Homeland Security
Science and Technology

Summary

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective operational tests on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

To contact the SAVER Program Support Office
Telephone: 877-336-2752
E-mail: saver@dhs.gov
Visit the SAVER Web site:
https://www.rkb.us/saver

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the United States Government. Neither the United States Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

Handbook of Access Control Technologies

SPAWAR Systems Center, Charleston, prepared the Handbook of Access Control Technologies *at the request of the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Charleston, SC, 2005. The handbook is available by request at* https://www.rkb.us/saver.

Background

The *Handbook of Access Control Technologies* provides a review of the many technologies that comprise access control systems. The handbook provides basic information to organizations whose primary functions may not encompass designing, evaluating, or building access control systems, but need knowledge of such tools. Any organization seeking to build an access control system should do so only with the assistance of personnel or organizations that specialize in designing and building such systems. Establishing an integrated access control system involves not only design, construction, and testing, but also the long-term issues of operation, training, and maintenance.

Access Control System Employment Considerations

Operational Requirements

Access control systems should be tailored to the needs and requirements of the resource or area to be protected. The starting point for defining needs and requirements is to perform a vulnerability assessment. The type of facility, the nature of the environment, the organization's previous experience with access control programs, and assumptions about potential threats will influence the approach used to develop a solution from the vulnerability assessment. Several other factors should be considered in the vulnerability assessment: the nature and tempo of activity in and around the site, the size of the authorized population, varying degrees of accessibility, the physical configuration of the facility, the surrounding natural and human environment, fluctuations and variations in the weather, permanence, training, and support.

Physical Control: Drop arm barriers are commonly used at parking lots and garages. The arms of some products are capable of stopping unauthorized vehicles when in the down position. Some drop arm barriers incorporate a cable designed to lasso and destroy the front end of a vehicle attempting a penetration. These devices are available with crash test ratings up to the highest DoS level.

With modern electronics, the flexibility to integrate a variety of equipment and capabilities enhances the potential to design an access control system to meet specific needs. There are four main elements of an access control system:

1. Access control barrier;
2. Access control verification or identification equipment;
3. Access control panel that controls the barrier;
4. The communications structure that connects these elements and connects the system to the reaction elements.

Performance Characteristics

The performance measure that characterizes all the categories of access control equipment in the handbook is throughput, the measure of the number of authorized persons or vehicles that can process through an ingress or egress point within a period of time.

Some of the most sophisticated equipment can allow quite high throughput rates. In general, the higher the security requirement and the greater the number of access control devices one must pass through, the lower the throughput rates.

Architecture of Access Control Systems

In general, access control infrastructure, both personnel and equipment, consists of the following elements:

- Intrusion detection
- Surveillance
- Communications
- Response systems

Direct interaction with access control systems normally begins at entry points around a facility's perimeter. At this point and at locations inside, access control may be manual or automated in some fashion. Automated equipment may have an entire database resident at the site of the equipment, or the access control device may communicate with a centrally located or remote database. The manner in which authorized user data is handled at any location depends on the overall system and equipment choices and should be considered carefully with access control engineering professionals during the design process.

