10/4-7-94 95(1)

SANDIA REPORT

SAND93—2030 • UC—706
Unlimited Release
Printed December 1993

Overview of Locking Systems

K. T. Gee, S. H. Scott, M. G. Wilde, S. E. Highland

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000

MASTER

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A06
Microfiche copy: A01

SAND93-2030
Unlimited Release
Printed December, 1993

Distribution
Category UC-706

Overview of Locking Systems

K. T. Gee
Surety Technology Department II

S. H. Scott
Access Delay Technology Department

M. G. Wilde
Surety Technology Department II

Sandia National Laboratories
Albuquerque, NM 87185

S. E. Highland
Albuquerque Safe Company
Albuquerque, NM 87107

Abstract

The purpose of this document is to present technical information that should be useful for understanding and applying locking systems for physical protection and control. There are major sections on hardware for locks, vaults, safes, and security containers. Other topics include management of lock systems and safety considerations. This document also contains notes on standards and specifications and a glossary.

This work has been sponsored by the
DOE Office of Safeguards and Security
under tasking SNL86005-93.

Contents

Figures

Tables

Acknowledgements

The authors wish to acknowledge Priscilla A. Dwyer of the Nuclear Regulatory Commission for permission to use NUREG/CR-5929, Locking Systems for Physical Protection and Control, as a basis for this document.

The authors also wish to acknowledge Pat Romero and George Perry of Bill's Lock and Key, Albuquerque, and Kenneth G. Adams, Kenneth R. Ludwick, and other Sandia technical experts for their excellent assistance in preparing this document.

1 Introduction

1.1 Purpose

This document is a summary of technical information that is useful in implementing locking systems for physical protection and control. The purpose is to help security personnel to make informed decisions on lock selection and management.

The primary emphasis is on lock technologies. For each technology, there is a section on uses, hardware description, application considerations, and standards and specifications. In addition, some related security issues are discussed. These issues include vaults; safes and security containers; management of lock systems; and safety considerations of locks.

To keep this document unclassified, a very limited discussion of vulnerabilities and inspection techniques is presented.

1.2 DOE Requirements

Title 10 of the Code of Federal Regulations encompasses all Federal Agencies and Departments dealing with energy. Within Title 10, Chapters 2, 3, and 10 are pertinent to the Department of Energy (DOE). DOE Orders are written to establish DOE internal requirements to meet the requirements of Title 10. Summaries of some of the DOE Orders concerning physical security follow this Introduction.

DOE requirements are not addressed in the technical portions of this document. Discussion of equipment or systems does not constitute acceptance or endorsement by DOE. The included summaries of DOE Orders may provide guidance toward applicable DOE requirements. For complete information on the requirements, the appropriate DOE Orders should be acquired.

References:

DOE Order 5632.1B - Protection Program Operations

This Order establishes DOE policies for protection of security interests and standards of protection which must be met. Six specific areas are identified:

- Physical Protection of Special Nuclear Material and Vital Equipment;
- Physical Protection of Classified Matter;
- Physical Protection of Departmental Property and Unclassified Facilities;
- Protective Forces;
- Systems Performance Tests;
- Issuance, Control, and Use of Badges, Passes, and Credentials.

This Order is the authority for the Protection Program Operations. It establishes both the authority and responsibilities of managers and a framework for the DOE 5632 series of orders. The DOE 5632 series of orders defines the policies and baseline requirements of related aspects of the Protection Program Operations. Basic definitions are given for some terms such as Security Container, Safe, Vault, Vault-type Room, and Special Nuclear Material Vault.

DOE Order 5632.1B refers to other DOE Orders which describe specific security requirements for the six areas above.

Protection Program Operations, Standards and Criteria

This document addresses five major activities of the Protection Program Operations:

- Physical Protection of Special Nuclear Material and Vital Equipment;
- Physical Security of Classified Matter;
- Physical Protection of DOE Property and Unclassified Facilities;
- Protective Forces;
- System Performance Tests.

This is a set of general specifications for meeting DOE requirements and testing the implementation for compliance. For each specification, appropriate DOE Orders are referenced, as well as Federal/Military/Commercial standards. Protection requirements are ranked by classification or sensitivity level, as well as potential public risk in case of loss or theft.

Examples of specifications found in this document are those that address general facility design, such as the quality of hardware used in securing facilities; monitoring devices and alarm systems; security containers, vaults, and vault-type rooms (including locks, hasps, and hardware); backup power supplies for security systems; and control of combinations and keys. Quotes from applicable DOE Orders are included.

DOE Order 5632.2A - Physical Protection of Special Nuclear Material and Vital Equipment

This Order establishes DOE policies for protection of Special Nuclear Material and Vital Equipment. Security requirements for Special Nuclear Material differ depending on quantities involved. Category I quantities of Special Nuclear Material are treated in the most restrictive fashion, followed by Categories II and III. Included are requirements for usage/processing areas, storage areas, and transport.

DOE Order 5632.5 - Physical Protection of Classified Matter

This document states requirements for handling classified material, as opposed to classified information. This material may be Special Nuclear Material (SNM), or other material which is classified because of its physical configuration. If the classified material is also SNM, the minimum protection allowed is that required for SNM or that required by this Order, whichever is more restrictive. Requirements are stated for the use, processing, storage, and transport of classified material.

Under the sub-paragraph which addresses Security Containers, definitions are provided for Security Cabinet, Safe, Vault, and Vault-type Room. A requirement is stated that built-in combination locks used with Security Containers must meet Underwriters Laboratories Standard 768, Group 1R, or other standards which provide equivalent protection.

DOE Order 5632.6 - Physical Protection of DOE Property and Unclassified Facilities

This document establishes basic criteria for protection of unclassified facilities and access control for them. Attention is given to providing reasonable security measures, including monitored access control, physical barriers, keys and locks, and intrusion detection and mitigation. This Order specifies that locks are to be resistant to opening with a jimmy or wedge, and that keys or combinations are to be controlled.

DOE Order 5635.1A - Control of Classified Documents and Information

The majority of this Order addresses general security precautions for guarding Classified Documents. Areas addressed include authorities for original classifiers; security reports; and preparation, marking, and destruction of documents. Chapter VII addresses security container requirements for storage of classified documents, and Chapter XI adds caveats concerning recording combinations of security containers used for storage of Top Secret documents. In both Chapters VII and XI, requirements are stated for a central record of lock combinations.

DOE Order 5635.2B - Protection of Classified National Security Council Information

This document addresses protection and handling of National Security Information (NSI) when in possession of DOE and its contractors. Storage of NSI is permitted in DOE security containers which are approved for the DOE equivalent classification level.

DOE Order 5635.4 - Protection of Unclassified Controlled Nuclear Information

Guidance is provided in handling, transport, storage, and dissemination of unclassified controlled nuclear information. In a controlled area, an unlocked desk or file cabinet is acceptable; in an area which is not controlled, a minimum of a locked desk or file cabinet is required.

DOE Order 6430.1A - General Design Criteria

DOE Order 6430.1A is broken into several sub-parts called 'Divisions.' Each division addresses a different area of facility design, planning, and construction.

Division 1 is titled 'General Requirements' and lists names, reference numbers, and sources for standards and specifications for planning and construction of all DOE facilities. Section 110-13 addresses Physical Protection requirements for all DOE facilities, including requirements for Access Control and Security Areas; Property Protection Areas; Limited Areas; Exclusion Areas; and Protected Areas, Material Access Areas, and Vital Areas. Physical Barriers, Intrusion Detection, and Communications are also addressed. This section also specifies that facility designs will adhere to the Life Safety Code, NFPA 101. Additional requirements for Special Facilities, including Vaults and Vault-type Rooms, are addressed in Section 110-99.

