NISTIR 89-4027

Preliminary Performance Criteria for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities

Robert D. Dikkers, Robert J. Husmann, James H. Webster,
John P. Sorg, and Richard A. Holmes

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(Formerly National Bureau of Standards)
National Engineering Laboratory
Center for Building Technology
Building Environment Division
Gaithersburg, MD 20899

January 1989

Prepared for
U.S. Department of Justice
National Institute of Corrections
Washington, DC 20534

NISTIR 89-4027

Preliminary Performance Criteria for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities

Robert D. Dikkers[1], Robert J. Husmann[2], James H. Webster[3], John P. Sorg[4], and Richard A. Holmes[5]

[1]U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(Formerly National Bureau of Standards)
National Engineering Laboratory
Center for Building Technology
Building Environment Division
Gaithersburg, MD 20899

[2]Omni Signal, Inc.
Capitola, CA 95010

[3]Architect
Arlington, VA 22207

[4]Consultant
Annandale, VA 22003

[5]Sure-Lock Holmes, Inc.
Albany, NY 12203

January 1989

National Bureau of Standards became the National Institute of Standards and Technology on August 23, 1988, when the Omnibus Trade and Competitiveness Act was signed. NIST retains all NBS functions. Its new programs will encourage improved use of technology by U.S. industry.

Prepared for
U.S. Department of Justice
National Institute of Corrections
Washington, DC 20534

U.S. DEPARTMENT OF COMMERCE
C. William Verity, Secretary
Ernest Ambler, Acting Undersecretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Raymond G. Kammer, Acting Director

PREFACE

This study was sponsored by the National Institute of Corrections, U.S. Department of Justice. Points of view or opinions stated in this report do not necessarily represent the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The authors greatly appreciate the helpful comments and suggestions of the following individuals who represented organizations interested in this project and who agreed to serve on a review committee to discuss a draft of this report:

Sheriff James W. Black Larimer County Sheriff's Dept. Ft. Collins, Colorado	National Sheriffs' Association
Mr. James E. Murphy Criminal Justice Services College Park, Maryland	ACA Adult Local Detention Committee
Chief James W. Painter Los Angeles County Sheriff's Dept. Los Angeles, California	American Jail Association
Mr. Allen L. Patrick Patrick + Associates Columbus, Ohio	AIA Committee on Architecture in Justice
Mr. Francis J. Sheridan NY Dept. of Correctional Services Albany, New York	ACA Design and Technology Committee

We also gratefully acknowledge the following individuals who have provided encouragement and support for this project: Mr. Robert O. Viterna, Chairman, ACA Adult Local Detention Committee; and Mrs. Norma Phillips Lammers, Executive Officer, California Board of Corrections.

Finally, we greatly appreciate the financial sponsorship received from the National Institute of Corrections (NIC) and the advice and encouragement obtained from NIC staff (Raymond C. Brown, Director; Susan Hunter; and Thomas Fisher).

INTRODUCTION

Background

Because of the rapid increase in new jail and prison construction, and the lack of performance criteria and standards for building materials, equipment and systems used in such facilities, many correctional agencies have experienced equipment and system performance problems in their facilities. In some instances, these problems have necessitated expensive facility retrofits, repairs, or other fixes. In September 1986, the National Institute of Corrections (NIC), U.S. Department of Justice, initiated a study at the Center for Building Technology, National Bureau of Standards (NBS)[1]. The general objective of this study is to develop guidelines, test methods and the technical bases for standards which would assist in the selection, application, and maintenance of building materials, equipment and systems for use in detention and correctional facilities.

During the first year of this study, the primary focus was on determining the state-of-the-art in the design and construction of detention and correctional facilities. The data and information on the performance of various materials, equipment and systems, along with information on available guidelines and standards, were incorporated into a NBS report published in November 1987[2]. Based on information presented, it was concluded that performance criteria and various standards are needed to improve the selection of materials, equipment and systems. A document containing performance criteria for detention and correctional facilities was identified as one of the high priority activities by a NBS Project Review Committee. This Review Committee consisted of representatives from the National Sheriffs' Association, Association of State Corrections Administrators, American Jail Association, American Correctional Association (ACA) Adult Local Detention Committee, ACA Design and Technology Committee, and the AIA Committee on Architecture for Justice.

Objectives

The preliminary performance criteria contained in this report have the following objectives:

a. Establish performance levels for building materials, equipment and systems which are consistent with the security and custody levels used in detention and correctional facilities.

---

1. On August 23, 1988, the National Bureau of Standards became the National Institute of Standards and Technology (NIST).

2. "Standards for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities," Robert D. Dikkers, Belinda C. Reeder, NBSIR 87-3687, November 1987.

b. Establish standard performance measures with regard to security, safety and durability for building materials, equipment and systems.

When completed, these performance criteria are intended to serve as a technical resource and reference for correctional officials, architects, engineers, material and equipment manufacturers, contractors, and standards writing organizations. The criteria are also expected to benefit jail and prison building programs by providing a technical performance assessment base from which project specifications and uniform methods for evaluating materials, equipment and systems can be developed.

Scope

Part I (Chapters 1 - 4) of this report contains general considerations pertaining to the overall facility -- its mission, security levels, and operation; and various options and issues relating to the selection of the facility site. The purpose of this part is to point out some considerations which should be examined to help ensure that the systems, materials, and equipment specified and selected will be consistent with the mission, security levels, and services and programs of the proposed facility.

Part II (Chapters 5 - 8) contains requirements and criteria relating to the perimeter security of the facility. The primary systems discussed are perimeter fencing and intrusion detection systems.

Part III (Chapters 9 - 15) includes requirements and criteria pertaining to various building systems. Systems covered are: walls, floors/roofs, doors, windows, glazing, locks and locking devices, control center, alarms and communications.

Format

Except for Chapters 1 - 4 and 6, performance statements in this preliminary report are presented in the Requirement, Criterion, Evaluation, and Commentary format.

The Requirement is a qualitative statement giving the user need or expectation for the item being addressed. It is a general statement of what the system or its components should be able to do.

The Criterion is generally a quantitative statement giving the level of performance required to meet the application or expectation for the item being addressed. The criteria associated with each requirement state those considerations necessary to meet the requirement. Due to limitations in the state-of-the-art, a quantitative statement is not always contained in each criterion. In addition, quantitative statements are intentionally omitted in some criteria where values are to be provided by the owner or designer.

The Evaluation sets forth the record of experience, methods of test and/or

other information upon which an evaluative judgement of compliance with a criterion will be based. It states the standards, inspection methods, analyses, review procedures, historical documentation, or other methods that may be used in evaluating whether not the system and its components comply with the criterion.

The Commentary provides background information and presents the rationale behind the selection of specific data presented in the Requirement, Criterion or Evaluation. The Commentary is intended for informational purposes and in some instances, provides design guidance. Such guidance is only a suggestion of appropriate methods; in most instances, there will be other methods equally as effective. Including a commentary ensures a workable process of updating performance criteria, and when questions arise as to the basis for a particular criterion, the reader will have available the rationale for its selection.

Note: At this time, due to limitations of current knowledge, it has not been possible to develop performance levels and standard performance measures for all materials, equipment and systems discussed in this report. Accordingly, the reader will note that some criteria are expressed more in "prescriptive" or "guide specification" terms rather than in preferred "performance" terms.

Future plans

The performance criteria in this report should be considered as preliminary in nature. Accordingly, review comments and suggestions are encouraged and should be directed to: Robert D. Dikkers, Group Leader, Building Security, Center for Building Technology, National Institute of Standards and Technology, Building 226, Room B320, Gaithersburg, MD, 20899.

Future plans are to revise this report on the basis of review comments and suggestions received. In addition, it is anticipated that other systems (e.g., lighting, CCTV, fire safety) not covered herein will also be included in a future revised report.

TERMINOLOGY[3]

ACA: American Correctional Association.

AMS: Alarm monitoring system.

And/or (circuits): "and" circuits" and "or" circuits are derivations of and/or gates which are logic terms associated with computers and other electronic functions. "And" is used to mean that sensor one and sensor two must both be activated to create an alarm. Either sensor, by itself, can create an alarm in an "or" circuit.

ASTM: American Society for Testing and Materials.

Barriers: Any physical object that is constructed to hinder an individual from transiting an area. Fences, barbed tape, and walls are all examples of barriers.

Bi-static: Permanently mounted sensing devices that consist of a transmitter and receiver pair; i.e., microwave, infrared, laser.

Breaching aids: Any device or tool which might be used in an attempt to escape detection by sensors or facilitate the overcoming of a barrier.

Buffer area/zone: A clear space devoid of buildings, trees or other objects that could be used for concealment.

CCTV: Closed circuit television.

Channeling: A design plan that forces or encourages several people to use the same path through a perimeter barrier.

Coplanar: Two or more sensing systems that occupy essentially the same space such that an individual who causes an alarm on one sensor will simultaneously cause an alarm on the other sensor(s).

Correctional facility (or prison): A facility, usually under a state or federal agency, which has custodial authority over persons sentenced to confinement for more than one year.

Cylinder plug (or core): The central part of a cylinder, containing the keyway, which is rotated by the key to operate the key mechanism.

Custody: The degree of staff supervision necessary to ensure adequate control of an inmate.

---

[3] The definitions given here are for use in this document only.

Dead bolt: A lock bolt which does not have an automatic spring action and a bevelled end, as opposed to a latch bolt which does.

Dead lock: A lock equipped with a dead bolt. Also, a lock having a mechanical blockage which prevents opening of a snap lock or the movement of a sliding door.

Defeat: (As applied to sensors) The act of transiting through the sensor without detection. (As applied to barriers) The act of passing through, over or under a barrier in a shorter time frame than would be expected.

Deploy: Construct; utilize.

Detention facility (or jail): A facility which holds persons detained pending adjudication and/or persons committed after adjudication for sentences of generally less than one year.

Dry cell: A cell with no toilet or lavatory fixtures.

E-Field: (As applied to sensors). Sensors which generate an electrostatic field along a combination of parallel field and sensing wires.

EMI: Electromagnetic interference.

Escutcheon plate: A surface-mounted cover plate, either protective or ornamental, containing openings for any or all of the controlling members of a lock such as the knob, handle, cylinder or keyhole.

FAA: Federal Aviation Administration.

False alarm: An alarm that can not be attributed to some environmental phenomenon (i.e., an alarm caused by faulty components, loose wire connections, etc.)

Frame: The component that forms the opening of and provides support for a door, window, skylight, or hatchway.

Head: Top horizontal member of a door or window frame.

Jail: See detention facility.

Jamb: The exposed vertical member of either side of a door or window opening.

Joint domain: A design that incorporates two or more sensors in a manner that both or several sensors must be activated within a certain time frame for an alarm to occur.

Keeper (or strike): A metal plate attached to or mortised into a door jamb to receive and hold a projected latch bolt and/or dead bolt in order to secure the door to the jamb.

Latch bolt: A metal lock component having a beveled end which projects from the lock front (or face) by spring action in its extended position, but may be forced back into the lock case by end pressure or drawn back by action of the lock mechanism. This type of bolt is used in slam locking.

Lever tumbler lock: A key-operated lock that usually incorporates five or more lever tumblers, which must be raised to a specific level so the fence of the bolt is aligned with the gate of each tumbler in order to withdraw the bolt.

Light: A space in a window or door for a single pane of glazing. Also, a pane of glass or other glazing material.

Master keying: A method of keying locks which allows a single key to operate multiple locks, each of which will also operate with an individual change key.

Member: A part or segment.

Mogul cylinder: A heavy-duty pin tumbler cylinder. The diameter of a mogul cylinder is generally about twice the diameter of a normal cylinder. Generally used for mechanical operation of electric locks.

Nuisance alarm: An alarm that can be attributed to some environmental phenomenon such as wind, rain, snow, animals, etc.

Outriggers: Limb-type devices attached to the top of fence posts that support multiple strands of barbed wire or tape. Commonly used on chain link fences to inhibit climbing over the fence.

Paracentric: A term used in connection with keyway cylinder plugs having projections on the sides of the keyway that extend beyond the vertical center line of the keyway. A form of a ward, used primarily to make picking more difficult and to limit the accessibility of the keyway to prescribed key designs.

Pin tumbler lock: A lock having a cylinder employing metal pins (tumblers) to prevent the rotation of the core until the correct key is inserted into the keyway. Small coil compression springs hold the pins in the locked position until the key is inserted.

Prison: See correctional facility.

Perimeter corridor: The span of ground surrounding a facility that is allotted to both perimeter sensors and fencing.

Sally port: An enclosure or vestibule with doors or gates at both ends, only one of which opens at a time.

Sanitized: The process of clearing an area of vegetation and providing means for blocking the intrusion of small animals and debris.

Sash: A frame containing one or more lights.

Security level: The nature and number of physical design barriers available to prevent escape and control inmate behavior.

Sensor zone: An area that contains one or more sensors and is defined as a specific zone for the purpose of response to an alarm.

Shall: Term used to indicate a provision (requirement or criterion) is mandatory.

Should: Term used to indicate a provision (requirement or criterion) is not mandatory, but is recommended as good practice.

Sill: The lower horizontal member of a door or window opening.

Spoofing: (As applied to perimeter sensors) The act of causing nuisance alarms, erratic behavior, or insensitivity to human presence.

Sub-system: A device or group of devices, electronic or mechanical, designed to be an integral part of a larger system.

Transverse: Cross over or pass through.

UPS: Uninterruptable power supply.

Venetian effect: The blocking or inhibiting of a normal view because of a angular collective effect of many small objects that are spaced such that they would not individually block the view if seen from a different angle.

Ward: An obstruction within the lock which prevents the wrong key from entering or turning in a lock.

Wet cell: A cell with toilet and lavatory fixtures.

PART I - FACILITY AND SITE

CHAPTER 1

FACILITY MISSION

CHAPTER 1

FACILITY MISSION

1.0 Introduction

Part I (Chapters 1 through 4) of this document provides general background information to aid in the facility development process, including the selection of materials, equipment and systems for detention and correctional facilities. Accordingly, the primary audience for this part is the new or less experienced professional in the corrections field who may be assigned some responsibility for the planning, design and construction of a new facility. Such professionals may also wish to refer to other publications which provide more detailed information and guidance (e.g., Planning of New Institutions [1]*; Design Guide for Secure Adult Correctional Facilities [2]; Jail Planning and Construction Guide [3]; More for Le$$ - Jail Construction Cost Management Handbook [4]; Correctional Facility Planning and Design [5].)

This chapter sets forth important factors that should be considered in the development of the facility mission. The mission will influence the selection of many systems and materials to be used in the facility. For example, if the facility is "maximum security", the selection of the doors and locking systems would reflect the maximum security mission. A medical treatment mission would affect the selection of mechanical and communication systems. These considerations, along with other elements that need to be evaluated in the facility development process, will also impact the physical layout and other attributes of the facility.

The mission of a correctional facility differs significantly from that of a detention facility. The differences must be recognized when selecting or evaluating the performance of systems and materials. A detention facility will generally house prisoners for a short period of time and consequently large numbers of people are processed yearly through the facility on a daily basis. Materials must be able to withstand more wear and tear in a detention facility versus a correctional facility. The behavior of prisoners in a detention facility is more unpredictable than inmates in a correctional institution. Therefore, a greater percentage of secure cells should be available in a jail as compared to a medium security correctional facility.

1.1 General. Certain physical requirements should be considered before the design and construction of detention and

* Numbers in brackets [ ] indicate references at the end of this chapter.

correctional facilities can begin. Among these are factors which help determine the mission of the facility -- the number of inmates, their age, sex, adjudication status, and physical and mental health condition.

The number of inmates in the facility is the most significant criteria for its design. The ACA Standards identify a 500 bed facility as being the most ideal [6]. However, many state and county jurisdictions must build facilities with capacities far greater than ACA's recommendation. The mission of larger facilities must provide services and programs for its inmates regardless of the size of the facility.

In the past, the physical and mental health needs for inmates were minimal. They were basically healthy people. The mental institutions cared for the insane and sociopathic individuals. Those needing medication or mending were treated at the local hospital and brought back to the facility to recuperate. Today, however, conditions are quite different. Many mental institutions have been closed and many of the former patients are living in the streets until they violate some law. Then they are housed in detention or correctional facilities. Medical needs are also different. Many hospitals are not equipped or do not want to deal with inmates under the influence of drugs or those with contagious diseases. The incidence of Acquired Immune Deficiency Syndrome (AIDS) among inmates has caused great National concern. In many of the older correctional facilities, it is impossible to adequately segregate AIDS infected inmates from the rest of the inmate population. The projected mission of a new facility should include provisions for dealing with these new medical problems.

1.2 Number of inmates by age and sex. The number of youth, adult and geriatric men and women housed in the facility will be a major factor in determining the mission.

Youth and young adult men and women normally require more programs than do the older inmates. The educational and vocational training space should be more than that required for adult facilities. Adults serving long sentences will have less need for educational and job skills training but will require more industrial work space. Other than housekeeping chores, the geriatric inmates require little vocational or industrial work space. They will, however, need space without long flights of stairs. They also should be protected from those inmates who might prey upon the more helpless inmates. A change in an institution's mission

with no regard for the amount of available program space can create unanticipated costs, security problems or an inappropriate use of the facility and its staff.

1.3 Unsentenced and sentenced inmates. Sentenced inmates should generally be housed out of sight and sound from those who are unsentenced.

The unsentenced inmates are basically housed in detention facilities and are concerned with their Court appearances. They need to have frequent contact with their attorneys and families. The ideal location for a detention facility would be adjacent to the Court buildings complex. Some options to this location would include provisions to locate some court functions to a suburban location with the detention facility or the use of closed circuit television for some of the pretrial adjudication activities. These options would lessen the risk from some unsentenced inmates who are dangerous and unpredictable. The requirement to transport such inmates long distances to Court is expensive and places corrections staff in jeopardy.

1.4 Mental health and medical isolation. The mission of the facility should include provisions for the detention and treatment of inmates with mental deficiencies and contagious diseases.

The provision for treatment and care of the mentally ill is becoming increasingly necessary in correctional facilities. The increase in incarceration of those with AIDS has led the Federal Prison System to begin tests and screening of all Federal offenders. Some state systems have followed this practice. In all correctional systems, a policy will be necessary to protect staff and the uninfected inmate population from contamination by the AIDS virus. The National Institute of Corrections, the American Correctional Association, and the National Sheriffs' Association have been actively engaged in studies and symposiums on the impact of AIDS-infected inmates within the United States Corrections System.

1.5 Drug addiction treatment. The mission of the facility should include provisions for housing inmates with a dependency on drugs.

The assumption that a drunk tank will solve a jail's drug problems is no longer valid. Alcohol is still the nation's number one debilitating drug. However, mind-altering drugs are now being used which truly bring out the beast in man.

Those people high on such drugs can sometimes reach super human strength and endurance. Adequate provisions must be made to allow corrections staff to deal with these inmates. The facility mission concerning drug users must focus on today's problems. However, the facility design must be flexible enough to deal with changes in the medical treatment of drug offenders. One example of design flexibility would be to design housing units that are near the hospital so they can be included as part of the medical program when necessary.

Chapter 1 - References

1. Planning of New Institutions, NIC Jails Division, Boulder, CO, 1986.

2. Design Guide for Secure Adult Correctional Facilities, American Correctional Association, College Park, MD, 1983.

3. Jail Planning & Construction Guide, Nebraska Jail Standards Board, Nebraska Commission on Law Enforcement and Criminal Justice, 1987.

4. More For Le$$ -- Jail Construction Cost Management Handbook, prepared by Kitchell CEM for State of California Board of Corrections, 1987.

5. Correctional Facility Planning and Design, Jay Farbstein, Van Nostrand Reinhold Company, Inc., Second Edition, 1986.

6. "Standard 2-4160," Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

CHAPTER 2

SECURITY LEVELS

CHAPTER 2

SECURITY LEVELS

2.0 Introduction

This chapter sets forth general considerations that should be evaluated in determining the security levels of the facility. These considerations directly affect the selection of materials, equipment and systems to be used in the facility.

2.1

Inmate classifications. The task of defining the security classification of inmates is now and has always been a difficult one. The maximum security group are easy to recognize. They are escape risks, aggressive and sometimes dangerous. They are typically serving a long sentence before any chance of parole. Many of the maximum security inmates are difficult to confine. A large number of the inmates serving long sentences were involved in the distribution of illegal drugs. They frequently are both intelligent and ruthless, and have time to find a weakness in the security systems. Some also have money to buy outside help for an escape attempt.

However, the classification which is the most difficult to identify is medium security. Somewhere between maximum and minimum is the vast majority of inmates in the correctional systems in the U.S. today. They are serving one to three year sentences. Some are violent, some young and unpredictable, and some will escape if given a chance. Others in medium classification are minimum security inmates who have a detainer on them by another jurisdiction. This means that once the current sentence is served the inmate will be transported to another jurisdiction for prosecution and perhaps serve additional time for another crime. This situation can increase the risk of escape and causes the inmate to serve time as medium custody.

The uncertainty of the meaning of medium security and the shifting nature of the confined population has led many correctional systems to erect identical perimeter security barriers for maximum or medium facilities. This makes sense in two ways. First, the difference between maximum and medium classifications is not as critical for those having to make the decisions. Second, future needs may dictate more or less of one security type and a change in inmate control would be less costly to accomplish. In some cases, only the addition or reduction of staff could change the security levels without rebuilding the facility. See additional discussion in Part II on facility security levels vs. perimeter security levels.

2.2 Facility security level. Facility security level has been defined as "the nature and number of physical design barriers available to prevent escape and control inmate behavior [1]*."

The definition and number of security levels for jails and prisons varies among different jurisdictions (local, state, and Federal). The National Institute of Corrections (NIC) has identified five different levels of prison security. They are: Maximum, Close, Medium, Minimum, and Community [2]. Often, different areas of a single institution provide different security levels. The use of measures such as perimeter security, existence and operation of towers, use of external patrols and detection devices, and housing arrangements, to differentiate institutions by security levels is shown in Table 2.1. In this report, the primary focus is on only three security levels -- maximum, medium, and minimum.

A detention facility, however, must generally rely upon the building perimeter to provide the primary security barrier. The prisoners are classified as either needing secure confinement in cells or can be adequately housed in dormitories. The minimum security inmates are the housekeeping workers in the jail and are usually serving less than one year.

2.2.1 Maximum security facilities. The buildings, building equipment and systems, and furnishings should provide a level of performance consistent with a maximum security use.

Housing in maximum security facilities generally consists of small numbers of cells in a living unit. Some state standards have limitations on the number of cells allowed in a living unit. Single occupancy cells should have a remote controlled dead bolt locking system. Doors should be swinging or sliding and generally made of steel. A stainless steel combination toilet and lavatory, and a stainless steel mirror should be provided in each cell. A secure lighting fixture and all furnishings such as bed, desk, stool and locker should be anchored to the floor or wall. Some jurisdictions use a raised concrete slab for a bed. (Note: See Part III for detailed guidance on the selection of various equipment and systems.)

* Numbers in brackets [ ] indicate references at the end of this chapter.

Table 2.1 - Security Levels [2]

SECURITY SYSTEM	COMMUNITY	MINIMUM	MEDIUM	CLOSE	MAXIMUM
PERIMETER	None	Single fence and/or unarmed "posts"	Secure	Secure	Secure
TOWERS	None	Optional (manned less than 24 hrs.)	Manned 24 hrs.	Manned 24 hrs.	Manned 24 hrs.
EXTERNAL PATROL	None	Intermittent	Yes	Yes	Yes
DETECTION DEVICES	None	None	Yes	Yes	Yes
HOUSING	Single rooms and/or multiple rooms	Single rooms, multiple rooms and/or dorms	Single cells or rooms and/or dorms	Single outside or inside cells	Single inside cells

Definitions:

Secure perimeter - Walled or double-fenced perimeter with armed towers. All entry and exit into and out of the compound is via sally ports.

Inside cell ------ A cell which is contained on four sides within a cellhouse; i.e., if an inmate escapes from the cell, he is still confined within the building.

Outside cell ----- A cell with a wall or window immediately adjacent to the outside of the building; i.e., if an inmate escapes from the cell, he has escaped from the building.

Written policy should identify the inspection frequency for cells, furnishings and inmates' personal property. Staff should look for vandalism, normal wear and tear and defects in the equipment and furnishings. The cell and the inmate's personal property should be inspected for contraband items [3,4].

The maximum security environment expects and usually gets the worst behavior possible from inmates. The only housing more harsh than maximum security is segregation housing which is exactly the same except it is equipped with a secure light fixture, a stainless steel toilet and lavatory, and is furnished with only a bed. Maximum security housing can sometimes be used for protective custody housing. In this instance, the inmates are not only dangerous but are at risk of being harmed by other inmates who may try to breach security. The protective custody housing units should be designed to be out of sight and sound of other housing. Exercise and other program activities are provided within or contiguous to the housing unit.

