Designation: F 1465 – 03

Standard Guide for Selection of Security Control Systems[1]

This standard is issued under the fixed designation F 1465; 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:*

F 1577 Test Methods for Detention Locks for Swinging Doors[2]

2.2 *International Electrotechnical Commission:*

IEC 1131 Part 3—Programming Languages[3]

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.

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).

---

[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 F 1465 – 99.

[2] *Annual Book of ASTM Standards*, Vol 15.07.

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

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 so forth.

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.

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.

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
- a. What operational philosophy will be followed?
  - i. Direct supervision
  - ii. Indirect supervision
- b. What staffing restrictions will be confronted?
  - i. Due to size of staff
  - ii. Due to location of facility
  - iii. Due to education and training
  - iv. Due to current pay scales
- c. What environmental limitations will be confronted?
  - i. Due to terrain
  - ii. Due to weather
- d. Building design and layout?
  - i. Centralized or decentralized control
  - ii. Podular or linear arrangement of cells
  - iii. Single building or campus arrangement
  - iv. 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

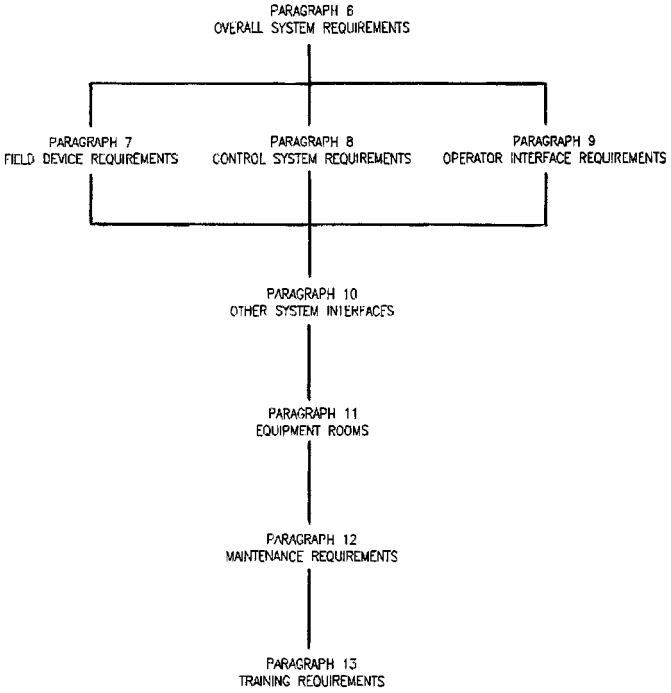

FIG. 2 Flow Chart of Document Sequence and Organization

5.5 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 Subsytem 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 F 1577.

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 sensored 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 to be mounted high.

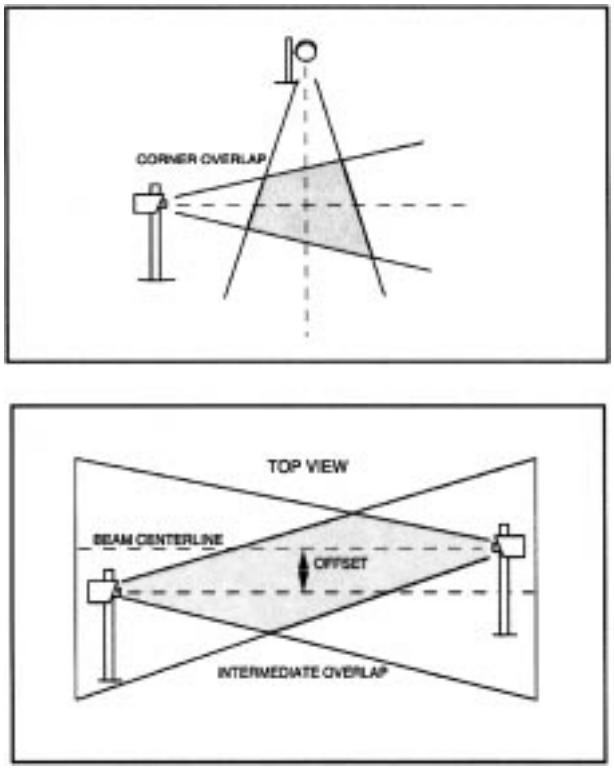

FIG. 3

(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, microcracking 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.

(2) Fixed.
(3) Manual.
(4) Automatic.
7.4.1.5 *Zoom Lenses*:
(1) Manual—Not typically utilized in a correctional facility.
(2) Motorized:
(a) Advantages:
(1) Ability to increase/decrease the focal point on an object within the parameters of the lens.
(2) Remote adjustment of the lens.
(b) Limitations:
(1) May not be currently set at desired viewing preference.
(2) Increased operator complexity.
(3) Increased cost.
(4) Increased maintenance complexity.
7.4.1.6 *Filters*:
(1) Light level filters.
(2) UV cut filters (skylight).
(3) Lens speed.
7.4.2 *Enclosures*
7.4.2.1 *Security*:
(1) Advantages:
(a) Resistant to vandalism/tampering.
(2) Limitations:
(a) Increased cost.
(b) Structural impact (for example, weight of enclosure and mounting requirements).
(c) Restrictive housing selection.
7.4.2.2 *Fixed*:
(1) Advantages:
(a) Lower cost per camera.
(b) Always directed at target.
(c) Reduced operator complexity.
(2) Limitations:
(a) Cannot be positioned at a different target remotely.
7.4.2.3 *Movable*:
(1) Advantages:
(a) Ability to cover a larger area with less equipment.
(2) Limitations:
(a) Higher cost per camera.
(b) Increased maintenance complexity.
(c) May not be positioned at desired target area.
7.4.2.4 *Indoor*:
(1) Ceiling (surface/recessed)
(a) Advantages:
(1) Does not allow for inmates to utilize the housing as a means to hang rope or other materials from unit.
(b) Limitations:
(1) Requires ceiling system coordination (for example, acoustical, security metal).
(2) Does not allow for environmental conditions (for example, heater/blower and exterior environments).
7.4.2.5 *Corner/Wall*.
7.4.2.6 *Covert*:
(1) Advantages:
(a) Reduced ability for subjects to detect the camera's presence.
(2) Limitations:
(a) Increased cost.
(b) Does not promote active viewing detectable by subjects (for example, subjects are not conscious of being viewed).
7.4.2.7 *Track*:
(1) Advantages:
(a) Ability to cover a larger area with less equipment.
(2) Limitations:
(a) Increased operator complexity.
(b) Increased maintenance complexity.
(c) Limited number of suppliers.
7.4.2.8 *Outdoor*—Outdoor enclosures and associated equipment have a greater potential for receiving a lightning/surge input.
(1) Building corner/wall/parapet.
(2) Pole mounted.
(3) Pedestal.
7.4.3 *Monitors*:
7.4.3.1 Color/B & W will match cameras and resolution (compatibility issue).
7.4.3.2 *Size*—The size of the monitor directly affects the size of the target in a particular setting (for example, the person is only ¼ in. tall on the monitor).
7.4.3.3 *Quantity*—The quantity of monitors can affect the space requirements of the control/viewing location and the overall ergonomics of this space.
7.4.3.4 Video on CRT (non-dedicated monitor).
7.4.3.5 *Environmental Impact (Heat, Space, Lighting, and so forth)*—Consideration should be given to the amount of heat generated by the monitors and the overall lighting conditions required to obtain the desired picture quality.
7.4.4 *Switching Systems*:
7.4.4.1 Manual/sequential.
7.4.4.2 Microprocessor.
7.4.5 *Storage/Retrieval Devices*:
7.4.5.1 VCR (video cassette recorder):
(1) Real time.
(2) Time-lapse.
7.4.5.2 Digital:
(1) Real time.
(2) Time-lapse.
7.4.5.3 Tape.
7.4.5.4 Disk:
(1) Floppy.
(2) DVD/CD.
(3) Hard disk.
7.4.5.5 Security:
(1) Searching.
(2) Ability.
(3) Storage media life expectancy.
(4) Storage capacity.
7.4.6 *Transmission Media*:
7.4.6.1 Hard copper.
7.4.6.2 Coaxial cable.
7.4.6.3 Twisted pair cable.

7.4.6.4 Category 5 cable:

(1) Data.

(2) Public lines.

(3) Modem.

7.4.6.5 Fiber-optic.

7.4.6.6 Microwave.

7.4.6.7 Infrared.

7.4.6.8 Radio frequency (RF).

7.5 As the name implies, all duress alarms report that a person is in a duress situation. This section discusses only dedicated duress alarm systems mounted in fixed locations or carried by the person to be protected. These are called duress alarms, panic alarms, body alarms, personal duress alarms, personal protection alarms, or personal alarm transmitters. Also discussed in this section are options that can be offered with many technologies. Maintenance and supervision capabilities are also presented. Not addressed here are duress signals that are functions or features of other systems. This latter category includes, but is not limited to: a special code on an access control keypad, a special code on a telephone or cell phone handset, and a telephone set being left off-hook (off-hook alarm).

7.5.1 *Duress Systems May Report*:

7.5.1.1 Name of the person in duress if the database is maintained.

7.5.1.2 Location of the person in duress.

7.5.1.3 Both the location and the identification of the person in duress if the database is maintained.

7.5.1.4 Previous one or more locations of the person prior to the duress alarm.

7.5.1.5 One or more updates of the location of the person subsequent to the duress alarm.

7.5.1.6 Continuous location updates, even when no duress alarm has been issued (tracking).

7.5.2 *Technologies*—There are a variety of technologies used to provide duress alarm protection to staff in corrections facilities. Major advantages and limitations of each major technology are summarized as follows. There are many variations and combinations of technologies offered by vendors. Additional technologies, and new implementations or new combinations of existing technologies might be available or might become available. It is important that the capabilities of a product are fully researched before specifying or purchasing it to ensure that the product meets the site's requirements. Trade-offs in design and functionality can result in significantly different performance from competing products using the same technology. Limitations of a specific technology may range from critical to irrelevant, depending on the requirements of the users. The following sections discuss the most frequently used technologies and combinations of technologies currently offered by vendors.

7.5.3 *Fixed Location Duress Alarms* are fixed devices that are typically attached to walls or located under office desks. The user activates the device to signal a duress situation. Communication between the device and annunciator is usually hard-wired, but some systems offer an RF (wireless) option for communications. Batteries may be required for RF solutions.

7.5.3.1 Advantages:

(1) Low hardware cost.

(2) Low maintenance cost.

(3) Simple, reliable technology.

(4) System reports exact location of a duress alarm.

(5) Does not require batteries (unless wireless communication is used).

7.5.3.2 Limitations:

(1) Does not report the identity of the person in duress (although this might be inferred if, for example, the alarm is at Mr. Smith's desk).

(2) The person in duress may be blocked from reaching the device.

(3) Less useful for mobile staff who might not be near the device, or might be prevented from reaching the device when a duress situation occurs.

(4) System performance is not generally supervised. Devices must be activated to test this part of the system.

(5) Devices must be installed in each room where protection is required. Wiring or RF links must be provided from each device. Wireless systems must provide batteries for each device.

(6) Alarms may be activated by unauthorized personnel.

7.5.4 *Ultrasonic*—The person to be protected wears an ultrasound transmitter with a device that is activated in the event of a duress situation. Ultrasound receivers are installed in each room or area where an alarm is to be reported. All receivers must communicate to a reporting system. When a duress alarm is activated, the transmitter emits an ultrasonic signal that is received and decoded by one or more receivers mounted in the facility. When the signal is recognized, the system signals an alarm to the reporting system. Some systems use one frequency. Others emit two signals of different frequencies to provide greater immunity to noise that might cause false alarms.

7.5.4.1 Advantages:

(1) Reports the location of an alarm.

(2) Ultrasound signals are not blocked by most clothing.

(3) Transmitters are not location specific.

7.5.4.2 Limitations:

(1) Does not report the ID of an alarm.

(2) Not suitable for larger outdoor areas.

(3) Receivers must be installed in each room where protection is required.

(4) Ultrasound signals can be blocked in some situations.

7.5.5 *Infrared*—The person to be protected wears an infrared transmitter with a device that is activated in the event of a duress situation. Infrared receivers are installed in each room or area where an alarm is to be reported. All receivers must communicate to a reporting system.

7.5.5.1 Advantages:

(1) Reports both ID and location of alarm.

(2) Some systems can provide continuous tracking of staff by automatically transmitting a signal at regular intervals.

7.5.5.2 Limitations:

(1) Infrared signals can be blocked by clothing or other objects and thus can prevent an alarm from being reported.

(2) Infrared alarm signals can be blocked by dense smoke.

(3) Not suitable for outdoor use in sunlight.

(4) Not suitable for use in large outdoor areas.

(5) Will not report an alarm in any closed room, closet, or other area not containing an installed receiver.

(6) Shorter range than some other technologies and may require multiple receiver installations for reliable coverage.

7.5.6 *Radio Frequency (RF)*—The person to be protected carries a RF transmitter (a dedicated unit or a two-way radio with a device that is activated in the event of a duress situation. A RF receiver is installed at a central location to receive alarms from all, or a large area, of the facility.

7.5.6.1 Advantages:

(1) The RF signal is very difficult to block.

(2) The system reports the ID of the alarm transmitter.

(3) Can be used in large outdoor areas.

(4) Only one, or very few, receivers required.

7.5.6.2 Limitations:

(1) Does not report location of alarm; location can be reported only by restricting the transmitter to a known location.

(2) Some "dead" spots may occur in facilities with large amounts of concrete or metal.

7.5.7 *Radio Frequency/RF Location Using Low-Power Transmitters and Limited Sensitivity Receivers*—The person to be protected carries a RF transmitter with a device that is activated in the event of a duress situation. A number of RF receivers are installed throughout the facility. The RF receivers are adjusted in sensitivity so that only one or very few receivers will receive a duress transmission. A location of the receiver that detects the duress transmission is reported by the control computer as the location of the alarm.

7.5.7.1 Advantages:

(1) The RF signals are difficult to block.

(2) Provides both ID and location of alarm.

(3) Can be used in large outdoor areas.

7.5.7.2 Limitations:

(1) Receivers may need to be located in areas occupied by inmates.

(2) Equipment must be installed in every area that will identify a separate location.

(3) Each installed piece of equipment must be hard-wired to the control computer.

(4) The RF obstacles in the vicinity can block transmissions of low-powered transmitters from receivers with low sensitivity.

(5) Metal in the vicinity can negatively impact location accuracy.

7.5.8 *Radio Frequency/RF Location Using High-Power Transmitters and High-Sensitivity Receivers*—The person to be protected wears a RF transmitter with a device that is activated in the event of a duress situation. A number of RF receivers are installed throughout the facility. Multiple RF receivers detect the duress transmission and report information about the transmission to the control computer. The control computer calculates the location of the transmitter.

7.5.8.1 Advantages:

(1) The RF signal is almost impossible to block.

(2) Provides both ID and location of duress alarm.

(3) Equipment is not located in areas accessible by inmates.

