



Designation: F 1465 – 99

Standard Guide for Selection of Operational Security Control Systems¹

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 (Appendix X2)²

2.2 *International Electrotechnical Commission:*

IEC 1131 Part 3—Programming Languages³

3. Terminology

3.1 *Definitions:*

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

3.1.2 *audio threshold sensing, n*—mechanism which monitors a pre-set 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 *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.

3.1.5 *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.

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

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

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

3.1.9 *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.

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

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

3.1.12 *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.

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

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

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

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

3.1.17 *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).

¹ This guide is under the jurisdiction of ASTM Committee F-33 on Detention and Correctional Facilities and is the direct responsibility of Subcommittee F33.06 on Operational Systems.

Current edition approved Jan. 10, 1999. Published May 1999. Originally published as F 1465 – 93. Last previous edition F 1465 – 95.

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

³ Available from American National Standards Institute, 11 W. 42nd St., 13th Floor, New York, NY 10036.



F 1465

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

3.1.19 *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.

3.1.20 *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*).

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

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

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

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

3.1.25 *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.

3.1.26 *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.

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

3.1.28 *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 3.1.16 and 3.1.46; *control station* means either type of interface.)

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

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

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

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

3.1.33 *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.

3.1.34 *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).

3.1.35 *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.

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

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

3.1.38 *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.

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

3.1.40 *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).

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

3.1.42 *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.

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

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

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

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

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

3.1.48 *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 constructable, 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.

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.

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

- Step 1: Define the characteristics of the proposed facility
- What operational philosophy will be followed?
 - Direct supervision
 - Indirect supervision
 - What staffing restrictions will be confronted?
 - Due to size of staff
 - Due to location of facility
 - Due to education and training
 - Due to current pay scales
 - What environmental limitations will be confronted?
 - Due to terrain
 - Due to weather
 - Building design and layout?
 - Centralized or decentralized control
 - Podular or linear arrangement of cells
 - Single building or campus arrangement
 - Low rise or high rise
- Step 2: Evaluate the selections of Step 1 for conformity to ALL of the decisions, capabilities, and restrictions defined in Step 1. Re-evaluate 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

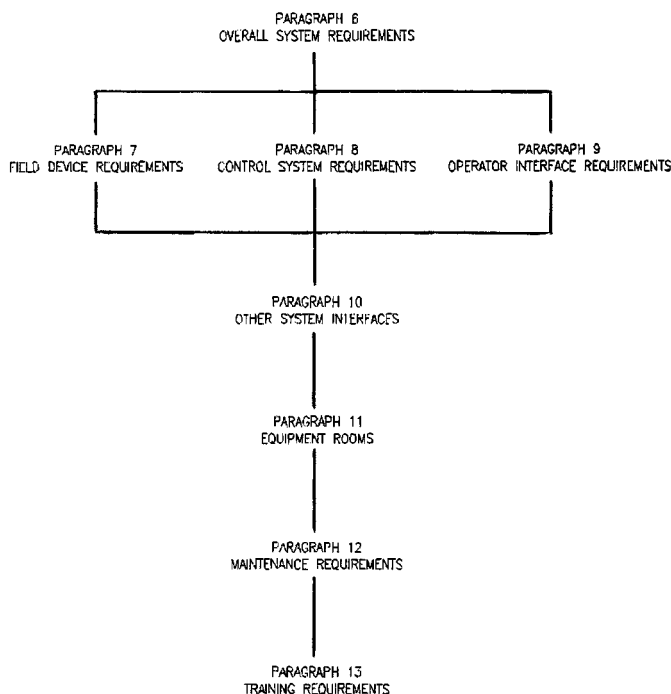


FIG. 2 Flow Chart of Document Sequence and Organization

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 by-passed perimeter zones and systems off-line for maintenance.

7. Establishing Requirements for Field Devices

7.1 This section is being developed.

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. 3). 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.

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 on-line.