Division 8 is titled 'Doors and Windows' and specifies which building codes must be met in facility design. Attention is given to NFPA 101, the Life Safety Code, which provides for emergency egress from areas of danger. Requirements for door and window hardware are referenced, including general hardware and security/locking hardware. This extends to combination locks, combination and key padlocks, key locks, panic locks, and magnetic locks.

Division 13 is titled 'Special Facilities' and covers Nuclear Facilities and Explosives Facilities. Section 1300-10 addresses Physical Protection for Special Nuclear Material and

Vital Equipment. Attention is given to requirements for monitoring access and storage areas with intrusion alarms, including requirements that backup power be supplied and that installations be both tamper resistant and tamper indicating.

The Glossary of the document contains a reference of terms and abbreviations, including definitions of SNM Vault and Vault-type Room.

These documents are available from the DOE/Office of Safeguards & Security (DOE/OSS) or the DOE/Office of Security Evaluations (DOE/SE).

2 The Role of Locking Systems in Physical Protection and Control

Four elements form the foundation for an effective physical protection system. These elements are

(1) detection and assessment systems that detect and verify any unauthorized intrusion attempt by outsiders or any serious malevolent acts by insiders or outsiders;

(2) communication systems which ensure that all pertinent information is transferred to the point(s) where appropriate action can be taken;

(3) delay systems that impede continued adversary penetration into, or exit from, the area being protected; and

(4) response systems, or forces, that counteract adversary activity and neutralize the threat.

These elements are equally important and none of them can be eliminated or compromised if an effective physical protection system is to be achieved. Detection, which encompasses not only intrusion detection but also entry control, is an important element since any delay scheme can be penetrated eventually. Without detection, the response force would not be alerted. Communication systems are necessary to make sure that the right people have accurate and timely information. Delay elements should provide sufficient time after detection for communication and arrival of the response force. Finally, the response force should be adequately prepared to neutralize adversary actions.

Locks are important elements in the delay system of a facility since they secure the moveable portions of barriers. However, no lock should be depended upon as a stand-alone means of physical protection. Given sufficient skill and time, all locks can be defeated.

In all applications, the design goal is to have the lock-delay capability match the penetration resistance of the rest of the secured barrier. It does not make sense for either security or economic reasons to select a lock which is either significantly stronger or weaker than the rest of the barrier.

3 Lock Technologies

The purpose of this section is to provide detailed information on commercial lock technologies. This includes the basic design and its variations, uses, pros and cons, design features which affect security, and standards and specifications. This information is supplied for key locks; combination locks; mechanical and electrical bolts, strikes, and latches; mechanical coded locks; electromagnetic locks; and self-contained electronic locks. The Hirsch Electronics access control systems are also covered because they are important to DOE.

The time and skill required to defeat a lock are significantly affected by the type of lock. For instance, key locks are typically less secure than combination locks because the keyway leaves the lock mechanism more exposed. Convenience options, such as master-keying and removable cores, further decrease security. Padlocks are in general more vulnerable to forcible attack than locks which are protected by a security barrier. While some generalizations apply, the relative vulnerabilities will depend on the specific designs being considered.

Surreptitious defeat of a lock usually requires a thorough knowledge of lock construction as well as some level of attack skill. In addition, special tools (which are available commercially) are frequently required. Defeat methods which are more forcible require less knowledge of locks, while purely forcible defeat requires no lock knowledge.

Defeat times vary greatly depending on the type of attack. Often, longer surreptitious and forcible defeat times result when unique features are designed into the locking device. These features are described in detail in this section.

3.1 Key Locks

This section covers all types of key-operated locks, including door locks, cabinet locks, padlocks, and locks for security containers.

3.1.1 Uses

Permanently mounted key-operated locks are found in all applications requiring levels of security from minimal to high. They are found in container locks, door and cabinet locks, and switch locks. Key locks typically are the primary devices safeguarding the secured item or volume. They are not typically used to actuate another securing mechanism.

Key-operated padlocks are found in quality levels and grades ranging from low security warded key locks to high security shrouded-shackle padlocks. High security models are used to secure safes and security containers.

3.1.2 Hardware Description

Key locks are locks which operate through the use of a mechanical or magnetic key. Use of the correct key allows retraction of the bolt or latching mechanism granting access. Most key locks fall into four general classes: warded locks, wafer (or disk) locks, pin-tumbler locks, and lever locks. In addition, key locks also include some unique options and variations of these general classes of locks. Each of these lock classes and their options and variations are discussed in the following subsections.

3.1.2.1 Basic Designs

Warded Locks

Warded locks incorporate fixed wards or obstacles (external and/or internal wards) in the lock structure which a key has to clear in order to rotate and operate the bolt or latching mechanism. The key for a warded lock has ward cuts placed at designated locations to allow key rotation. Figure 3-1 illustrates a typical warded lock with the correct key inserted and with an incorrect key inserted. Warded locks were once popular as door locks and may still be found in some older hotels and residences. Currently, most warded locks manufactured in the United States are padlocks. Both the padlock and the warded door lock are easily picked. In addition, warded skeleton keys (passkeys) are easy to fabricate and are readily available through commercial sources.

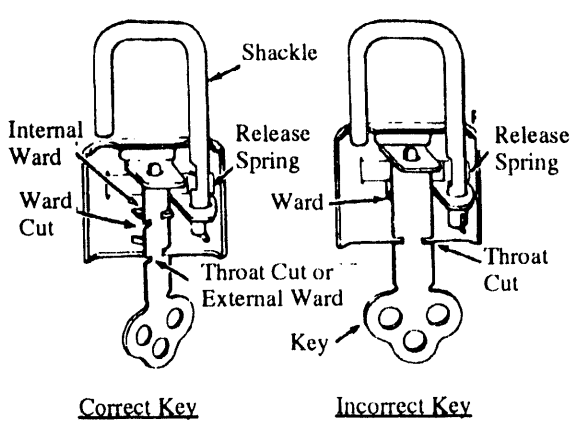

Figure 3-1. Warded lock

Since the warded lock cannot be keyed with a master key, it has limited usefulness and versatility. If a warded lock is compromised, it should be removed from service since it cannot be recoded for a different key.

Wafer Locks

Wafer locks were invented in the United States in the late 1800s. Their low manufacturing cost and mass production capability have led to the widespread use of wafer locks for many different applications: locks for luggage, showcases, desks, cabinets, and some types of padlocks and switch locks. Wafer locks offer better resistance to picking and impressioning than do present-day warded locks. Master-keying of wafer locks is possible; however, only 200 to 500 usable combinations are available. These locks can be rekeyed, but, due to their low cost, replacement of the lock is more practical. The wafer lock, shown in Figure 3-2, consists of a cylinder plug or core which is held in place by a stack of spring-loaded, flat metal wafers. Each wafer has a rectangular cutout in the center through which the key needs to pass; the ends of the wafers protrude from the cylinder plug into the cylinder housing. When the proper key is inserted into the lock, the wafers are aligned so that none protrude from the cylinder plug, allowing the plug to rotate within the cylinder housing.