2.2.2 Medium security facilities. The buildings, building equipment and systems, and furnishings should provide a level of performance consistent with a medium security use.

Housing in medium security facilities generally consists of living units of between 50 and 100 cells each. Single occupancy cells may have key operated doors with a dead bolt override from a remote location. In some instances, inmates carry the key to their cells. Equipment and furnishings in the cells are at the discretion of the various correctional agencies. However, the furnishings need not be anchored to the floor or walls. Sometimes electric outlets are provided for inmates personal sound and television equipment. The outlets should be Ground Fault Interrupters (G.F.I.) to protect inmates and staff from accidental shock.

Written policy should provide for inspections of cells and inmates' personal property. The procedure for cell inspections should be the same as for those in the maximum security housing [3,4].

Medium security institutions are generally programmed to provide work, training and leisure activities that keep inmates out of the housing units for most of the day. The cell, in effect, becomes a bedroom. Dayrooms provide relief from confinement in the cells and consequently the cells can be smaller than those in maximum security facilities. The ACA Standards recognizes this difference and recommends smaller square footage allowances in medium security cells for those confined in cells less than 10 hours a day [5].

2.2.3 Minimum security facilities. The buildings, building equipment and systems, and furnishings provide a level of performance consistent with a minimum security use.

Housing units in minimum security facilities generally house up to 100 inmates each. Housing may be wet cells, dry cells or dormitories. The dormitories should provide 50 square feet per inmate in the sleeping area [6] and 35 square feet per inmate in the dayroom space [7].

Written policy provides for inspections of housing and inmates personal property to insure that fire safety and personal hygiene standards are met.

Minimum security facilities usually have programs that provide work opportunities for able-bodied inmates. In some correctional systems, the minimum security facilities include large agricultural operations. Inmates are able to work outside with a minimum of staff supervision.

Chapter 2 - References

1. Guidelines for the Development of a Security Program, James D. Henderson, W. Hardy Rauch, American Correctional Association, College Park, MD, 1987.

2. Prison Classification -- A Model Systems Approach, National Institute of Corrections, Washington, DC, 1983.

3. Standard 2-4192, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised March 1983.

4. Standards 2-5179 and 2-5180, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

5. Standard 2-4132, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised August 1986.

6. Standard 2-4131, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised August 1986.

7. Standard 2-4137, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

CHAPTER 3

OPERATIONAL CONSIDERATIONS

CHAPTER 3

OPERATIONAL CONSIDERATIONS

3.0 Introduction

This chapter sets forth general considerations relating to the overall operation of the facility. These considerations pertain to the services and programs to be provided; the heating and cooling requirements; transportation, motor pool, and fire station requirements; and preventative maintenance.

3.1 Services and programs. The operation of a facility includes provisions for all of the service and program functions.

The service functions include health care, food service, maintenance, laundry, barber shop and canteen. The majority of the inmate work force is used within these functions. The program functions consist of education, vocational training, industrial work, religious, therapeutic, visiting and leisure activities. The purpose of the program functions is to offer an inmate an opportunity for self improvement.

The ability of a material or a system to perform adequately is affected by the use of inmate workers. Floors and walls endure a constant buffeting by the inmate housekeepers. Stair surfaces are worn down much faster than those in typical commercial buildings due to the almost constant inmate traffic. Adding vandalism and physical abuse to the wear and tear of a material leaves few choices in a correctional facility other than durable materials such as concrete, masonry and steel. Recent experience in direct supervision facilities, however, indicates reduced vandalism and graffiti, and opportunities to utilize other materials, thereby reducing both construction and operating costs [1]*.

3.2 Heating and cooling requirements. The site and its geographic location determines the heating and cooling needs of the facility.

An early aid when considering the type of heating and cooling system to use is an life-cycle cost evaluation of various mechanical systems. The mechanical system for a correctional facility must include provisions for smoke evacuation, proper location of filters, and protection of equipment and controls from vandalism. The type of fuel is dependant on geographic location and availability of certain fuels. Those areas with abundant supplies of coal or fuel

* Numbers in brackets [ ] indicate references at the end of this chapter.

oil are ideal for central power plant designs. The power plants can be located either inside or outside the perimeter security. In medium and minimum security facilities, the power plants may be located inside the perimeter security. In these facilities inmates work inside and help maintain the power plant. Power plants in most maximum security facilities are located outside the perimeter security and are maintained by a minimum security work cadre housed adjacent to the facility.

Air conditioning is another important early design decision. The use of central air conditioning can sometimes reduce the cost of construction of portions of a facility. For example, the windows in an air conditioned housing space can be narrow with fixed glazing material since they are not required to provide natural ventilation.

3.3 Transportation, motor pool and fire station requirements. In all facilities, the motor vehicle and fire station functions are usually located outside the institution's perimeter security.

The threat of vandalism and escape attempts makes parking motor vehicles inside the secure perimeter a hazard. If repairs to vehicles must be made by inmate workers, the vehicles can be brought in for repairs or service and moved outside security once the work is completed.

If fire fighting equipment is supplied by the institution, it should be compatible with that which is used by the local fire department. Periodic visits by local fire department personnel to the facility will allow them to orient new staff and become aware of operational or equipment changes within the facility.

3.4 Preventative Maintenance. The facility should establish a preventative maintenance program for all facility equipment and systems. Such a program, as recommended by ACA Standards [2,3], will help reduce the likelihood of unexpected equipment and system failures which could compromise security as well as increase operating costs.

Chapter 3 - References

1. "Cost Savings in New Generation Jails: The Direct Supervision Approach," W. Raymond Nelson, National Institute of Justice Construction Bulletin, July 1988.

2. Standard 2-4151, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

3. Standards 2-5133, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

CHAPTER 4

SITE SELECTION

CHAPTER 4

SITE SELECTION

4.0 Introduction

This chapter sets forth various considerations relating to the selection of the facility site. Among subjects discussed are: inmate and staff design capacity, geographic proximity to urban areas, topographic and seismic considerations, shape of site, buffer zone requirements, perimeter roads and gun towers, sub-soil and water conditions, off-site utilities, sewage and water treatment plants, parking, outdoor recreation, outdoor firing range and farming requirements. Not all of the above considerations may be applicable to the selection of a specific site. Similarly, it is recognized that some considerations (e.g., topographic, sub-soil, and seismic conditions) are not unique to detention and correctional facilities.

Climatic and site considerations pertaining to electronic perimeter security systems are also discussed in Part II, Chapter 6. Information on how the Federal Bureau of Prisons selects and acquires sites for new institutions is described in Reference [1]*.

4.1 Inmate and staff design capacity. The mission statement of the facility should identify the number of inmates to be housed and the number of staff working in the facility. The size of the site will be determined by the number of inmates housed within the secure perimeter.

4.2 Geographic proximity to urban areas. The ACA recommends a correctional institution site be located within 50 miles of a major urban center [2].

While this recommendation will cause an increase in the purchase price of land versus a site in a rural area, the benefits are numerous. An urban location will make it easier to attract professional staff to employment in the facility. Additionally, inmates can be located closer to their families and be able to have frequent visits. Suppliers can also provide the facility with goods and services more frequently. This service can create a need for less warehousing and storage space in the facility and therefore reduce the initial construction cost.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

An urban location is ideal for a detention facility [3]. The facility must provide space for police vehicles, bus loading and unloading, outdoor recreation, and provisions for family visiting. Usually the facility is a multi-story building and is located adjacent to or integrated with other criminal justice facilities.

4.3 Topographic and seismic considerations. Special design considerations should be given to sites which are located on top of a mountain or on a seismic fault. While it is possible to build on these locations, it would certainly be advisable to obtain an estimate of the added construction costs and to compare them against the purchase of an alternative site.

4.4 Contiguous site. The site should be one contiguous parcel of land free from easements. Buildings are usually not allowed within an easement, and normally the easement must be accessible by the holder.

4.5 Buffer zone requirements. Correctional facilities with perimeter gun-tower coverage should have from 150 to 300 feet of buffer within the shooting areas of the towers.

It is necessary to protect the surrounding neighbors from any risk of gun fire from the facility. The neighbors will sometimes build houses up to the facility's property line. Therefore, any buffer zones provided should be the responsibility of the correctional facility or department. The neighbors cannot be expected to buffer themselves.

4.6 Perimeter roads and gun towers. Perimeter roads should have all-weather surfaces. If they are used by security patrols, they must have hard surfaced areas for use as quick turn arounds for change of directions. Commercial vehicles should never be allowed on the perimeter patrol road.

Gun towers,if used, should be positioned so the line of sight is directly down the fence. When two fences are used the sight line should be down and between the fences. The tower officer should be able to shoot three-fourths of the distance to the next tower. Tower officers must be able to communicate with other towers in a hands-off mode. Towers should also be taller than the tallest building inside the fences to facilitate surveillance.

4.7 Sub-soil conditions. Sub-soil test borings should be made on each site being considered for a correctional facility use. The discovery of rock, high water table, hazardous buried fill or organic material could render the site unsafe or too costly.

4.8 Water conditions. If the site is located in a flood plain, the U.S. Army Corps of Engineers will have restrictions on its use for construction. Sometimes the site will have to be filled with compacted earth to divert potential flood water. Other expensive preventative methods may include construction of dikes or levees, elevated pads under each building, or building the facility on stilts.

4.9 Off-site utilities. In some rural site locations, utilities are not available or they are prohibitively expensive to run to the site. Off-site utility costs to consider are electricity, gas lines, water lines and sewer lines.

4.10 Sewage and water treatment plants. When off-site sewage and water facilities are not available, the correctional facility design must include their construction and operation. The costs must include the staff costs which may require full-time supervision of the treatment plants.

4.11 Parking requirements. The number of parking spaces required for a correctional facility is determined by the number of staff posts in the facility. Parking spaces should be provided for the posts covered by the two largest shifts. In addition, space should be provided for official visitors and inmate visitor parking. Visitor parking is influenced by visiting room capacity and the frequency that visiting is allowed. All parking circulation should be kept off the perimeter security roads.

4.12 Outdoor recreation requirements. The amount of outdoor space used for inmate recreation is dependent upon the type of recreation allowed and the age of the inmate population. If contact sports are allowed, then a football or soccer field is appropriate as well as a baseball or softball field. Older inmates usually limit physical exercise to jogging, walking, shuffleboard, etc. A jogging track can usually encircle basketball or handball courts and will not require much additional space. The ACA Standards recommend a minimum of two acres of outdoor recreation space for a 500 bed correctional facility. Additionally, 90 square feet is recommended for each inmate over the 500 bed capacity [4].

4.13 Outdoor firing range requirements. There have been cases when stray bullets have struck adjacent property owners' houses as the result of an improperly located and operated firing range. Accordingly, the range should be situated so the line of fire is away from adjacent property boundaries.

Firing ranges are also traditionally used by other law enforcement agencies. However, the firing range should always be under the supervision of the correctional facility Range Officer regardless of who might be using it.

4.14 Farming requirements. The farming and ranching operation of a correctional facility can provide food and income for itself and many other facilities within the system. The agriculture program should utilize minimum security inmates. The minimum security units could be located in an annex outside the security of a maximum or medium security facility on the same site.

Chapter 4 - References

1. "Acquiring New Prison Sites: The Federal Experience," Wade B. Houk, National Institute of Justice Construction Bulletin, NCJ 106784, U.S. Department of Justice, Washington, DC 20531, December 1987.

2. Standard 2-4161, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

3. Standards 2-5140, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

4. Standard 2-4157, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

PART II - PERIMETER SYSTEMS

CHAPTER 5

GENERAL

CHAPTER 5

GENERAL

5.0 Introduction

This chapter sets forth general requirements and criteria that pertain to the perimeter security of the facility or institution. Specific requirements and criteria for perimeter fencing and intrusion detection systems are covered in Chapters 6 through 8 of Part II. For some facilities, particularly those located in densely populated urban areas, perimeter security may be provided by only the exterior walls of the facility (see part III).

5.1 Requirement

Objectives. The perimeter security system of the facility should possess a delay and detection capability which is consistent with the facility security levels and inmate custody categories.

Commentary

Given the various classes of security associated with the corrections industry, it would appear that there could be various classes of perimeter security that would need to be established to match the security levels of the institution. For example, it could be argued that a minimum security facility would require a lower level or less expensive type of perimeter security system than does a medium or maximum facility. Although there may be requirements for varying levels of perimeter security for different types of institutions, there is not, however, a direct correlation between the level of sophistication of the perimeter security system and the institution's security classification. In other words, it is not necessarily true that a minimum security institution should have a minimal perimeter security system and that a maximum security institution should have the maximum in perimeter security system sophistication. The apparent needs of perimeter security for each of the three classes of institutional classifications, i.e., minimum, medium and maximum, are examined in the following paragraphs.

Minimum security. A minimum security institution, by its nature, is used to confine inmates of low risk both from the standpoint of their likelihood to escape and/or their propensity towards violent behavior. In a true minimum security facility, the inmates are given so much latitude and freedom of movement, including movement that may go beyond the boundary line of the institution, that any fence barriers erected around the institution are simply for the purpose of defining the boundary of the institution and

deterring unwanted and unofficial contact between the inmates and free persons on the outside. Most escapes from correctional facilities take place from minimum security facilities. In most cases, these escapes are "walk away" situations.

If there is a strong concern by the institution administration for the exchange of contraband or other illicit contact between inmates and outsiders, this problem can most effectively be solved through the use of increased staff supervision or inmate reclassification.

Maximum security. At the other end of the spectrum, the "high" or "super" maximum security facility houses the inmates that have been classified as being a high threat in terms of violent behavior and their desire and propensity to escape given their length of sentence or some other past behavior criteria. Again, however, it is questionable as to whether or not there will be a requirement for a high level of sophistication for perimeter security. The needs for complex perimeter security in a maximum security institution are limited by the following factors:

1. The design of the institution is generally such that the inmate is confined to a cell and/or a living unit for most of the time and is under close observation any time that he is removed from that living unit for exercise, eating, medical needs or other administrative requirements.

2. The design of a maximum security institution is such that the exterior walls of the buildings constitute an almost impregnable barrier as well as perimeter. In other words, the institution is turned inward and inmate movement usually occurs in exercise areas, courtyards or corridors that are surrounded by buildings and/or walls with sufficient heights to make escape all but impossible. With such a design, the inmate not only does not have access to the outer perimeter fencing and associated systems, but his absence from any assigned area would be cause for an immediate alarm.

3. Maximum security inmates do not have the same type of work programs (if any) as other classifications of inmates. Therefore, they will not have access to the tools and/or materials that will permit them to build breaching aids.

4. Visitation is much more closely controlled. Therefore, the inmates are much less likely to have contraband passed to them that can be used in creating a breaching aid and effecting an escape.

In summary, a super maximum security facility, when appropriately designed and properly operated, provides the inmates with a minimal opportunity to ever reach or otherwise come in contact with the perimeter fence and associated sensor electronics. It is also recognized that the term "maximum" is often applied to a facility that has a broad mix of inmates including those that would be classified as both medium and minimum security risks.

Medium security. For the reasons described above, the scope and focus of the Part II criteria that follow will be devoted to correctional facilities that generally fall in a category of medium security and/or maximum security facilities that were not designed solely for housing high risk inmates as described previously. As previously stated, these criteria can be extrapolated to accommodate both minimum and maximum security institutions where special requirements dictate a specific level of security.

Prisons vs. Jails. It is easier to classify the security level of a state prison than to classify the security level of a jail or short-term holding facility. The word "jail", as used here, is defined as a short-term holding facility for pretrial inmates, prisoners awaiting sentence as well as convicted misdemeanants. As such, it may contain a broad spectrum of inmate classifications ranging from the overnight drunk to the serial killer.

The relatively short duration of the holding time for pretrial or pre-sentenced inmates usually limits the internal inmate movement and freedom thereby obviating the need for perimeter security. Convicted misdemeanants are often put in a low security facility that also has little requirement for high security perimeter systems.

There are exceptions to all of these "norms", however, and there is an increasing demand on jails to hold the "backup" from the state prison systems.

When jails take on the role of a prison, the same security requirements will exist, including the need for adequate perimeter security.

5.1.1 Criterion

Vulnerability Analysis. The vulnerability of the perimeter system to escapes and other potential threats should be consistent with the security level(s) of the facility.

Evaluation — Facility plans should be analyzed to determine the delay times provided by various perimeter barriers and the times to move between barriers. For delay time of fence barriers, see Criterion 7.1.1. For detection and visual assessment criteria, see Chapter 8.

Commentary — Various techniques are available to identify all the routes that might be used in an escape attempt [1]*. Using these techniques, the estimated escape times should be determined. Detection and surveillance systems should be provided so that correctional officers can respond to the attempted escape or other threat within the total time determined in the vulnerability analysis.

To increase delay time and detection capability in many maximum and medium security institutions, all major elements of perimeter security -- fences/walls, gun towers, intrusion detection systems, and perimeter patrols [2,3] -- are generally used.

5.1.2 Criterion — Surveillance. Surveillance of all areas adjacent to the facility perimeter shall be consistent with the security level(s) of the facility [4].

Evaluation — Review drawings for adequate buffer zones and surveillance systems -- gun towers, closed circuit television (CCTV), exterior lighting, perimeter patrol roads. See Requirement 8.3.

Commentary — To provide good surveillance, adequate buffer zones are suggested both inside and outside the secure compound. Recommendations suggest that the minimum distance between the outer perimeter fence and the institution's property lines be at least 300 feet [5]. Similarly, as discussed in Section 4.5, a buffer zone should be provided where gun towers are used.

For good surveillance inside the compound, the desired minimum distance between buildings and the inner perimeter is 100 to 150 feet of unobstructed space [6].

5.1.3 Criterion — Entrances/exits. All pedestrian and vehicular entrances and exits through the facility perimeter shall be consistent with the security level(s) of the facility.

Evaluation — Review drawings and security operating procedures.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Commentary

In maximum security facilities, all entrances and exits to the institution should be through sally port arrangements [6]. In all facilities, all pedestrian and vehicular traffic should enter and exit at designated points in the perimeter [7,8].

Chapter 5 - References

1. "Vulnerability Analysis -- Finding the Weakest Link and Fixing It," John A. Milloy, Corrections Today, American Correctional Association, College Park, MD, April 1988.

2. "Electronic Perimeter Security: Have You Purchased a Solution or a Problem?," Francis J. Sheridan, ACA 116th Congress of Correction, Las Vegas, Nevada, August 1986.

3. "Stopping Escapes: Perimeter Security," George and Camille Camp, National Institute of Justice Construction Bulletin, NCJ 104600, Washington, DC, March 1987.

4. Standard 2-4178, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

5. Design Guide for Secure Adult Correctional Facilities, American Correctional Association, College Park, MD, 1983.

6. Standard 2-4179, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised August 1983.

7. Standard 2-4180, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised August 1983.

8. Standards 2-5121 and 2-5167, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

CHAPTER 6

CLIMATE AND SITE

CHAPTER 6

CLIMATE AND SITE

6.0 Introduction

This chapter sets forth climatic and site considerations for the use of electronic perimeter security in correctional facilities. These considerations are broad in scope and include, but are not limited to, basic facility design as well as such factors as the impact of small animals indigenous to the site.

Electronic perimeter security is a sub-system of the total perimeter security system which, in turn, is a sub-system of the entire facility security operation. Electronic perimeter security, in turn, is made up of many sub-systems. For each of these sub-systems, certain requirements have evolved, all of which influence the effectiveness of the perimeter security system. Operational and design decisions related to any of the higher level or lower level sub-systems may have a profound effect on the utility of the electronic perimeter system.

It is critical that the electronic sensing system be properly integrated and work in harmony with the overall operating policies of the facility and can be operated effectively within the climate, site conditions, building arrangement, fence design and other environmental conditions that will impact on its operations, usefulness and life cycle cost.

6.1

Climatic considerations. Climatic conditions including wind, precipitation, temperature and the like exert a strong influence on the design and choice of electronic perimeter security components and sensors. Accordingly, the designer of the system should determine in advance the average number of days in any year that some climatic condition or weather phenomenon will impact the reliability of the system.

Climatological data is available from several sources, both local and Federal. For instance, the existence of an airport within the region will ensure that the FAA maintains comprehensive climatological data that can be purchased for a minimal fee. These reports provide, on a monthly basis, the average number of days for each type of weather phenomenon such as precipitation, temperature, visibility, fog, etc., all of which are pertinent to the design of the perimeter security system.

In establishing the type of weather that will impact the system and calculating the number of days that such an impact will force deterioration of performance, the designer can make a choice as to whether to compensate through the use of redundant or more sophisticated perimeter components during these periods or whether it is more cost effective to simply revert to more visual surveillance through a temporary increase of manpower assigned to towers, vehicle or foot patrols.

One of the more obvious weather factors that would require such a decision is that of accumulated snowfall. If the facility is located in a climate wherein there is occasions for periodic accumulations of snow (including snow drifts) amounting to 3 feet or more, such an accumulation may well negate the usefulness of many electronic sensors. The perimeter system designer must calculate and choose the most cost-effective means of operating when such heavy accumulations occur. Options include alternative sensors that can operate effectively above this accumulation, the possibilities of snow removal equipment that will return the perimeter conditions to normal or the employment of additional manpower to provide visual surveillance until the snow is either physically removed or reduced by melting and sublimation.

Similar calculations are required for periods of reduced visibility due to fog, thunderstorm activity and other phenomenon that can severely impact sensor performance.

The most common negative result associated with weather phenomenon and deteriorated performance is an increase in the false/nuisance alarm rate. It is not uncommon for a designer to specify that a system will perform with some specific limitation on the nuisance alarms that are allowed over some specific time period. For example, a specification may call for the limitation of one nuisance alarm per zone per week. This simplistic limit ignores the possibility that there will be a zero nuisance alarm rate for long time spans, possibly as long as a year, followed by a rapid and almost continuous nuisance alarm problem in one or more of the zones when a specific weather phenomenon, extremely deleterious to that type of sensor, occurs in the area of the facility. The relative susceptibility of various sensors to nuisance alarms due to the environment is shown in Table 6.1 [1]*.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Table 6.1
Relative Susceptibility of Sensors to Nuisance Alarms [1]

Type of Environment	Electric-Field	Microwave	Infrared	Fence Motion	Taut-Wire	Seismic	Seismic/Magnetic	Ported Coax
Weather								
Wind - to 47 km/hr	L	VL	VL	L	VL	L	L	VL
Wind - 47 to 115 km/hr	M	L	L	H	VL	M	M	VL
Wind - over 115 km/hr	M	L-M	L-M	VH	L	H	H	VL
Rain	L-H	L	L	M	VL	L	L	M
Runoff, Standing Water	VL	M-H	L	L	VL	L	L	H
Snow	M	L-M	M	L	VL	L	L	L
Fog	VL	L	M	VL	VL	VL	VL	VL
Animals								
Small (Rabbits, Squirrels)	M	M-H	M	L	VL	L	L	VL
Large (Dogs, Deer)	VH	VH	VH	M	L	VH	VH	M
Birds								
Small	L	VL	L	L	VL	VL	VL	VL
Large	M	M	M	L	VL	VL	VL	VL
Electrical Interference								
Lightning - 1 mile	M	L-M	L	L	VL	L	H	M
Overhead Power Lines	VL	L	VL	VL	VL	L	M	VL
Buried Power Lines	VL	VL	VL	VL	VL	M	H	VL

KEY: VL - very low; L - low; M - medium; H - high; VH - very high.

The most common example of this problem occurs with wind and more particularly wind gusts. Most fence mounted sensors will perform well on a properly constructed fence in the absence of high wind gusts. The climate of the region may be such that there are only a few weeks out of the year when heavy wind gusts occur. The designer should not obviate the use of such a sensor because of its vulnerability to wind over a limited period. It is probable that a cost effective analysis would show that the use of increased visual surveillance, even if the sensor needs to be shut down, is a better option than another much more expensive sensor system which is impervious to this temporary wind gust condition.

Design specifications regarding performance of sensors and their processors (or communication processors) associated with temperature limits also requires careful analysis. It has become more and more common to specify that the electronic components will operate throughout an extreme temperature range (-40 degrees centigrade to + 70 degrees centigrade). While the high limit may have some validity due to the possibility of high internal temperatures within data gathering panels or junction boxes in moderately hot weather, the requirement for operations at the -40 degree centigrade level can be unwarranted given the infrequent occurrence that the climate will fall to those temperatures in most regions. A specification with such a rigid temperature requirement can greatly increase the cost to the user by limiting the number of vendors and/or requiring a responsive vendor to utilize costly components (particularly micro processors) that would otherwise not be required. Extremely low temperatures will seldom cause damage to the components. Rather, they perform erratically. Again, it may be more cost effective to shut the system down during such severe weather or, alternatively, it may be more practical to add heating elements in the processor enclosures or data gathering panels that can be activated automatically under thermostat control during periods of extreme low temperature.

6.2 Site conditions. The individual charged with the design of a correctional perimeter security system will usually not have much say in site selection for the facility. In many cases, perimeter security requirements are for an existing facility. Nevertheless, many site factors, if considered early in the planning stages, can be controlled to the benefit of perimeter security effectiveness.

