws, including those pertaining to international human rights, international humanitarian law, international criminal law and other relevant criminal law. Signatory Companies will maintain records adequate to demonstrate attendance and results from all professional training sessions, including from practical exercises.

Management of Weapons

Signatory Companies will acquire and maintain authorizations for the possession and use of any weapons and ammunition required by applicable law.

Signatory Companies will neither, and will require that their Personnel do not, possess nor use weapons or ammunition which are illegal under any applicable law. Signatory Companies will not, and will require that their Personnel not, engage in any illegal weapons transfers and will conduct any weapons transactions in accordance with applicable laws and UN Security Council requirements, including sanctions. Weapons and ammunition will not be altered in any way that contravenes applicable national or international law.

Signatory Company policies or procedures for management of weapons and ammunitions should include:

- Secure storage;
- Controls over their issue;
- Records regarding to whom and when weapons are issued;
- Identification and accounting of all ammunition; and
- Verifiable and proper disposal.

Weapons Training

Signatory Companies will require that:

- Personnel who are to carry weapons will be granted authorization to do so only on completion or verification of appropriate training with regard to the type and model of weapon they will carry. Personnel will not operate with a weapon until they have successfully completed weapon-specific training.
- Personnel carrying weapons must receive regular, verifiable and recurrent training specific to the weapons they carry and rules for the use of force.
- Personnel carrying weapons must receive appropriate training in regard to rules on the use of force. This training may be based on a variety of relevant standards, but should be based at a minimum on the principles contained in this Code and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990), and national laws or regulations in effect in the area duties will be performed.

Management of Material of War

Signatory Companies will, and will require that their Personnel to, acquire and maintain all authorizations for the possession and use of any materiel of war, e.g. hazardous materials and munitions, as required by applicable law.

Signatory Companies will neither, and will require that their Personnel will neither, possess nor use any materiel of war, e.g. hazardous materials and munitions, which are illegal under any applicable law. Signatory Companies will not, and will require that their Personnel not engage in any illegal material transfers and will conduct any materiel of war transactions in accordance with applicable laws and UN Security Council requirements, including sanctions.

Signatory Company policies or procedures for management of materiel of war, e.g. hazardous materials and munitions, should include:

- Secure storage
- Controls over their issue
- Records regarding to whom and when materials are issued
- Proper disposal procedures

Incident Reporting

Signatory Companies will prepare an incident report documenting any incident involving its Personnel that involves the use of any weapon, which includes the firing of weapons under any circumstance (except authorized training), any escalation of force, damage to equipment or injury to persons, attacks, criminal acts, traffic accidents, incidents involving other security forces, or such reporting as otherwise required by the Client, and will conduct an internal inquiry in order to determine the following:

- Time and location of the incident
- Identity and nationality of any persons involved including their addresses and other contact details

- Injuries/damage sustained
- Circumstances leading up to the incident
- Any measures taken by the signatory company in response to it

Upon completion of the inquiry, the signatory company will produce in writing an incident report including the above information, copies of which will be provided to the client and, to the extent required by law, to the competent authorities.

Safe and Healthy Working Environment

Signatory Companies will strive to provide a safe and healthy working environment, recognizing the possible inherent dangers and limitations presented by the local environment. Signatory Companies will ensure that reasonable precautions are taken to protect relevant staff in high-risk or life-threatening operations. These will include:

- Assessing risks of injury to Personnel as well as the risks to the local population generated by the activities of Signatory Companies and/or Personnel;
- Providing hostile environment training;
- Providing adequate protective equipment, appropriate weapons and ammunition, and medical support; and
- Adopting policies which support a safe and healthy working environment within the Company, such as policies which address psychological health, deter work-place violence, misconduct, alcohol and drug abuse, sexual harassment and other improper behaviour.

Harassment

Signatory Companies will not tolerate harassment and abuse of co-workers by their Personnel.

Grievance Procedures

Signatory Companies will establish grievance procedures to address claims alleging failure by the Company to respect the principles contained in this Code brought by Personnel or by third parties.

Signatory Companies will:

- Establish procedures for their Personnel and for third parties to report allegations of improper and/or illegal conduct to designated Personnel, including such acts or omissions that would violate the principles contained in this Code. Procedures must be fair, accessible and offer effective remedies, including recommendations for the prevention of recurrence. They shall also facilitate reporting by persons with reason to believe that improper or illegal conduct, or a violation of this Code, has occurred or is about to occur, of such conduct, to designated individuals within a Company and, where appropriate, to competent authorities;
- Publish details of their grievance mechanism on a publically accessible website;

- Investigate allegations promptly, impartially and with due consideration to confidentiality;
- Keep records about any such allegations, findings or disciplinary measures. Except where prohibited or protected by applicable law, such records should be made available to a Competent Authority on request;
- Cooperate with official investigations, and not participate in or tolerate from their Personnel, the impeding of witnesses, testimony or investigations;
- Take appropriate disciplinary action, which could include termination of employment in case of a finding of such violations or unlawful behaviour; and
- Ensure that their Personnel who report wrongdoings in good faith are provided protection against any retaliation for making such reports, such as shielding them from unwarranted or otherwise inappropriate disciplinary measures, and that matters raised are examined and acted upon without undue delay.

No provision in this Code should be interpreted as replacing any contractual requirements or specific Company policies or procedures for reporting wrongdoing.