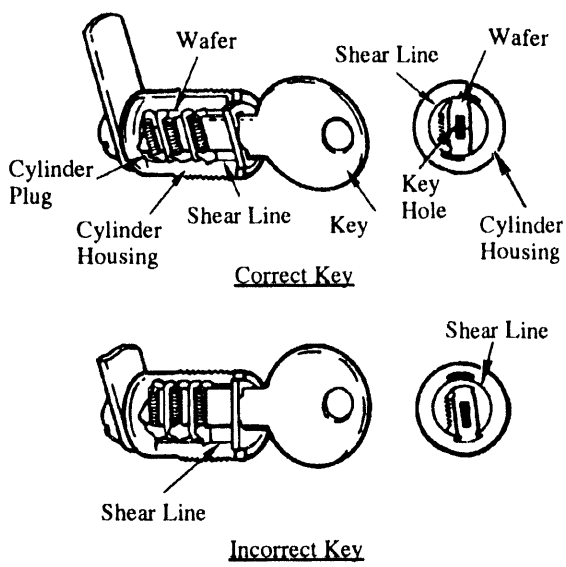

Figure 3-2. Wafer lock

Pin-Tumbler Locks

Pin-tumbler locks, patented by Linus Yale in the late 1800s, offer more security than warded or wafer locks. However, in their standard form, pin-tumbler locks are also vulnerable to picking and impressioning.

The standard pin-tumbler lock, shown in Figure 3-3, consists of a cylinder case which contains a cylinder plug or core. The lock case houses several small, spring-loaded pins placed in line and extending into the keyway. The top (or driver) pins are forced down by the springs into the plug to prohibit plug rotation. The cone-shaped end of each bottom (or key) pin rests against the inserted key; if the key is properly cut, it raises the break between the top and bottom pins so that each break is even with the outer surface of the cylinder plug (shear line). When the pins are thus aligned, the cylinder plug can be rotated.

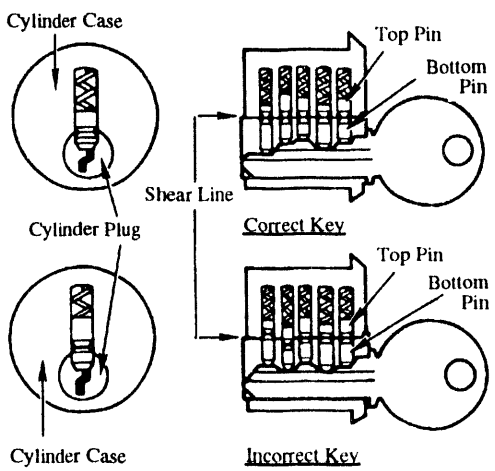

Figure 3-3. Standard pin-tumbler lock

Pin-tumbler locks are usually manufactured to high tolerance specifications and offer a number of different possible key codes. They can easily be master-keyed for tens of thousands of possible combinations. Very complex master-keying systems can be developed using pin-tumbler locks. The pin-tumbler lock is widely used in the United States in padlocks and door locks, and for special applications.

Lever Locks

Lever locks originated in Europe in the late 1700s and are still widely used. In the United States, their principal application is in locks for post office letter boxes, pay telephone coin boxes, safe deposit boxes, and several types of padlocks. Lever locks can provide medium to high resistance to picking.

Different key combinations for lever locks can be obtained by either changing the position of the levers or by replacing the

levers. The lever lock is usually limited to a simple master-keying system unless it is master-keyed within the key.

The operation of a typical lever lock is illustrated in Figure 3-4. Several flat metal levers (or tumblers) are attached by a pin to a common point at one end of the lock in such a way that the levers are free to swing slightly and are positioned so that rotation of the key exerts a force that retracts the bolt. Each of the levers has a rectangular gate cut in the free end. The bolt has a protruding fence which rests against the free ends of the levers to prevent retraction of the bolt when it is locked. When the correct key is inserted and rotated, the bitting or key cuts on the key elevate the free ends of the levers so that the gates are aligned, thus permitting the fence on the bolt to enter the gates. After the fence enters the gates, bolt retraction is completed by further key rotation.

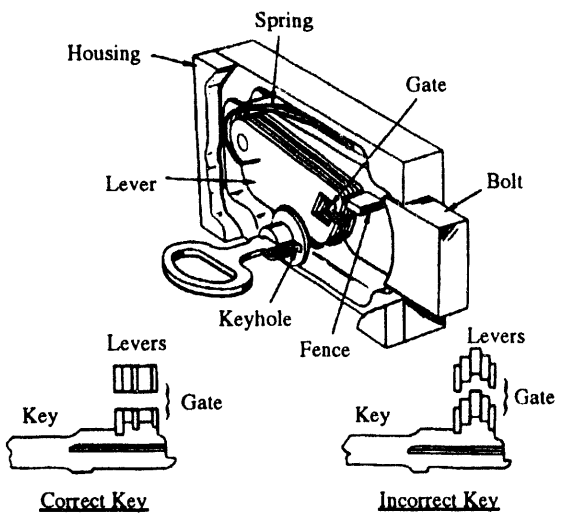

Figure 3-4. Lever lock operations

Large lever locks are commonly used in prison security applications. These larger locks are resistant to picking, primarily due to their massiveness and the strength of the springs on the levers. A further refinement incorporated into some lever locks requires that the key be turned several times in order for the bolt to be completely retracted. In this case, a lock would have to be picked once for each required key rotation.

Another feature incorporated into some lever locks to increase resistance to picking is the use of serrations (teeth). If the fence prematurely contacts the end of the lever tumblers, as it needs to do if an attempt is made to pick the lock, the serrations on the levers engage similar serrations on the fence and prevent the movement necessary to align the gate.

3.1.2.2 Master-Keying

Master-keying is an option in the keying of a set of similarly keyed locks to open with a common key. While other types of locks can be master-keyed, only the pin-tumbler plug mechanism is designed for complex master-keying. For this reason, the pin-tumbler lock is very popular. The pin-tumbler lock can be master-keyed by splitting the bottom pin or pins into two or more segments (master wafers), thereby allowing more than one shear line to become available. This principle is illustrated in Figure 3-5.

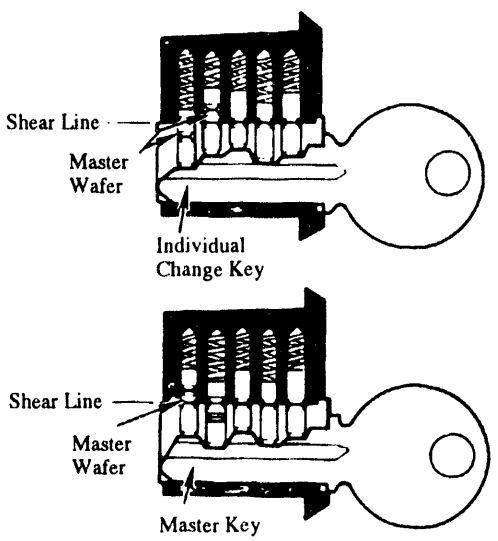

Figure 3-5. Example of pin splitting for master-keying

As the number of master key levels increases, i.e., master, grand master, etc. (see Figure 3-6), so does the number of splits required. This affects security in several ways:

(1) The probability that a lock can be compromised by picking or impressioning increases sharply with increasing levels of master-keying.

(2) The number of usable key codes sharply decreases with increasing levels of master-keying. This occurs because key codes have to be set aside for each level of master-keying.

(3) If key codes are not assigned systematically, a key which is not intended to work in a given lock could accidentally work. The more levels of master-keying, the more likely this is to happen.

(4) Loss or compromise of a master key affects many locks.

(5) Increasing levels of master-keying make the lock more complex. It is likely that it will be more difficult to maintain, and is therefore more vulnerable.