(4) Can be used in large outdoor areas.

7.5.8.2 Limitations:

(1) Not suitable for installations covering only a few rooms or small part of the facility.

(2) If major building construction occurs, the system may need to be recalibrated. Accuracy may be less in construction which does not use metal, concrete block, or other RF attenuating materials.

7.5.9 *Radio Frequency/IR Location with Installed IR Receivers*—The person to be protected carries a RF transmitter with a device that is activated in the event of a duress situation.

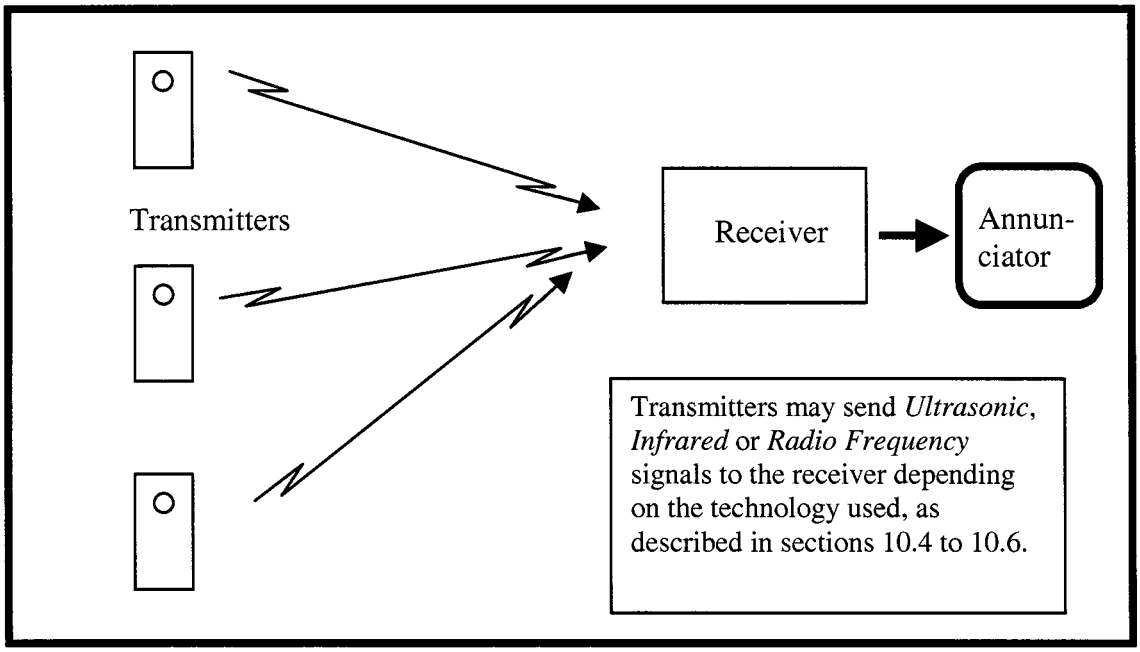

FIG. 4

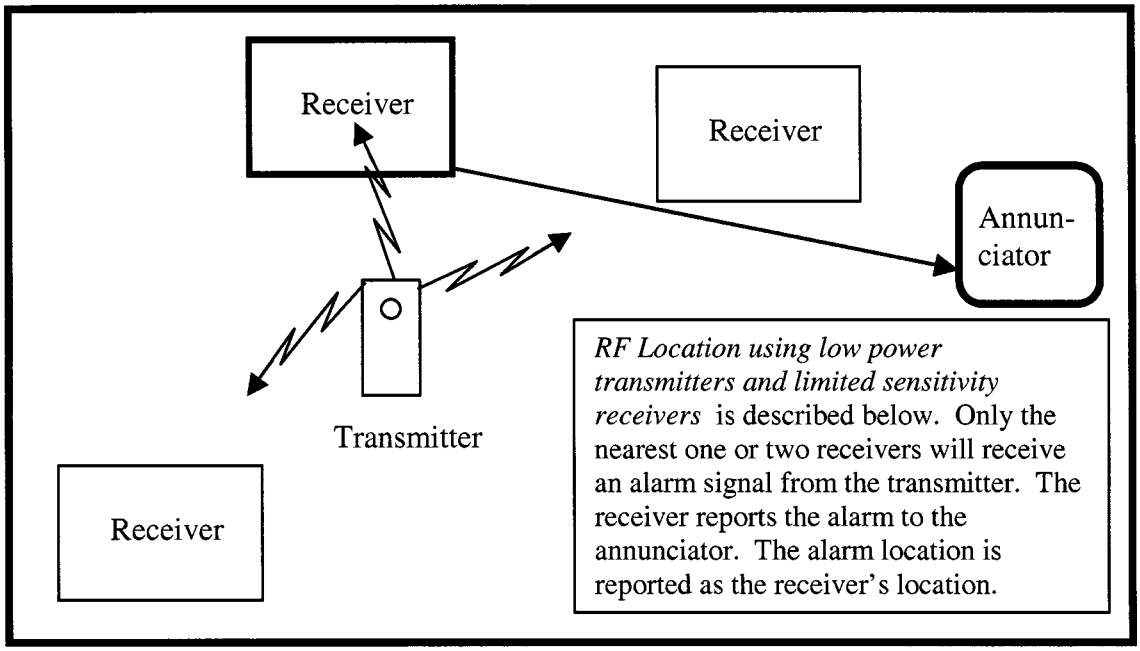

FIG. 5

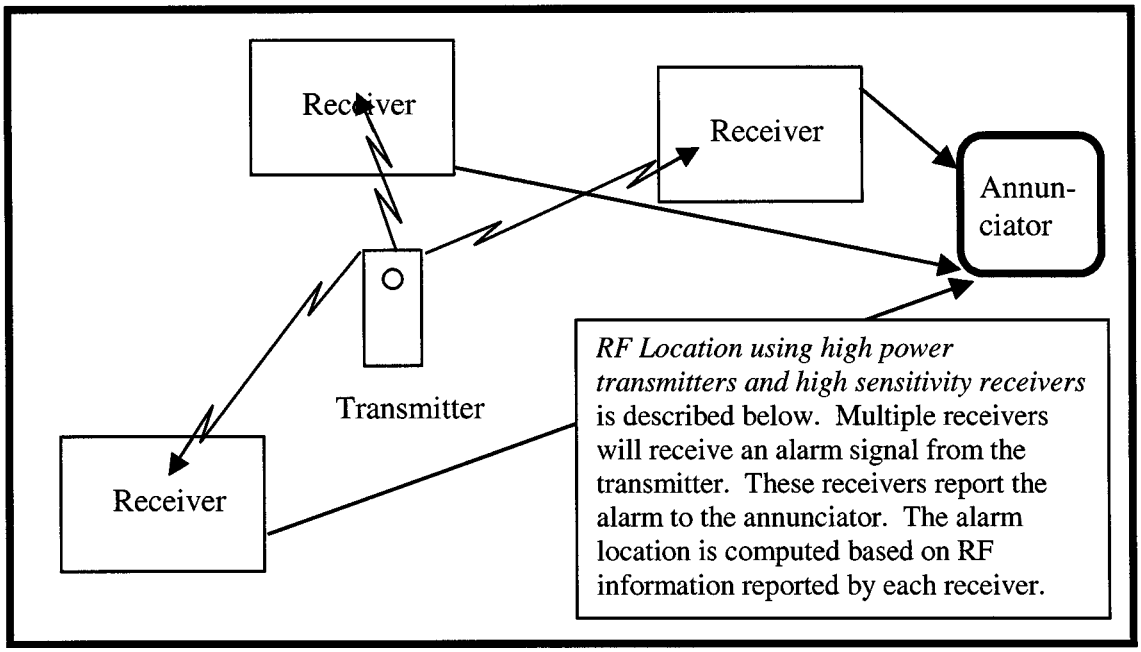

FIG. 6

The duress alarm also contains an IR transmitter. A number of RF receivers are installed throughout the facility. A number of IR receivers are also installed throughout the facility to locate the duress alarm. The IR receivers are usually co-located with the RF receivers. All RF and IR receivers must communicate to the control computer using installed wiring.

7.5.9.1 Advantages:

(1) Provides location and ID of duress alarm.

7.5.9.2 Limitations:

(1) The IR receivers can be blocked, location is not determined.

(2) Large rooms may require multiple receiver installations for reliable coverage.

(3) The IR receivers must be installed in every room where location is to be reported.

7.5.10 *Radio Frequency/IR Location with Installed IR Transmitters*—The person to be protected wears a RF transmitter with a device that is activated in the event of a duress situation. The duress transmitter also contains an IR receiver. A number of RF receivers are installed throughout the facility and are wired to the control computer to report a duress alarm transmission. A number of IR transmitters are installed

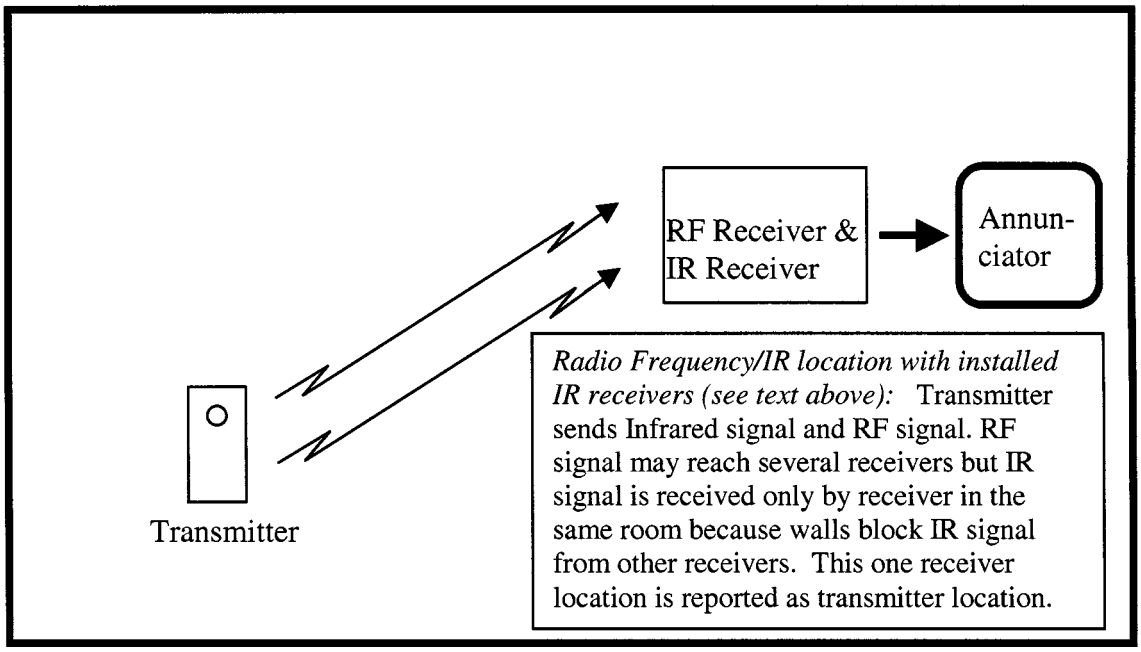

FIG. 7

throughout the facility to locate the duress alarm. The IR transmitters do not need to be wired to the control computer and are powered by battery or AC, depending on the product and vendor. The location of the duress transmitter may be identified when the transmitter enters a room (portal system) or it may be reported when the transmitter is anywhere in the room.

7.5.10.1 Advantages:

(1) Provides ID and location of the alarm.

(2) Continuous location of tags can provide tracking system for corrections officers and staff, as well as automatic testing of transmitters in some vendor's systems.

7.5.10.2 Limitations:

(1) The IR transmitters can be blocked, resulting in ID but not location being reported.

(2) Large rooms may require multiple IR transmitters.

(3) IR transmitters must be installed in every room requiring accurate location, including unsupervised areas.

(4) IR Transmitters are not supervised and failures may not be reported.

7.5.11 *Radio Frequency/Ultrasonic Location using Installed Ultrasonic Receivers*—The person to be protected wears a combination ultrasonic/RF transmitter with a device that is activated in the event of a duress situation. Ultrasonic receivers

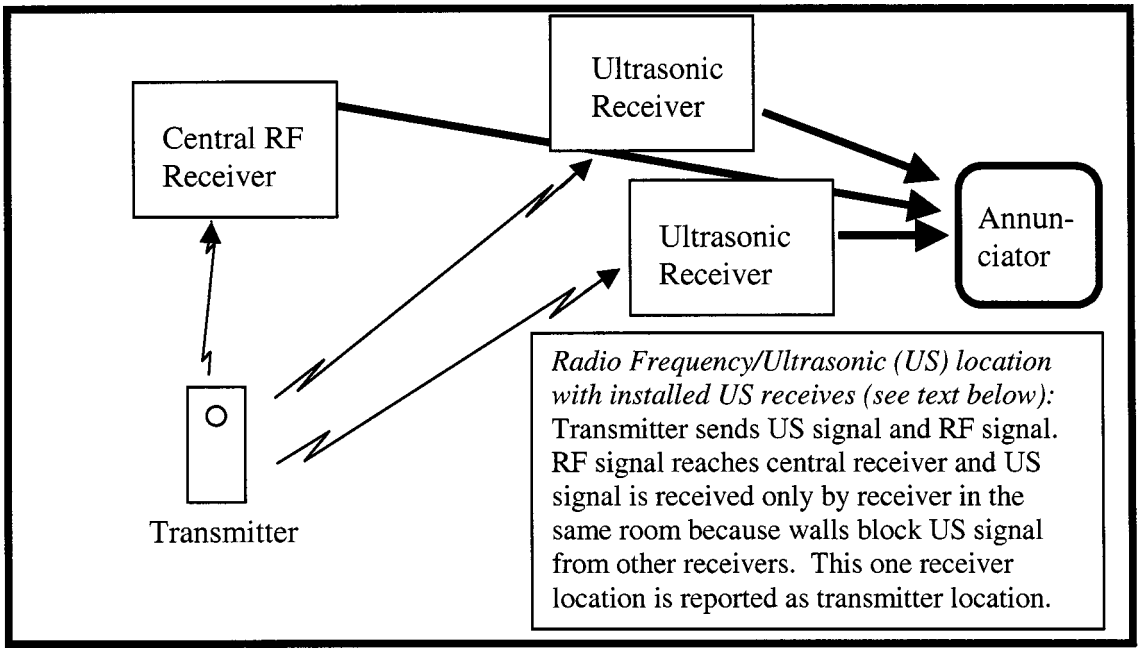

FIG. 8

are installed in each room or area where an alarm is to be reported. A RF receiver is installed at a central location to receive data from all or a large area of the facility. The ultrasonic receiver reports its location to the central control unit and the RF transmission reports the transmitter ID. The transmitter ID can be translated to the name of the person carrying that transmitter.

7.5.11.1 Advantages:

(1) Reports the identification of an alarm indoors and outdoors.

(2) Reports the identity of the person initiating the alarm.

(3) Ultrasonic signals are not blocked by most clothing.

