



Designation: F1465 – 03

Standard Guide for Selection of Security Control Systems¹

This standard is issued under the fixed designation F1465; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ϵ) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide covers the identification of issues and decisions that need to be addressed to meet the objective of specifying an operational security control system for a detention facility.

1.2 **Appendix X1** contains additional sources of information that may be useful to the user of this guide.

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*²

F1577 Test Methods for Detention Locks for Swinging Doors

2.2 *International Electrotechnical Commission:*
IEC 1131 Part 3—Programming Languages³

3. Terminology

3.1 *Definitions:*

3.1.1 *analog, adj*—representing a range of values in the form of a continuously variable property, such as voltage in a circuit. Analog often refers to transmission methods for audio and video signals.

3.1.2 *audio threshold sensing, n*—mechanism which monitors a preset noise level and generates an alarm when that level is exceeded.

3.1.3 *biometrics recognition, n*—means of automatically identifying persons on the basis of unique personal characteristics, some of which include fingerprints, voice, retina, and hand geometry.

3.1.4 *bolt position switch (BPS), n*—electrical device that identifies the status of the deadbolt, roller bolt, or latchbolt within a locking mechanism.

3.1.5 *building automation system, n*—a system which includes multiple tasks such as HVAC (heating, ventilation, air conditioning) controls, in addition to specific correctional functions and MIS (management information systems), etc.

3.1.6 *Class A communications, n*—bidirectional signal within a looped wiring topology. Two cuts anywhere in the loop will disable the area between the cuts, but all other points in the loop will still communicate. A single cut will not result in a loss of communications.

3.1.7 *Class B communications, n*—a unidirectional signal within a radial wiring topology. Any interruption in the signal path will disable all points beyond the interruption.

3.1.8 *client, n*—a computer or application that makes use of the services provided by a server. A client typically has one user, whereas a server is shared by many different users.

3.1.9 *coaxial cable, n*—two-conductor cable in which a center conductor is surrounded by a shield. Used for transmitting/receiving radio and video signals.

3.1.10 *conformal coating, n*—plastic coating to protect electronic circuitry from moisture deterioration.

3.1.11 *deadlock status switch, n*—an electrical component within a device that provides the monitoring of a mechanical deadlock mechanism.

3.1.12 *detention, n*—a term which includes all types of facilities where people are held in custody, such as jails, prisons, and mental health facilities.

3.1.13 *dedicated microprocessor, n*—a software-driven control system created specifically to handle a defined application.

3.1.14 *digital, adj*—representing a range of values in the form of binary (that is, on or off) digits.

3.1.15 *digital signals, n*—electrical information in the form of a sequence of on/off voltage. The information may be coded in many ways, so more definition is required for any particular application.

3.1.16 *direct supervision, n*—management concept for operating a detention facility that relies on staff's ability to manage through personal interaction between the officer and inmate—does not rely on physical barriers or technology as the primary management mechanism.

¹ This guide is under the jurisdiction of ASTM Committee F33 on Detention and Correctional Facilities and is the direct responsibility of Subcommittee F33.06 on Control Systems.

Current edition approved Sept. 10, 2003. Published September 2003. Originally approved in 1993. Last previous edition approved in 1999 as F1465 – 99. DOI: 10.1520/F1465-03.

² For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

³ Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036.

3.1.17 *discrete logic*, *n*—a combination of distinct electronic components which performs a predetermined function in response to a defined input signal(s) (always custom to the application).

3.1.18 *door position switch (DPS)*, *n*—an electrical device to monitor whether a door or other opening is open or closed.

3.1.19 *Doppler frequency shift*, *n*—a change in frequency due to motion of an object through a radio field. A well-known example is police radar for speed measurement.

3.1.20 *dry circuit contact*, *n*—metallic points that complete or open a circuit upon occurrence of some defined condition.

3.1.21 *duress alarm*, *n*—system for reporting when staff needs emergency assistance; also known as body alarm or personal alarm.

3.1.22 *electromagnetic interference (EMI)*, *n*—most electronic systems require varying degrees of shielding to protect against EMI. Examples of common sources include lightning, fluorescent lights, switching of motors, and radio and TV stations.

3.1.23 *emergency release*, *n*—the release of inmates or relocation of inmates, or both, by a local or remote unlock mechanism that maintains the safety of staff, inmates, and visitors.

3.1.24 *environmental conditions*, *n*—conditions affecting the equipment and personnel including, but not limited to, lighting, temperature, humidity, square footage, ventilation, and noise level.

3.1.25 *event message field*, *n*—a display area used to list received information, typically with the ability to scroll the entire list.

3.1.26 *fail safe*, *n*—the security hardware reverts to an unlocked condition upon loss of power.

3.1.27 *fail secure*, *n*—the security hardware reverts to a locked, or secured condition upon loss of power.

3.1.28 *false alarm rate (FAR)*, *n*—frequency of errant alarms due to malfunction with no discernible outside stimulus.

3.1.29 *fault-tolerance*, *n*—a design method that ensures continued system operation in the event of individual failures by providing redundant levels.

3.1.30 *Form C relay*, *n*—a type of dry circuit contact that has one input and two possible outputs, one of which is normally closed (N.C.) and one of which is normally open (N.O.) when the relay is not energized.

3.1.31 *frequency division multiplexing (FDM)*, *n*—a means of information transmission where the data is divided into several transmission frequencies. Many signals can be carried on a single pair of conductors or strand of fiber.

3.1.32 *gas discharge arrestor*, *n*—a sealed device filled with a gas, which will allow a circuit to exist above a certain threshold voltage. Frequently used to bypass extreme electrical surges around electronic systems.

3.1.33 *hard control panel*, *n*—an operator interface consisting of individual control and annunciation devices grouped on a fixed plate.

3.1.34 *hard wire*, *n*—a system in which a direct conductor (wire) connects a control switch and the controlled point; or between a sensor and its indicator on the panel (always custom to the application).

3.1.35 *hermetically sealed relay*, *n*—a relay which has its contact in a sealed enclosure (usually made of glass) so that any arcing is prevented from affecting the surrounding atmosphere such as becoming an ignition source.

3.1.36 *ID codes*, *n*—personal identification numbers assigned to each person uniquely.

3.1.37 *ID code reader*, *n*—device to identify persons on the basis of ID codes embedded in tokens carried by the person, some of which include card, keys, badges, and wrist bands.

3.1.38 *indirect supervision*, *n*—management concept for operating a detention facility that relies on physical barriers to separate officers and inmates, and technology for control (also referred to as *remote supervision*).

3.1.39 *intercom system*, *n*—mechanism providing two-way audio communication between two or more points.

3.1.40 *last state*, *n*—the position of the lock (that is, either locked or unlocked) prior to a given event.

3.1.41 *local operation*, *n*—ability to monitor a device or control a device, or both, at or in close proximity to the device.