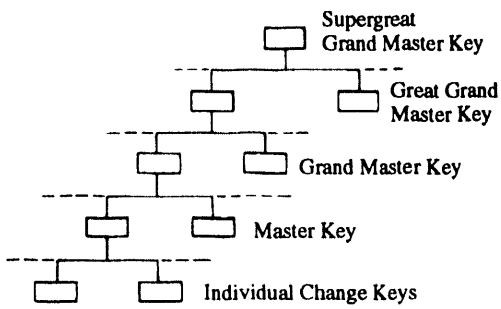

Figure 3-6. Master-keying system

The picking vulnerabilities inherent in conventional master-keying have created a widespread need for more sophisticated key cylinders. Several cylinders are available which provide greater security than those previously discussed. An example of such a sophisticated cylinder is the bicentric cylinder (see Figure 3-7), which is constructed of two separate rotating plugs. One form of this lock requires two keys for entry. A second option allows entry through the use of either an individual change key or a master key. No degradation occurs within the first level of master-keying.

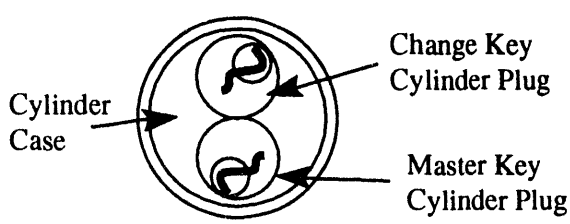

Figure 3-7. Bicentric cylinder

Another method of first-level master-keying is accomplished through the use of a master ring formed around the regular plug. The addition of this ring results in the creation of two shear lines (see Figure 3-8).

A fourth method of master-keying provides for keying within the key, rather than within the cylinder. Since master-keying is not accomplished in the cylinder, the total system cannot be defeated by simply disassembling the cylinder in order to determine the key combination. In the multirow radial pin-tumbler design described later, the master key contains all valid impressions necessary for entry as well as false impressions. An example of such a master key is shown in Figure 3-9. This key cannot be duplicated on standard duplicating machines.

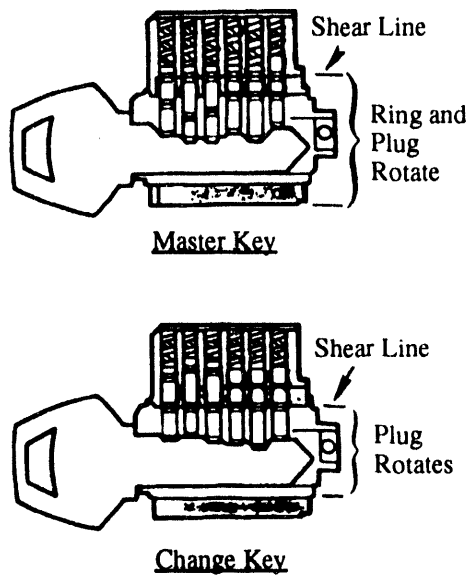

Figure 3-8. Master ring

Figure 3-9. Self-contained master-keying key

Keying Alike

An alternative to master-keying is keying alike. Keying alike is the identical keying of several different locks to one key by the use of identical pins for each lock. Although this method of keying does not generate the multiple shear line vulnerability of master-keying, it does allow each key-holder to have access to more than one lock.

3.1.2.3 Proprietary Systems

The only readily available proprietary system is one in which an exclusive keyway is used. An agreement may be made with the manufacturer to provide the exclusive keyway only to specified customers.

Keyways are keyholes designed using wards or obstacles which increase the master-keying capability of a locking system. Examples of different keyway cross sections are shown in Figure 3-10. The term "restricted keyway" refers to the option offered by some manufacturers in which a particular keyway cross section is exclusively assigned to a customer, and blank keys with that cross section are sold, as authorized, to that customer alone. Restricted keyways are often used to restrict entry in a given keyed section of a total master-keyed facility.

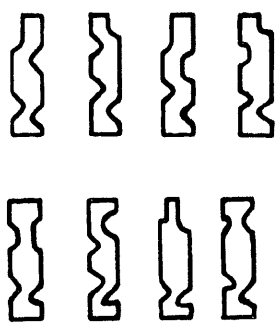

Figure 3-10. Keyway cross sections

3.1.2.4 Other Key Lock Options and Variations

Pin and Lever Variations

A number of features or principles have been used to improve the standard key lock design. For example, variations in the standard straight cylindrical pins of the pin-tumbler lock can increase its resistance to picking; lever locks which employ false gates are also less susceptible to picking (Figure 3-11). Such variations are used to confuse individuals attempting surreptitious entry and increase the amount of time required to defeat the lock.

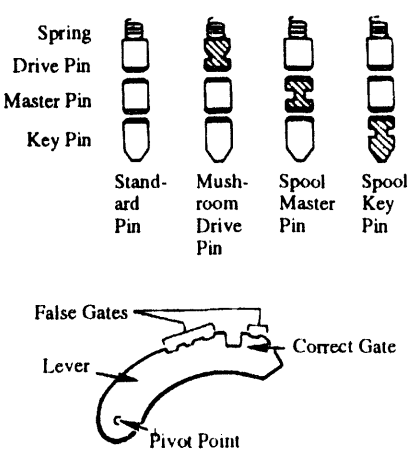

Figure 3-11. Pin and lever variations

Tubular Locks

The tubular lock, shown in Figure 3-12, uses a round key to depress the concentric pattern of pin tumblers projecting toward the face of the lock. The tubular lock has been used extensively in the past, although acceptance of this lock for sensitive applications has decreased recently. This is primarily due to the appearance on the market of pick tools tailored especially to this type of lock.

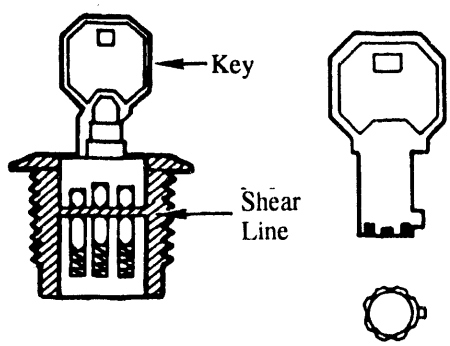

Figure 3-12. Tubular locks

Dual Pin Action

Some pin-tumbler lock cylinders require that the pins, in addition to being elevated to the shear line, also be rotated to a proper orientation to increase pick and impressioning resistance. This dual pin action is accomplished by the use of key cuts that have varied angles and depths. A comparison between a standard, one-motion pin-tumbler lock and key, and a dual, or two-motion, system is shown in Figure 3-13.

Multirow Radial Pin-Tumbler Locks

Another unique method of keying the pin-tumbler lock entails the use of pins arranged radially in the cylinder so that the pins rest on more than one surface of the key, as shown in Figure 3-14. This type of keying produces a smooth profile key rather than the traditional sawtooth key. The key contains dimples located on the sides of the key to position the pins to their proper depth. Because more key surface contact is available, the number of pins contained within the cylinder can be increased and therefore can increase pick resistance.

