Designation: F 1576 – 95a

AMERICAN SOCIETY FOR TESTING AND MATERIALS
1916 Race St Philadelphia, Pa 19103
Reprinted from the Annual Book of ASTM Standards Copyright ASTM
If not listed in the current combined index, will appear in the next edition

Standard Guide for Selection of Security Control Systems Part II—Defining the Central Control System[1]

This standard is issued under the fixed designation F 1576; 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 This guide focuses specifically on those issues and decisions relating to the central control system. For related information on defining the operator-system interface, see Guide F 1465.

2. Referenced Document

2.1 *ASTM Standard:*

F 1465 Guide for Selection of Security Control Systems Part III—Defining the Operator System Interface[2]

3. Terminology

3.1 *Definitions:*

3.1.1 *audio threshold sensing, n*—mechanism that monitors a preset noise level and generates an alarm when that level is exceeded (see Guide F 1465).

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

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

3.1.4 *discrete logic, n*—a combination of distinct electronic components that performs a predetermined function in response to a defined input signal(s) (always custom to the application). See Guide F 1465.

3.1.5 *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).

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

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

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

3.1.9 *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.

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

3.1.11 *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 requirements for software or hardware, or both, implementation.

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

3.1.13 *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 and systems.

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

3.1.15 *scream alarm*—See *audio threshold sensing.*

3.1.16 *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.

3.1.17 *sound disturbance alarm*—See *audio threshold sensing.*

3.1.18 *sound activated alarm monitoring (SAAM), n*—See *audio threshold sensing.*

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

3.1.20 *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 Fig. 1, which shows 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 tech-

[1] This guide is under the jurisdiction of ASTM Committee F-33 on Detention and Correctional Facilities and is the direct responsibility of Subcommittee F33.04 on Operational Systems.

Current edition approved July 15, 1995. Published September 1995. Originally published as F 1576 – 95. Last previous edition F 1576 – 95.

[2] *Annual Book of ASTM Standards*, Vol 04.07.

In the design and selection of the security control systems consistent with the principles outlined in Guide F 1576, 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 Guide F 1576 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 Flowchart of Selection Process

nology for specific applications. It attempts to identify points of experience that 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 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.

6. Establishing System Requirements

6.1 *Signal Conversion:*

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

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

6.2 *Logic:*

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

6.2.2 Methods of implementing logic include:

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

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

6.3 *Signal Transmission:*

6.3.1 Signal transmission is sending a message from Point A to Point B.

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

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

6.3.3.1 Twisted pair(s) of wire,

6.3.3.2 Coaxial cable,

6.3.3.3 Fiber-optic link,

6.3.3.4 Radio link.

6.3.4 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 the following:

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

6.3.4.2 Systems monitoring the outside perimeter.

6.3.4.3 Systems related to personal safety.

6.3.5 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 the following:

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

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

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

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

6.4 *Data Storage and Retrieval:*

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

6.4.1.1 Manually generated.

6.4.1.2 Automatically generated.

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

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

6.4.2.2 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.

6.4.3 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:

6.4.3.1 Hard wired systems.

6.4.3.2 Relay logic systems.

6.4.3.3 Discrete logic systems.

6.4.4 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 as follows:

6.4.4.1 *Administrative*—Interlock overrides, emergency