POA – PHYSICAL SECURITY

INTRODUCTION

PPS - Physical Protection System.

- Primary function of PPS = detection, delay, and response.
- Secondary function of PPS = deterrence.

Physical Security

- that part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material and documents; and to safeguard them against a security incident.
- PPS Functions: People, Procedures, and Technology (hardware and software):
    - Hardware components of a PPS include:
        - Sensors, cameras, lighting, alarm monitoring, equipment, exit and entry control devices, barriers, and guard force equipment, such as radios, handcuffs, duress devices, and weapons.

Development of security system:

1. definition of the problem and a determination of the system's goals and objectives.
2. Next major stages = Design, Analysis, and Implementation.
    a. In the Design stage, specific security equipment and measures are divided into 4 groups, according to function:
        i. Deterrence, Detection, Delay, and Response.

CHAPTER 1 PROBLEM DEFINITION

- Security manager oversees the process of providing an integrated system solution to physical security problems.
- Business goals and objectives frame high-level PPS goals and objectives.

System

- collection of products, processes, or both, combined to provide a solution to a problem or goal.
- systems, not components, are optimized to yield the most effective design solution to the problem.

Integration

- the combination of a variety of components (such as people, procedures, and technology) to form a system.
- Includes:
  - Electrical integration – where components receive power and are interconnected).
  - Functional integration – (detection, delay, and response).

Systems Approach to Problem Solving

- a logical method for problem solving in which a comprehensive solution is developed in relation to a problem having several dimensions.
- Follows 3 general steps:
  - Assessment of *vulnerability*.
  - Implementation of *countermeasures*.
  - Evaluation of *effectiveness*.

Risk Management

- coordinated activities to direct and control an organization with regard to risk.
- Relies on Risk Assessment, which in turn, relies on Vulnerability Assessment.
- Overall Risk Management Process – threat, asset value, and vulnerability.

Risk Assessment/Management

RISK

- developed in the insurance industry.
- Risk (Insurance industry) – annualized loss expectancy.
  - Product of Potential loss and Likelihood of the event.
- Risk (Security Industry) – an uncertain situation in which a number of possible outcomes might occur, one or more of which is undesirable.
- Adverse outcomes, Probability, Magnitude, and Imminence.

RISK ASSESSMENT

- part of risk management.
- Process of defining how big the risk is.
    - May be heuristic (ad hoc), inductive, or deductive.
    - Quantitative or Qualitative.
- Quantitative – requires measurable data.
- Qualitative – often based on lists and depend on how analysts feel about the solution.
- Inductive techniques:
    - Using a bottom-up approach.
    - Identified at the beginning of the analysis rather than as a result of a systematic, deductive, top-down approach.
    - May provide incomplete results by focusing on scenarios.
    - Event trees – trace an initiating event through a sequence with different possible outcomes, use inductive logic to infer results.
        - useful, but do not readily handle feedback loops in the system.
- Deductive Risk Assesment:
    - Uses Logic Diagrams to determine how an undesired event may occur.
    - Fault trees – used with event trees to determine the basic causes of the event.
    - Also used are Influence Diagrams (often used in computer systems).
        - Conditional probabilities are assigned to various events.
- Probabilistic Risk Assessment:
    - More formal, scientific, technical, quantitative, and objective than risk management, which is based on value judgment and heuristics and is more subjective, qualitative, societal, and political
    - Probabilities should be based on objective likelihood:
        - In security, it is common to estimate likelihood based on subjective factors, such as intuition; expertise; partial, defective, or erroneous data; and dubious theories. These qualitative factors introduce much uncertainty.
        - Uncertainty in security systems is especially great due to lack of dependable data on all types of adversary attacks.
        - Not all scenarios can be anticipated.
- Simulation tools (often software):
    - Used to complement logical models.
    - Can help evaluate scenarios created through the logical model.
    - May be clustered into related groups to make numbers more manageable.
    - Must be validated before being used.

Risk Assessment – examines the outcome of an attack, its likelihood, how it will unfold, and how many people will be affected.

- Societal risk – if an entire population is at risk.
- 3 questions:
    - What can go wrong?
    - What is the likelihood?
    - What are the consequences?

Risk Management – comes next.

- Builds on risk assessment.
- Second set of questions:
    - What can be done?
    - What options are available?
    - What are their associated tradeoffs (costs, benefits, risks).
    - What are the impacts of current management decisions (policy) on future operations?
        - The last question leads to the optimal solution.
- Risk management is a systematic, statistically-based, holistic process that employs formal risk assessment and management and addresses the sources of system failures.

Security systems face many unpredictable elements, such as the probability of attack by all threats (human adversaries) in a statistically accurate sense.

In general, risk can be reduced by:

- Preventing an attack (requires intelligence gathering and deterrence).
- Protecting against an attack.
- Reducing (mitigating) consequences.
    - Can be done before, during, or after an attack.
    - Mitigation measures.

Risk Management should include:

- Risk financing (insurance), and
- Risk control tools.
- Approaches should include:
    - Avoidance, Reduction, Spreading, Transfer, and Acceptance.
    - PPS is one subsystem in an overall strategy.

Risk – threat, consequence, vulnerability.

Threat – combination of adversary capabilities, equipment, motivation or intent, and likelihood of an attack.

- Likelihood – measured in frequency or probability.
    - Frequency – number of times happened over a period of time.
    - Probability – the likelihood of one outcome out of the total of all possible undesirable outcomes – expressed as a number between 0 and 1.

Consequence – the undesirable outcome itself.

System effectiveness – the ability of the PPS to prevent a successful attack once it has been initiated.

Vulnerabilities – system weaknesses that can be exploited by adversaries.

Risk Assessment – overall process of risk identification, risk analysis, and risk evaluation.

- involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event aring from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

Vulnerability Assessment –performed after threats and assets are defined, to establish a baseline of PPS effectiveness in meeting goals and objectives.

- a decision must then be made whether the existing PPS is meeting goals and objectives…..IF not, it is time to begin Part 2 of the PPS cycle, the Design phase.

Threat Definition

- must be created during the risk assessment.
- Specific characteristics.
- Specific information about the adversary:
    - Outsiders, insiders, and outsiders in collusion with insiders.
    - For each, tactics (deceit, force, stealth, or any combination).
- Design Basis Threat (DBT)
    - The adversary against which the utility must be protected.
    - Threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence.
    - Treated as sensitive material
- In this context, threat comes from malevolent humans, not accidental (safety related) events.
    - PPS is designed to prevent malevolent attacks

- Safety vs. Security:
  - Safety – measures used to prevent or detect an **abnormal** condition that can endanger people, property, or the enterprise.
  - Security – measures used to protect people, property, or the enterprise from **malevolent** human threats.
- DBT includes vehicles, weapons, tools, or explosives, as well as the threat's motivation.
- Tool that the VA team and system designers use to establish system requirements.
- During the Vulnerability Assessment (VA), the DBT will help in gauging the effectiveness of the individual PPS components, and the overall system.
- Verifying system performance against the defined threats is the basis of vulnerability assessment (VA).
- Adversaries:
  - protection system needed is based on the adversary's motivation.
- Vulnerability Assessment (VA)
  - Verifying system performance against the defined threats.

Threat Spectrum

- variety of threats.
- Uses categories or labels to describe the threat characteristics for various levels of threat.
  - Specific characterizations, not a general listing.
- Vandals – small group, usually at night, may use drugs/alcohol, no insider assistance, not highly motivated, will flee.
- Disgruntled employee (insider)- acting alone, drugs/alcohol?, mentally unstable?, highly motivated, doesn't expect to be caught.
- Criminals – 1-5 people, financial gain, carefully plan, will flee if detected.
- Extremists – medium to large group, to bring attention, ideological, non-violent but may resist, will ignore commands to leave.
- Use of low, medium, or high levels to describe various threats.
- Using the threat spectrum to design a PPS that is effective against all threats and the full range of adversarial tools.

Likelihood

- additional element of threat definition is estimating likelihood.
- Using incident reports or other sources (immediate area, L/E).
- Can be a frequency, a probability, or a qualitative estimate.
  - Frequency calculations – where considerable data is available.
  - Probabilities – based more on a theoretical view.
  - Qualitative estimates – rank the attack possibility as very likely, highly unlikely, etc.
- Conditional risk – when there is no data to support an estimate – assume there will be an attack and evaluate risk on this basis.

Historical Experience

- usually not enough data:
  1. Lack of availability of information.
  2. Organization into a format that permits statistical processing.
- Useful – statistics shows that frequency of occurrence suggests the possibility of future recurrence.
- <u>Distribution curve</u> – number of past occurrences indicates which events have a high probability of occurring again.
- accuracy of predictions increase with the accumulation of historical data.
- <u>Principle of predictability</u> – the larger the number of events of the kind that includes the predicted event, the greater the agreement between the predicted pattern and the actual pattern of occurrence.
- Modern security departments use a database of incidents.
- Manual incident reports are used to simplify the input into the database.
- Codes denote the type of incident or the method of operation.
- Real value in vulnerability assessment.
- After the DBT and estimate of likelihood, the second key aspect of defining goals and objectives is -----Asset Identification.

Asset Identification

- assign a value to the asset (criticality, consequence of loss, or severity).
- Effect their loss could have on the site or enterprise.
- 3 general methods of valuating assets:
  - dollar amount, consequence criteria, or policy.

Loss Impact

- most important = monetary terms.
- Other measurements – employee morale, community relations.
- Compare the cost of estimated losses with the cost of protection.
- Quantitative evaluations of the security effort.
  - Financial terms: profits achieved or costs reduced.
- Cost-justified – not spending more than the benefits derived are worth.
- Direct and indirect costs:
  - Indirect – reputation, goodwill, morale, turnover.
- <u>Permanent Replacement</u> – lost asset.
  - costs to return to former location.
  - Purchase price/manufacturing cost, shipping, labor (make ready).
- <u>Temporary Substitute</u> – while awaiting permanent replacements.
  - Lease/rental, premium labor (overtime).
- <u>Related or Consequence Cost</u>
  - Downtime, loss of discounts in paying bills, delay in accounts payable.
- <u>Lost Income Cost</u>
  - income from not investing the cash.
  - <u>Lost Income</u> – additional cost margin - use of the money for loss replacement.
- <u>Cost abatement</u> – purchase cost of insurance subtracted from payment.

- Cost-of-Loss Formula – taking the worst case position and analyzing each security vulnerability in light of the probable maximum loss for a single occurrence of the risk event.
    - Extensive criticality data – insurance department.
    - Loss-risk probability data – asset protection or security department.
        - (MUST be combined).

- Consequence Criteria – another approach to asset valuation.
    - Harm, days to recover, reputation.
    - Each criterion needs value ranges to help assess the value of an asset.
        - Quantitative or qualitative.
        - (Best to use Quantitative).
        - Only 4 to 8 criteria
    - Appropriate consequences – then assets ranked accordingly.
    - Redundancy is a useful criteria.
        - If other locations exist, overall consequence may be lower.
    - Next step in the risk analysis – Vulnerability Assessment.

Vulnerability Assessment (VA)

- process of identifying and quantifying vulnerabilities.
- Vulnerability Analysis – method of identifying weak points of a facility, entity, venue, or person.
- Evaluates the state of the PPS at a facility to determine how well it meets the defined goals and objectives.
- Vulnerability – intrinsic properties of something that create susceptibility to a source of risk…that can lead to a consequence.
    - Weakness that can be exploited by an adversary.
- Baseline PPS -> Repeated to verify effectiveness -> conducted periodically.
- A well-designed, integrated PPS is more effective against lower-level threats.

VA Team

- led by a security specialist experienced in security systems design and project management.
- Security Systems Engineer – detection, delay, and response technologies and security system integration.
- Response Experts – weapons, guard force tactics/training, contingency and emergency planning, and investigation techniques.
- Data Analyst – computer modeling to predict system performance.
- Experts – in other areas.
    1. Determine system goals and objectives:
        a. Output – design base threat or threat spectrum.
    2. Site survey – facility characterization and current security.
    3. Baseline is analyzed.
        a. If risk is acceptable, existing system is satisfactory.

VA Concepts

- must take a holistic view.
- Overall system – not individual components.
    - Will expose other factors.
- Vulnerabilities that may be exploited by a threat.
- All PPSs have some weaknesses – there will always be some risk.
- Detailed threat definition is critical to VA and risk assessment.

VA Objectives

- Facility Characterization – evaluation of the facility's PPS.
- Goal is to identify PPS components in the functional areas of detection, delay, and response and gather data to estimate performance against particular threats.
- Accurate data are the foundation for true analysis of PPS ability.
    1. Facility tour.
    2. Review of key documents and interviews of key personnel.
    3. Evaluation testing – whether personnel have the skills and abilities to perform their duties, whether procedures work, and whether equipment is functional and appropriate.
        a. Functional tests – verify that a device is on and performing.
        b. Operability tests – verify that a device is on and being used properly.
        c. Performance tests – repeats a test enough times to establish a measure of device capability against different threats.
- Vulnerabilities at the facility at all times (24/7/365).

3 Primary Functions of PPS:

Detection, Delay, and Response.

Detection

- discovery of covert or overt action by an adversary.
    - Entry control – allowing authorized and detecting unauthorized.
- Throughput – number of authorized personnel allowed access over a given period of time.
- False Acceptance Rate – rate at which false identities or credentials are allowed entry.
- False Rejection Rate – frequency of denying access to authorized personnel.

Delay

- slowing down of adversary progress.
- Time required by the adversary (after detection) to bypass each delay.
    - Delay before detection – primarily a deterrent (not additional time for response).

Response

- actions by security officers to prevent adversary success.
- Interruption.
- Response effectiveness is measured by time between:
    - Receipt of a communication and interruption of adversary action.

The amount of protection required = value of the asset and the risk tolerance of the enterprise.

Determine security system effectiveness.

Master Project Agreement – defines the protection of the final report and appropriate distribution.

A Vulnerability Assessment report is the analysis of system requirements that must occur before system design and implementation.

Risk Assessment

- provides the answers to 3 questions:
    1. What can go wrong?
    2. What is the likelihood?
    3. What are the consequences?
- Risk analysis is conducted.
- As threat capability increases, performance of PPS decreases.
- System Effectiveness – measure of system vulnerability – combined with threat and asset value to determine the baseline risk.

Analysis Approaches:

Compliance-based – depend on conformance to specified policies and regulations.

Performance-based – actually evaluates how each element of the PPS operates and what it contributes to overall system effectiveness.

- underlying premise is that overall system effectiveness is the goal of a VA.
- (Recommended method).
- 6 step process in performance-based (qualitative or quantitative):
    1. Create an adversary sequence diagram for all locations.
    2. Conduct a path analysis.
    3. Perform a scenario analysis.
    4. Complete a neutralization analysis, if necessary.
    5. Determine system effectiveness and risk.
    6. Develop and analyze system effectiveness upgrades if risk not acceptable.

R = T x A x V:
R = residual risk
T = threat (threat definition and likelihood of attack
A = Asset to be protected.
V = Vulnerability, represented by system effectiveness.

Management Decision – whether to accept the risk or fund the PPS.

Risk is estimated through the use of a vulnerability assessment.

System view – rather than a component view.

CHAPTER 2 DESIGN PRINCIPLES AND CONCEPTS

- a well-engineered PPS exhibits the following characteristics:
    - Protection-in-depth.
    - Minimum consequence of component failure.
    - Balanced protection.

Protection-in-Depth

- requires a number of protective devices in sequence to be avoided/defeated.
- Increases uncertainty about the system (to the adversary).
- Requires more preparation prior to attacking.
- Creates additional steps (adversary may fail or abort mission).

Minimum Consequence of Component Failure

- Component failure due to:
    - Environmental factors.
    - Adversary actions.
- Contingency plans – redundancy equipment automatically takes over.
- Aid required from other sources as needed (ie. Law enforcement).

Balanced Protection

- Effective elements of the PPS will be encountered no matter how the adversary attempts to accomplish their goal.
- Adequate protection against all threats on all possible paths, and to maintain a balance with considerations such as: cost, safety, and structural integrity.

Design Criteria

- Design process based on performance criteria.
- Elements and procedures according to the contribution they make to overall system performance.
- The Effectiveness measure = overall system performance.
- Feature Criteria Approach – selects elements or procedures to satisfy requirements that certain items present.
    - The effectiveness measure is the presence of those features.
    - NOT DESIRABLE:
        - Overall system performance, NOT features or components.
- Performance criteria vs. Feature Criteria:
    - Performance – requires detection of intruder.
    - Feature – identifies type and quantity of sensors (motion, fence, etc.).
    - PERFORMANCE BASED – meets the approach of PPS objectives.

Performance measures for the PPS functions:

1. Detect.
2. Delay.
3. Response.

Additional Design Elements

- an effective PPS combines People, Procedures, and Equipment into an integrated systems that protects assets from the expected threat.
- Procedural changes are cost-effective – but only protect against the lowest threats.
- Investigations – in response to a loss, or to prevent/anticipate a threat (ie. Background Investigations).
    - another design element in the PPS.
- Technical Surveillance techniques – areas free of recording devices to protect against industrial espionage.
- Design elements will depend on:
    - Threat
    - Likelihood of an attack
    - Consequences of loss of the asset.
- Procedural elements – ie. Shredding, locks, passwords, drug searches, periodic audits, parking permits, etc.

3 Primary Functions of a PPS:

1. Detection.
2. Delay.
3. Response.

SECONDARY function of PPS is DETERRENCE:

- Measures that adversaries will perceive as too difficult.
    - Makes facility an Unattractive Target.
- Officers, signs, lighting, barriers, etc.
- Deterrence is difficult to measure.
    - No statistically valid information to support effectiveness.
- Relying on deterrence is risky.
- Some employees feel they will NEVER be caught.

CHAPTER 3 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

CPTED Proper design and effective use of the built environment can lead to a reduction in the opportunity, fear, and incidence of predatory stranger-to-stranger type crime, as well as result in improvement of the quality of life of where we live, work, and play.

- Design or redesign of a venue to reduce crime opportunity:
  - Through Natural, Mechanical, and Procedural means.
- Crime prevention theory based on environmental criminology.
- Involves planners, designers, architects, users, etc.

CPTED targets:

- Places – designed to produce behavioral effects that reduce opportunity.
- Behavior – some locations promote or allow criminal activity.
- Design and Use of Space – encourage desirable behavior/discourage crime.

CPTED Fundamentals – design of physical space:

- Mechanical means – target hardening, physical security hardware and technology.
- Human and Organizational measures – provides the opportunity and ability to observe, report, and intervene.
- Natural measures – good space planning:
  - reduce inhabitant conflict by considering compatible circulation patterns.
  - Unobstructed line of sight, landscaping, bollards.
- **even when supplied mechanically (ie. Lamps), lighting is classified as a *Natural Surveillance Component.***

Natural Access Control

- employs both real and symbolic barriers (doors, fences, shrubbery).

Natural Surveillance

- increasing visibility by occupants and others.
  - Increases detection of trespassers and misconduct.
- Removing barriers to sight and providing better observation.
  - ie. Chain link fence vs. solid wood fence.

Natural Territorial Reinforcement

- establishing a sense of ownership and responsibility (owners/occupants) to increase vigilance in identifying issues.
- Psychological Ownership – will pay more attention to a defend a space.
- Territorial reinforcement measures:
  - Physical or symbolic.
  - Natural because it results from normal, routine use of the environment.

Management and maintenance

- to look well cared for and crime-free.
- Impression of abandonment – increased crime opportunity.

Legitimate Activity Support

- criminal activity thrives in spaces residents/management fail to claim through legitimate activities.

CPTED Solutions should be integrated with the functions of the buildings, etc.

CPTED differentiates from traditional target hardening and fortressing techniques.

- target hardening is usually NOT architecturally or aesthetically pleasing.

CPTED strategies for specific places:

3-D Concept – areas that are:

1. Defined.
2. Designated.
3. Designed.

Graphics and Signage for CPTED

- COMMUNICATES message regarding designated use.
- Graphic – symbol that conveys a message PICTORALLY.
- Signage – conveys a message with LETTERS/WORDS.
- Sets expectations or ground rules.
- Just putting up a sign does not relieve the owner of liability.
- Reduces wandering and those with nefarious intentions.
- Architectural design considerations:
    - Size, typeface, distance, lighting, reflectivity.
    - 20/20 vision @ 50 feet =
        - letters at least 6 inches high.
        - Graphics/symbols at least 15 inches high.
    - Lighting levels = at least 20 foot-candles (215 lumens per sq. meter).
- Systems considerations:
    - Consistent, uniform, and well-distributed. Systematically displayed.
- Procedural considerations:
    - Used to clarify procedures (ie. Wearing of ID badges).
- If the users do not follow the rules, the burden of responsibility shifts, and they can be challenged as to their intent.
- Without signage/graphics – subject to personal interpretation and difficult to challenge.

History of CPTED

- first study in 1920s.
- Jane Jacobs 1961 – Defensible Space Theory.
    - Orient buildings towards the street, clearly distinguish public and private areas, placing outdoor spaces near intensively used areas.
- Oscar Newman 1973 – explored human territoriality, natural surveillance, and modification of existing structures to reduce crime.
- Defensible spaces release tenants' latent attitudes allowing them to adopt behaviors necessary to protect their rights and property.
- 1996 – International CPTED Association (ICA).
    - CPTED practitioner certification program.
- 3 first principles of CPTED:
    1. Access Control.
    2. Natural Surveillance.
    3. Territoriality.

Crime Prevention Assumptions

- reducing criminal motivation by reducing opportunities to commit crime.
- Law Enforcement – after the fact solving and apprehension - NOT prevention of crime.
- Crime prevention strategies should focus on the ACT, not the perpetrator.

Contemporary Thinking on Crime and Criminals

- a site's physical features may influence offender choices by altering the chances of detection or changing other factors.
- Places become derelict or underused and lack natural surveillance.
- An area is either very quiet or very busy.
- People feel there is nothing to do.
- A place feels as if it's not under supervision.
- Untidy or unattractive – impression that crime and disorder is tolerated.
- Target selection – successful initial offense and information gained from that experience.

CPTED measures should focus on preventing the most severe acts and protecting the most frequently victimized persons or locations:

- Quickly remove signs of vandalism.
- Improve physical security.
- Block easy access to targets – real or symbolic.
- Protect especially vulnerable targets.
- Regulate access to high-risk assets or areas.