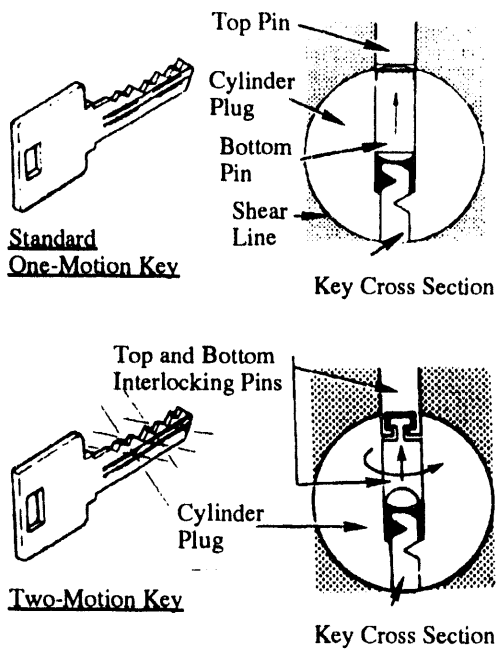

Figure 3-13. Standard and dual pin-tumbler keys and cylinders

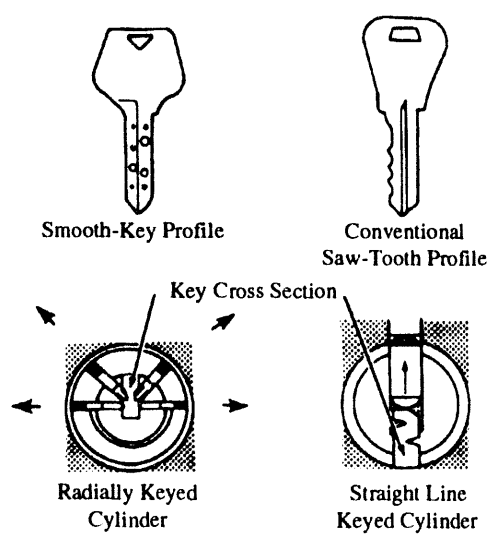

Figure 3-14. Standard and multirow radial keys and cylinders

Rotating Tumbler Disk Locks

Rotating tumbler disk locks are highly pick-resistant locks which operate using a specially cut cylindrical key that rotates individual disks in the cylinder to different turn angles. When the key is inserted and rotated, the disk notches align, allowing a locking bar to drop into position. This action frees the otherwise constrained plug containing the disks and allows the plug to rotate. An example of the tumbler disk lock is shown in Figure 3-15.

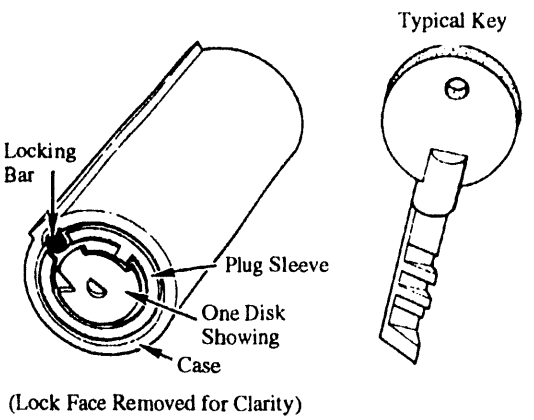

Figure 3-15. Rotating tumbler disk lock

Removable Core Locks

The cost of lock hardware becomes a predominant factor in lock selection when several hundreds or thousands of padlocks and door locks need to be quickly replaced or rekeyed. Removable core locks are often used by large facilities because they can be exchanged expediently. During the exchange procedure, the entire key mechanism is removed and replaced with a differently keyed core. This operation requires only seconds to perform. Removable cores can be retained within the lock in several different ways, as shown in Figure 3-16.

3.1.3 Application Considerations

3.1.3.1 Pros and Cons

The major feature of key locks, especially pin tumbler locks, is their adaptability to many levels of master-keying. The advantage of this adaptability is increased convenience; the disadvantage is reduced security. For each level master key incorporated into the design, an additional shear line has to be designed into the lock. For each additional shear line the mechanical structure of the lock is weakened and the susceptibility of the lock to picking is increased.

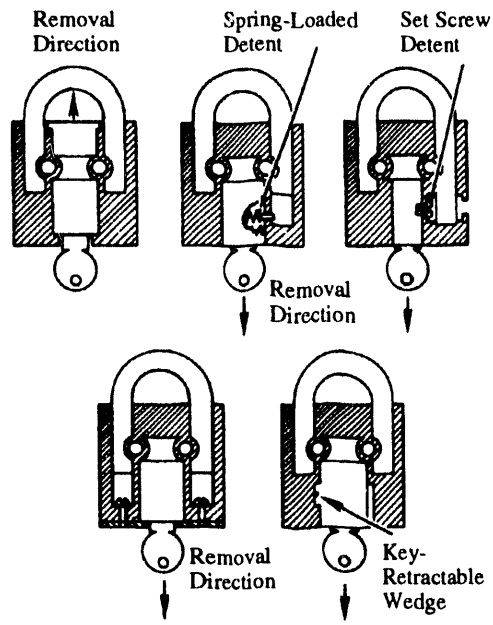

Figure 3-16. Removable core key mechanisms

Another advantage of key locks is the wide range of designs available. From this pool, an appropriate lock may be selected to fit almost any set of design constraints and security requirements. Other advantages are the short time interval required to operate a key lock, and the elimination of the need to memorize a multi-digit combination.

Additional disadvantages of key-operated locks include the necessity to maintain replacement parts for changing the keying of the lock; the need to track and control possession and duplication of keys; and the vulnerability of key-operated locks to surreptitious attacks.

Some methods for defeating key locks are picking, decoding, impressioning, x-rays, impact vibration, bolt manipulation, core removal, environmental and chemical attacks, and force. These methods are described in the Glossary.

3.1.3.2 Design Features Which Affect Security

When assessing security of key-operated locks, the single most important aspect is the design of the lock. Typically, the warded lock is least secure for three reasons: it is easily picked, it can be opened by a skeleton key, and the lock cannot be recoded. Wafer locks offer better resistance to picking and impressioning than warded locks. However, the typical number of possible combinations, 200-500, is low compared with the more secure designs.

Pin tumbler locks are more secure than warded or wafer locks because there are thousands of possible combinations. Several design variations covered in Section 3.1.2 increase resistance to picking and impressioning.

For several reasons, the most secure key-operated lock is the lever lock. First, lever locks are less frequently used in the United States than pin tumbler locks. Therefore, attack methods are less well-known. Second, pin tumbler locks allow more levels of master-keying. As discussed in Section 3.1.2.2, master-keying increases vulnerability to attack. Third, lever locks can be designed so that multiple turns of the key are required to fully retract the bolt. This increases pick resistance because the lock must be picked once for each rotation of the key. While this feature could be designed into a pin-tumbler lock, it is not a typical design. Fourth, the pin tumbler lock can be attacked by forcibly pulling the cylinder (core-pulling). Once the cylinder is removed, the bolt can be easily retracted. The lever lock does not share this vulnerability.

Locks can be made more resistant to picking and forcible attack by increasing the size and strength of materials.

Master-keying seriously compromises the security of a system (see Section 3.1.2.2). An awareness of the trade-off between convenience and security is necessary in making decisions about where master-keying would be appropriate.

The security of the pin tumbler, wafer, and lever designs may be augmented by increasing the number of pins, wafers, or levers. UL Standard 437 specifies that door locks and locking cylinders have a minimum of 1000 key changes possible, while key locks intended for security containers must have a possible 1,000,000 key changes. For dual-key security locks, 64 guard key and 15,000 user key changes are required by this specification.

Cabinet door and drawer locks covered under MIL-L-2898D, and padlocks covered under GSA Commercial Item Description A-A-1930A, are required to have at least 1200 key changes available. Medium security padlocks specified in MIL-P-43951A, and high security padlocks specified in MIL-P-43607G, are required to allow 100,000 different key changes.