6.2.1 Soil compaction. Soil density and stability is fundamental to building construction. It is not as frequently considered regarding its effect on perimeter security. Wind and/or water erosion of soil can cause considerable long term problems with perimeter security and impact on the choice of sensors. For example, soil erosion that causes valleys can obviate the effectiveness of microwave. Soil type and density will also be a serious consideration in the design and selection of both barriers and sensors as it relates to the prospects of tunneling. Some soils create problems with alignment of infrared systems.

6.2.2 Grading. Ideally, a perimeter security system should be constructed on flat terrain. This provides the maximum number of options for the selection of sensors and decreases general construction costs. However, rolling and uneven terrain must be dealt with at certain facilities. Typically, considerable grading is a part of new construction. However, all too often, the planners do not anticipate the grading requirements associated with the perimeter systems.

No simple criteria or specification can be established for perimeter grading at an institution. However, as previously stated, whatever grading can be done to provide level terrain along the perimeter will enhance performance and reduce costs. Additionally, the general facility grading should be accomplished in a manner which does not cause the perimeter to be a part of the water runoff scheme. Otherwise, the perimeter area will be subject to erosion and/or water sheathing that can adversely effect certain sensor types.

6.2.3 Vegetation. Vegetation and perimeter security do not mix. Therefore, the planning of any perimeter security system should include means of controlling all vegetation including grasses, weeds or other scrub brush that may be indigenous to the area. Additionally, preventative measures must be taken to preclude dead shrubbery (such as sage brush) from blowing into the perimeter corridor from other areas of the site or areas adjacent to it. For example, a simple trash fence which can block flying debris as well as small animals from entering into the perimeter corridor can easily and inexpensively be included in the early planning stages of the system's design.

Such a fence will also create a line of demarcation for the inmates and also may be useful as a snow fence to keep drifts from reaching the sensor zones. Typically, such

fences can be of inexpensive small gauge fabric and need be only 4 to 5 feet in height.

Unless a groomed lawn is anticipated for the perimeter corridor, it is usually advisable to use a vegetation control chemical within the perimeter corridor at a width which will preclude growth along the fence lines, sensor areas and of sufficient width to ensure that vegetation cannot be used as a hiding place for an escapee. In addition to growth retardation chemicals, it is common practice to use an overlayment of polyvinyl or similar sheeting to inhibit vegetation growth. Where such an overlayment is used, consideration must be given to drainage so that water will not pool in the perimeter corridor. This can be accomplished by ensuring that the plastic overlayment is perforated sufficiently to let the water drain through and that sufficient rock is placed on top of the plastic to facilitate water drainage.

The use of rock as a bed for the perimeter corridor has many other advantages. In addition to providing drainage, properly chosen colored rock can provide ground cover which makes it easier to see a prone inmate whose prison garb contrasts with the rock color. It is not uncommon to use larger boulders on the exterior of high fences such that an inmate who has been able to scale the fence and defeat the barriers will require a breaching aid to reach ground level since a jump from any height is likely to result in a severe leg/ankle injury.

6.2.4 Wildlife. Considerations regarding the control of wildlife in the perimeter corridor should take place in the early planning stages. Properly designed fences including the trash or drift fence should exclude all larger animals from the perimeter corridor. Occasionally, facility management encourage the keeping of certain pets, particularly cats by the inmate population on the basis that it enhances morale and retards the rodent population. If such is the case, extra measures should be taken to preclude these pets from having access to the perimeter corridor. Simple drift or trash fences may be inadequate. Additional wire mesh may be required.

It is much more difficult to control birds. A single small bird would usually not be a problem with any sensor, but a flock of migrating small birds can create an unacceptable nuisance alarm problem for several months at a time. Large black birds, sea gulls, herons etc. are individually capable of causing nuisance alarm problems. The designer, therefore, must be keenly aware of the birds that are

indigenous to the area or that may migrate through the area and plan accordingly.

Again, the type of bedding that is used in the corridor will impact on the likelihood of the corridor being used as a bird sanctuary or landing zone. Additionally, it has been found that fine wire strung on top of fences or on top of the outriggers will discourage the birds from using the fences and outriggers as a perch.

Burrowing animals such as prairie dogs, gophers etc. are usually too small to disturb fence or other free standing sensors. Nevertheless, they can effect buried sensors through seismic action and/or the disturbance/chewing of direct burial cable.

6.2.5 Electromagnetic interference. Electromagnetic interference (EMI) can have a significant impact on electronic perimeter components. The designer must be cognizant of the full spectrum of EMI potential that may exist presently and in the future in the region of the facility. This spectrum includes everything from lightning through aircraft and other radar emissions down to the simple EMI caused by transmission from a walkie-talkie or patrol vehicle. Some of this EMI is extremely difficult to predict and to guard against. For example, a direct lightning strike on a fence mounted sensor will likely wipe out the components on any nearby circuit board irrespective of the preventative measures that have been taken including lightning protection devices such as gas discharge tubes. On the other hand it is within the designer's responsibility to investigate the proximity of transformers and power substations, local military/FAA radars, overhead transmissions lines, and the frequency of low flying military or other sophisticated aircraft that are likely to emit electromagnetic radiation.

It can be anticipated that major power lines will transverse the perimeter in one or more places to bring local utility power to the facility. These power line locations must be known and accommodated in the design.

All equipment proposed for the electronic perimeter sensors and communication wiring should be examined for the susceptibility to interference within the 60 hertz range. This type of EMI is inevitably going to be present by virtue of power to the system itself or power required for perimeter lighting which will be in proximity to the perimeter corridor.

Chapter 6 - References

1. Intrusion Detection Systems Handbook, SAND76-0554, Sandia National Laboratories, Albuquerque, New Mexico, August 1983.

CHAPTER 7

PERIMETER FENCING

CHAPTER 7

PERIMETER FENCING

7.0 Introduction

This chapter sets forth requirements and criteria pertaining to perimeter fencing as it would generally apply to a medium security institution.

The criteria are limited to that fencing which is specifically engineered to act as a delay barrier in conjunction with the electronic sensor systems. Other pedestrian fencing and/or internal inmate movement control fencing is not considered in these criteria.

Note: Most of the criteria in this chapter deals with commonly used chain link fences. It is recognized, however, that there are other types of fences and fence fabrics that have proven to be very effective barriers or "sensor + barriers" when used in detention and correctional facilities.

7.1 Requirement

Fence barriers. The fence barriers shall be of sufficient height and structure so as to provide the necessary delay to permit an adequate assessment and response in apprehending an inmate after the inmate has triggered the intrusion detection system.

Commentary

Delay time is achieved through a combination of ground space that must be transversed and the time required for breaching of fence barriers including augmenting fence top, outriggers or helical barbed concertina wire or tape. The fence or fences, however, provide the foundation for any of these integrated delay structures.

7.1.1 Criterion

Delay time. The fence structure and accessories in combination with properly designed barbed taped obstacles should create a minimum delay time of three minutes for one individual without breaching aids and a minimum of one minute delay time for two people with breaching aids that include bolt cutters, pliers, blankets and rope with a single tonged grappling hook. Ladders or ladder type structures should not be included as breaching aids in this criterion.

Evaluation

The testing for delay time should be accomplished with test panels of fencing and barbed tape with breaching aids made available as appropriate. Individuals performing the test should be permitted to attempt to decrease their breaching

time using various combinations of breaching aids on three consecutive days so as to permit them to go through a planning and learning cycle.

Commentary — The multiple attempt routine over several days is a means of simulating a single attempt by an inmate who has studied the barrier structure for several years and has planned a systematic attack on the fence.

Available data [1]* indicates that the delay time (penetration) for a single chain link fence is no more than thirty seconds. The addition of barbed tape coils or obstacles placed on and near the fence will about double the delay time.

7.1.2 Criterion — Number of fences. A minimum of two fence structures should be employed as part of the barrier structure.

Evaluation — Review of drawings.

Commentary — The need for at least two fences is derived from a combination of requirements including but not necessarily limited to the following:

1. Two fences decrease the ability of an outsider from assisting in an escape by advanced destruction of the fabric barriers or other fence structure.

2. Double fencing provides a better psychological deterrent for the inmates since they realize they can be trapped between the two fences where no hiding place is available.

3. It is often not possible to put barbed obstacles on the inside fence because the area immediately inside the fence is not a no-man's land.

4. A corridor between two fences is often the best location for a sensor system. Such a corridor should be a minimum of 20 feet wide. Twenty five to thirty feet is required for proper sensor operation if the corridor also contains barbed tape on the ground.

7.1.3 Criterion — Fence height. At least one perimeter fence should have fabric that extends to a height of 12 feet.

Evaluation — Review drawings and specifications.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Commentary

Two 6-foot individuals can combine to reach a height of over 12 feet. Outriggers and helical tape also must be employed at the top of the fence to cause both individuals to step back from the support of the fence posts and fabric in order to reach the barbed tape that is supported by the outrigger. Outriggers should point away from the area of confinement since they can provide an aid in climbing the fence if pointing inward. See Criterion 7.2.8.

The designer should give careful consideration to the height of the fence and length of the outrigger so as to take advantage of standard lengths of fence posts and standard widths of fence fabric. In some case it is less expensive to go higher with standard post lengths (considering the buried portion) and standard width of fabric than use non-standard posts and fabric for an arbitrary lower height. Most manufacturers can weave fabric with a 12 foot (or less) width.

7.1.4 Criterion

Clearance. Adequate clearance should be provided between the fence(s) and light standards, utility poles and lines, etc.

Evaluation

Review of plans.

Commentary

Clearance is necessary to prevent these objects from being used in attempts to scale the fence(s).

7.2 Requirement

Design and installation. The fence barriers should be designed and installed to prevent scaling, breaching and tunneling.

7.2.1 Criterion

General. As applicable, fence materials (fabric, posts, rails, fittings, barb wire) and their installation shall be in accordance with national standards.

Evaluation

Except as noted elsewhere in this chapter, chain-link fence materials and their installation shall conform to the following standards:

- Installation -- ASTM F567-84 [2];
- Fence fabric -- ASTM A392-84 [3], A491-84 [4], or ASTM F668-84 [5];
- Posts and rails -- ASTM F669-81 (Reapproved 1985) [6];
- Fittings -- ASTM F626-84 [7];
- Barb wire -- ASTM A121-86 [8] or ASTM A585-86 [9].

Commentary

Commonly used materials used in perimeter fencing of correctional facilities are: fence fabric -- No.9 gage (0.148 in. dia.) steel wire, 2-in. mesh; line posts--galvanized steel pipe (or equivalent tubing), minimum outside diameter of 2.875 in., minimum weight of 4.64 lb per lin. ft.; terminal posts (end, corner, gate) -- galvanized steel pipe (or equivalent tubing), minimum outside diameter of 4.0 in., minimum weight of 6.56 lb per lin. ft.; and rails and post braces --galvanized steel pipe (or equivalent tubing), minimum outside diameter of 1.66 to 2.375 in. [10].

Vertical posts and horizontal tubing (rails) should be placed on the side of the fence least accessible to the inmates. Tension wires are sometimes installed in place of a top rail.

7.2.2 Criterion

Stretching of fence fabric. The fence fabric shall be stretched and installed in such a way that no single cut of the fabric will permit unraveling of the fabric to permit an aperture greater than 6 inches in diameter.

Evaluation

The fabric should not deflect more than two inches when pulled with a force of 30 pounds. Each panel of the fence should be tested. The force should be exerted at a point which is mid-point between the tie positions.

Commentary

The ability to unravel the weave of a fabric following a cut is a function of the tension on the fabric. Thus, the proper installation, including proper stretching, is critical in institutional fencing. Proper fabric stretching is also critical to the performance of any fence sensor system. The test procedure cited above is used by the California Department of Corrections [11].

7.2.3 Criterion

Support of fence fabric. The lower edge of the fence fabric shall be secured to a bottom rail which is anchored to a concrete grade beam.

Evaluation

The fabric should be supported in a manner which precludes the possibility of being pried upward so as to permit a crawl space.

Commentary

Tubing, cable and concrete footings can all be used to inhibit prying of the fabric. A concrete footing or grade beam can also serve as an anti-tunneling barrier. However, if the fabric is embedded directly in the concrete, it is very difficult to re-stretch the fabric at a later date. A concrete barrier in combination with a bottom support tube and anchors is the best long-term solution.

7.2.4 Criterion

Upper fence portion. The upper edge of the fence fabric should not be supported by a rail or other device which can be used as a support in a climbing attempt. Additionally, the upper portion of the fence fabric should be of a type that will not permit a toe hold with common foot wear.

Evaluation

A test panel should be used to evaluate multiple climbing attempts using various types of hard and soft soled shoes.

Commentary

The criteria can be achieved by using a tension wire at the top, and a different type of fabric for the top portion of the fence or by adding inexpensive small meshed fabric to the primary fence fabric.

It is not desirable to use too small of a weave for fabric which is on the lower half of the fence because it can restrict sight-lines through the fence due to the "venetian effect". However, a fine wire mesh added on top of the primary fabric has proven to greatly reduce the possibility of climbing over the fence. A 4-foot wide mesh is generally wide enough to preclude reaching over the mesh to secure a handhold. The smooth edge of the mesh should extend one inch above the main fabric.

7.2.5 Criterion

Size of wire ties. The fabric shall be secured to the vertical and horizontal fence tubing with wire ties that are either 9-gage (0.148-in. dia.) steel or 6-gage (0.192-in. dia.) aluminum.

Evaluation

Review drawings and specifications. Fence fittings (other than size of wire ties) shall conform to ASTM F626-84 [7].

Commentary

The gauge of the wire ties is predicated on the assumption that the ties should be as difficult to cut as the fence fabric.

7.2.6 Criterion

Spacing of wire ties. The wire ties shall be spaced on twelve (12) inch centers on both the vertical tubing and horizontal tubing (or tension wire).

Evaluation

Review drawings and specifications.

Commentary

The recommended spacing is closer than that specified in ASTM F567-84 [2] (i.e., 15 in. on vertical tubing and 24 in. on horizontal tubing).

7.2.7 Criterion

Installation of wire ties. The wire ties shall be installed by means of a 180-degree bend over the tube and two complete circles around the fabric at each end.

Evaluation — Review drawings and specifications.

Commentary — The common commercial practice for wire ties is a simple hook-type turn over the fabric on each side. This means of attachment is unsatisfactory for maintaining the proper tension and avoiding a source of rattle noise on an institutional fence.

7.2.8 Criterion — Outriggers. The inboard outrigger should be of a break-away type so that it cannot be used as a support member for someone attempting to scale the fence.

Evaluation — The outriggers should be tested to ensure that they collapse when a dead weight of no more than 100 pounds is exerted directly on the outrigger.

Commentary — The outriggers must be strong enough to support the weight of barbed tape and, in some cases, snow and ice accumulation. The loads specified above are less than the minimum vertical load (i.e., 250 lb) required in ASTM F626-84 [7].

7.2.9 Criterion — Barbed tape obstacles. The barbed tape obstacles should include multiple rolls of ground barriers and at least one roll at the top of the fence. All barbed tape should be installed in accordance with the manufacturer's recommended length per roll coverage.

Evaluation — Review drawings and specifications.

Commentary — Recommended barbed tape is available in concertina and double coils (i.e., a smaller diameter coil placed inside a larger diameter coil). Typical diameters range from 30 in. to 60 in. Single helical coils are not appropriate.

At present, there are no national standards for barbed tape. A number of available barbed tapes are fabricated from stainless steel strip which measures 0.025 in. thick by 1.0 in. wide. The steel strip is usually reinforced with a high strength stainless steel wire (typical diameter, 0.098 in.) Length, type and spacing of barbs also varies between different products. Clips or spot welds for attaching adjacent coils to obtain concertina are generally capable of withstanding a minimum tensile load of 200 lb.

7.2.10 Criterion — Ground barriers. The ground barrier tape rolls shall be at least 30 inches in diameter and stacked at least two rolls high in such a manner that an individual stepping on the barrier will cause the un-deflected portion of the roll to snag in the crotch area.

Evaluation — Review drawings and specifications.

Commentary — Ground barrier barbed tape rolls should be concertina or double coils.

7.2.11 Criterion — Top mounted rolls. Barbed tape rolls that are mounted on the top portion of the fence should be attached to the barrier at two places on the circumference of the roll and with spacing along the roll in conformance with the manufacturer's recommendation.

Evaluation — Review drawings and specifications.

Commentary — Assuming that there is an outrigger on the top of the fence, the roll should be attached to both the outrigger and the fence fabric. This double attachment as well as the frequency of the attachment is particularly important if a fence sensor is to be used on the same fence.

Chapter 7 - References

1. Barrier Technology Handbook, SAND77-0777rev, Sandia National Laboratories, Albuquerque, NM, 1981.

2. Standard Practice for Installation of Chain-Link Fence, ASTM F567-84, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1984.

3. Standard Specification for Zinc-Coated Steel Chain-Link Fence Fabric, ASTM A392-84, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1984.

4. Standard Specification for Aluminum-Coated Steel Chain-Link Fence Fabric, ASTM A491-84, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1984.

5. Standard Specification for Poly(Vinyl Chloride) (PVC)-Coated Steel Chain-Link Fence Fabric, ASTM F668-84, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1984.

6. Standard Specification for Strength Requirements of Metal Posts and Rails for Industrial Chain Link Fence, ASTM F669-81, Reapproved 1985, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1985.

7. Standard Specification for Fence Fittings, ASTM F626-84, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1984.

8. Standard Specification for Zinc-Coated (Galvanized) Steel Barbed Wire, ASTM A121-86, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1986.

9. Standard Specification for Aluminum-Coated (Galvanized) Steel Barbed Wire, ASTM A585-86, American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103, 1986.

10. Standards for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities, Robert D. Dikkers, Belinda C. Reeder, NBSIR 87-3687, National Bureau of Standards, Gaithersburg, MD 20899, November 1987.

11. Design Criteria Guidelines, Planning and Construction Division, Department of Corrections, State of California, Sacramento, CA, 1985 (with revisions through June 1988).

CHAPTER 8

INTRUSION DETECTION SYSTEMS

CHAPTER 8

INTRUSION DETECTION SYSTEMS

8.0 Introduction

This chapter sets forth requirements and criteria that pertain to electronic intrusion detection systems used for the perimeter security of a detention or correctional facility. Although the primary focus is on the selection and application of perimeter security sensors, criteria for the alarm monitoring system and visual assessment are also included. Figure 8.1 is a flow diagram illustrating the various hardware and functions which comprise the intrusion detection system [1]*.

Electronic security sensors when integrated properly with other perimeter security devices can provide increased cost-effective means for facility security. In this case, facility security is defined and limited to that associated with the escape of an inmate through the defined perimeter system and/or the deterrence and detection of those who would either intrude into the facility grounds for the purpose of bringing in contraband and/or assisting in an escape or any other malevolent purpose.

Heretofore, the selection and design of an electronic perimeter security system has often been an after-thought to the basic facility design and even an after-thought to the design of the fences and other barbed tape barriers that are used to define that line of demarcation called the "prison perimeter". It is axiomatic in perimeter security that the perimeter system serve the purpose of (1) establishing the line of demarcation between outside and inside, (2) act as a deterrence against crossing that line by either inmates wishing to escape or free persons wishing to enter, (3) detect any attempt to breach that perimeter and finally, (4) adequately delay the intruder for sufficient time so that he can be apprehended.

It is also axiomatic that any perimeter system can be defeated and/or breached. In fact, a perimeter can be successfully defeated without detection if the appropriate breaching aids are available. Hence, it must be a design criteria to deploy both sensors and barriers in a proper combination such that the escapee is forced to use sophisticated breaching aids if a successful escape is to be achieved.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

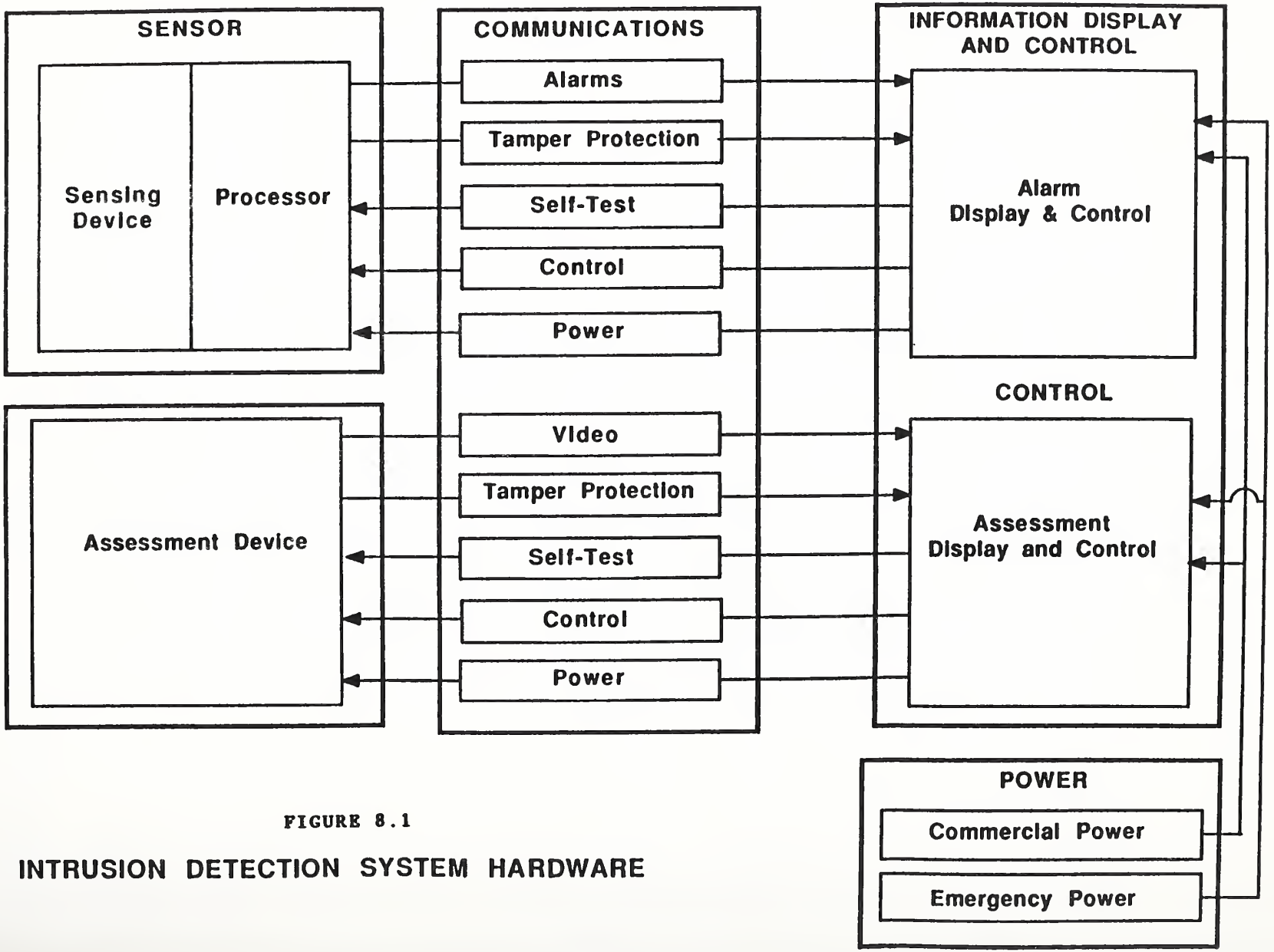

FIGURE 8.1

INTRUSION DETECTION SYSTEM HARDWARE

As a consequence, it becomes the responsibility of the institution's management to ensure that the inmates do not have access to sophisticated breaching aids or to the tools which would be required to construct such a breaching aid. It should also be a goal of the facility designers to establish a sufficient buffer area outside the perimeter area to preclude others from bringing breaching aids to the perimeter from some outside source. This design criteria also has the effect of channeling an escape attempt into one area as opposed to allowing one or more inmates to attack the perimeter security at many points simultaneously.

In summary, the electronic sensors are a sub-system to the total perimeter security system which, in turn, is a sub-system to other institutional functions and operations.

8.1 Requirement

Sensors. The perimeter security system shall incorporate electronic sensor technology that will provide an absolute and reliable means of detecting an escape attempt by one or more inmates.

Commentary

There are an infinite number of scenarios that can be developed regarding the means by which inmates will attempt to escape confinement. This requirement is limited to covert escape attempts through the perimeter which is defined as that fence line system that surrounds and defines the limits of the confinement area including the portals that are a part of that perimeter. The requirement, as stated herein, does not include escape attempts that are of an overt or violent nature. Nor does the requirement include covert escape attempts by means of using false identification or hiding in transient or other out-going vehicles.