Capable Guardian

- Routine Activity Theory – suggests capable guardians may deter crime.
    - Armed, capable of resistence, or potentially dangerous.
    - Criminals look for easiest, least-risky path.

Situational Crime Prevention

- sought to reduce crime opportunities in all behavioral contexts, not just buildings and other spaces.
- Opportunity-reducing measures.
- Boundary setting rules and stimulating the conscience of potential offenders.
- Manages, designs, or manipulates the environment in a systematic way as permanently as possible – to increase the effort and risks of crime and reduce the rewards as perceived by a wide range of offenders.
- Uses Rational Choice Theory as its theoretical framework.
    - Methodology that analyzes the opportunities.
    - Prescribes solutions.
    - Offender weighs the costs, risks, and rewards.
- Situational Crime prevention methods:
    - Increase the effort.
    - Increase the risk.
        - Screening, CCTV, employee surveillance, natural surveillance.
    - Reduce the rewards.
    - Remove excuses (by inducing shame or guilt).
        - Rule and boundary setting – removes ambiguity.
        - Stimulating the conscience.
        - Facilitating compliance – making it easier to act properly.

Defensible Space

1. Define perceived zones of territorial influence.
2. Provide surveillance opportunities for residents/guests.
3. Place residential structures (public areas and entries) close to safe areas.
4. Design sites and buildings so occupants are not perceived as stigmatized or vulnerable.

- link territoriality and surveillance by creating designs that lead people to consider the area as being within their sphere of influence.
- Ownership and responsibility – therefore try to protect the area.
- Community development – both social and physical.
- Second Generation CPTED :
    - social prevention and opportunity reduction balanced together.

Crowe and CPTED (1991)

- 3-D approach to CPTED.
    - A design is proper if it recognizes the designed use of the space; defines the crime problem incidental to and the solution compatible with the designated use; and incorporates the crime prevention strategies that enhance (or at least do not impair) the effective use of the space.
    - Definition, Designation, and Design.

Second Generation CPTED:

- return physical CPTED to its origins in community development.
- Not only reducing physical opportunities BUT: create a sense of neighborliness.
- 4 main strategies:
  1. Cohesion – community groups, neighborhood associations, personal development programs (personal/financial assistance).
  2. Capacity Threshold – tipping point theory.
     a. Balances land uses and urban features.
  3. Community culture.
  4. Connectivity – link neighborhood to surrounding areas and to funding and political support from corporations and upper level of government.

CPTED 3-D and Beyond

- evaluate the purpose of a space, its definition in terms of management, and its design as it relates to desired function and behavior management (the 3 D's).
- Space is assessed according to how well it supports:
  - Natural access control, natural surveillance, and territoriality.

Reducing Crime Through Architectural Design

- CPTED features into the facility design.
  - More cost-effective during initial planning stage.

Traditional Building Planning

Programming – building's purpose and occupants.
- **Security needs addressed in programming phase of design.**

Schematic designs

- bubble diagrams – circulation patterns and proximity relationships.
- Evolve into floor plan drawings, site plan, and elevations.
- Beginnings of engineering considerations.

Design development

- structural, mechanical, electrical, ventilation, site planning
- Drawings – larger scale – in US = ¼ inch to 1 foot.

Construction documents or Working drawings

- final drawings.
- Technical data accompanied by technically written specifications.

Bids for construction and selection of contractor.

3 Challenges for architects:

1. Determining requirements – supporting desired behaviors and the intended function of space.
2. Knowing the technology.
3. Understanding architectural implications.

- Architect then converts the security requirements into an architectural program
- Circulation, access, building materials, fenestration (windows/doors).
- Natural and normal uses of environment can accomplish the effects of mechanical hardening and surveillance:
    - Natural access control, surveillance, and territorial reinforcement:
    - Through staffing, mechanical/technology, and natural methods (site planning, design, landscaping, and signage).

<u>Access Control, Surveillance, and Territorial Reinforcement</u>

<u>Access Control</u> – strategy to deny access to a crime target and create in offenders a perception of risk as well as detection, delay, and response.

- Surveillance strengthens access control.
    - Organized – police and security patrols.
    - Mechanical – lighting and video.
    - Natural – windows, low landscaping, and raised entrances.

<u>Site Development and Security Zoning</u>

- goal = meets architectural requirements and provides security advantages.
- Topography, adjacent land uses, circulation patterns, crime patterns, sight lines, utilities, lighting, access points, etc.
- Site analysis represents the **first** level of security defense planning.
- **Second** level of security defense planning is the perimeter or exterior of the building.
    - After site perimeter and grounds – building shell and openings are the second line of defense against intrusion.
    - 4 sides, and a top and bottom.
    - Doors/windows – provide poor resistance to penetration.
- **Third** level is internal space protection:
    - Unrestricted zones – lobbies, reception, snack bars, meeting rooms.
    - Controlled zones – must have a valid purpose for entry.
    - Restricted zones – sensitive areas – may require additional access control.

<u>Visibility: Privacy versus Security</u>

- adding trees may provide a sense of enclosure but still allow ability to see.
- Block/brick walls – provides security but also hides thieves.
    - Bare walls invite grafitti.
- Bushes, hedges, ferns – harder to carry out large stolen goods.
- Earth berms – natural access control but a visual obstruction.
    - ie. No more than 2.5 feet.
- <u>Landscaping and planting:</u>
    - Low growing plants – set back 1 yard from paths.
    - No higher than 32 inches.
    - Spiny or thorny shrubs – for potential hiding places.

    - Hard landscaping – may be used as projectiles.
    - Furniture – designed to prevent sleeping.
    - Tree canopies – trimmed up to 8 feet – reduces hiding spots.
    - Lighting – from tops of trees – Downward.
    - Trees may affect video surveillance.

Office Buildings

- corporate assets that are vital to be protected.
- 3 categories: **people, information, and property**.

People

- most valuable asset.
- Who, why, what do they do, when, where, how (access, circulation).
- Information is used to develop schematic drawings, development drawings, and construction documents.

Assets

- who has access, what is the information, format, how transferrable and transportable, why is it worth protecting.
- Information Protection Plan.
    - Develop architectural, technological, and organizational responses that support a comprehensive information asset protection strategy.
- Architectural Design:
    - Doors and windows – visibility of information, activities and equipment.
    - Reception desk – view of all entry doors and elevators.
        - Establishes the layering of public vs. private.
    - Controlled areas.
    - Computer rooms and computer anchoring.
    - Employee traffic patterns.
    - Elevators – open into the supervised core area.
    - Loading dock – separate access road.
        - Ground loops and intercom.
        - Shipping and receiving areas – Separated.
    - Mail room – secured.
    - Appropriate vaults.
    - Conference meeting facilities – outside the restricted area, before the security access point.

Property

- same six questions (5 w's and how)
- environmental conflicts that provide opportunities for offenders.

CPTED for Offices and Office Buildings

- site location and landscaping, external areas (garages and parking lots).
- Video surveillance after circulation patterns.
- Limited number of access points – if additional needed, use exit only.
- Lobby – higher grade materials – success, stability, power.
- Reception desk – layer in building security. Emergency call button.
- Access control and video surveillance during building design and architectural programming.
- Pedestrian access – directly from street to front of building.
- Orientation – allow views into site.
- Doors and windows – especially on ground floor.
- Conduits – security needs and capacity for future needs.

Industrial Buildings

- high risk of employee theft, burglary, robbery, commercial espionage, vandalism, and arson.
- Minimize openings in building shell.
  - Reinforce larger than 96 square inches, or lower than 18 feet.
- Separate paths for public, private, service vehicles.
- Emergency exits alarmed and video surveillance.
- Separate shipping and receiving.
- Compactors/Incinerators – access without leaving building.
- Research and Development – away from normal circulation paths.
- Entrances directly off parking lots.
- Personnel office – outer edge of building.
- Ceiling closures.

Parking Facilities

- surveillance/access control/territorial reinforcement through:
  - design, security patrol, and technology.
- Vulnerability Assessment.
  - Landscaping, lighting, stairwells, elevators, cameras, access control, signage, restrooms, revenue collection, line of sight.
- Ground (surface parking):
  - Perimeter definition and access control.
  - Walls: screened on ground and open on above floors:
    - Provides natural surveillance.
  - Exterior doors – egress only.
  - One means of entry and exit with arm, roll down gate, attendant booth, video, and good lighting.
  - Avoid pedestrians crossing in front of cars.
  - Attendants – radio or telephone for assistance.
    - Drop safes.
    - Restroom with alarm.
  - Exclude public restrooms – difficult to secure (privacy).

- Structural elements:
    - Round columns – better visibility.
    - Stairwells visible from ground level – clear enclosures.
    - Elevators – as much glass as possible.
        - Should not go directly to residential floors
- Surveillance:
    - Cameras with dark polycarbonate domes.
        - Resist vandalism and obscure where camera is looking.
    - Integrated panic buttons.

Lighting:

- Stairs, elevators, ramps – 5 to 6 foot candles (54 to 65 lumens per square meter).
- Walkways around garages – 5 foot candles of lighting.
- Open parking lots – 3 foot candles (32 lumens per square meter).
- Entrances – 10 foot candles (108 lumens per square foot) OR:
    - twice the level of surrounding area to stand out/increase visibility.
- Perimeter fencing – at least ½ the average horizontal illumination on both sides of the fence to reduce hiding spots.

Height of Light Fixtures:

- ability to see past shadows:
- Typical light poles are 30 to 45 feet high and cast a wide swath of lighting but create deep shadows between cars.
- Pedestrian level lighting – 12 to 14 feet high casts light that will go through the windows of cars and reflects off cars – reducing shadows and dark spots.
- Pathways to garages – 3 foot candles (32 lumens per square meter) to allow visibility of persons 30 feet away.
    - Average-to-minimum lighting ratio not to exceed 4:1.
- Open parking lot – should have a combination of high and low lighting.
- Painted - light colors to increase light reflection.
- Lamps:
    - Most CPTED practitioners prefer:
        - Metal Halide lamps:
            - Last about 20,000 hours.
            - Accurately reproduces color.

        Low-pressure sodium vapor lamps:
        - last about 50,000 hours and most energy-efficient.
        - Poor color rendition.

        High-pressure sodium vapor lamps and Mercury Vapor:
        - less expensive but do not last as long.
        - Poor color rendition.

Signage

- for parking facility – Letters at least 8 inches high.
- Graffiti-resistant epoxy paint.
- Attempts to prevent send a message that territory belongs to rightful owners.

Mixed Uses

- Having legitimate users increases eyes on the street. (Surveillance)
- Copying facilities, fast food, car washes – draw legitimate users.

Schools

- CPTED and technology can make contributions without turning school into a fortress.
- Site, building design, interior spaces, systems and equipment.
- Perimeter fencing and gates – must allow a view for natural surveillance.
- Planting should not provide hiding spaces.
- Clear views from administrative offices (ie. Parking).
- Parking and circulation areas – observation from classrooms.
- Traffic calming – few or no long runs.
- Spatial/temporal issues
  - Spatial - Useful to place safe activities in unsafe locations.
    - Adult education after hours.
  - Temporal – different lunch times for older and younger students.
    - Driver education in parking lots.
- Windows – a group of small windows provide the same benefits of a large window, but with greater security.
  - Clerestory windows – along the top of a wall.
    - Provides security and natural lighting.
- Video surveillance, duress alarms, securing computers.

Automated Teller Machines

- adequate lighting.
- US has no standards but some states and cities do have typical standards:
  - Face ATM - 25 foot candles (269 lumens per square meter).
  - Within 5 feet of face – 10 foot candles (107 lumens per square meter).
  - 50 to 60 feet away – 2 foot candles (22 lumens per square meter).
    - (measured at 3 feet above the ground)
- Photo sensors to turn lights on automatically.
- Landscaping – allow for good visibility, remove hiding places.
- Rearview mirrors on ATMs.
- Install where natural surveillance is plentiful:
  - Pedestrians and drivers.
  - Large vision panels.
- Duress alarms

- <u>ATM as a target itself</u>:
    - alarm system components, shock and seismic sensors, sufficient weight and tensile strength, heat detectors, and locking mechanisms.
- Install at police stations – natural surveillance.
- Surveillance cameras – deters robbery and fraud. Identifies criminals.
- **Do not use dummy cameras unless there are working cameras:**
    - False sense of security.
    - May lead to a security negligence lawsuit:
        - **"Illusion of Security".**
- Install devices to allow victims to summon police:
    - ie. Reverse PINs.
- Deploy private security officers.
- Prohibit loitering and panhandling.
- Locking doors.
- Daily withdrawal limits – not worth the risk of apprehension.

U.S. Federal Buildings

- GSA standards: security glazing, bomb resistant design and construction, landscaping and planting design, site lighting, and natural and mechanical surveillance opportunities.
- Setbacks – as far out as possible. 100 feet recommended.
- Concrete barriers (planters) – less than 4 feet spacing between.
- Simple rectangular shape – minimizes blast waves.
    - Diffraction effect - Blast waves from U or L shaped buildings.
- Building ornamentation could break away in a blast.
- Eliminate hiding places and unobstructed views.
- Parking as far from building as possible – Not under building.
- Secure access to heat, water, gas, electric.
- Eliminate Perpendicular lines of vehicle approach to building.
- Although CPTED may not be able to stop the most determined terrorist or criminal, even acts of terrorism usually start with trespassing or unauthorized access as the property is scoped for vulnerabilities.

<u>CPTED Survey (appendix)</u>
(only certain items listed here)

Incorporating CPTED design principles into proposed projects:

1. Natural Surveillance.
    i. Blind corners, mirrors.
    ii. Site and building layout – natural observation.
    iii. Main entrance facing street.
    iv. Shopping centers face street.
    v. Trash bins that do not allow opportunity to hide.
    vi. Visibility to entrances before entering.
    vii. Fences – solid fences – visibility above 5 feet or open elements.

   viii. Lighting in accordance with Illuminating Engineering Society.
   ix. Useful ground coverage of an elevated light fixture is:
      a. Roughly twice its height.
   x. Avoid lighting of areas not intended for nighttime use to avoid giving false impression of use or safety.
   xi. Select and light “Safe Routes”.
   xii. Photoelectric – rather than time switches for exterior lighting.
   xiii. Mix of uses – increases natural surveillance.
   xiv. Bars/Shutters/Doors – visually permeable (see-through).

2. Access Control
   i. Building identification – number.
   ii. Minimize the number of entrances.
   iii. Location maps and signage.
      i. Simple graphics.
3. Ownership
   i. Maintenance – create a “cared for image”.
   ii. Materials – that reduce the opportunity for vandalism.

PPS FUNCTION

DETECTION

The physical protection systems function of detection is addressed in the next five chapters:

- SENSORS
- VIDEO SUBSYSTEMS and ALARM ASSESSMENT
- LIGHTING
- ALARM COMMUNICATION and DISPLAY
- ENTRY CONTROL

CHAPTER 4 SENSORS

- Basic building blocks of an intrusion detection system.
- Initiates the detection function of the security system.
- All logical activities occur after the initial alarm – due to the technology on which the sensor is based.
- Critical to properly match the sensor to the threat and operating environment and integrate it into the overall physical protection system (PPS).
- <u>Intrusion Detection Systems:</u>
    - Include interior/exterior intrusion sensors, video alarm assessment, entry control, and alarm communication systems working in combination.
    - The intrusion detection boundary should be thought of as a sphere surrounding the protected item.

Performance Characteristics

<u>3 main characteristics:</u>

1. Probability of Detection (PD).
2. Nuisance Alarm Rate (NAR).
3. Vulnerability to defeat.

<u>Probability of Detection (PD)</u>

- a perfect probability of detection would be 1.
- Effectiveness of the sensor = PD and Confidence Level (CL).
    - If CL not stated – implied 90 percent for CL.
- PD depends on:
    - Target to be detected, hardware, installation, sensitivity, weather, condition of equipment.
- System design is driven by the DBT (design basis threat):
    - The more capable the adversary, the higher PD needed.
- Clear and measurable set of conditions, not just a general statement.
- Multiple sensors recommended.

<u>Nuisance Alarm Rate (NAR)</u>

- <u>Nuisance Alarm</u> – any alarm not caused by an intrusion.
- Alarm assessment determines the cause and decides if response necessary.
    - May be caused by vegetation, wildlife, weather.
    - Without assessment, detection is incomplete.
- <u>False Alarm</u> – nuisance alarms caused by the equipment itself.
- Specify an acceptable false alarm rate (FAR) when designing a system.

Vulnerability to Defeat

- all existing sensors can be defeated.
- Bypass – going around its detection volume.
- Spoof – any technique that allows passage through without alarm.

Alarm Initiation Conditions

Types of sensors:

Intrusion sensors	- occurrence of a potential intrusion event.
State sensors	- change in safety or process condition. (temperature, smoke)
Fault event sensors	- loss of electrical power.
Tamper sensors	- opening, shorting, or grounding of the device circuitry or tampering with the sensor's enclosure or distributed control panels (transponders).
Failure of the sensor itself	- fault event that should be detected.

Standards

UL Standards

- guide to device manufacturers.
- Device is submitted and certified if it meets standards.
- Periodic UL directories.
- Security devices listed in *Automotive, Burglary, Protection and Mechanical Equipment Directory.*
- In some municipal building and fire codes – UL approval is a requirement.
- UL is Safety Standards NOT Security Standards.
  - Safety does not address device's vulnerabilities or ability.
- Many UL standards are designated a national standard by ANSI.

ASTM Standards

American Society for Testing and Materials

- committee to deal with security standards.
- ASTM standards not yet developed for security alarm systems or sensors.

Other Standards and Specifications

- US General Services Administration (GSA) – 1969.
- National Fire Protection Assoc. (NFPA)
  - Standards for municipal, central station, proprietary, and local fire alarm systems.

Exterior Sensors

Classification – 5 methods (Passive or Active, Covert or Visible, Line-of-Sight or Terrain Following, Volumetric or Line Detection, Application).

Passive or Active

- Passive sensors – operate in two manners:
    - 1. Detect energy omitted by the object of interest
    - 2. Detect a target-caused change in a natural field of energy.
    - Use a receiver to collect energy emissions.
    - Does not emit energy – harder to find by adversary.
- Active sensors – transmit energy and detect changes in the received energy.
    - Contain a transmitter and a receiver.
    - Microwave, infrared, and other radio frequency (RF) devices.
    - Fewer nuisance alarms – due to stronger signals.

Covert or Visible

- Covert – more difficult for intruder to detect. Does not interfere with appearance.
- Visible – may deter intruders.

Line-of-Sight or Terrain-Following

- Line-of Sight (LOS) – requires clear line of sight between transmitter and receiver.
- Terrain-Following – can be used on irregular terrain.
    - Transducer elements and a radiated field follow the terrain.

Volumetric or Line Detection

- volumetric sensor - generates an alarm when an intruder enters the detection volume.
    - Harder for an intruder to determine.
- Line Detection sensor – detects motion along a line.
    - ie. Detecting fence motion.
    - Usually easier to identify.

Application

Mode of application

1. Buried line.
2. Fence-associated.
3. Freestanding.

Types of Exterior Intrusion Sensors

Ported Coaxial Cables

- Active, covert, terrain-following sensors.
- Buried underground.
- Also called leaky coax or radiating cable sensors.
- Respond to the motion of material with high dielectric constant or high connectivity (Human bodies and metal vehicles).

Fence Disturbance Sensors

- Passive, visible, terrain-following sensors.
- Installed on chain-link fences.
    - Terrain following since mesh itself follows the terrain.
- Can detect motion or shock. (climbing or cutting fence).
- Nuisance alarms caused by rain, wind, hail, debris, and seismic activity from nearby traffic and machinery.
    - Debris and animals – NARs reduced by installing on inner fence.
- Can be defeated by tunneling under or climbing over.
    - PD will be very low or zero.

Sensor Fences

- Passive, visible, terrain-following sensors.
- Form the fence out of the transducer elements themselves.
- Designed to detect climbing or cutting of fence.
- Taut-wire sensor fences – many parallel, horizontal wires connected under tension to transducers – Detects deflection of the wires.

Electric Field or Capacitance

- Visible, terrain-following sensors.
- Designed to detect a change in Capacitive coupling among a set of wires attached to, but electrically isolated from a fence.
- More difficult to defeat by digging/climbing because detection volume extends beyond the fence plane.
- Can be mounted on posts instead of fences.

Freestanding Infrared Sensors

- Active, visible, line-of-sight, freestanding Infrared (IR) sensors.
- IR beam transmitted from IR light-emitting diode through a collimating lens.
- Collected on other end of detection zone by a collecting lens that focuses energy onto a photodiode.
- Detects the reduction in received infrared energy.
- IR beams travel in a straight line – LoS (Line-of-Sight) sensors.

Bistatic Microwave Sensors

- Active, visible, line-of-site, freestanding sensors.
- 2 identical microwave antennas – installed at opposite ends.
    - One is connected to a microwave transmitter;
    - One is connected to a receiver that detects microwave energy.
- Respond to changes in the vector sum (direct beam and reflected signals) caused by moving objects.
- Often installed to detect a human crawling or rolling on the ground.
- Zone of no detection – first few yards/meters in front of antennas.
    - Offset Distance.
        - Requires overlapping of antennas.
- Best to have no vegetation.

Exterior Video Motion Detectors (VMDs)

- Passive, covert, line-of-site sensors that process video signals from closed-circuit television (CCTV) cameras.
- Sense a change in the video signal.
- Allows for alarm assessment by providing a video image.
- Masking – selecting only parts of the video scene that the VMD will protect, ignoring activity in the unmasked portions.
- Increased sensitivity = increase in nuisance alarms.
- VMD best if used in conjunction with other sensors.
- Best suited for interior application.
    - Exterior – further development necessary to reduce NARs.

Technology Maturity

- Is the technology ready for deployment?
- Risk of immature security technology fielded prematurely.
- Maturity Model:
    - Research.
    - Level I – feasibility. Laboratory demonstration.
    - Level II – Research prototype – hand-built.
    - Level III – Engineering prototype – 90% functionality.
    - Level IV – Field prototype – fully functional.
    - Level V – (COTS) Commercial off-the-shelf technology.
        - manufactured production units available.
    - Level VI – Performance testing.
        - PD, NARs, VD, performance degradation, interference.
        - 12-months for outdoor applications – all weather.
    - Level VII – Onsite testing – actual performance.
    - Level VIII – Nontechnical maturity factors – concept of operations.