Another factor affecting the security of key-operated locks is the distance the bolt extends from the lock body (the "throw") when it is locked. These requirements are specified in the applicable specifications (Section 3.1.4).

Still another security feature for key locks is that the key not be removable when the lock is not secure. This makes it more difficult for a lock to be left unsecured.

Specific design features which affect security are included in Section 3.1.2.

One security feature offered on some padlock designs prevents the shackle from being fixed in position unless both ends of the shackle are inside the lock case. Padlocks are usually monitored by pulling on the lock case to ensure the shackle does not come out. If the shackle can be fixed in position outside the lock case, it could feel as if the lock is secured when it is actually open. This feature is particularly important in applications where the lock is difficult to visually inspect.

The shackle should also be designed so that a positive pull is required to remove the shackle from the lock body. A spring-loaded shackle makes it easier for someone using surreptitious techniques to attempt to gain unauthorized access. If the shackle springs open, it takes less time for each successive opening attempt.

3.1.3.3 Other Factors Which Affect Security

Factors such as wear and tear, corrosion, and lack of preventive maintenance can affect the security of a lock.

For example, a failure can be made credible. If a lock is broken, it could be attributed to the condition of the lock, rather than an attack. Furthermore, an adversary could forcibly open the lock, then substitute a non-working replacement lock.

An adversary may also be able to open the lock more easily if the lock is worn. Wear can cause parts to fit more loosely, allowing picking tools to be more easily inserted.

Finally, a poorly maintained lock can be difficult to open by an authorized user. When a lock is difficult to open, it is also difficult to verify that it is locked, introducing still another vulnerability.

3.1.4 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

3.1.4.1 Permanently Installed Key Locks

ANSI/BHMA A156.2-1989 - American National Standard for bored and preassembled locks & latches

This standard establishes requirements for bored and preassembled locks and latches. The standard includes performance tests, strength tests, operational tests, finish tests, and dimensional criteria.

This specification defines two series of key-in-knob design locks: the series 2000 and the series 4000. The series 2000 preassembled locks and latches mount in a slot cut into the door edge. The series 4000 bored locks and latches mount in holes bored through the door. Three grades of lock are defined: Grades 1, 2, and 3, with Grade 1 being the highest security. Series 2000 locks are available in Grade 1 only, while series 4000 locks are available in all three grades.

Thirteen types of preassembled locks and latches are described, with appropriate functions and function numbers for each type of lock. Nineteen types of bored latches are similarly described. Testing methods and required results are specified for operational, strength, cycle, material evaluation, and finish testing.

This specification may be obtained from the Builders Hardware Manufacturers Association, Inc.

ANSI/BHMA A156.5-1984 - American National Standard for auxiliary locks & associated products

Part I of this standard covers auxiliary bored and mortise locks, rim locks, and cylinders. Security tests, operational tests, finish tests, and dimensional criteria are included.

Part II of this standard establishes requirements for exit alarms and locks, electric strikes, and indexed key control systems. It also includes operational and finish tests.

The following is a summary of Part I. Other parts of this standard are reviewed in the appropriate section of this document.

Part I contains pictures and descriptions of many types of locks, describes various lock parts, and provides a good overview. Other specifications are referenced for details.

Three operational and security grades are described, with Grade 1 being the highest. Test equipment and methods are specified. Operational tests include torque, force, minimum projection of latch or bolt, warped door, bolt strength, axial load, vertical load, cycle tests, and finish tests. Security tests include impact, tension, torque, bolt sawing, and bolt pressure.

Cylinders are required to be of the pin tumbler type, with at least five pin tumblers. There are specific performance, strength, operational, picking, and cycle tests on cylinders.

The part numbering scheme describes how to specify what you want to purchase. The numbering scheme describes material, type of product, product function, and grade.

This specification may be obtained from the Builders Hardware Manufacturers Association, Inc.

ANSI/BHMA A156.11-1991 - American National Standard for cabinet locks

This standard describes the requirements for cabinet locks used on doors, drawers, and furniture. Included are descriptions of use for eight different types of cabinet locks which may be supplied in three security grades. Grade 1 is the highest security and operational grade. Testing methods for operational, strength, cycle, and finish tests are provided, as well as required test results for the three grades.

Pictures and descriptions of many cabinet lock designs are included. The part numbering scheme describes how to specify what you want to purchase. The numbering scheme describes material, type of product, product function, and grade.

This standard may be obtained from the Builders Hardware Manufacturers Association, Inc.

ANSI/BHMA A156.12-1986 - American National Standard for interconnected locks & latches

This standard establishes the requirements for interconnected locks. An interconnected lock is one which has a separate, mechanically connected latch, deadlatch, or deadbolt. The latch or bolt is designed for installation in the edge and face of a door stile. The standard includes operational tests, security tests, cycle tests, finish tests and dimensional criteria.

The standard also defines series 5000 interconnected locks and latches in three security grades. Grade 1 is the highest operational and security grade. Twelve types of locks are described, with appropriate functions and function numbers for each type of lock.

This standard may be obtained from the Builders Hardware Manufacturers Association, Inc.

ANSI/BHMA A156.13-1987 - American National Standard for mortise locks & latches

This standard establishes requirements for mortise locks and latches. Mortise locks or latches are those which are installed in cavities prepared in the edge of a door, with access to the lock for key cylinders and knobs provided by holes bored through the door.

The standard includes operational tests, security tests, cycle tests, finish tests, material evaluation tests, and dimensional criteria.

The standard describes series 1000 mortise locks and latches in three security grades. Grade 1 is the highest operational and security grade. The grade in operational classification must be expressed separately from the grade in security classification. This appears to be different from the other ANSI/BHMA specifications. Twenty-four different types of mortise locks are described, with appropriate functions and function numbers for each type.

This specification may be obtained from the Builders Hardware Manufacturers Association, Inc.

MIL-L-2898D - Locks, Flush, Metal and Wood Door and Drawer, Naval Shipboard

This specification covers metal and wood cabinet door and drawer locks for Naval shipboard use. Materials and construction are specified, as well as required dimensions and tolerances. Each lock is required to have 1200 possible key changes. Type "A" locks, for use on doors, must have a deadbolt and must have three or more levers or pin tumblers. The bolt must extend 1/4 to 5/16 inch when engaged. Type "B" locks, for use on drawers, have similar requirements, with a bolt throw of 1/4 inch. Other specifications are concerned with workmanship, quality, and packaging.

This specification may be obtained from the Defense Printing Service.

UL 437 - Key Locks

This specification covers door locks, locking cylinders, security container key locks, and two-key locks. Specifications include construction. materials, number of key changes, and testing. Test requirements include salt spray corrosion, endurance, and attack resistance.

For endurance testing, 10,000 complete lock/unlock cycles at a 50 cycle-per-minute rate must not degrade the performance. For those designs incorporating changeable cores, 50 changes of core or key must not degrade performance.

Door locks and locking cylinders must have a minimum of 1000 key changes possible, while key locks intended for security containers must have a possible 1,000,000 key changes. For two-key locks, 64 guard key and 15,000 user key changes are required by this specification.

The attack resistance testing method describes tools permitted, and specifies time requirements during which the lock must successfully resist eight different types of attacks.

This specification may be obtained from Underwriters Laboratories, Inc.

A-A-1932A Commercial Item Description, Lock Set, Rim

This commercial item description covers rim type lock sets for residential and industrial applications. They must conform to ANSI/BHMA A156.5. They will use a key on the outside and a thumb turn on the inside. The locking mechanism can be a latch, bolt, deadlatch, or deadbolt. Each lock must be individually keyed. Key blanks are, in general, commercially available.