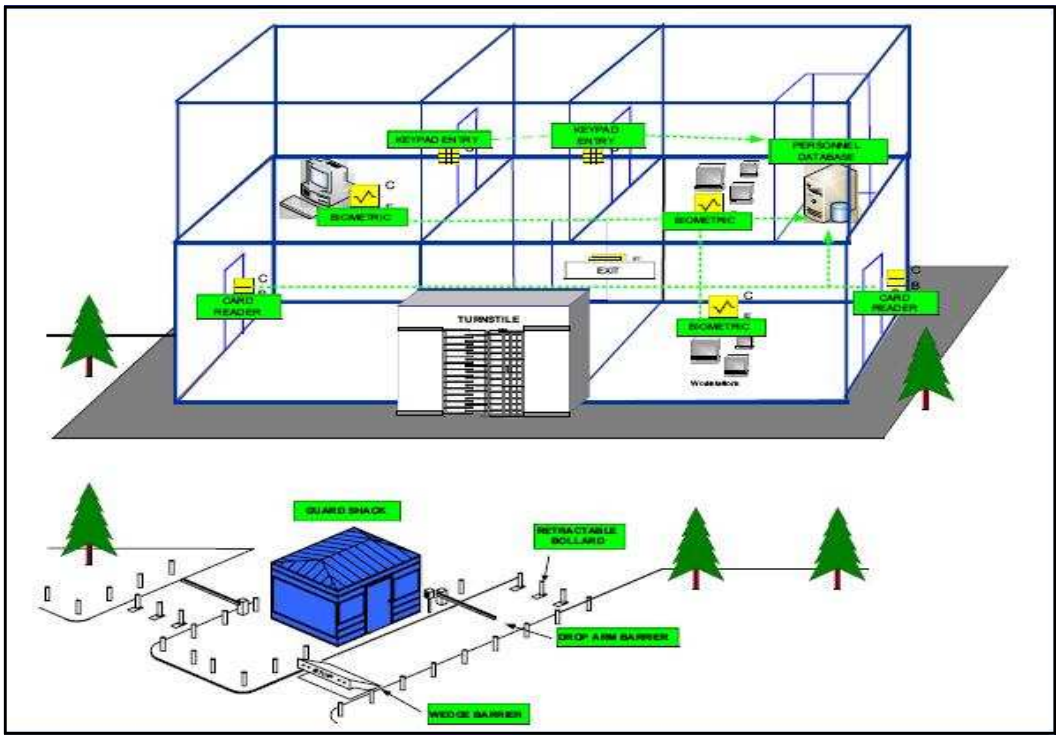
Databases of Authorized Personnel

Data regarding personnel authorized to enter parts of facilities may be on paper, automated, or a mixture of the two. Small facilities or those who have relatively low security requirements may use personnel to manage information by hand. Many facilities still manage adequately with security guards and identification badges or a token driven turnstile system that does not query a database.

Many electronic token systems and biometric systems interact with automated databases. The management of authorized user information gets more complicated as the types of access control technologies in a facility's overall system grows with the size of organization and the number of people it monitors.

Environmental Considerations

Many access control zones may have unique characteristics imposed by the environment that must be considered when designing the system, selecting the equipment, and performing the installation. Exterior zones are likely to be affected by the prevailing climate, seasonal extremes, and fluctuations in weather conditions. Man-made environmental



Access Control Schematic:
Many applications of access control technologies inside and outside of a protected area.

factors, such as activity patterns, electrical fields, radio transmissions, and movements of vehicles, trucks, trains, or aircraft also influence the design and performance of integrated security and access control systems.

Interior zone access control equipment will generally be in more controlled climates, but several environmental factors, such as electronic interference or vibrations, must still be taken into account.

Alarm Monitoring Systems

In addition to the off-the-shelf access control technologies that are discussed in this handbook, there is a variety of alarm monitoring systems available. State-of-the-art systems provide visual and audible indications of an alarm. Although each access control system is unique in the number and scope of the options available, all unmanned systems perform the basic function of annunciating alarms and displaying the alarm locations in some format.

Alarm Assessment

Assessing an access control system involves evaluating the alarm and analyzing audible and visual data to determine if an unauthorized access has been attempted or has occurred. The operator performs an assessment using closed circuit television, thermal imagery, and sometimes response force observation. Several control systems can automatically direct video or thermal imaging cameras toward a zone to provide the security personnel with a real-time view of the situation, to track the progress of an unauthorized access, and to hand off to adjacent monitoring and surveillance components as an intruder moves to other zones.

Integration

All access control technologies have vulnerabilities and can generate false acceptances or rejections. Generally, access control systems should be supplemented with multiple access control technologies to protect against the weaknesses of any one technology, to enhance the system's overall effectiveness, and to provide means for security personnel to assess alarms and attempts to gain unauthorized access.

Different access control devices can be integrated to reduce the chances of false acceptances and to provide alternatives for false rejections or inabilities to use a certain type of system.