Continuous Line of Detection

- Around the perimeter.
- Overlaps – to cover gaps.

Protection-In-Depth

- Use of multiple lines of detection.
- At least 2 = fail-safe.

Complementary Sensors

- Not only multiple lines, BUT multiple types.
- Different sensor technologies (different PD, NARs, VD).
    - Microwave/infrared, microwave/ported coaxial cable, ported coaxial cable/infrared.
- Patterns must overlap to be complementary.
- An alternative to dual technology sensors.

Priority Schemes

- Order of assessment for multiple simultaneous alarms.
- Priority based on the probability that an alarm event corresponds to a real intrusion.

Combination of Sensors

- Should have high Probability of Detection (PD)And Low Nuisance Alarm Rate (NAR).
- No single exterior sensor currently available meets both.
- OR gate/combinations:
    - Make up for each other's deficiencies.
    - Each sensor detects particular types of intrusions.
- AND gate/combinations:
    - Respond to different things.

Clear Zone

- Perimeter intrusion detection system performs best in an isolated clear zone.
- Zone usually defined by two parallel fences.

Sensor Configuration

- Overlapping – to create a larger overall detection volume.

Site-Specific System

- PPS designed for one site cannot be transferred to another.
- Demonstration sector on-site before committing.

Tamper Protection

- Tamper-**resistant**, Tamper-**indicating**.
- Line Supervision – detects if lines have been cut, disconnected, short-circuited, or bypassed.

Self-Test – ability to detect must be tested regularly.

Pattern Recognition – patterns that are particularly characteristic of an intruder.

Effects of Physical and Environmental Conditions

- can affect exterior detection systems and are different at every site.
  - Topography, Vegetation, Wildlife, Background noise, Wind.
  - Traffic – roads should be kept smooth and speed limit low.
  - Climate data, soil, concrete or asphalt.

Lightning Protection

1. Signal cables should be shielded.
2. Good ground system is needed.
3. Passive transient suppression devices at the ends of cables.

Fiber-optic transmission cables are not affected by lightning.

Integration with Video Assessment System

- CCTV is used for alarm assessment.
- Systems/subsystems must be compatible.
- Sensor engineers want wide area; Video engineers want narrow:
  - Compromise clear zone – 10 to 15 yards.
- Camera towers placed 1 to 2 yards inside the outer fence.

Integration with Barrier Delay System

- Barriers or access denial systems.
- Barriers installed on or near the inner clear zone fence.

Procedures (people, procedures, equipment)

- Procedures related to installation, maintenance, testing, and operation.
- Periodic maintenance – poor maintenance affects PD, NAR, VD.
- Operational tests – to verify sensor performance against DBT.
- Contingency plans – ie. Portable sensors, security officers.
- Key Documentation – troubleshooting, maintenance, training, etc.

Interior Sensors

- Unauthorized presence of insiders and outsiders.
- Clear and measurable specification for interior sensor performance.
- <u>Nuisance Alarms:</u>
    - Electromagnetic, acoustic, thermal, meteorological, seismic, optical effects, and wildlife.
- <u>False Alarms:</u>
    - Nuisance alarms generated by the equipment itself.
- Often placed in access mode during normal working hours, making them more susceptible to tampering.

<u>Classification:</u>

- Active or passive; Covert or visible; Volumetric or Line Detection; Application.

<u>Active or Passive</u>

- <u>Active</u> – transmit a signal from a transmitter and, with a receiver, detect changes or reflections of that signal.
        - Generate a field of energy.
        - Adversary can detect presence of the sensor.
    - <u>Bistatic</u> – transmitter and receiver separated.
    - <u>Monostatic</u> – transmitter and receiver located together.
- <u>Passive</u> – produce NO signal from a transmitter and are simply receivers of energy in the proximity of the sensors.
        - More difficult to detect.
        - Safer in environments with explosive vapors or materials because they do not emit energy that might ignite explosives.

<u>Covert or Visible</u>

- Covert - hidden.
- Visible – plain view.
    - May deter.
    - Easier to install and repair.

<u>Volumetric or Line Detection</u>

- <u>Volumetric</u> – entire volume or a portion of the volume of a room.
    - Will detect regardless of point of entry.
- <u>Line Detection</u> –line-type sensors that detect activity at a specific location or very narrow area.
    - Violating a specific entry point.

<u>Application</u>

- <u>3 classes</u>:
    1. Boundary-penetration sensors.
    2. Interior motion sensors.
    3. Proximity sensors.

Types of Intrusion Sensors (grouped by application):

Boundary-Penetration Sensors:

- Vibration and electromechanical technologies.
- Ceilings, floor, walls, and doors.

Vibration Sensors:

- Passive.
- Visible or covert.
- Detect movement of the surface to which they are fastened (surface vibration).
- Simple jiggle switches, complex inertial switches, piezoelectric sensors.
    - Inertial switches – a metallic ball mounted on metal contacts.
        - Ball looses contact with the mount – causing an alarm.
        - Typically detects vibration frequencies of 2 – 5 kHz.
    - Piezoelectric sensor – mounted on the vibrating surface and moves relative to the mass of the sensor body.
        - Flexes the piezoelectric element, creating a voltage output.
        - Detects vibration frequencies of 5 – 50 kHz.
    - Glass-break sensors – mounted directly on glass.
        - Detects frequencies associated with breaking glass.
          (normally above 20 kHz)
        - Introduces a vibration into the protected glass and listens for the signal received by another transducer.
        - Cost more but produce fewer nuisance alarms.
    - Newer Fiber-Optic Intrusion Sensors
        - Detects microbending of fiber-optic cable.
        - Microbending – minute movement of cable due to vibration.
        - A processing unit transmits light down the cable and receives it at the other end – detects changes in the light received.
        - Possible to use with Pulse Accumulator or Count Circuit.

Electromechanical Sensors

- Passive, Visible, Line sensors.
- Switch unit and a magnetic unit.
    - Switch unit – contains a magnetic reed switch.
    - Magnetic unit – permanent magnet mounted on the moveable part.
    - Can be defeated by using a strong magnet.
- Balanced Magnetic Switches (BMSs) – magnetic sensors with bias magnets.
    - Provide greater protection.
    - However, only activates if intruder opens door or window.
- Hall Effect Switch – new type of magnetic switch.
    - Completely electronic, without reed switches, requires power.
    - Higher level of security than balanced magnetic switches.
    - Measures and monitors the magnetic field strength of magnetic unit.
    - Harder to tamper with and defeat than BMS.

- Continuity or Breakwire Sensor – electromechanical sensor.
    - Can be formed in any pattern.
    - Wire must be broken to initiate alarm = fewer nuisance alarms.
    - Another version uses optical fibers instead of electrical wire.

Interior Motion Sensors

- Most common = Monostatic microwave sensors and Passive Infrared sensors.
- Microwave sensors are active, visible, volumetric sensors.
- Establish an energy field usually at frequencies of about 10 GHz.
- Usually in Monostatic configuration – single antenna for transmission and reception.
    - Intrusion detection relies on the Doppler frequency shift between transmission and reception caused by a moving object within the energy field.
- Optimum detection for microwave sensors – when target is moving toward or away from the sensor, NOT across detection zone.
- Microwave energy penetrates most glass, plaster, gypsum, plywood, and most normal wall construction.
    - Disadvantage – may detect something moving outside protected area.
- Monostatic microwave devices should be mounted:
    - Near the ceiling – aimed in direction of desired coverage.
    - No fluorescent lights within detection area.
    - Often used in automatic doors at supermarkets/airports.

Passive Infrared Sensors

- Visible and volumetric.
- Respond to changes in energy transmitted by a human intruder.
    - Equal to heat from 50-watt light bulb.
- Infrared Radiation – 4 main characteristics:
    1. Emitted by all objects.
    2. Transmitted without physical contact.
    3. Warms receiving surface – detected by device capable of sensing temperature.
    4. Invisible to the human eye.
- Passive Infrared sensor – thermopile or pyroelectric detectot that receives radiation from the intruder and converts it into an electrical signal.
- Detection is based on difference in temp. – Intruder and background.
    - Difference is Minimum Resolvable Temperature (MRT)
        - Some specify an MRT as low as 1 degree C (1.8 F).
- Infrared energy does not penetrate most building materials, including Glass.
- Installed away from heat sources.
- Be careful of sunlight heating surfaces – thermal gradients can cause nuisance alarms.

Dual-Technology Sensors

- Active and Passive, visible, and volumetric.
- Absolute alarm confirmation – achieved by combining two technologies each with a high probability of detection and no shared susceptibilities to nuisance alarms.
- Combines a microwave sensor with a passive infrared sensor.
- Alarm is produced only after nearly simultaneous alarms from both.
- Dual technology should NEVER be used in place of two separately mounted sensors.
- Probability of detection:
    - Microwave – motion directly toward or away from sensor.
    - Infrared – motion across the field of view.

Video Motion Detection (VMD)

- Passive sensor that processes the video signal from a CCTV camera.
- Analog and Digital:
    - Analog – detects changes in brightness in the video scene.
    - Digital – digitizes the signal and processed digitally.
        - Divides scene into cells.
        - Cells are monitored for changes in brightness or contrast, logical movement across cells, speed, size of objects, and global changes.
- VMDs are effective for interior use.

Proximity Sensors

- 2 types – Pressure mats and Capacitance sensors.
- Pressure mats – virtually obsolete.
    - Version of mat still in use = weight transducer.
        - ie. Weight of individual vs. access card presented.
- Capacitance sensor
    - Large electrical condenser that radiates energy and detects change in the capacitive coupling between an antenna and the ground.
    - Capacitance sensor wire is connected to an object to be protected, such as a safe or file cabinet.

Wireless Sensors

- Radio frequency (RF) – typically in US = 300 MHz or 900 MHz bands.
- Consists of sensor/transmitter units and a receiver.
- Raises concerns of collisions, signal fade, and interference.

Other Interior Sensor Concepts

Environmental Conditions

- Outside noise sources can degrade sensor performance.
- Environmental conditions that can affect **Interior** sensors:
    - Electromagnetic energy – interference.
        - Minimize: Electromagnetic shielding to system components.
    - Nuclear radiation – can damage various sensor components.
    - Acoustic energy – may affect performance.
    - Thermal environment – uneven temperature distribution.
    - Optical phenomena – sensors may be affected by light energy.
    - Seismic phenomena – vibrations.
    - Meteorological phenomena – can affect interior intrusion sensors.

Sensor Selection

- Consider interaction among equipment, environment, and potential intruders.
- Construction of building, equipment/objects that occupy the space.

Procedures

- Can increase system effectiveness, such as 2-person rules.
- 2-person rule – requires that 2 people be involved in a situation or activity to prevent compromise by a single insider. (ie. Granting access).

Testing Mechanisms

- Audible/visible alarm – recognized from a distance of 10 to 35 feet.
- Walk tests every day.
- All sensors - Performance tested after maintenance.
- Random tests.

Inspection - after maintenance.

- Security involved with plant modification.

Documentation

- – theory of operation, functional block diagrams, cabling diagrams, schematics, parts lists, maintenance logs, etc.

System Integration

- combining technology elements, procedures, and personnel into a single system.

Line Supervision

- A way to monitor the communication link between a sensor and the alarm control center.
- If numerous interior sensors are connected to a single alarm processor, line supervision is required between the processor and each detection sensor.

Summary

- Sensor classification and application, PD/NAR/VD.
- Design goals, balanced and integrated PPS, clear zone, tamper protection, integrated with video and barrier subsystems.

CHAPTER 5 VIDEO SUBSYSTEMS AND ALARM ASSESSMENT

Designing a CCTV application:

- CCTV is a visual tool.
- **Application dictates the equipment, not the other way around.**
- The system will become obsolete but not necessarily ineffective.
- Design with potential future growth or changes.

Theory of Visual Security

- Video motion is an illusion – sequence of images that the brain perceives as movement.

<u>Analog systems</u> – horizontal and vertical sweep lines meet at a:

    - Point or pixel of energy.
    - More pixels = better overall resolution.
- Vertical resolution is restricted by NTSC or PAL standards:
    - National Television Standards Committee (NTSC).
        - 60 fields per second at 525 vertical lines
    - Phase alternation line (PAL).
        - 50 fields per second at 625 vertical lines.
- Horizontal resolution is limited only by camera imager, monitor, and bandwidth of the transmission and recording medium.
    - Most common measurement of quality and detail in an analog image.
- All analog CCTV monitors and cameras employ a 2:1 interlace pattern.
- Odd and even numbered horizontal sweep lines:
    - 60 fields (half pictures) of information per second;
    - viewer sees 30 complete frames.

<u>Digital video technology</u> – full grid of small, colored squares or pixels.

- Measured in terms of images or frames per second (ips or fps).
- Not held to NTSC or PAL standards but instead to various digital standards established for visual media.

Use of Video Subsystems in Security

CCTV systems = visual assessment or visual documentation tools.

- <u>Visual assessment</u> – having visual information of an identifying or descriptive nature during an incident.
- <u>Visual documentation</u> – having visual information stored in a format that allows the study or review of images in a sequential fashion.
    - Includes various embedded authenticity points, such as time/date stamp or character generation.

<u>3 Reasons to have cameras:</u>

1. Obtain visual information about something that **is happening**.
2. Obtain visual information about something that **has happened.**
3. To **deter** undesirable activities.

Base camera selection on camera's sensitivity, resolution, features:

- Sensitivity – minimum amount of visible light necessary to produce a quality image.
- Resolution – image quality from a detail or reproduction perspective.
- Features – the aspects that give one camera an advantage over another.
    - Video motion detection, dual scanning, and built-in character generation.
- **Camera should be chosen BEFORE the lens.**
- Common to use different cameras – verify compatibility of language and format.
- Incompatibility mostly affects digital systems.
- Lenses – determine what amount and type of image will appear on monitor.
    - Subject identification, action identification, and scene identification.

<u>Subject Identification</u>

- Visual information must be sufficient for identification.
- How the camera's angle of view affects the results available from CCTV system.
- Depends on the size and detail of an image; and the angle of view.
- Object should occupy at least 10% of the scene's width.
- Based on a minimum 325 horizontal line resolution – Television quality.

<u>Action Identification</u>

- Captures what happened.
- CCTV systems should be automated through a trigger:
    - Video motion detection, pressure on floor mat, or breaking of photoelectric beam.
- The system records important actions and captures useful evidence.

<u>Scene Identification</u>

- Each scene should stand on its own merit.
- The angle of view and the pixels per foot or meter dictate the placement and selection of cameras and lenses.

ANALOG System Components

3 main components:

1. Camera – transforms a reflected light image into an electronic signal.
2. Transmission Cable – transmits the electronic video signal from the camera to the monitor.
3. Monitor – used to translate the video signal into an image on a screen.

Other parts of ANALOG video system:

- Pan or pan/tilt unit
  - Pan unit moves camera – side to side.
  - Pan/tilt unit moves camera side to side and up and down.
    - Single unit protected inside a dome (Auto-dome).
    - More cost effective to use several fixed cameras.
- Alarm Interfacing – an event is used to trigger a response from the camera system.
- Pre-positioning – directs camera to return to a particular pan/tilt and zoom position when a signal is tripped.
- Controller – commands a function of pan unit, pan/tilt unit, automatic lens.
- Switcher – shows the display from several cameras on a monitor.
  - Dwell time – time a sequential switcher automatically switches from camera to camera.
  - Sequential switcher – automatically switches from camera to camera.
  - Quad Splitter – displays 4 images on a single screen.
  - Multiplexing Switcher – interacts with system's video recorder to store more information per camera.
    - Can play back video separately or in quad format.
  - Matrix Switcher – can organize large groups of video inputs and outputs and integrate them with alarms and viewing options.
- Lens – focuses light onto a chip or tube within a camera.
- Video Transmitter/Receiver – allows the video signal to be transmitted via a cable, phone line, radio waves, light waves, or other means.
  - Coaxial Cable – most common.
  - Fiber Optic Cable – outside. Uses two-wire (twisted pair)transmission.
- Amplifier – strengthens the video signal for long distance runs.
  - Avoid amplifiers when possible as they are not usually balanced.
  - Better to replace coaxial with: Fiber Optic, microwave, or two-wire.
- Video Recorder – retains the video information.
  - Features include: time-lapse, event-triggered, 24 hr., 72 hr., etc.

***** Application drives the choice of equipment. *****

DIGITAL System Components

The term CCTV will change to:

- Digital Imaging System (DIS), or
- Visual Imaging System (VIS).

<u>3 main parts:</u>

1. Camera.
2. Digital electronic signal carrier (ie. Cat 6e cable or digital network).
3. PC with viewing or recording software (sometimes accessible via Web browser or remote device – smartphone or tablet).

<u>Other parts of a DIGITAL video system:</u>

- <u>Digital electronic scanning software</u> – programs that allow a fixed, megapixel camera to appear as if it were a mechanical pan/tilt device.
    - Scans across the imager, as opposed to physically moving the camera.
- <u>Controller</u> – computer programs that work with a joystick or mouse.
    - Many IP cameras use GUIs.
    - IP = Internet Protocol – language for digital transmission.
    - GUI = Graphical User Interface – visible screen.
- <u>Switcher</u> – digital CCTV uses three types of switching:
    1. High speed analog to digital converter (encoder) that accepts multiple analog signals and outputs a single Multiplexed digital signal.
    2. High speed digital switcher that in essence is a Multiplexer.
    3. Some DVRs contain built-in multiplexers.
- <u>Lens</u> – one of the few elements NOT converting to digital.
- <u>Video Transmitter/Receiver</u> – Ethernet is most common though not always the best application for all cameras in a system.
    - Outside run on Fiber Optic cable that uses two-wire transmission.
    - RG-59/U, RG-6/U and RG-11/U coaxial cables can be used to carry a digital video signal via specialized signal modification equipment.
- <u>Amplifier</u> – Repeaters in the digital world.
    - Digital signals are binary codes that do not require amplification.
    - Maximum cable length for digital transmissions is 100m or 312 feet, unless wireless, microwave, fiber optics, modified coaxial, etc. designed for long distance transmissions.
- <u>Video Recorders</u>
    - DVRs are NOT true digital recorders – they accept and output Analog.
    - DVRs are being replaced by massive hard drives or digital based storage systems.
- <u>Multiplexing</u> – combines the signals from several video cameras into a single data stream.
- <u>Carrier</u> – the electronic signal on which the digital stream or sequence of electronic commands rides.

System Design

- Not as complicated as they appear.
- Camera, cable, monitor – anything else is peripheral.
- Let the application choose the equipment.
    - Determine the needs first.
- Design generically – open based on site or scene requirements.
- Design for the best option first – then adjust for budget.
- Don't feel as though it all has to be built at once.
    - Installation may be stretched out over time.

Step 1: Write the Purpose of the Proposed CCTV System

- write out the purpose.
- If used for other than security, split the costs with other departments.

Step 2: Write the Purpose of Each Camera in the System

- Security risk of each area.
- High security – interface with an alarm device.
- Visible or covert – be aware of privacy rights.

Step 3: Define the Areas to be Viewed by Each Camera

- Height and compass points (ie. 30 feet high, N/E corner of building.

Step 4: Choose a Camera Style

- Based on sensitivity, resolution, features, and other design factors.
- Sensitivity – minimum amount of light required by camera to produce an image. Lighting in the area.
    - Exterior – lighting study using a good light meter.
    - Consider visible and Infrared (IR) lighting – not visible to human eye.
    - 3 basic sensitivities – full-light, lower-light, and low-light (most $$$).
- Resolution – number of horizontal scan lines or digital pixel arrays that the camera captures. Critical measure of picture quality.
    - Analog = number of horizontal scan lines.
    - Digital = number of pixels per sq. ft. or meter.
    - Viable visual evidence.
    - Desired identification information.
    - High Density Video (HDV) – international standard of 1080p.
        - 1080 pixels on a 16:9 ratio.
    - Megapixel – imager made up of millions of pixel points.
    - 7 theoretical identification views:
        - General – 5 pixels/ft.
        - Monitor – 7 pixels/ft.
        - Detect – 11 pixels/ft.
        - Observe – 18 pixels/ft.
        - Recognize – 35 pixels/ft.
        - Subject Identification – 46 pixels/ft.
            - Analog view – subject is 20% of overall scene width based on min. 325 horizontal line resolution.
        - License Plate Identification – 70 pixels/ft.
        - Facial Recognition – 88 pixels/ft. – extreme detail.

Features of CCTV cameras:

Automatic Gain Control (AGC) – internal video-amplifying system in cameras that maintain the video signal at a specified level as the amount of available light decreases.

- All outside cameras – should have AGC switched ON.
- AGC increases noise in the video picture by a factor of 10.
- AGC sensitivity should not be confused with its general sensitivity.

Electronic Shuttering – manual or automatic. Ability to compensate for light changes without automatic or manual iris lenses.

- Same as eyeglasses that turn dark in sunlight.
- Reduces amount of light that reaches the camera's imaging.

Backlight Compensation – subject in front of bright background.

- Auto-iris lens – most common tool to control brightness of image focused onto a chip.
  - As video signal increases or decreases, the auto-iris lens closes or opens in direct proportion.
  - Ensures video image remains at average of one volt peak-to-peak (vpp).
  - Cannot keep up with everyday application.
- Masking – digital interfacing with the video signal. Built into specific cameras and controllers.
  - Divides video image into grid sections.
  - Various sections are programmed to be ignored.
- Electronic Iris – first true method of digital signal enhancement that obviates the need for auto-iris lenses.
  - Works on true video signal averaging.
  - De-amplifies the super-brights and amplifies the sub-blacks, creating an equal 1 vpp video image.
- Super Dynamics (Panasonic) – this analog method of electronic backlight compensation double-scans the CCD.
  - In digital cameras – referred to as multi-scanning.
- Auto focus – ability to focus on a scene automatically.
  - Camera and lens work in concert.
  - Dome covers can interfere with auto focus.
- Privacy Blocking or Image Protection – digital effect to obscure a specific area within an image.
  - Locked positioning – ability to pan/tilt/zoom while continuing to mask the desired area.
  - Flexible drawing – ability to mask a section regardless of size/shape.
  - Password protection – against unauthorized reprogramming.
  - Ability to temporarily remove mask or view through it during playback.