8.1.1 Criterion

Sensor deployment. The sensor system shall be deployed as a means of detection throughout the entire perimeter of the facility including portals. Buildings that form part of the perimeter shall employ roof-top systems to provide perimeter detection integrity unless it is clearly determined that, under no circumstances, can an inmate have access to the roof-top because of the height of the building walls and/or absence of inside stairs, air ducts, etc.

Evaluation

Each 300 foot section or other appropriate zoning should be evaluated to determine the feasibility of circumventing the detection means. Each such zone should be given a numerical evaluation score from zero to one hundred percent with zero indicating that the evaluation indicates a zero probability that the zone can be used as a corridor for undetected escapes.

The following factors should be considered and scored:

a. Tunneling;
b. Bridging;
c. Sensor crossover points;
d. Sensor spoofing;
e. Sensor tampering;
f. Creation of artificial nuisance alarms; and
g. Sensor ineffectiveness due to precipitation, fog, wind or other environmental conditions.

No single factor should have a probability higher than 5 and the combined total of this numerical scoring should not exceed a value of twenty. A higher score is cause for a re-evaluation of the sensor choice, sensor pattern or the design of a perimeter as a whole.

As an example, assume a zone evaluation resulted in the following scores: tunneling - 0%, bridging - 0%, sensor crossover points - 0%, sensor spoofing - 3%, sensor tampering - 3%, creation of artificial nuisance alarms - 5%, and sensor ineffectiveness - 5%. The zone would pass the quantitative evaluation because none of the probability estimates exceeded 5% and the total percentage of 16% is below 20%.

Commentary

Systematic evaluation of each segment or zone of the perimeter is required to ensure perimeter detection and security integrity. For example, if an inmate is able to covertly create a persistent false alarm situation in one zone and is further able to determine that the high false alarm rate has brought numerous responses which has abruptly stopped even though the alarms are continuing, the sensor effectiveness in that zone has dropped to zero and the probability of detection has been dramatically reduced. Similar critiques must be made of fence lines, particularly intersecting fences that can be used for bridging a sensing system such as microwave or infrared. Potential weaknesses of integrity at portals where sensors must be deactivated during authorized pedestrian or vehicle movement is also important.

8.1.2 Criterion

Dual sensors. Dual or redundant sensors shall be employed for all perimeter zones except those that protect portals which are under 24 hour visual surveillance or on roof tops where the likelihood of inmate presence is less than 5%.

Evaluation

Review plans, specifications, operational policies and procedures.

Commentary

The incremental costs of adding a second sensor to each typical zone on the perimeter is a small percentage of the total system cost since the initial sensor system requires labor, electrical power, communications and alarm monitoring. As an example, a 6,000 foot perimeter might be comprised of twenty 300 foot zones. A reasonable budgetary estimate for such a system would be between $300,000 and $350,000. The administrative costs for specification writing, bidding and overseeing the construction would probably cost the user another $100,000 for a total of nearly $ 0.5 million overall costs. A second sensor system added to the package would typically have an installed cost of approximately $10 per foot for a total of $60,000. The additional cost therefore is about 13% of the total cost for a single sensor system only. For that 13%, the user gets a large increase in probability of detection, full redundancy if one sensor system should fail as well as considerable flexibility in combining the sensors using "and" circuits and/or "or" circuits. Additionally, the knowledge that there are two sensor systems to defeat will greatly reduce the inmates temptation to attempt an escape.

8.1.3 Criterion

Dual sensor selection. The dual sensors should be selected and configured in such a manner that each is impervious to environmental conditions that may negatively impact the other sensor.

Evaluation

The specifications of each of the sensors should be carefully analyzed and, if necessary, the sensors should be tested under various environmental conditions to ensure that environmental phenomenon that effects one of the sensors has little or no impact on the second sensor. Specifications, empirical testing as well as common sense analysis will determine these factors.

Commentary

An assumption is made in this criterion that the perimeter corridor for each sensor system has already been sanitized as much as possible against negative environmental impact. As an example, it is assumed that there is no vegetation and that proper fences, including drift fences, have been erected to eliminate or reduce the possibility of small animals activating the sensors. However, natural elements such as wind, precipitation, lightning, birds, etc. can not be as easily controlled. Alarm assessment and the decision as to its cause can be simplified if the operator knows that both sensor systems will not respond to the same environmental cause. Thus, a simultaneous alarm from both sensors would indicate a high probability of an escape attempt. For additional discussion regarding environmental considerations, refer to Chapter 6.

8.1.4 Criterion

Dual sensor operation. If it is anticipated that the dual sensor systems will be operated in a "joint-domain" ("and" circuit) mode, the two sensor systems should be essentially coplanar.

Evaluation

Compliance with this criterion can be established by insuring that a person will cause a joint-domain alarm when transiting the two sensor systems within the prescribed time window.

Commentary

The time window in which both sensors must be activated is one of many variables that must be considered in this criterion. The purpose of the criterion can best be demonstrated by two extreme examples. Assume a perimeter zone with two 12 foot fences. Also assume a buried ported coax 20 feet on the secure side of the inside fence and a microwave link between the two fences. Since a substantial barrier separates the two sensor corridors, there will be a considerable interval between the time an escapee activates the ported coax system and the time that he activates the microwave system. The two activations would typically be outside of the normal time window allowed for a joint-domain system. Therefore, an inmate could transit both sensor lines without both sensors being activated within the time window required for a joint-domain alarm. If only joint domains are monitored, or alternately, if joint domain is considered a high priority alarm, the design is self defeating.

Secondly, assume that the microwave is moved directly on top of the ported coax system. A very short time window can be set for the joint-domain alarm in as much as a person will activate both the ported coax and the microwave sensors at essentially the same time. A second optimum scenario would be to mount an electric-field (E-field) system on a fence which is also equipped with a fence mounted sensor. Any attempt to cut or scale the fence would activate both sensors at essentially the same time.

When the sensors and configuration are properly designed, the joint-domain configuration permits a very short time window to be utilized. The shorter the time window, the less likely that an environmentally induced alarm will cause both sensors to be activated within the window. The result is a nuisance alarm rate (NAR) which is significantly lower than that which will occur using only a single sensor or two sensors in a "or" configuration.

In a joint-domain system where both sensor outputs are uncorrelated and occur at a random rate that is much less than one output per selected time interval, T, then for two sensors, the nuisance alarm rate is calculated as follows:

$$NAR = \frac{T}{60(NAR\ 1)(NAR\ 2)}$$

where T is in minutes and NAR 1 and NAR 2 are in alarms per hour. [1]

For example, assume that two sensors are used in joint-domain configuration and that the time window (T) is 15 seconds. Assume that sensor 1 has a nuisance alarm rate (NAR 1) of 5 and sensor 2 has a NAR of 8. The joint-domain NAR, which is all the operator would normally see, would be calculated as follows:

$$NAR = \frac{0.25}{60(5)(8)} = 0.0001 \text{ per hour}$$

or 1 nuisance alarm every 10,000 hours or essentially non-existent.

8.1.5 Criterion

Sensor location. If the institutional setting is such that the perimeter fence can be approached by someone on the outside without being observed, at least one of the sensors should be located between the two perimeter fences.

Evaluation

The ability of an outsider to approach the outer fence unobserved is dependent upon many factors including but not necessarily limited to perimeter patrols, location of guard towers, the proximity of the outer fence to trees, other vegetation, parking lots, etc. This evaluation should consider times of restricted visibility including nighttime and dense fog or both.

Commentary

If one accepts the axiom that delay time is fundamental to security, it is also axiomatic that the perimeter design must preclude the ability of an outsider to eliminate the delay time for an escapee by covertly cutting the fabric of both fences and then creating the illusion of fence integrity by some temporary but very weak device such as a wire tie. If an outsider is given the means to accomplish this, the delay barriers can be totally compromised. Therefore, as a minimum, the inside fence must be protected by a sensing system which will serve a dual purpose of detecting an intruder as well as the escapee.

8.1.6 Criterion

Sensor self-test. Each sensor system shall be designed and installed in a manner which will permit the sensors to be exercised by a self-test.

Evaluation

The system configuration should be designed to remotely and automatically activate a test circuit and associated apparatus such that each sensor is caused to go into an alarm state.

Commentary

Some sensor systems are, by their nature, easily configured to meet this criterion. As an example, a microwave link can easily be tested by simply momentarily interrupting the power of the transmitter. A better and more sophisticated means of accomplishing this test would be to momentarily increase or decrease the output of the transmitter to a level such that the receiver is triggered within the sensitivity/threshold level equivalent to an intruder crawling through the microwave beam.

Other sensors require more complex self-test mechanisms. As an example, a fence sensor which is designed to detect vibration (climbing or cutting) on the fence, may require some type of external and separate vibration source mounted to the fence in such a manner that it will, upon remote command, momentarily vibrate the fence structure at a disturbance level comparable to the minimum vibration that the sensor has been set to detect. Other sensors, such as a taut wire system that uses a simple mechanical switch, may require some type of solenoid or other displacement technique.

It can be argued that a periodic "walk around" test by institution personnel can accomplish the same assurance of sensor integrity. In the light of history, however, it is improbable that adequate administrative procedures can be established and meticulously followed to ensure that (1) the walk around test is in fact accomplished, (2) that the test is accomplished each time in a manner which truly tests the threshold or sensitivity of the system and (3) that the failure of a sensor system to pass the test is adequately logged and acted upon by maintenance personnel. In other words, if an officer is sent out to test a fence mounted sensor system, it is extremely likely that he will shake the fabric until an alarm is generated. Such "hands-on" testing does not permit the testing of sensitivity levels which are critical to the probability of detection theorems.

8.1.7 Criterion

Acceptance tests. The acceptance test of a new electronic perimeter security system shall put each sensor in each zone through three test procedures: (1) empirical (actual breaching attempt); (2) a self-test; and (3) a manufacturer suggested and user accepted, scientifically structured threshold test.

Evaluation

The empirical test procedures will differ with each type of sensor. It should include running, walking, and crawling for bi-static and buried sensors; climbing and cutting for fence sensors and various penetration attempts for barrier and E-field sensors. Several attempts should be conducted in each zone. Some States have adopted empirical test procedures for intrusion detection systems [2,3].

The self-test should be conducted by a system or apparatus as described in Criterion 8.1.6.

Sandia National Laboratories, the U.S. Army Corps of Engineers, and several other government agencies have developed scientific means of simulating intrusion attempts through the many types of sensors that are available today. For example, a 12-inch aluminum sphere pulled through a microwave beam at a speed of 6 inches per second is a standard for that type of sensor. Other repeatable tests have been developed as standard for other sensor types.

In the absence of any national test standards, various manufacturers have had to establish their own engineered testing procedures to ensure quality control. If used for acceptance tests, the scientific basis for such tests should be fully explained and satisfactory to the user. In addition, the tests should have been proven to give repeatable and consistent results. The tests should be performed on each sensor as many times as is necessary to show that the sensor has uniform and/or adequate detection sensitivity throughout the zone and at zone junctions or crossover areas.

Commentary

Each of the three tests recommended in the above criterion combine to provide a reliable and repeatable means of determining sensor effectiveness. In the past, either empirical or scientific testing was performed as part of the acceptance procedure. However, empirical testing is not truly repeatable and scientific testing, by itself, cannot assure the user of the actual probability of detection. Neither of these two tests can be routinely performed often enough to ensure the user that the sensors sensitivity (or threshold level) is remaining at a steady and consistent level to ensure long term probability of detection.

If, during the acceptance test, all three tests show a consistent level and pattern of sensor actuation, then the self-test can be relied upon as a means for ensuring on-going acceptable sensor performance. A repeat of the acceptance test should be performed annually as a minimum and following any significant change in climate to ensure that the self-test results remain consistent with the empirical and scientific test procedures.

8.1.8 Criterion

False alarm rate. A sensor zone should have no more than one false alarm per month. (A rash of false alarms due to an electrical/electronic malfunction of unknown origin which occurs within any 4 hour period shall be considered one false alarm).

Evaluation

Record and analyze false alarms for each sensor zone. See Criterion 8.2.11.

Commentary

By definition, a false alarm is an alarm that cannot be attributed to some intrusion or environmental phenomenon and therefore is attributed to the faulty operation of the sensor, communications or alarm monitoring system. This criterion, therefore, applies to the entire electronic network associated with the detection system and not simply to the sensor. Typically, the cause of a false alarm is such that it will be intermittent or may occur during periods of extremely high or low temperatures, high humidity, or high EMI. Causes for false alarms are potentially infinite. Typical causes are mal-adjusted processors, faulty and unstable components or circuit boards, loose wire connections, etc. A false alarm problem with greater frequency than that set forth in the criterion should be considered unacceptable and a reason for prompt trouble shooting leading to corrective action.

8.1.9 Criterion

Nuisance alarm rate. The average nuisance alarm rate for the entire perimeter system should not exceed 4 during any 8-hour shift.

Evaluation

Record and analyze nuisance alarms. See Criterion 8.2.11.

Commentary

It is difficult, if not impossible, to design an electronic intrusion detection system that will not be impacted by some environmental cause. Indeed, it may not be cost-effective to attempt to do so. Additionally, an argument can be made that a system which is totally free from all nuisance alarms for long periods of time can result in complacency and deterioration of training for those who operate and/or assess the cause of the alarms.

Conversely, a plethora of nuisance alarms during any one shift quickly deteriorates the confidence in the system and dramatically lowers the probability of detection. In this case, the probability of detection may not be lowered in terms of sensor detection but rather in the proper assessment of a real alarm in the presence of numerous nuisance alarms.

The word "average" in the criterion provides some tolerance for unusual conditions where a rash of nuisance alarms takes

place during a brief period of some unusual environmental phenomenon. For example, assume that a system has been designed in an arid location that seldom has rain or thunder storm activity. If an unusual weather pattern should occur that brings heavy rain in combination with lightning for some 8 or 10 hour period, and, as a result of this activity the system experiences numerous nuisance alarms due to the sensor susceptibility to this phenomenon, the criterion limitation would clearly not apply. In some cases, the extraordinary environmental conditions may be so severe as to compromise the entire intrusion detection system and the institution may have to revert, at least temporarily, to an increased perimeter patrol force to compensate for the problem.

8.1.10 Criterion

MTBF. The Mean Time Between Failure (MTBF) for each sub-assembly of the electronic perimeter security system shall be a minimum of 5 years.

Evaluation

Although the initial contractor will not normally be responsible for maintenance of the system for period in excess of 2 years, the institution should initiate a maintenance log that establishes a chronology of maintenance actions including component failures. Typically, this would be done on a personal computer utilizing a data base management system that would catalog all components by manufacturer and part or model number such that any particular component can be looked at for its replacement history.

Commentary

This criterion is not established simply to protect the institution against defective or poorly designed parts. Such a maintenance record can also indicate some other design or installation error which is contributing to the failure of that component. As an example, there may be 25 sensor processors on a specific perimeter system. The maintenance record may show that the processors on the south portion of the perimeter have a markedly higher failure rate than all other processors. This could indicate that the heat of the southern sun at mid-day is contributing to the failure and that corrective action should be taken in the form of sun shades or other means of stabilizing the temperature in those enclosures.

It is highly probable that solid-state electronic components will readily meet the criteria provided that they are operated within the limitations of their specifications including temperature, humidity, voltage etc.

8.2 Requirement

Alarm monitoring system (AMS). An electronic perimeter security system shall include the means for displaying the status of the sensors within each zone as well as the alarm/security status of the system as a whole.

Commentary

The alarm monitoring system as described herein includes the means for communicating the alarm status and other pertinent information from the zone to the operator's console and the various components that comprise the operator's console and display equipment.

The communication means, depending upon size, will either be a hard-wire type or an electronically multiplexed type. The selection between the two types is generally based on the size of the perimeter and the cost trade-off between wire or cable as compared with the cost of the multiplexing components in combination with its lesser wire costs.

Direct, hard-wire connections provide the highest possible reliability provided that the circuit is properly supervised. However, multiplexing technology can, through looping arrangements, provide redundancy that is extremely costly in a hard-wire configuration.

There are several techniques for multiplexing signals over the same wire pair or wire bundle. As the price of optical fiber and associated accessories decrease, fiber optic multiplexing is becoming more and more common. Fiber optics present many advantages over hard-wire in that it is intrinsically more reliable and is immune to electromagnetic interference. Thus, it is less likely to be effected by electromagnetic interference from local power poles, lightning, radar signals and the like that were not anticipated when the system was designed and installed.

8.2.1 Criterion

Redundancy. The communication lines associated with the alarm monitoring system should be fully redundant and utilize two different paths from each zone to the AMS processor.

Evaluation

The schematic should be studied to determine if a cut in any portion of the wiring between each zone and the AMS processor will disrupt power and/or signal transmission such that the zone sensors will become inoperative.

8.2.2 Criterion

Full duplex. The communication system for the AMS shall be full duplex, i.e., it shall be capable of communications to and from the zone.

Evaluation The specifications of the AMS including the zone transponder shall be capable of sending and receiving electronic signals so as to permit the sensor status to be reported to the AMS display. Additionally, the operator should be capable of activating a sensor self-test device.

Commentary Present technology offers full duplex or two-way communication for little, if any, additional cost over one-way communication. Considerable benefits can be derived by having either the operator or the processor activate devices in the various system zones. For example, the self-test device can be activated by this means. Additionally, there may be a systems requirement for central control (or AMS) actuation of surveillance cameras, lights, heaters, etc.

8.2.3 Criterion Actuation of devices. The communication link between central control and each zone shall permit the actuation of a minimum of four different devices within each zone.

Evaluation Review drawings and specifications.

Commentary A minimum is established in order to provide for existing and future activation of components within the zone. It should be recognized that this criterion will also impact on the cost-effectiveness trade-off of hard-wire versus multiplex communications.

8.2.4 Criterion Spare inputs. The communication link between the zone and the central processor shall accommodate all sensors, tampers, faults as well as any other devices that must report to the AMS and shall, in addition, provide a minimum of two spare inputs.

Evaluation The specifications and schematics must be carefully examined to determine that all inputs associated with each zone are accommodated and that two spare input terminals will be available.

Commentary The two spare inputs are required for future design changes and additions. The two spare inputs should not be considered as part of the requirement for spare wiring or communication links as described by Criterion 8.2.5.

8.2.5 Criterion Additional capacity. A minimum of 20% additional conductor capacity shall be provided, or in the case of multiplexing, additional channels shall be available between each zone and the central processor. The minimum number of spare conductors, in any situation, shall not be less than 3.

Evaluation — The specifications and schematics should be examined to ensure that adequate communication links are available.

Commentary — This criterion relates to hard-wire signaling systems more than multiplex signaling systems. However, it applies to both. Its purpose is to provide spare signal wiring in the event that a break occurs in the initially installed wiring or cable. The criterion does not apply to fiber optic transmission techniques.

8.2.6 Criterion — Spare power conductor. There shall be a minimum of one spare conductor for power to all system components whenever the distance between terminations exceeds 50 feet or where the conduit path would make the pulling of new wire difficult.

Evaluation — Specifications and schematics should be examined to ensure compliance.

Commentary — There may be reasonable exceptions to this criterion. Normally, number 14 and larger conductors would be exempt.

8.2.7 Criterion — Map display. A map display utilizing perimeter graphics on a mimic board or CRT display shall be used whenever the perimeter has 6 or more zones.

Evaluation — Review drawings and specifications.

Commentary — This criterion, along with Criterion 8.2.8 and 8.2.9, address the human factor or "user friendly" aspect of the system.

8.2.8 Criterion — Key board. The operator shall be able to control and manipulate the system through the use of special function keys on a key pad or a key board. The normal operator function keys shall be color coded and embossed with the alpha-numerics characters. Additionally, any other keys on the key board will be inoperative during normal periods of operation.

Evaluation — Ensure that all operator keys have meaningful alpha-numeric designations in lieu of conventional typewriter key designations that require the operator to memorize and translate from function to meaningless alpha-numeric designations.

Commentary Existing technology makes the use of the PC (personal computer) an inexpensive and attractive choice for providing multiplex communications and video graphic displays. However, a microprocessor-based system that was not initially designed as an AMS can have many short comings, particularly, in the area of human factors.

It is not appropriate for a contractor to substitute a "home grown" AMS system based on a PC or clone and then place the burden of human factors on the operator or institution administration. The requirement for a software program which disables all non-functional keys provides a plateau of sophistication which will inhibit and hopefully preclude a contractor from attempting to substitute an inadequate PC design into the specification that was written around a well engineered AMS system.

8.2.9 Criterion — Operator function switches. The AMS system shall contain, as a minimum, the following operator function switches/ buttons: acknowledge alarm, secure zone, and access zone.

Evaluation Review drawings and specifications.

Commentary The operator should have the option of either acknowledging an alarm or resetting the zone to the secure mode. He should also have the capability for putting various zones in access (non-secure) as would be required for a sally port zone or a zone that is undergoing maintenance. These control functions should be very simple key stroke operations.

8.2.10 Criterion — AMS processor. The AMS processor, at a minimum, should contain the following functional capabilities: auto reset, non-secure zone reminder, auto-test, auto-initialize, microprocessor and memory self diagnostics and on-board battery back-up.

Evaluation Each of the above mentioned features should be carefully tested during the acceptance test process.

Commentary Most, if not all, of these features are capable of being incorporated in AMS processors that were specifically designed for perimeter alarm monitoring. The features are essentially software oriented and can be added to other microprocessor based systems that were developed for more generic uses.

8.2.11 Criterion

Data storage and processing. The AMS should include a means for storing events such as alarms and operator actions and responses. The storage should be in RAM with the capability for periodic copying to an archive file. The system should also include a means for printing out the events in chronological order by the operator. The stored data should be in a data base form that permits manipulation by authorized personnel.

Evaluation

The AMS specification should clearly indicate the requirement for these capabilities and provide the technical specifications for each feature.

Commentary

This is essentially a requirement for a data base management system that stores event data in addition to or in lieu of a "hard copy" printout technique. The data base storage and manipulation is essential for the determination of other performance criteria. As an example, the determination of how many false or nuisance alarms took place or accumulated in a given time period (Criteria 8.1.8 and 8.1.9) is, at best, a time consuming task if the data are simply accumulated on a paper printout. As a minimum, manipulation of the data base should include the means for examining alarm data by zone as well as time periods.

Once a data base management system is incorporated, the system can be engineered to incorporate many other valuable features including weather data (using a digital weather station) and remote access (modem). The data base system should accumulate data in a real-time mode. Typically, this will require a separate processor for the storing and manipulating of data since it is unlikely that one processor can perform all of the alarm monitoring functions and serve the data base function at the same time. A third interface processor between the alarm monitoring processor and the data base management processor may be required to provide real-time transfer from one processor to the other.

8.3 Requirement

Visual assessment. The perimeter security system shall include means for visually assessing the cause of an alarm in a time frame that will permit proper response in the event the cause is an escape attempt.

Commentary

Assessment of an alarm in a timely manner is fundamental to effective electronic perimeter security. Assessment consists of visually determining the cause of the alarm. The potential causes generally fall into four categories:

1. An actual escape attempt;
2. An inadvertent intrusion by staff;
3. A nuisance alarm; and
4. A false alarm.

The assessment must be rapid in order to insure that the cause is not an actual escape attempt since the time between when an alarm occurs to the time that an inmate is free of physical barriers may be less than a minute. Lack of rapid assessment may also allow an inmate to hide or move to another area which may not be searched. In either case, the probability of a successful escape increases dramatically.

The means of assessment could be any one or a combination of the following:

1. Visual observations from a tower;
2. Visual observations from a patrol vehicle;
3. Visual observations by foot patrol; and
4. Visual observations via CCTV.

The first three means have the advantage of permitting immediate action to be taken, e.g., apprehension or the threat/use of firearms. Numbers one and four have the advantage of providing instant assessment rather than a delayed assessment.

It has been shown that if assessment is rapid and easy, there will be more tolerance by staff of nuisance alarms. This can lead to a greater choice in sensor selection and can impact on cost. Rapid assessment can also decrease the requirements for providing for delay time. This will obviously impact on the cost of physical barriers.

There is no simple or single answer to the choice or mix of assessment techniques. Towers offer the double advantage of instant assessment and the ability to use weapons. However, multiple towers are both expensive to build and to staff.

The corrections industry has been slow to properly utilize CCTV for assessment. The evolution from the wall/tower mentality in combination with a past over-reliance on CCTV for other surveillance purposes is probably a factor. New solid-state cameras, properly integrated with the alarm monitoring system provide an excellent substitute for both towers and perimeter patrols.

When properly located and equipped, stationary patrol vehicles can substitute for towers and retain the advantage of being available for rapid response.

In summary, the critical aspect of assessment is the rapid determination as to whether or not an actual escape attempt is in progress. If such is not the case, additional time is available for the determination of the cause, be it staff, nuisance or electronic malfunction. However, it should be understood that it is unlikely that one can even determine the cause of a nuisance alarm if the assessment time is more than a few seconds.

8.3.1 Criterion — Time period. The time between an alarm and a first visual assessment should be less then 5 seconds.

Evaluation — Analyze and test the visual assessment sub-systems in conjunction with the intrusion detection sub-systems.