Other requirements include finish, workmanship, quality assurance, packaging, and marking. Ordering data, which should be included when purchasing to this specification, is included.

This specification may be obtained from the Defense Printing Service.

3.1.4.2 Key-Operated Padlocks

ASTM F 883-90 - Standard Performance Specification for Padlocks

This standard contains environmental, functional, operational, and security requirements for both key and combination padlocks. Included are function descriptions, cycle tests, operational tests, environmental tests, forcing tests, surreptitious entry tests, and a glossary of terms related to padlocks. Six levels of padlock performance criteria are defined, with level 1 the lowest grade and level 6 the highest.

This standard does not include criteria for specially made padlocks used by the Department of Defense or others in highly sensitive locations.

Forcing tests include specific instructions to conduct a tensile test, a drop test, a shock test, a cylinder plug pulling test, a cylinder plug torque test, and a shackle cutting test.

Surreptitious entry tests require the padlock to resist entry for a period of time contingent upon the grade. Areas covered include picking (key padlocks) or manipulation (combination padlocks); cylinder impressioning and decoding; shackle shimming; cylinder drilling and shimming; and rapping.

Environmental tests include salt spray for corrosion resistance, dry contaminants, ultraviolet radiation, and wet freezing environment.

References to other applicable standards and documents are included.

This specification may be obtained from the American Society for Testing and Materials.

MIL-P-43607G - Padlock, Key-Operated, High Security, Shrouded Shackle

This specification defines a key-operated, high security, shrouded shackle padlock that employs a changeable cylinder and a deadbolt locking mechanism. The padlock must use a proprietary military keyway which has a control key for cylinder removal. Padlocks must be keyed individually.

Included in this specification are requirements that define materials, design, quality control, and testing. The padlock must be capable of 100,000 different key changes, and keys must be marked "US MILITARY PROPERTY - DO NOT DUP."

Requirements for shackle pull out resistance, heat resistance, low temperature operation, salt spray resistance, drop resistance, wear resistance (10,000 cycles of operation), shock resistance, and corrosion resistance are included.

The lock must withstand surreptitious entry attack for not less than 15 minutes before and after the wear resistance cycling test. For forcible entry testing, a list of permissible tools is included. The lock must withstand five minutes of attempted forced entry.

Keys are also specified. Operating keys are used to lock and unlock the padlock and must not be capable of rotating the cylinder. The control key, however, must be capable of rotating the cylinder so it can be removed. Specifications include hardness, deformation resistance, shapes, bit cut, and marking. Tests for key operation and key integrity are included.

Also included are defect inspection lists and requirements for marking and packaging.

This specification may be obtained from the Defense Printing Service.

MIL-P-43951A - Padlock, Key-Operated, Medium Security, Regular Shackle

This specification is very similar to MIL-P-43607G. The subjects covered are the same, but some major differences between the two specifications follow.

This specification covers a medium security, regular shackle padlock. MIL-P-43607G covers a high security, shrouded shackle padlock. This specification has some additional tests for cylinder plug pulling resistance, cylinder plug torque, and shackle cutting resistance. The lock must withstand four minutes of attempted forced entry. MIL-P-43607G requires five minutes.

This specification may be obtained from the Defense Printing Service.

A-A-1927C Commercial Item Description, Padlock (Pin Tumbler Mechanism)

This specification covers key-operated, pin tumbler, deadbolt padlocks intended for low security use. Padlocks supplied under this specification must conform with applicable requirements of ASTM F 883, Grade 2.

The specification includes requirements on case and shackle hardness, shackle design, dimensions, number of pin tumblers (ranging from four to five, depending on padlock size), materials, number of possible key changes (ranging from 3000 to 10,000, depending on padlock size), corrosion, part numbering, and quality assurance provisions.

Padlocks may be keyed alike, keyed individually, master-keyed, or grand master-keyed. Keys are generally made from key blanks which are commercially available. Ordering information is included.

This specification may be obtained from the Defense Printing Service.

A-A-1930A Commercial Item Description, Padlock (Disk or Blade Tumbler)

This specification covers key-operated, disk or blade (wafer) tumbler padlocks intended for low security use. Padlocks supplied under this specification must conform with applicable requirements of ASTM F 883, Grade 2.

The specification includes requirements on shackle design, dimensions, number of disk or blade tumblers (10), materials, number of possible key changes (1200), corrosion, and quality assurance provisions.

This specification may be obtained from the Defense Printing Service.

3.2 Traditional Combination Locks

This section covers mechanical dial combination locks.

3.2.1 Uses

Permanently mounted, dial-type combination locks are typically found in applications requiring medium to high security such as safes, security files, vault doors, and other security containers. In high security applications, they are usually not the primary securing device for the container. Instead, the bolt on this type of lock will typically be used to prevent operation of a series of bolts or pins which do the actual securing of the container (see Figure 3-17). This arrangement serves two purposes. First, the container is secured at multiple points around the perimeter of the closure, providing much higher resistance to forcible entry. Second, the bolt of the combination lock is protected by the secure container, providing an extra level of protection against an attack directed at the lock itself.

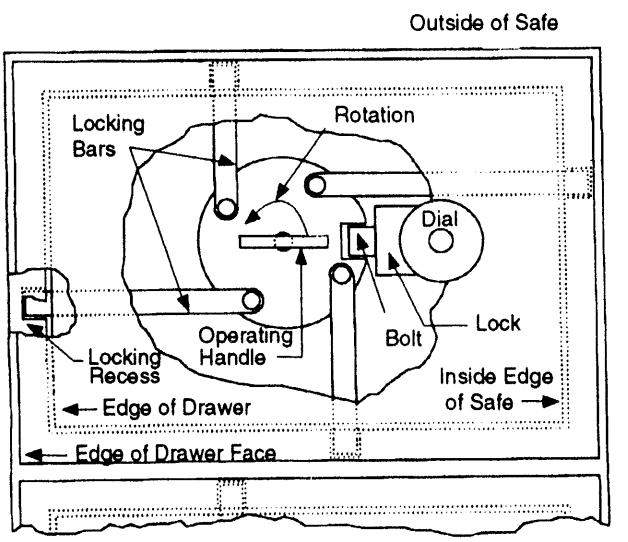

Figure 3-17. Typical arrangement of lock bolt and locking bars on a safe

Combination padlocks are used as stand-alone devices in low to medium security applications. They are also used in high security applications in conjunction with other security measures. This type of lock is usually the primary securing device of the container. Because of the vulnerability to direct physical attack, combination padlocks should not be used in high security applications unless other security measures are used.

In situations where it is important to know if the lock has been defeated, it is appropriate to use a lock which has a high level of tell-tale to unauthorized entry. This is covered in Section 3.2.3 and in the Federal Specification on Changeable Combination Padlocks, FF-P-110G.

3.2.2 Hardware Description

Combination locks are incorporated into padlocks and door locks. They range from simple locker-room variety padlocks to highly developed security vault door locks. However, the basic principle of operation is the same for all combination locks.

The dial is usually divided into sections marked with numbers. An index mark(s) is located on the door lock dial ring or, in the case of a padlock, on the padlock body. In the door lock, the dial and dial ring are usually the only visible portions of the lock. When the dial is rotated, its motion is transmitted to code wheels located within the lock case. Correct positioning of the wheels allows the bolt to be retracted.