3.1.42 *location discrete*, *n*—the ability to annunciate an alarm by identifying a specific area in the protected facility.

3.1.43 *lock status switch*, *n*—an electrical component(s) within a lock that monitors the position of a bolt or latch, or both, in a lock.

3.1.44 *low voltage system*, *n*—electrical or electronic system operating in accordance with the definitions of the National Electrical Code (NEC) NFPA-70.

3.1.45 *masking*, *v*—a process by which a system ignores designated signals while receiving others.

3.1.46 *mean time between failures (MTBF)*, *n*—a statistical estimate of the expected operating time between failures, representing the potential reliability of an electronic system or component.

3.1.47 *mean time to repair (MTTR)*, *n*—time required to diagnose a system failure when it occurs and return the system to proper operation.

3.1.48 *microcomputer*, *n*—standard commercial computer system which can be customized through software to perform predetermined functions.

3.1.49 *mission statement*, *n*—defines the goals and objectives of the client/agency regarding the facility.

3.1.50 *mortise*, *adj/n*—a space hollowed out, as in door or frame, to receive a lock.

3.1.51 *multimedia*, *adj*—a computer technology that integrates full motion video, audio, graphics, text, or animation, or a combination of these, into a single operator interface.

3.1.52 *multiplex*, *n*—the process of sending two or more messages through a single communications media, such as a pair of wires, or a fiber optic link, etc.

3.1.53 *NEMA enclosure*, *n*—housing type tested to meet standards of the National Electrical Manufacturers Association. The housing type number describes the environment in which the contained electrical equipment can be safely operated.

3.1.54 *network*, *n*—a data communication channel connecting a group of computers and associated peripherals for purposes of messaging and resource sharing.

3.1.55 *normally closed (connected) circuit (N.C.)*, *n*—an electrical circuit which provides a change of status by the interruption of current flow.

3.1.56 *normally open circuit (N.O.)*, *n*—an electrical circuit which indicates a change of status by the initiation of current flow.

3.1.57 *nuisance alarm*, *n*—an alarm which is generated by a stimulus similar to that which the system is designed to detect, but not the correct stimulus.

3.1.58 *operator interface*, *n*—converts machine signals to an audio/visual (hard panel or video) display, and human actions into control signals that a security control system can act upon. (See 3.1.33 and 3.1.93; *control station* means either type of interface.)

3.1.59 *operator interface (OI) software*, *n*—commonly referred to as “video display application software.”

3.1.60 *paging system*, *n*—mechanism providing one-way audio communication to a single or multiple location.

3.1.61 *paradigm of display*, *n*—prescribes when and how information is displayed and to what degree automation is utilized.

3.1.62 *peer*, *n*—peer networks make the data and resources of any video control station available to any other video control station.

3.1.63 *peripheral device*, *n*—a device connected to a system to provide communication (as input or output) or auxiliary functions.

3.1.64 *pixel*, *n*—a contraction for “picture element.” In video detection it refers to the smallest detection area.

3.1.65 *point to point*, *n*—term used to describe wiring run from one point to another. (Not the same as “hard wired.”)

3.1.66 *probability of detection (POD)*, *n*—the odds of detecting a real event in an area of monitoring. (See also *nuisance alarm* because the rate of these is closely related to POD.)

3.1.67 *programmable controller*, *n*—an industrial automation product which can be customized through IEC1131 compliant software to perform predetermined functions.

3.1.68 *proprietary programmable controller*, *n*—an industrial automation product that can be customized through software to perform predetermined functions, but which does not comply with IEC1131 implementation requirements for software or hardware, or both.

3.1.69 *radome*, *n*—plastic face on microwave transmitter and receiver which allows RF signal to penetrate enclosure to antennae.

3.1.70 *redundant signal*, *n*—a signal that is transmitted at least twice (for example, verified) independently, before action is taken on the signal. A means of reducing false alarms caused by extraneous noise.

3.1.71 *relay logic*, *n*—the next higher level of complexity from hard wire which uses devices that enable direct branching and distribution of signals (always custom to the application).

3.1.72 *remote operation*, *v*—monitoring devices and systems or controlling devices or systems, or both, from a location that is separate and physically removed from the devices/systems.

3.1.73 *remote release*, *n*—device to unlock secured doors from a location which is separate and physically removed from the doors.

3.1.74 *run-time module*, *n*—a version of software that provides only the features used by the operator.

3.1.75 *sallyport (security vestibule)*, *n*—a compartment provided with two or more doors where the intended purpose is to prevent continuous and unobstructed passage by allowing only one door to be open at a time. Some jurisdictions reserve the term “sallyport” for vehicular access points and use “vestibule” for pedestrian access points.

3.1.76 *scream alarm*, *n*—see *audio threshold sensing*.

3.1.77 *screen depth*, *n*—screen depth is used to indicate the number of levels in the display hierarchy (that is, how many steps are required to “drill-down” from the site map to the lowest level).

3.1.78 *secure*, *n*—a term which describes the desired state of a monitored condition. An example would be that a door is “secure” when it is closed, and deadlocked.

3.1.79 *security control system*, *n*—physical and associated electronic devices used by staff to monitor and control the movement of inmates.

3.1.80 *self-test generator*, *n*—a circuit which allows the controller to simulate a stimulus to a sensor. Also called “remote test generator.”

3.1.81 *server*, *n*—any computer that makes access to files, printing, communications, and other services available to “clients” on a network. A server typically has a more advanced processor, more memory, a larger cache, and more disk storage than client computers.

3.1.82 *shunting*, *v*—a process that disables communications between pieces of equipment. (Not to be confused with “masking.”)

3.1.83 *signal line security*, *n*—a term which describes the ability of a communications link to resist tampering or interference. Needs to be accompanied by defining parameters.

3.1.84 *signal to noise ratio (SNR)*, *n*—relation of sensor output as seen at the controller input to the total signal, which includes interfering electrical noise. A low ratio increases nuisance and false alarms.

3.1.85 *sound activated alarm monitoring (SAAM)*, *n*—see *audio threshold sensing*.

3.1.86 *sound disturbance alarm*, *n*—see *audio threshold sensing*.

3.1.87 *span-of-control*, *n*—area(s) or function(s) controlled and monitored by an operator interface.

3.1.88 *time division multiplexing*, *n*—signals from each point are given a specific time slot to report their status. (Most common method is referred to as “polling” where the controller interrogates each point, which then reports its status.)

3.1.89 *transponder*, *n*—transmitter/receiver that provides information when queried.

3.1.90 *trickle charge*, *v*—a process of maintaining a small charging current to a battery to ensure that it remains fully charged at all times.

3.1.91 *trim*, *n*—door hardware term referring to the part of a lock which is used to operate the latch or pull the door open, or both. Examples are knobs, levers, and **Documents**

3.1.92 *ultrasonic detector, n*—a sensor which responds to an acoustical energy pattern in the frequency range from 19 to 45 kHz. This frequency range will not penetrate walls, floors, or ceilings.

