# CHAPTER 3

# ACCESS CONTROL SYSTEMS

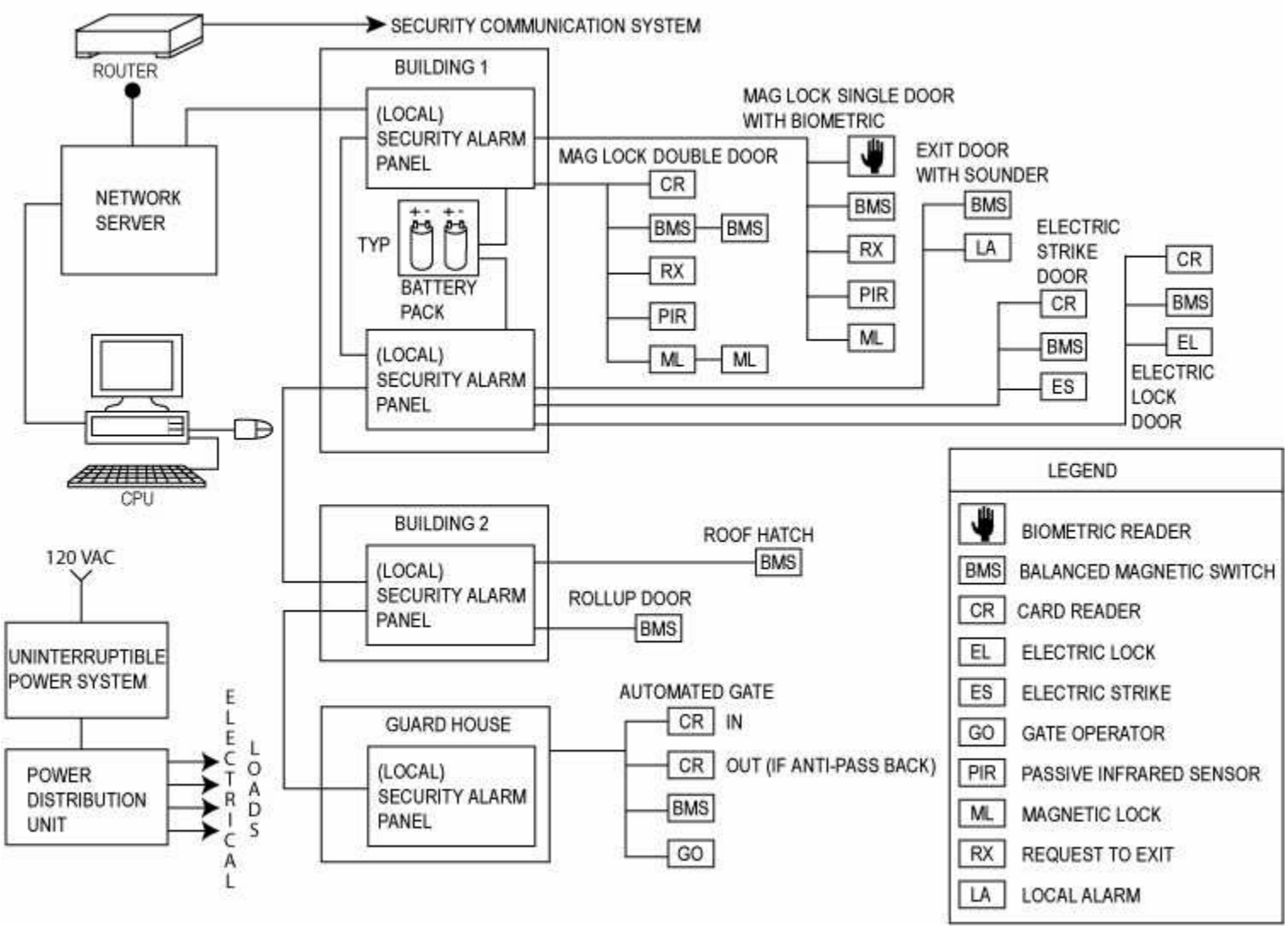
## 3-1 OVERVIEW

3-1.1 The function of an ACS is to ensure that only authorized personnel are permitted ingress and egress from a controlled area. The ACS should be able to log and archive all transactions and alert authorities of unauthorized entry attempts. ACS can be interfaced with the CCTV system to assist security personnel in the assessment of unauthorized entry attempts.

3-1.2 As illustrated in Figure 3-1, an ACS has many elements, including electric locks, card readers, biometric readers (when required, but not always part of every system), alarms, and computer systems to monitor and control the ACS. An ACS generally includes some form of enrollment station used to assign and activate an access control device. Detailed descriptions of the various elements of an ACS are described later in this chapter.

3-1.3 In general, an ACS compares an individual's credential against a verified database. If authenticated, the ACS sends output signals which allow authorized personnel to pass through controlled portals such as gates or doors. The system has the capability of logging entry attempts (authorized and unauthorized) that are archived. (Event and tracking logs are discussed in more detail in a subsequent subsection.) Typically the ACS interfaces with the IDS for input of digital alarm signals at access portals controlled by the ACS. An example of this would be "door forced" alarms at a card reader controlled door. Similarly, the ACS interfaces with the CCTV system in that cameras could be placed at remote gates to verify identity of entrants before manually actuating the remote gate. Signals from the ACS are communicated to the Dispatch Center through the transmission lines of the DTM. Further information on the specifics of ACS interfaces with the rest of the ESS are developed in Chapter 8, "ESS Subsystem Integration."