Other design factors:

Environment – protected, blend in, excessive dirt or dust, sun shield.

- Temperatures below 35F – housing will need a heater.
- Temperatures above 80F – fan or possibly an air conditioner.

Mounting – maintenance, camera angle, distance.

- Should not auto pan (side-to-side) more than 45 degrees from center of major focus.
- High security locations = 4 analog cameras to view a 360 degree area.
    - Digital technology = megapixel 180 degree and 360 degree cameras.

Step 5: Choose the Proper Lens for Each Camera

3 different factors: camera format, distance from camera to scene, field of view.

Format Size – size of the imager area onto which the lens focuses light.

- Measured diagonally.
- If format size too small – will resemble tunnel vision.

Distance from Camera to Scene – determines focal length of lens.

- Pythagorean Theorem A2 + B2 = C2

Field of View – height or width of area being viewed.

- More area = less detail.
- Megapixel technology – larger area without losing detail.

Step 6: Determine the Best Method for Transmitting the Video Signal from the Camera to the Monitor.

- Coaxial cable is generally sufficient.
- Distances of 1,000 feet = best to use Fiber-Optic cable.
- System may use more than one method of video transmission:
    - Coaxial cable, fiber-optic cable, twisted pair (two wire), Cat 5 or Cat 6 (networking) cable, microwave, RF (wireless), IR technology, transmission over telephone lines, Internet, Intranet.

Step 7: Lay Out the Control Area and Determine What Enhancements are Needed Based on each Visual Assessment Point's Requirements

- assign triggers and priorities and determine which features the control equipment must have.
    - Helps automate the video system.
- Recording or storage system is also needed.
    - Preference to digital recording.
    - DVRs – analog based cameras only.
    - NVRs (Network Video Recorders) – analog, IP, or hybrid.
    - Internet (cloud storage) – server or network, or off-site.

Equipment Selection

- Define the operational parameters required by the application.

Cameras

4 main types:

Standard Analog Cameras

- May or may not have digital effects.
- Work well in all indoor and many outdoor applications.
- Light sensitivity = .005 lux to 10 lux (very high).

IP Cameras

- Require visible light to create an image.
- 3 styles: Standard, Megapixel, and Smart.
- Measure their resolution as a multiple of the Common Intermediate Format (CIF), which is a resolution of 352 x 240 (352 pixels horizontal/ 240 Verical.
- Referred to as "edge devices" because they take the computing factors or features to the outer edge of the system as opposed to sending the information to the controller to be deciphered.
- Powered via transformers OR
- Power Over Ethernet (POE) – receive their operational power from the digital switching system via the network.

Infrared (IR) Cameras

- Require an IR light source.

Thermal Cameras

- Require no visible or IR light.
- Monitors the temperature of objects.
- Temperatures represented by colors – Cold/Blue, Hot/Red.

Lenses

Second most important decision.

- 5 main types:
    - Wide-angle lens – short ranges, 0 to 15 feet.
    - Standard lens – equivalent to human eye – 15 to 50 feet.
    - Telephoto lens – narrow area at long range – over 50 feet.
    - Zoom lens – incorporates moving optics that produce the same views provided by wide-angle, standard, and telephoto lenses ALL in one device.
        - Tracking mechanism – physical tie between the focal optics and the zoom optics – automatically adjusts the focus as the lens is zoomed out (telephoto to wide-angle).
    - Varifocal lens – smaller version of manual zoom lens.
        - Tune the view on-site.
        - Do not have tracking mechanisms.

Compatibility Between the Lens and the Camera.

1. Will camera be installed in area where lighting is fixed, minimally variable, or highly variable?
    - Determines if application requires a lens with a fixed iris, manual iris, or auto iris.
    - Lighting has the greatest impact on performance.
2. Is the camera ¼ in., ½ in., 2/3 in., or 1 in., or megapixel format?
    - Format size of the lens must equal or exceed the format size of the camera.
3. Is the camera a color camera?

    If so, a color lens must be used.
4. Is the camera C or CS standard camera?
    - CS cameras – late 1990s – do not penetrate as deeply into camera.
5. Will camera accept an AC/EC (video) or DC/LC lens?
    - Cameras designed since 2002 only accept DC/LC.
6. Is the camera a megapixel camera?
    - Megapixel lens is much higher quality.
7. Does the application use infrared (IR) enhancement lighting?
    - Camera specification sheets – which lenses the camera will accept.
    - Lens specification sheets – whether the lens will live up to the demands of the camera.

Camera Formats and Lenses

- The key is to know what the standard lens for the camera is and calculate from there.
    - 25mm lens = Standard lens for 1 inch camera.
- Field of View – final size of the viewing area measured in width and height.
- Resolution of digital camera – measured in terms of Common Intermediate Format (CIF).
- Resolution of Image – determined by:
    - 1. Camera, 2. Transmission method, 3. Weakest link in video system interface, 4. Reproduction capability of the image storage system.
    - Higher resolution = sharper image.
    - Analog video recorders average playback of 325 horizontal lines.
    - Multiplexers – another source of loss – up to 25% of resolution.
    - Coaxial cable – can cost another 10 to 15% of resolution.
    - Digital Resolution – unlimited and extremely flexible.
    - H.264 – most effective compression standard in digital imaging market.
    - Once an image is compressed – very seldom able to be returned to original quality or detail.

Controlling Software

- Tied directly to a DVR (analog), NVR, or Server.

- Node – a central point for individual pieces to come together for insertion into a network path. Most cameras are cabled to nearest node.
- Home run – cabled directly to central control point.
- Network Path – central connection between all field nodes and the head-end.
- Consideration must be given to how much equipment will be connected at each node.
- Will cameras be viewed at more than one point, and will they have separate controlling capabilities?
  - Cabling requirements, bandwidth requirements, software requirements.
- Interfaced alarm trigger points:
  - Allows user to concentrate on other tasks until alarm is triggered.
  - Door contacts, IR motion detectors, and photo beams.
- Will the switcher be required to trip other devices (buzzers or alarms) in the event of an alarm?
  - Email, text, or video image to a portable device?
- Future expansion – can network and nodes handle the expansion?
  - Plan ahead.
- Type of Monitoring Station – rack mounted, table, or desktop application.

Recording Systems

Is system's purpose to verify information, prove it, or aid in prosecution?

- Determines type of video imaging, degree of quality or resolution, and number of images per second/per camera that are best for the situation.
- To save space
  - Reduce the number of images per second.
  - Reduce the amount of resolution required (via compression factors).
  - Reduce the amount of recording time per unit (via triggers).

Types of Recorders:

- Digital Video Recorders (DVRs) – converts analog signals to digital format.
  - Compresses the video image using a particular Codec (a compression engine or command sequence that causes the unit to combine colors, drop resolution, or both).
    - Once compressed, image quality may be poor.
- Network Video Recorders (NVRs) – Digital – accept digital or analog signals.
  - Much better than DVRs. Can handle several hundred cameras.
- Server/Cloud Applications – Digital
  - For systems that require sophisticated software applications for control, analytics, or other intricate interfacing.
  - Very large systems – incoming digital signals are compressed and stored in complex levels on servers.

Additional Design Considerations for Video Assessment

- Video assessment system designed as a component of the total intrusion detection system.

Site/Sector Layout

- Perimeter assessment – display as much as possible of the clear zone, including inner and outer fences.
- Each exterior assessment zone should use one fixed camera per zone.
    - Provides assessment capability.
    - Simplest if each alarm is assessed by only one camera.

Video/Sensor Interface - Interference that could cause nuisance alarms.

Monitor Location - that allows effective, rapid assessment.

Construction – Installing signal and power distribution cables and modifying buildings for equipment installation.

- Include room for system expansion.

Alarm Assessment by Response Force

- Most effective if assessed quickly after being reported.

Integration with Safety Systems

- Separate these functions so that security is not distracted by safety events.
- Could mask an attack and compromise security system effectiveness.

Legal Issues

- Privacy – places where there is a reasonable expectation of privacy.
- Liability to use "Dummy cameras" – establishes an expectation of protection.
- Recorded video must meet standards to be admissible.
    - Unique scene identifier.
- Electronic images – use digital watermarks.
    - Various levels of legal acceptance.

Procedures

- Camera selection based primarily on sensitivity required for full video output signal in the lighting environment in area to be assessed.
- Next is the Resolution Imager – determines number of cameras required.
    - Greater the resolution – greater the spacing between cameras.
- Camera format size determines the sensitivity of the image tube.
- Evaluate cameras under real lighting environment expected.
- Consider difficulty of maintenance, packaging of the camera based on environment, manufacturer support, and documentation support.

Acceptance Testing

- Incoming inspection before final system installation.
- Evaluation cameras compared to other cameras.
- Determine conformity with: specifications, compatibility, consistent performance.
- Exterior cameras – appropriately sized targets in assessment zones to verify they can be classified.
- Size of target can be varied – resolution charts can be used.
- Rotakin – to determine resolution.
- Determine resolution needed before buying the cameras.
- Verified in laboratory using a test bench.
    - Can be more cost-effective than performance testing.
- Exterior lighting surveys – using high-quality light meters.
    - Repeated yearly.
- Speed of video subsystem tested to verify alarm sensing and video capture occur rapidly – to capture the actual intrusion event.
- Adequacy of resolution, speed of recording, number of alarms that can be acquired in one second.
- Periodic maintenance as per equipment manufacturer.
- Always check equipment after maintenance.
- Equipment logs/Maintenance logs – repair or replacement.
- Spares – 10 to 20% recommended, especially for cameras.
- Contingency plans if CCTV capability is lost.
- Manufacturer's equipment documentation – stored at using site and central document storage location.

Evaluation of Video Assessment Systems – to determine effectiveness.

- Minimum time between sensor alarm and video display.
- Complete video coverage.
- Ability to classify category of a 1 foot target at far edge of assessment zone.
- Minimal sensitivity to environmental conditions.
- Minimal obscuration of assessment zone (trees, etc.).
- Camera field of view.
- Verify operational and time/date stamps or other text messages.
- Test targets to verify image quality– based on horizontal field of view of 6 horizontal television lines (HTVL) per foot.
    - Painted black on one side and white on other to check image resolution in dark and bright spots.
- Lighting, camera mounting, transmission system, integration of switchers and controllers.
- Far Field – the furthest distance from the camera.
- Likely that recorded image will not have same resolution as live image.

Future of CCTV

- Becoming obsolete – replaced with Digital Imaging Systems (DIS).
- Full facial recognition.

CHAPTER 6 LIGHTING

The Study of Lighting:

- Lighting science and technology.
- Electrical systems.
- Aesthetic design of fixtures and socioeconomic considerations.
  - Cost, light trespass, chemical effects (ie. Mercury).
- Requires an appreciation of the subjective reaction of people to different lighting environments.

<u>Security Lighting – 3 primary functions:</u>

1. Deterrence to criminal activity.
2. Life-safety functions (pathways and parking lots).
3. Lights an area for the use of video subsystems.

Lighting and Lighting Definitions

<u>Lumens</u> – quantity of light emitted by a lamp.
(100w bulb = 1700 lumens)
<u>Spotlight</u> – concentrates output in a small area.
<u>Floodlight</u> – disperses light over a larger area.
<u>Illuminance</u> – concentration of light over a particular area.

- Measured in lux:
  - Number of lumens per square meter, or
  - In foot-candles – number of lumens per square foot.
- One foot-candle = 10.76 lux (often approximated to 1:10).

<u>Sensitivity of a CCTV camera:</u>

- Minimum amount of illumination required to produce a specified output signal.
  - Usually specified as the minimum illuminance level that will produce a full 1 volt peak-to-peak video signal.
  - Scene illuminance OR the faceplate illuminance.
  - Illumination source is usually an incandescent lamp operating at a color temperature of 2,854 degrees Kelvin.

The amount of light necessary to produce a useable video signal from any video camera is a function of:

- Type and brightness of the source.
- Amount of light energy illuminating the scene.
- Portion of light reflected from the scene.
- Amount of light transmitted by the lens to the imager.
- Sensitivity of the imaging device itself.

Successful deployment of a CCTV system:

- Relative levels of scene illumination produced by:
    - Natural sources
    - Light reflected from typical scenes.
    - Resultant faceplate illumination levels required.

50,000 foot-candles = Upper limit of visual tolerance.
0.000001 = Absolute limit of seeing.

Reflectance – Percentage of light reflected from a scene.

- depends on incident light angle and on the texture and composition of the reflecting surface.

2 most important parameters of a lighting system for CCTV:

1. Minimum Intensity – must be great enough to ensure adequate performance of the chosen camera system.
2. Evenness of illumination – characterized by light-to-dark ratio (maximum intensity to minimum intensity).
    a. Design ratio of 4:1 is preferred.

Cameras are light-averaging devices:

- Entire field of view should be illuminated evenly, not assessment area alone.
    - Contributes to light-to-dark ratio.
    - Lighting survey to determine a baseline light-to-dark ratio.

Corrected Color Temperature (CCT)

- Measure of the warmth or coolness of a light.
- Measured in: degrees Kelvin (which is centigrade Celsius).
    - Red hot = above 2700 degrees Kelvin.
    - White hot = approx. 4100 degrees Kelvin.
    - Blue hot = approx. 5000 degrees Kelvin (similar to daylight).
- Warm: 3000 degrees Kelvin.
- Neutral = 3500.
- Cool = 4100.
- Daylight = 5000.

- Low pressure sodium lamps – 1750 K
- High pressure sodium lamps – 2000 K

<u>Color Rendition</u> – ability of a lamp to faithfully reproduce the colors in an object.

- Measured as a Color Rendition Index (CRI) – scale of 0 to 100.
    - CRI of 70-80 = good, above 80 = excellent, 100 = considered daylight.
- High and low pressure sodium and mercury vapor light sources have very low CRI values and should NOT be used with color camera applications.
    - Low pressure sodium light – green shirt will have a blue hue.
- High CRI increases visual clarity.
    - Higher morale and greater productivity
    - Outdoor location at night = see at greater distance and better depth perception.
- <u>Brightness</u> – human perception of the amount of light that reaches one's eye.
- <u>Glare</u> – Excessive brightness.
    - Hurts the eye and affects eye's efficiency.
    - Can be used to deter unauthorized activity.
    - May cause light trespass.

Lighting Systems

<u>Lamp</u> – (light bulb) – filament or arc tube, glass casing, and electrical connectors.

- Incandescent, high or low pressure sodium, mercury vapor, light emitting diode arrays (LED), etc.

<u>Luminaire</u> – (fixture) – complete lighting unit.

- lamp, holder, reflectors, diffusers (used to distribute and focus light).
- Means of connecting to the power source.
- <u>Ballasts</u> – to generate the correct starting and operating voltage, current, and waveform.
- <u>Photosensors</u> – to control switching of lights based on ambient lighting conditions.

<u>Mounting Hardware</u> – wall bracket or light pole.

<u>Electrical Power</u> – operates lamp, ballasts, and photocells.

- some lamp technologies are sensitive to reduced voltages:
    - example: High Intensity Discharge (HID) family of lamps.
        - Metal halide, mercury vapor, high-pressure sodium.
- Consider backup batteries, generators, and Uninterrupted power supply (UPS).

Lighting Economics

- Cost of lighting:
    - Capital items (8% of cost).
    - Maintenance (4% of cost).
    - Energy (88% of cost).

- Energy efficiency of the lighting – lamp's efficacy.
    - Measured by the lamp's output in lumens divided by the lamp's power draw in watts.
- 8760 hours in a year (8 hours per day = 2920 hrs. per year).
- Lumen output of lamp will decline due to dirt.
    - Power consumption remains the same.
- Clean environments – output declines 3 to 4 percent per year.
    - Performance of most lamps declines with age.
- Highest cost – Incandescent.
- Lowest cost – Low-pressure sodium.
- Less expensive in labor to perform a planned replacement of all or group.
- Uniformity:
    - Some variation in light levels is acceptable and measured as uniformity – the ratio between the average light level and the minimum light level.

Starting and Restrike

- time to relight.
- High-intensity (HID) – extended relighting time:
    - Since they rely on an arc to produce light.
    - HID and fluorescent – take time on starting from cold to reach their designated light output levels.
        - Fluorescent – especially in cold weather.
        - Some HIDs have two tubes to reduce these times.
- Incandescent, Halogen, Fluorescent – Instant start times.

Security Lighting Applications

General rule:

- 0.5 fc for Detection.
- 1.0 fc for Recognition.
- 2.0 fc for Identification.

Perimeter Fencing

- Deterrent.
- Aids in CCTV alarm assessment.
- Consider light trespass on property of neighbors.

Site landscape and perimeter approaches:
Vertical lighting – shining onto the horizontal walkway or roadway.
Horizontal lighting – pedestrians to see each other.
Ground lighting – focused up into trees to prevent hiding places.

Building façade – if good reflectance, there will also be horizontal light.

Parking Structures – lack of ceiling clearance restricts the height of luminaires (fixtures) – requires the fixtures to spread the light horizontally.

Open parking – higher light sources provide horizontal illumination.

- be aware of light trespass.

Loading docks – nighttime lighting for off-hours activity.

Security Control and Monitoring Rooms
Minimize glare – positioning of luminaires and angle of screens.

- flat screens or anti-glare coatings or covers.
- Reduce ambient light levels to minimize glare and increase contrast.

Guard and Gate Houses

- lighting reduced at night to below exterior levels to permit good visibility.
- Increased lighting increases security.

Security Lighting and Closed-Circuit Video Systems

Consider:

- Color Rendering Index (CRI) for accurate reproduction and identification of colors.
- Reflectance of materials.
- Directionality of the reflected lighting.

<u>Wavelength of Source Illumination:</u>
<u>Visible spectrum</u> – human eye.
<u>Electromagnetic spectrum</u> – human eyes not sensitive to it.
<u>Infrared (IR) light source</u> – camera requires a special sensing element such as:

Ex-wave CCD – allows views even where there is no visible light.

- restricts light trespass and provides covert surveillance.
- Monochrome only – NO color
- IR can be mounted on pan/tilt mechanism to follow direction of camera.

Color cameras require twice the light as monochrome cameras for same quality.

Minimum light levels for specific lens characteristics – minimum illumination.

<u>White balance</u> – automatic adjustment within a camera for the color temperature of the light source.

Standards for Security Lighting Levels

- first national standard issued in 1942.
- Illuminating Engineering Society of North America (IES).
    - ANSI A85.1
    - *Lighting handbook.*
- U.S. Army Field Manual.
- Nuclear Regulatory Commission (NRC).
    - Governs licensees who possess special nuclear materials.

CHAPTER 7 ALARM COMMUNICATION AND DISPLAY

AC&D – The part of a PPS that transports alarm and assessment information to a central point and presents the information to a human operator.

- decision is made as to what actions are needed.
- 2 critical elements:
    - Transportation and communication of data.
    - Presentation or display of that data to a human operator.

Attributes

- Designed to withstand environment.
- Robustness – measure of system performance in all probable environments.
- Reliable and long Mean Time Between Failure (MTBF).
- NO communication system is 100%.
- Provide redundancy and backup capabiltity for critical components.
    - Robustness Reliability Redundancy.
- AC&D speed should be a negligible factor in calculating response or assessment times.
- AC&D system speed is a measure of its effectiveness.
- System must be secure – information, components, and wiring.
- Easy for an operator to use – not overwhelming.
    - Reduces amount of training and retraining necessary.
- Most important measure – how well it quickly and clearly communicates alarm data from sensors to system operator:
    - Where occurred, who/what caused alarm, when.
- Human factors: Ergonomics, human factors engineering, physiology.
- AC&D system is divided into several subsystems:
    - Communications.
    - Line supervision and security.
    - Information handling.
    - Control and display.
    - Assessment.
    - Off-line subsystems.

Alarm Communication Subsystem

- Transfers data from one physical location to another.
    - Collection point (sensors) → Central repository (display).
- Characteristics: quantity of alarm data, high reliability needed for the system, and speed at which data must be delivered.
- Assured Message Delivery – communication must be reliable and timely.
- Human factors require alarms to be reported with no perceptible delay.
    - Few tenths of a second.
- Physical media – must have sufficient bandwidth to handle communications.
- Protocols – special set of rules for communicating:
    - used by end points in a communication system when sending signals back and forth.

- System speed – dictates the types of protocols used in the system.
    - Protocol overhead – must be appropriate for type of data being transmitted.
- Channel Bandwidth and Protocol Overhead – must be balanced to provide the required system speed.
- Balance between cost of system and performance.
- Redundant hardware is required – with automatic message routing.

Security Communications

- Communications media of choice is Optical Fiber or satellite rather than copper wire.
    - Less expensive and provides security, high-speed transmissions, and versatility. Cable of choice for terrestrial communications carriers.
    - Satellite technology – versatile and useful in developing areas.

Concerned with:

- Integrity of communication medium (availability of the message path).
- Integrity of the message (complete and errorless transmission of data).
- Timeliness of the transmission (data comm. – appropriate time frame).
- Message security (accessibility of the comm. to authorized persons only).

Wire and Cable Communications

- Alarm signals may be transmitted on an unshielded pair of direct current (DC) conductors.
    - Size of wire and resistance must be considered.
    - Effective length of line is limited by the wire resistance.
        - Resistance varies directly with length.
        - Inversely with the diameter of the wire.
- Audio transmissions require use of shielded twisted pairs of alternating current (AC) wires (referred to in telephone parlance as voice-grade lines).
    - Alarm signals and audio transmissions can both be transmitted on AC.
- Signals can also be transmitted on lines installed to carry electric power.

Optical Fiber

- Transmit extremely large volumes of information at the speed of light.
- Can support any combination of video, data, and audio transmitted.
- Strand of high-purity spun glass.
- Light source such as laser or light-emitting diode (LED).
- Carried to the other end – modulated beam is decoded.
- LED is preferred light source.
- Not affected by electromagnetic interference (EMI).
- Not affected by radio frequency interference (RFI).
- Does not carry electrical current and does not radiate signals.
- Much smaller and flexible.
- Not vulnerable to interception by acoustical or inductive coupling.