8.3.2 Criterion — View. The assessment technique shall permit a clear view of the entire alarmed zone as well as an area in both adjoining zones.

Evaluation — Review drawings and specifications.

Commentary — It must be assumed that the escapee may be at the border of a zone when the alarm occurs. Therefore, the assessment must include an area in each adjoining zone that could be reached by the inmate in the time between alarm and actual assessment.

8.3.3 Criterion — Lighting. A minimum of 5 footcandles of lighting should illuminate the perimeter to permit adequate visual and CCTV assessment.

Evaluation — An industrial-grade light meter should be used to test the light level throughout the perimeter in the sensor area as well as the area between the sensor and barriers. Testing should be accomplished during a period of moderate rain.

Commentary — Each perimeter design will have its own lighting requirements. In some cases, it may be more cost effective to use two levels of lighting -- one for general illumination and impact lighting when an alarm occurs. Impact lighting should not be used or, alternately, left on during periods of frequent nuisance alarms.

While lighting should be concentrated on the sensor area, some lighting should be directed at the exterior of the fencing to deter those who would assist an escapee from the outside.

8.3.4 Criterion

CCTV camera. When CCTV is used as an assessment technique, the cameras should be color and of a fixed focus, static position type and/or employ automatic positioning to view the alarmed zone.

Evaluation

Review specifications.

Commentary

The need for rapid assessment does not allow for the time that is required to use manual pan, tilt and zoom.

8.3.5 Criterion

Camera optics. CCTV cameras should utilize solid-state imaging optics and should be housed in appropriate weather proof housings.

Evaluation

Review specifications. The cameras should not utilize vidicon or nuvicon tubes. Rather, they should utilize the new solid-state "Charged Coupled Device" (CCD) imaging optics.

Commentary

While the older optics are less expensive and are adequate for other surveillance purposes, the perimeter security cameras will be mounted in places that are hard to service. Therefore, the life-cycle costs will be lower if the more reliable solid-state imaging optics are used.

8.3.6 Criterion

Video switching. A video switching system should be employed that will permit all zones to be viewed on one monitor. The switching apparatus should permit automatic camera sequencing, alarm controlled camera selection as well as manual camera selection.

Evaluation

Review specifications to ensure that the switching device is compatible with and under the control of the alarm monitoring processor.

Commentary

CCTV should not be used as a primary means of detection on a large perimeter system. Specifically, an officer should not be expected to monitor many zones at one time as a primary means of detecting an escapee. Rather, the CCTV system should have a primary function as an assessment tool and be used in a sequence mode for deterrence as a secondary function after an alarm.

8.4 Requirement

Training. The operation and maintenance of an electronic perimeter security system should be carried out by trained staff that understand the capabilities as well as the limits of the sensors, communications, alarm monitoring systems and all other ancillary systems associated with the system.

Commentary

Perhaps the greatest single reason for the lack of success of the application of electronic perimeter security technology to the corrections industry is the inadequacy of training. Most specifications include a requirement for several days of operator and maintenance training at the time of commissioning. However, no provision is made for on-going training, a crucial need in light of the many shifts, post rotations, and high turn-over rate common to the industry.

The correction industry's inability to meet the competitive wage scale for electronic technicians is also a major problem. The sophisticated equipment, including microprocessors, associated with modern perimeter security is generally beyond the "plant electrician."

The military faced the same problem during the technology explosion following World War II. Innovative training programs were created to permit those with limited education to operate and maintain sophisticated weapon systems. These programs are still being used effectively by the U. S. Armed Forces.

The key to these programs is an instructional methodology that places the burden on the student to acquire the necessary skills and obtain a level of proficiency in operations and/or maintenance so as to become qualified and "certified" on some specific system or sub-system.

The "self-help" or "self-teach" technique requires motivation. Motivation comes from the promise of both recognition and financial reward. Many staff training programs now exist that provide both in other areas of correctional officer training. Similar programs should be considered for electronics proficiency.

8.4.1 Criterion

Training manuals. Training manuals should consist of lesson plans that progressively instruct the correctional officer starting with the fundamentals of the electronics involved and proceed to detailed operating/maintenance procedures.

Evaluation

Review training manuals.

Commentary

Lesson plans should incorporate an appropriate mix of the following learning techniques:

- Text and drawings,
- Video tapes,
- Hands-on experience with the guidance of previously qualified instructors, and
- Examinations.

The U.S. military services use a standard format of instruction that has been well proven and has been adapted to a myriad of weapon systems and other skill requirements. It is called the "Personal Qualification Standard" or PQS System. These documents are readily available as a guide for the contractor, equipment vendor or the institutional administrator.

The potential for success of the program will be in the fact that it becomes self-perpetuating when training is the responsibility of the trainee and his peers, both of whom are or will be responsible for the perimeter security system operation.

Chapter 8 - References

1. Exterior Intrusion Sensor Technology, Sandia National Laboratories, Albuquerque, NM.

2. Design Criteria Guidelines, Planning and Construction Division, Department of Corrections, State of California, Sacramento, CA, 1985 (with revisions through June 1988).

3. D & C Master Specifications, Design and Construction Group, New York Office of General Services, Albany, NY, March 2, 1987.

PART III - BUILDING SYSTEMS

CHAPTER 9

GENERAL

CHAPTER 9

GENERAL

9.0 Introduction

This chapter sets forth general requirements and criteria that pertain to the design and selection of various building systems and equipment used in detention and correctional facilities. Specific requirements and criteria for structural systems, doors, windows, glazing, locks, alarms and communication systems are contained in Chapters 10 through 15.

9.1 Requirement

Objectives. Building systems and equipment used in the facility/institution should be closely related to the level of security required.

Commentary

As discussed in Part I of this report, the facility mission will influence the selection of many types of materials, systems and equipment to be used in a facility. Although quantitative performance information is limited or unavailable for many types of systems and equipment, a primary objective, nevertheless, should be to select such systems and equipment on the basis of their expected performance (strength, safety, durability, etc.) and their expected use conditions within the facility. Similarly, the performance levels of various components which make up a security barrier or system should be comparable (i.e., don't use a lock that can easily picked on a fortress-like door).

9.1.1 Criterion

Vulnerability analysis. The vulnerability of the building systems to escapes and other potential threats should be consistent with the security level(s) of the facility.

Evaluation

Facility plans, systems, and operating procedures should be reviewed to determine the delay times provided by building barriers (walls, floors, doors, windows, locks, etc.) and the times to move between barriers.

Commentary

Multiple zones or barriers within a facility (cell, housing unit, building perimeter) means multiple delays to escape attempts, and multiple opportunities for staff to detect barrier penetrations and to take appropriate action. See Requirement 2.2.

Various techniques are available to identify all the routes that might be used in an escape attempt [1]*. Using these techniques, the estimated escape times should be determined.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Supervision, detection and surveillance systems should be provided so that correctional officers can respond to the attempted escape or other threat within the total time determined in the vulnerability analysis.

ACA standards recommend that maximum and medium security inmates be personally observed by a correctional officer at least every 30 minutes [2]. Accordingly, it has been recommended that security materials, hardware and equipment should retain its integrity and function for this time interval or longer (up to 60 minutes) [3].

9.2 Requirement

Codes and standards. Building systems and equipment shall be designed, constructed and installed in accordance with applicable codes and standards.

Commentary

Detention and correctional facilities should be designed and built to conform to the applicable standards and codes of the jurisdiction in which they are located. In the absence of local or state requirements, reference should be made to national standards and model codes [4,5,6,7,8,9].

ACA standards [10,11] relating to the physical plant, security, and fire safety should also be considered in the selection of building systems and equipment.

9.3 Requirement

Suicide prevention. In selecting systems, equipment, fixtures, and furnishings for inmate housing units, consideration shall be given to the potential suicide hazards of such systems, equipment, etc.

Commentary

Since suicide is the leading cause of death in our nation's jails, suicide prevention programs are very important. These programs should include written rules and procedures, staff training, intake screening, communication between staff, and human interaction. A capable and properly trained staff is the key part of such a program [12].

Data from a study of jail suicides in 1986 indicates that 94% of the suicides were by hanging [12]. Accordingly, potential means or devices for fastening bedding, clothes, etc. should be minimized. For example, safety clothes hooks and ventilation grills with small openings (i.e., 1/4-in. openings on 1/2-in. centers [13]) should be used in a cell. In addition, glazing installed in cell doors should be of sufficient size to allow staff to observe the inmate's activities with the fewest possible number of blind spots.

9.4 Requirement

Contraband prevention. In selecting and installing systems, equipment, fixtures, and furnishings for inmate housing units, consideration shall be given to the potential places for hiding contraband.

Commentary

The physical plant of any detention and correctional facility creates a natural haven for the concealment of contraband. If there is a crack, hole, nook or cranny anywhere in an inmate's cell, the inmate will know how to camouflage it so it is invisible to officers conducting a cell search [14].

Among potential contraband hiding places are: joints in walls, floors, and ceilings; plumbing fixtures; lighting fixtures; vents; beds and other furnishings. Accordingly, it is very important that the design and construction of these various systems and equipment attempt to minimize such hiding places.

9.5 Requirement

Costs. In selecting materials, equipment, and systems, all costs (capital, operating, and maintenance) shall be considered. Costs shall be analyzed on a life-cycle basis.

Commentary

Although security and durability are primary design considerations in most facilities, there are still many opportunities to select alternate materials, equipment, and systems with different levels of performance. Operating costs (personnel, utilities and building maintenance) are the most critical since they have been estimated as representing 80 to 90% of the life-cycle costs of a facility [3,15].

Procedures for evaluating life-cycle costs of buildings and building systems are described in ASTM Standard E917-83 [16].

Chapter 9 - References

1. "Vulnerability Analysis -- Finding the Weakest Link and Fixing It," John A. Milloy, Corrections Today, American Correctional Association, College Park, MD, April 1988.

2. Standard 2-4182-3, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981, revised August 1983.

3. Correctional Facility Design and Construction Management, Dale K. Sechrest, Shelley J. Price, National Institute of Justice, February 1985.

4. BOCA Basic/National Building Code, BOCA Basic/National Mechanical Code, BOCA Basic/National Plumbing Code, Building Officials and Code Administrators International, Inc., 4051 W. Floosmoor Road, Country Club Hills, IL 60477-5975.

5. Uniform Plumbing Code, Uniform Mechanical Code, International Association of Plumbing and Mechanical Officials, 20001 Walnut Drive South, Walnut, CA 91789-2825.

6. Uniform Building Code, Uniform Mechanical Code, International Conference of Building Officials, 5360 South Workman Mill Road, Whittier, CA 90601.

7. Southern Building Code, Southern Plumbing Code, Southern Mechanical Code, Southern Building Code Congress International, Inc., 900 Montclair Road, Birmingham, AL 35213-1206.

8. Code for Safety of Life from Fire in Buildings and Structures, NFPA 101-88, National Fire Protection Association, Batterymarch Park, Quincy, MA 02269.

9. National Electrical Code, NFPA 70-87, National Fire Protection Association, Batterymarch Park, Quincy, MA 02269.

10. Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

11. Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

12. National Study of Jail Suicides: Seven Years Later, Lindsay M. Hayes, Joseph R. Rowan, National Center on Institutions and Alternatives, Alexandria, VA, February 1988.

13. "Guidelines for Utilizing Detention Equipment and Materials in the New Generation Corrections Facilities," F. Wayne Nadon, CH2M Hill, Redding, CA, July 1985.

14. "How to Conduct Cell Searches," Jail Operations Bulletin, Volume 1, Number 1, American Jail Association, Hagerstown, MD, 1988.

15. "Cost Savings in New Generation Jails: The Direct Supervision Approach," W. Raymond Nelson, National Institute of Justice Construction Bulletin, July 1988.

16. Practice for Measuring Life-Cycle Costs of Buildings and Building Systems, ASTM E917-83, American Society for Testing and Materials, 1983.

CHAPTER 10

STRUCTURAL SYSTEMS

CHAPTER 10

STRUCTURAL SYSTEMS

10.0 Introduction

This chapter contains requirements and criteria pertaining to various systems (walls, floors, columns, beams) which comprise the building structures of a facility. Primary focus is on structural systems which are used in maximum and medium security institutions. Among topics covered are: security, durability, and safety.

Types of systems. There are a variety of structural systems which can be used in the construction of detention and correctional facilities. Among commonly used systems are: cast-in-place concrete, precast concrete, tilt-up concrete, masonry, and steel. The type of system to be used for a particular facility will depend upon several factors including: security; durability; height (low rise vs. high rise); local conditions (soil conditions, existing construction on site, available contractors and prefabricators); construction schedule; and cost. Some of the advantages and disadvantages of the various systems are briefly reviewed in the following paragraphs. Because of local conditions, however, it is important that these advantages (or disadvantages) be examined closely for each individual facility.

Cast-in-place concrete. Although cast-in-place concrete has many typical uses (slabs on grade, topping for roof and floor decks), it is generally more expensive and the construction schedule is slower. It can be a competitive solution for high-rise buildings if the structural components are also used for floor, ceiling and wall components [1]*.

Precast and tilt-up concrete. Precast (including modular units) and tilt-up concrete requires less field construction time compared to cast-in-place concrete or masonry construction. Problems with the weather are minimized with precast members because fabrication can take place inside a plant and the building shell can be erected rapidly to protect other construction trades. To reduce costs, the number of different precast pieces should be kept to a minimum and the shapes be as simple as possible. When using tilt-up concrete construction, the schedule must ensure the floor slabs are in place and provide enough area to cast the walls. With modular units, because of larger weights and sizes, higher transportation and erection costs are a disadvantage [1,2,3].

* Numbers in brackets [ ] indicate references at the end of this chapter.

An advantage with modular units is an opportunity to install plumbing and electrical utilities, fixtures, and hardware at the plant, thereby reducing field connections.

Masonry. Masonry construction, especially concrete block, is usually equal to or less than the cost of cast-in-place or precast concrete construction. This is especially true in buildings with many different wall shapes or configurations [1]. Masonry walls, like concrete walls, can provide load bearing capability as well as exterior and interior enclosures.

Steel. Structural steel, which typically takes less time to fabricate and erect than concrete, is generally more economical as a framing system than concrete [1]. One disadvantage, in many instances, is the need to fireproof structural members.

Table 10.1 compares some of the key factors (security, durability, schedule, cost) of the various alternative structural systems discussed above. As mentioned previously, local conditions and other factors need to be evaluated before selecting the structural system for a specific facility.

TABLE 10.1
Comparison of Alternative Structural Systems *

Factors	Cast-in-Place Concrete	Precast Concrete	Tilt-up Concrete	Masonry	Structural Steel
Security	H	H	H	H	M-H
Durability	H	H	H	H	M-H
Schedule	S	M-F	M-F	M	M-F
Cost	H	M-H	M	M	M

* Based on information in Reference [1].

Legend: H - High; M - Medium; S - Slow; F - Fast.

10.1 Requirement

Codes and standards. Structural systems (including non-load bearing walls) shall be designed and constructed in accordance with applicable codes and standards.

Commentary

For conventional materials, such as concrete, masonry, and steel, building codes contain specific requirements for materials, and their design and construction. They also include requirements for allowable building heights and areas, and fire resistance. See Requirement 9.2.

10.2 Requirement

Walls/floors/ceilings. Walls/floors/ceilings shall provide a level of performance consistent with the level of security and durability required.

10.2.1 Criterion

Physical attack resistance. Where maximum or medium security is required, walls/floors/ceilings shall be capable of resisting physical attack.

Evaluation

Review of building plans and specifications. Where physical attack testing is required, it should be conducted in accordance with procedures described in Criterion 11.1.1.

Commentary

In general, walls/floors/ceilings in maximum and medium security housing units, administrative segregation housing units, control center, armories, dispensaries and various equipment rooms should be capable of resisting physical attack.

Based on testing (see Tables 10.2 and 10.3) and satisfactory long-term performance under in-use conditions, various prescriptive requirements (discussed below) have evolved for concrete and masonry construction.

Concrete. High strength concrete (4,000 to 5,000 psi minimum compressive strength) and normal steel reinforcement provided for shrinkage and temperature control will generally provide the necessary resistance for security. Non-loadbearing walls of 4-in. thickness and loadbearing walls of 6 to 8-in. thickness are common. Floor slabs are usually 4 to 8 in. thick. [4]

Masonry. Where maximum security is needed, concrete masonry walls are usually 8-in. thick, reinforced with steel bars 8-in. on centers (both horizontally and vertically), and solidly grouted [5,6]. Medium security walls may be 6-in. thick and the steel reinforcement placed at 16-in.intervals. Proper supervision of masonry construction is very important to insure that the steel reinforcement and concrete grout are properly installed.

TABLE 10.2
Penetration Time* (Minutes) for Concrete and Masonry Walls [7]

Wall Construction	Tools	Mean Time
4-in. concrete (3000 psi), one layer 1/4" x 6x6" mesh	Sledge, hand hydraulic boltcutters	3.2**
6-in. concrete (3000 psi), one layer No. 5 bars, 6-in.o.c.	Sledge, hand hydraulic boltcutters	7.6**
8-in. concrete (3000 psi), two layers 1/4" x 6"x6"mesh	Sledge	12.1 (no hole)
12-in. concrete block, cores unfilled, no rebar	Sledge	1.5
8-in. concrete block with No. 8 rebar in each core, mortar filled	Sledge, cutting torch	2.7
12-in. concrete block, cores filled, No. 6 bars, 8" o.c.	Sledge, prybar, hydraulic boltcutters	20

TABLE 10.3
Penetration Time* (Minutes) for Floor and Roof Construction [7]

Construction	Tools	Mean Time
3-in. concrete topping on top of 2.5 in. concrete slab with 6-in. sq. mesh of No.10 wire	Sledge, boltcutters	4.6**
4-1/2 in. concrete with No.3 rebar on 18-in. centers placed on 16 gauge steel decking	Sledge, fire axe	4.7**
Asphalt built-up roof with gravel, 3-in. vermiculite concrete, 2-in.rigid insulation, 16-gauge steel decking	Fire axe, shovel	3.2
Asphalt built-up roof with gravel, 2-in. rigid insulation, 2-1/2 in. lightweight concrete with 6x6x10-gauge wire fabric on 22-gauge steel decking	Mattock, fire axe, bar	4.0

* Time to produce a hole and one person to crawl through it.
** Estimated penetration time based on judgement and test data from similar type barriers.

Chapter 10 - References

1. More For Le$$ -- Jail Construction Cost Management Handbook, prepared by Kitchell CEM for State of California Board of Corrections, 1987.

2. "Florida Sets Examples With Use of Concrete Modules," Charles B. DeWitt, National Institute of Justice (NIJ) Construction Bulletin, NCJ 100125, Washington, DC, March 1986.

3. "California Tests New Construction Concepts," Charles B. DeWitt, NIJ Construction Bulletin, NCJ 101593, Washington, DC, June 1986.

4. Precast and Prestressed Concrete for Justice Facilities, Walker McGough Foltz Lyerla and The Consulting Engineers Group, Inc., Prestressed Concrete Institute, 1985.

5. Design Criteria Guidelines, Planning and Construction Division, Department of Corrections, State of California, Sacramento, CA, 1985 (with revisions through June 1988).

6. Design Guide for Secure Adult Correctional Facilities, American Correctional Association, College Park, MD, 1983.

7. Barrier Technology Handbook, SAND77-0777rev, Sandia National Laboratories, Albuquerque, NM, 1981.

CHAPTER 11

DOORS

CHAPTER 11

DOORS

11.0 Introduction

This chapter sets forth requirements and criteria for the selection and use of doors, frames, and hardware in maximum and medium security facilities. Among performance topics covered are: resistance to physical attack, ballistic resistance, fire safety, and installation.

For related requirements and criteria pertaining to glazing, locks, and locking systems, see Chapters 13 and 14.

11.1 Requirement

General. Doors, frames, and hardware should provide a level of performance consistent with the level of security and safety required, and the type of surveillance utilized.

Commentary

Steel doors and frames are generally used where maximum and medium security is required (i.e., sally ports, control rooms, maximum and medium security housing units). Doors can be hollow with steel face sheets; steel plate; bar-grille, bar-grate or woven steel rods, or wooden. The type of door to be used for cells will depend upon a number of factors including: (1) the type of inmate being incarcerated (security and vandalism risks); (2) physical attack resistance; (3) surveillance; (4) voice communications and noise control; (4) air circulation; (5) appearance; and (6) costs (initial and maintenance).

Hollow metal doors. In contrast to commercial grade hollow metal doors which are typically 1-3/4 in. thick and have steel face sheets of 18 gauge (0.0478 in.) thickness, detention security hollow metal doors are usually 2 in. thick and face sheets range from 12 gauge (0.1046 in.) to 14 gauge (0.0747 in.) in thickness. Internal stiffeners in security doors are also spaced closer than in commercial grade doors. In addition, the hollow metal frames are generally 12 gauge minimum, and the doors and frames are reinforced with additional plates for locks and other hardware.

Steel plate doors. Steel plate doors (3/16-in. thick) are also used for security doors; however, because of their weight, they are more frequently used for chase and control cabinet doors [1]*. See Criterion 14.4.4.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Bar-grille doors. Bar-grille doors are available in a variety of shapes and materials, including different types of meshes and woven rods, tubular steel bars and solid steel bars. A disadvantage of these doors is that the inmates have access (depending upon the spacing of the bars) to the outside of the door and the locks. Advantages of these doors include good surveillance, voice communications, and air circulation.

Wooden doors. Some facilities, particularly those using direct supervision, have reported the successful use of solid core, wooden doors [2].

The selection of door frame and hardware is generally based on the door type, locking system, and whether the door swings or slides. (See Chapter 14 regarding the use of swinging and sliding doors.) The frames may be manufactured locally, but they are generally purchased with the entire door system allowing for single point responsibility [1].

11.1.1 Criterion

Physical attack resistance. Where maximum or medium security is required, the door assembly (door, frame, lock, hinges, glazing) shall be capable of resisting physical attack.

Evaluation

Review of specifications and physical attack test data. Physical attack testing shall be conducted in accordance with any one of the following standards: HPW-TP-0400.01 [3], or SD-STD-01.01 [4]. Hollow metal doors shall meet the requirements of NAAMM Standard HMMA 863-88 [5]. Compliance with this criterion may also be documented with data on satisfactory long-term performance under in-use conditions.

Commentary

If defeating or breaching a door system or assembly will jeopardize security, such doors should be capable of resisting physical attack for extended time period (i.e., 15 to 60 minutes) in order to allow staff to respond to attempted escapes and other emergencies.

For measuring physical attack resistance, a variety of test methods are currently in use. In the two test methods cited above [3,4], the door assembly is attacked by men using various assault tools, including sledge hammers, steel pipe, chisels, battering rams, etc. The end of the test occurs when entry has been achieved, a given number of impacts have been delivered, or a specific time interval has been reached.

Existing ASTM standards relating to the security of swinging door [6] and sliding door assemblies [7] are not applicable to medium and maximum security applications since they

pertain primarily to single- and multi-family residential housing. However, ASTM Committee T03 on Detention and Correctional Facilities is currently developing a specification for swinging detention door assemblies.

The NAAMM standard for detention security hollow metal doors and frames [5] contains five tests: (1) static load test; (2) rack test; (3) impact load test; (4) removable glazing stops test; and (5) bullet resistance test. Under the static and rack tests, a completely fabricated flush door blank is subjected to specified loads. In the static load test, the maximum midspan deflection of the door can not exceed 0.58 in. when a total load of 14,000 lbs. is applied at the outer quarter points. After release of load, deformation can not exceed 0.015 in. In the rack test, the door is supported on three corners, and a load of 7,500 lbs. is applied at the unsupported corner. Maximum deflection at this corner can not exceed 3.5 in. and there can be no buckling or failure of welds. The purpose of the static load and rack tests is to check the adequacy of construction methods, quality of welds, strength of materials and rigidity of the door assembly.

The impact test in the NAAMM standard is intended to provide a more realistic measure of a door's ability to withstand attack it may receive under riot conditions. For this test, a door complete with hardware is mounted in its frame with the entire assembly in the vertical position so that the door and locking hardware are operable. The door is then subjected to a series of impact loads from a pendulum ram capable of delivering impacts of 200 ft-lbs. Four hundred impacts are applied within 6 in. of the bolt, and 150 impacts are applied within 6 in. of each hinge. Throughout the testing, the door must remain closed and locked, and the assembly must not be damaged to an extent that forcible egress can be obtained.

In many applications, physical attack testing of steel plate and bar-grille doors should not be necessary because these doors have performed successfully for a considerable period of time in maximum and medium security installations.

11.1.2 Criterion

Ballistic resistance. Where maximum security is required, the door assembly shall be capable of resisting ballistic attack.

Evaluation

Review of drawings, specifications, and ballistic test data.

Ballistic testing shall be conducted in accordance with any one of the following standards: NIJ 0108.01 [8], ANSI/UL 752 [9], or HPW-TP-0100.00 [10].