(4) Transmitters need not be kept in one area of a facility.

7.5.11.2 Limitations:

(1) More complex than single technology system.

(2) More costly than single technology system.

(3) Repeaters may be required to prevent RF dead spots.

7.5.12 *Radio Frequency/RF Location with Installed RF Transmitters*—The person to be protected carries an RF transmitter that is activated in the event of a duress situation. The duress transmitter also contains an RF receiver. A number of RF receivers are installed throughout the facility and are wired to the control computer to report a duress alarm transmission. A number of RF transmitters are installed throughout the facility to locate the duress transmitter. The location of a duress transmitter is identified when the transmitter enters the room (portal system), but is reported to the control computer upon transmission of an alarm. The RF transmitters do not need to be wired to the control computer and are powered by battery or AC, depending on the product and vendor.

7.5.12.1 Advantages:

(1) Provides ID and location of the alarm.

(2) Continuous location of tags can provide tracking system for corrections officers and staff, as well as automatic testing of transmitters, in some vendor's systems.

7.5.12.2 Limitations:

(1) Rooms with multiple doors will require multiple RF transmitters.

(2) The RF transmitters must be installed in every room requiring accurate location, including inmate accessible areas.

(3) The RF transmitters are unsupervised and failures may not be reported.

7.5.13 *Options*—Each of the preceding technologies (except fixed location alarms) can have other features and options added:

7.5.14 *Man-down Switch*—Sometimes called a tilt switch. This feature causes an alarm to be reported automatically if the orientation of the alarm is such that it indicates the wearer has been prone for more than a few seconds.

7.5.14.1 Advantages:

(1) Provides a higher level of safety for staff that might be unable to sound an alarm while disabled or if unconscious.

7.5.14.2 Limitations:

(1) Prone to false alarms in some situations such as when the wearer sits down to rest or to use the toilet.

7.5.15 *Lanyard Pull*—Sometimes called grenade pin; this is a pin placed in a duress transmitter so that an alarm will be sounded automatically if the pin is removed. The pin usually is attached to the wearer's belt or clothing and removal of the pin occurs when an attempt is made to remove the duress alarm from the wearer.

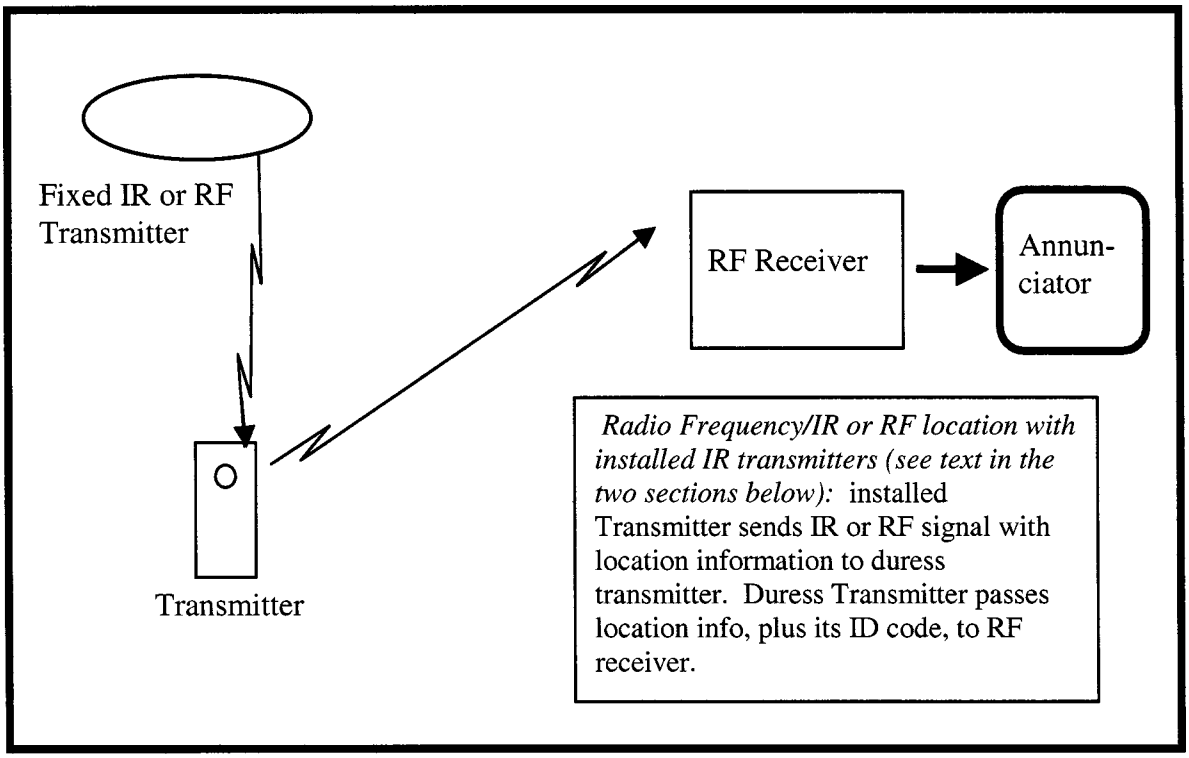

FIG. 9

7.5.15.1 Advantages:

(1) Causes an alarm if the duress transmitter is taken by an inmate.

7.5.15.2 Limitations:

(1) Prone to false alarms due to accidentally catching the cord holding the pin in some systems. Reliability of this switch type often deteriorates with extended use.

7.5.16 *Motion Switch*—The motion switch detects the absence of motion and sounds an alarm if the duress transmitter has not been moved for a predetermined number of seconds. The absence of motion is presumed to mean that the wearer is incapacitated or that the duress alarm has been removed from the corrections officer.

7.5.16.1 Advantages:

(1) Provides a higher level of protection for the wearer in high-risk situations.

7.5.16.2 Limitations:

(1) May be prone to false alarms when the wearer is not walking or moving.

(2) Installation Costs—Costs are associated with the installation of each piece of equipment, and the delivery of communications and power to each device. Reference has been made above to the amount of equipment required for each technology. Communications and power can be delivered by many different means. Constraints are different for new and retrofit situations. Cost advantages may be gained by sharing power or communications with other systems. Refer to Guide F 1465-98 for a discussion of communication technologies. Installation costs should be researched carefully when specifying a system. Two major factors affecting installation costs are:

(a) The number of receivers and other devices required: This number is a function of the alarm technology and has been noted for each of the technologies.

(b) The technology offered for power and communication between the receivers and the central reporting system. Some technologies require less or no installation wiring and offer the advantage of lower installation costs.

7.5.17 *Transmitter Test Station*—Many systems do not automatically test transmitters. Some of these systems offer a special device where transmitter functionality and battery status can be tested at the start of each shift.

7.5.18 *Automated Self-Test and Diagnostics*—Most computer- or microprocessor-based systems offer some form of self-test and diagnostics. Some systems are more comprehensive than others. It is important to learn about the capability of each system being considered.

7.5.19 *Reporting of Alarm Location Information*—There are at least four types of systems offered. Some systems may offer multiple options for alarm reporting. Options include:

7.5.19.1 A simple panel showing a text description of the alarm location. A fixed map of the facility, with a light at each point that corresponds to an alarm location.

7.5.19.2 A PC-based site map(s) of the facility, displaying the location and ID of the alarm.

7.5.19.3 A software communications link to other equipment, so that another installed control system, and not the vendor's system, will be used to report the alarm.

7.6 *Systems Nurse Call*

7.6.1 A nurse call system is provided in the medical area of a correctional facility to allow the inmates the ability to communicate between their location and the nursing station and consideration is made for the level of the inmates' mobility. Local and national codes and standards such as NFPA and UL should be considered.

7.6.2 *Types of Systems*:

7.6.2.1 *Audible/Visual*—A combination of an audible tone and visual indication serving as notification to staff.

(1) Advantages:

(a) Simplicity.

(b) Lower cost equipment installation.

(2) Limitations:

(a) One-way communication limits information.

(b) No exchange of information.

7.6.2.2 *Audio/Visual*—Same as audible/visual with the addition of two-way voice communications.

(1) Advantages:

(a) Two-way communication.

(b) Staff communication available.

(c) Provides audio monitoring.

(2) Limitations:

(a) Cost of equipment and installation may be higher than audible/visual system.

(b) Possible staff harassment through exchange of information.

7.6.3 *Implementation*—Stand-alone versus integrated (PLC-controlled or logic system controlled, or both).

7.6.3.1 *Stand-alone (Packaged)*—A complete system that is not interfaced to any other system in the facility.

(1) Advantages:

(a) Stand-alone system does not depend on other systems for basic operation.

(b) Code compliant stand-alone systems are readily available.

(c) Information delivered to multiple locations.

(d) Frequently more features available.

(2) Limitations:

(a) Additional system maintenance.

(b) Control room space limitations (space constraints).

(c) Operationally inefficient.

7.6.3.2 *Interfaced*—A stand-alone system that has secondary annunciation without control or audio capability, or both.

(1) Advantages:

(a) Same as stand-alone system.

(b) Shares information that allows automatic activation of other systems (that is, video call-up).

(2) Limitations:

(a) Same as stand-alone system.

7.6.3.3 *Integrated*—A configuration that shares common controls with other systems.

(1) Advantages:

(a) More flexible operation.

(b) Simplified maintenance.

(c) More efficient operation.

(d) Improved space utilization.

(2) Limitations:

(a) More difficult UL compliance.

(b) Single failure may affect more than one system.

(c) Custom software applications may be more difficult to support.

7.6.4 *Field Devices*—Field devices should be selected with consideration to operational requirements, environmental conditions, and local/national codes and standards. The following list, although not all-inclusive, is representative of the types of field devices used in correctional facilities.

7.6.4.1 Patient station.
7.6.4.2 Emergency station.
7.6.4.3 Corridor lamps.
7.6.4.4 Zone lamps.
7.6.4.5 Duress station.
7.6.4.6 Code blue station.
7.6.4.7 Duty station.
7.6.4.8 Nurse Locator.

7.7 *Utility Control Systems*—The following list, although not all-inclusive, is representative of the auxiliary control/annunciation items that are found in a correctional facility.

7.7.1 General alarm conditions.
7.7.2 Emergency generator set.
7.7.3 Frozen food alarm.
7.7.4 Primary power failure.
7.7.5 U.P.S.
7.7.6 Compressor failure (pneumatic locking systems only).
7.7.7 System fault.
7.7.8 Low air pressure (pneumatic locking systems only).
7.7.9 Dryer failure (pneumatic locking systems only).
7.7.10 Lighting:
7.7.10.1 Cells (individual and group).
7.7.10.2 Night light.
7.7.10.3 Dayroom lights.
7.7.10.4 Outdoor lighting.
7.7.11 Water.
7.7.12 Receptacles.
7.7.13 Inmate telephones.
7.7.14 Sprinklers.
7.7.15 HVAC.
7.7.16 Chemical agents.
7.7.17 Smoke control.
7.7.18 Television (MATV).
7.7.19 Pharmacy alarms.
7.7.20 Isolation pressure alarm.

7.8 *Access Control* is generally used by the staff in a correctional facility. It is primarily seen in nonsecure administration areas to aid the staff in gaining access to a particular area without having to contact a remote control station. The three most common types of systems are:

7.8.1 *Mechanical Lock and Key System*:
7.8.1.1 Advantages:
(1) Lower initial costs.
(2) Familiarity; everyone knows how to use.
(3) Ease of use.
7.8.1.2 Limitations:
(1) Frequently have higher total cost of ownership due to rekeying, maintenance, and operations of mechanical devices.
(2) Slow response to lost key.

7.8.2 *Keyless, Human Intervention, Access Control (Staffed Control Point)*:
7.8.2.1 Advantages:
(1) Presence of human observer provides impression of greater security.
(2) Ability to assess the conditions such as duress, contraband, and so forth.
7.8.2.2 Limitations:
(1) Human operator must recognize the person requesting access.
(2) Requires more staff.
(3) Data is not logged automatically.

7.8.3 *Automatic Keyless Access Control*—Keyless Access control is a detector device that is located near a locked door or gate which is connected to a microprocessor; when the correct "token of identity" is presented, access will be granted to that given locked door or gate. Table 1 shows the various type of "tokens of identity" used in the access control industry to date.
7.8.3.1 Advantages:
(1) This system allows for the passage of authorized persons only, not merely the passage of an authorized badge together with, hopefully, the authorized badge holder in possession of the badge.
(2) Less expensive than a conventional system because of the cost associated with issuing badges and keys.
7.8.3.2 Limitations:
(1) Requires more maintenance than the other two preceding systems.
(2) Typically requires backup power to allow for continued operation during normal power failure.

7.8.4 *Field Devices*—This portion is not intended to be fully comprehensive. The access control equipment is a rapidly changing technology, and therefore, consideration should be given to new technology not covered in this guide.
7.8.4.1 Keypad.
7.8.4.2 Scramble keypads.
7.8.4.3 Magnetic stripe cards/readers.
7.8.4.4 Weigand cards/readers.
7.8.4.5 Proximity cards/readers.
7.8.4.6 Multi-technology cards.
7.8.4.7 Smart cards.
7.8.4.8 Biometric readers.

7.9 *Watch Tour*—A means of recording that required inmate welfare checks have been performed and facility security checks with both time-based and risk-based issues. Watch tours may be performed on a scheduled or random basis. The American Correctional Association and American Jail Association makes recommendations, and most states have specific

TABLE 1

Token of Identity	Linkage
Access cards—insertion or proximity	access tied to badge and not holder
Access cards with code—insertion or proximity	access tied to badge and not holder (who knows the code)
Intelligent keys/tags	access tied to badge and not holder
Codes (keypad)	access tied to badge holder (who knows the code)
Biometrics	access tied to badge holder (who has the physical attributes)

regulations on inmates' welfare as it pertains to intervals. There are several methods used to provide a facility with a watch tour system.

7.9.1 *Technology*:

7.9.1.1 One means is to have the staff person manually write an affidavit that they did a tour at a particular time. A second means is to use a stand-alone system where fixed locations around facilities are visited by the staff person. A third means is to have the fixed locations connected to the security system.

7.9.2 *Watch Tour Input Services*:

7.9.2.1 Stand-alone systems use a portable lock which has a means of recording location-specific data with a time of action. The systems range from key imprint on a paper tape to electronic data recorded on some type of media.

(1) Advantages:

(a) No wiring, inexpensive, locations can be easily changed.

(b) Difficult to alter data.

(2) Limitations:

(a) Not integrated, requires separate data transfer, battery failure, report capabilities.

7.9.2.2 Integrated systems use electrically connected field devices to input actions directly to the security system.

7.9.2.3 *Wireless Device*:

(1) Advantages:

(a) Locations can be easily changed.

(b) Easily installed in existing facility.

(2) Limitations:

(a) Facility construction can interfere with signals.

(b) Battery failure.

7.9.2.4 *Hard-Wired Devices*:

(1) Push Buttons

(a) Advantages:

(1) Simple to use.