**Figure 3-1. Example Access Control System (ACS)**



## 3-2 ACS ENTRY-AUTHORIZATION IDENTIFIERS

3-2.1 ACS entry-authorization identifiers are grouped into three categories:

- Credential devices
- Coded devices
- Biometric devices

These devices operate on three basic techniques:

- Something a person has, such as a common access card (CAC), swipe card, or proximity card
- Something a person knows, such as a personal identification number (PIN)
- Something a person is or does, such as a biometric identifier

3-2.2 **Credential devices**. Credential devices identify a person as having legitimate authority to enter a controlled area. A coded credential (such as a plastic card or key) contains a prerecorded, machine-readable code. When the card or key is read, an electric signal unlocks the door if the prerecorded code matches the code stored in the system. A credential device only authenticates the credential; it assumes a user with an acceptable credential is authorized to enter. Various technologies are used to store the code within a card or key. The most common types of cards are described in more detail in the section *Card Types*.

3-2.2.1 Advantages and disadvantages of using credential devices are shown in Figure 3-2.

**Figure 3-2. Advantages and Disadvantages of Using Credential Devices**

**Advantages**

- Cards and card readers are reliable.

**Disadvantages**

- Cards can be lost or stolen.
- Some types of cards can easily be duplicated.

Each type of card and card reader has its own advantages and disadvantages. Refer to the subsections *Card Readers* and *Card Types* in the section *ACS Equipment* in this chapter for more on the advantages and disadvantages of each.

3-2.3 **Coded devices**. Coded devices such as a keypad or microprocessors operate on the principle that a person has been issued a code or PIN to enter into the device that will verify the authenticity of the code entered. Any person entering a correct code is authorized to enter the controlled area.

3-2.3.1 Advantages and disadvantages of using coded devices are shown in Figure 3-3. For information about the different types of coded devices see the section *Keypads and PIN Codes,* later in this chapter.

**Figure 3-3. Advantages and Disadvantages of Using Coded Devices**

Advantages

- Keypads are compact and easily understood.
- Different codes may be used to give access to different points and doors.
- Maintenance is easy.
- Keypads are not expensive. They are reliable and easily replaced or repaired. Little complex hardware is needed.
- No cards or tokens need be carried so there is nothing to lose.
- A duress code, known only to the user, can be input covertly if a legitimate person is forced to enter under duress.

**Disadvantages**

- Codes are easily passed on to other unintended or unwelcome visitors.
- The code can possibly be viewed by others and thus used for unapproved entry.
- Hands-free operation is not an option.
- The number of allowable unique codes can be limited. For example, a four-digit PIN only provides 10,000 different possible codes.

3-2.4 **Biometric devices**. Biometric devices rely on measurements of biological characteristics of an individual, such as a fingerprint, hand geometry, handwriting, voice, or iris patterns. Selected individual characteristics are stored in a device's memory or on a card, from which stored reference data can be analyzed and compared with the presented template.

3-2.4.1 A one-to-many or a one-to-one comparison of the presented template with the stored template can be made, and access granted if a match is found (depending on the authorized security level). There are two important acceptance results of which to be aware. They are *false reject* and *false accept*. False reject is denying entry to authorized personnel. This is inconvenient, but does not compromise security. False accept is granting access to non-authorized personnel. This is the most critical result, as highly-secure facilities cannot afford the error of a false accept. All ACS have some percentage of false positive (accept) alarm signals, ESS system designers should understand the issues and work to minimize the number of false positive (accept) events. From a logistics perspective, missions cannot be accomplished if false reject

rates are high and authorized personnel are regularly unable to enter their workspace or facility.

3-2.4.2 Advantages and disadvantages of using biometric devices to grant or deny access are shown in Figure 3-4. For information about the different types of biometric technologies, see the subsection *Biometric Readers* in the section *ACS Equipment* in this chapter.

**Figure 3-4. Advantages and Disadvantages of Using Biometric Devices**

Advantages

- They provide automated verification that the person attempting to gain access is authentic.
- Biometric credentials are extremely difficult to duplicate.

**Disadvantages**

- The cost is slightly higher.
- Longer verification time.
- Require special housings.
- Do not work well in exterior environments

3-2.5 **Combining credentials**. A site's security can be significantly enhanced by combining two or more types of automated access control credentials - such as a biometric characteristic with a smart card or a proximity card with a PIN code. However, combining credentials results in increased verification time and will decrease throughput rate. Throughput time should be considered when making decisions about whether or not to use redundant verification. Another consideration in combining two types of credentials is that a system can be required to use one device during lower risk times (such as during normally staffed times) and two devices can be required for entry after hours. The same philosophy can be applied for access control enhancement during times of heightened force protection threat levels. A risk assessment needs to be performed to help determine the degree or level of credentially.

3-2.6 **Identification Method Selection**. The type of identification method (card, PIN, biometric attribute or a combination thereof) that will be used needs to be determined early in the project. Identification of the existing ACS token media and system capacity should be assessed during project kickoff or the early programming phase. Per DoD Directive 8190.3, the CAC is the preferred card.

## 3-3 OTHER ACS IMPLEMENTATION CONSIDERATIONS

3-3.1 Other things to consider implementing as part of an ACS include anti-passback, anti-tailgating, the two-man rule, and performing event tracking. These are described in the following sections.

3-3.2 **Life Safety Code Compliance.** Anti-tailgating and anti-passback features must be consistent with the philosophy of the Life Safety Code and the Means of Egress for Buildings and Structures, unless specifically over-ruled by Government Authority.

3-3.3 **Anti-passback**. Anti-passback is a strategy where a person must present a credential to enter an area or facility, and then again use the credential to "badge out." This makes it possible to know how long a person is in an area, and to know who is in the area at any given time. This requirement also has the advantage of instant personnel accountability during an emergency or hazardous event. Anti-passback programming prevents users from giving their cards or PINs to someone else to gain access to the restricted area. In a rigid anti-passback configuration, a credential is used to enter an area and that same credential must be used to exit. If a credential holder fails to properly "badge-out", entrance into the secured area can be denied. Anti-passback is a standard feature for Commercial-Off-The-Shelf (COTS) access control systems and is typically disabled but can be enabled through software programming.