Commentary

Ballistic resistant door assemblies should be used in areas such as housing-unit control stations, facility control centers, sally ports, and gun towers. The specified ballistic threat levels and ratings of the door assemblies should be consistent with the probable type of weapon which could be used in an attack (e.g., the NAAMM standard [5] and the California Department of Corrections specify a .44 Magnum handgun [11]). A summary of ballistic threat levels and ratings for handguns is listed in Table 13.2.

11.1.3 Criterion

Hinges. Hinges for maximum and medium security doors shall be of the security or detention type.

Evaluation

Review of plans and specifications.

Commentary

In addition to the security considerations, the type of door hinges will depend on the weight of the door and its frequency of use (openings and closings). Security or detention hinges are generally five inches high with 3/8- or 1/2-in. thick leaves, full surface type, have non-removable pins, and security studs. Three hinges are required for each door, except doors over three feet in width should have four.

Various performance requirements (including frequency of use) for hinges are contained in ANSI/BHMA Standard A156.1-1981 [12].

11.2 Requirement

Fire safety. Clear width of doors and fire ratings of door assemblies shall be in accordance with applicable codes and standards. See Requirement 9.2.

11.3 Requirement

Installation. Installation of doors, frames and hardware shall be in accordance with accepted industry standards and manufacturer's recommendations.

Commentary

For security, hollow metal frames in concrete and masonry walls should be completely filled with grout and appropriately anchored (i.e., generally, anchors should be spaced no more than 16 in. apart). Hardware should be installed in accordance with the hardware manufacturer's templates and instructions. For additional recommendations pertaining to hollow metal doors, see NAAMM Standard 863-88 [5] and Criteria 14.7.1 and 14.7.2.

Chapter 11 - References

1. More for Le$$, Jail Construction Cost Management Handbook, prepared by Kitchell CEM for the California Board of Corrections, 1987.

2. "Can Cost Savings be Achieved by Designing Jails for Direct Inmate Management?," W. Raymond Nelson, First Annual Symposium on New Generation Jails, National Institute of Corrections, May 1, 1986.

3. Forced Entry Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria, HPW-TP-0400.01, H.P. White Laboratory, Inc., Revised July 1985.

4. Forced Entry Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria, SD-STD-01.01, U.S. Department of State, Revision D, May 1983.

5. Guide Specifications for Detention Security Hollow Metal Doors and Frames, NAAMM Standard HMMA 863-88, National Association of Architectural Metal Manufacturers, 1988.

6. Standard Test Methods for Security of Swinging Door Assemblies, ASTM F476-84, American Society for Testing and Materials, 1984.

7. Standard Test Methods for Measurement of Forced Entry Resistance of Horizontal Sliding Door Assemblies, ASTM F842-83, American Society for Testing and Materials, 1983.

8. Ballistic Resistant Protective Materials, NIJ Standard 0108.01, National Institute of Justice, U.S. Department of Justice, September 1985.

9. Standard for Bullet-Resisting Equipment, ANSI/UL 752-1985, American National Standards Institute/Underwriters Laboratories, Inc., Revision 13, May 1988.

10. Transparent Materials and Assemblies for Use in Entry or Containment Barriers, HPW-TP-0100.00, H.P. White Laboratory, Inc., Rev. B, December 10, 1983.

11. Design Criteria Guidelines, Planning and Construction Division, Department of Corrections, State of California, Sacramento, CA, 1985 (with revisions through June 1988).

12. Butts and Hinges, ANSI/BHMA A156.1-81, American National Standards Institute/Builders Hardware Manufacturers Association, 1981.

CHAPTER 12

WINDOWS

CHAPTER 12

WINDOWS

12.0 Introduction

This chapter sets forth requirements and criteria for the selection and use of windows in maximum and medium security facilities. Among performance topics covered are: security, natural lighting, ventilation, and weather protection.

For related requirements and criteria pertaining to glazing, see Chapters 13.

12.1 Requirement

Housing unit windows. Exterior housing unit (cell or dormitory) windows shall provide the required levels of security protection, natural lighting, ventilation, and weather protection.

Commentary

In addition to creating a more normal environment for inmates, security windows can provide ventilation, lighting, and aesthetic qualities to facility exteriors [1,2]*. The five basic types of security windows include:

Fixed windows - windows which have a frame to retain the glazing. Security is obtained through the use of security glazing and limitations on the size of openings. Steel angles can be used instead of hollow metal frames [3].

Guard windows - windows that employ a fixed main frame or grilles with restricted glazing sizes and superimposed ventilators attached to the inside or outside of the grilles. Normal bar spacings which form the grille are 6-3/8 in. by 9-3/8 in. on centers.

Awning windows - windows with horizontal, round, steel bars spaced 6 in. on centers concealed within the head rail of the ventilators and in the frame's sill. The horizontal bars penetrate rectangular bars concealed in the jamb members to form a security grille.

Protected air vent windows - windows providing a large light area with indirect ventilation and sub-frame construction. A hinged air vent is located in front of an integral slotted interior grill protected with a sub-frame. The air vent is operated in a continuous opening and closing cycle by rotating a cone in either direction. Steel bars can be incorporated to form a security grid.

---

* Numbers in brackets [ ] indicate references at the end of this chapter.

Side pivoted combination windows - windows providing a non-institutional appearance and having many different layouts. The opening may be composed of one or more casement ventilators combined with fixed panes of glazing. Steel bars can be incorporated to form a security grid.

For medium security windows, industry practice is to use mild steel for the steel bars (mentioned above), and for maximum security windows, tool-resisting steel bars are used.

Where desired, high tensile strength stainless steel wire cloth can be placed inside a window to protect the glazing against vandalism, to provide contraband protection, and to prevent easy access to the security grill or bars for the purpose of anchoring belts, pillow cases, etc. for attempted suicides.

Security windows which require a cone for operation should be provided with a non-removable cone so inmates can not use the cone as a weapon.

12.1.1 Criterion

Opening size. One dimension (either horizontal or vertical) of any glazed opening (or light) in exterior windows should not exceed five (5) inches.

Evaluation

Review of plans and specifications. For fixed slit-type windows, the limiting dimension is the clear dimension between jambs or between the head and the sill. For larger openings, the limiting dimension is the clear dimension between adjacent steel bars or between a steel bar and the window frame.

Tool-resisting steel bars, where specified, shall conform to ASTM Standards A627-68(1981) [4] or A629-77(1981) [5].

Commentary

An opening size of five (5) inches is generally considered as too small to allow an inmate to escape (i.e., because the head of a human is an average of 6 in. in the narrowest direction). Where steel bars or framing members are used to limit the size of the opening, the bars and framing members should be of such size and weight to restrict any deflection or damage to the window.

In a study of 50 facilities, of which 45 were county jails, only 56% of the facilities having cell windows with glazed openings 5 in. or less in the narrowest dimension experienced any cell window damage [6]. By contrast, 87% of the facilities with openings greater than 5 in. in the narrowest direction suffered damage. Only 33% of the facilities with smaller openings experienced escapes through

a cell window, whereas 70% of the facilities with the larger openings had escapes. Escapes through the smaller 5-in. openings were due to a successful attack on both the glazing and the window framing.

For criteria for the selection of glazing, see Chapter 13.

12.1.2 Criterion Anchorage. Window frames and glazing stops shall be securely anchored.

Evaluation Review of plans and specifications. Where testing may be required to determine the strength of removable glazing stops, the procedures described in NAAMM Standard HMMA 863-88 [7] should be used.

Commentary Since window frames and glazing are both subject to physical attack, the frames should be welded to an appropriate number of steel anchors or studs which are embedded in the surrounding wall. Where possible, this anchorage should be protected by adding a surround or by having an integral potion of the security window overlap the interior wall surface.

Removable glazing stops should be applied, wherever possible, on the outside to prevent inmate tampering. Where stops must be placed on the inside, they should be secured with an ample number of strong, properly installed, tamper-proof fasteners. See Requirement 13.4.

Where it is deemed necessary to measure the physical attack resistance of security windows (including anchorage methods), it is recommended that the test procedures described in Criterion 11.1.1 or Criterion 13.1.2 be used.

12.1.3 Criterion Natural light. Where desired, security windows should be used as a source of natural light for cells or multiple occupancy rooms.

Evaluation Review of plans.

Commentary ACA standards for detention and correctional facilities [8,9] recommend that natural lighting be available either by exterior cell or room windows or from a source within 20 feet of the room or cell.

The use of daylight, in conjunction with task lighting, is one of the window design strategies discussed in Reference [10].

12.1.4 Criterion — Ventilation. Where desired, security windows may be used to provide some of the ventilation air requirements.

Evaluation — Review of specifications and calculations for mechanical systems.

Commentary — ACA standards for detention and correctional facilities [8,9] recommend that ventilation in housing units be at least 10 cubic feet of outside air or recirculated filtered air per minute per human occupant. Proposed ASHRAE Standard 62-1981R [11] recommends the following ventilation rates for correctional facilities: cells - 20 cubic feet per minute (cfm); dining halls - 15 cfm; and guard stations - 15 cfm.

12.1.5 Criterion — Air leakage. Exterior security windows should be designed to limit the maximum air infiltration rate to 0.5 cubic feet per minute per foot of sash crack.

Evaluation — Review results of tests conducted in accordance with ASTM Standard E283-84 [12].

Commentary — The recommended maximum air infiltration rate is the same as the rate specified in ANSI/ASHRAE/IES Standard 90A-1980 [13].

12.1.6 Criterion — Water penetration. Exterior security windows should not leak when subjected to a 15-minute water spay test conducted in accordance with ASTM Standard E331-86 [14].

Evaluation — Review of test results. Unless otherwise specified, ASTM Standard E331-86 uses a test-pressure difference across the window of 2.86 lb. per sq.ft.

Commentary — A test-pressure difference of 2.86 lb. per sq.ft is equivalent to the effect of a 33 mph wind.

Chapter 12 - References

1. "Choosing the Best Security Window," Ryne R. Johnson, Corrections Today, American Correctional Association, College Park, MD, April 1984.

2. Steel Windows - Specifications, Steel Window Institute, Cleveland, OH, May 1983.

3. More For Le$$ -- Jail Construction Cost Management Handbook, prepared by Kitchell CEM for State of California Board of Corrections, 1987.

4. Standard Specification for Homogeneous Tool-Resisting Steel Bars for Security Applications, ASTM A627-68(1981), American Society for Testing and Materials, 1981.

5. Standard Specification for Tool-Resisting Steel Flat Bars and Shapes for Security Applications, ASTM A629-77(1981), American Society for Testing and Materials, 1981.

6. "Windows and Glazing: A Summary of 10 Years of Controversy," Dennis A. Kimme, Washington Jail Architectural Symposium and Materials Fair, October 1, 1980.

7. Guide Specifications for Detention Security Hollow Metal Doors and Frames, NAAMM Standard HMMA 863-88, National Association of Architectural Metal Manufacturers, 1988.

8. Standards 2-4130 and 2-4131, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

9. Standards 2-5112, 2-5113, & 2-5114, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

10. Window Design Strategies to Conserve Energy, S. Robert Hastings, Richard W. Crenshaw, NBS Building Science Series 104, National Bureau of Standards, June 1977.

11. Ventilation for Acceptable Indoor Air Quality, ASHRAE Standard 62-1981R, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., Atlanta, GA, October 1988 Draft.

12. Standard Test Method for Rate of Air Leakage Through Exterior Windows, Curtain Walls, and Doors, ASTM E283-84, American Society for Testing and Materials, 1984.

13. Energy Conservation in New Building Design, ANSI/ASHRAE/IES Standard 90A-1980, American National Standards Institute/American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., Illuminating Engineering Society of North America, 1980.

14. Standard Test Method for Water Penetration of Exterior Windows, Curtain Walls, and Doors by Uniform Static Air Pressure Difference, ASTM E331-86, American Society for Testing and Materials, 1986.

CHAPTER 13

GLAZING

CHAPTER 13

GLAZING

13.0 Introduction

This chapter sets forth requirements and criteria pertaining to the selection and use of security glazing. Among performance areas covered are: resistance to ballistic attack, resistance to physical attack, durability, fire safety, and installation.

A wide variety of glazing materials and glazing assemblies are available for various applications within detention and correctional facilities. A comparative summary of glazing materials characteristics is shown in Table 13.1.

Glass products are comparatively low in strength but high in heat and scratch resistance. In security applications, annealed glass is usually strengthened and laminated with similar or other materials. For ballistic resistance, it is often laminated in its pure form due to its ability to flatten bullets. Also, its breakage pattern reduces vision less than other products when shattered [1]*. Its tensile strength may be increased by heat or chemical treatment. The disadvantages of glass are its weight, its vulnerability to heavy-impact (e.g., sledge hammer), and its tendency to spall more than other types of glazing material [2].

Plastic materials such as polycarbonate have good strength, flexibility, and light weight, but compared to glass, have low resistance to heat, scratching, marring, discoloration and a high coefficient of expansion. Surface treatments will significantly improve resistance to abrasion and discoloration [1]. The chief advantages of plastics over glass are a savings in weight, less spalling and greater resistance to heavy impact [2].

Laminated products. Laminations of glazing materials are adhered by interlayers of various chemical compositions and thicknesses. These interlayers also provide additional strength to the product by the way of shock absorption. Laminated glass with thicknesses of 1-1/4 inches or greater have excellent ballistic resistance. Laminated polycarbonates provide excellent resistance to impact. Laminated glass and polycarbonate products combine the best qualities of both materials -- the heat and mar resistance of glass and the impact resistance of polycarbonate. When glass and polycarbonate are laminated, the interlayer must be highly

* Numbers in brackets [ ] indicate references at the end of this chapter.

TABLE 13.1
Characteristics of Glazing Materials [1]

Product	Comparative Strength	Cost	Breakage Pattern	Cut on Job	Distortion
Annealed	1	1	Long sharp splinters, radial cracks.	Yes	No
Heat Strengthened	2	2.6	Long sharp splinters, radial cracks.	No	Yes
Semi-Tempered	4	2.5	Splinters, local pulverizing, cracks.	No	Yes
Heat Tempered	4-5	2.8	Small cubes, pebbles, vision obscured.	No	Yes
Chemically Strengthened	3-4	2.4	Long sharp splinters, and some pulverizing.	Yes	No
Polycarbonate	250	3	Shear cracks and some pulverizing.	Yes	No

flexible, yet stable, to maintain bond throughout temperature extremes, because polycarbonate has a coefficient of expansion eight times that of glass [1].

Air separated glass and polycarbonate. This product is available in a variety of glazing types and thicknesses. One advantage of this product is the elimination of potential delamination. Another advantage is that some of these products can have an outer layer of glass replaced without replacing the entire unit, thereby reducing life-cycle costs [1].

13.1 Requirement

General. Glazing and glazing assemblies should provide a level of performance against ballistic and physical attacks which is consistent with the level of security and safety required and the type of surveillance utilized.

Commentary

Two important considerations for the selection of security glazing in detention and correctional facilities are their resistances to ballistic and physical attacks. Because a system's overall protective level is no better than its weakest component, the level of glazing resistances selected

should be consistent with the resistances of the surrounding walls, doors, louvers, and other building components.

13.1.1 Criterion Ballistic resistance. Where maximum security is required, glazing and glazing assemblies shall be capable of resisting ballistic attack.

Evaluation Review of drawings, specifications, and ballistic test data.

Ballistic testing shall be conducted in accordance with any one of the following standards: NIJ 0108.01 [3], ANSI/UL 752 [4], or HPW-TP-0100.00 [5].

Commentary Ballistic-resistant glazing and glazing assemblies should be used in areas such as housing unit control stations, facility control centers, and sally ports. The specified ballistic threat levels and ratings of the glazings should be consistent with the probable type of weapon which could be used in an attack (e.g., the California Department of Corrections specifies a .44 Magnum handgun [6]).

A summary of ballistic threat levels and ratings for handguns in the standards noted above are listed in Table 14.2. Ratings to be included in a new standard being developed by an American Society for Testing and Materials (ASTM) committee are also listed in Table 13.2 [7]. It is anticipated that this ASTM standard will be approved in 1989.

Where glazings may also be subject to physical attack, see Criterion 13.1.2.

13.1.2 Criterion Physical attack resistance. Where penetration of glazing presents a threat to security and/or glazing is subject to vandalism, such glazings and glazing assemblies shall be capable of resisting physical attack.

Evaluation Review of drawings, specifications, and physical attack test data.

Physical attack testing shall be conducted in accordance with any one of the following standards: HPW-TP-0100.00 [5], WMFL [8], or procedures established by the California Department of Corrections [9].

Commentary As noted in various reports [10, 11], many owners have been disappointed with glazing performance because their glazing was considered to be "unbreakable" or "virtually indestructible." Given the right weapons and an adequate amount of

Table 13.2
Summary of Ballistic Threat Levels and Ratings for Handguns [1]

Standard[2]	Threat Level, Rating	Weapon Caliper	Bullet Weight (Grains)	Bullet Velocity[3] (fps) Min.	Max.	No. of Shots	Range (feet)
HANDGUNS (AUTOMATIC PISTOLS & REVOLVERS)							
NIJ	I	.22 L.R.[4]	40	1010	1090	5	16.0
HPW	A	.38 Spec.[5]	158	700	800	3[6]	20.0
NIJ	I	.38 Spec.	158	800	900	5	16.0
NIJ	II-A	9mmx19 (LV)[7]	124	1050	1130	5	16.0
HPW	B	9mmX19 (HV)[8]	124	1100	1180	3[6]	20.0
NIJ	II	9mmx19 (HV)	124	1135	1215	5	16.0
ANSI/UL[9]	M.P.S.A.	.38 Super Auto.	130	1152	1344	3	15.0
ASTM	.38 Super	.38 Super Auto.	130	1230	1330	3[10]	25.0
NIJ	II-A	.357 Mag.(LV)	158	1200	1300	5	16.0
ANSI/UL[9]	H.P.S.A.	.357 Mag.(HV)	158	1305	1523	3	15.0
ANSI/UL[9]	S.P.S.A	.44 Mag.	240	1323	1544	3	15.0
ASTM	.44 Mag.	.44 Mag.	240	1400	1500	3[10]	25.0
HPW	C	.44 Mag.	240	1350	1450	3[6]	20.0
NIJ	III-A	.44 Mag.	240	1350	1450	5	16.0

Notes:
1. Data for each class of weapon is listed in approximate order, starting with lower power weapons and ending with higher power weapons.
2. For standards, see references 3,4,5 and 7 listed at the end of this chapter.
3. The various standards specify different locations to measure the bullet velocity; see standards for details.
4. L.R. - Long rifle.
5. Spec. - Special
6. Three (3) shots required for the base materials and twelve (12) shots required for assemblies.
7. LV - Lower velocity
8. HV - Higher velocity
9. All ratings also require one (1) shot from a 20 gauge shotgun.
10. Minimum number of shots.

time, all glazing products can be damaged and penetrated, as can virtually any construction material.

Key considerations where glazing is used (e.g., housing unit windows and doors, dayrooms, control rooms and stations, sally ports, visitation areas) are: (1) whether or not penetration of that glazing will compromise security and/or allow passage of contraband; (2) degree of staff supervision or surveillance; and (3) anticipated amount of vandalism. Since penetration of glazing in control rooms and stations, and sally ports will jeopardize security, glazing in these areas should be able to withstand both physical and ballistic attacks for an extended time period (i.e., 30 to 60 minutes). In other areas such as maximum and medium security housing units, glazing should have adequate physical attack resistance to allow staff to respond to attempted escapes or other emergencies. If the glazing opening is less than 5 inches wide in one direction or the opening is protected by steel bars or rods, vandalism (and subsequent maintenance) should be the important considerations for the selection of that glazing and glazing assembly.

Exterior glazings or other glazings subject to large variations in temperature or humidity should be shown to be capable (through testing or long term performance under in-use conditions) of satisfactory service under such environmental conditions. The loss of vision through a glazed opening after an attack is another important consideration. Because of the thickness and properties of some security glazing, sound transmission through such glazing is much more difficult than through ordinary glass. Where voice communications through the glazing is required, a system utilizing individual speakers and microphones should be specified.

For measuring physical attack resistance, a variety of test methods are currently in use. In two of the test methods cited above [5,8], the glazing is attacked by men using various assault tools, including sledge hammers, steel pipe, chisels, battering rams, propane torch, etc. The end of the test occurs when a hole of a given size has been made or a specific time interval has been reached (see Table 13.3).

In order to better determine the comparative qualities of different security glazing products, the California Department of Corrections has developed a laboratory controlled testing procedure with uniform impact forces [9]. As indicated in Table 13.3, testing on a product is discontinued when a six-inch round opening is produced or when thirty minutes elapses, whichever occurs first. This test method and the results of this test program are now

Table 13.3
Summary of Physical Attack Test Methods for Security Glazing

Test Method	Sample Size	Impact Tools	Force (ft-lbs)	No. of Impacts	Time	End of Test
HPW-TP-0100.00 [5]	36" x 48"	12-lb. sledge hammer, 4" pipe, CO_2 extinguisher, 120 lb. ram, propane torch & chisel, gasoline, wood maul, 1-1/2" pipe, fire axe, angle iron, keyhole saw, crowbar, etc.	Not specified.[1]	No. of impacts varies (10 to 25) with each type of tool.	Not specified.	Passage of 8" x 8" x 5" shape.
WMFL [8]	18" x 96"	2 lb. claw hammer, steel chisel, 10-lb. sledge hammer, 1-1/2" pipe, No. 8 rebar, 4"x3" oak post, fire extinguisher, knife, propane torch, 4-lb. hammer, 3 in. dia. steel pipe. or angle iron.	Not specified.[2]	5 minutes each tool; sledge hammer used twice.	30 or 60 minutes (max.)	10-in. dia. hole.
California Dept. of Corrections [9]	29-3/4" x 29-3/4"	(1) 12-lb. sledge hammer (2) 30 oz. ballpeen hammer & L.P. gas torch (3) 6-lb. fire axe	190 62 100	200 (max.) 200 (max.)	30 minutes (max.)	6-in. dia. hole.
NBS [12]	12" x 12"	1-in. (1.3 lb.) chisel plus propane torches	110	Not specified.	5.5 to 6.5 seconds between impacts.	1-in. dia. hole.

Notes: 1. Attack force consists of not more than six young (18 - 30 years of age), muscular males (180 - 250 pounds), in good health, who carry out the assault with enthusiasm.

2. Attack force consists of six men. Each man attacks glazing for 1 minute at a time and then a fresh man takes over. Time clock stops during change in attack force.

being used in the State of California new prison construction program.

In a NIJ sponsored research project, NBS has also conducted research toward the development of a test method to evaluate the penetration resistance of glazing materials subjected to a simultaneous attack with a sharp-nosed tool and heat application (see Table 13.3) [12]. The new test method for security glazing materials and systems being developed by ASTM Committee F12 on Security Systems and Equipment [7] contains similar provisions for physical attack tests to those contained in other existing test methods [5,8].

13.2 Requirement — Durability. Glazing materials shall not be affected by environmental factors to an extent that will significantly impair their function during their design lives.

13.2.1 Criterion — Environmental degradation. Glazing materials shall not be adversely affected by exposure to sunlight, and extreme temperature and humidity conditions.

Evaluation — Compliance with this criterion may be documented with data on satisfactory long-term performance under in-use conditions and/or applicable laboratory testing.

Commentary — Plastic materials (e.g., polycarbonate) are particularly susceptible to degradation from prolonged exposure to solar radiation. Accordingly, such materials should be UV stabilized or treated with an UV resistant coating (if not glass cladded).

Laminated glass and polycarbonate products should be capable of withstanding extreme temperature and humidity conditions without any delamination or cracking.

Ballistic tests of exterior glazings should be conducted in accordance with the extreme temperatures specified in applicable standards [4,7].

13.2.2 Criterion — Abrasion. Where used in areas subject to abrasion and scratching, glass, glass-clad or mar-resistant materials should be used. See Criterion 15.3.2.

Evaluation — Review of specifications and test data. Test procedures for abrasion resistance are provided in ANSI Z26.1 - 83 [13].

Commentary — To avoid abrasion and other problems, cleaning of security glazing should be in accordance with the manufacturer's recommendations.

13.3 Requirement

Fire safety. Fire resistance and flame spread of glazing materials and assemblies shall be in accordance with applicable codes and standards. See Requirement 9.2.

13.4 Requirement

Installation. Installation of glazing and glazing assemblies shall be in accordance with accepted industry standards and manufacturer's recommendations.

Commentary

Good glazing practices, such as those recommended by the Flat Glass Marketing Association [14], should be followed in installing laminated glazing. Manufacturers of security glazings also provide detailed information and procedures for storage, handling, cleaning, and framing of their products. Sealants and gaskets should be compatible with the glazing materials used.

Glazing stops should be sized according to the size of the openings and the materials used. In general, the glazing stops should not be less than one (1) inch. See Criterion 12.1.2.