(2) Low cost per unit.

(b) Limitations:

(1) Not easily relocated.

(2) Inmate vandalism.

7.9.2.5 *Key Switches*:

(1) Advantages:

(a) May be integrated with door lock.

(b) May use same key as door hardware.

(c) Relatively secure station.

(2) Limitations:

(a) Not easily relocated.

(b) Key control.

(c) Inmate vandalism.

7.9.2.6 *Card Readers*:

(1) Advantages:

(a) Broadly available technology.

(b) Numerous coding options.

(c) Higher security level.

(d) Improved vandalism resistance.

(e) Card control is easier than key control.

(2) Limitations:

(a) Not easily relocated.

(b) Some technologies require higher maintenance.

(c) High replacement cost.

(d) Administrative enrollment time.

8. Establishing Requirements for Internal Systems Design

8.1 The technology used for the internal design of the system should be considered carefully (see Fig. 10). Significant factors include:

8.1.1 Size of the facility,

8.1.2 Project budget,

8.1.3 Availability of technology,

8.1.4 Maintainability,

8.1.5 Complexity of operational functions desired,

8.1.6 Incorporated sub-systems,

8.1.7 Cost benefit and payback, and

8.1.8 Record keeping needs.

8.2 All of the technologies listed as follows have advantages and limitations that depend on the nature of the facility.

8.2.1 *Hard Wire Advantages Include*:

8.2.1.1 For small systems, it can be a simple design.

8.2.1.2 Requires minimal technical maintenance skills.

8.2.1.3 Few environmental restraints on installation.

8.2.2 *Hard Wire Limitations Include*:

8.2.2.1 Lack of flexibility prevents the implementation of logic functions.

8.2.2.2 Future expansion can be difficult, expensive, or impractical, or a combination thereof.

8.2.2.3 For medium to large systems, the design may become cumbersome.

8.2.2.4 Difficult to implement redundant control.

8.2.2.5 As size increases, cost effectiveness decreases with respect to some other technologies.

8.2.3 *Relay Logic Advantages Include*:

8.2.3.1 For small systems, it can be a simple design.

8.2.3.2 Requires minimal technical maintenance skills.

8.2.3.3 Few environmental restraints on installation.

8.2.3.4 Permits the implementation of simple logic functions.

8.2.3.5 Allows implementation of redundant control.

8.2.4 *Relay Logic Limitations Include*:

8.2.4.1 Future expansion can be difficult, expensive, or impractical, or a combination thereof.

8.2.4.2 For medium to large systems the design may become cumbersome.

8.2.4.3 Size or complexity, or both, increases maintenance requirements.

8.2.4.4 As complexity increases, cost effectiveness decreases with respect to other technologies.

8.2.5 *Discrete Logic Advantages Include*:

8.2.5.1 For small systems it can be a very simple design, allowing logic functions to be implemented.

8.2.5.2 Modular repair instead of component repair that requires minimal technical skills.

8.2.5.3 Modular design makes expansion easier than for hard wire systems.

8.2.5.4 Few environmental restraints on installation.

8.2.6 *Discrete Logic Limitations Include*:

8.2.6.1 Logic functions are limited compared to programmable controls.

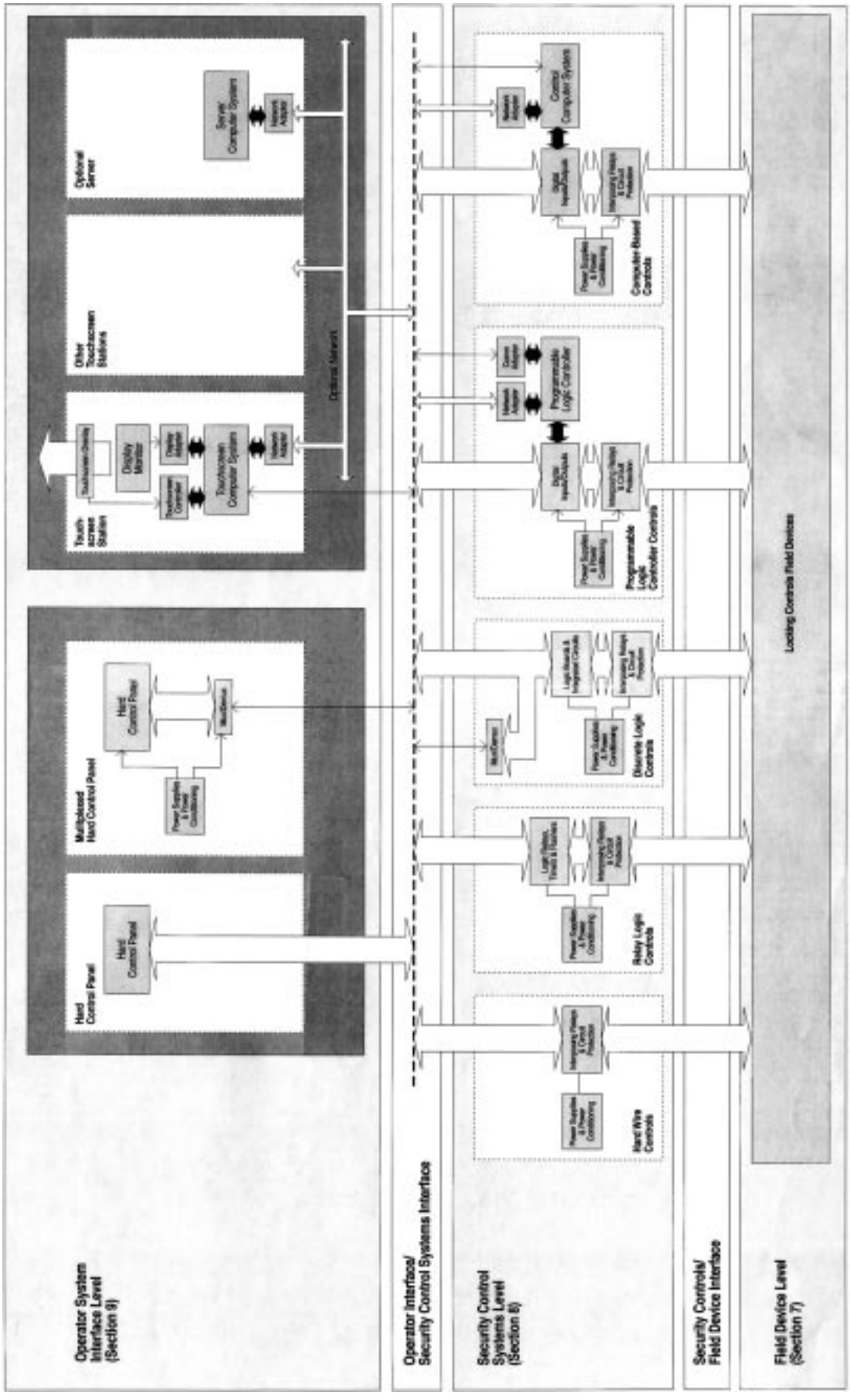

FIG. 10 Overview Diagram—System Interrelationships and Technology Options

8.2.6.2 For medium to large systems the design becomes cumbersome.

8.2.6.3 Limited ability to implement self diagnostics.

8.2.6.4 As complexity increases, cost effectiveness decreases.

8.2.7 *Programmable Controller Advantages Include*:

8.2.7.1 Based on technology that has been proven in critical industrial applications for many years.

8.2.7.2 Capable of revision of logic programs.

8.2.7.3 Incorporates transparent hardware checks prior to executing operations.

8.2.7.4 Capable of functioning with any of the operator interface (OI) technologies identified in this guide.

8.2.7.5 Cost increase is not in proportion to the increase in complexity.

8.2.8 *Programmable Controller Limitations Include*:

8.2.8.1 Requires a higher level of technical skills to modify, or upgrade.

8.2.8.2 Has limited fault tolerance.

8.2.8.3 Use of continuous power is recommended.

8.2.8.4 Requires environmentally controlled space.

8.2.8.5 May require relay interface due to low current carrying capabilities of output modules.

8.2.9 *Proprietary Programmable Controller Advantages Include*:

8.2.9.1 Can be more economical when applied to complex systems.

8.2.9.2 Capable of functioning with any of the operator interface (OI) technologies identified in this guide.

8.2.10 *Proprietary Programmable Controller Limitations Include*:

8.2.10.1 Requires a higher level of technical skills to modify, or upgrade.

8.2.10.2 Availability of replacement parts.

8.2.10.3 Proprietary nature of software.

8.2.10.4 Limited fault tolerance.

8.2.10.5 Use of continuous power is recommended.

8.2.10.6 Requires environmentally controlled space.

8.2.10.7 May be difficult to document reliability claims.

8.2.10.8 May require relay interface due to low-current carrying capabilities of output modules.

8.2.10.9 A method of AUTO-RESET is recommended in the event of any type of non-programmed interruption.

8.2.11 *Computer Based*—A software-based system where the logic is resident in a central computer. Advantages include:

8.2.11.1 An apparent low initial cost.

8.2.11.2 Ability to incorporate software written for related applications.

8.2.11.3 System can be programmed to implement considerable self diagnostic procedures.

8.2.12 *Computer-Based System Limitations Include*:

8.2.12.1 Difficult and time consuming to bring online.

8.2.12.2 Custom software development costs.

8.2.12.3 Response time can be slow because of central processing.

8.2.12.4 Does not do hardware checks prior to executing operations.

8.2.12.5 Difficult to document reliability claims.

8.2.12.6 Requires much higher technical skills to modify or upgrade.

8.2.12.7 Requires much higher technical skills for maintenance.

8.2.12.8 Limited fault tolerance.

8.2.12.9 Environmental conditions of installation.

8.2.12.10 A method of AUTO-RESET is recommended in the event of any type of non-programmed interruption.

8.2.13 *Hybrid Systems*—There are applications where a combination of two or more of these technologies into a single system may be advantageous.

8.3 *Signal Conversion*:

8.3.1 Method by which changes in the condition of monitored devices is converted to an operator display based upon a predetermined set of rules.

8.3.2 Method by which the condition of controlled devices are changed by operator actions, based upon a predetermined set of rules.

8.4 *Logic*:

8.4.1 The set of rules that determines what action(s) results from information received.

8.4.2 Methods of implementing logic include:

8.4.2.1 *Firmware*—Implementation that is determined by the physical interconnection of components, such as relays.

8.4.2.2 *Software*—Implementations that are determined by binary data stored in memory and executed by systems, such as programmable controllers, microprocessors, and microcomputers.

8.5 *Signal Transmission*:

8.5.1 Signal transmission is sending a message from point A to point B.

8.5.2 The first selection is to determine whether the transmission is discrete or multiplexed.

8.5.3 It is necessary to consider the media that is to be used for the signal transmission.

8.5.3.1 Twisted pair(s) of wire.

8.5.3.2 Coaxial cable.

8.5.3.3 Fiber optic link.

8.5.3.4 Radio link.

8.5.4 Consideration should be given to supervision of transmission circuits against tampering. Supervision should be consistent with the type of circuit and the consequences of a circuit failure. Some examples where line supervision may be desirable include:

8.5.4.1 Door and lock status switches through security/perimeter barriers.

8.5.4.2 Systems monitoring the outside perimeter.

8.5.4.3 Systems related to personal safety.

8.5.5 Transmission circuits carrying serial data should be supervised to confirm that data is being transferred between the desired points. Some examples of data supervision methods include:

8.5.5.1 *Redundant Path*—Transmission of the same data over multiple channels and verification that the received signals are the same.

8.5.5.2 *Redundant Transmission*—Transmission of the same data multiple times over a single channel followed by verification that the received signals are the same.

8.5.5.3 *Handshaking*—Verification that the line is clear prior to sending data, followed by verification that data has been received.

8.5.5.4 Some of the means available for ensuring data integrity include parity checking, check-sum, and cyclical redundancy checking.

8.6 The choice of architecture for each facility requires knowledge of the facility's unique operational features, as well as consideration of the desired performance, reliability and cost. Appropriate solutions also include hybrid systems of two or more intermixed architectures. Each of these alternative architectures is described and discussed in the following paragraphs. Video control system architectures include:

8.6.1 *Stand–Alone Systems*—Stand–alone system architectures include systems with only one video control station, and systems with multiple video control stations that are unconnected to one another. A stand–alone system architecture may be chosen with multiple video control stations if:

8.6.1.1 The video control stations operate with complete independence from one another, and

8.6.1.2 No control hierarchy or other requirement for communications exists between video control stations.

8.6.1.3 Fig. 11 illustrates a stand–alone system with two video control stations.

8.6.1.4 The primary advantage to stand–alone systems is simplicity. In addition, stand–alone systems can be a direct replacement to existing hard control panels in systems where the security control system interface is compatible.

8.6.1.5 The limitations of stand–alone systems include their inability to support advanced control functions involving more than one video control station, and potential for catastrophic system failure due to a lack of redundancy.

8.6.2 *Networked Peer Systems*—Peer systems are interconnected over a particular type of network that allows each video control station to communicate with every other video control station on the network as its peer.

8.6.2.1 Fig. 12 illustrates a peer system with two networked video control stations.

8.6.2.2 Peer systems provide improved reliability to stand–alone systems in that video control stations remain functional despite the failure of other peers. The primary advantage peer systems provide over stand–alone systems is the ability for multiple video control stations to share more advanced control and monitoring functions. Examples of such functions include:

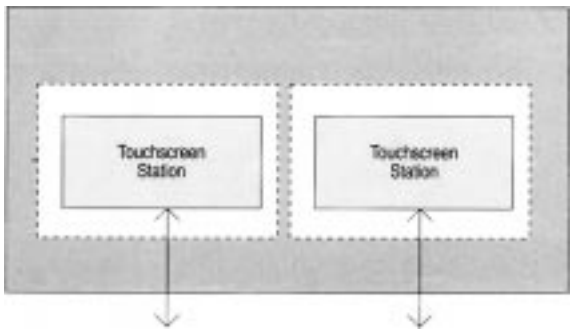

FIG. 11 Stand-Alone System Architecture

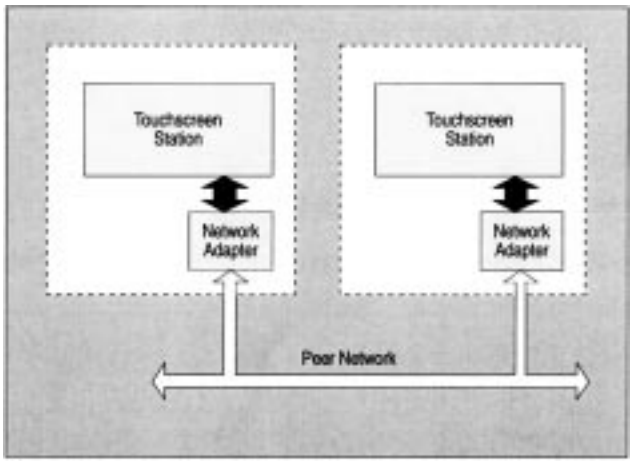

FIG. 12 Networked Peer System Architecture

(1) Work sharing between video control stations,

(2) Control hierarchies,

(3) Control transfers and overrides,

(4) Centralized alarm reporting and logging, and

(5) Centralized troubleshooting, and software modifying and upgrading across the network.