3-3.3.1 An alternative approach to "badging out," which is not as rigid as the process described above, is use of a time delay on entrance readers. In this design, the credential (Card or PIN) can not be reused within a prescribed minimum time period. This time delay feature can be programmed and set for a time period such as a half-hour. During the half-hour time period, the same card or PIN can not be used for a second entry. While affording some increased security, this process is not as rigid or secure as a 'badge-out" process.

3-3.4 **Anti-tailgating**. While not commonly required, a project security requirement may be to deter tailgating. Tailgating is the act of a person following another authorized person closely in order to gain ingress through the same portal when the authorized person's credential grants access. An example of a simple anti-tailgating requirement would be a pedestrian turnstile for access control. Since turnstiles are easily defeated, when significant, anti-tailgating measures are required, high-security vestibules or guard-controlled entrances can be a solution. Such application may slow down access.

3-3.5 **Two-man Rule**. The two-man rule is a strategy where two people must be in an area together, making it impossible for a person to be in the area alone. Two-man rule programming is optional with many identification systems. It prevents an individual cardholder from entering a selected empty security area unless accompanied by at least one other person. Once two token holders are logged into the area, other token holders can come and go individually as long as at least two people are in the area. Conversely, when exiting, the last two occupants of the security area must leave together using their tokens. Use of the two-man rule can help eliminate insider threats to critical areas by requiring at least two individuals to be present at any time. Most ACS software will enable the assignment of a *specific* second person that can be established (such as clearance escort requirement).

3-3.6 **Exit Technologies**. While access control is principally concerned with entry requirements, some consideration must be given to exit technologies and methods. Door hardware or locking mechanisms specified to enter access portals influence exit

hardware. Life safety codes in the United States dictate that personnel can not be locked in such that they are restricted from free exit. When an opening is locked from the public side and free exit is required from the secure side, there are several methods that can be employed as discussed below. Refer to Chapter 9 for more information.

3-3.6.1 The simplest door hardware is a “crash bar”. This strictly mechanical device merely requires exiting personnel to hit the “push-to-unlock” bar. If an electric strike is used as a door lock, generally the door has a twist door-knob handle that allows free exit.

3-3.6.2 If magnetic locks are used to secure the door than both an automatic and manual method of existing the door must be provided. Generally, the manual method is a Request to Exit button, sometimes abbreviated as a REX. When this device is pressed, power to the door locks is shunting allowing exit. The most common form of an automatic sensing device that will release the door lock when a person approaches a door in the exiting direction is a Passive Infrared Sensor (PIR). This device senses the infrared heat signature of a person and automatically shunts door lock power allowing free exit. PIRs have a significant security shortfall in that any person passing by or loitering in the sensing area of a the opening can activate the PIR and shunt door lock power. For this reason, magnetic locks should be the designer’s last choice for door locking mechanisms.

3-3.6.3 Card readers or keypads can be used for anti-passback, “badge out” procedures but require building code variance or approved special circumstances for locking an exit portal for a normal existing individual. Badge out card readers over more specific identification of existing personnel over keypads, where a number of individuals could have knowledge of the exit numerical code.

**Table 3-1 Exit Technologies (Pros and Cons)**

| | **Pros** | **Cons** |
|---|---|---|
| **Door Hardware** | Easy to implement<br>Cost effective<br>Simple | Does not “track” who left the facility or space.<br>No additional security. |
| **Request-to-Exit Button** | Slightly simpler to implement than keypads or cardreaders.<br>No additional Pros, typically mandated in U.S. by use of “mag locks” as door locking device. | Generally requires complementary automatic exiting devices such as a PIR.<br>No additional security.<br>PIRs can release the door lock if someone lingers in detection cone. |
| **Keypads** | Some additional security afforded in that exiting person needs to know the exit code. | Requires variance or alternate method to U.S. life safety code for exit doors.<br>Exit code can be shared.<br>Additional construction cost. |

| | | |
|---|---|---|
| **Cardreaders** | Can be used to achieve anti-passback function.<br>Allows tracking of exiting personnel by individual identification. | Requires variance or alternate method to U.S. life safety code for exit doors.<br>Extra construction cost and programming. |

3-3.7 **Event tracking/event logs**. Event tracking/event logs are lists or logs of security events recorded by the access control system that indicate the actions performed and monitored by the system. Each event log entry contains the time, date, and any other information specific to the event.

## 3-4 ACS EQUIPMENT

3-4.1 Once the type of identifier and other implementation strategies are determined, the type of equipment to use can be determined. Various types of ACS equipment are available, as described in the following sections.

3-4.2 **Badging Equipment**. When credentials have associated identification badges, ancillary badging equipment is needed. Note that besides the CAC issued to all government employees, supplemental badging may be required during CAC card implementation-transition or for certain restricted access facilities. The Activity must provide justification to support the requirement for any badging equipment. This equipment should be scrutinized before deciding to purchase. Badging equipment includes:

3-4.2.1 Camera for capturing photographs

3-4.2.2 Software for creating badge images

3-4.2.3 Signature capture tablet

3-4.2.4 Biometric template capture device (where applicable)

3-4.2.5 Badge printer capable of printing a color ID template on the front and back of the badge, and capable of encoding a magnetic stripe or smart card (where applicable). There are new technology printers that are capable of printing pseudo holograms on the clear protective laminate, which may be considered for higher security applications.

3-4.2.6 Computer for retention and programming of the security credential database. This computer may be a stand-alone or client workstation that is connected to the ACS server database in a client/server architecture.

3-4.2.7 Equipment to encode badges (depending on types of badges). The badge printer may be equipped with a magnetic stripe encoder or a separate stand-alone magnetic stripe encoder or both may be necessary where required. The new GSC-IS V2.1 contactless technology tokens require a card reader/writer to encode (not encrypt) the token. For more information, refer to the *Government Smart Card Interoperability Specification.*

3-4.2.8 If there is no existing badging location and equipment, the design must include the badging infrastructure described above as well as space allocation for equipment and storage requirements.