Chapter 13 - References

1. More for Le$$, Jail Construction Cost Management Handbook, prepared by Kitchell CEM for the California Board of Corrections, 1987.

2. Bullet Resistant (BR) Glazings, Engineer Technical Letter, Department of the Army, Office of the Chief of Engineers, Draft 1986.

3. Ballistic Resistant Protective Materials, NIJ Standard 0108.01, National Institute of Justice, U.S. Department of Justice, September 1985.

4. Standard for Bullet-Resisting Equipment, ANSI/UL 752-1985, American National Standards Institute/Underwriters Laboratories, Inc., Revision 13, May 1988.

5. Transparent Materials and Assemblies for Use in Entry or Containment Barriers, HPW-TP-0100.00, H.P. White Laboratory, Inc., Rev. B, December 10, 1983.

6. Design Criteria Guidelines, Planning and Construction Division, Department of Corrections, State of California, Sacramento, CA, 1985 (with revisions through June 1988).

7. Standard Test Method for Security Glazing Materials and Systems, American Society for Testing and Materials (ASTM), Committee F12 on Security Systems and Equipment, Draft 1988.

8. Testing criteria established by the architectural firm of Walker, McGough, Foltz and Lyerla (WMFL). Criteria is described in test reports prepared by Wiss, Janney, Elstner Associates, Inc., Northbrook, Illinois.

9. Security Glazing Testing Program and Recommendations, prepared by Kitchell/CEM for the California Department of Corrections, July 10, 1985.

10. "Windows and Glazing: A Summary of 10 Years of Controversy," Dennis A. Kimme, Washington Jail Architectural Symposium and Materials Fair, October 1, 1980.

11. Standards for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities, Robert D. Dikkers, Belinda C. Reeder, NBSIR 87-3687, National Bureau of Standards, November 1987.

12. Development of a Test Method to Evaluate the Penetration Resistance of High-Security Glazing Subjected to Mechanical Impact and Heat, L.I. Knab, S. Fischler, J.R. Clifton, N.E. Waters, NIJ Report 300-85, National Institute of Justice, Washington, DC, November 1986.

13. Safety Code for Safety Glazing Materials for Glazing Motor Vehicles Operating on Land Highways, ANSI Z26.1 - 83, American National Standards Institute, 1983.

14. Glazing Manual and Sealant Manual, Flat Glass Marketing Association, Topeka, Kansas.

CHAPTER 14

LOCKS AND LOCKING SYSTEMS

CHAPTER 14

LOCKS AND LOCKING SYSTEMS

14.0 Introduction

This chapter contains requirements and criteria for locks and locking systems. Among topics covered are: locking devices, key-operated locks, door/lock controls, key control, installation, maintenance, and training.

Since locks and locking systems "secure" the moveable penetrations (doors and gates) located in the various facility barriers (walls and fences), they are very important elements in the overall security of the facility. In so far as possible, the security and durability of the locks and locking systems should be comparable with that of the doors/gates in which they are installed.

14.1 Requirement

General. Locks and locking systems should provide a level of performance consistent with the level of security, control, safety, and durability required, and the type of surveillance utilized.

Commentary

The design and selection of locks and locking systems requires the consideration of a number of factors including: (1) the level of security and control required; (2) fire safety (inmates and staff); (3) type of surveillance; (4) operational convenience and simplicity; (5) durability; (6) flexibility to meet changing facility needs; and (7) cost.

14.2 Requirement

Locking devices. Where a high degree of security and door control is required, sliding door locking devices should be provided. Such devices should be capable of being operated from a secure control station.

Commentary

Locking devices are mechanisms or series of mechanisms used to control a door/gate or group of doors from a remote location. Accordingly, locking devices offer several advantages over key-operated locks (i.e., doors are controlled from a protected position; locking components are inaccessible to inmates).

A variety of sliding door/gate locking devices are available -- rack and pinion, chain drive, pneumatic, hydraulic, and mechanical linkage. In rack and pinion devices, an electric motor drives a gear system that moves a rack above the door, unlocks the door and moves the door open or closed and relocks the door. In chain drive devices, an electric motor drives a gear system that moves a chain connected to the door system, etc. In pneumatic devices, the sliding door is

unlocked, moved open or closed and relocked by pneumatic pistons and assemblies. In hydraulic devices, a pump forces a fluid through hoses or tubing to a hydraulic motor. Wheels connected to these motors then drive a rail connected to a door or gate. Mechanical linkage devices operate by the movement of mechanical devices, i.e., a wheel, a crank or levers, which unlock, open or close and relock the sliding doors.

Rack and pinion, pneumatic, hydraulic, and mechanical linkage devices have an advantage over chain drive devices in that they can be stopped (from a control station) during travel and the door can not be moved manually until it is mechanically released. In chain link devices with a clutch assembly, an inmate can block a door and then push it open or closed without it being mechanically released.

Mechanical linkage devices have a disadvantage compared to other devices in that blocking of the any door can stop movement of all doors which are grouped together. In addition, blocking of the door with a strong object can result in considerable damage to the door.

14.2.1 Criterion

Maximum/medium security. Where maximum or medium security is required (i.e., cell doors, sally port doors, and entrance doors in maximum or medium security housing units), fully controllable or manually operated sliding door locking devices should be used.

Evaluation

Review of plans and specifications.

Commentary

Fully controllable locking devices (i.e., capable of locking, unlocking, opening and closing from a control station) are generally used for maximum security applications. Manually operated devices are used in medium security applications as well as some maximum security applications. In manually operated devices, the door is unlocked or released (by either an electric motor operating a linkage, by pneumatic assemblies, or by the movement of mechanical devices) and a spring opens the door a few inches. At this point, further opening or closing of the door is done manually. In fully controllable devices, convenient adjustments should be provided for increasing or decreasing the door movement pressure.

At present, there are no standards relating to the performance of locking devices. Accordingly, the selection of such devices has to based primarily on satisfactory long-term performance under similar in-use conditions.

14.2.2 Criterion

Vehicle sally port gates. Vehicle sally port gates should be capable of being operated and locked from a remote location. Provisions for manual operation and locking should be available when power is off.

Evaluation

Review of plans and specifications.

Commentary

Vehicle sally port gates should be operated by a mechanism which unlocks the gate(s), moves it open, and closes and relocks it. A variety of locking devices are available; see Requirement 14.2.

A manual operating system should be part of the assembly. One such system is a manual or crank operation from an emergency column secured with a prison deadlock. Where subject to freezing temperatures, some devices may have to be equipped with electric heating elements to ensure proper operation.

14.2.3 Criterion

Interlock circuitry. Sally port gates or doors shall be provided with interlock circuitry to prevent the opening of more than one gate or door simultaneously. Where appropriate, all sally port gate or door locks should be operable by key from two sides.

Evaluation

Review of plans and specifications.

Commentary

Sally port gates/doors shall unlock, open, by the person accessing the gate/door and relock when closed by the gate/door closer or the person at the gate/door by the snap lock feature of the lock. Interlock circuitry may also be useful in other gate/door arrangements to improve the circulation of personnel while maintaining security.

14.3 Requirement

Key-operated locks. Lock operation and size of lock bolt shall be compatible with the frequency of operation, the construction of the door and frame, the level of security required, and the type of surveillance utilized.

Commentary

Similar to locking devices, there is a large variety of key-operated locks (mechanical, electro-mechanical, and pneumatic) available for applications requiring different levels of use and security. Mechanical locks are usually mounted on swinging doors and provide for deadlocking or slam-locking with automatic deadlocking. Electro-mechanical locks are generally jamb mounted and provide for slam-locking and remote, electric unlocking. Pneumatic locks provide features similar to those of electro-mechanical locks.

14.3.1 Criterion

Maximum security. Where maximum security is required, lever tumbler locks should be used. Such locks shall be capable of a high frequency of operation per day.

Evaluation

Review of plans, door schedules, and specifications.

Although current standards do not specifically address the type of heavy-duty locks used in maximum security areas, such locks should meet the applicable performance requirements set forth in UL Standards 437 [1]* and UL 1034 [2].

Commentary

Lever tumbler locks should be used in high security areas such as holding cells, segregation cells, secure storage and utility room doors. The bolt is retracted by a paracentric key. These locks can be keyed alike or keyed separate; master keying is not available. Normally, there are five levers in the lock. Six levers are available for higher security applications. Lever tumblers should have anti-pick notches.

Where doors are scheduled to be keyed from two sides, the locks may require shimming. The shank of the cylinder plug must extend into the escutcheon at both sides to assure that the key can be inserted from both sides. A key should not be left in a lever type lock since any turning device inserted into the cylinder plug from the opposite side can operate the lock. It is also important that the locks be installed right side up. If a lever type lock is installed upside down and a spring breaks, the lever drops and the key will not work. If the lock is right side up and a spring breaks, the lever tumbler can generally be fished with a key and the lock will continue to operate. In a correct installation, the keyway of the cylinder plug should align with the bottom of the lock bolt. Also when lever locks are installed upside down, the key rotates in the opposite direction. In such cases, the officer, from the habit of turning the key in the same direction, could be unlocking a lock that was intended to be locked.

14.3.2 Criterion

Medium security. Where medium security is required, lever tumbler or mogul cylinder locks should be used. Such locks shall be capable of a high frequency of operation per day.

Evaluation

Review of plans, door schedules, and specifications. Although current standards do not address the type of heavy-duty locks used in maximum or medium security areas, such

* Numbers in brackets [ ] indicate references at the end of this chapter.

locks should meet the applicable performance requirements set forth in UL Standards 437 [1] and UL 1034 [2].

Commentary

In mogul cylinder locks, the bolt is retracted by mechanical action of the cam on the cylinder plug by the turning of a (mogul) key. The keys and cylinders for these locks are larger and more durable than normal cylinder locks. These locks can be master keyed, keyed alike or keyed separate. They are often used to operate electric locks for manual override.

Normal cylinder locks, and commercial or institutional hardware are generally used in minimum security applications, administration buildings, etc.

14.4 Requirement

Controls. Controls shall be provided to operate the locks and locking devices in the required modes.

Commentary

The switches, relays and other devices should make up a control system compatible with the locks and locking devices and should be capable of providing the switching necessary to satisfy all desired operational modes.

14.4.1 Criterion

Control console/panel. A control console or panel should be provided to operate locks and locking devices.

Evaluation

Review of plans and specifications.

Commentary

A control console/panel should be designed to display all switches to the operator. Normally installed in a secure area, i.e., an officer's control station, the console should be equipped with a switch for each door, a group switch for each wing of the building and switches for the corridor gates, which control access to those wings. There should also be a power cut-off switch to deactivate the console whenever the officer must leave his station.

14.4.2 Criterion

Status indication. The status of sally port and cell doors shall be indicated on the control console or panel.

Evaluation

Review of plans and specifications.

Commentary

Status indication shall indicate the closed and locked position of the gate/door. On sliding gates/doors, it shall indicate the dead locked position of the gate/door and the locked position of the front or rear locking bar. On swing gates/doors with jam mounted electric release locks, the status indication shall sense the closed position of the gate/door, the projected position of the lock bolt and the

depressed position of the dead lock roller bolt. In many facilities, status indication consists of a green and red light system. A green light indicates a closed and locked condition, and a red light indicates all other conditions.

14.4.3 Criterion — Control functions. In the event of power failure, the locking systems should be fail-secure.

Evaluation — Review of plans and specifications.

Commentary — A fail-secure locking system is held mechanically locked and only releases with electric or mechanical functions. A fail-secure system is recommended for use in correctional and detention facilities so inmates do not cause a power outage to their advantage and escape.

14.4.4 Criterion — Control cabinets. In areas accessible to inmates, closed, lockable cabinets should be used to house switches and manual controls of a locking system.

Evaluation — Review of plans and specifications.

Commentary — The security level of a control cabinet is normally high since inmates often pass within arms reach of the cabinet. For maximum security, 3/16-in. steel plate doors and housings secured with a heavy-duty lock are often used. Lighter construction and a normal cylinder lock can be used for minimum security. The cabinet lock should be keyed to a master key system.

14.5 Requirement — Emergency release. Provisions shall be made for unlocking or gang-release of cell doors in case of fire or other emergencies.

Evaluation — Review of plans and specifications. Locking and release of cell doors should be in conformance with NFPA 101-88 [3] or other applicable life safety requirements.

Commentary — ACA Standards for adult correctional and detention facilities require written policy and procedures for the release from locked areas in case of an emergency [4,5].

One type of emergency release is some form of mechanical linkage, chain or cable system, or an assembly of all of the above connected to each cell which, when activated, will release all doors. Individual, selective release of doors

is available, but the cost of these systems is greater. An alternate emergency release system requires a supervisor to go to each door and operate a key to release that door. Master keying can be used on pin tumbler locks but not on lever tumbler locks.

14.6 Requirement — Key control. A key control system shall be established for each facility. See Requirement 15.10.

Commentary — ACA Standards for adult correctional and detention facilities require written policy and procedures governing the control and use of keys [6,7].

14.6.1 Criterion — General. The key control system shall ensure an accounting of the location and possessor of each key.

Evaluation — Review of operating policies and procedures.

Commentary — One suggested approach is the use of a keyboard with hooks on the keyboard identified by a letter and number combination (i.e., vertical rows being alphabetical and the horizontal rows being numerical). Each key ring should have two tags, one to identify the ring number and the second shall state the total number of keys on that ring. The original key should be kept in a secure key room for a pattern key to cut duplicates from. The pattern keys should never be issued. Fire (or emergency) key rings should be tested on a scheduled basis to assure that they work. Keys should have stamped numbers for identification only and should not in any way identify the combination of the key.

14.7 Requirement — Manuals and instructions. Manuals and instructions shall be provided for the installation, operation and maintenance of the facility locks and locking systems.

14.7.1 Criterion — Installation. Locks, locking systems and controls shall be installed in accordance with the project drawings, specifications and manufacturer's recommendations.

Evaluation — Review plans, specifications, and installation instructions.

Commentary — Doors and frames - Alignment of the frame is most critical to the performance of a door and lock. On lever locks, assure that the lock is installed properly; see Criterion 14.3.1. The bolt must align with the keeper.

14.7.2 Criterion

Field testing. After installation, each door and lock and locking system should be field tested to ensure satisfactory operation.

Evaluation

Sliding doors - Test for smooth operation and desired closing pressure of the door. Run the door a number of times to assure it does not go out of adjustment.

Swing doors - Test for smooth operation. Door should swing free throughout its entire swing to assure there is no binding at the hinges. Door should align with the frame with all spaces between the door and frame equal. Door should align vertically with the frame at both hinge side and lock side. Lock bolt should engage the keeper without binding or play.

14.7.3 Criterion

Maintenance. The facility should establish a plan for preventative maintenance or emergency repairs.

Evaluation

Review of maintenance plans, manuals, and instructions.

Commentary

ACA Standards for adult correctional and local detention facilities require a written plan for preventative maintenance of the physical plant with provisions for emergency repairs or replacement of equipment [8,9].

Maintenance manuals shall contain information on adjustments, lubrication, electrical and mechanical trouble shooting, and ordering of spare or replacement parts.

General suggestions pertaining to maintenance are as follows:

1. Adjustments - Follow manufacturer's recommendations. All adjustments should be made with provisions for future adjustments to compensate for wear. The use of stop nuts and/or cotter keys is desired where adjustments are frequent and to assure the adjustments do not loosen through use.

2. Lubrication - Follow manufacturer's recommendations. Moving parts should be lubricated to reduce wear. Lubricant should reduce friction, but not collect dirt and cause an increase in wear. Lubricant should stay where put and not run causing damage to electrical components or danger to passers-by. Lubricants used for exterior applications in freezing temperatures must retain the lubrication ability through a wide range of temperature changes such as minus 50 degrees F. to plus 120 degrees F.

3. Electric troubleshooting - Use proper test equipment and test circuit by circuit using manufacturer's and installer's

wiring diagrams. Test circuits for continuity. Terminations are most causes of loss of continuity. Testing should be performed by a qualified electrician or electronic technician.

4. Mechanical troubleshooting - Test for smooth operation. Check for burrs on devices which contact each other and for proper engagement of gear assemblies. Test cable assemblies for binding when operated.

14.8 Requirement

Training program. The facility should establish a staff training program for the operation of locks/locking systems under normal and emergency conditions.

14.8.1 Criterion

General. Training should be provided to all facility staff who have responsibility for the operation and maintenance of locks and locking systems.

Evaluation

Contract documents covering the installation of new locks and locking systems should include provisions for adequate training of facility staff by the equipment manufacturer or other appropriate party. Ongoing training should be included in the facility operating policies and procedures.

Commentary

ACA Standards for adult correctional and local detention facilities require written policies and procedures for training and staff development [10,11].

Chapter 14 - References

1. Standard for Key Locks, UL 437-86, Underwriters Laboratories, Inc., 333 Pfingsten Road, Northbrook, IL 60062, 1986.

2. Standard for Burglary Resistant Electric Locking Mechanisms, UL 1034-87, Underwriters Laboratories, Inc., 333 Pfingsten Road, Northbrook, IL 60062, 1985.

3. Code for Safety of Life from Fire in Buildings and Structures, NFPA 101-88, National Fire Protection Association, Batterymarch Park, Quincy, MA 02269, 1985.

4. Standard 2-4173, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

5. Standard 2-5160, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

6. Standard 2-4196, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

7. Standard 2-5190, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

8. Standard 2-4151, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

9. Standard 2-5133, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

10. Standards 2-4079 through 2-4101, Standards for Adult Correctional Institutions, American Correctional Association, College Park, MD, Second Edition, January 1981.

11. Standards 2-5076 through 2-5089, Standards for Adult Local Detention Facilities, American Correctional Association, College Park, MD, Second Edition, April 1981.

CHAPTER 15

CONTROL CENTER, ALARM & COMMUNICATION SYSTEMS

CHAPTER 15

CONTROL CENTER, ALARM & COMMUNICATION SYSTEMS

15.0 Introduction

This chapter sets forth the requirements and criteria for the control center in a secure, long-term correctional facility. Included are requirements and criteria for the physical plant as well as the communications systems and the interface with all of the various alarm systems found in such a facility. As appropriate, these requirements and criteria should be modified to meet the operational needs of other types of facilities.

The control center is the "nerve center" for the entire facility. Control center activities frequently include observing and controlling the institutions entrance and exit traffic, recording all inmate counts, monitoring fire and security alarm systems, operating central communications systems, issuing and maintaining an inventory of institution keys, operating electrically controlled doors, monitoring the perimeter and closed circuit television (CCTV), and operating telephone equipment. Each of these activities has a critical impact on the institution's orderly and secure operation.

The control center operation integrates all internal and external security communication networks. It must be secure from outside assault and at the same time afford good visibility of the areas it is designed to monitor. Its size is determined largely by the type and amount of equipment used and the extent of the duties assigned to the staff in the area. The equipment should be organized so that one person can monitor and operate it easily.

All control center activities are under the supervision of the chief of security, and the center is staffed 24 hours a day, seven days a week by at least one staff member. During periods of peak activity, such as inmate counts and staff shift changes, additional security officers are often assigned to this area. To alleviate the heavy daytime workload, incoming telephone calls to the institution are often answered by a receptionist stationed in the front entrance building. At night, when a receptionist is not needed at this post, incoming calls are switched to the control center. [1]*

* Numbers in brackets [ ] indicate references at the end of this chapter.

15.1 Requirement

Location. The control center should be strategically located.

Commentary

The location of the control center within the institution is of utmost importance since the control center officer must make many decisions and perform many tasks that control inmate movement.

Control centers operate in different fashion depending on correctional philosophy of the chief executive officer and requirements of the jurisdiction. However, in all cases, certain basic functions are constant. All of these require contact with all staff members and ability to know what is going on in the institution.

15.1.1 Criterion

Vision. The control center shall be located so as to afford maximum visibility of the front entrance, interior compound and as many other functions as possible.

Evaluation

Review plans for sight lines.

Commentary

Since there are an infinite number of layouts for institutions, it is impossible to state exact relationships of functional areas. However, the control center should be located so that vision is not blocked to the main pedestrian entrance sally port and to maximize visibility of the inner compound and entrances to as many areas as possible. Although many areas are under the surveillance of CCTV, direct visibility by the control center officer is a plus.

Views on the location of control center are changing. Some are now advocating that the control center should be out of sight and in a location secure from an attack outside the institution.

15.1.2 Criterion

Traffic pattern. The institution shall be designed so as to locate the control center in a position that all pedestrian traffic in and out of the institution must pass within a few feet and within clear visibility of the control center officer. Also, it should be located within about 50 feet of the main entrance.

Evaluation

Review plans.

Commentary

All persons entering and leaving the institution must be identified by the control center officer. This includes staff, inmates, visitors, vendors, volunteers, contractors, etc. Therefore, location of the center in terms of the traffic flow is extremely important.

15.2 Requirement

Adequate space. The space (room) provided to house the control center must be designed for the functions and equipment to be contained.

Commentary

Careful consideration must be given to the equipment and functions to occur in the control center. Changing technology often requires expansion or reconfiguration of the control center. Also, a change in mission of the institution or a change in operating procedures can have a dramatic effect on the control center. Without forethought it is very easy to get "locked into" a control center that later becomes nonfunctional. Programming and design phase is the time to ensure that all functions are considered and that provisions are made for future changes and expansion.

Because the control center becomes the focal point for so many functions, it has a way of also becoming a haven for junk. Adequate, closed "out of sight" storage is a must.

The operations to be conducted in the control center must be clearly defined. Often times the center not only serves as the communications hub and alarm monitoring center, but also as a central issue point for keys, flashlights, portable radios, riot gear, etc. It is important that all of these functions be accommodated.

15.2.1 Criterion

Size and configuration. The size of the space shall take into account the equipment, people and activities to be contained. The control center console in particular should be ergonomically designed. Placement of the equipment should consider access for repair and maintenance.

Evaluation

Review drawings, equipment shop drawings, and specifications.

Commentary

Since the control center is usually located in the administration building, which contains many important functional areas, there is often a tendency to condense the control room and equipment space. Size is an important factor and some room for growth should be provided as frequently new functions and/or equipment are added to the control operation and the equipment room.

Careful planning must go into the size and shape of the room. The mission of the control center and functions to be carried out must be clearly defined. A room that does not consider distances between and relationships of equipment can be a nightmare for the operator. Inadequate storage space will result in various materials and equipment stacked on top of equipment making an unsightly mess.

In addition to the control center proper, an equipment room must be provided adjacent to it to house the radio equipment, telephone switch gear, terminal board, uninterruptable power supply system, batteries, workbench, etc.

15.2.2 Criterion — Access to cables and equipment. All cables and equipment should be readily accessible for use, maintenance and repair.

Evaluation — Review plans, shop drawings, and equipment specifications.

Commentary — Often times, equipment is placed for each of the operations with no thought given to access for repair and maintenance. The control center proper should only contain the terminals, keyboards, etc. necessary for the operators use. All switches, equipment and other related equipment should be located in an equipment room adjacent to the control center. Space should be allowed so that all access doors and panels can open and so that technicians can gain access to the equipment without totally interfering with control center operations.

15.2.3 Criterion — Climate control. The control center and equipment room shall have independent climate control systems including heating, ventilation and cooling capable of maintaining human comfort conditions and humidity of 50% or less.

Evaluation — Review plans and specifications.

Commentary — The control center must be totally climate controlled for operator comfort and for proper operation of all of the electronic equipment. All of the climate control systems must be independent of other building systems to prevent introduction of noxious gases (including tear gas and smoke) in the center and to ensure that the center can stand alone.

15.2.4 Criterion — Toilet facilities. The control center shall be equipped with toilet facilities within the secure envelope of the center.

Evaluation — Review plans and specifications.

Commentary — Since the control center officer can not leave the confines of the center, toilet facilities must be provided. These facilities should be accessible for handicapped persons as the control center officer is one of a few positions in the institution that can be filled by a handicapped individual.

15.3 Requirement — Physical Security. The control center shall be secure and capable of withstanding an attack without interruption of activities within the center.

Commentary — The control center is considered the one part of an institution that must be capable of functioning throughout any disturbance including a riot that may be occurring in the institution. It must be impenetrable by most hand tools and weapons including firearms.

15.3.1 Criterion — Wall, floor and ceiling construction. The walls, floors, and ceiling of the control center and the equipment room shall be constructed in a manner that will prevent breakthrough using hammers, bars, battering rams, etc.

Evaluation — Review plans and specifications. See requirements and criteria in Chapters 10 and 11.

Commentary — Since the control center must be considered the last line of defense in time of disturbances, its envelope must be as secure as possible. It must be assumed that anything available may be used as a battering ram; however, it is not feasible to ensure against a jack hammer breaking through.

15.3.2 Criterion — Windows. A large expanse of glazing shall be provided for good visibility, but at the same time, the glazing shall be able to withstand physical and ballistic attacks.

Evaluation — Review plans and specifications. See Criteria 13.1.1 and 13.1.2, and 13.2.2.