Video Transmission

- Transmitted on coaxial and optical fiber cable, standard telephone lines, or on balanced twisted-wire pairs.
- Coaxial – video signal does not require further processing.
  - Amplification required over 1000 ft.
- Normal telephone circuits – transmission is first converted to digital, then to audio signals, and reconverted to video at receiving end.
- Optical fiber – converted from video to optical signal at transmitter and reconverted at the receiver.
  - Transmission distance without amplification is 1 mile.
- Systems support monochrome or color.
- Data signals to control equipment (ie. PTZ) transmitted over same optical fiber. Simultaneously in two directions on one fiber.
- Dedicated twisted-pair wires – up to 4,000 feet.

Status and Alarm Transmission

- 3 types of line transmission installations: Loop, Point-to-Point, Multiplex.
- Loop – installed on a pair of wires, looped through building, connected to control center.
  - Short circuit or broken connection in loop may interrupt all signals.
  - Can be partially corrected using a McCulloh circuit where the circuit is switched to send current from the control unit over both sides of the circuit wires out to the break point.
- Point-to-Point – each sensor connected directly to control center by a pair of wires.
  - More expensive but only one detector is influenced by a line fault.
  - Better than Loop where all detectors could be disabled by interrupting the loop.
- Multiplexing – technique to transmit several messages simultaneously on same medium - Wire, Radio frequency (RF), microwave, or optical fiber.
  - More cost effective installation but multiplexing equipment is expensive.
  - Interruption results in all signals interrupted on that link.
    - Redundant path can be an alternate multiplex trunk.
  - Individual signals must be separated so they do not interfere with each other, by either:
    - Time separation or Time Division Multiplexing (TDM).
      - Each sensor is assigned a time segment to transmit.
      - Same transmission path but not simultaneously.
    - Frequency separation or Frequency Division Multiplexing (FDM).
      - Signals occupy different portions of the frequency spectrum kept individually identifiable at receiver.
      - Example: system where three transducer outputs modulate three subcarrier frequencies (730 Hz, 560 Hz, 400 Hz) – unused guard bands ensure separation.

Wireless Communications

Requires:

- Transmitter – to furnish radio frequency energy.
- Antenna – to radiate the energy into the atmosphere.
- Receiver.
- Power – for transmitter and receiver.

- Transmitter modulates in AM or FM:
    - AM – Amplitude Modulation – variations are in the amplitude or range of the carrier signal.
    - FM – Frequency Modulation – variations in carrier frequency.
- Receiver – resonates or tunes the signals, amplifies, and demodulates.
- Unscrambled/Unencrypted – subject to interception.
- Voice Radio – base transmitter, mobile units – on same frequency.
    - Required output level = transmission distances, physical barriers, and signal interference.
    - Repeater stations or remote transmitters – receive and amplify.
- Wireless Alarm Signals – alarm detection array and an RF interface module.
    - Alarm sensor activated, coded alarm signal is transmitted by an omnidirectional antenna to all base stations within range. The base station receiving the strongest signal transmits to central station.
- Cordless telephones – usually not used in security operations.
    - Transmits by RF (range = 700 to 1,000 feet).
    - Certain frequencies offer more security – but don't discuss sensitive.
- Cellular telephones – provides user with mobile link via a computer controlled switching center, with landline or another mobile unit.
    - Service areas are divided into cells, which are grouped in clusters.
    - Group of frequencies is assigned to each cluster with DIFFERENT frequencies used in adjoining cells.
    - One cell site serves each cell. When a user moves from one cell to another, the in progress call is handed off – second cell/new frequency.
    - Cellular systems use the 800 MHZ or 1,900 MHz frequency range.
    - Signal Compression – 2 forms to maximize the use of spectrum space:
        - TDMA – Time Division Multiple Access – divides calls into pieces of data that are identified on the receiving end by the time slots to which they are assigned.
        - CDMA – Code Division Multiple Access – spreads segments of calls across a wide swath of communication frequencies. The segments carry a code which identifies originating telephone. The receiving equipment uses the code to reconstitute the original signal.
            - Offers 10 to 20 times the capacity of analog.

- <u>Scrambling</u> – applicable to cellular communication.
  - Scrambler is required at originating and terminating locations.
  - Telephone privacy vendor – customer calls a toll-free number, gets a dial tone, and dials the terminating number.
    - Landline version compatible with fax machines.
- <u>Analog Cellular</u> – Advanced Mobile Phone Service – 800 MHz.
- <u>Digital Cellular</u> – Digital Cellular Service (DCS) – 1,900 MHz.
  - also called: Personal Communication Service (PCS).
  - Analog voice message is converted into a string of binary digits.

- <u>Private Fixed Wireless Systems</u>
  - Wireless Private Automatic Board Exchange (PABX).
  - Uses low-power transmitter to communicate with handheld telephones within a limited range.
  - Can be intercepted.
  - <u>Local Digital Fixed Wireless Systems</u>
    - Providers compete and lease facilities from the local service provider whose cables are already in place.
- <u>Satellite Communications</u>
  - Geo-stationary earth orbit (GEO) satellites.
    - Inherent signal delay.
    - New technology used in low earth orbit (LEO) will benefit delay-sensitive communications.
    - Compatible with existing cellular networks and switch back and forth depending on availability of cellular service.
    - Susceptible to interception.
    - GEO – fixed position, 22,300 miles above earth.
    - MEO (medium) – 6,500 miles above earth.
    - LEO (low orbit) – 480 miles above earth.
- <u>Wireless Interference</u> – unwanted signals = interference.
  - Signals from other transmitters, industrial and atmospheric noise.
  - Noise interference – man-made or natural
  - Man-made – electrical arching. More serious for AM than FM.
  - Natural – characterized by static.
  - Heavy steel and concrete limit distance to which signals can be received ------- solved through use of antenna radiating through loop or leg strung throughout the structure.
- <u>Microwave Transmissions</u>
  - Transmitter operates at super-high frequencies.
  - Microwave generator, power amplifier, means of modulating the microwave carrier, and antenna to transmit signals into atmosphere.
  - Often require FCC licenses.
  - Not affected by man-made noise.
  - Microwaves travel in straight line and can be reflected.
  - <u>Passive reflector</u> – surface against which microwave can be bounced like a billiard shot.
  - Repeater can be used to extend the range of the microwave system.

- Laser Communication – **L**ight **A**mplified by **S**timulated **E**mission of **R**adiation.
    - Light is Coherent – tightly focused in one direction.
    - Modulated by passing laser beam through a crystal.
    - Electric field is applied to crystal and modulates the polarization of the laser's monochromatic light beam.
    - Receiver – beam is focused on a photo-detector that demodulates or recovers the electric field changes. Electric signal is converted to conventional audio or video signals.
    - Line-of-sight transmission is necessary – or mirrors are necessary to reflect the laser beam.
- Interconnection
    - The FCC has ruled that private communication systems may be interconnected with the public telephone network.

Communications

Line Protection- installed underground or inside installed in conduits.

- Underground should not be taken from nearest utility pole.
    - Use a more distant source to obscure the wire path.
- Dividing communications requirements between two providers will give a measure of assurance that communications can be maintained.
- Line Supervision:
    - To check the circuits automatically and immediately signal line faults.
    - Simplest method – end-of-line resistor installed to introduce a constant, measureable electrical current.
        - Detects an open circuit (broken connection), a ground, or a wire-to-wire short.
    - High value assets:
        - Minimizing the permissible variance in circuit value.
        - Using quasi-random pulses, which must be recognized by control equipment.
        - Use shifts in transmission frequency.
    - An **analog** transmission is a mere audio reproduction of the source signal (voice, musical, tone).
    - A **digital** transmission is analog converted to a string of binary digits.

Scramblers – tool to disguise information - is unintelligible to eavesdroppers.

- Copper wire in telephone network can be intercepted.
- Voice has two characteristics that can be modified:
    - Frequency (the pitch of the voice).
    - Amplitude (its loudness).
- Frequency Inverters – invert the frequency content in the voice.
    - Low cost and can be understood by a trained listener.
- Bandsplitters – extensions of the frequency inverter.
    - Single speech band is broken up into smaller frequency bands.
- Rolling Bandsplitters – continuously modify the way frequency bands are interchanged in accordance with a predetermined pattern.

    - Trained listener can obtain some information.
- Frequency or Phase Modulators
    - Frequency modulator scramblers cause the voice spectrum to be inverted and continuously changed in frequency – predetermined pattern.
    - Phase modulators – similar but it is the phase rather than frequency of the voice wave that is changed.
- Masking – modifying the amplitude of the voice by adding another signal into the voice band. (Single tone, combination of switched tones, RF noise).
    - high degree of security if used with bandsplitter or frequency or phase modulator.
- Rolling Codes – scrambled format to be changed periodically in a predetermined manner.
    - Key-stream – the electronic control signals that change the scrambled format.
    - Psuedo-random generator – generates longer and different key-streams.

Alarm Control and Display

AC&D subsystem that provides information to a security operator and enables him to enter commands affecting the operation of the AC&D system.

- The subsystem's goal is to support rapid evaluation of alarms.
- Alarm display equipment (console) receives information from alarm sensors.
    - Quickly, clearly, and only necessary information.

Ergonomics: Human Factors

- designed to serve the human operator.
- Effectiveness, reduced frustration and fatigue.
- Adjustable lighting.
- What the operator needs to: see, hear, reach and manipulate.
- The area around the operator consists of zones of varying accessibility and visibility:
    - Displays perpendicular to operator's line of sight.
    - Primary interface area - Most important displays.
        - Not much head/eye movement – within 30 degree viewing cone.
    - Secondary Interface area - operational displays used often.
        - Move eyes but not head.
        - Support displays used infrequently placed beyond secondary area.
- Audible signals are used to alert the operator.

- <u>Displays:</u>
    - Installed in center of console.
    - Touch panels to eliminate the need for other control devices.
    - Visual signals – flashing or blinking messages.
    - Colored lights (ie. Traffic light colors):
        - Red = alarm/action.
        - Yellow = caution/abnormal.
        - Green = proceed/normal.
    - Install communications equipment in a separate room:
        - More space in control room.
        - Not disturbed by maintenance and noise.
        - Equipment – environment temperature needs.
        - Better secured against tampering.
    - <u>Operator/equipment interrelationships</u> – essential equipment should be duplicated for each operator, but operators can share access to secondary or infrequently used equipment.

<u>Ergonomics: Graphical Displays</u>

- Well-designed <u>Graphical User Interfaces (GUIs)</u> – various graphical information.
- On-screen display – text, graphics, or controls.
    - Up to 3 windows displayed at once.
    - Full size screen = overview of system status.
    - Half screens = subordinate information.
    - Operators should not have to move or resize windows.
- Menus are nested – displayed along side. Selecting an item causes a subordinate menu to be displayed.
    - Good menu = no more than 9 items and 3 levels.
- Common commands should not be placed in menus but should be available as buttons. (On-screen is like a push-button switch).
    - Visible buttons – limited to 9.
- Maps quickly show the location of a security alarm.
    - Leave out excessive details.
- Text display – only vital details.
- Color – no more than 7. (Red, Yellow, Green reserved for sensor status).
- <u>Operator First</u> – overriding design philosophy:
    - number of actions to perform a command minimized, not able to access sensor if already accessed, annunciator should not override operations in progress (non-intrusive notification).
    - Should not be annoying.

Summary

Assessment and surveillance are not the same:

- Assessment – associates immediate image capture with a sensor alarm.
- Surveillance – collects video information without associated sensors.

Video Alarm Assessment System

- Consists of :
  - Cameras at assessment areas.
  - Display monitors at the local end.
  - Various transmission, switching, and recording systems.
- Major Components:
  - **Camera and lens** to convert an optical image of the physical scene into an electrical signal.
  - **Lighting system** to illuminate the alarm location evenly with enough intensity for the camera and lens.
  - **Transmission system** to connect the remote cameras to the local video monitors.
  - **Video switching equipment** to connect video signals from multiple cameras to monitors and video recorders.
  - **Video recording system** to produce a record of an event.
  - **Video monitors** to convert an electrical signal to a visual scene.
  - **Video Controller** to interface between the alarm sensor system and the alarm assessment system.

The level of **resolution** required in the video subsystem depends on:

- Expected **threat.**
- Expected **tactics.**
- **Asset** to be protected.
- The way the video information will be **used.**

Alarm assessment system performance MUST support protection system objectives.

- Alarm assessment system is a component of the intrusion detection system.

Alarm Communication and Display (AC&D) system:

- Collects alarm data, presents information to a security operator, and enables the operator to enter commands to control the system.
- AC&D is a key element in the successful and timely response to a threat.
- The system controls the flow of information from sensors to the operator and
  - Displays this information quickly and clearly.

Goal of display system – to promote the rapid evaluation of alarms.

CHAPTER 8 ENTRY CONTROL

- Subsystem that allows the movement of authorized personnel and material into and out of facilities, while detecting and possibly delaying movement of unauthorized personnel and contraband. (Part of the Detection function).
- Provides information for assessment and response.

Entry Control – physical equipment used to control movement of people/material. (Hardware).

Access Control – process of managing databases or other records and determining the parameters of authorized entry such as who or what will be granted access, and when and where they may enter. (Administrative Controls).

Performance measures of entry control subsystems:
Throughput – measure of time it takes for an authorized person or material to successfully pass an entry or exit point.
Error rates – discussed later.

Personnel Entry Control

- portion used to authorize entry and to verify the authorization of personnel seeking entry to a controlled area.
  1. Carrying a credential.
  2. Personal Identification Number (PIN).
  3. Biometrics.

(what you have, what you know, and what you are).

- combinations will reduce throughput but will make the system harder to defeat.

Personal Identification Number (PIN)

- PIN entered into keypad.
- Sometimes a coded credential is used to locate the reference file.
  - Credential is inserted and PIN code entered.
- Problems:
  - PIN and credential could be given to unauthorized person.
  - Shoulder surfing – observation surreptitiously by an adversary.
  - PIN could be obtained by coercion.
- Four digits allow for 10,000 combinations.
- Some systems provide a maximum number of attempts before disallowing.

Tokens – also called credentials.

- Photo ID badge.
- Exchange badge.
- Stored Image badge.
- Coded credential (checked automatically).

Photo Identification Badge

- Not always effective.
  - False badges, guard inattentiveness.

Exchange Badge

- Matching badges are held at each entry point.
- Guard exchanges the badge and allows entry.
  - Employee badge is held at entry point.
  - Employee wears the exchanged badge which is never allowed to leave the area.

Stored-Image Badge

- Stored image (Video Comparator) – guard verifies visual characteristics.
- Enrollment Capability – maximum number of images that can be stored.
- Access Time – time required from entry of the identification number until the stored image is displayed for viewing.
- NOT considered to be personnel identity verification.

Coded Credential – also called key-card systems.

- maintenance of entry authorization records for each coded credential; unique identification code numbers; termination of entry authorization without retrieving badge; provision for several levels of authorization (ie. Locations or times).
- Techniques for coding a badge: Magnetic stripe, wiegand wire, bar codes, proximity, and smart cards.
- Magnetic Stripe – encoded with data → slotted magnetic reader.
  - Coercivity – resistance of magnetic material to changes in the stored information when exposed to magnetic field.
    - magnetic intensity of an applied field required to change the information.
    - Oersted - Unit of magnetic intensity - to describe Coercivity.
      - Credit cards – 300 oersted (low-coercivity).
      - Security creds. – 2500 - 4000 oersteds (high-coercivity).
- Wiegand – not used much. Wiegand data protocol still in common use.
- Bar Code – Widths of bars and spaces scanned by optical sensor.
  - Two-dimentional symbologies (2-D bar codes) store more info.
- Proximity Badge - can be read without placing into reader.
  - Classified by the method of powering the badge, operating frequency range, and read only or read/write capability.
  - Small RF transponder/transmitter – powered in some way.
  - Passive badge draws power from the reader through RF signal when entering the interrogation field.
    - Others continually broadcasts and the reader antenna picks up the RF data as the badge enters the reading field.
  - Low-frequency (125 kHz), High-frequency (2.5 MHz to over 1 GHz).

- Smart Cards – integrated circuit embedded in card.
    - Gold contacts on surface – communicates with reading device.
    - Contactless smart cards use RF communications.
    - True smart card includes a microprocessor that makes the card smart and sets it apart from memory cards.
    - High degree of resistance to forgery or compromise.
    - Many have ability to encrypt communications.
    - High cost.
- Homeland Defense Presidential Directive 12 (HSPD12) – requires the entire federal government and contract agencies to use a single, high-security credential.
    - Compliance – the vendor believes the product meets requirements.
    - Certified – product must be submitted to GSA and NIST for testing.

Personnel Identity Verification (Biometrics)

- One or more unique physical biometric characteristics.
    - Hand/finger geometry, handwriting, eye pattern, fingerprints, speech, face, and various other physical characteristics.
- Verification vs. Recognition:
    - Verification – person initiates a claim of identity – equipment agrees.
    - Recognition – person does not initiate – device attempts to identify the person by comparing biometric information with database.
- Error rates as performance indicators:
    - Type I error – false reject – improper rejection of a valid user.
    - Type II error – false accept – improper acceptance of unauthorized person.
    - Decision made as to balance between false accept and false reject rates:
        - Low false accept – compromises system security but allows authorized users entry.
        - False rejects – high security but may deny authorized users.

Hand/Finger Geometry

- Shape of hand – three-dimensional features.
    1. Initiated by presenting a coded credential or PIN.
    2. Hand is placed on reflective platen – device has guide pins.
        a. Right hand. Left hand – palm up.
    3. Solid state camera takes picture.
    4. System measures length/width and creates a representation of the hand called a Feature Vector.
    5. Feature vector is compared to template (previous measurements).
- A similar system uses two fingers (index/middle).

Handwriting

- Signatures are easily forged.
- Uses handwriting dynamics such as:
  - Displacement, Velocity, and Acceleration.
- Transducers measure characteristics.
- Provides low security.

Fingerprints

- Used as a personnel identifier for more than 100 years.
- Automated systems – rely on image processing and pattern recognition.
- Most use Minutia points (fingerprint ridge endings and bifurcations) as the identifying features of the fingerprint. Some systems use the whole image.
- Optical methods – use a prism and solid-state camera.
  - Dry or worn fingerprints are difficult to image using optical methods.
- Ultrasound – can image below the top skin surface to the lower layers where the fingerprint is not damaged.
  - Not as fast as optical:
    - Ultrasonic transducer requires Raster Scan.
- Other: Direct imaging sensors, capacitive, electric field, thermal.

Eye pattern

- Uses the Iris (colored portion of the eye) to identify.
- Video camera images the iris structure of the eye.
- Recognition mode – entry of a PIN is NOT required.
- 10-12 inches so no physical contact.
- Externally illuminated with visible light – NO LED.
- Issues with: eyeglasses glare, blindness, iris issues, very dark irises, extremely dilated eyes.

Voice

- Speech measurements – waveform envelope, voice pitch period, relative amplitude spectrum, and resonant frequencies of the vocal tract.
- Low security.
- Issues: voice can change due to sickness or stress. (Backup method nec.)

Face

- distinguishing characteristics of the face.
- Image is captured by video camera (or thermal image using an infrared imager).
- Issues: wide variations in PRESENTATION of the face (ie. Head tilt), and lighting variations.
- Potential to provide face-in-the-crowd identifications.

Other

- Keystroke (typing patterns), ear shape, gait, fingernail bed, body odor.
- Studied but little development.

Personnel Entry Bypass Control

- keyed locks as a bypass route – useful in case of component or power failure.
  - Add door sensor to notify of opened door by key or picked.
  - Only one door per room or area is necessary.

Contraband Detection

Contraband – any item prohibited from an area.

- weapons, explosives, tools, drugs, cell phones, radio equipment, etc.

Manual Search

- Can be very effective, but:
- Reduced throughput and high labor costs.

Metal Detectors:

Magnotometer – (use is discouraged)

- Passive device that monitors the earth's magnetic field and detects changes caused by ferromagnetic (attracted by a magnet) materials.
- Copper, alumininum, zinc – NOT detected.

Most metal detectors currently in use:

- Actively generates a varying magnetic field over a short period.
- Detects changes to that field due to introduction of metal, or detect the presence of **eddy currents** that exist in a metallic object caused by a pulsed field.
- Magnitude of response determined by: conductivity of the metal, magnetic properties of the metal (relative permeability), shape and size, and orientation of the object within the magnetic field.
- 2 Methods:
  - Continuous wave – (no longer available) – generate a steady-state magnetic field.
  - Pulsed-field detectors – fixed frequency pulses (400-500 per second).
- Steady-state sinusoidal – magnetic field passes between transmitter and receiver coils. Routed to a balanced differential amplifier which amplifies only the difference.
  - Signal is further amplified and phase-checked.
  - Alarm if a selected threshold is exceeded.
    - Ferromagnetic – high relative permeability.
    - Non-ferromagnetic – low relative permeability.
  - Balanced receiver coils are not required for pulsed-field.
- When a metallic object is present in the arch, the collapse of the magnetic pulse induces an **eddy current** in the metal.
- Phase detection detects ferromagnetic or non-ferromagnetic.
- Modern digital technology differentiates between real targets and harmless metallic objects carried by people.
  - Handheld metal detectors recommended.
- Portal metal detector used to detect very small quantities (ie. Gold).
- Be aware of surrounding area of metal detectors.
  - Magnetic field is not limited to area between coils.

  - Electromagnetic transients – radios, power line, flickering fluorescent lighting.
  - Do not install a metal detector against a steel support beam.
- No-move rule – following installation testing, metallic items in vicinity should not be moved.

Package Search

- manually or active interrogation.
- Active Interrogation – ie. X-rays:
  - single-energy transmission x-ray, multiple-energy x-ray, computed tomography (CT) scan, and backscatter x-ray.
  - Not safe for use on personnel screening, except Backscatter x-ray.
- Conventional single-energy transmission x-ray
  - Produces an image for an operator to inspect.
  - Will not penetrate heavy materials (shipping containers or vehicles).
    - High-energy x-rays or Multiple-energy x-rays can be used.

Explosives Detection – bulk and trace.

- Bulk (macroscopic) – detonable amounts.
  - Uses ionizing radiation – not suitable for people.
- Trace (vapor of particle) – residue associated with handling.