3-4.2.9 Badging may require an interface to an existing personnel database where the necessary information is stored and maintained. If so, requirements for this database interface and security must be established

3-4.3 **ACS Central Processing Unit (CPU)**. The CPU is the physical intelligent controller(s) where the ACS application software and database reside and where all ACS system activity is monitored, recorded into history, commanded and controlled by the operator. Examples of ESS CPU's include: microprocessors, servers, programmable logic controllers (PLCs), or even personal computers (PCs). Conceptually, the CPU can be thought of as the "brain" of the ACS system. Formerly, the CPU was a discrete component located at the "head-end" of the system, typically the Dispatch Center. Current state-of-the-art ACS use distributed intelligence that allows each local security panel to hold (in microprocessor memory) the system logic for its associated devices. The CPU retains the system specific programming for "action/reaction" logic steps necessary for an ACS to allow entry (access) for authorized personnel and deny access to unauthorized personnel. A sample sequence is shown in Figure 3-5.

3-4.3.1 Communications failure between the CPU and the local access control processor equipment could result in new users not being permitted entry. Additionally, during any communication failure, users who are no longer authorized will still be able to enter the area. It is important to provide sufficient backup power capability for the CPU, local processors, and other critical infrastructure to prevent the loss of control of authorized access. Redundant, fault-tolerant communication systems are required in high-security areas where loss of communications (including partial links) cannot be tolerated.

3-4.3.2 A specialized case of a CPU is a Premises Control Unit (PCU). A PCU is a DCID 6/9 term used to describe a specific controller located within the confines of a Sensitive Compartmented Information Facility (SCIF). Per the *Physical Security for SCIFs:* "A PCU is a device that receives changes of alarm status from IDS sensors, and transmits an alarm condition to the monitoring station." The PCU resides in an internal location, safe from external tampering and controls and monitors ESS equipment for the protected area as shown in Figure 3-6.