Commentary — There are many aspects of control center glazing that must be considered. It must withstand breakthrough, be bullet resistant, be scratch resistant, provide maximum visibility and still be architecturally pleasing.

Scratch resistance is an important factor because staff members are constantly tapping on the windows, frequently with keys, to get the attention of the control center officer. Physical attack and ballistic resistance, of course, are self explanatory.

One solution that has been used quite successfully is glass clad polycarbonate and then steel tubes, 2 in. by 2 in., with 5 inch clear spacing on the outside of the glazing. The steel tubes must be securely welded into a steel frame that is securely anchored to the wall.

15.3.3 Criterion

Entrance. Entrance to the control center shall be gained through one sally port with a remotely controlled electric lock on the exterior door and a key-operated lock on the inside door.

Evaluation

Review plans and specifications. See Chapters 11 and 14 for requirements and criteria for doors and locks.

Commentary

Only one entrance/exit shall be provided for the control center. Traffic in and out of the center should be confined to only those few officers that work there and any technicians that may be servicing the equipment.

The entrance must be a sally port; the exterior door locked with an electric lock controlled from within the control center and the inner door controlled by a key-operated prison type (lever tumbler) lock also controlled by the control center officer. Persons waiting to gain entry to the control center must be plainly visible to the control center officer and a means of verbal communication must be provided (either an "audio port" as used at a bank, or a two station intercom). Keys to gain access to the control center in the event of an emergency inside the center (such as illness of the operator) must be kept in a secure location outside the center.

The doors must meet the most rigid strength criteria and must have at least a 2-hour fire rating to meet the National Fire Protection Association (NFPA) Life Safety Code [2].

15.4 Requirement

Console design and operation. The control center console shall be designed for efficient and convenient use by the officer or officers and shall serve all the alarm and communication functions in one consolidated unit.

Commentary

The control center, being the focal point of a such a vast number and variety of alarm and communication functions, often becomes so busy that important functions can be easily overlooked. The console equipment must consolidate as many functions as possible and put the response switches in convenient positions for human action. Insofar as possible, chances for human error should be removed.

15.4.1 Criterion

One operator. The console should be designed for one-person operation under normal conditions.

Evaluation

Review plans.

Commentary

During normal operation, the control center will be staffed by only one officer. Therefore, careful consideration must be given to location and configuration of the console, monitors and map display so that the officer can perform all the necessary functions from one position. Wireless head sets combining all forms of communications (telephone, radio, paging, etc.) should be used to allow the officer both hands free for operating switches and initiating telephone calls.

Consideration should be given to making the console height adjustable for comfortable operation by individual operators, both male and female, for both sitting and standing positions.

15.4.2 Criterion

Multiple operators. The console should have the built-in flexibility to allow two operators with complete redundant features.

Evaluation

Review plans and specifications.

Commentary

During periods of peak activity, it may take two officers to adequately operate the console. Therefore, it should be designed so that both work stations have access to all functions.

One way this has been done successfully is by placing the console in the center of the control room rather than the traditional method of placing it against the wall under the windows. The center location allows movement all around the unit and by placing monitors and controls on both sides with the map display horizontally between the operator locations, both operators can access all of the functions. This configuration also allows all of the wall space to be used for storage of equipment in an orderly fashion and makes movement in the control center very easy for one or more officers.

15.4.3 Criterion

Systems integration. The control console shall be so designed and configured to integrate all of the alarm and communication systems into one unit.

Evaluation

Review the plans and specifications, and perform operational tests.

Commentary

With so many communication and alarm systems terminating and/or originating in the control center, individual control panels are unwieldy. One solution is to feed all the information into a central processing unit (CPU) that is programmed to generate the appropriate alarm and then the officer can respond. The CPU is programmed to prompt the appropriate response from the officer and will not reset until the action is taken. Also, the CPU can be programmed to make other reactions to the alarm simultaneous, such as notifying both the control center and the mobile patrol vehicles of a perimeter alarm or automatically activating certain locks on an alarm.

For orderly and accurate activities to take place in a setting as busy as most control centers, it is imperative that time and thought be given to integrating the systems.

15.4.4 Criterion

Event recording. Alarms of all types should be recorded automatically giving the date, time, event and action taken.

Evaluation

Test operate the system and compare the print out with events tested.

Commentary

Many institutions rely on paper and pencil logs maintained by control center officers. With all of the various activities occurring in the control center, it is impossible for such record keeping to be accurate. The activity logs are very important in reconstructing events such as escape attempts and must be timely and accurate. Accurate records of time and place of all the various alarms is also necessary to ensure that the systems work properly. Manual attempts at recording all perimeter alarms have been totally unsuccessful. If systems tend to alarm frequently, the officer gets more complacent about making entries in the log. (See Criterion 8.2.11.)

The CPU operating the control console should be capable of displaying all alarms (duress, perimeter, fire, etc.), initiating audible signals and generating a hard copy printout.

15.4.5 Criterion

Console construction. The console including graphic displays, CCTV monitors, switches and indicator lights shall be designed and constructed with ease of operation and longevity foremost considerations. The entire console should be constructed in accordance with NEMA [3] standards and should be of UL listed equipment.

Evaluation

Review shop drawings and specifications.

Commentary The face of graphic displays should be of textured, non-glare, durable, scratch resistant material. Light-emitting diodes (LED), zone status indicators and membrane switches should be mounted beneath the display to ensure a continuous flush surface. Non-graphic panels should be low-voltage type control panels with switches and LEDs grouped for ease of operation. Dual CPUs should be provided for redundant operation.

See Criteria 8.2.7, 8.2.8, and 8.2.9 pertaining to perimeter systems and Criteria 14.4.1 and 14.4.2 pertaining to locking systems.

15.5 Requirement Alarm monitoring. The control center officer shall have the capability of monitoring all of the various alarm systems used throughout the institution.

Commentary Although institution design may dictate local alarm monitoring in housing units, the control center officer must also receive the alarms. Fire alarms, smoke alarms, and inmate-duress alarms may annunciate on local panels with pinpoint location, and then annunciate in the control center by zone or unit only. Control center monitoring should be as passive as possible so that the officer is notified of an alarm rather than constantly watching for signals.

15.5.1 Criterion Fire alarm and detection systems. An institution wide fire alarm and detection system approved by the appropriate jurisdiction shall be provided with alarm system monitoring in the control center and local annunciation in each zone.

Evaluation Review plans, specifications, NFPA Life Safety Code [2], and local code requirements.

Commentary The control console must contain a panel which will sound an audible alarm and display a visual indicator showing the alarm zone. Some jurisdictions require that alarms also be annunciated in the responding fire department. A monitor should be used to display the exact location and all alarms shall be printed out in hard copy.

15.5.2 Criterion Staff-duress alarms. A staff-duress alarm in any zone shall be annunciated at the control center as a single alarm on the map display.

Evaluation Review plans and specifications.

Commentary — A wireless radio frequency (RF) staff-duress alarm system should be capable of annunciating alarms within designated zones throughout the facility.

15.5.3 Criterion — Inmate-duress alarms. Where required by the NFPA Life Safety Code [2], a system shall be provided to permit all inmates be able to signal for help when in locked cells or rooms.

Evaluation — Review plans and operating procedures.

Commentary — In housing units that are not staffed 24 hours a day with adequate staff to monitor each cell or room, a signaling system must be provided inside the cells or rooms not monitored. These alarms, whether annunciated verbally or otherwise, must be monitored in an area that is staffed 24 hours a day. In many institutions, that area is the control center.

15.5.4 Criterion — Perimeter alarms. All perimeter alarm systems shall be monitored in the control center. All control and reset functions shall be in the control center.

Evaluation — Review specifications.

Commentary — The control console shall be capable of monitoring all sensors and control points and displaying the alarm on the graphic display, activating LEDs and sounding audible alarms. All reset capability shall be at the control console. Perimeter alarms must be investigated and classified (real, test, wind, etc.) before the system can be reset. See Criteria 8.2.9 and 8.2.10.

All perimeter patrol vehicles should be equipped with miniature site graphic maps to simultaneously display the status, including alarms, of the perimeter intrusion detection system as indicated on the large site graphic map in the control center.

15.5.5 Criterion — Miscellaneous alarms. The control center shall be the central monitoring and annunciating point for all other intrusion and operational alarms.

Evaluation — Review plans, specifications, and operating procedures.

Commentary In addition to the alarm systems mentioned elsewhere in this chapter, many other alarms are found in institutions. Intrusion alarms are often used on drug storage areas, hospital pharmacies and "hot" storage rooms.

Condition monitoring alarms are often used on refrigeration equipment, blood banks, boiler pressure monitoring devices, etc. Often times this equipment is located in areas not supervised 24 hours a day and therefore the alarms must be annunciated in the control center.

15.5.6 Criterion Closed circuit television (CCTV). All CCTV cameras used throughout the institution should be monitored in the control center. See Criterion 8.3.4 and 8.3.5.

Evaluation Review specifications and operating procedures.

Commentary It is important that video switching be used to keep the number of monitors to a minimum. The switching should permit automatic as well as manual switching of cameras. As with all other alarm monitoring in the control center, CCTV monitoring should be passive. The officer should not have to stare at a monitor or several monitors. Rather, he should be signaled audibly when viewing is necessary by motion detection built into the CCTV cameras that activate the monitor.

15.6 Requirement Door and gate control. The control center console shall contain graphic displays depicting the status of controlled doors and the necessary switches to activate the locks on these doors and gates.

Commentary Certain doors or gates in every institution (i.e., sally ports, segregation entrance, etc.) must be locked and unlocked by the control center officer. A graphic display must be included in the console to clearly show the status of these doors (locked, unlocked). When the officer gets a verbal request to unlock a given door, he can view the entrance on CCTV to identify the requestor and then activate the lock. After the door is closed, the graphic should again indicate the locked status of the door. See Criteria 14.4.1 and 14.4.2.

15.7 Requirement Telephone system. An electronic private automatic branch exchange telephone system (EPABX) interconnecting with the local telephone company shall be provided.

Commentary — There are several standard EPABX systems available that can be programmed or configured to provide the inside and outside telephone service required. Industry standard features such as compatibility with local telephone company, internal communications using only 4 digits, use of wide area services (WATS), speed dial and others are appropriate. In addition, the system must meet Federal Communications Commission (FCC) regulations.

15.7.1 Criterion — Selection of service class. The institution staff shall have the capability of programming each station for the appropriate class of service.

Evaluation — Review specifications and FCC regulations, Title 47, Part 68 [4].

Commentary — The system must allow for placing call restrictions on individual call stations throughout the facility depending on the use of the station and the security of the station. The four classes of service are: (a) direct access to local telephone company, i.e., dial 9 feature; (b) direct access to wide-area service, i.e, dial 8 feature; (c) access to local and wide-area service through central console only; and (d) inside service only.

15.7.2 Criterion — No-dial alarm. A circuit shall be provided that will give an alarm in the control center when dialing does not take place within 14 seconds on the first and second digits.

Evaluation — Review specifications.

Commentary — When a no-dial alarm condition exists, that station shall lock out and be positively identified on an annunciator in the control center. An audible signal shall be provided at the annunciator with an audible silence capability. This feature shall be reset by the act of returning the alarming station to an on-hook status and acknowledgment to the equipment.

15.7.3 Criterion — Fire and emergency reporting. The station number 222 shall be dedicated as the fire and emergency reporting number.

Evaluation — Review specifications.

Commentary — There shall be a minimum of six answering stations with an indicator panel in the control center to indicate the status (on-hook/off-hook) of each answering station.

The operation shall be such that when 222 is dialed from any station, the originating station will be locked in and positively identified by an annunciator in the control center. The acknowledgment shall be an equipment operation and may be in the form of a "reset" button.

15.7.4 Criterion — Watch-call. The station 333 shall be dedicated as the watch-call circuit.

Evaluation — Review specifications.

Commentary — This line shall be connected to a hands-free speaker phone. The first call entering this circuit shall enter with standard ringing. Successive calls shall enter the circuit automatically with no noise. There shall be an optional annunciator provided in the control center indicating the line or lines connected to this circuit. This will be a "non-busy" number, allowing access to all classes of stations.

15.7.5 Criterion — Executive Right-of-Way (EROW). Stations designated for executive right-of-way shall be able to break into a busy line.

Evaluation — Review specifications and test stations.

Commentary — A single audible notification shall be given to the called party. This feature should be provided for at least the chief executive officer, associate wardens and the chief of security.

15.7.6 Criterion — Conference call. The station 211 shall be dedicated as the emergency conference call originating only from EROW stations. The capability of connecting lines into this circuit shall be provided.

Evaluation — Review specifications and test stations.

Commentary — The operation shall be such that when 211 is dialed by any EROW station, all stations in this network shall instantly be placed in an "emergency conference". Idle stations will ring continuously until answered. Busy stations will have existing conversations terminated and after a tone, will automatically be placed into the conference. An optional annunciator shall be provided for all stations connected into this network to indicate status (on-hook/off-hook).

15.7.7 Criterion — Annoyance-trap. Any station user receiving an annoyance type call can alert an associate to call and ask the control center officer to call the station and identify the calling station.

Evaluation — Review specifications and test stations.

Commentary — Using the annoyance-trap feature will not tie up the exchange in any manner.

15.7.8 Criterion — Direct-fire line. The system should accommodate a direct line to the fire department serving the institution.

Evaluation — Review specifications and test the line.

Commentary — The NFPA Life Safety Code [2] and many local jurisdictions require a direct telephone line to the local fire department. This should be done via a separate station and instrument located in the control center. The instrument should automatically connect with the fire department without dialing. It should be clearly marked "Fire Phone".

15.7.9 Criterion — Inmate telephones. Inmate service telephone stations shall be programmed to accommodate collect calls only.

Evaluation — Review specifications.

Commentary — Inmate service telephones should be placed in each housing unit day room. They should be programmed to access the operator who will place collect calls only. All of these phones should be equipped for monitoring by a designated staff member, and a cut-off switch shall be located in a designated area so the instrument can be made inoperable.

15.7.10 Criterion — Direct-connect lines. In addition to and separate from the EPABX, at least one direct line to the local telephone company shall be provided.

Evaluation — Review the specifications.

Commentary — In the event of failure of the EPABX, at least one independent line from the control center to the telephone company is necessary for emergency calls.

15.8 Requirement

Radio system (voice communications). A 2-way radio system shall be installed to provide communication between the control center and officers within the institution, in mobile patrol vehicles and within a reasonable distance away from the institution as well as with local law enforcement personnel.

Commentary

Most law enforcement radio systems now in use are FM (VHF high-band, 150-174 MHz). Normally four frequencies are required: (1) custodial frequency for transmission of messages relating to inmate counts and other security related events; (2) administrative frequency for communications related to other routine matters such as movement of staff through the institution, maintenance personnel communicating with each other, etc.; (3) body alarm frequency (not voice) for transmitting personal duress alarms; and (4) local law enforcement frequency compatible with the local police or sheriff's department for use in escape hunts, etc.

Several guides, published by the National Institute of Justice, contain very useful information regarding the selection of appropriate radio and communications equipment [5,6,7].

One important aspect of the radio system is proper maintenance and servicing of the equipment. Usually the best approach is a service contract with the manufacturer. All radio equipment shall meet FCC regulations.

15.8.1 Criterion

Base station. A base station shall be installed with adequate power to service communications within the institution and outside for approximately a 20 mile radius.

Evaluation

Test portable-to-base station operation throughout the desired area of service.

Minimum performance requirements and test methods for fixed and base station FM transmitters and antennas are contained in NIJ Standards 0201.01 [8] and 0204.01 [9], respectively.

Commentary

The base station and antenna should be located outside of the secure perimeter of the institution with remote operation from the control center console.

15.8.2 Criterion

Mobile units. Mobile radio units shall be provided in all perimeter patrol vehicles and other vehicles used for routine patrols, escape hunts or for transporting inmates outside of the institution.

Evaluation — Test communications between mobile units and between mobile and base station units in the desired area of coverage.

Minimum performance requirements and test methods for mobile FM transceivers and mobile antennas are contained in NIJ Standard 0210.00 [10] and NILECJ Standard 0205.00 [11], respectively.

Commentary — In a base station-mobile station communication link, the weakest part is usually the inability of the mobile transmitter to be heard by the base station receiver. The base station can usually be heard in the vehicles. Additional information on the selection and use of mobile communications equipment is provided in Reference [5].

15.8.3 Criterion — Personal/portable units. Portable radios to be carried by officers shall be capable of transmission to and from anywhere within the institution and must be extremely durable.

Evaluation — Test portable-to-base and base-to-portable transmission throughout the desired area of coverage.

Performance requirements and test methods for personal FM transceivers are included in NIJ Standards 0209.01 [12] and 0224.00 [13]. Performance requirements and test methods for personal transceiver batteries are provided in NILECJ Standard 0211.00 [14].

Commentary — The number of portable units should be kept to a minimum or the frequency will become so busy they will be useless. Approximately 40 units should be the maximum number used.

The charger for the portable units must be kept in a convenient location so that the control center officer can monitor the charging time on the individual batteries. The charging/storage unit should also be below the glazing level of the control center so it is hidden from view outside of the control center.

15.9 Requirement — Intercommunication systems. Intercom and paging systems shall be provided for in-house communications independent of the telephone system.

Commentary — An intercom system independent of the telephone system, fire alarm and all other forms of communications is required for 2-way communication between certain locations such as centrally controlled doors and gates. Also, a paging system is required to make announcements to either the entire population or selected areas.

15.9.1 Criterion

Intercom. A dedicated intercom system shall provide 2-way communication between the master station in the control center and selected remote stations.

Evaluation

Review specifications.

Commentary

The dedicated intercom is used for 2-way communication between the control center and certain designated areas that require frequent contact such as doors and gates that are controlled from the control center. The control center can initiate a conversation with any of the stations. A remote station must alert the control center that a conversation is desired by depressing a "push-to-talk" button on the intercom unit. The control center officer then initiates the communication link. These are often used to identify persons and to request actions from the control center officer. Because of the location of the units in areas of inmate traffic, they should be flush mounted and vandal resistant.

The intercom service can be provided via the telephone system, however, system redundancy is then sacrificed.

15.9.2 Criterion

Paging (Public Address). A public address system, which is audible in all areas of the institution and includes zoned or general paging, shall be provided.

Evaluation

Review specifications.

Commentary

The paging system shall take precedent over all other connected systems. The system shall be engineered to provide good audio in each of the zones and to make the zones easily identifiable. All too often the control center officer takes the easy way out and uses the "all-page" button thereby disrupting the entire institution when only one housing unit need be paged. Since the speakers are located in areas of inmate traffic, they should be flush mounted and vandal resistant.

15.10 Requirement

Key Control. A system for key control shall be provided for in the control center.

Commentary

Without positive control of all keys (knowing exactly where each key is at all times), an institution is totally at risk. Inmates are capable of duplicating keys in the most ingenious ways. Also, special purpose keys or sets of keys must be readily identifiable and available, such as in case of fire or other disturbances. See Requirement 14.6.

15.10.1 Criterion — Key issue and return. There should be a convenient facility and method for the issue and return of keys to and from staff members by the control center officer.

Evaluation — Review plans and operating procedures.

Commentary — The issue and return of keys at shift change time is an important function of the control center. At some shift changes, scores of staff members must turn in keys. Since their shift is over, everyone is in a hurry to leave and does not want to be unduly delayed. The control center officer must be able to handle the key exchange quickly and concisely without losing control of his other functions in the control center.

Location and convenience of the key pass is most important. Consideration must be given to the possibility of a long line of people waiting their turn and therefore blocking traffic.

15.10.2 Criterion — Inventory control. Keys should be stored so that missing keys can be readily noted and identified.

Evaluation — Review plans and operating procedures.

Commentary — Keys must be stored on a board with individual hooks for each set of keys. A "chit" system of key issue works very well. Each officer has a chit, usually brass, engraved with his unique number. When he draws his keys from the control center, his chit is hung on the hook in place of the keys. This allows the control center officer to note missing keys and to readily identify who took the keys last. The key board often times becomes too large and cumbersome. Sectional hinged boards may be used that allow the board to fold up and to be hidden from view.

15.11 Requirement — Reliable power. A reliable, independent power supply shall be provided for the control center.

Commentary — Even if the electrical power fails everywhere else in the institution, it must not fail in the control center. The control center equipment must be able to function independent of all other electrical equipment in the institution.

15.11.1 Criterion

Engine-generator. The institution shall be equipped with an engine-generator set or multiple synchronized sets to power all essential equipment in time of normal power failure. The control center and all of its equipment must be fed from circuits that automatically switch to generated power in time of normal power failure.

Evaluation

National Electrical Code [15] requirements and NFPA Life Safety Code [2] requirements.

Commentary

Usually the institution will have two sources of normal electrical power with the appropriate switching equipment. In addition, an engine-generator set is provided for essential power in the event of loss of normal power. However, in the event of an internal incident, the generator power may not be available to the control center and it is necessary to also provide an uninterruptable power supply (UPS) system. See Criterion 15.11.2.

15.11.2 Criterion

UPS system. An uninterruptable power supply (UPS) system shall be provided that can supply electrical power to all control center equipment and all alarm systems for a minimum of four hours.

Evaluation

National Electrical Code [15] requirements and electrical load requirements.

Commentary

The UPS system should be installed in the equipment room as a secondary power source for all essential equipment in the control center and all alarm system components. The system shall have a capacity of 140% of the connected load and shall provide uninterruptable power to the loads. The system should be complete with nickel cadmium or jell-cell batteries, charging system and all essential monitoring equipment and indicators. The system must produce "computer grade" power.

Chapter 15 - References

1. Design Guide for Secure Adult Correctional Facilities, American Correctional Association, 4321 Hartwick Road, Suite L-208, College Park, Maryland 20740, 1983.

2. Code for Safety of Life from Fire in Buildings and Structures, NFPA 101-88, National Fire Protection Association, Batterymarch Park, Quincy, MA 02269, 1985.

3. National Electrical Manufacturers Association (NEMA), 2101 L Street, NW, Washington, DC 20037.

4. Code of Federal Regulations, Title 47, Telecommunications, Part 68-Connection of Terminal Equipment to the Telephone Network, Federal Communications Commission, Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

5. Mobile Radio Guide, NIJ Guide 202-83, National Institute of Justice, 1983.

6. Personal Radio Guide, NIJ Guide 203-83, National Institute of Justice, 1983.

7. Guide to Base Station Communications Equipment, NIJ Guide 204-83, National Institute of Justice, 1983.

8. Fixed and Base Station FM Transmitters, NIJ Standard-0201.01, National Institute of Justice, September 1987.

9. Fixed and Base Station Antennas, NIJ Standard-0204.01, National Institute of Justice, December 1981.

10. Mobile FM Transceivers, NIJ Standard-0210.00, National Institute of Justice, May 1986.

11. Mobile Antennas, NILECJ Standard-0205.00, National Institute of Justice, May 1974.

12. Personal FM Transceivers, NIJ Standard-0209.01, National Institute of Justice, September 1985.

13. Personal/Mobile FM Transceivers, NIJ Standard-0224.00, National Institute of Justice, May 1986.

14. Batteries for Personal/Portable Transceivers, NILECJ Standard-0211.00, National Institute of Justice, June 1975.

15. National Electrical Code, NFPA 70-87, National Fire Protection Association, Batterymarch Park, Quincy, MA 02269, 1987.

FORM NBS-114A (REV 11-84)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NISTIR 89-4027	2. Performing Organ. Report No.	3. Publication Date January 1989

4. TITLE AND SUBTITLE

Preliminary Performance Criteria for Building Materials, Equipment and Systems Used in Detention and Correctional Facilities

5. AUTHOR(S) Robert D. Dikkers, Robert J. Husmann, James H. Webster, John P. Sorg, Richard A. Holmes

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.
Grant No. 45

8. Type of Report & Period Covered
Preliminary

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

U.S. Department of Justice
National Institute of Corrections
Washington, DC 20534

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

In a National Institute of Corrections (NIC) sponsored study initiated in 1986, the National Bureau of Standards (now the National Institute of Standards and Technology) identified many important criteria and standards which need to developed for improving the selection of materials, equipment and systems for use in detention and correctional facilities. The development of performance criteria was one of high priority activities identified.

The preliminary performance criteria for materials, equipment, and systems contained in this report have the following objectives: (1) establish performance levels which are consistent with the security and custody levels used in detention and correctional facilities; and (2) establish standard performance measures with regard to security, safety and durability. Part I contains general criteria pertaining to the overall facility -- its mission, security levels, and operation; and various considerations relating to the selection of the facility site. Part II contains requirements and criteria relating to the perimeter security of the facility. Part III includes requirements and criteria pertaining to structural systems, doors, windows, glazing, locks, control center, alarms and communication systems.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)
Alarms, building materials, communication systems, doors, fencing, glazing, intrusion detection systems, jails, performance criteria, prisons, windows.

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☐ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA 22161

14. NO. OF PRINTED PAGES
172

15. Price
$18.95

USCOMM-DC 85-6006