8.2.12.2 Custom software development costs.

8.2.12.3 Response time can be slow because of central processing.



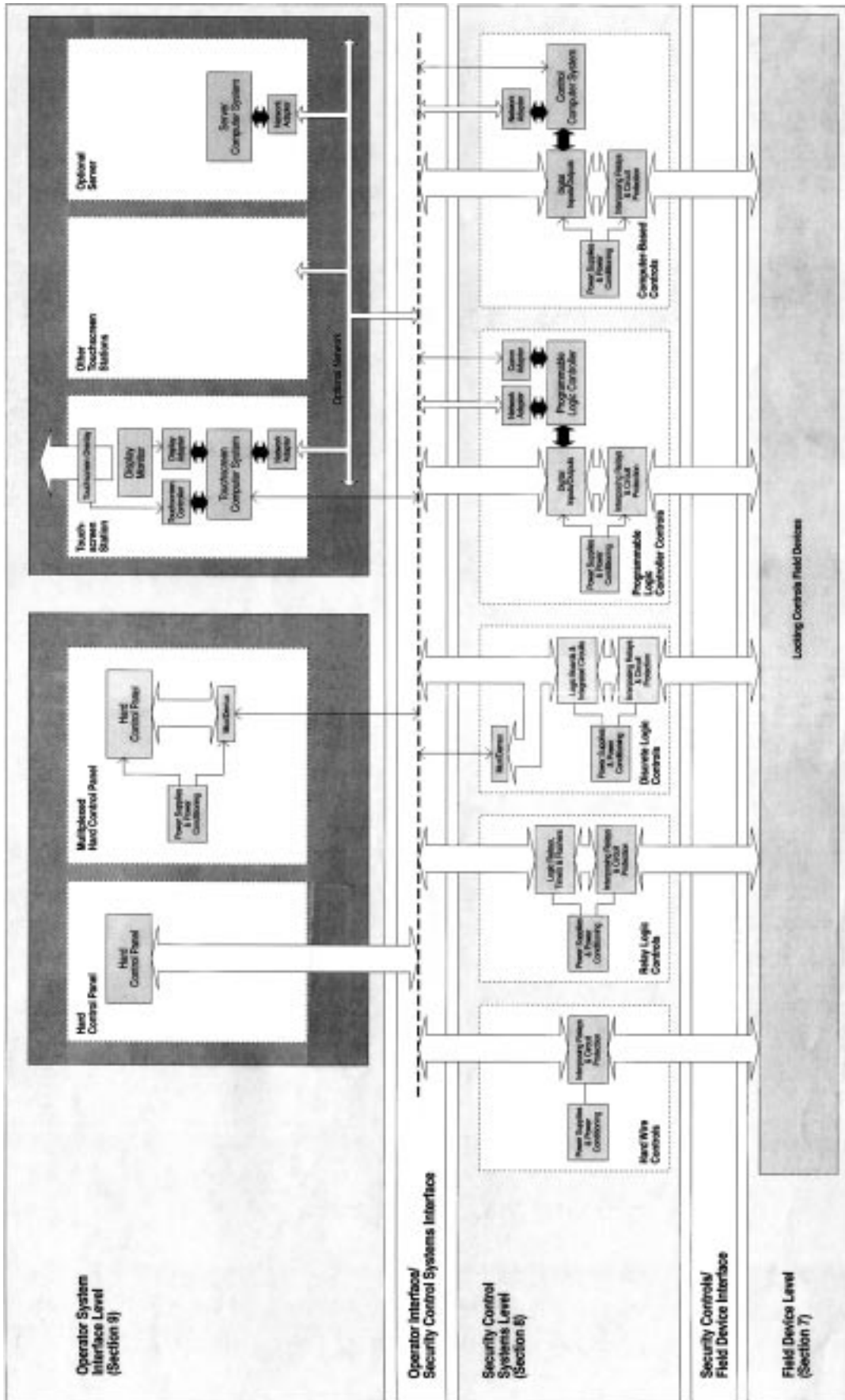


FIG. 3 Overview Diagram—System Interrelationships and Technology Options



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. 4 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. 5 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

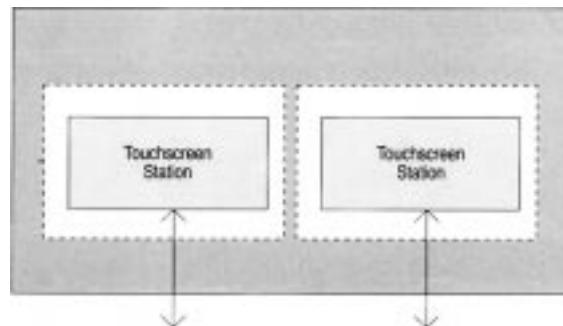


FIG. 4 Stand-Alone System Architecture