3.1.93 *video control station, n*—operator interface having dynamic presentation of control and annunciation elements.

3.1.94 *watch tour system, n*—mechanism to record staff patrols throughout the facility, usually recording the time a particular officer was at a specific location.

3.1.95 *zone, n*—defined area or point for directing attention for the purpose of individual response or assessment.

4. Summary of Guide

4.1 This guide is summarized in Figs. 1 and 2, which show the essential sequence of analysis and topics of analysis that must be followed in order to obtain a technology that is constructible, maintainable, operable, and functions in the manner desired.

5. Significance and Use

5.1 **Warning:** This guide does not identify specific technology for specific applications. It attempts to identify points of experience which will enable the planner(s) to make informed selections.

5.2 This guide should be used early in the planning stages of a project so that the proper security scope is established at the same time that the facility mission is established.

5.3 The proliferation of security technologies has become so great that evaluation and selection has become difficult.

In the design and selection of the security control systems consistent with the principles outlined in this guide, the following steps should be followed:

- Step 1: Define the characteristics of the proposed facility
- What operational philosophy will be followed?
 - Direct supervision
 - Indirect supervision
 - What staffing restrictions will be confronted?
 - Due to size of staff
 - Due to location of facility
 - Due to education and training
 - Due to current pay scales
 - What environmental limitations will be confronted?
 - Due to terrain
 - Due to weather
 - Building design and layout?
 - Centralized or decentralized control
 - Podular or linear arrangement of cells
 - Single building or campus arrangement
 - Low rise or high rise
- Step 2: Evaluate the selections of Step 1 for conformity to ALL of the decisions, capabilities, and restrictions defined in Step 1. Reevaluate Step 1 to be absolutely sure that all restrictions have been identified, that capabilities have been accurately assessed, and that decisions are truly appropriate. Changes at this stage are still easy and relatively inexpensive.
- Step 3: If everything is consistent and positive, write the specifications making certain that any features that have been selected from the guide are incorporated specifically and explicitly.
- Step 4: Enforce the specification. Changes made after the specification is put out for bid have a high probability of being inconsistent with other specification sections, and may deviate from the operational decisions made in Step 1.

FIG. 1 Flow Chart of Selection Process

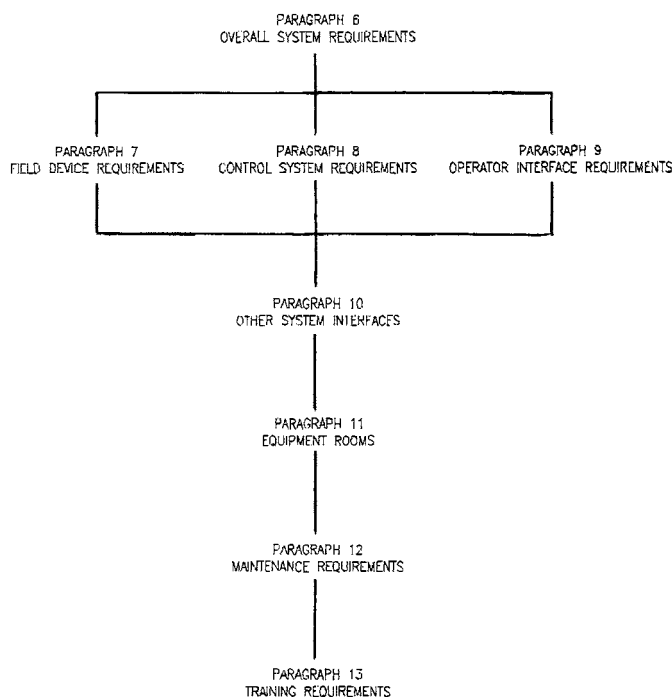


FIG. 2 Flow Chart of Document Sequence and Organization

5.4 This guide shows the planner(s) the steps required to establish the necessary and sufficient requirements for the application, and from those, how to evaluate the possible technologies for conformance to those requirements.

5.5 Using this guide, the planner(s) should be able to produce a more complete and accurate specification that meets the operational goals of the facility.

6. Establishing System Requirements

6.1 Staff capability should be evaluated to determine the level of sophistication that can be supported by the operational and maintenance staff (see Figs. 1 and 2). Carefully consider the following issues;

6.1.1 Physical location of the facility in relation to the technical capability of the work force that will maintain and operate the facility.

6.1.2 Training of initial and replacement staff, since the adequacy of this training will determine if the system will be utilized effectively.

6.1.3 Budgets for staff and training necessary to afford the competent level of expertise and sophistication required for system operation and maintenance.

6.2 Conditions in which the control system exists, or the application environment, should be evaluated. Carefully consider the following issues;

6.2.1 Management philosophy, such as direct or indirect supervision, for affect on location of control panels and for environmental conditions that may be encountered. Control panels in areas accessible to inmates typically need to be configured to resist abuse and prevent operation by unauthorized persons.

6.2.2 Control station visibility due to effects of both natural and artificial lighting.

6.2.3 Protection from the elements and safety of persons and equipment where panels are exposed to an outdoor or similar environment.

6.3 Security functions that the operator and system need to perform should be considered. Typical functions include;

6.3.1 *Locking Control*—Consider the need and evaluate the means for the restriction and control of movement of people throughout the facility.

6.3.1.1 Remote control provides efficient control of movement of people throughout the facility with reduced staff.

6.3.1.2 Local control may be provided by key, key operated switch, ID code reader, or biometrics recognition.

6.3.2 *Emergency Release*—Consider the need for quick release of a secured means of egress in the case of emergencies. Evaluate the time required for orderly evacuation or relocation of people while maintaining the safety and security of staff, visitors and inmates. Local release (in accordance with applicable codes) for a small quantity of doors or a group of cell doors may be allowable. More doors may require remote release.

6.3.3 *Emergency Annunciation*—Consider visual and audible annunciation of emergency functions that require quick response for effective control.

6.3.3.1 *Fire Alarm*—Annunciation of a potential fire condition including smoke detection, manual fire pull, or fire sprinkler system water flow.

6.3.3.2 *Duress Alarm*—Annunciation of a personal alarm or panic button activation.

6.3.3.3 *Intrusion Alarm*—Annunciation of an intrusion detection system alarm indicating an escape or unauthorized presence in a restricted space.

6.3.3.4 *Medical Alarm*—Annunciation of a medical emergency in a health or psychiatric unit requiring additional staff support.

6.3.4 *Life Safety Controls*—Consider inclusion of special control functions for the protection of people in life-threatening situations.

6.3.5 *Auxiliary Control Functions*—Consider control of devices and equipment to assist in supervision and control of activities.