Bulk Explosives Detection

- Characteristics of the presence of bulk explosives measured by:
  - X-ray absorption coefficient, x-ray backscatter coefficient, dielectric constant, gamma or neutron interaction, and microwave or infrared emissions.
- Characteristics of explosives – high probability if:
  - Calculated mass, density, nitrogen, carbon, oxygen, and effective atomic number (effective Z).
- Sensitivity required:
  - Minimum detectable amount LESS than threat mass.
- Backscatter technologies are safe for human imaging.
- Single-energy transmission x-ray does NOT provide enough information for explosives search.
  - Dual-energy measures mass absorption coefficient and enables approximation of the effective Z-number.
- Computer Tomography (CT) – automated technology that provides detection of small threat masses.
  - Gantry spins around the package and images from many angles.
  - Constructs a three-dimensional representation.
    - Mass, density, and mass absorption coefficient.
  - High nuisance alarm rates of up to 20%.
- High-energy x-ray devices – vehicles and cargo container searches.
- Low-Dose backscatter x-ray – can safely examine people.
  - Image of body beneath the clothes. Scanned 2x (front/back).

- Nuclear technologies – interrogates vehicle/package using gamma rays or neutrons.
  - Gamma rays – similar to high-energy x-ray devices.
  - Thermal Neutron Activation (TNA) – determine nitrogen content.
- Quadrupole Resonance (QR) technology – uses pulsed low energy radio waves to determine the presence of nitrogen-rich materials.
  - very sensitive, compact and low cost.
- Raman analysis – uses laser interrogation followed by analysis of the spectrum of scattered light to identify materials.
- Technologies for standoff detection (safe distance)
  - Infrared cameras, passive and active millimeter-wave imaging systems, laser methods.

Trace Explosives Detection

- Common at checkpoint screenings.
- Trace vapors and microscopic particles.
- Ion mobility spectrometry, colorimetry, chemiluminescence, mass spectrometry, fluorescence, and canine olfaction.
- Performance metrics:
  - Limit of detection – smallest detectable amount.
  - Selectivity – ability to distinguish one material from another.
- Sampling – delivered to a detector for analysis.
  - Swipe sampling – most efficient.
    - Swab is vaporized by heating and examined.
  - Vapor sampling – air next to object is sampled.
    - Most efficient for inside containers and soft surfaces.
- Ion mobility spectrometer (IMS) – high sensitivity to dynamite, military grade TNT, and plastic explosive compounds.
- Colorimetry – change in color is evidence of explosive presence.
- Chemiluminescence detectors – use photochemical detection.
  - Uses a fast gas chromatograph – identification of several explosives from a single sample is possible in under a minute.
- Electron capture detector (ECD) – take advantage of high electron affinity of nitro compounds to identify trace explosives in a vapor sample.
  - Can be coupled with a Gas Chromatograph (GC).
- Mass Spectrometry – ions are processed in magnetic and electric fields to determine their mass-to-charge ratio.
    - Gold standard of the analytical chemistry laboratory.
  - Quadrupole mass spectrometer – sample molecules are negatively ionized with an electrical discharge, accelerated and focused onto an ion detector with the magnetic field of a quadrupole.
  - Quadrupole ion trap time-of-flight mass spectrometer – collects the ions in the trap, where they orbit.
- Fluorescent – amplifying fluorescent polymers can change their fluorescence in the presence of some explosives.

- Canine Olfaction (smelling by dogs) – hidden explosives and drugs.
    - Detection actually made by HANDLER who observes the behavior of the dog.
    - Constant retraining required.
    - Frequent breaks required.
- Trace explosives detection portals – deployed at many airports.
    - collects particles and vapor samples from a person after agitating the person's clothing with short bursts of air.
- Detectors must meet the needs of the facility.
- Vendor claims must always be verified through testing in operating environment.
- Factors: sensitivity, NAR, response time, operating and maintenance costs, and list of explosive materials in the threat definition.

Chemical and Biological Agent Detection

- Typically performed with point sensors at the site perimeter.
- Some chemical sensors use optical methods to achieve standoff detection.
- Biological agent detection differs from chemical detection:
    - Not immediately lethal.

LOCKS

- Important element of the entry control system.
- Secures the moveable portions of barriers.
- Complimentary protection measures – guard checks and sensors.
- 2 types: purely mechanical and combined electrical/mechanical.

Mechanical Locks

Components:

- Bolt or latch.
- Keeper or strike into which the bolt or latch fits.
    - Provides a secure housing for the bolt when locked.
- Tumbler array – barrier or labyrinth.
- Key or unlocking device.

Primary Types:

- Warded Lock – oldest. Open see-through keyway and long, barrel-like key.
- Lever Lock – (18th c.) – Lever tumblers are flat pieces of metal held to a common pivot and retained in place inside the lock case by the tension of the spring wire. Inherently susceptible to picking.
- Pin tumbler lock – (19th c. Linus Yale) – most widely used in United States.
    - Conventional Cylinder – key pins equally spaced in one row only.
        - Contains 5, 6, or 7 pins.
    - High Security Cylinder – pins and driver are interlocked so that random movement of the pins by lock picks or keys not specifically coded for the lock will not properly align the pins and driver.

        - keys are cut at precise angles, as well as depths
        - Medeco – instead of grooves at the bottom of the plug:
            - A side bar is moved into a cutout housing….
    - Wafer Tumbler Lock – utilizes flat tumblers fashioned of metal or other material to bind the plug to the shell.
    - Dial Combination Locks – operate by aligning gates on tumblers to allow insertion of a fence in the bolt.
        - Maximum number of combinations is the base number of positions on each tumbler, raised to the power of the number of tumblers.
            - Four tumblers with 100 numbers:
                - 100^4 or 100,000,000 changes.
    - Electronic Combination Locks – combination numbers are displayed via LED rather than by gradations on the dial. (use 2-person rule and audit trails as appropriate).

Master Keying – used to provide a Hierarchy of access to groups of locks.

- Maintain effective master key accountability.
- Additional positions or possibilities are presented for surreptitious unlocking by the creation of multiple shear lines or gate openings.
- Additional maintenance required.

Security Vulnerabilities of Mechanical Locks

- Attack by force.
- Surreptitious attack (picking).
- Attack by impression-making and "try" keys.
    - Impression making – makes faint marks on key blank.
    - "Try keys" or "Jiggle keys" – key blanks milled to fit the particular keyway and contain random bitting – turning/raking movements.

Rearranging Mechanical Locks:

1. Simplest is relocation of the lock.
2. Rearrange the actual tumblers within each lock to a new combination. (more-effective).
3. Convertible or Interchangeable core – very rapid redistribution of combinations. Can be replaced on the spot by another core already arranged to the new scheme.

Electrified Locking Mechanisms

- Locked and unlocked by a remote device.
- **Boolean logic** – allows the organization of concepts together in sets.
    - Combination of conditions – ie. "if door A is locked and door B is locked, then door C can be unlocked".
        - Useful in "mantraps".
- Fail-safe vs. Fail-secure (fire/life safety codes):
    - Fail safe – unlocks under any failure condition.
        - Free egress (ie. Panic bar if energized or not).
    - Fail secure – remains locked when power lost
        - May be used for egress if panic bar, etc. is installed.

Primary types:

Electric deadbolt – a solenoid (electro-magnet) moves a deadbolt.

- can be fail safe or fail secure.

Electric latch – solenoid activated, mounts on door and uses strike plate in door.

- beveled latch is used instead of a deadbolt.
- Latch does not need to be withdrawn for the door to close.

Electric strike – operates as an adjunct to any standard mechanical lock.

- Electrical energy is delivered to a solenoid that either opens or closes a mechanical latch keeper on strike plate.
- Not a lock but operates with a lock to hold the door closed or to permit it to be opened.

Electric lockset – a regular mortise lockset that has been electrified to control the ability to turn the handle.

- controlled by an access control device (ie. card reader) while the secure side handle remains operational at all times for unimpeded egress.

Exit device – panic bar or crash bar. (allows a path of egress).

- can be electrified to permit remotely controlled re-entry via a push button or card reader/keypad.
- Delayed egress locking system – compromise between safety and security.
    - 15 or 30 second delay after which the door unlocks.
    - Example - alarm is sounded and CCTV camera can be used.

Electromagnetic lock (magnetic lock)

- uses an electromagnet and a metal armature or strike plate.
- When energized – holds the door closed.
- Rated by pounds of force required to separate armature or strike plate from the electromagnet.
- Involves no moving parts.
- Better electromagnetic locks have built-in switches to monitor bonding of magnet and armature, and door position.
    - These sensors void placing a non-metallic sheet between the magnet and strike to reduce bonding power.
    - Intrinsically Fail safe because removal of power releases the strike.
        - High security requires back-up power.

Designing Secure Locking Systems

- designed to control the opening of a door or portal to an area.
- Also used to control the usage of equipment.
- Protection measures must assess the totality of the area:
    - Door/frame, surrounding walls, windows, ceiling, floor.
- What assets are to be protected and what is their value?
- What are the threats and the probabilities of those threats occurring?
- Who requires access and how often?
- Impact of implementing controls to regular operations.
- Organization's culture or image.
- Staff resources or outsourced.
- Budget to implement, operate, and maintain.

<u>Design Plan</u>

- locking systems are coordinated arrays of mutually supportive and complimentary locking elements. Design plans consider:
    - different, concurrent levels of security, unanticipated changes, etc.
- System must be DESIGNED, NOT simply installed.
- Who has access to what spaces.
    - Provide multiple levels of access.
- Designed to be both secure and convenient. (Balance)

<u>Locking Policy</u>

- written policy with a systematic approach.
- All persons must comply (evaluated on performance at review time).

System Integration and Installation Issues

- entry control is a component of a protection system.

- it must be determined if the entry control and AC&D functionality are to be implemented on the same host computer or separately:
    - Fully integrated or parallel systems.
- CCTV surveillance? Masking of sensors?
- Many AC&D systems incorporate entry control features.
- Fully integrated AC&D entry control systems:
    - Door sensor masking happens automatically when fully integrated.
    - May suffer performance degredation:
        - Reporting of alarm must take priority over handling entry control requests.
- Contraband detection equipment – high NAR due to pocket clutter.
- Consider impact of fire codes.
    - Fire door must have a single-hand/single-motion exit device.
    - When fire doors do have controlled entrance and free exit, an additional means of local masking of the door alarm must be implemented. Masking the alarm for exits is usually accomplished through the use of a request-for-exit sensor.

        - Infrared sensors detect persons approaching door from inside and alert the system.
    - Can also provide an additional secure BUT safe area beyond.

Procedures

- entry control systems require a procedural component as well.
    - ie. presenting and wearing badges, not disclosing PINs, no tailgating.
- Enforcement and training required.
- How many tries allowed before access request is denied?
- Preventative maintenance.
- Calibration of metal detectors.
- Random searches.
- Company policies and training.

Administration

- the system defines who gets access.
- Backup procedures.
- Handling visitors.
- Database management – continually updated.
    - Access to database limited with 2-person consent.
- Office/person assigned to manage access controls should be at the location that issues employee and visitor credentials.
- Recommended – access control system SEPARATE from the AC&D host computer.

Summary

- Entry control systems - Personnel entry control, contraband detection, and detection.
- Objective:
    - Movement of authorized personnel and material.
    - Detecting and delaying unauthorized movement of personnel and material.
- Methods:
    - Credentials, PINs, and automated Personal Identity Verification.
- Errors:
    - False rejection and false acceptance.
- Contraband:
    - Unauthorized weapons, explosives, drugs, and tools.
    - Methods of detection:
        - Metal detectors, package searches, explosive detectors.

The entry control system is an important part of the detection function of an integrated PPS. When combined with entry control procedures and a process for access control, entry control provides another method of delivering balanced protection-in-depth at a facility.

DELAY – the second primary function of a PPS.

CHAPTER 9 DELAY BARRIERS

- Delay provides time for the response force to arrive or additional remotely controlled delay and response systems to be activated.
- Barriers are only potential obstacles:
  - Depends greatly on adversary's tools and techniques.

Barrier Types and Principles

<u>Passive barriers</u> – structural barriers:

- doors, walls, floors, locks, vents, ducts, and fences.
- Always in place – fail secure – even if they fail they provide a delay value.
- Traditional barriers – not likely to delay well-equipped, dedicated adversaries for long.
- Barriers must not unduly impede the facility's normal operations

<u>Security Officers</u> – can delay adversaries but may not be able to stop adversaries using force, unless officers in a fixed, protected position.

- can provide flexible, continuous delay.
- Expensive and can be overwhelmed.

<u>Dispensable Barriers</u> – deployed when necessary during an attack.

- chemical fogs and smokes, foams, and irritants.
- Compact and readily deployable.

<u>Deliberate placement</u> – would be to install detection systems and barriers next to each other so that adversary encounters:

1. First, the sensor.
2. Then, the barrier.

<u>Balanced Design</u> – each aspect of barrier configuration should provide equal delay. *"Delay-in-Depth".*

<u>Penetration</u>

- a barrier is considered penetrated when a person passes through, over, under, or around it.
- Penetration effort begins 2 ft. in front of barrier and ends 2 ft. beyond it.
- <u>Penetration time</u> – time to travel through the barrier.
- Very thick walls require a larger-diameter crawling holes than do thin walls:
  - Increases the barrier's delay time.
- Barrier penetration time depends on method of attack and equipment:
  - Hand tools, powered hand tools, thermal cutting tools (oxyacetylene torches, oxygen lances), explosives, vehicles.

- Vehicle Barriers:
    - Considered penetrated when:
        1. Ramming vehicle passes through/over and still functions, or a second vehicle is driven through breached barrier.
        2. Vehicle barrier is removed or bridged and functioning vehicle passes through/over.
- Distance from vehicle areas to the target area makes a difference:
    - Adversary will have to carry heavy equipment a long way.
    - Until detected – this delay is NOT included in system effectiveness.
    - Barriers OUTSIDE detection/assessment zone are NOT recommended.

Perimeter Barriers

- outermost protective layer of a PPS (physical protection system).
    - Coupling vehicle and personnel barriers into a perimeter.
        - Delay intruder at point of detection – improves assessment.
    - Enables the response force to intercept.
    - Vehicle barriers around a site's perimeter.
        - INSIDE the perimeter SENSORS.

Fences:

- Barbed wire, general purpose barbed-tape obstacle, or barbed-tape concertina (BTC) – can increase fence's delay capability.
    - Roll of barbed tape to outriggers (cost-effective).
        - Direction of outriggers makes little difference.
- Barbed-tape rolls placed Inside/outer perimeter, and outside/inner perimeter (prevents accidental injury).

Gates:

- points of entrance and exit.
- Pedestrian flow and traffic patterns.
- Orientation of vehicle gates and driveways can reduce vehicle breaches:
    - Multiple turns reduces approach and departure speed.
- Use several gates at perimeter.
    - Holding area – one gate closed and locked before the other opens.

Vehicle barriers:

- Should be installed inside the detection and assessment zone to ensure valid delay.
- Define the asset and the threat (threat vehicle).
    - Concrete filled pipes.
    - Cable barriers defeated easily.
- Optimum barrier height typically about 30 inches.
- Denying vehicular access forces the adversary to carry tools.
- Barrier system must be able to stop a defined threat vehicle at a SPECIFIC distance from a secured area, regardless of where the attack begins.

- For the vehicle to be stopped, its Kinetic Energy must be dissipated.
    - Kinetic energy (proportional to the square of its velocity and to its mass.
- Vehicle arrestor – absorbs most of kinetic energy, gradually over a longer distance. (eg. Dragged weights).
- Crash cushion- short distance (eg. Liquid filled plastic containers).
- Inertia device – exchanges momentum and kinetic energy (eg. Small concrete shapes and unanchored sand-filled barrels.
- Rigid device – almost all kinetic energy is dissipated as it deforms during impact. (eg. Massive concrete shapes).
- US Department of State formerly set performance standards:
    - Now the new standard is ASTM F 2656-07.

Structural Barriers

- Walls, doors, windows, utility ports, roofs and floors.
    - Walls/locked doors penetrated in less than a minute.
    - Doors provide an easy adversary path through walls.

<u>Walls:</u>

- generally more resistant to penetration than doors, windows, vents.
- Upgrades extend the penetration delay against hand, power, thermal tools.
- Reinforced concrete walls – designed for structural loads – NOT security.
    - Using two reinforced walls in a series results in longer penetration delays than using one wall as thick as the two walls combined.
    - Removing the rebar takes longer than removing the concrete.
        - Add additional rebar, rebar size, decrease spacing.
- Overburden – cheap and effective defense against all methods.

<u>Doors:</u>

- The weakest portion of a barrier determines the barrier's ultimate value.
- Weak link in a structure – because of functional requirements and associated hardware.

- <u>Balanced design</u> – doors, frames, hinges, bolts, locks – STRENGTHENED to provide same delay provided by floors, walls, and ceilings.
    - most common exterior doors – 1 ¾ in. thick with 16 or 18 gauge steel surface sheets.
- Standard key locks – susceptible to picking.
- If no entry needed – fully flush mounted with no external hardware.
- External doors susceptible to vehicle ramming.
- Search and rescue tools can also be used.
- First step in upgrading – eliminate unnecessary doors.
- Next step – eliminate unneeded windows, louvers and external knobs and keyways.
- Add steel plates, grout frames with concrete.

- Lock/frame area – sheet steel strip welded or bolted to door.
    - same height as door – 2 in. wide with 1 in. overlap to doorframe.
    - Frame grouted with concrete 18 inches above the frame strike location on both sides of frame.
- Upgraded hinges with stud-in-hole feature.
- Bolt/weld a steel Z-strip to the rear face of the door.
- Full-length hinge designs.
- Panic or Crash bars – install a bent metal plate. Prevents chiseling and wire hooking. Drill resistant section extends penetration time.
- Louvers and glazing material – reduced in size to prevent crawl through.

Windows and Utility Ports

- frames, glazing materials, protective coverings, etc.
- Utility Ports:
    - all types of unattended framed openings aside from doors and windows.
- Window frame strength and weight – concealed materials that resist cutting.
    - Window locking mechanism may be a weak link.
    - Attachment of window frame to structure can be strengthened.

Glazing materials:

- Standard Glass – highly frangible.
- Tempered glass – can be broken with impact tools.
- Wire Glass – diamond, square, or hexagonal wire patterns.
- Laminated glass – two or more panes of annealed float, sheet, or plate glass bonded to a layer or layers of plastic.
- Transparent Plastics – may be restricted by fire codes.
    - Lucite and Plexiglas – can be broken in 10 seconds.
    - Polycarbonates – resist impact as well as bullet-resistant glass.
    - Glass/polycarbonate – composite glazing – touch core of polycarbonate between two layers of glass.
- Grills, bars, expanded-metal mesh, screens – placed at or after appropriate detection measures.

Tunnels – used to link buildings are not protected very well.

- pipe channels, ducts – should be enhanced with interior barriers.

Roofs and Floors

- quantity of steel reinforcement, and concrete strength required to carry the loads.
- Improvements BELOW the roofline are best.
    - More effective without significant modifications.
    - Optimum distance between roof and second barrier is 10 to 12 in.
- Adding a roof covering – buried and cut-and-cover use an earth covering to delay access and protect against blasts.

Dispensable Barriers – deployed only when necessary. (Active or Passive).

- Active dispensable barriers – when activated – stop or delay an adversary.
- Command and control hardware receives the activation decision and operates the dispensing hardware.
- Dispensable material – stored in compact form.
    - Expands to effective delay state through chemical or physical reaction.
    - Forces the adversary to defeat the barrier and evade the response force.
- Passive dispensable barriers – do not require a command and control system.
    - activated by adversary's penetration attempt.
    - Sometimes cheaper than active.
    - Rigid polyurethane foam, stabilized aqueous foam, smoke or fog, sticky thermoplastic foam, and various entanglement devices.
        - Irritants can be added to aqueous foam
        - Entanglement devices work best in combination with smoke/fog barriers.
    - Dispensable barriers are usually deployed very near the assets being protected.
- New technologies: Remotely fired weapons systems, millimeter waves to produce a severe burning sensation in adversary's skin (without harm).

Procedures

- normal cleaning, periodic inspection, upkeep.
- Passive must be checked for damage and appropriate pressure.
- Active require routine testing of the command and control system.

Safes

- safes designed for fire protection would not be effective against forced entry.
    - Thick, solid steel walls transfer heat rapidly to interior – paper destroyed quickly.
    - Underwriters Laboratories (UL) – expected protection.
    - UL requires: Safes less than 750 lbs. (340 kg.) be anchored.

Record safes for fire protection

- Magnetic media (discs and tapes) – more vulnerable to heat and flame.
- Incorporates moisture in insulation to help dissipate a fire's heat so the internal temperature does not rise to a level that destroys the contents.
    - Moisture evaporates overtime – rated value of 20 to 30 years.
- UL labels indicate whether fire-resistant or insulated records container.
    - Indicates: Hours of protection and temperature.
- Fire Resistant safes – must pass tests against fire, explosion, and impact.
    - 350-4 hours/ 350-2 hours/ 350 1 hour.
- Insulated Filing devices – less protection for records than the three levels of fire-resistive containers.
- UL label indicates – fire-resistant/record container/insulated filing device.
    - Insulated filing device – protection against burnout in fire-resistant buildings in areas with small quantity of combustible material.

Electronic Data Processing Record Protection

- magnetic media begin to deteriorate at 150 degrees F. (66C).
- lower at humidity levels more than 80%.
- Container must withstand humidity levels and extreme heat.
- "Safe-within-a-safe" – inner insulated places in fire-resistant
- Safe passes testing if information loss after fire does NOT exceed 1%.

Safes designed to protect valuables (Burglary protection)

- requirements of the Insurance Services Office and U.L.
- generally do not protect against fire.
- Should be installed in steel-clad concrete box or otherwise anchored.
- Burglary Resistive:
  - Laminated (two or more sheets of steel with facing surfaces bonded together); or solid steel.
- Burglary/Fire-Resistive Containers
  - Heavy insulation around the safe contents leaving no voids for heat to penetrate.
  - Insurance underwriters – careful attention when establishing insurance premiums.
- GSA-Approved safes – General Services Admin. – storage of government classified information.

Vaults

- specially constructed rooms or areas intended to limit access and provide protection to the assets in the space.
- Also applies to protection from fire, not only theft.
- Consider asset being protected and its vulnerability.
- Consider: Special regulatory requirements or standards established by an insurance carrier or government agency.