Token and Cipher Systems: Cipher lock door systems are widely used for access control in areas that must support frequent movement of authorized users and occupants but exclude the general populace. Cipher locks control access using something an individual knows, rather than something an individual has (in token-based systems) or is (in biometric systems). Door lock systems of this type may be either mechanical or electronic. Mechanical cipher locks normally attach to the door itself, while electronic cipher locks may be mounted on the door or on a wall next to the door they control. Electronic cipher locks control an electric strike, striker plate, or latch, and are operated by pressing a combination of buttons or rocker switches. The buttons are often located behind a shield to prevent the combination from being observed. The buttons on a mechanical cipher lock are arrayed in a circle or a vertical line near the knob that moves the bolt once the lock has been released. This knob is known as a thumbturn or deadbolt lever.

Communications

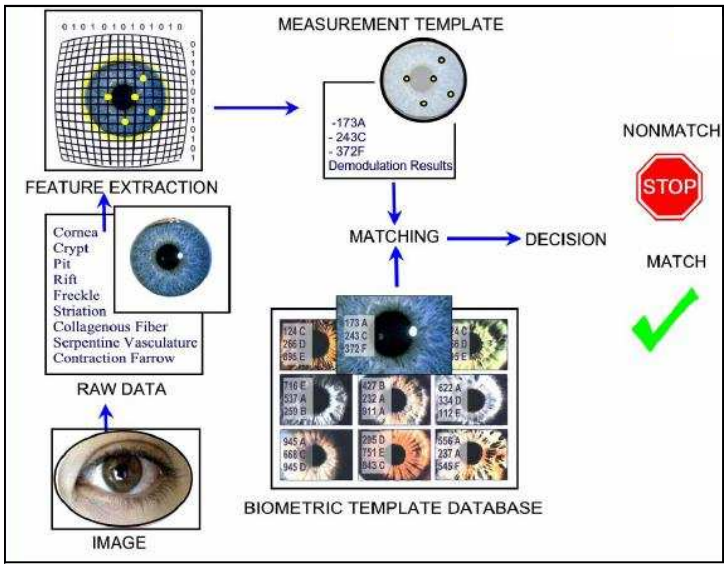
Communications between the command-and-control unit and the access control devices employ a variety of standard communications protocols. RS-485, RS-232, Frequency Shift Keying (FSK), and Dual Tone Multi Frequency (DTMF) dial are the most common. Occasionally a manufacturer will use a proprietary communications protocol that can limit the possibility for future upgrades and system expansions.

Power Supply

Regardless of the quality of design and installation, most access control systems are vulnerable to electric power losses. Some systems may not be able to reset automatically and would require operator intervention to restore. Potential intruders may be aware of these vulnerabilities and may seek to cut or interrupt power if they cannot circumvent the system by other means. It is critical that all elements of the system have backup power systems incorporated into the design and operation to guarantee the system's uninterrupted integrity, alarm reporting, situation assessment, and the response force's reaction.

Costs

The overall costs of an access control system are easy to underestimate and should be based on life cycle considerations. A vendor's bid may represent only the hardware cost, and may not include the costs of engineering design, installation, construction, training, or maintenance. Often the costs associated with infrastructure or the assessment and alarm reporting systems outweigh the costs of the access control components. Costs can be minimized by defining threats carefully, buying multiple types of systems, and selecting several technologies that provide similar categories of protection. Since infrastructure can also be a significant cost driver, using suitable existing infrastructure, such as power cabling or conduit, can help mitigate some costs. Upgrade costs can sometimes be mitigated by choosing equipment compatible with older systems or with parts of older systems.



Biometric Systems: Iris recognition and retinal scanning are two biometrics associated with the human eye that are often confused by the public. This is probably because retinal scanning is the eye-related biometric most often shown in movies. These are two completely different biometric technologies. In retinal scanning a visible light illuminates the retina, the back of the eye, from a close range and is considered by users to be intrusive. The iris recognition system takes an infrared picture of the iris, the colored part of the eye, from a distance of 3 to 18 inches. This is considered by users to be less intrusive.