8.6.2.3 All network-based systems have the disadvantage of dependency on the network for system-wide and multiple-station functions. Methods to improve network reliability and fault tolerance include:

(1) Self-diagnostic and/or self-healing networks, or both,

(2) Distributed processing architectures,

(3) Non-proprietary, standards-based ("open") architectures,

(4) Uninterruptible power supplies,

(5) Technician network certification, and

(6) Installation utilizing rated cabling and surge protection in compliance with industry standards and codes.

8.6.2.4 The specific limitations of peer systems (when compared to other network architectures) in systems with many video control stations and advanced control functions include the potential for reduced performance and reliability due to:

(1) Preempting local video display functions with status reporting, data logging, file transfers or other system-wide functions,

(2) Lost or hung-up communications during reboots, or

(3) Incompatible multiple file versions throughout the network.

8.6.3 *Networked Central Server Systems*—Central server systems incorporate a dedicated server computer to provide video control station clients with system-wide services across the network. Central server architectures permit the same function sharing as peer systems, but may improve performance and reliability, especially in systems with numerous video control stations.

8.6.3.1 Fig. 13 illustrates networked central server architecture.

8.6.3.2 In comparison to peer systems, central server advantages include:

(1) Improved configuration control of software modifications and upgrades,

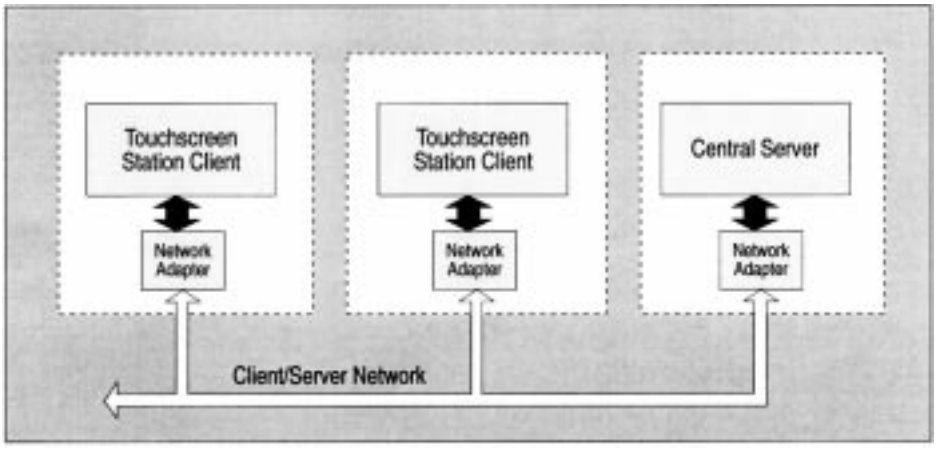

FIG. 13 Networked Central Server System Architecture

(2) Easier implementation of advanced control functions, and

(3) Enhanced diagnostic and troubleshooting tools.

8.6.3.3 The primary limitation of central server systems is their dependency on the central server computer for all system-wide functions (that is, single point of failure). Methods to improve server system reliability and fault tolerance include fault-tolerant or redundant servers, uninterruptible power supplies, and server rated equipment.

8.6.4 *Networked Distributed Processing Systems*—Like central server systems, distributed server systems use servers, networks and client/server software to off-load system-wide services from the video control stations. However, as implied by their name, these systems distribute system-wide functions across multiple servers, each one forming an independent "site" that remains operational despite the failure of other server sites.

8.6.4.1 Fig. 14 illustrates a two-site networked distributed server system architecture.

8.6.4.2 In comparison to central server systems, the advantages of a distributed server system is its enhanced reliability and an improved ability to optimize system-wide performance.

8.6.4.3 Like peer systems, a limitation of distributed server systems is the potential for conflicts from multiple file versions or conflicting data on different servers. This places a greater burden on configuration control with distributed server systems.

8.7 *Minimum Video Control System Hardware*:

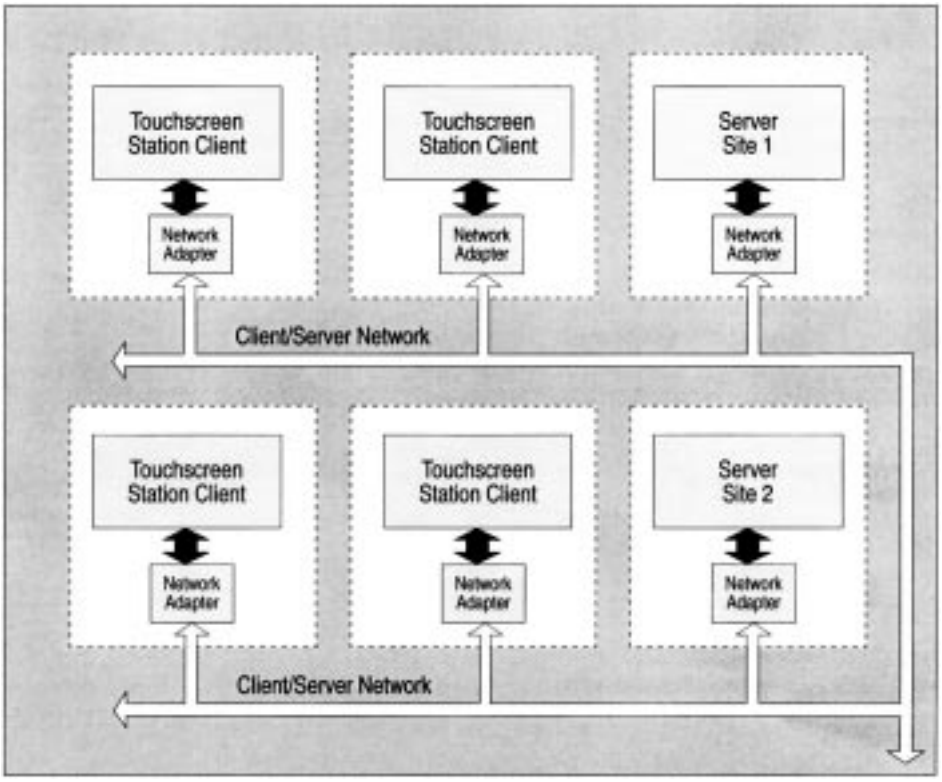

FIG. 14 Networked Distributed Processing System Architecture

8.7.1 A single-station, stand–alone video control system represents the minimum system hardware necessary for a video display operator interface. Fig. 15 illustrates an individual video control station, which is comprised of the following component parts:

8.7.1.1 *Display Monitor and Adapter*—High-resolution color video displays are the most visible component of the video control station. They interconnect to the computer systems input/output bus or local bus through a display adapter. Display monitor types include: cathode-ray tube (CRT) type, and flat panel type.

(1) Flat panel displays should be considered in special situations, such as consoles with restricted mounting depth or small, localized video control stations. Display area at time of this publication is a major limitation.

(2) Total screen size is limited by the display area available on each given display monitor and is typically somewhat smaller than the overall monitor size. For example, a 483-mm (19-in.) CRT type monitor has a display area of approximately 345 mm (13.6 in.) by 274 mm (10.8 in.).

8.7.1.2 The video graphic function can be an integral part of the motherboard or a separate plug-in card.

(1) The advantages of an integral style system (on-board) are probably cost and space.

(2) The disadvantages of an integral style system are single component failure requires motherboard replacement; and the inability to upgrade graphics performance.

(3) The advantages of separate plug-in cards are the upgrade flexibility for increased performance; and replacement of the graphic card without replacing the motherboard.

(4) The disadvantages of separate plug-in cards are cost, technical compatibility issues, and space.

8.7.1.3 *Touchscreen Overlay or Pointing Device and Controller*:

(1) For touchscreen pointing devices a transparent overlay is mounted on the face of the display monitor. The overlay both transmits light from the monitor and senses the point on a grid at which "stylus" (that is, finger) touches the screen. The most commonly used touchscreen overlay types for security control include: surface acoustic wave, analog capacitive, infrared, and analog resistive.

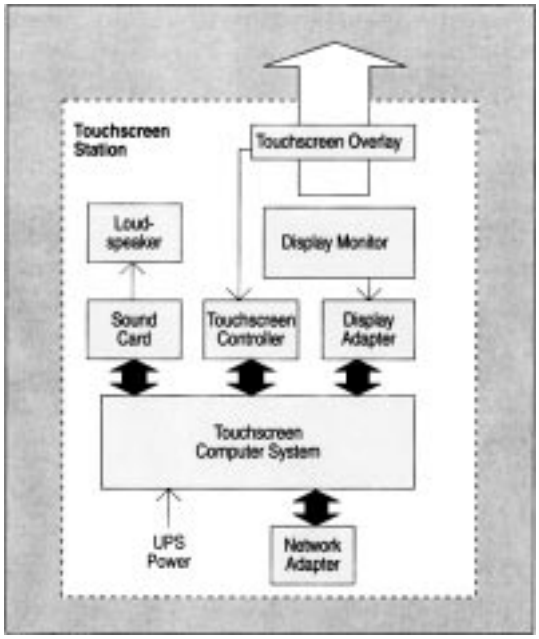

FIG. 15 Touchscreen Station Hardware

(2) Choice of overlay type involves consideration of its light transmission characteristics, touch resolution, calibration drift, price, speed, durability, resistance to vandalism, and suitability using a finger as the stylus.

8.7.1.4 Other common pointing devices (stylus) include: mouse, trackball, and touchpad.

8.7.1.5 These pointing devices are used to move a cursor around on the screen. Selection of an activation point is made by depressing one or more adjacent buttons, rather than by directly touching the screen.

8.7.1.6 As activation points are selected by the pointing device, the controller processes the raw sensor information into *X-Y* coordinates needed by the operator interface software. Assuming that the location then corresponds with an icon or similar valid selection, the software acts upon this input signal. Pointing device controller types include:

(1) External or internal serial controllers that interface to one of the computer systems serial communication ports.

(2) Internal bus controllers that interface directly with the computer systems input/output bus and mount inside the computer itself.

8.7.1.7 *Sound Card and Loudspeaker*—Together, sound cards and loudspeakers provide advanced audible annunciation through the capability to reproduce speech and a wide range of audible tones. Like display adapters and bus controllers, sound cards also interface to the computers input/output bus. The sound function can be an integral part of the motherboard or a separate plug-in card.

(1) The advantages of an integral style system (on-board) are probably cost and space.

(2) The disadvantages of a integral style system are single component failure requires motherboard replacement; and the inability to upgrade audio performance.

(3) The advantages of separate plug-in cards are the upgrade flexibility for increased performance; and replacement of the audio card without replacing the motherboard.

(4) The disadvantages of separate plug-in cards are cost, technical compatibility issues; and space.

8.7.1.8 *Computer System*—The computer system is either a personal computer or an industrial computer. While more expensive than personal computers, industrial computers locate the processor and other active components on a single board that plugs into a "passive backplane," rather than on a large "motherboard" that is more cumbersome to replace. Other advantages of industrial computers in comparison to personal computers include:

(1) Ease of mounting in standard equipment racks.

(2) Ability to withstand wider environmental extremes.

(3) Protection from dust infiltration and accumulation.

(4) Improved protection from electrical interference and vibration.

8.7.1.9 Both personal computer and industrial computer systems consist of the following components:

(1) Processor and related components,

(2) Memory,

(3) Hard disk drive,

(4) Keyboard (optional),

(5) Internal I/O bus and local bus, and

(6) External communication ports.

8.7.1.10 For security purposes, the components of the video control station computer system may be mounted behind locked cabinet doors or in the equipment room with only the display monitor and pointing device available to the officer. Typically, the computer system is accessed only during startup and subsequent troubleshooting. Similarly, the keyboard is often removed, except during startup and troubleshooting.

8.7.1.11 Peer, central server, and distributed server system architectures all depend upon the components of a data network for system-wide communications. The hardware employed in all these systems consists of the following standard network components: network adapters, network cable, hubs or taps, switchers, routers, bridges and gateways.

(1) Network adapters inside each computer system make the physical connection between the computer systems input/output bus and the network. A computer system can simultaneously connect to multiple networks through the use of additional network adapters.

(2) Network cable options include unshielded twisted pair (UTP), shielded twisted pair (STP), thin coaxial cable, thick coaxial cable, and fiber optic cable. Topology options include star, ring, bus, and star-wired tree. The choice of cable media and topology is dependent on network type and design.

(3) Hubs split the network signal between individual video control stations and simplify cabling. Twisted pair cabling networks generally use hubs, while coaxial cabling networks do not. Coaxial cables are split by merely "T"-tapping at each network adapter. Cabling between hubs or tees is referred to as the "backbone" of a network.

(4) Switchers, routers, bridges and gateways are devices used to interconnect networks. Switches connect similar network segments, thereby extending and speeding up the combined network. Routers, bridges and gateways connect together similar or dissimilar network segments into a larger, combined network.

8.7.1.12 *Server Computer Systems and Printers*:

(1) The server computer systems used in central server and distributed server systems have component parts similar to the video control computer systems, but may not have a permanent display. In such cases, displays are temporarily connected only when needed for maintenance. Small monochrome display monitors and adapters are usually sufficient at servers, since these computers don't display operator interface graphics.

(2) Typically having greater processing demands than each video control station client, system performance can sometimes benefit from use of faster processors at the servers. Various schemes of hard-disk redundancy are also available to safeguard server data.

(3) Printers running off either a server computer or a network are used to obtain hard copy reports for operational or maintenance purposes, or both.

8.7.1.13 UPS units are often installed with a control system to ensure uninterrupted security during a power interruption and the transfer to standby power. Even though standby power may be available in less than 1 min, UPS capacity and battery life is usually provided to monitor alarms for several hours, in case standby power fails.

(*1*) UPS considerations include its sizing for both duration and load, and its power quality performance (noise filtering and surge suppression). Another key consideration is whether to include door hardware loads and communication subsystems on the UPS, so that operations may continue when standby power is unavailable.

8.8 The software components of a video control system include the following:

8.8.1 Operator interface (OI) software (commonly referred to as "video display application software") is the main application program run by a video control station. The OI software dynamically presents to the officer status-change events, such as icon changes, message field changes, status indications, beeps, or voice messages. It also relays officer actions to the security control system, such as activation point selections. The software frequently displays graphics against the backdrop of a facility floor plan drawing.

8.8.1.1 Operator interface software is written and developed using one of three methods: custom source code, commercial off the shelf (C.O.T.S.) packages, or dedicated applications or languages.

8.8.1.2 Custom source code is written in a high-level programming language, such as C++ or BASIC. This software is developed specifically for detention facility video control station applications. Custom source code is generally written as a collection of software modules, each of which implements individual functions or unique variations of functions. The modules then reference various libraries, tables, or databases, or a combination of these, that hold the specific configuration of each unique facility.