Fire-Resistive Vaults

- National Fire Protection Association (NFPA).
  - Does NOT consider forcible entry.
- Key issue is if vault will be located in fire-resistant building.
- Avoid installing below grade – smoldering debris in basement, mold, floods.
- Vault construction:
  - Reinforced concrete, steel rods ½ in. diameter, spaced 6 in. on center, running at right angles in both directions.
  - Structural steel frame with 4 in. of concrete/brickwork, tied with steel ties or wire mesh (No. 8 ASW gauge wire on 8 in. pitch).
  - Fire resistance determined by wall thickness.
    - Min. for 4 hour vault = 12 in. brick/8 in. reinforced concrete.

Media Storage and Protection

- additional container within the vault to protect such assets.
- Standards:
    - American National Standards Institute (ANSI),
    - American Society for Testing and Materials (ASTM),
    - Factory Mutual Research Corporation (FMRC),
    - National Fire Protection Association (NFPA),
    - Underwriters Laboratories (UL).

Vaults for Protection Against Forced Entry

- exterior wall location is NOT desirable.
- Equal protection on all 6 surfaces (box).
- Concrete can be penetrated – structural load, not security.
    - Brittle and poor tensile, flexing properties.
    - Steel reinforcing bars – Rebar.
        - ASTM vault construction specifications.

Penetration Techniques

- explosives are particularly effective.
- Steel reinforcement increases the penetration delay.
    - Size of steel reinforcement has a significant effect on protection.

Wall Construction and Penetration

- Vault with time lock – even if alarm signals, it will be impossible to open the vault door until programmed time.
    - CCTV with audio and lighting recommended to create a record.

Vault Vulnerability Considerations

- Inadequate policies and procedures for opening and closing vaults are often the downfall of even the best designed vaults.

Summary

- Barriers delay the adversary during an attack.
- Multiple barriers of different types.
    - Complicates adversary’s progress and requires different tools and skills.
- Dispensable barriers, such as entanglement devices, and dispensable chemicals such as obscurants, irritants, and foams, offer significant potential for increasing adversary delay.

CHAPTER 10 RESPONSE

(Third and final primary function of a PPS is reponse)

- Responding Personnel and the Communications Systems they use.

Security Operations

- On-site or off-site.
- Proprietary or Contract guards.
- *Guards* – on-site personnel available to respond.
- *Response Force* – security response personnel, on or off-site.
- Different targets require different plans.
- After-the-fact recovery – investigative tools.
  - Recovery strategy may not be acceptable for all assets.
- Timely response = better detection and delay than a recovery strategy.

General Considerations

- Staffing of the response force is fundamental to the performance of the response function.
- Training:
  - Proprietary – employee training.
  - Contract services – training incorporated into vendor contract.
- Civil Law = intentional torts (assault, false arrest, defamation, negligence).
- Criminal Law = trespassers, drug use, sexual, theft, fraud.
  - Evidence collected for prosecution with L/E.
- Labor Law = wrongful termination, labor union activity, strike surveillance.

Contingency Planning

- identify potential targets, respond to different threats, interact with outside agencies, and determine level of force that can be used in various situations.
  - Identification of assets, likely adversary routes, tactical plans.
- Different response force strategies:
  - Containment; Denial; occasionally Assault.
- Containment:
  - Strategy used against adversary with THEFT as a goal.
  - Prevent adversary from leaving site.
- Denial:
  - Strategy used when adversary's goal is SABOTAGE or VIOLENCE.
- Tactical Planning (Assault):
  - Guard actions, equipment, outside support (written agreement with outside agencies).
  - Off-site credentials and authority to facilitate the response force's ability to operate outside the facility's boundaries:
    - Deployment and Pursuit.

Misc.

- Security may be asked to assist in natural disasters, bad weather, accidents:
  - Should not be allowed to compromise the protection of assets.
- Procedures must be developed with input of various components (BUs).
- Processes and procedures to resume operations ASAP while still collecting and preserving evidence.
- Communications – evaluate alternate means during abnormal or malevolent conditions.

Performance Measures

- used to evaluate an immediate response to a security event.
  - Time it takes guards to arrive.
  - Probability of communication.
- Interruption – the arrival of response personnel at a location to stop the adversary from progressing in the attack.
  - depends on reliable, accurate, fast alarm reporting and assessment, along with reliable communication and effective deployment.
- Neutralization – defeat of the adversary by responders.
  - response tactics, use of force procedures and post-detainment actions, training, numbers of response personnel, equipment, etc.
- Guard fatigue
  - An additional factor related to human-machine interaction, decreased performance from cognitive failure, and means of quantifying fatigue effects.
  - Smart Scheduling:
    - Shift lag – rapidly rotating plans better than slowly rotating.
    - Shift length – no more than 8 hours (12 for jobs with low physical and emotional work).
    - Night Shifts – preferably NO MORE than 3 in a row.
    - Recovery – 24 hours of recovery (not time off) after each night shift.
    - Weekends – schedule the max. number of free days on weekends.
    - Days Off – at least 104 days per year (ie. 52 weekends).
    - Equity – equal demand for all workers.
    - Predictability – easy to understand schedule.
    - Good Quality time off – 3 or more consecutive days.

CHAPTER 11 ANALYSIS OF THE PHYSICAL PROTECTION SYSTEM

- Analyze how effective the design will be in meeting objectives.
- Evaluation of the PPS compared to threats and asset value.
  - NOT the overall risk analysis.
- Design and Implementation depend on a facility's goals/constraints.
- Qualitative analysis – applies for lower security applications.
- Quantitative analysis – assets with unacceptably high consequence of loss, even if probability of attack is low.
  - only justified if assets require this level of protection.
- Analysis of a PPS provides two key benefits:
  - Establishes the assumptions under which design was formed.
  - Relates system performance to threats and assets.
    - Helps with cost-benefit decision.
- Initial baseline must be established.
  - Upgrades are considered if the baseline shows that the PPS does not meet goals and objectives.
  - Analyzing a PPS assists in deficiencies, improvements, cost vs. effectiveness comparisons.
    - Analyze an existing PPS or proposed system designs.

Analysis Overview

Compliance-based vs. Performance-based.

Compliance-based – conformance to specified policies or regulations.

- Metric = equipment and procedures.
- (only effective against low threats).
- Easier to perform because the only measure of system effectiveness is the presence of prescribed PPS equipment, procedures, and people.

Performance-based – evaluates how each element of the PPS operates.

- and what it contributes to overall system effectiveness.

Quantitative Analysis

- The use of numerical measures for PPS components.
- Not applicable to every facility.
  - Used for critical or unique assets (critical infrastructure or national security assets).
- System effectiveness:
  - Timely detection.
    - If detection occurs at the asset, the PPS is flawed.
  - Timely/accurate assessment of alarms.
    - NARs should be low.
    - The best technique = automatic display of video showing sensor alarm sources.
  - Communicate alarm information to response forces or Record for after-the-event response.

  - Performance measures for each PPS function:
    - Detection, delay, and response.
    - For each defined threat category or level.
    - Under varying operational conditions.
  - Ensure detection occurs before delay.
  - Delay the adversary long enough.
  - Protection-in-depth (multiple layers)
    - Avoids single point failures.
  - Ensure balanced protection – same effectiveness for all paths.
  - Engage and neutralize the adversaries.
  - Conduct path and scenario analyses.
- Quantitative analysis applies these principles and uses numerical estimates, such as probabilities and delay or response times to represent their application.
- Characterizing technology by testing to statistical standards is still the best technique to objectively assess security elements and systems.
  - Consider techniques, weather, installation, operation/maintenance.
- Testing provides insight – performance expected from a given device for a given threat.
  - Serves as the basis for application of degradation factors used in a VA analysis.

Analysis Tools

- Some are software based and some are paper-and-pencil.
- Tabletop models.
- Investigative tools – <u>Timeline analysis</u> – the sequence of actions described by witnesses or supported by evidence).
- Tools only – analysis still depends on the appropriate interpretation of data by the VA team.

<u>Qualitative Analysis – Carver</u>

- developed by the US Government as a targeting tool (best targets for attack).
  - Criticality – measure of public health and economic impacts.
  - Accessibility – ability to physically assess and egress from target.
  - Recuperability – ability of a system to recover from an attack.
  - Vulnerability – ease of accomplishing an attack.
  - Effect – amount of direct loss measured by loss in production.
  - Recognizability – ease of identifying a target.
- A modified CARVER also evaluates the combined health, economic, and physical impacts of an attack, or the shock attributes of a target, considered on a national level.
- Multi-step process to subjectively evaluate an asset as a target of attack from the perspective of the adversary.
- Works best when comparing assets that share a mission or are in the same infrastructure (does poorly otherwise).

Performance-Based Analysis

1. Adversary Sequence Diagram (ASD) for all asset locations.
2. Path Analysis.
3. Scenario Analysis.
4. Neutralization Analysis, if necessary.
5. System Effectiveness – determine.
6. Develop and analyze upgrades, if system effectiveness (or risk) is not acceptable.

Interruption – arrival of responders to halt adversary progress.
Neutralization – defeat of the adversaries by responders (face-to-face).

Performance measures used for these elements (Interruption/Neutralization):
(PI) – Probability of Interruption
(PN) – Probability of Neutralization

(PE) – Physical Protection System - PPS effectiveness

$$PE = PI \times PN$$

- if no PN (ie. adversary surrenders, or no response):
    - then PE is equal to PI (interruption only)

- in a qualitative performance-based analysis, designators are:
    - high, medium, and low to represent interruption, neutralization, and system effectiveness.

Analysis Process

- Performance-based analysis process.
- Qualitative or Quantitative techniques – used for performance-based evaluation.
- Based on Adversary paths to an asset.
- Insider analysis – similar but eliminates some layers of protection due to authorized access to some areas of a facility.
- Adversary Sequence Diagram (ASD):
    - Functional representation of the PPS at a facility that is used to describe the specific protection elements present.
    - Illustrates the paths that adversaries can follow to accomplish sabotage or theft.
    - Path analysis determines if a system has sufficient detection and delay to result in interruption, therefore it is conducted first.
    - Estimated performance measures based on the defined threat tools and tactics to predict weaknesses in the PPS along all credible paths.
    - The most vulnerable path can be determined.

- 3 basic steps in creating an ASD:
  - Describe the facility – separate into adjacent physical areas.
  - Define protection layers and path elements between adjacent areas.
  - Record detection and delay values for each path element.
- View the facility as concentric layers.
  - Biggest mistake is to follow a single path.
- Consider all paths using site drawings
- Concentric triangles to represent adjacent areas – models a PPS by identifying protection layers between adjacent areas.
  - First layer = off-site.
  - Last layer = Asset.
  - each protection layer consists of number of path elements (PE)
- one ASD must be created for each asset (target location).
- Assign detection and assessment probabilities, delay times for PPS elements under different facility states, and additional notes for each path element (PE).
- Entry path segment – off-site to asset.
- Exit path statement – from asset back to off-site.
- ASD represents ALL adversary paths to an asset.
- Sensitivity Analysis – how well system performs against higher or lower threats.
- Sabotage Analysis – only entry paths are evaluated.
  - Denial Strategy.
- Theft Analysis – entry and exit.
  - Containment Strategy.
- Path Analysis – provides an overall view of the robustness of the PPS.
  - whether system has many weak paths or only a few.
  - Estimates of path element performance determines where vulnerabilities exist.
  - Can reveal if PPS is balanced or not.
    - If layer is balanced, upgrades must be applied to each protection element to maintain balance.

Scenario Analysis

- Conducted to determine whether system has vulnerabilities – resulting in lower effectiveness of the PPS.
- Using defined threats and path analysis, scenarios are generated by llooking at weak paths. Preferred method so that no credible paths are missed.
  - Scenario timeline.
  - Performance estimates.
- Analyst reduces all possible paths to those that are most credible.
  - Very weak paths (PI).

- Scenario analysis begins when path analysis is complete:
    - Develop attacks and tactics designed to exploit weak paths.
    - Modify performance estimates for path elements using these tactics.
    - Document the assumptions used and the results of the scenario.
- Scenario analysis is aided by the creation of adversary task timelines and the associated performance of any path elements along the path.
    - For example: Communicating using alternate means during jamming.
        - Additional time required is added to response time.
    - Attacks on responders.
    - On-site tools – forklifts, explosives, cutting torches, ladders, power tools.
- Time for alarm assessment information to be relayed to responders is included in the response time.
- Scenario analysis considers response to attacks on multiple distributed assets at a facility.
    - Theft and sabotage = both containment and denial.
- Consider different operating states – open/closed, day/night, etc.
- Effort to identify the worst-case attacks – tests the limits of PPS effectiveness.

<u>Estimate Neutralization</u>

- Immediate response resulting in any face-to-face confrontation.
- How effective the response will be under different attack scenarios is a measure of response force capability, proficiency, training, and tactics.

<u>Other Analysis</u>

- Blast effects modeling, response storyboards, and sand tables.
    - <u>Blast effects modeling tools</u> – output is graphic showing an approximation of blast damage.
    - <u>Storyboard</u> – series of cartoon panels.
        - Depicts where responders and adversaries are at periodic intervals – every 30 to 60 seconds “snap shots”.
    - <u>Sand table</u> – toy soldiers are used to depict responders and adversaries.

Calculate System Effectiveness

- Qualitative or quantitative.
- If interruption and neutralization are used:
    - System effectiveness = product of PI and PN .
    - PE can be no higher than the lower of the two values:
        - ie. 0.9 x 0.2 = 0.18
- Calculated for each threat category – since varying performance for different threats.

<u>Upgrade Analysis</u>

- If baseline analysis of the PPS does not meet its protection objectives, it is vulnerable.
- VA team suggests upgrades:
    - Functional Improvements NOT specific technical recommendations.
        - Passed onto Upgrade Design Team.
- Once the analysis is completed, it is important to clearly present both the baseline and upgrade analyses to establish the need for improvements and show the return on investment in upgrades.
- During the upgrade analysis, consider contingency plans and equipment.
- <u>Contingency Plans</u> – for:
    - Equipment in repair (out of service); or
    - If required equipment to meet objectives are deemed to be too great.

Summary

- chapter described analysis of the PPS using both qualitative and quantitative techniques.
- Compliance-based or Performance-based.
    - <u>Compliance</u> – conformance to specified policies/regulations.
    - <u>Performance</u> – evaluates how each element of the PPS operates and what it contributes to overall system effectiveness.
- System effectiveness is a result of proper implementation of the security principles of:
    - Equipment, people, and procedures.

CHAPTER 12 IMPLEMENTATION OF THE PHYSICAL PROTECTION SYSTEM

- Last stage in the process, after:
  1. Problem definition.
  2. Physical Protection System Design.
  3. Analysis.
- Invloves: basis of design, design criteria, design, procurement, installation, training, testing, and maintenance.
- Four elements of physical design:
  - Deterrence, Detection, Delay, Response.
- Results in a fully integrated security program that blends architectural, technological, and operational elements into a flexible, responsive system.
- Factors in system design:
  - Environment or unique needs of the facility, taking into account anticipated threats, risks, vulnerabilities, and constraints.

<u>Basic tasks of security systems implementation:</u>

- Planning and assessment to determine system requirements.
- Developing conceptual solutions for resolving vulnerabilities.
- Preparing security systems design and construction documentation.
- Soliciting bids and vendor negotiations.
- Installing, testing, and commissioning.

Systems Design Process

- Study and Report.
- Preliminary and final design.
- Bid and negotiation.
- Construction.
- Operation.

<u>Planning and Assessment phase:</u>

1. Identification of critical assets, potential threats, subsequent vulnerabilities, likely risks, and functional requirements. (Proactivity vs. Reactivity).
2. Analyze security requirements and formulate solutions or countermeasures concepts to reduce or eliminate vulnerabilities and mitigate risks.
   - when validated operationally and in budgetary terms:
     - Output of the design phase.

- The systems design process is a serial process – each phase and task must be performed sequentially before the next can begin.
  - Design/build relationship with a contractor, OR
  - Design, procurement, construction with architect or owner.

Initial Phases

Planning and Assessment phase

- Project requirements and constraints.
- Output of design process = "Basis of design".
- Conceptual design solution.
- Define threats, identify assets, consider vulnerabilities via analysis, and assess risk.
- Teamwork – operational, facilities, engineering, and architectural.
- Three key ingredients:
  1. Multidisciplinary and committed approach.
  2. Spending necessary time and effort in planning phase.
  3. Decisions are made on the basis of sound and relevant risk and asset environmental information.
- analytic process where a solution is engineered and constructed.
- Outcome = set of security requirements, or objectives used as a basis of the eventual design (Design basis).
- Site survey and vulnerability assessment, apply the risk assessment and design process. Results in a conceptual design that:
  - Categorizes vulnerabilities by their criticality.
- Develop a business case (ie. cost).
- Economic metrics – ROI, payback, net present value of cash flow, etc.
- Requirements analysis – uses the threat, assets, and risk analysis as its basis.
- Formulate a statement of the overall objectives or mission of the:
  - Integrated security system (ISS).
- Add a level of confidence factor to each functional security requirement.
  - *Detect* and *Delay* rather then *prevent.*
- Evaluate all vulnerabilities and list specific functional requirements and resultant protection strategies.
- The level of protection for a group of assets MUST meet the protection needs of the most critical asset in the group.
  - Or separate the critical asset for specific protection.

- Requirements analysis
  - Use --- Assets --- Criticality --- Threats --- Vulnerabilities --- Risk.

Basis of design

- Documents assets deemed critical.
- Overall objectives of asset protection program.
- Results of the risk analysis.
- Functional requirements to be satisfied by the eventual design.
- Narrative operational description of the proposed systems, personnel, and procedures that constitute the security system or program.

- Becomes the designer's means to obtain consensus from the design team.
- When project is first conceived – NOT time for engineering details, budgets or specific countermeasures.

Conceptual Design (Design Concept)

- Last task of planning and assessment process.
- Initially developed as a product of the VA.
- Designer completes a complete security solution for assets to be protected.
    - General narrative and descriptive terms.
- Architectural perspective - Initial conceptual design or schematic phase.
- Integrated, holistic approach by designer with site owner.
- Concentric rings around protected assets – progressively more difficult to access and escape. (Protection-in-depth or redundant schemes).
- Redundant security scheme – *10 principles of probability,* Marquis de Laplace.
    - Probability of one detection system being circumvented is high,
    - But probability that all detectors would be compromised is very low.
- Intended subsystems – narratively described along with the interaction with one another to form a complete system.
    - Representative details.
    - Overall block diagrams.
- Mark up architectural floor plans.
- Seek management approval.
- Countermeasures depend on their cost-effectiveness.
- Security designers identify four principle security strategies:
    - Prevention, Detection, Control, and Intervention.
- Homeland Security:
    - Preparation, Prevention, Detection, Response, and Recovery.

Design Criteria

- Ground rules and guidelines for the design.
    - Additional design requirements that the design must consider along with the risks.
    - System performance, operational and financial considerations, style, design, codes, and standards.

Codes and Standards

- Compliance with national and local building, fire, and life safety codes.
- Work rules, insurance coverage, acceptable color schemes, competitive bidding, etc.
- Life safety codes (ie. doors, locking mechanisms).

Quality

- Balance between quality components and overall cost.
    - Document the trade-offs between cost and quality.
- Quality must be applied consistently.

<u>Capacity</u>

- Number of users, alarm zones, controlled doors, etc.
- General estimate.
- Consider expansion capacity – add 10 to 15 percent spare capacity.

<u>Performance</u>

- Component performance is detailed in a performance or project specification.
- Examples of performance parameters:
    - Entry control system must connect to an existing LAN.
    - ECS must effectively manage personnel traffic at shift change.
    - Minimum throughput of 500 per hour and evacuation in 10 minutes.
- Include reliability and maintainability criteria.

<u>Features</u>

- major system features summarily defined.
- If design functions are not readily available, procurement competition could be limited and costs could escalate.

<u>Cost</u>

- Design fees and Projected system construction costs.
- Knowledgeable person to lead the integrated design process.
- A budget is often a required design goal and should be included in the initial design criteria.

<u>Operations</u>

- Minimum negative impact on productivity and facility operations.
    - Operations managers should be consulted.
- Security operations should be seen as a natural use of security systems.

<u>Corporate Culture</u>

– significant factor in design and implementation.

- Culture distinguishes one organization from another.
- Determines how security is defined and implemented.

<u>Image</u>

– perception of the organization by the outside world.

<u>Monitoring and response</u>

- Design of a centrally located security operations center.
    - Monitor and respond.
    - Small organization – may use a central station.
    - Large organization – on-site security in a security operations center.

Preliminary Cost Estimate

- Initial Budget – capital expenditures and recurring costs.
- Since early in process, budget is just a conceptual, order-of-magnitude estimate at best.
- Conceptual but should be within 15 to 20 percent of final bid prices.
- Capital Projects:
  - Installation costs, project management and supervision labor, etc.
- Service projects and recurring costs:
  - Payroll, equipment, training, maintenance, consumable supplies, etc.

Design Team

- Determine who in the organization should be involved.
  - They can contribute to initial preliminary design process and benefit from knowledge of it.
    - CEO or CFO can send delegates.
    - HR mgr., IT mgr., facilites, etc.
- Security manager lives with the consequences of system failure.
- If expertise is lacking, hire specialists.

Design and Documentation Phase

- split into two phases = Design development phase and Construction documents phase.
- Alternatively, single phase = Construction documents (CD).
- Objective is to complete the design and to document the process to the level of detail necessary for the chosen method of procurement.
- Complete set of procurement documents
  - Known as contract (or bid) documents.
  - Consists of 3 sections:
    - Contractual details, construction specifications, and construction drawings.

Contractual Details

- Included in contract documents.
- Insurance and bonding requirements, site regulations, labor laws, delivery and payment terms, partial payment, owner recourse, termination, unit pricing, instructions to bidders.