6.3.5.1 *Lighting*—Control of selected lighting circuits to reduce lighting during night hours or increase lighting during emergencies. Override control of selected lighting functions in the case of emergencies or restriction periods.

6.3.5.2 *Telephone*—“On/Off” control of telephone use during restriction periods.

6.3.5.3 *Receptacles*—“On/Off” control of power to equipment such as televisions and radios during restriction periods or for disciplinary action on an individual basis.

6.3.5.4 *Cigarette Lighters*—“On/Off” control of power to cigarette lighters during restriction periods.

6.3.5.5 *Water*—“On/Off” control of water in case of piping damage or drain problems, that is, toilets and sinks. Water to showers may be controlled to establish timing restrictions. There may be a need to provide for the separate “on/off” control of water to individual cells to prevent the flushing of contraband.

6.3.6 *Operational Trouble or Tamper Alarms*—Consider the need for annunciation of a failure of a critical building system.

6.3.6.1 *Heating, Ventilating, Air Conditioning*—Annunciation of a failure of system equipment or control.

6.3.6.2 *Emergency Power*—Annunciation of a failure or potential failure of an emergency power source due to system malfunction, such as low fuel or low battery.

6.3.6.3 *Control Systems*—Annunciation of a failure of a component in any control or monitoring system.

6.3.6.4 *Fire Systems*—Annunciation of trouble indication on fire alarm or sprinkler systems.

6.3.7 *Audio Communication*—Consider the need for voice communication throughout the facility.

6.3.7.1 *Intercom*—Audio communications between the control location and a controlled door or restricted space.

6.3.7.2 *Call-in*—Manual call to monitoring location from a remote space or location.

6.3.7.3 *Threshold Sensing*—Call-in means used where a manual push button is not sufficient or monitoring of the space is desired.

6.3.7.4 *Paging*—Distribution of audio to a large area or groups of areas for general or emergency announcements.

6.3.8 *Visual Communication*—Consider visual observation throughout the facility.

6.3.8.1 *Direct*—Direct visual observation of the controlled device or location is preferred.

6.3.8.2 *Indirect*—Where direct visual observation is not possible or enhancement of direct visual observation is desirable, video communication equipment, that is cameras, monitors and other video peripherals may be used to augment operation.

6.3.8.3 Consider the choice of color or monochrome video. The additional cost of color may be justified when considering the additional capabilities for visual identification.

6.3.8.4 *Video Recording*—Consistent with state and federal law consider the application of video recording equipment in areas where visual documentation may support future disciplinary or legal action.

6.4 Shared operation of control functions should be considered. Priority of control must be determined as well as disabling needs. Examples of areas that may require shared operation include:

6.4.1 Sallyports or safety vestibules,

6.4.2 Duplication of control and monitoring functions for reduced staffing levels, and

6.4.3 Master panels for total facility supervision and emergency control.

6.5 *Record Keeping*—Recording of activities and operations may be desirable in cases of potential legal, disciplinary, or maintenance actions. Time, date, event number, and operator ID should be recorded on all events. Recorded data should be unalterable, and maintained in a secure location in accordance with a planned documentation retention policy. Examples of record keeping include:

6.5.1 Identification of staff, visitors, and inmates via such means as manual input, or presentation of a card or badge,

6.5.2 Reporting of watch tours.

6.5.3 Reporting of emergency alarms, that is fire, intrusion, audio disturbance,

6.5.4 Audit trail of control actions taken in response to emergency alarms,

6.5.5 Reporting of, and identification of accesses to restricted areas, that is evidence lockers, armory,

6.5.6 Reporting of head counts in housing and program units on a random, or as needed basis, and

6.5.7 An automated preventative maintenance schedule based on hours of operation or operating cycles.

6.6 *Data Storage and Retrieval:*

6.6.1 The system should be structured to record events as appropriate for desired administrative and maintenance purposes. Events may be:

6.6.1.1 Manually generated, or

6.6.1.2 Automatically generated.

6.6.2 Data retrieval needs should be considered in defining storage requirements.

6.6.2.1 Events which require immediate utilization, such as for shift change information, should be printed out.

6.6.2.2 Events that are recorded for future administrative analysis should be put on some form of long-term media, such as magnetic media or optical media.

6.6.3 It should be understood that certain security system technologies do not have automatic data collection, storage, and retrieval capabilities. Manual record keeping may be necessary for the following types of systems.

6.6.3.1 Hard wired systems,

6.6.3.2 Relay logic systems, and

6.6.3.3 Discrete logic systems.

6.6.4 Consideration should be given to the types and nature of administrative, security and maintenance events which it may be useful to record. Some examples of these events are listed below.

6.6.4.1 *Administrative*—Interlock overrides, emergency functions, test sequence initiations, watch tours, operator identifications and acknowledgements, and alarm events.

6.6.4.2 *Maintenance*—System trouble reports, communications failures, and door operations.

6.6.4.3 *Security*—Exceptions to secure status, such as bypassed perimeter zones and systems off-line for maintenance.

7. Establishing Requirements for Subsystem Selection and Associated Field Devices

7.1 *Electrical Interface Considerations for Locking Hardware*

7.1.1 *General Considerations for Swinging Doors; Basic Considerations of Locking:*

7.1.1.1 Door Position Switch (DPS).

7.1.1.2 Bolt Position Switch (BPS).

7.1.1.3 Lock Status Switch (LSS).

7.1.1.4 Deadlock Status Switch (DSS).

7.1.1.5 Generally, it is the responsibility of the owner and the designer to determine which of the preceding are necessary to perform the security function of a specific facility or application, or both. Additionally, the least expensive solution is to specify the minimum number sufficient to accomplish the facility mission.

7.1.1.6 A general comment about switches is that they are mechanical devices which will require maintenance and adjustment. Combining the switch indicators or annunciating them individually has advantages and limitations which should be considered.

(1) Cost.

(2) Ease of troubleshooting, that is, maintenance.

(3) Clarity of presentation of information on panel.

7.1.1.7 There are three basic electrical/pneumatic locking functions:

(1) Fail secure.

(2) Fail safe.

(3) Last state.

7.1.1.8 Remotely controlled or monitored door-mounted locks (mortise), or both, require some form of power transfer device to get signals and energy from the frame to the door.

7.1.1.9 Electric hinges, generally have small wires, such as #24 AWG. Consideration should be given to the possibility of abrasion and breakage due to flexing.

7.1.1.10 Electric pivots, which are similar to hinges, except that some manufacturers have special models with larger gage wire, such as #18 AWG.

7.1.1.11 “Power transfers” are generally designed to minimize flexing by coiling the wire like a telephone cord. Some incorporate special wire protection to minimize the potential for abrasion or pinching. Some are available with larger gage, such as #18 AWG wire.