(1) The advantages of custom source code over commercially-published OI software packages include its flexibility to accommodate unique functions and procedures, and its performance. Because it is dedicated to corrections and detention applications and compiled as a fully integrated program, custom source code is self-contained, more efficient, and executes faster.

(2) The limitations of custom source code include the trouble facilities will have maintaining or modifying this software independently of the original programmers, without access to the source code, detailed code-level documentation, and the programmers' follow-up technical support. These limitations may be mitigated through attention to contract terms and license agreements and their enforcement.

8.8.1.3 Commercial off the shelf (C.O.T.S.) packages were originally developed for factory floor applications. Many commercially-published OI packages have the flexibility to be used as operator interface software in corrections and detention facilities. Most packages consist of a development module from which individual run-time modules are developed. Software development is required both to tailor the programs for

application to corrections and detention facilities, and to develop the screens for an individual facility.

(1) After each video control station's screens are developed, they are compiled from the development module into the run-time modules that execute on the video control stations. Communications between the OI software and other applications performing security controls generally use the interprocess communication capabilities of the operating system. The channel for this interchange of information between applications is illustrated in Fig. 16.

(2) In comparison to custom source code, commercially-published OI packages can reduce the level of technical skill required to develop video control applications and can prevent sole-source reliance on the developer for maintenance and support.

(3) Commercially-published OI packages do not eliminate the need for the owner to receive pre-compiled application source code.

(4) Its limitations include reduced performance from less efficient code and its interprocess communications. Other limitations include a lack of flexibility inherent in each publisher's object model and paradigm, especially related to highly-customized corrections and detention applications.

8.8.1.4 Dedicated applications and languages, although not commercially available, are technically feasible. Using such a language, a developer would need only to generate the backgrounds and libraries for a specific facility and to compile the commands necessary to implement the facility's operator interfaces.

(*1*) Dedicated applications software for operator interfaces in corrections and detention facilities have been written and provide functionality similar to a dedicated language. At time of last revision of this guide such software was not sold separately from the video control system itself.

8.8.2 *Operating System and Various Device Drivers for Each Computer System, Both Video Control Stations and Optional Servers*:

8.8.2.1 Operating systems provide access to computer system resources for OI software and other applications. All shared resources, such as memory, microprocessor time, disk drive space, communication ports, and certain data files are allocated and managed by the operating system. Its intermediary role between the applications and the hardware is illustrated in Fig. 16.

(*1*) Operating systems are written and compiled specifically for each family of computer processor, although some are portable across platforms. Considerations include single-tasking versus multitasking, single-user versus multiuser, processor family, reliability, and built-in networking. It is not necessary that all computers in a system employ one operating system. Servers and clients within the same system often run different operating systems.

8.8.2.2 Peripheral devices are also managed by the operating system through lower-level software modules known as device drivers. Displays, display adapters, printers, keyboards, mice, and similar peripherals interface to the operating system through device drivers. Device-specific drivers are required for each peripheral, so that the device can be communicated with and managed by the operating system. As shown in Fig. 16, the device drivers typically interact with the hardware through a level of firmware known as the computer's basic input/output system (BIOS).

8.8.3 *Optional Network Operating System(s)*:

8.8.3.1 Networked systems require either a separate network operating system (NOS) or an operating system with built-in networking capability. In either case, the software makes the resources of other computer systems available locally to every other computer system on the network. In the case of a server-based network, the software redirects client service calls or remote procedure calls to the serving resource, wherever it resides on the network. This redirection, in this case to two different networks, is illustrated in Fig. 16.

8.8.4 *Various Utility or Diagnostic Software Programs, or Both*:

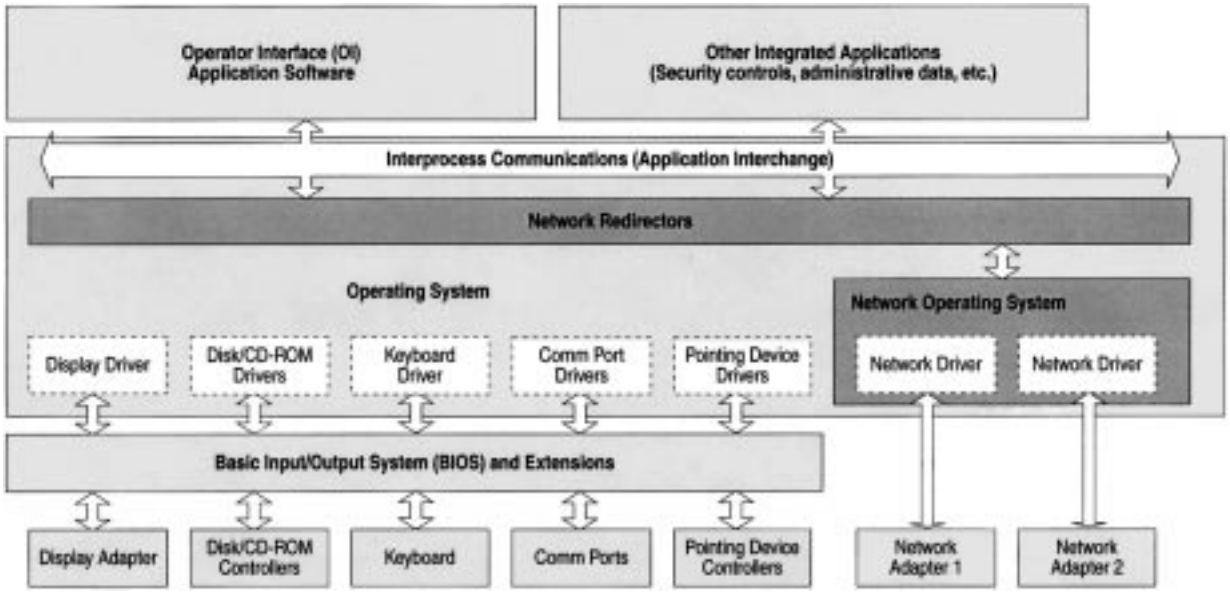

FIG. 16 System Software Illustration—Touchscreen Client with Commercial OI Package

8.9 A typical relationship between the first three software components and the video control station hardware is illustrated in Fig. 16.

8.10 *System Reliability*:

8.10.1 Reliability problems and down time will interrupt normal facility operations and may cause a sense of frustration and can compromise security. Some design measures to improve reliability include:

8.10.1.1 Providing a well-conditioned uninterruptible power source,

8.10.1.2 Signal protection from electromagnetic interference and lightning,

8.10.1.3 Redundant or fault-tolerant components,

8.10.1.4 Backup systems, and

8.10.1.5 Built-in diagnostic tools.

8.10.2 Long-term reliability may also be enhanced during construction through adherence to proper installation practices and implementation of comprehensive startup, testing and troubleshooting procedures. Adequate warranty and maintenance service throughout the systems' life will further contribute to long-term reliability.

9. Establishing Requirements for Operator Interface Presentation

9.1 Physical display and layout of the operator system interface is critical to the effective operation of the facility and the training of staff.

9.1.1 *Graphic/Nongraphic Displays*:

9.1.1.1 Graphical orientations display objects against the backdrop of facility floor plans or site plans, or both, and serve to relate objects within a defined geographical area (a housing pod, for example). If intuitively designed, graphical orientations can help the operator remain spatially oriented within the facility.

9.1.1.2 Nongraphic displays consist of rows of control or indicating devices. These displays are appropriate where orientation is obvious due to the positioning of the control station and direct visual observation of the area.

9.1.2 *Passive/Nonpassive Displays*:

9.1.2.1 Passive displays, sometimes referred to as "exception only" display, indicate only those conditions that are not normal (nonsecure). Thus the display will not highlight normal (secure) conditions and will avoid continuously displaying unneeded information.

9.1.2.2 Nonpassive, or active, displays highlight both secure and on-secure condition of devices, equipment, or areas.

9.1.2.3 Consideration should be given to the quantity of information being presented to the operator. The display can become so congested that it is difficult for the operator to identify important information.

9.1.3 *Annunciation*—Visual and audible annunciation is a key ingredient in the effective operation of a display unit.

9.1.3.1 Visual and audible annunciation should provide distinction among systems, and between normal or emergency alerts for various systems. Careful consideration should be given to the number of distinct signals selected. Too many signals will slow down the operators' response time to the event.

9.1.3.2 Acknowledgement of audible/visual annunciation should be on a zone-by-zone basis.

9.1.3.3 Certain systems, such as perimeter alarms, staff duress, and suicide monitors should be reset on an individual basis as opposed to an overall basis.

9.1.3.4 Visual annunciation may distinguish between systems on the basis of color, or distinguish between different alert status on the basis of color. See Table 2 for suggested indicator colors.

(1) Normal Visual Alert or Call—An alert that requires action or attention, but is for a situation that is not life-threatening. Some examples of such alerts or calls include communications calls, door unlock requests, and most system trouble alerts requiring maintenance actions.

(2) Emergency Visual Alert—An alert that requires immediate action or attention due to a life-threatening emergency. Some examples of such alerts include fire alarms, and staff duress alarms.

(3) Information Visual Alert—Some examples of such information include the location of video monitoring, and cleared alarms.

9.1.3.5 Audible alert volume should be adjustable at the control location to support varying staffing configurations. Audible alert should provide distinct signals for different situations.

(1) Normal Audible Call or Alert—An alert that requires action or attention, but for a situation that is not life-threatening. Some examples of such alerts or calls include communications calls, door unlock requests, and most system trouble alerts requiring maintenance action.

(2) Emergency Audible Alert—An alert that requires immediate action or attention due to a life-threatening emergency. Some examples of such alerts include fire alarms, and staff duress alarms.

TABLE 2 Suggested Indicator and Device Colors

NOTE 1—Most manufacturers use light emitting diodes (LEDS) for visual annunciation because they are reasonably priced, reasonably bright, and very reliable. However, the availability of colors is limited to red, green, yellow, and orange (blue is available at a cost penalty of approximately 20 times the cost per indicator).

System Identification by Color		
System	Function	Color
Locking Control	Secure	Green
	Non-secure	Red
	Interlock	Amber
Alarms	. . .	Red
Audio Communications	. . .	Yellow
Video Communications	. . .	Yellow
Auxiliary Controls	. . .	Orange
Alert Status Identification by Color		
System	Function	Color
Locking Controls	Authorized Use	Green
	Alarm	Red
	Interlock	Yellow
	Trouble	Yellow
Communications	Audio	Orange (S)
	Video	Orange (F)
Auxiliary Systems	Lighting	Yellow

(3) The audible alert should be capable of being silenced at the control station. A subsequent alarm will reactivate the audible alert.

(4) Audible alerts shall not conflict with any other systems sharing the control area.

9.1.4 *Labeling*—Labeling is a key ingredient in the effective operation of a control display.

9.1.4.1 Labels should be short and clear in meaning in order to avoid clutter.

9.1.4.2 Labels should relate to the specific function being described. For example, a swinging door should be labeled "unlock," whereas a sliding door should be labeled "open." Another example may be water control, which should be labeled to describe the condition of the water supply, not the electrical condition of the control device.

9.1.4.3 Labels must have high visual contrast to backgrounds.

9.1.5 *Control Hierarchy and Transfers Between Control Points*—Between control posts a control hierarchy is often established wherein the responsibilities of a particular control post can be assumed or overridden by posts of greater responsibility. When designing hierarchies, transfers and overrides consider the need to provide remote audible and visual communications to remote control posts. Remote communications can require a considerable number of cameras and intercoms with duplicate cabling and communications equipment at each post, as well as large audio and video switchers. Methods of transfer or override, or both, to a post of higher responsibility (for example, central control) include:

9.1.5.1 *Emergency Takeover*—An involuntary transfer of control initiated by central control.

9.1.5.2 *Logout*—A voluntary or scheduled transfer to central control initiated from local control, for example, at the end of a shift.

9.1.5.3 *Duress Shut-Down*—An emergency alarm transmission accompanied by a transfer of control to central control initiated from local control under emergency conditions.

9.1.5.4 *Group Override*—Initiation of grouped or common controls from central control either instead of, or in addition to, local control.

9.1.5.5 *Control-Only Transfer*—Annunciation, and possibly communications, remain at the local post after transfer, but control functions are transferred.

9.1.6 *Security Login/Logout*—Control systems should be designed with security, at a minimum via password protection and login/logout procedures. Consideration should be given to the following items:

9.1.6.1 Numeric keypads which present digits in random order, and

9.1.6.2 Biometrics recognition or higher security measures.

9.2 *System Response*:

9.2.1 The amount of time control systems take responding to operator actions is dependent on many factors. The response time of the security control system and the field devices, such as lock hardware or pan/tilt unit, is also a significant factor in overall system response time (for actions involving those devices).

9.2.2 Noticeable delays in system response time can make a system cumbersome to operate and may undermine staff's confidence in the system. Acceptable performance is ensured by adding system performance standards and test methods to contract documents. Measurements after installation may then confirm whether or not performance results have been achieved

9.3 Consideration needs to be given to the number of operator actions (or steps) that are required to achieve a function. For instance, the passage of a person through a controlled door involves the following steps: (*1*) the person requests passage, (*2*) the officer verifies identity of requestor by audible or visual means, or both, (*3*) the officer unlocks door, (*4*) the officer locks door, (*5*) the officer resets call. Different systems require significantly different numbers of operator actions to accomplish these steps, and some of these differences are based on valid security principles.

9.4 *Hard/Video Control Panels*—When selecting operator interfaces, give consideration to the following comparative factors of each type.

9.4.1 Hard control panels are fixed in physical makeup and form and are used for locations where physical changes to the facility are not likely to occur in the future.

9.4.2 Video control stations are another type of operator interface. They form a "soft" control panel by interactively displaying dynamic, color-graphic displays and activation points to a control officer. Consideration should be given to redundancy in soft control panels. They may be:

9.4.2.1 Used to control multiple areas from a single location by displaying alternate graphic displays.

9.4.2.2 Passive in concept but utilize a broad range of indicator colors.

9.4.2.3 Include, or be accompanied by the use of text to direct operator actions.

9.4.2.4 Multilevel structures. In this case, consideration should be given to the time required to access functions.

9.4.2.5 Located to provide adequate physical protection.

9.4.2.6 Although video display operator interface systems are sometimes more expensive than hard panels and require more sophisticated maintenance, video control stations provide certain advantages over hard panels that, if justifiable and well designed, can help staff more effectively operate a facility.

9.4.2.7 Because video display operator interfaces are dynamic, not physically fixed like a hard panel, their geographic span-of-control may be readily changed with changes in staffing. Video control stations can assume the functionality of other stations, allowing officers to control unmanned posts remotely, so long as audible and visual communications are duplicated. With hard panels, such duplication may increase console size and cost to accommodate the duplicate panels at each post.