Categories of Equipment

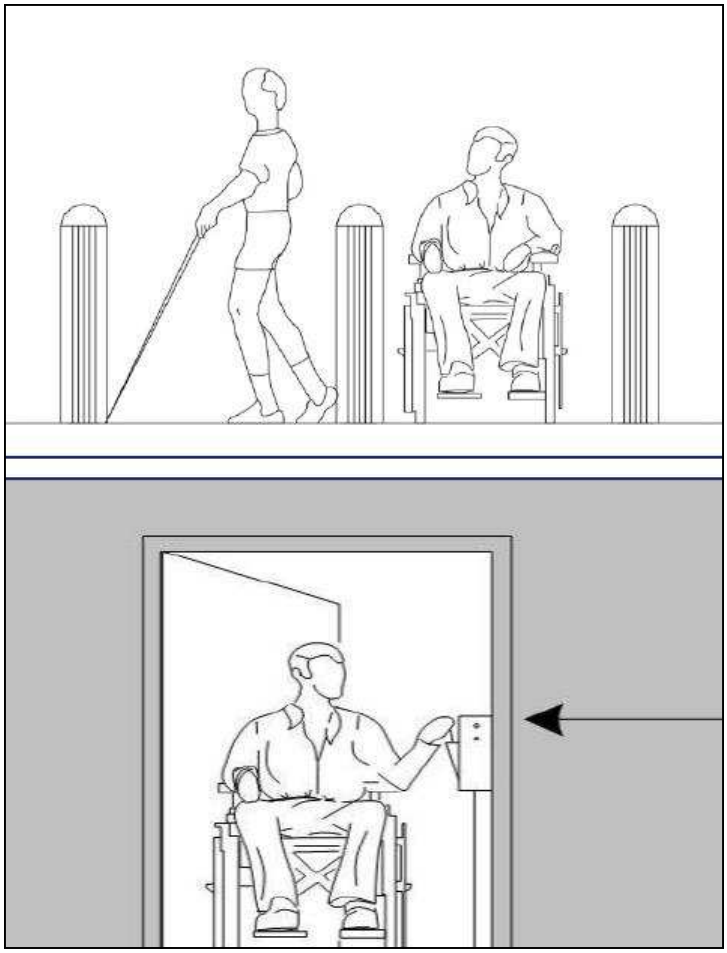
The access control equipment discussed in the *Handbook of Access Control Technologies* can be divided into four categories:

1. Physical control: Physical control equipment begins the access control process at a distance outside a facility's perimeter up to points of entry mainly by controlling vehicular movement near points of entry. The topics covered in the section on physical access control systems are barriers, bollards, turnstiles and portals, and guard facilities.

2. Tokens and cipher systems: Tokens are hand held or portable mechanical or electronic devices that facilitate authentication for the bearer to enter a protected space. Cipher locks perform the same function using a different method. The topics covered in the section on tokens and cipher systems are identification cards and badges, keycard door systems, cipher lock door systems, magnetic stripe cards, Wiegand cards, contact smart cards, contactless smart cards, and key fobs.

3. Biometric systems: Biometrics use physiological or behavioral data measurements to determine authorization for access. The topics covered in this section of the handbook are facial recognition, fingerprint recognition, hand/finger geometry, vein geometry, iris recognition, retina scan, voice recognition, and signature dynamics.

4. Assistive technologies: These technologies involve the use of alternative or specially designed equipment or implementation of systems to assure that personnel with disabilities can participate in the access control process.



Assistive Technologies: A broad definition of an assistive technology (AT) is any technology that enables someone to do something that they otherwise could not do. ATs use improved engineering designs and well-planned user interfaces to help disabled individuals achieve previously unreachable goals. Often, an AT is simply an existing device or technology that has been modified to suit the abilities of a handicapped individual or group. While there is no single AT that can meet the requirements for all disabilities, the operation of many existing access control systems can be improved with AT and applications of Universal Design principles, which strive for flexibility, intuitive operation, and tolerance of errors and faults. Disabled employees and other authorized facility users may be eligible to request "reasonable accommodations" under the Americans with Disabilities Act (ADA). A reasonable accommodation is essentially a request for an application of AT for a certain set of circumstances and specific purposes. AT is an important element of the design of any access control system.