7.1.1.12 The more conductors included, the greater the problems with abrasion and flexing.

7.1.2 *Types of Remotely Operated Door-Mounted Locks:*

7.1.2.1 Exit devices operate on low voltage or pneumatic energy, or both, and are generally described as fail secure. The exit devices require a minimum of two wires to perform the unlocking function. There are some models which provide other signals, and hence require more wires.

7.1.2.2 Mortise locks are available which operate on low voltage DC or AC energy and also on pneumatic energy. Mortise locks are available in both fail secure and fail safe varieties. These locks require a minimum of two wires to perform the locking or unlocking function. Mortise locks generally include the LSS function, and a few include the DSS function. Many vendors combine the two switches as a single signal in their standard product. Total wire count will range from four to eight.

7.1.2.3 Cylindrical locks (key in the knob) are available which operate on low-voltage DC or AC energy. Cylindrical locks are available in both fail secure and fail safe varieties. These locks require a minimum of two wires to perform the locking or unlocking function. Cylindrical locks generally include the LSS function. Total wire count is generally four.

7.1.2.4 Electrically controlled trims are available which operate on low-voltage DC or AC energy. These trims are available in both fail secure and fail safe varieties. These trims require a minimum of two wires to perform the locking or unlocking function. Controlled trims generally include the LSS function. Total wire count is generally four.

7.1.2.5 Bolt position monitoring is generally provided by a frame-mounted device, such as a keeper switch.

7.1.2.6 Door position monitoring is generally provided by a frame-mounted device, which may be combined with the power transfer device.

7.1.3 *Types of Remotely Operated Frame-mounted Locks:*

7.1.3.1 Frame-mounted locks are available in high- or low-voltage AC, DC, or pneumatic versions and in several physical sizes to accommodate varying degrees of security as defined in Appendix X2 of Test Methods **F1577**.

7.1.3.2 It is important to note that most, but not all, frame-mounted locks are normally manufactured with a mechanical latch-back that holds the door unlocked until the door is physically opened, at which time the latch bolt extends allowing the door to relock automatically when the door is closed. This feature is generally not desirable on doors that are unlocked remotely, particularly if the door is part of an interlocked group because the door cannot be remotely relocked. The door must be physically opened and then closed in order to release the mechanical latchback device and re-extend the latchbolt.

7.1.3.3 Some frame-mounted locks are available with a special mechanical input (usually for a cable) that can be attached to a mechanical remote gang release.

7.1.3.4 Frame-mounted locks generally provide a form of combined signal to indicate status. This is usually done by the DSS which is mechanically arranged so that it can not signal true unless the latch-bolt is extended fully and the actuating mechanism is in the locked position. A weakness of this arrangement is that it can be tricked into providing a secure indication with the door open. Therefore, a door position switch is a necessary component of the system.

7.1.3.5 A common arrangement with frame-mounted locks is to connect the DSS and DPS in series so that both have to be true (secure) to get a secure signal to the control system, and either will provide a false (unsecure). A weakness of this arrangement is that there is no indication of which switch is providing the unsecure signal, leaving the maintenance person to troubleshoot the problem.

7.1.3.6 Energizing mechanisms for frame-mounted locks include electric solenoids, electric motors, and pneumatic solenoids.

7.1.3.7 Electric solenoids are available in high- or low-voltage AC and low voltage DC.

7.1.3.8 Advantages of solenoids include:

(1) Solenoids react quickly. The time to unlock or relock is typically ½ s.

(2) Solenoids make noise that tells the person at the door that the lock has operated, either like a hammer (DC/pneumatic) or a loud buzz (AC).

7.1.3.9 Limitations of solenoids include:

(1) Low-voltage solenoids have limited mechanical power which means that the door can be bound up mechanically and the lock will fail to unlock.

(2) Solenoids intrinsically require substantially more current during pull than during hold, some by a factor of 15 times, but typically about 10 times.

(3) Solenoids require the continued application of power to retain the unlocked state if fail secure or the locked state if fail safe.

(4) Electric motors are available in high- or low-voltage AC, and low-voltage DC.

7.1.4 *General Considerations for Sliding Door Operators:*

7.1.4.1 There are several types of sliding door operators and the following list is not meant to address all possibilities but, rather address the most common types.

(1) Cell sliding door.

(2) Passage/corridor sliding door.

(3) Vehicular sliding door/gate.

7.1.5 The majority of sliding doors operate in three types of modes:

7.1.5.1 Manual which is opened and closed manually upon the individual unlocking the door with the key.

7.1.5.2 Kick release (KR) which is remotely unlocked and opened from a control station. Upon unlocking the kick release type of sliding door operator, the door will travel a few inches (usually 3 to 4 in.) without intervention by a device internal to the sliding door operator and requires an individual to fully open or close the door manually. (A kick release door operates similar to a remotely operated swing-type door where the individual must open or close the door after the control system has unlocked the door.) It is possible to have a kick release door lock in the opened position, to close the door an individual would need to remotely release the door and when released, the door travels a few inches from the locked open position allowing the individual to close the door to the secured position.

7.1.5.3 Full-power sliding door operators are remotely opened and closed from a control station. Upon opening the door, the door typically travels to the fully open position (unless the control system tells it to reverse travel) and stops in the locked open position. Similarly, closing the sliding door operator typically shall cause the door to unlock from the locked open position and travel to the fully closed position and lock. It should be noted that some sliding doors have the requirement to have a stop feature which can stop the door in either the opening or closing travel. Typically, the stop feature for a sliding door operator is used when the door covers a large opening (usually greater than 3 feet) or perhaps a vehicular-type application.

7.1.6 The status switches for the sliding door operators generally have two mechanical devices known as door position switches (DPS) and lock bar status switch. The sliding door operator may have an open door status switch and a closed door status switch.

7.1.6.1 Status switches require maintenance and adjustment. Combining the switch indicators or annunciating them individually has advantages and limitations which should be considered.

7.1.7 *Sliding Door Power Considerations (do not apply to manual device):*

7.1.7.1 Several types of remotely controlled sliding door operators have different power requirements. These requirements should be considered when selecting the type of operator. Typically, the sliding door operators are powered by 24 VDC, 120 VAC, 208 VAC, and 480 VAC. The pneumatic sliding door operators fall into the 24 VDC category.

7.1.7.2 24-VDC Operators:

(1) Advantages of 24-VDC operators:

- (a) May reduce power draw (including UPS if utilized).
- (b) Operator control wire/cable can be combined with other cables where code allows (for example, intercom wire/cable).

(c) Ability to use battery lockup.

(2) Limitations of 24-VDC operators:

- (a) Additional equipment required, such as 24-VDC power supplies.

7.1.7.3 120-VAC Operators:

(1) Advantages of 120-VAC operators:

- (a) Increased torque over the 24-VDC operators.
- (b) Does not require 24-VDC power supplies.

(2) Limitations of 120-VAC operators:

- (a) Some operators require a delay in applied power when trying to reverse travel.
- (b) Cannot combine with cables for other systems (that is, intercom).