**Figure 3-5. Basic Access Control Sequence**

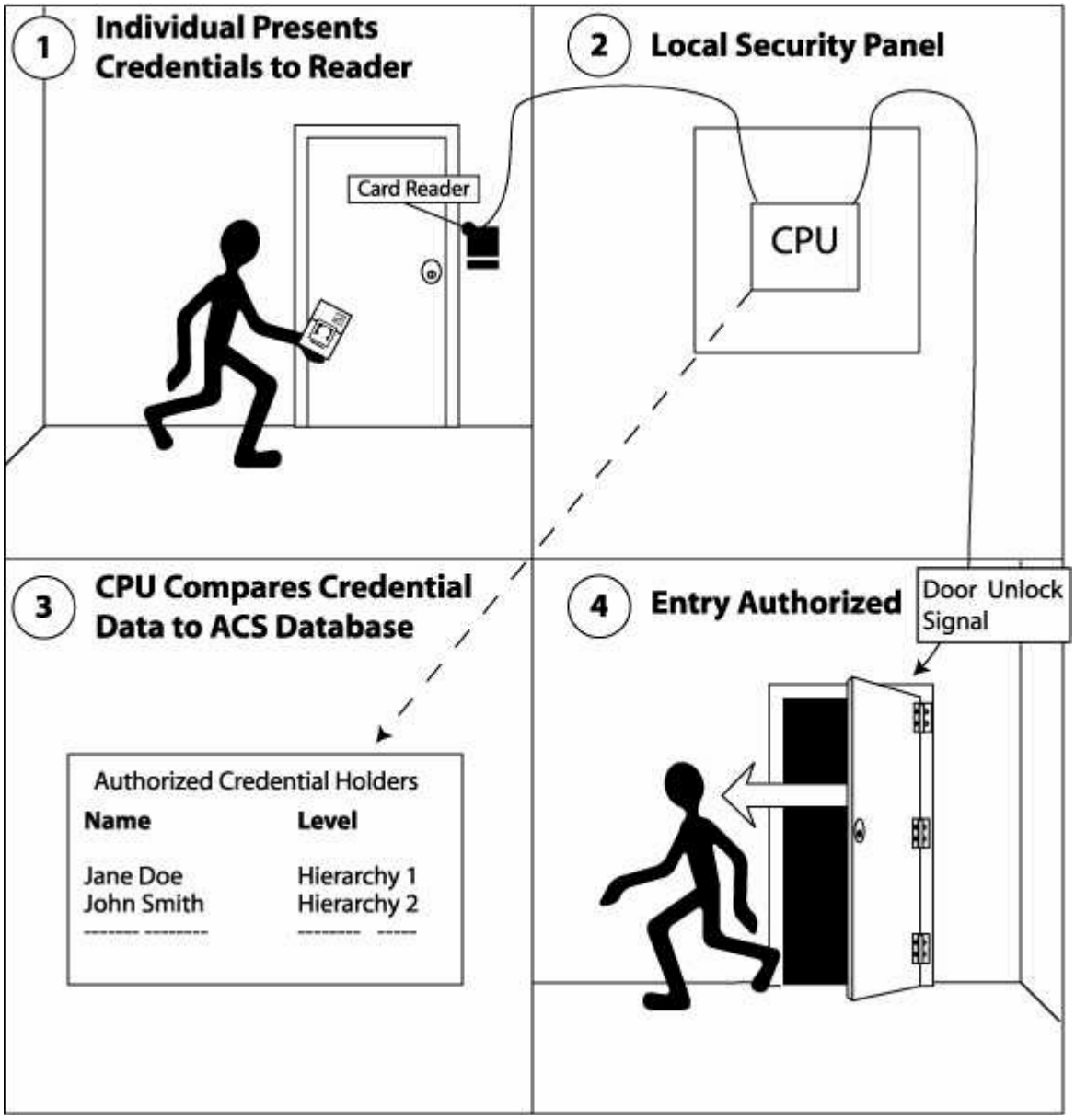
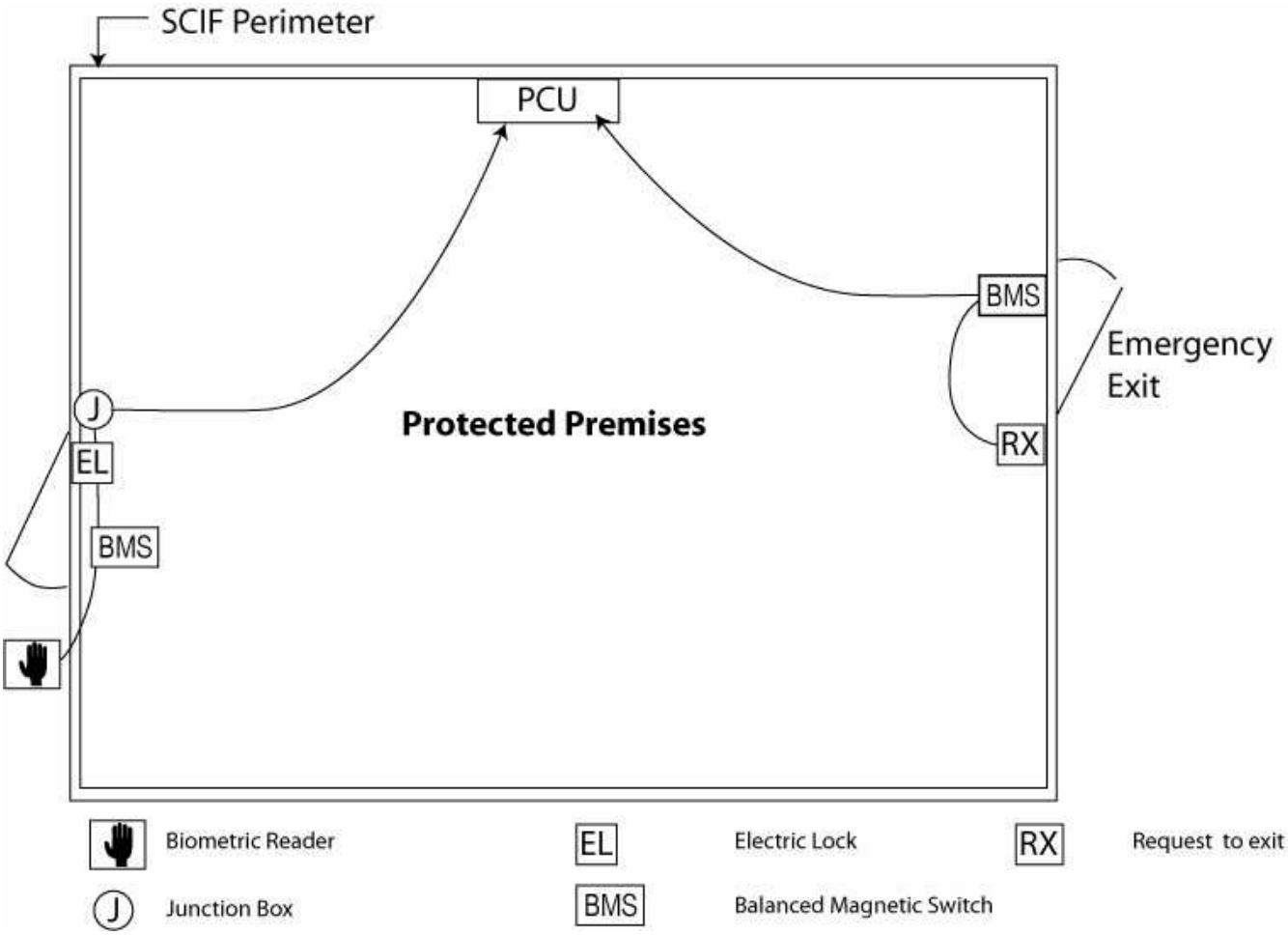


**Figure 3-6. PCU In A SCIF**




3-4.4 **System Display**. The system display is the screen or monitor that allows personnel to view and interact with the ACS hardware and software. Typically, it is a computer screen. The location of the system display should be identified early in the design process. The system display and control can be anywhere a computing device is connected to the network. The software can reside on any computing device (preferably a server) and be accessed by anyone connected to the network provided they have access rights to the software. Furthermore, it can be made accessible to the Dispatch Center. This means that existing computer systems can be used when integrating the system. Contact the base security and communication office (information technology) for system capacity issues and coordination.

3-4.5 **Security Alarm Panels**. Security alarm panels collect inputs from card readers, biometric devices, door sensors, and so on. and provide output signals to electronic door locks, electric strikes, or gate operators. Security alarm panels are connected to the CPU that provides the database intelligence for determining whether to grant or deny access. Newer security alarm panels incorporate the following features:

3-4.5.1 Multiple connection methods such as dial-up modem, serial (RS-232), multi-drop (RS-485), and network TCP/IP.

3-4.5.2 Integrated CCTV camera connectivity, allowing CCTV camera information to be shared with the ACS.

3-4.5.3 Capability for asset tracking within a facility, such as with radio frequency identification (RFID) tags connected to critical assets.

3-4.5.4 Capability for incorporating duress or panic alarm capability.