9.4.2.8 Video display operator interfaces can also change dynamically with operating mode or officer action. This can simplify the operator interface by only displaying information in the context of when it is needed. For example, camera controls can be hidden until the camera is selected, controls for a certain area can be visible only during the shift they are in use, and policies or procedures can "pop-up" when needed. Because hard panels are fixed in form, such indicators and

controls must always be present on the panel, corresponding again to larger consoles and increased physical space.

9.4.2.9 The spatial efficiency of video control stations also provides an ability, within limits, to integrate a larger number of systems into a single-operator interface, rather than installing a hard panel for every system. Examples include systems such as personal alarms or access controls that might otherwise have their own video display or hard panel operator interface. Another example includes the potential for integration with administrative data that would otherwise require a separate workstation.

9.4.2.10 The operator interface can be changed over time. Functions can be modified or evolve toward a more desirable sequence after operational experience is gained with the system. Features or functions that aren't initially implemented can be added later. This flexibility is one of the key benefits.

9.5 *Hard Panel Materials*—The materials used in the panels should be evaluated for such factors as, but not limited to, durability, reliability, resistance to abuse, ease of operation, and visual presentation.

9.5.1 The background material should be selected with consideration for the following:

9.5.1.1 Finish and color to reduce eye strain caused by reflection of surrounding illumination, and

9.5.1.2 Material that is durable and easily maintained or replaced.

9.5.2 The use of colors plays a significant role in the effective operation of the control panel.

9.5.2.1 Graphics should be distinct yet not interfere with the color of devices (lights and switches). The number of colors used should be limited in order to avoid confusion. See Table 3 for suggested graphic colors.

9.5.2.2 Color of devices or device covers should be uniform throughout a facility.

9.5.3 Both control and annunciating devices should be selected with consideration for the following:

9.5.3.1 *Breakage Caused by Repeated Operation and Abuse*—Select a material and design durable enough to resist damage.

9.5.3.2 *Ease and Speed of Device Replacement*—Ratings for physical and electrical operations should be evaluated for items being controlled. For example, a cell door operating twice a day will take over 34 years to see 25 000 operations. A sallyport door may see 100 operations a day and therefore reach 25 000 operations in less than nine months.

9.5.4 Control devices should be selected with consideration for the following:

9.5.4.1 The operating characteristics of the facility. For example, a cell door will have multiple functions including, but not limited to: group control, inmate access, lock down, emergency release, and remote release.

9.5.4.2 The characteristics of the device being controlled.

9.5.4.3 Prevention of accidental operation for functions which are seldom used, or which have a critical impact on the safety or security of the facility.

9.5.4.4 The type of action required to operate a control device: some examples of which include rotary, toggle, push on – release off, and push on – push off.

TABLE 3 Graphic Background Colors

NOTE 1—The following colors are suggested for use on graphic control panels to effectively orient the operator and provide distinction for ease of operation. Each column represents a set of contrasting colors according to a specific color identification system. The colors in adjacent columns may or may not appear equal to all observers.

Color	Pantone[A] PMS Number	Pratt and Lambert Number[B]	Sherwin Williams Color[C]	Federal GSA Standard 595B[D]
Black	Process Black U	. . .	. . .	37030
White	. . .	Y393W	White	37875
Off White	Cool Gray 1U	YG540W	Buff White	37769
Light Blue	297U	B739P	Egyptian Blue	35550
. . .	. . .	. . .	Pale Blue	35450
Medium Blue	Process Blue U	B761M	Bali Blue	35250
Dark Blue	Blue 072U	B762A	Danish Blue	35095
. . .	. . .	. . .	Highgate Green	34672
Light Green	375U	YG551Y	Pale Green	34491
Green	355U	G572A	Freeway Green	34540
. . .	. . .	. . .	Emerald Green	34090
Light Yellow	1345U	Y343P	Ivory	33613
Yellow	113U	Y340M	OSHA Yellow	13591
. . .	. . .	. . .	Fire Red	31302
Dark Red	Proc. Magenta U	R11R	Bright Red	21105
Purple	Purple U	V048A	. . .	. . .
Orange	Orange 021U	0216Y	Light Orange	32555
Beige	Warm Gray 1U	Y437W	Tan Beige	33564
Light Brown	451U	Y0294M	Sandle Brown	30475
Tan	466U	. . .	Horse Chestnut	30111
. . .	. . .	. . .	Grey Suede	36586
Gray	Warm Gray 4U	Y399P	Light Grey	36314
. . .	. . .	. . .	Grey	36251
. . .	. . .	. . .	Dark Grey	36152
Flor. Green	802U	. . .	. . .	38901
Flor. Yellow	803U	. . .	. . .	38907
Flor. Orange	804U	. . .	. . .	38903
Flor. Pink	805U	. . .	. . .	. . .
Flor. Purple	806U	. . .	. . .	. . .

[A] Available from Pantone, Inc., 55 Knickerbocker Rd., Moonachie, NJ 07074.
[B] Available from Pratt and Lambert, Inc., Screen Printing Products, P.O. Box 22, Buffalo, NY 14240.
[C] Available from Sherwin Williams, Inc., Screen Printing Products, 101-T Prospect Ave., N.W., Cleveland, OH 44115.
[D] Available from General Services Administration, Business Service Center, Federal Supply Service, Washington, DC 20407.

9.5.5 Annunciation devices should be selected with consideration of the following:

9.5.5.1 The functions required to meet the operating characteristics of the facility. For example, an inmate call may be annunciated at multiple locations due to staffing patterns.

9.5.5.2 The size, brightness, and longevity of the visual annunciating devices.

9.5.5.3 Annunciation devices should be uniform throughout a facility.

9.6 *Video Control Stations*—The materials used in video control stations should be evaluated for such factors as, but not limited to, durability, reliability, resistance to abuse, ease of operation, and visual presentation.

9.6.1 *Individual Video Control Functions*—The design of each individual video control station requires a series of design decisions with regard to:

9.6.1.1 *Geographic Span-of-Control*—A specific geographic area is controlled and monitored by the video control station. This span of control may be either static or dynamic (for example, the primary control station may control an outer sallyport door to an area, while the inner door is under control of a secondary control station. Inner door control may be transferred to the primary control station).

9.6.1.2 *Functional Span-of-Control* (that is, level of systems integration)—Control, monitoring or communication functions are assigned to a specific video control. Assignment of functions may be independent of a geographical area. Typical system functions (which may be the same as for hard panels) are listed under "Establishing System Requirements" (see 6.3). Integration of too many systems or functions, or both, into a single video control station may become unwieldy to operate, especially with high-screen depth or busy graphic presentation. Integration of fire alarms should give consideration to agency listing and approval requirements for such equipment and may justify its own operator interface for primary notification.

9.6.1.3 *A Paradigm of Display—How*—Automation of policies, procedures, and operator help functions.

(1) What Degree of Automation?—Online," pop-up" policies and procedures provide a high degree of automation if presented in context with their associated actions, such as help or warning messages. Implementation of automated functions requires decisions of how rigid responses will be and what latitude the operator is given to intervene (for example, confirmation messages).

(2) Pop-up policies and procedures.

(3) Help menu.

(4) Automated purposes.

9.6.1.4 *Prioritization of Control and Annunciation Functions*—Control and annunciation events are prioritized in accordance with a preset logical scheme. Events of an equivalent priority will appear in the event message field on a "first-in/first-out" basis so that they are dealt with in the order received. When a higher priority alarm is received (for example, officer duress), it goes to the top of the queue for immediate attention. System functions are listed under "Establishing System Requirements" (see 6.3) in order of their suggested priority for alarm and control.

9.6.2 *Work Sharing at Control Points*—Redundant video control stations are sometimes provided at critical control posts to respond both to variations in work load and staffing at the particular control post (that is, work sharing). A collateral advantage of redundancy is backup control in the event the primary video control station were to fail. Methods of work sharing include:

9.6.2.1 *Parallel Event Response*—Video control stations indicate events simultaneously. Any video control in the group can respond.

9.6.2.2 *Geographic Division*—Video control stations divide responsibility for the control post geographically and each video control station only receives the events within its geographic area of responsibility.

9.6.2.3 *Functional Division*—Video control stations divide responsibility for the control post functionally by system and each video control station only receives the events for the systems it is responsible for.

9.6.3 *Security Login/Logout*—Control systems should be designed with security, at a minimum via password protection and login/logout procedures. Consideration should be given to the following items:

9.6.3.1 Numeric keypads which present digits in random order.

9.6.3.2 Keyboards providing multiple-level access. Entries should be masked.

9.6.3.3 Biometrics recognition or higher security measures.

9.6.3.4 Other security considerations include limiting use of the video control station to the intended application. In particular, video control systems should prevent operators from playing computer games and from accessing the operating system where they can perhaps create a system failure by renaming files or similar activity.

(1) Lockout computer games.

(2) Lockout unauthorized access to operating system.

(3) Basic input/output system (BIOS) protection.

9.6.4 *Integration of Security/Control with Administrative Data*—Legitimate concerns include possible preemption of high-priority security and control tasks with low-priority administrative duties. The potential exists for administrative applications to crash, inhibit, or degrade performance of the video control application. An appropriate level of integration and method of implementation might well overcome these concerns and provide benefits to the officer.

9.6.4.1 Accessing current classification and arrest records for an inmate (possibly on a read-only basis).

9.6.4.2 Provides the ability to make on-line notes to other shifts regarding inmate management status.

9.6.4.3 Possible methods of implementation include:

(1) Serving the security application as a client with records from other systems.

(2) Multitasking another application on the video control station running simultaneously with security and control.

9.6.5 *Training Features*—Redundant video control stations at individual control points can act as training stations when not being used on a work sharing basis. This requires implementation of a training mode where the station operates off-line and the development of programs that realistically simulate actual operating events with which the officer may interact.

9.6.6 *Screen Composition*—The entire display area is generally filled with a white or colored background and the screen composed by overlaying this background with the following screen elements:

9.6.6.1 *Screen Function Area*—One or more screen areas that organize the screen's functions by geographic area or functional group.

(1) Like hard control panels, options for graphic presentation of the screen function area include both graphical and linear orientations.

(2) Typically multiple drawings are required to display the facility at a usable scale. While the background drawing scale should minimize the number of screens by displaying as wide

a geographical area as possible, ideally the scale will be no smaller than [1:100] (0.125 in. equals 1 ft).

(3) Linear orientation is often useful for functional groups, such as utility screens, that do not benefit from a graphical orientation or have no geographical relationship to the facility.

9.6.6.2 *Global Function Area*—One or more screen areas, that organize the functions displayed on every screen, such as date and time. Global function areas should remain consistent from screen to screen and should be designed to leave a usable size and shape of screen function area. They are typically implemented as a menu bar or function group on either the bottom, top, or sides of each screen.

9.6.7 Screen visual design adherence to the following visual design suggestions will minimize screen clutter and provide an intuitive“ look and feel” to individual screens:

9.6.7.1 Use of hidden pop-up boxes and menus that are hidden until selected and disappear after use.

9.6.7.2 Provide multiple methods of control including event-driven selections.

9.6.7.3 Maintain consistency between screens in the location and appearance of similar screen elements, and control objects (for example, graphical standards including colors, grey scales, line weights, and other graphical elements).

9.6.7.4 Whenever possible, use a consistent scale and level of detail for graphical backgrounds.

9.6.7.5 Adjust text for screen titles, room titles and general information text. Use a uniform font and point size for text of each given category.

9.6.8 *Navigational Aids*—Navigational aids are a global function on every screen that are used by the officer to move between individual screens. A variety of navigational aids should be provided with the most common methods being those described in the following paragraphs:

9.6.8.1 *Key Map*—A key plan of the project, building or part of the building, should be displayed on all screens. Selecting a segment of the key plan shall cause the map of that area to be displayed. The key map shall indicate the location of the operators viewing location at all times.

9.6.8.2 “Previous screen” icon moves from the currently viewed screen to the screen previously selected.

9.6.8.3 “Select” or “go to” icon selects an activity that is highlighted in the event message field. This feature gives the operator the ability to allow events to drive the map movement when the event is selected.

9.6.8.4 “Site” or “main” icon takes the operator immediately to the site or main screen regardless of which screen is currently being displayed.

9.6.8.5 “Utilities” icon accesses a utility screen which may list the various screens in a tabular form with a brief description.

9.6.8.6 Directional arrows.

9.6.8.7 Pop-up screen list box.

9.6.8.8 Manual zooming.

9.6.9 *Global Functions*—In addition to navigational aids, the global function area should provide access to control objects and data that should be readily available for the functionality of every screen. The global function area should organize these in a consistent manner between screens.

9.6.9.1 *Global Buttons and Icons*—Logoff, system utilities, alarm silence, and alarm reset.

9.6.9.2 *Global Data*—Screen identification, time of day and date, and event message field (for example, typically four events).

9.6.10 *Screen Depth*—High-screen depths add complexity to the operator interface and create a tendency for officers to lose their orientation within the system. Approximately one-half of all projects can be limited to a screen depth of two (the site map, plus individual pod and area screens). Approximately 40 % of all projects may need a screen depth of three (the site map, building-wide screens, and individual pod and area screens). Fewer than 10 % of all projects ought to need a screen depth of four or greater.

9.6.11 Control objects include icons, buttons, message fields, etc.

9.6.11.1 Generally, an object shall provide status indication by its color, associated text, animated components, or a combination of these elements. Activation points represent the area limits above and around control objects that a pointing device will activate. For ease of selection, it is common for activation points to be somewhat larger than the control object itself.

9.6.11.2 Consideration must be given to both minimum activation point size and separation between activation points, considering parallax and calibration drift. Small, closely-spaced activation points may increase screen clutter, fatigue the operator and create inadvertent control operation. Large, widely-spaced activation points may also slow down operations by limiting the number of functions per screen and increasing time spent navigating between screens.

9.6.11.3 With a finger as the stylus and touchscreen as the pointing device, the following minimum sizes are typically used for control objects:

(1) Control Icons and Buttons (Switch Functions)—Greater than or equal to 13 mm (0.5 in.) square with a minimum spacing (touch resolution) of greater than or equal to 19 mm (0.75 in.) between centers.

(2) Status Icons (Visual Indicators Only)—Greater than or equal to 5 mm (0.1875 in.) in diameter, square or rectangle in shape. For priority alarms (that is, personal alarms and fire alarms) a minimum of 13 mm (0.5 in.) in diameter or equivalent square or rectangle is recommended.

9.6.11.4 With pointing devices other than touchscreens, for example mouse-driven systems without a touchscreen option, activation points may be smaller. However, they should not be so small as to cause fatigue.

9.6.12 *Ergonomic Considerations*:

9.6.12.1 Consideration shall be given for operators that are visually color impaired. Each icon shall be distinct for its assigned function and consist of symbols and colors. Each change of status shall include that for both selection and verification. Icons shall be created so that change in state is indicated by both color and graphical change.

9.6.12.2 Ergonomic design (avoiding information overload), as well as the ergonomic environment around the video control stations (total interface environment).

9.6.12.3 Number of selections or steps per function.

9.6.12.4 ADA and bilingual considerations.
9.6.12.5 Visual, tactile and audible feedback.
9.6.12.6 User settings/preferences based on login.