7.1.7.4 208/480-VAC Operators (typically vehicle operators):

(1) Advantages of 208/480-VAC operators:

- (a) Increased torque over 24-VDC and 120-VAC operators.

(2) Limitations of 208-VAC operators:

- (a) Operator power cable cannot be combined with control cable.

7.2 Perimeter Security Devices

7.2.1 Elements to be considered for the proper selection and continued operation of outdoor perimeter security systems.

7.2.1.1 Probability of detection (POD).

7.2.1.2 Nuisance alarm rate (NAR).

7.2.1.3 False Alarm Rate (FAR).

7.2.1.4 Vulnerability to defeat (VD).

7.2.1.5 All elements of the sensor subsystem should be electronically monitored to ensure system integrity.

7.2.1.6 Preoperational Testing of all functions and performance.

7.2.1.7 Periodic testing:

- (1) On each shift, check status of each zone and verify operation.
- (2) Daily testing for detection.
- (3) Each zone and all functions shall be re-verified at least once per year.
- (4) Each zone and all associated functions shall be re-verified after any work done in the area.

7.2.1.8 A combination of technologies may be used to achieve the desired detection.

7.2.1.9 Multiple layers of detection may be used.

7.2.2 Volumetric Sensors:

7.2.2.1 “Microwave” Systems—Short wavelength radio frequency systems. Require a transmitter and a receiver.

7.2.2.2 Bi-static—The transmitter and receiver are in separate units to create a volumetric field of detection between them. An alarm is generated when a target enters the detection field and causes the received signal to increase or decrease beyond a preset threshold.

(1) Potential applications:

(a) Create a sensed area in open space where a line of sight exists between the transmitter and receiver locations. Examples: Sallyports, area between fences, area in front of fences, and over roofs.

(b) Advantages of bistatic technology:

- (1) Independent of other structures.
- (2) Not affected by fence maintenance.
- (3) Installed cost.

(c) Limiting conditions to consider:

- (1) Uneven terrain affects detection.
- (2) Control of vegetation and debris.
- (3) Space for “offset” and “overlap.” See Fig. 3.
- (4) Shooting through or over moving objects such as streams, wildlife, or fans in HVAC units.
- (5) Stable mounting locations.
- (6) Frequency and antenna selection are dependent on the application.

7.2.2.3 Monostatic—The transmitter and receiver are combined into a signal unit. Work on the Doppler principle. The alarm is generated by a change in frequency due to a moving target.

(1) Potential applications:

(a) Where the physical characteristics of the site discourage the use of bi-static such as filling dead zones in bi-static applications.

(2) Monostatic microwave systems must use one or more technologies to enable the unit to distinguish between targeted and nontargeted objects or environmental conditions.

(3) Advantages of monostatic technology:

- (a) Independent of other structures.
- (b) Not affected by fence maintenance.
- (c) Installed cost.

(4) Limiting conditions to consider:

- (a) Uneven terrain affects detection.
- (b) Control of vegetation and debris.
- (c) Shooting through or over moving objects such as streams, wildlife, or fans in HVAC units.
- (d) Stable mounting locations.
- (e) Frequency and antenna selection are dependent on the application.

(5) Typical required maintenance:

- (a) Periodically clean the radomes; at least once a year or as required by site conditions.
- (b) Vegetation must be kept short enough that it does not move in the wind.

7.2.2.4 Passive Infrared (PIR)—Establishes a detection envelope and looks for temperature variations between the target and the background that are in excess of a preset threshold.

(1) Potential applications:

(a) Detection envelope can be configured to handle tight sites.

(b) Typically used as a complementary sensor to other primary sensors.

(c) Principle limitation is nontarget objects within the detection envelope that are subject to changing temperatures, such as air conditioning units.

(d) Another limitation is that it needs a clear line of sight.

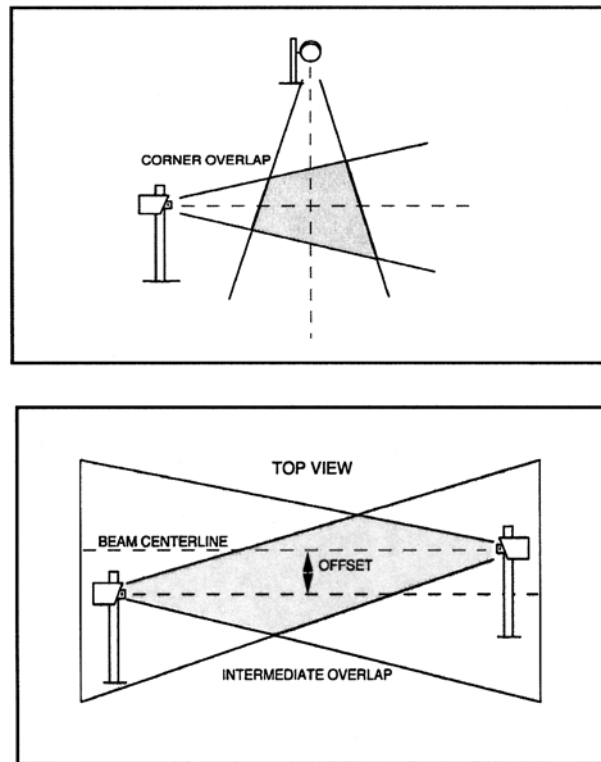


FIG. 3

(e) Passive Infrared (PIR) systems must use one or more technologies to enable the unit to distinguish between targeted and nontargeted objects or environmental conditions. Some of these technologies are:

(1) Use of “curtain” patterns for common mode rejection.

(2) Use of environmental housings; that is, heaters and blowers, and so forth.

7.2.2.5 “Electric Field” systems use a transmit wire to create an electric field in the space around the wire, and an array of sensing wires to detect changes in that electric field.

(1) Potential applications include:

(a) Creates a non-restraining physical barrier.

(b) Can be used on rooftops.

(2) Advantages include:

(a) Terrain following.

(b) Because it creates a volume of detection, you know when something is approaching the barrier.

(c) Operates independent of fence condition, that is, retrofit.

(3) Limitations of the technology include:

(a) Installed cost.

(b) Maintenance: array spacing changes with temperature.

(c) Sensitive to flora and fauna.

(d) Water or snow accumulating on or near the bottom wire of the array.

7.2.2.6 Buried ported coaxial cable sensors consist of either a single- or a dual- cable sensor system. A single-sensor system includes both transmit and receive cables in a single trench. Two cable sensor systems consist of separate receive and

transmit cable in separate trenches. The detection field is formed by radio frequency (RF) signals carried by the sensor cables buried along the perimeter. The RF signals form an invisible electromagnetic detection field around the sensor cable(s) that can detect the presence of an intruder passing through the field. The standard burial depth of the sensor cable(s) is 23 cm (9 in.) in soil and 6 cm (2.5 in.) in hard surfaces such as asphalt or concrete.