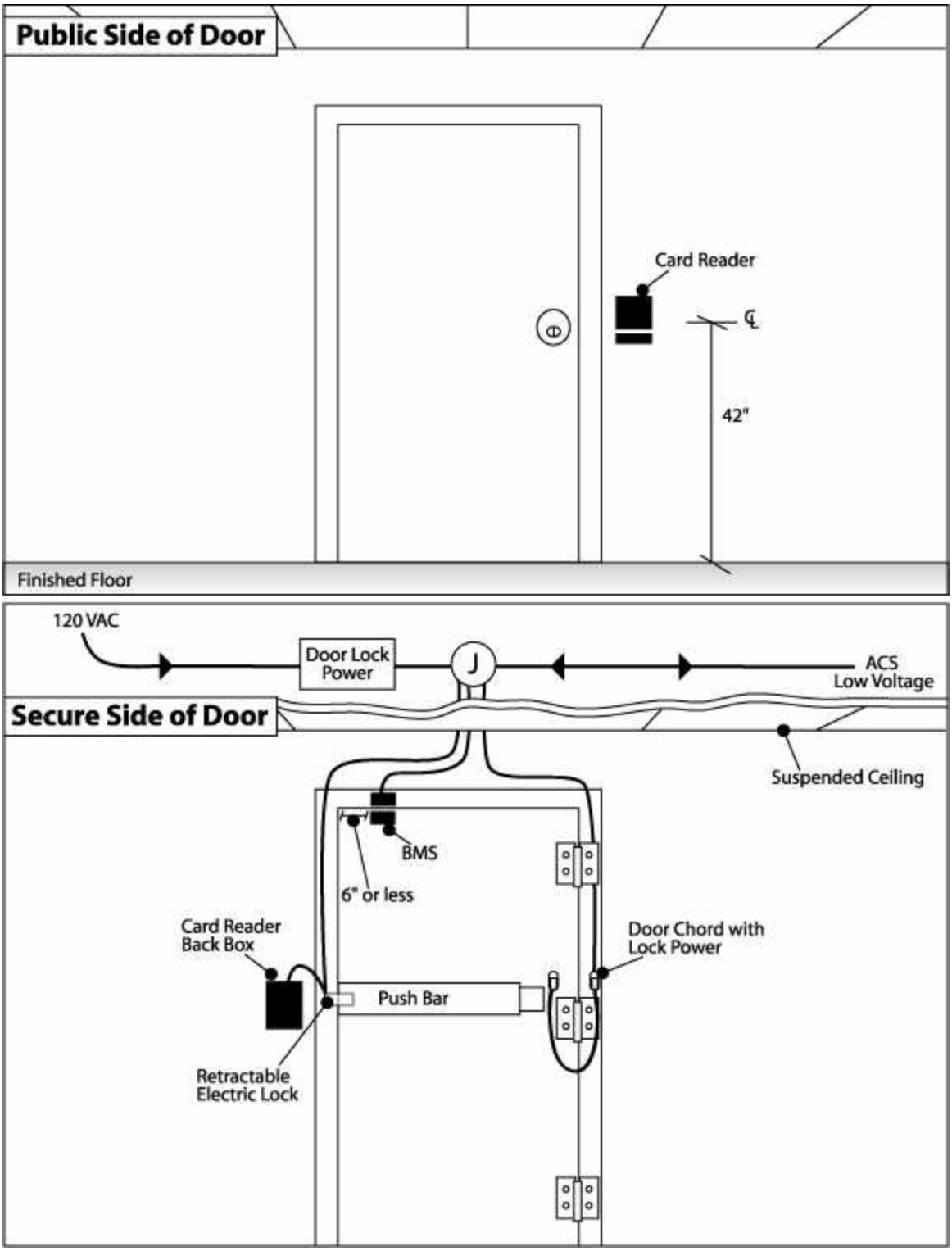
3-4.6 **Card Readers**. The most common form of credential verification is a security card reader.

3-4.6.1 **Types of Card Readers.** There are a number of different types of card readers**.** Insertion readers require that you insert the card into a slot that is just large enough to accommodate the card and then remove it. Swipe readers require that you swipe the card through a long narrow slot that is open at each end. Proximity and contactless readers require that you hold the card in front of the blank face of the reader.

3-4.6.2 Insertion and swipe readers, while functional, are older technologies; however, at this writing the use of the CAC requires use of the insertion type magnetic stripe reader or a bar code reader. Insertion or swipe readers require the credential to be inserted into the reader and the card can wear out over time. Once the CAC is converted to a contactless read capability, use of insertion or swipe readers should be an unusual design for new projects because of the dated technology. Until the CAC is converted to contactless read capability, the insertion magnetic stripe reader is preferred over the bar code reader, which is more easily compromised. Proximity readers are popular and require the user to pass the card within an adjustable distance (one to two inches from the reader). While commonly used in commercial non-DoD applications, testing has demonstrated that it is possible to intercept the unencrypted (125kHz proximity card) signals. Smart cards are also wireless, contactless credentials that can be read in close proximity to a smart card reader.

3-4.6.3 Figure 3-7 displays a typical configuration for a single door equipped with a card reader and electric lock. Refer to the subsections on *Doors* and *Door Locks* in Chapter Nine, General Requirements and Cross-Discipline Requirements for additional information on door hardware types and interface considerations.

**Figure 3-7. Sample Card Reader Door Configuration**



3-4.7 **Card Types**. Card readers use a number of different card types, the most common in use are described in the following subsections.

3-4.7.1 **Magnetic Stripe Cards**. Magnetic stripe (mag stripe) cards consist of a magnetically-sensitive oxide strip fused onto the surface of a PVC material. They are inexpensive, easily manufactured, and can carry alphanumeric data. (Magnetic cards used within the DoD should comply with SEIWG-012, which specifies numeric data only.) A magnetic stripe card is read by swiping it through a reader or by inserting it into a position in a slot. A magnetic stripe card can be individualized by color coding the cards and printing photo information onto them. The magnetic stripe card is disadvantaged in that it may be physically damaged by misuse and its data can be affected by magnetic fields, even when they are of only low potential. Other problems associated with this type of card are related to the high volume of equipment available for the reading and copying of cards so that unauthorized duplication and copying can never be entirely negated.