10. Establishing Requirements for Control System and Communication Subsystem Interfaces

10.1 In most systems, video control station computers perform only as the operator-interface "front-end" to a complete security control system. In this case, the video control system communicates with the security control system through a security control system interface. In small, stand-alone systems, the video control station may sometimes double as a computer-based security control system, in which case the system does not have an interface. See Fig. 10.

10.2 Video control stations typically interface to discrete logic, programmable logic controller, computer-based, or distributed control type security control systems. They are seldom, if ever, interfaced to hard wire or relay logic controls.

10.3 The two alternatives for the security control system interface are illustrated in Fig. 17 and include:

10.3.1 *Direct Interface*:

10.3.1.1 The video control station's external communications port is connected directly to a communications port on the programmable logic controller or the computer-based control system. The direct interface is a serial communications link (that is, RS-232-C, RS-422, RS-485 or similar standard) between ports.

10.3.1.2 Advantages of the direct interface include its simplicity and ease of installation, troubleshooting and maintenance.

10.3.1.3 Its limitations include reduced performance in comparison to networks and reduced ability to support distributed processing.

10.3.2 *Network Interface*:

10.3.2.1 A network is used to interface video control stations to the security control system. Even stand-alone systems can have a network interface to the security controls. In networked systems, the video display network may be used or, if the security controls system is also networked, the interface may be through the security controls network. Fig. 17 illustrates both types of network interface.

10.3.2.2 Advantages and limitations of network interfaces to the security control system are the same as for networked video control systems in general.

10.4 *Communication Subsystem Interfaces*:

10.4.1 Associated communication functions include visual identification and surveillance via closed circuit television (CCTV) video subsystems and audible communications through intercommunication and paging subsystems. "Operator interfaces" to these subsystems are typically console-mounted adjacent to the video control station display monitor. These interfaces are illustrated in Fig. 18 and described below.

10.4.2 *Video (CCTV) Subsystem Interface*:

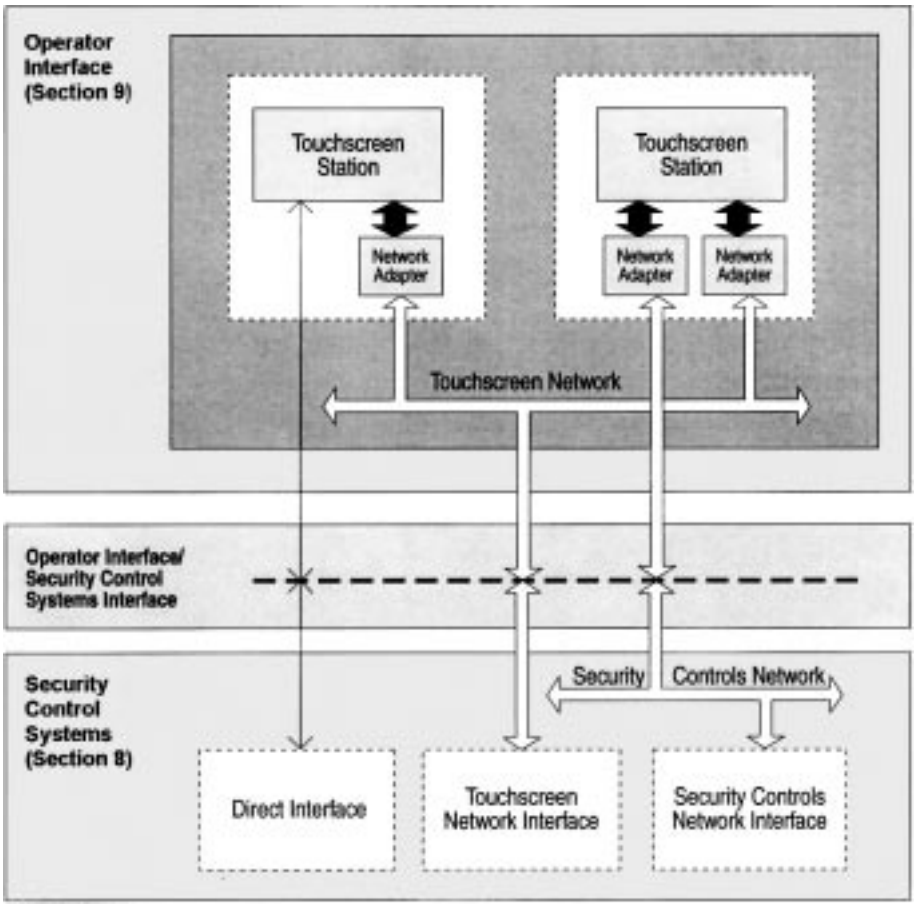

FIG. 17 Security Control System Interfaces

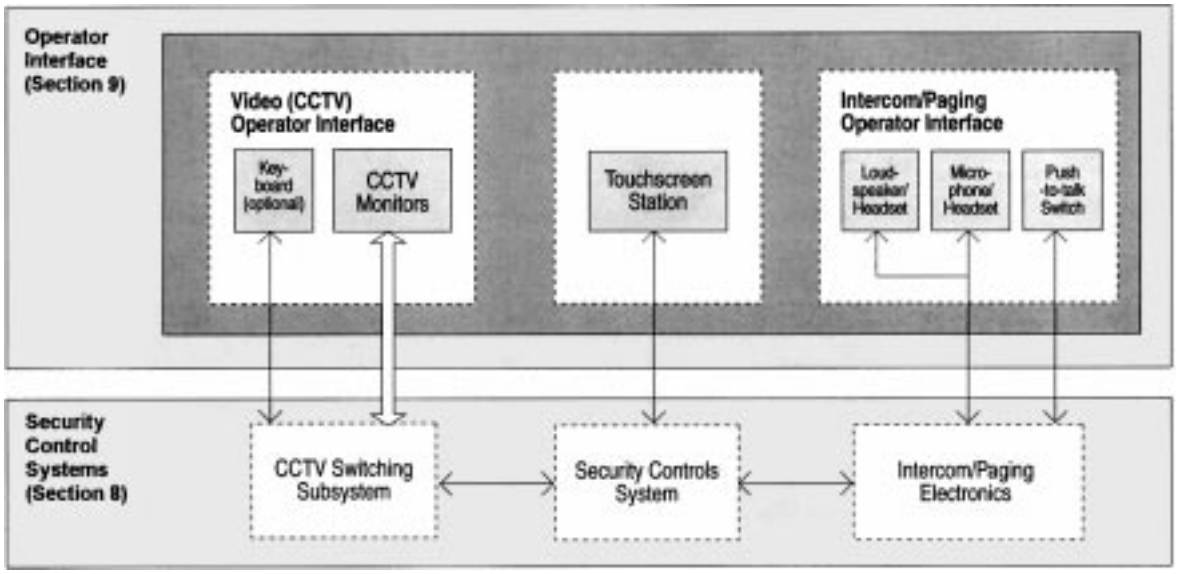

FIG. 18 Communication Subsystem Interfaces

10.4.2.1 Video monitors perform the operator interface function, either singly or in groups. Ergonomic considerations include locating monitors within the officer's range of vision without obstructing security sight lines, reducing glare on the monitors, and providing optimal image size and quality.

10.4.2.2 Integration between video control stations and camera switching is obtained via an interface from the security controls system and the CCTV switching subsystem. If desired, optional keyboards provide manual override and programming capability at the officer's position.

10.4.3 *Intercom/Paging Subsystem Interface*:

10.4.3.1 An intercom/paging master station typically acts as the operator interface for the audio subsystems, both intercom and paging.

10.4.3.2 Minimum components include a master station loudspeaker and microphone. Intelligibility and officer comfort are often enhanced through the use of optional headsets and half-duplex or full-duplex communications. If push-to-talk switches are needed for simplex communications, they are often located remote from the video control station on the master station, or sometimes a foot switch serves this function.

10.4.4 *Digital Multimedia Operator Interface*:

10.4.4.1 The above interface descriptions are based on analog technology. A multimedia operator interface bringing both digital video and digital audio into the video control station itself is technically feasible, but was not particularly cost-effective at the time this guide was last updated.

10.5 *Associated Control and Alarm Subsystem Interfaces*:

10.5.1 Specialized control and alarm functions, such as access control of security doors, are often performed through interfaces to a separate subsystem. These interfaces are most commonly made through the security control system in similar fashion to communication subsystem interfaces.

10.5.2 Example control and alarm subsystem interfaces include:

10.5.2.1 Access controls interface,

10.5.2.2 Fire alarm interface,

10.5.2.3 Personal alarm interface, and

10.5.2.4 Perimeter security interface.

11. Equipment Rooms

11.1 Physical environment considerations include:

11.1.1 *Space*—Failure to consider space requirements at the beginning of the project may significantly limit the choice of technology, which can impact cost. The amount of space must be sufficient to provide accessibility for maintenance, proper code clearances, and for future expansion.

11.1.2 *Environmental Conditions*:

11.1.2.1 The technology selected determines whether temperature- and humidity-controlled equipment rooms are required.

11.1.2.2 Equipment should be placed in enclosures that provide ventilation and dust protection.

11.1.3 *Location*:

11.1.3.1 Is the equipment room inside or outside the security perimeter.

11.1.3.2 It should not be routinely accessible to either the operating staff or inmates.

11.1.3.3 The technology selected and the cost may affect the choice of location.

11.1.4 *Security*:

11.1.4.1 Minimize the need for maintenance staff to bring tools into or through secure areas.

11.1.4.2 Protect against water damage.

11.1.4.3 Vulnerability to sabotage by inmates or unauthorized staff.

11.1.4.4 Monitor doors into equipment rooms and equipment enclosures.

11.2 Electrical environment considerations include:

11.2.1 *Power Supply*:

11.2.1.1 All power sources to security systems need to be reliable systems, which includes being on the emergency generator.

11.2.1.2 The quality of the power supply is an issue depending on the technology selected.

11.2.1.3 Distributed power supplies, by function, can provide significantly enhanced reliability. When distributed power supplies are used, provide a mechanism to report any failures back to central control.

11.2.1.4 Uninterruptible power supplies should be used on all systems, or they should be battery backed up.

11.2.2 *Grounding*:

11.2.2.1 Proper grounding is important.

11.2.2.2 The higher the level of technology, the more important the quality of the ground.

11.2.2.3 The lightning environment is an important consideration in designing the grounding system.

11.2.3 *Surge/Transient Protection*:

11.2.3.1 Surge and transient protection should be implemented on all systems, including power, control, and communications circuits.

11.2.3.2 The higher the level of technology, the more important surge and transient protection becomes.

11.2.4 *EMI/RF Protection*:

11.2.4.1 Security systems should be assembled in metal cabinets with good grounding.

11.2.4.2 Consider both facility based and external potential sources of interference.

12. Maintenance

12.1 The level of technology skills available within the facility staff or from the surrounding community has an effect on the selection of technology.

12.2 When maintenance is not provided by facility staff, then the distance to the servicing facility and their response time to a service request should be specified.

12.3 Make an assessment of critical spare parts to be turned over to the owner at contract completion.

12.4 Determine the availability of replacement parts:

12.4.1 Vendor only.

12.4.2 Multiple sources.

12.4.3 Delivery time.

12.5 Consideration should be given to the availability of extended service contracts for electronic systems.

12.6 Users should be cautious about selecting technology that uses custom designed products, which may impact future availability of parts, service, or expandability of the system.

12.7 Consideration should be given to technologies which support preventive maintenance programs.

13. Training

13.1 Training of staff, both for operation and maintenance, should be considered in the initial selection and specification of systems. Ease and speed of training is essential to initially staff the facility or to train replacement staff in order to maintain an effective operation.

13.1.1 *Operational Staff*—Structured training using audio-visual aids and actual hands-on practice should be considered.

13.1.1.1 Ongoing training to implement system upgrades should be scheduled on at least an annual basis.

13.1.1.2 Training manuals providing written description of operations should be created.

13.1.1.3 Redundant video control stations at individual control points can act as training stations when not being used on a work sharing basis. This requires implementation of a training mode where the station operates off-line and the development of programs that realistically simulate actual operating events with which the officer may interact.

13.1.2 *Maintenance Staff*—Structured training using audio-visual aids should be considered. Maintenance staff should participate in operational training as well as specific maintenance training. Maintenance contracts should be considered. Include the following:

13.1.2.1 Preventive as well as periodic maintenance techniques,

13.1.2.2 Inventory procedures for spare and replacement parts, and

13.1.2.3 Procedures for identification and resolution of maintenance requirements.

14. Keywords

14.1 access control; control panel; correctional facility; detention facility; detention security; duress; intercom; locking controls; man down; nurse call; paging; perimeter detection; programmable logic controller; touchscreen

APPENDIX

(Nonmandatory Information)

X1. ADDITIONAL REFERENCES

X1.1 American Correctional Association

Contact: American Correctional Association
8025 Laurel Lakes Court
Laurel, MD 20707

X1.1.1 ACA Stds. for Adult Local Detention Facilities, 3rd Ed.

X1.1.2 ACA Stds. for Small Jail Facilities, 1989

X1.1.3 ACA Stds. for Adult Correctional Institutions, 3rd Ed.

X1.1.4 ACA Stds. for Juvenile Detention Facilities, 3rd Ed.

X1.1.5 ACA Handbook on Facility Planning and Design for Juvenile Corrections

X1.1.6 ACA 1992 Standards Supplement

X1.2 Electronic Industries Association (EIA)

Contact: Electronic Industries Association
2001 Pennsylvania Avenue, N. W.
11th Floor
Washington, DC 20006

X1.3 General Service Administration (GSA)
Contact: Business Service Center
Federal Supply Service
Washington DC 20407

X1.4 Institute of Electrical and Electronic Engineers (IEEE)
Contact: Institute of Electrical and Electronic Engineers
345 East 47th Street
New York, NY 10017-2394

X1.5 National Fire Protection Association (NFPA)
Contact: National Fire Protection Association
1 Batterymarch Park
Quincy, MA 02269

X1.5.1 NFPA 70 National Electrical Code
X1.5.2 NFPA 101 Life Safety Code

X1.6 National Institute of Corrections (NIC)
Contact: National Institute of Corrections
1790 30th Street
Boulder, CO 80301

X1.7 National Institute of Standards and Technology (NIST)
Contact: National Institute of Standards and Technology
Building and Fire Research Laboratory
Gaithersburg, MD 20899

X1.8 Model Building Codes

X1.8.1 Building Officials Code Association (BOCA)
Contact: Building Officials and Code Admin. International
4051 West Flossmoor Road
Country Club Hills, IL 60478-5795

X1.8.2 Southern Building Code (SBC)
Contact: Southern Building Code Conference International
900 Montclair Road
Birmingham, AL 35213-1206

X1.8.3 Uniform Building Code (UBC)
Contact: International Conf. of Building Officials
5360 South Workman Mill Road
Whittier, CA 90601

X1.9 State and Local Codes