(1) Potential applications include:

(a) Perimeters where a covert sensor is desired.

(b) Perimeters where volumetric detection is desired but terrain is not suitable for line-of-sight sensors.

(2) Advantages include:

(a) Terrain following.

(b) Volumetric detection field can be made to extend below ground.

(c) Does not require a mounting structure.

(d) Not affected by ground vibration.

(e) Not affected by snow.

(f) Power and alarms can be transmitted over sensor cable.

(g) Difficult to defeat or tamper with since there is no visible indication of its presence or location.

(h) Can be installed in a variety of soil types, asphalt, and concrete.

(3) Limitations of this technology include:

(a) Installed cost.

(b) Soil conditions.

(c) Running or standing water.

(d) Maintenance: keeping it buried, wind, water, and frost heaving.

(e) Metal objects in the desired detection field must be avoided.

(f) Flora and fauna.

(g) Detection is affected by sharp corners.

(h) Repair costs.

7.2.2.7 Outdoor Video Motion Detection (VMD) Systems process video signals from video cameras and create a detection zone by dividing the field-of-view (FOV) into a series of detection “cells.” An alarm is generated when a preset number of cells are disturbed based on intruder contrast, size, speed, and direction. Most outdoor VMDs utilize advanced signal processing techniques and algorithms designed to reject nuisance alarm sources, such as weather conditions and small animals, inherent to the uncontrollable outdoor environment. There are many different VMD systems available, each having distinct advantages and disadvantages. Therefore, additional reference materials should be reviewed depending on the VMD application.

(1) Potential applications include:

(a) Can be used on building’s exterior, clear rooftops, in open space, between fences, and near fences.

(b) Can be used as a primary sensor if other technologies are limited by site constraints. Some nuisance alarms are acceptable and a sufficient clear zone is available with little or no blowing of debris or vegetation.

(c) As a secondary sensor to complement one or more primary or early warning sensors.

(d) As an early warning sensor to complement one or more primary or secondary sensors.

(2) Advantages include:

(a) Allows detection and assessment through a single video surveillance system.

(b) Can be incorporated into existing exterior video surveillance system with little or no site disruption.

(c) Can be visible or covert depending on the video surveillance system.

(d) Capable of detecting intruders in a large area based on the associated camera’s FOV. However, extreme distances may affect the operator’s ability to properly assess the cause of the alarm.

(e) Can be used in extreme temperatures and high humidity, and is generally unaffected by soil conditions and fence maintenance (unless the fence is in the active detection area).

(f) Can be independent of other structures.

(g) Can be used for nighttime detection with adequate normal lighting or the addition of infrared illuminators if a covert system is required.

(h) Low installed cost based on existing video surveillance cameras.

(3) Limitations include:

(a) THE VMD systems are subject to all of the limitations of any CCTV system.

(b) Performance of VMD products vary greatly in outdoor applications.

(c) Setup of some VMDs may be complicated or require frequent adjustments, or both.

(d) Detection is subject to the quality of the video signal, to the video contrast of the intruder, and to the amount of video change being created by the environment.

(e) VMD systems are subject to the effects of severe weather conditions (fog, rain, snow, and blowing sand) that deteriorate the video quality.

(f) Nuisance alarms can be generated by shadows from moving clouds and vehicle headlights, small animals, blowing debris, moving vegetation, and insects close to the camera.

7.2.3 Fence-mounted systems recognize that chain link fences are somewhat flexible structures. An attempt to climb the fence generates two types of movement; a slow side to side movement of the fabric, and an impulsive vertically oriented movement. An attempt to cut the fabric generates an impulsive shock which is transmitted through the fabric. This latter shock is generated by a combination of mechanical shearing of the wire, and by the release of the mechanical tension in the fabric. The systems consist of a combination of sensors and signal processors that employ some criteria to differentiate between intrusions and nuisance indications. There are five basic types of fence-mounted sensors which detect different types of fence movement.

7.2.3.1 Mechanical fence sensors all operate on the principle that movement of the fence will cause a switch mechanism to open or close a set of contacts.

(1) Advantages include:

(a) Terrain following on structure.

(b) A very simple technology.

(2) Limitations include:

(a) Position sensitivity makes it difficult to install.

(b) Potentially sensitive to corrosion that will affect reliability.

(c) Detection sensitivity is limited to one plane of movement, usually vertical.

(d) Numerous sensors in an array make it difficult to troubleshoot.

(e) Cannot be remotely tested.

(f) Uneven sensitivity between sensors.

(g) The cable may need to be applied to fence fabric to avoid inadvertent damage.

7.2.3.2 Electro-mechanical point sensors produce an analog signal instead of a switch closure.

(1) Advantages include:

(a) Terrain following on structure.

(b) Highly effective at detecting climb.

(c) The orientation in a single plane helps to eliminate nuisance alarms caused by wind-induced fence movements.

(2) Limitations include:

(a) Relatively high cost.

(b) Limited sensitivity to cutting.

(c) Large arrays of sensors makes it difficult to troubleshoot.

(d) Arrays must be factory-fabricated to match the fence.

(e) The cable must be applied to fence fabric to avoid inadvertent damage.

7.2.3.3 Strain-sensitive cables are sensors which are uniformly sensitive along their entire length and which produce an output voltage when the cable senses mechanical energy in the fence.

(1) Advantages include:

(a) Equal sensitivity throughout the entire length of the sensor.

(b) Terrain following on structure.

(c) Can tailor sensor application to fence to match structural changes; that is, corners, height, gage of fabric, curved, and so forth.

(d) Provide maximum information from the fence.

(e) Simple to install.

(2) Limitations include:

(a) Fence must be maintained to eliminate nuisance alarms.

(b) The cable must be applied to fence fabric to avoid inadvertent damage.

(c) The area around the fence must be maintained to keep vegetation and debris from impacting the fence.

7.2.3.4 Fiber-optic sensors are similar in appearance to a strain-sensitive cable, but detect mechanical energy from the fence as changes in the pattern of a transmitted laser light beam.

(1) Advantages include:

(a) Equal sensitivity throughout the entire length of the sensor.

(b) Terrain following on structure.

(c) Can tailor sensor application to fence to match structural changes; that is, corners, height, gage of fabric, curved, and so forth.

(d) Provide maximum information from the fence.

(e) Provides maximum protection against electromagnetic interference (EMI) and radio frequency interference (RFI).

(2) Limitations include:

(a) Fence must be maintained to eliminate nuisance alarms.

(b) The cable must be applied to fence fabric to avoid inadvertent damage.

(c) Area around the fence must be maintained to keep vegetation and debris from impacting the fence.

(d) Requires maintenance of a larger bending radius than strain-sensitive cable.

(e) Splicing and terminating fiber optic cable is more difficult.