3-4.7.2 **Proximity Cards**. Proximity cards (prox cards) use embedded antenna wires connected to a chip within the card. The chip is encoded with the unique card identification. Currently, the standard proximity card operates at a frequency of 125kHz. Distances at which proximity cards can be read vary by manufacturer and installation. Readers can require the card to be placed within a fraction of an inch from the reader to six inches away. Having the card out and at the same height of the reader, background electrical interference levels, and sensitivity of the reader affect the distance at which a card can be read. Proximity card technology (125kHz) should not be confused with wireless, contactless (13.56MHz) technology.

3-4.7.3 **Wiegand Cards.** The following information is cited from *Effective Physical Security (page 196):*

> The Wiegand card is also called an embedded-wire card. The technology is based on the Wiegand Effect, a phenomenon observed when specifically prepared ferromagnetic wires suddenly reveres themselves on exposure to an external magnetic field. Wires inside the Wiegand card are formed in a permanently tensioned helical twist. The order and spacing of the wires establish a unique code for each card. The magnetic reversals in the wires are converted into distinct, consistent electrical pulses that are read and processed. The card's thickness and stock composition make it resistant to pocket damage; however, it is susceptible to malfunction arising from wear after many passes through reader slots. The card is moderately priced, but capable of storing a moderate amount of data.

3-4.7.4 **Smart Cards**. Smart cards are credential cards with a microchip embedded in them. The term "smart card" can define cards that simply carry data, but more commonly is used describe cards with integral microprocessing and read/write data storage capability. Smart cards are available as a "Contact" type or more commonly as a "Contactless" (and wireless) type. An example of a "Contact" smart card is one which can interface to a computer through the embedded contact. The contactless, wireless

smart card operates at 13.56 MHz, which is more than a hundred times faster than the data exchange rate of 125kHz proximity cards. There are also hybrid cards available, which have either both types of smart card chips in one plastic body or have both contact and contactless interfaces to one microprocessor in the plastic body. Smart cards can store enormous amounts of data such as access transactions, licenses held by individuals, qualifications, safety training, security access levels, and biometric templates. One principal security advantage of smart cards is that cryptographic capabilities can be used to send card information to legitimate readers and encrypts that transmission such that the system remains immune from replay attacks. It is difficult to copy security credential information onto a forged card. For more information on the federal standard for electronic smart cards, refer to NIST FIPS 201.

3-4.7.5 **Common Access Card (CAC)**. The CAC is a credential used by the DoD to allow access to DoD computers and physical locations worldwide. For each individual, one card works for all access to computers and physical locations. The CAC is a JAVA-based smart card. It can store a number of personal demographic data elements. It supports multiple bar codes and a magnetic stripe for legacy applications, making the card extremely versatile. A standard developed by the Security Equipment Integration Working Group, SEIWG-012, provides details on the formatting of the information to be encoded on track two (2) of the magnetic stripe of the CAC. SEIWG's intent is to ensure that cards can store enough data to determine information such as the individual cardholder, the branch of the military from which the card was issued, and the base from which the card was issued.

Per DoD Directive 8190.3, the CAC should be "the principal card enabling physical access to buildings, facilities, installations, and controlled spaces. This policy does not require DoD components to dismantle immediately current access systems, or preclude the continued use of supplemental badging systems that are considered necessary to provide an additional level of security not presently afforded by the CAC (e.g., such as entrance into a SCIF or other high security space). The DoD plan is to migrate to the CAC for general access control using the CAC's present or future access control capabilities. In the future, CACs will be contactless (13.56 MHz) compliant with ISO 14443 and NIST 6887 (Government Smart Card Interoperability Specification). This technology is proposed to be included in the next generation of CAC. For more information on the Government smart card program, refer to Http://smartcard.nist.gov/.

Since the CAC is not fully implemented, an additional badge may be required for dependants, contractors, temporary employees, host-nation workers or when an additional card provides an added capability not currently provided by the CAC.

3-4.7.6 **Operational Strategies.** Operational strategies for badge policy such as where the badge is worn, the type of photograph (if required), backgrounds for area authorization, rules of challenge, penalties for not wearing, and losing are important but are not within the scope of this design guide.

3-4.7.7 **Card Reader/Card Type Recommendation**. New projects should consider new technology smart cards and the CAC. Magnetic stripe readers used with the CAC

allow the use of the encoding format defined in the SEIWG-012 standard (described in the previous section *Magnetic Stripe Cards*).

3-4.8 **Keypads and PIN Codes**. Coded devices use a series of assigned numbers commonly referred to as a PIN. This series of numbers is entered into a keypad and is matched to the numbers stored in the ACS. By itself, this technology does not offer a high level of security since a PIN can be stolen by even casual observation. However, coded devices can be effective when used in combination with another credential reading technology. Coded devices include electronic keypads and microprocessor-controlled keypads.

3-4.9 **Biometric Readers**. Biometric readers verify personal biological metrics (biometrics) of an individual. Biometric readers may be used in addition to credential devices or with a PIN code.

3-4.9.1 Biometric devices have uses at access control points, but may not be mature enough to use in throughput-critical applications such as vehicle entry gates. Designers have to evaluate the tradeoff between added security and decreased throughput.

3-4.9.2 Biometric readers are the future trend of security systems. Current gains in large-scale production of some types of biometric readers have brought biometrics close in cost to conventional card readers. Although biometrics are not as fast as other readers, these technologies are still evolving.

3-4.9.3 There are several types of biometric characteristics that can be used. The most common are described in the following sections.

3-4.9.3.1 **Fingerprint**. Fingerprint technology scans the loops, whorls, and other characteristics of a fingerprint and compares it with stored templates. When a match is found, access is granted (depending on the authorized security level). Advantages of fingerprint technology are that it is easily understood. Disadvantages are that the systems can be disrupted if cuts or sores appear on fingers or if grease or other medium contaminates the fingers and the scanning plates. Some systems create two templates for two different fingers, in the event that one finger is altered by injury or other means. Fingerprint technology is not convenient in environments where workers wear gloves. Early fingerprint readers were compromised by picking up a valid fingerprint from a reader with a manufactured “finger”. To combat this shortcoming of the technology, sensors were equipped with the ability to sense a pulse and temperature. Fingerprint technology is the first choice biometric method per the emerging FIPS201.