Construction Specifications

- Mirror and complement the actual systems design.
- Performance instructions, functional testing, continual periodic programmed testing.
- Drawings and plans show WHAT is to be constructed, WHEREAS the specification details owner's intent and how it is to be constructed.
- All bidders get same complete understanding of the requirements.
- Wordy and very technical.
- Boilerplate specifications are a starting point for customization.
- Specifications are numbered depending on construction trade so that each section can be issued separately.
- American Institute of Architects (AIA).
- Construction Specification Institute – MasterFormat and MasterSpec.
- Most architects and project managers prefer security systems all in one spec.
- Each individual specification section consists of a standard format divided into three parts: General, Products, Execution.
- Security system specification should include: instructions to bidders, list of project references, functional description, list of design drawings, products and services, products and services in other contracts, codes and standards, support services, technical descriptions, general site conditions.

Drawings

- Cornerstone of any construction project.
- Picture or Diagram – less likely to be misinterpreted by contractors.
- HOWEVER – Specifications have precedence over drawings
- Plans, Elevations, Details, Risers, Hardware schedules.

Plans

- Top-down, map-like view.
- Complete site, building floor, or part of a floor.
- Room numbers (targets or tags).
- Background drawings.
    - Manual drafting – transparent (reproducible) sheets.
- Background drawing files consist of a number of layers (walls, floors, furniture, lighting).
    - CADD draftsperson can select required levels and turn others off.
- Sets of security symbols:
    - ASTM Int'l *Standard practice for Security Engineering Symbols.*
    - *Architectural Graphics Standards – CAD Symbols for Security System.*

Elevations

- views of VERTICAL surfaces.
- Show mounting heights, and locations of wall mounted devices (cameras, card readers, and motion sensors).

Details

- Detailed drawing sheets can be developed to define elements of the system in more detail, since plans and elevations are shown in small scale.
- May include special mounting techniques, custom part design dimensions, or cable terminations.

Risers

- Representations of complete subsystems (ie. CCTV or access control).
- Schematically demonstrate all the associated devices and components and their interconnecting cables.
- Used as the master drawing by designers and contractors.

Hardware Schedules

- Tables of related security devices.
- Provide detailed information that cannot easily be shown on drawings or in the text of a specification. (Door schedules, Camera schedules, etc).

Design Coordination

- Between many other design disciplines.
- Architect – lays out space within a facility.
  - specifies door hardware and coordinates with factory re: door cuts.
- Electrical Engineer – ensures main electrical power is provided.
  - When designing a separate fire alarm system, coordinates its interface to cut power to fail-safe security door locks.
- Mechanical Engineer – HVAC.
  - Heat loads and duration of occupancy.
  - Ensures required environment is provided.
  - Security cabling must be coordinated with HVAC ductwork.
- Vertical Transportation Designer
  - Equipment for elevators – inside or outside cab.
  - Traveling cable, elevator machine rooms.
  - Escalators.

Construction Document Review, Approvals and Issue

- Set milestones to review progress:
  - By date, or
  - By percentage.
- Vulnerabilities are being addressed.
- Security program objectives are being met.
- Project remaining on budget.
- Scope of affected parties limited to portion that affects them.
- Changes early in the design process have less impact on cost.
- If formal approvals are required – obtain before issuing final construction documents.

- Final documents may need to be stamped – PE or architect.
    - Design liability passes to professional who stamps the drawings.
    - Security systems design work typically relies on low-voltage electrical systems, the need to stamp in infrequent and unnecessary.
- Complete set of Contract Documents (contractual details and construction documents) – may be issued to bidders.

Procurement Phase

3 major forms of security system procurement:

1. Sole source.
2. Request for Proposal (RFP).
3. Invitation for Bid (IFB).

- Type should be selected before or at the start of design phase.
    - Affects the level of detail required in construction documents.
- If vendor already onboard – sole source is appropriate.
- If vendor to be chosen competitively – Request for Proposal (RFP).
- IFBs key on a vendor's price to install and commission the systems specified.

Sole Source Procurement

- Small projects.
- Prequalifies a reputable security system contractor.
- Simple construction documents.
- Recommended only when security owner can perform the security needs analysis, and has prior knowledge of systems and prices.

Request for Proposal

- Based on a set of detailed design and construction documents.
- Specifications are Generic and Performance-based.
- Equipment models can be mandated or the phrase "or approved equal".
- Open to any contractor or limited to prequalified contractors.
- Responders may propose alternative solutions – "alternates".
- To compare properly, require the contractors to respond to the specified design and then, allow them to provide alternates and additional solutions.
- RFP does NOT restrict organization to lowest bid – BEST VALUE.
- Response to RFP takes longer because both a technical and cost proposal must be prepared.

Invitation for Bid (IFB)

- Used by government and other organizations requiring award be given to lowest qualified responsive bidder.
- No technical proposals or solutions are sought, so construction documents must be extremely explicit.
  - Design team selects equipment.
  - Award is the made without negotiation to lowest qualified bidder.
- Bids are commonly required to be sealed and delivered by specific time.
- Bids are opened (often publicly) and winner is announced.

Procurement Process

- May be important to hold a pre-bid conference – Rep. of each contractor.
  - Complete review of bid documents, and a walk-through.
  - Held approx. 1 week after construction documents issued for bid.
- Meeting minutes.
- Questions by contractors in writing – and answers transmitted to all prospective contractors.
- Proposals or bids are checked for accuracy.
- Life Cycle cost of each proposed system should be calculated.
  - Sum of capital cost and the maintenance cost over the useful life of the system.
  - Maintenance and warranty costs = 11 percent of total capital systems construction cost.
- If a low bidder has priced at low profit margin, they may make up the difference in high charges for maintenance.
- References should be checked before award decision is made.
- Negotiate final price on basis of VALUE.
- Business partnership – not a one-time sale.

Installation and Operation

Planning the Installation

- Plan correctly, everything in design package and on drawings.
  - Door hardware, sensors, cameras, console, etc.
- Contractor should visit site to confirm conditions agree with design package.
- Contractor should inspect, test, and document all existing physical protection equipment and signal lines that will be incorporated into the new system.

Component Installation

Card readers – suitable for surface, semi-flush, pedestal, or weatherproof mounting.
- In accordance with codes or standards or **authority having jurisdiction (AHI).**

Electric Door Strikes or Bolts

- Release automatically (fail-safe) or Remain secure (fail secure).
- Direct Current (DC) to energize the solenoids.
- Incorporate end-of-line resistors to facilitate line supervision.
- Solenoids, signal switches, tamper resistant (hardened), size and weight, mounting method.

Electromagnetic Locks

- Should contain NO moving parts.
- Depends solely on ELECTROMAGNETISM. (at least 1200 lbs. of holding force).
- Release automatically if power failure.
- End-of-line resistor for line supervision.
- Armature (internal circuitry), tamper resistance (hardened), mounting method.

Bell or Alarm Box

- front of facility in full view. Deterrent.
- High enough to be out of reach.

Control Panels

- located close to main entry and exit point.
- Should not be attached to combustible material.

Passive Infrared (PIR) Detectors

Door and Window Contacts

Shock sensors

- usually fitted to areas susceptible to forced entry (ie. panel on door).

Interconnection of Console Video Equipment

Signal paths:

- 25 feet or less	RG-59/U coaxial cable
- Longer	RG-11/U coaxial cable or Fiber-optic cable.

Cameras

- Connect, set, aim (aim sufficiently below horizon so camera will not directly face the sun), focus, synchronize.
- Exterior fixed mount

- Specified by manufacturer, proper sized mounting hardware, electrical and signal transmission cables, AC connection, pole wiring harness.
  - Ground rod for each camera pole.
- Exterior pan/tilt mount
  - AC power.

Monitors

- close to operators' eye level or lower.

Video recording and Switching Equipment

- Program the Video annotation for each camera.

Conduit

- Rigid, galvanized steel conduit (conform to UL standards).
  - Not required for same rack or cabinet.
- Tight tapered and threaded.
- Data transmission media should NOT be pulled into conduits with other building wiring.

Grounding

- Installed as necessary to keep ground loops, noise, and surges from adversely affecting system operation.

Enclosure Penetrations

- Should be from the BOTTOM unless otherwise required.
- Approved sealant.

Cold Galvanizing

- Cold galvanized paint – 95 percent zinc.

System Startup

- Do NOT apply power to the physical protection system until:
  - All PPS items set up, visual inspection, wiring has been tested, system grounding and transient protection, power supplies have been verified as to voltage, phasing, and frequency.

Configuration data

- all data needed to make the system operational into the PPS.
- Completed forms delivered to customer 30 days before database testing.

Graphics

- Contractor creates and installs the graphics needed to make the system operational.
  - Must have sufficient detail for the system operator to assess the alarm.

Signal and Data Transmission System (DTS) Line Supervision

- all lines should be supervised by the system by monitoring the circuit for changes or disturbances.
- System should initiate an alarm in response to a current change of 10 percent or greater.

Housing

- Interior sensors, Exterior sensors, Interior system electronics, Exterior system electronics, corrosive settings (housed in metallic enclosures), Hazardous environments (enclosures that meet the manufacturer's requirements.

Nameplates

- Laminated plastic nameplates provided for all major components of the system.
  - White with black center core.
  - Attached to inside of enclosure housing the major component.

Tamper Switches

- Cover-operated, corrosion-resistant tamper switches on hinged doors or removable covers.

Locks

- For maintenance purposes.
- "Do Not Duplicate".
- Keys can only be withdrawn in locked position.
- Key control plan.

Wire and Cable

- meet NFPA 70 standards.

Local Area Network (LAN) Cabling

Telecommunications Industry Association/Electronic Industries Alliance standard EIA-568 A or B, Category Five.

Quality Assurance

- all work and materials should conform to codes.

Tuning the System

- Tuned to the Operation of the Facility.
- Time periods for alarms
  - Patterns may emerge – alarms due to day-to-day operations.
- Responsibility for Monitoring Alarms
  - Constant alarms – to personnel in that area.
    - Maintenance – notify security first.
- Authorized personnel
  - SHUNTED so alarm will not be generated.
- Nuisance Alarms
- Improper application
  - Changed to eliminate nuisance alarms.

Maintaining the Operating Procedures

- Periodically reviewed.
- Changes should be documented with new revision number and date.
- Align awards and consequences:
    - Reward good security and consequences for not following operating procedures.
- Incident response policies – reviewed periodically by legal counsel.
- Consider the human element and staff procedures when designing.

Legal counsel assistance to avoid lawsuits:

Failure to adhere to duty guidelines – conduct beyond their established duties.
Breach of Duty – unreasonable conduct.
Proximate cause – officer was the immediate cause of injury.
Foreseeability – events that could have been determined were likely to happen.

Training

- without appropriate training, personnel are more likely to contribute to security risks accidentally.

General Training Requirements

- Proposal to conduct training courses for designated personnel in the operation and maintenance of the PPS.
- Training manuals and training aids provided to each trainee.
    - Additional copies archived at project site.
- All instructors – certified by equipment manufacturer for hardware and software.

Training Topics

System Administration

- Focuses on determining and implementing system operational parameters and making any necessary operational adjustments.
- First training class – 30 days before factory acceptance testing (if conducted) or site acceptance testing.
- Second training class – one week before start of acceptance testing.
    - System administrators should participate in acceptance tests and reliability testing.

System Monitoring

- Focuses on day-to-day system operation.
    - Monitoring alarm events.
    - Assessing, responding to, and clearing alarms.
    - Running routine reports.
- Each student should be able to start system, operate it, recover the system after a failure, and describe the specific hardware architecture and operation of the system.

Alarm Assessment and Dispatch

- teaches the PPS operators to assess the cause of different alarm conditions and properly deal with them.

Incident Response

- teaches the security response force about responding to different alarms and scenarios.

System Troubleshooting and Maintenance

- Focuses on the internal workings of the PPS so that students can troubleshoot and repair most problems.
    - System networking communications and diagnostics; device configuration and programming; controller setup, wiring, and diagnostics; software troubleshooting; and device programming.

IT Functions

- IT personnel need to understand how the security system functions within a LAN/WAN network infrastructure.
    - Network topologies and communications specific to each security subsystem, the impact of system functions such as digital video storage on network bandwidth, and the maintenance of data security.

System Overview

- How the system will help meet overall security goals and objectives.
- How the system has been customized to meet operational requirements.
- How to communicate security awareness to all employees.

Testing and Warranty Issues

- tests by implementation team involve equipment, personnel, procedures.
- The ideal acceptance tests stress the system up to the established limits of site-specific threats.
- Equipment Performance Testing
    - To determine if equipment is functional, has adequate sensitivity, and will meet its design and performance objectives.
        - NOT sufficient just to meet manufacturer's standards if the component proves ineffective during testing.
- Personnel Performance tests
    - To determine whether procedures are effective, whether personnel know and follow procedures, and whether personnel and equipment interact effectively.

Factory Acceptance Testing

- Contractor assembles a test system to demonstrate that system performance complies with specified requirements in accordance with approved factory test procedures.
    - Scheduled in advance of any installation of the new system.
    - Equipment for CCTV testing includes:
        - At least 4 video cameras and each type of lens specified.
        - 3 video monitors.

Site Acceptance Testing

- Plan to Calibrate and Test all components, verify data transmission operation, install the system, place the system in service, and test the system.
- Contractor to demonstrate that completed system complies with **ALL** contract requirements.

Reliability or Availability Testing

- Reliability testing shout NOT begin until acceptance testing has been satisfactorily completed, training completed, and all outstanding deficiencies have been corrected.
- Phase I Testing
    - Reliability test conducted 24 hrs./day for 15 consecutive days.
    - No repairs during this phase of testing unless authorized by customer.
- Phase I Assessment
    - Identify all failures, determine causes, repair failures, and deliver written report to customer.
- Phase II Testing
    - 24 hrs./day for 15 consecutive calendar days.
- Phase II Assessment
    - Identify all failures, determine causes, repair failures, and deliver written report to customer.

After-Implementation Testing

Operational tests

- performed periodically to prove correct system operation.
- Does not involve verification of equipment operating specifications such as detection patterns, or exact distance a door is opened.
- Checks if activation of alarms occurs.

Performance tests

- verifies the equipment conforms with equipment or system specifications.
- Determines probability of detection and may require additional measuring instruments or special testing methods.

Post-maintenance tests

- Operational tests conducted after preventative or remedial maintenance.

Subsystem tests

- ensures large parts of the system are all working together as originally designed.

Limited Scope tests

- used to test a complex system, which is broken down into several subsystems or segments that are tested separately.

Evaluation tests

- periodic, independent tests of the PPS to validate the vulnerability analysis and ensure that overall effectiveness is being maintained.
    - Performed at least once a year.

Warranty Issues

- Contractor – repair, correct, or replace --- 12 months from the date of issue of the certificate of practical completion.
- Common time to report to job site --- within 4 hours.
- Contractor to hold sufficient stock of spares.
- Warranty should include full maintenance.

Maintenance, Evaluation and Replacement

- Plan to minimize the potential for and impact of failures.
- Facility technicians, augmented by contact representatives to perform all tests, maintenance, calibrations, and repairs to keep PPS operational.
- Normally a system maintenance agreement includes Remedial and Preventative maintenance.
- Select a single contractor to take responsibility and to manage the process.

Remedial maintenance

- may be done by manufacturer, system integrator, maintenance contractor, users, or any combination. (Different skills may be required).
- Train staff to perform preventative maintenance.
- Consider periodic tuning of the security system.
- Service Levels:
    - Support plan and appropriate service level and response times for each component.
    - Components with high impact on system requires higher level of support. Extreme case = Engineer on-site with spares on hand.
    - Service levels that are realistic, measureable, and in accord with the organization's specific business needs.
    - Costs depend on location of system and ability for remote access.
- Roles and Responsibilities:
    - Minimize number of different parties involved in managing the maintenance program. All responsibilities clearly defined.
    - Company's central point of contact.
    - Facilities agreements between the parties.
        - Prime vendor or system integrator should manage the process.

- <u>Prices and Payments</u>
    - Scale of fees for support of products and delivery of services.
    - Fee may be a set percentage of the purchase price.
    - May be affected by geographic location of the system.
    - Economies of scale may affect pricing.
        - Large number of other customers in area.
    - NOT covered – misuse, vandalism, lack of training due to turnover, acts of God, etc.
- <u>Administration</u>
    - Security manager should regularly review the agreement, measure the provider's performance, and address the agreement's scope.
- <u>Documentation</u>
    - Configuration of the system and all components, switch settings, cable diagrams, spare parts lists, and installation steps, diagnostics, remote diagnostics.
    - <u>Upgrade service</u> – guarantees the latest engineering change orders and field orders --- extends system life.
- <u>Records</u>
    - Maintenance and operator records.
    - Keeping track of costs helps justify replacing unreliable systems.
    - <u>Maintenance records</u>
        - Kept to identify repair patterns.
        - Continuous log should be maintained for all devices.
    - <u>System Operator Records</u>
        - Problems operators have with subsystems or components.
        - Analyzed periodically to update operating procedures.
    - <u>Spare parts</u>
        - Procure spare parts and repair in advance.
        - 5% of capital cost of equipment allocated each year.
    - <u>Maintenance manuals</u>
        - For all equipment.

<u>Preventative maintenance</u>

- Checklists should be developed.
    - Incorporate guidelines from manufacturers.
    - IT support.
- Maintenance activities should be simultaneous with remedial maintenance.
- <u>Adjustments</u>
    - Periodically to ensure operating effectively.
    - Detection patterns for motion sensors – adjusted based on results of testing activities.

Backup Equipment

- Auxiliary power source – batteries or generators.
  - Switchover must be immediate and automatic.
  - Batteries required until generator comes up to full power.
- Regular test and maintenance program.
- Records of tests should be kept.

Evaluation and Replacement

- the system will complete its useful life and the process of replacement will begin.
- Security manager should form a team of stakeholders to select a system that will meet all stakeholders' needs.
- Build in considerable expansion potential for future plans.
- Include IT – which would have to work with it.
- Include HR – interface between employee database software and security system software.

Appendix A Estimation

Types of Cost Estimates

Budgetary Estimates

- prepared during initial planning phase of a new PPS.
- Used for getting new PPS into budget cycle.
- Large contingency – +/- 10 to 20 percent.
- Difficult to prepare without actually performing a good portion of system design.
- RSMeans – company that provides construction cost information.

Preliminary Design Estimates

- if PPS is part of a larger construction project.
- Developed at 50% design review stage.
- +/- 10%.

Final design Estimates

- developed using completed documents, drawings, and schedules.
- Minimal contingency - +/- 5%.

Life-Cycle Cost – actual cost of a PPS.

- Engineering and design costs; hardware; software; installation; operating costs; maintenance costs; other:
- (taxes, profit 10%, performance bonding 3-5%, and contingency 5%);
- Adjustments – RSMeans data are based on national averages and may need to be adjusted.

Detailed Estimating Procedures

Identify PPS subsystems:

- fences and barriers; security control, monitoring center; access control subsystem; CCTV subsystem; intrusion detection interior and exterior subsystem; lighting; power control and data distribution; communications subsystem; search equipment.

Identify other installation activities:

- Site preparation – civil or structural modifications; specialty construction.
- Develop a list of components for each subsystem.
- Establish component prices.
- Estimate installation labor.
- Identify required special equipment and rates.
- Use spreadsheet program – to compute the estimate for the project.

- use actual cost data or recent quotes from vendors.
- Quality review – comprehensive review to ensure all components are listed and in the correct quantities.

Summary of Costs:

Components
Tax and shipping
Installation labor
Subtotal
Profit (10%)
Subtotal
Performance Bond
Total cost estimate

Appendix B Specification

Part 1: General

- Authority and responsibility.
- Summary
- Objectives – so all bidders can understand what the system is intended to achieve.
    - SMART – specific, measureable, attainable, relevant, timebound.
- Submittal format – the outline and format for the proposals and specifies all items to be included in submittal.
- Performance Specifications – functional performance requirements for the system and equipment.
- Future Expansion
- System Interfaces – other systems that will or might be connected.
- Codes and Regulations – all relevant regulations.
- Customer-Supplied materials and services.
- Scheduling – time frame for contract placement and job completion.
- Statement of Compliance – statement that the system proposed and priced complies with the specification.
- Indemnity and Insurance
    - Contractor should indemnify and keep indemnified the customer.
    - Minimum of $1 million.
    - Expected to produce evidence of sufficient insurance coverage.
- Bonds:
    - Surety Bond – 3 party instrument between:
        1. Surety (insurance company).
        2. Contractor.
        3. Customer or project owner.
    - if the contractor unable to successfully perform the contract, the surety assumes the contractor's responsibilities and ensures that the project is completed.
    - 4 types of contract bonds:
        - Bid – guarantees bidder will enter into contract.
        - Payment – guarantees contractor will pay subcontractors.
        - Performance – contractor will perform the contract.
        - Ancillary – incidental and essential.
- Modifications and variations – written consent.
- Notification – notify customer immediately of any unforeseen circumstances.
- Warranty – 12 to 24 months from the date of issue of the certificate of practical completion.
    - Common report time to job site = 4 hours.
    - Sufficient stock of spares held by contractor.
    - Full maintenance of equipment in accordance with the manufacturer's recommendations.

- Maintenance – contractor should submit a full schedule of maintenance.
    - Contractor to install all hardware and software updates and upgrades.
    - Protects a customer from accepting an obsolete system.

Part 2: Products – equipment.

1. Specify every item by manufacturer and model number, or
2. Produce a performance-related specification with generic device descriptions.
    a. Performance specification leads to the most competitive prices.
    b. Another common technique is “or equal”.

Non-Proprietary Equipment

- all equipment must be commercially available, off-the-shelf products.
- Ensures future extensions to system may be carried out by any installing company.

Part 3: Execution

- Preparation of the site – condition of site and work to be done.
- Installation and quality control standards.
- Trade Coordination – with other contractors.
- Subcontracting:
    - Express written consent of customer required.
    - Intention must be clear in bid submission.
    - Customer should reserve the right to accept or reject.
- Special equipment – contractor provides.
- Health and safety – comply with all:
    - AHI – authority having jurisdiction.
- Preassembly and testing – prebuilt and tested at contractor’s premises before being delivered.
- Testing and Commissioning – certificate of completion issued after successful completion of reliability testing.
- Operating Instructions – provided by contractor.
- As-built drawings – contractor provides.
    - As-built wiring and schematic diagrams.
- Training – what, when, and where. Training materials and qualifications of trainer.
- Programming – done by contractor for all subsystems.
- Upgrades – contractor should provide at no cost during warranty period.