(f) If cable is not protected in cold climates, micro-cracking can occur.

(g) More expensive than coaxial cable.

7.2.3.5 Time domain reflectometer sensors utilize either a single-wire sensor or a looped wire sensor. The signal generator sends a pulse down the line similar to a radar pulse. The processor measures the energy reflected from a disturbance in the line that causes the pulsed energy to reflect (or return) rather than continue forward. The location of the disturbance is measured based on amplitude of returned signal and the time calculated for the return. This calculation gives the location of the disturbance. Most common application is cable mounted on chainlink fence.

(1) Advantages include:

(a) Ability to pinpoint disturbance to within 10 ft.

(b) Allows zones to be changed easily.

(c) Sensitivity can easily be set for each fence panel.

(d) Terrain following on structure.

(2) Limitations include:

(a) Fence must be maintained to eliminate nuisance alarms.

(b) No audio assessment capability.

(c) Sensor cable must be continuous—difficult to splice or make break for gates, and so forth.

(d) Microprocessor outdoors on fence must be protected from EMI/RFI interference.

(e) The cable must be applied to fence fabric to avoid inadvertent damage.

(f) Area around the fence must be maintained to keep vegetation and debris from impacting the fence.

7.2.4 A taut-wire sensor fence primarily consists of a dense “screen” of horizontal wires connected to a central detector post assembly and securely anchored at each end. The horizontal wires are tensioned upon installation, then attached to the sensor. Mechanical action taken against one or several of the tensioned wires, such as climbing or cutting through the fence, will generate an alarm condition.

7.2.4.1 Advantages include:

(1) Low-nuisance alarm rate.

(2) High probability of detection.

(3) Terrain following capability.

7.2.4.2 Limitations include:

(1) Requires substantial structure.

(2) Cost.

(3) Heavy maintenance requirements.

7.3 *Intercom and Paging Systems*—An intercom and paging system is utilized to provide voice communication between two or more locations. This section does not take into consideration the varying effects that the acoustics of the building can have on the equipment.

7.3.1 *Types of Systems*

7.3.1.1 *Intercom Systems:*

(1) *Single Master*—A single location where all peripheral devices are connected which originates and receives all calls.

(a) Advantages:

(1) Single location for maintenance.

(2) Simple to operate.

(b) Limitations:

(1) Incoming calls cannot transfer to another location during busy, nonresponsive or disabled master stations, or both.

(2) *Multiple Master*—Multiple master stations that are connected to their respective peripheral devices and each other.

(a) Advantages:

(1) Incoming calls can transfer to other master stations.

(2) Peripherals can be annunciated/controlled from multiple locations.

(3) One of the multiple stations can possibly mimic the functions of another station during the time that the designated master is inoperable.

(b) Limitations:

(1) Troubleshooting (maintenance on more than one station).

(2) Increased overall system cost.

(3) Station-to-Station—Two intercom devices that are directly connected together (that is, two-station intercoms, visitation telephones, and so forth).

7.3.1.2 *Paging Systems:*

(1) *Local/Zoned*—Paging into a selected area defined by the system operator or system configuration (that is, wiring scheme, or both).

(a) Advantages:

(1) Defined areas where page is directed.

(b) Limitations:

(1) Cannot distribute voice material to all areas connected to the system simultaneously.

(2) *Facility Wide*—Paging into all areas utilizing all peripheral devices connected to the system.

(a) Advantages:

(1) One-step system activation to allow material to be broadcast to all locations.

(b) Limitations:

(1) Cannot single out particular areas where the paging message is not required.

(2) Increased amplification is required.

7.3.2 *Audio Threshold*—This section addresses the two most common types of audio threshold technology. These technologies can apply to both stand-alone systems and systems that can add the technology as a feature. The purpose of this system is to annunciate an alarm when the audio level has risen above a preset value. Detection is subject to the quality of the audio environment. Setup of some audio threshold systems may be complicated, or require frequent adjustments, or both. Audio threshold systems typically are utilized in areas that require intense monitoring (for example, mental health).

7.3.2.1 *Type 1*—Continuous monitoring technology.

(1) Advantages:

(a) Calibrated to the acoustic characteristics of the monitored space.

(2) Limitations:

(a) More costly than Type 2.

7.3.2.2 *Type 2* —Scanning technology.

(1) Advantages:

(a) Lower cost than Type 1.

(2) Limitations:

(a) Missed short-term events.

(b) Single point of failure.

7.3.3 *Field Devices*—Field devices should be selected with consideration to operational requirements, environmental conditions, and local/national codes and standards.

7.3.3.1 Cone speaker type intercom station.

7.3.3.2 Folded horn type intercom station.

7.3.3.3 Call-in pushbutton station.

7.3.3.4 Combination audio and pushbutton station.

7.3.3.5 Baffles:

(1) Security.

(2) Environmental.

(3) Non-Security.

7.3.3.6 Paging speaker.

7.3.3.7 Paging horn.

7.3.3.8 Two-way talkback speaker.

7.3.3.9 Keyswitch intercom station.

7.3.3.10 Headset.

7.3.3.11 Handset.

7.3.3.12 Volume controls.

7.3.3.13 Microphones

7.4 *Video Devices*—A video system is utilized to augment operations for assessment, surveillance, and documentation/recording. This section is not intended to be fully comprehensive; the video equipment is a rapidly changing technology and therefore, consideration should be given to new technology not covered in this guide.

7.4.1 *Cameras/Lenses*

7.4.1.1 *Cameras:*

(1) *Color*

(a) Advantages:

(1) Greater information density (for example, is helpful when the facility utilizes color-keyed uniforms).

(b) Limitations:

(1) Decreased performance at low light levels.

(2) Increased cost.

(2) *Black and White*

(a) Advantages:

(1) Increased low-level light performance.

(2) Infrared capability is inherent.

(3) Lower cost.

(b) Limitations:

(1) Difficulty with color-keyed uniforms (distinction).

(3) *Dual Technology (Color and Black and White (B/W))*

(a) Advantages:

(1) Ability to switch between color and B/W to reduce the limitations in viewing the subject material at various conditions.

(b) Limitations:

(1) Increased cost.

7.4.1.2 *Infrared:*

(1) Advantages:

(a) No visible illumination required.

(b) Mobility.

(2) Limitations:

(a) Increased cost.

(b) The environmental conditions (for example, rain, fog, and so forth) can drastically affect the performance.

7.4.1.3 *Low-Light:*

(1) Advantages:

(a) Operates well in low-light conditions.

(2) Limitations:

(a) Increased cost.

(b) Lower resolution.

(c) Monochrome only.

(d) Low tolerance to bright light conditions or artificial light focused directly at unit.

7.4.1.4 *Lenses*—Caution should be exercised to ensure that the lenses are compatible with the format of the camera to achieve the desired field of view and level of detail for the targeted object.

(1) Iris control.