3-4.9.3.2 **Facial Image.** This technology measures the geometric properties of the subject’s face relative to an archived image. Specifically, the center’s of the subject’s eyes must be located and placed at precise (within several pixels) locations. Facial imaging is the backup technology for biometric authentication per FIPS 201.

3-4.9.3.3 **Hand Geometry**. This technology assesses the hand’s geometry: height, width, and distance between knuckle joints and finger length. Advantages of hand

geometry are that the systems are durable and easily understood. The speed of hand recognition tends to be more rapid than fingerprint recognition. Hand recognition is reasonably accurate since the shape of all hands is unique. A disadvantage is that they tend to give higher false accept rates than fingerprint recognition. As with fingerprint technology, hand geometry is not convenient in environments where workers wear gloves.

3-4.9.3.4 **Handwriting**. Handwriting recognition analyzes the pressure and form of a signature. This technology is only used in an ACS without heavy traffic because the procedure of verification is slow. A PIN is typically entered into the system first so that the computer can more quickly find a template against which to identify the person seeking entry. Handwriting systems are not widely used.

3-4.9.3.5 **Voice Recognition**. Voice recognition identifies the voice characteristics of a given phrase to that of one held in a template. Voice recognition is generally not performed as one function, and is typically part of a system where a valid PIN must be entered before the voice analyzer is activated. An advantage of voice recognition is that the technology is less expensive than other biometric technologies. Additionally, it can be operated hands-free. A disadvantage is that the voice synthesizer must be placed in an area where the voice is not disturbed by background sounds. Often a booth has to be installed to house the sensor in order to provide the system an acceptable quiet background. Voice recognition systems are not widely used.

3-4.9.3.6 **Iris Patterns**. Iris recognition technology scans the surface of the eye and compares the iris pattern with stored iris templates. Iris scanning is the most accurate and secure biometric. After DNA, irises are the most individualized feature of the human body. Even identical twins have different irises, and each person’s two irises differ from each other. The unique pattern of the human iris is fully formed by ten months of age and remains unchanged through a person’s lifetime. A benefit of iris recognition is that it is not susceptible to theft, loss, or compromise, and irises are less susceptible to wear and injury than many other parts of the body. Newer iris scanners allow scanning to occur from up to ten inches away. A disadvantage of iris scanning is that some people are timid about having their eye scanned. Throughput time for this technology should also be considered. Typical throughput time is two seconds. If a number of people need to be processed through an entrance in a short period of time, this can be problematic.

3-4.9.3.7 **Retinal Scanning**. Retinal scanning is an older, comparable technology that reads the blood vessel pattern on the retina in the back of the eye, but it is not readily available in the marketplace. Whereas iris scanners can work up to ten inches from the reader, retinal scanners require individuals to look into a device that shines a harmless infrared light into the eye. Hesitance to look directly into such a reader has curtailed the acceptance of retinal scanners in most applications.

## 3-5 ACS DESIGN GUIDANCE

3-5.1 **GENERAL**. The DoD is currently migrating to the CAC. New access control system designs should be based on the CAC as the primary access control credential. Designer options for new systems are:

3-5.1.1 Current CAC technology

3-5.1.2 Future CAC technology (contactless)

3-5.1.3 Bometrics.

3-5.2 **CONSIDERATIONS**. When designing an ACS the following should be considered:

3-5.2.1 Do not design an ACS based around a single access control credential.

3-5.2.2 A coded credential alone does not offer sufficient security.

3-5.2.3 At a minimum, all card readers must be equipped with a keypad.

3-5.2.4 All card readers must be UL 294 listed and CE certified.

3-5.2.5 Contactless card readers must conform to ISO 14443 Parts 1 through 4 and NIST IR 6887, The Government Smart Card Interoperability specification (GS-IS).

3-5.2.6 For facilities requiring a higher degree of security, provide biometric capability in addition to the minimum.

Per FIPS 201, fingerprint reading is the biometric technology of choice.. Facial imaging is listed as a secondary biometric credential.

3-5.2.7 Retina scanners should not be considered as they are being phased out of the marketplace.

3-5.2.8 Outside hand-geometry readers require special exterior housings. Check with manufacturer’s specifications for external applications on other biometric readers.

3-5.2.9 A common cable type for card readers is a twisted, shielded cable (typically, six conductor). One pair is used for low voltage dc power, one pair is used for data transmission, and one pair is normally used for LED or signal illumination. Verify the cable requirements with the equipment manufacturer.

3-5.2.10 Coordination with Building or Project Architect:

3-5.2.11 In general, the ESS designer must balance security requirements with life safety, fire-alarm interface, and normal operational convenience factors.

3-5.2.12 Exits and entrances should be separated.

3-5.2.13 Avoid using a life safety emergency exit as a high security entry portal.

3-5.2.14 Limit entrances into the controlled area. SCIFs are limited to one primary entrance.

3-5.2.15 Coordinate with the Architect to ensure proper doors, door frames, and door hardware are provided. For example, when an electric strike is specified, the door and door frame should be checked or specified such that it supports the electric strike (capable of routing cables and so forth).

3-5.2.16 Consider throughput and traffic low of normal operational traffic and emergency exiting requirements. Combined credentials may result in a decrease in the false acceptance rate but will increase verification time and decrease the throughput rate.

3-5.2.17 Decide early if there are special exit technology or egress monitoring needs. Special exit technologies (request-to exit buttons or cardreaders) require life safety code consideration and additional door hardware coordination.

3-5.2.18 Additional design guidance for ACS is provided in Figure 3-8.

**Figure 3-8. ACS Design Process**