Meeting Liabilities

Signatory Companies will ensure that they have sufficient financial capacity in place at all times to meet reasonably anticipated commercial liabilities for damages to any person in respect of personal injury, death or damage to property. Sufficient financial capacity may be met by customer commitments, adequate insurance coverage, (such as by employer's liability and public liability coverage appropriately sized for the scale and scope of operations of the Signatory Company) or self insurance/retention. Where it is not possible to obtain suitable insurance cover, the Signatory Company will make alternative arrangements to ensure that it is able to meet such liabilities.

H. Review

The Swiss Government will maintain a public list of Signatory Companies and convene an initial review conference with a view to reviewing the Code after governance and oversight mechanisms (as referenced in the Preamble and Section C "Implementation" to this Code) are developed.

11. Conclusion

This project makes an attempt to provide some standard guidelines for management of Security in Industry. The contents of this project should be useful for many in the industry and those interested in industrial security to refer to various provisions of rules and regulations in force as also to various benchmarking standard for physical security of industry. Such compilations in this manner are not commonly heard of or produced by any security expert in the country.

Considerable emphasis has been laid on technology and the availability of various security gadgets in the market. The security technology market is very huge and growing every day. In some international conferences on Security one can find nearly 700 vendors globally exhibiting their security wares. You name an activity in the industry which needs to be protected and you will find a gadget tailor made to suit your requirement. Security experts and managements should be aware of the existing technology and use them for protecting their assets.

Both manpower and technology are essential for effective security. Both have their inherent weaknesses and thus one complements the other in enhancing the security and at the same time overcoming the deficiencies of the other

A major concern for security management experts all over the country is the poor quality of private security. Police and CISF cannot be deployed everywhere as their priority is different. The responsibility of protection of assets of the organization lies with the management and there are primarily responsible for the protection of their assets.

Many Private Security agencies have mushroomed all over the country with commercial objectives and with very little background and expertise in security. Unfortunately except for some of the Central Public Sector Undertakings where CISF is deployed , most other public sector undertakings and Private security are at the mercy of private security operators. They might have some professionals at the helm of management but unfortunately the line formation is extremely poor in their appreciation and knowledge of security issues. Unless this is addressed, I am afraid the security of the Industry is in very poor hands and anything can happen any time and assets of the industry can continue to remain poorly guarded. Hence a lot of emphasis is being laid on the provisions of the PASARA act and their provisions. There is an urgent need for all industry managers to ensure that PASARA provisions are implemented fully while deploying security personnel for their industry. The provisions of PASARA are un-ambiguous and the model rules of GUJARAT provide guidelines for the implementation of the act.

The guidelines of the International Code of Conduct for Private Security operators is a good step in instilling a sense of ethics and fair administration of security services. It has been observed that many security service providers are poor in their implementation of good practices while providing security services. The purpose of Code is to set forth a commonly-agreed set of principles for PSCs and to establish a foundation to translate those principles into related standards as well as governance and oversight mechanisms

There is an urgent need for a paradigm shift in the management approach to security. Capital expenditure on security cannot be viewed as an investment for which there has to be an inevitable return. There are many intangible returns which cannot be quantified. Security is not a product in which money is spent on its manufacture and it is sold at a price once the product is produced. Security is a service and no value or cost can be attached to a service. For example many losses due to fire and theft are reported in the industry and the management unfortunately writes off these losses when this loss could have been prevented by some investment in security and safety. In some countries investment in security gets a tax rebate and standard practice in some of the developed countries is to spend nearly 5 % of the project cost on security. Managements have to take a call on spending more money on security. Some major industries like Reliance have a foolproof security system. It is important for managements to increase their investment in security proportionate to the value of assets as also the vulnerability from the security perspective and the threat perception.

An important approach for Industry managers is to provide an exclusive security department in their organization. In most organizations security is part of the HR department with little or no expertise in handling security matters. It is ironic to note that many security managers still include security as a part of HR department which means security means handling Human Resource responsible for security. This has been the bane of industry when manpower is no longer the lone provider of security. Security today is an integration of many dynamics of which manpower is only a part. The managers should realize that security has to be an independent department and not part of HR to enable it to deliver effectively.

Industry managers have to understand that in practical terms security management should be in two tiers. There has to be a hierarchy of security personnel in the organization responsible for security policy and overseeing all the security activities. The second tier has to be invariably private security guards or operators who do the physical security part of the security of the industry .Their permanent security staff of the organization should be able to oversee the working of the second tier of private security operators

If these steps are implemented we can be assured of a reasonable amount of security to the assets of the industry which runs into thousands of crores and which form the backbone of the nation’s economy

12. References

1. American Society of Industrial Society (ASIS) Protection of Assets 2012, Volume 1-8
2. Patterson David G : Implementing Physical Security Protection systems. ASIS 2013
3. Dey and Kaushal: Essays on Industrial Security
4. NISA Academy, Hyderabad: Notes from various lectures
5. S.Subramanyam: Industrial Security
6. Australian Government: Physical Security Management Guidelines 21 June 2011
7. Intertech 2013. ITU-me.com
8. International Code of Conduct for Private Security Service Providers. 9 N0 2010
9. PASARA ACT 2007
10. PASARA Rules of Govt of Gujarat 2007
11. Notes from Reliance Security Academy
12. Samsung SNO 6084 R Data sheet
13. Samsung SNP 5430 H Data sheet
14. Anixter.com