The combination dial is attached to a spindle (shaft) which, in turn, is attached to a drive cam. (See Figure 3-18). When the dial is rotated, the drive cam rotates. A drive pin projects from the flat surface of the drive cam and from each driving wheel. As the dial rotates the drive cam, its drive pin contacts a fly (limited-motion pin) on the wheel closest to it, causing the wheel to rotate around the wheel post. The drive pin on the opposite side of the wheel contacts the fly on the next wheel, rotating this wheel also. This continues until all wheels are in motion. The wheel farthest from the drive cam aligns on the first combination number and is referred to as wheel number 1. The direction of dial rotation is then reversed to align the second wheel on the second combination number, etc.

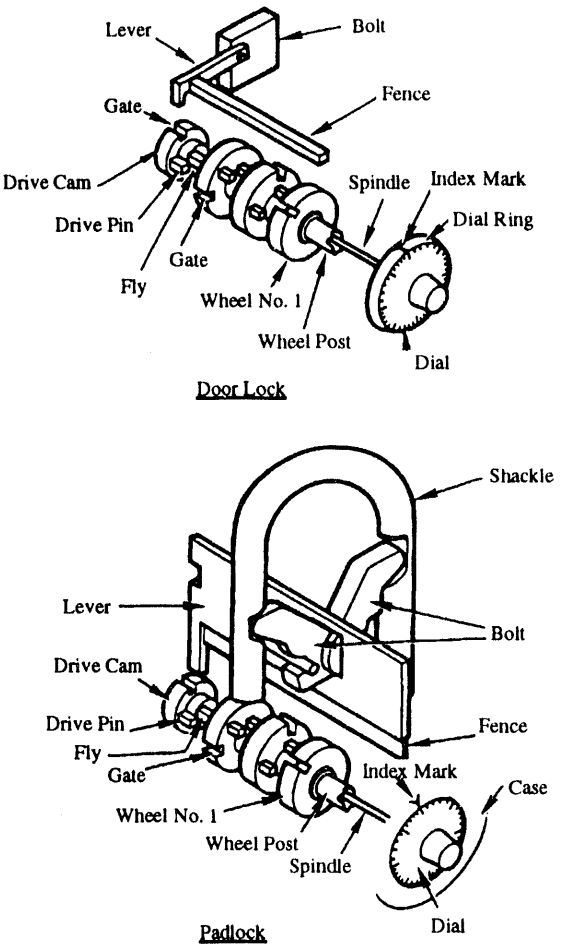

Figure 3-18. Combination lock mechanisms

The drive cam and each wheel have a gate cut in their circumference. When the correct combination is dialed, the gates of each wheel and the drive cam gate are aligned. The fence moves into the aligned wheel pack gates, and a lever attached to the bolt is allowed to nest its nose in the drive cam gate. In door lock configurations, continued dial rotation retracts the bolt into the lock case. Padlocks require a pulling action on the shackle for lever nesting and bolt retraction. These features of the combination lock are shown in Figure 3-18.

All combination locks contain the following common subassemblies: case, wheel pack, dial, and bolt.

Lock Case

Lock cases are usually zinc-alloy die castings. The combination door lock case, which is sometimes factory-dated, consists of a box structure and a rear cover plate. The case is typically cast with a lever stop, bolt track, and mounting holes. The cover often contains a key-change hole, breakaway lines to hinder forcible punch attacks, cam stops, and thermal sensors. Numerous case designs exist. Figure 3-19 illustrates these door lock case features.

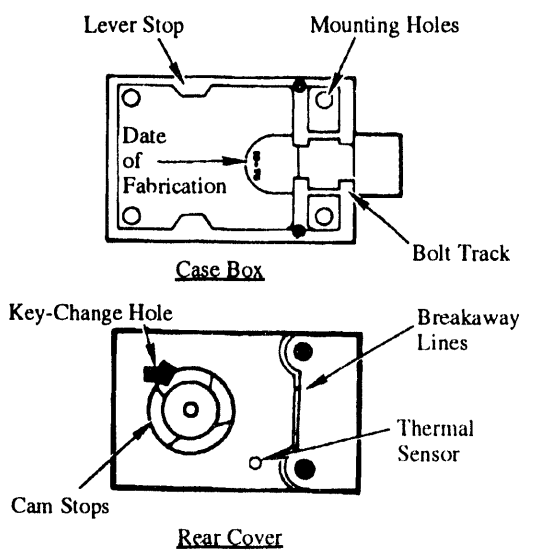

Figure 3-19. Case design, door lock

The combination padlock is a factory-sealed unit marked with several identifying serial numbers and its fabrication date (see Figure 3-20).

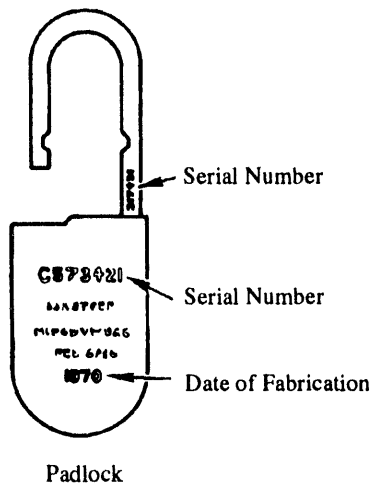

Figure 3-20. Case design, padlock

Wheel Pack

The wheel pack is assembled on a post, cast either on the rear cover or inside the box case. The wheels are separated by fixed spacer washers and are usually held under tension, as shown in Figure 3-21. Wheel pack tension varies from lock to lock and is a critical variable affecting wheel vibration and ease (or difficulty) of dial rotation.

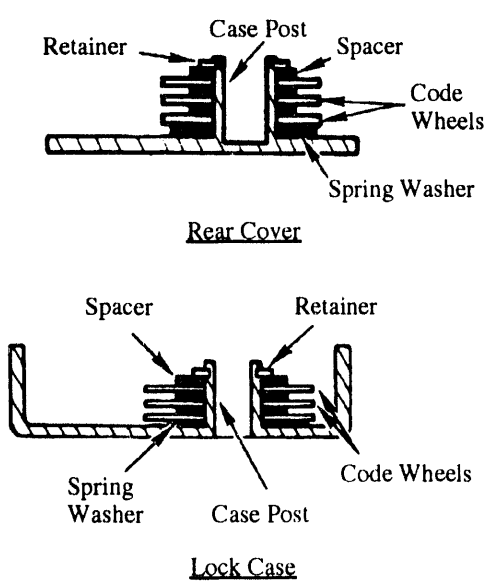

Figure 3-21. Wheel pack assembly

Combination locks typically have three or four code wheels. There are as many wheels as there are individual numbers in the combination. For example, the combination 11-34-46 has three distinct number sets and, correspondingly, the combination lock which used this combination would have three wheels.

Code wheels are usually balanced and constructed of metal or metal and plastic. The metal is usually machined brass or a die cast alloy. Plastic wheels are fabricated from Delrin or Lexan and are used primarily to provide x-ray resistance. Gate designs on the code wheels have varied over the years and from company to company. Three common gate configurations are shown in Figure 3-22.

Figure 3-22. Various code wheel gate designs

Lock combinations are either fixed or changeable. Most combination locks have hand- or key-change combinations. In order to change the combination in a combination lock, the angular position of each gate, relative to its drive pin, has to be changed in each wheel.

If the combination is hand-changeable, changing the combination is a difficult and time-consuming task, and requires complete wheel pack disassembly. A tooth-meshed wheel (Figure 3-23) is the most common design used in hand-change combination locks. The wheel consists of an inner and an outer ring. The drive pin is located on the inner ring, while the wheel gate is cut into the circumference of the outer ring. These rings have to be disengaged, rotated until the desired combination is selected, and then re-engaged.

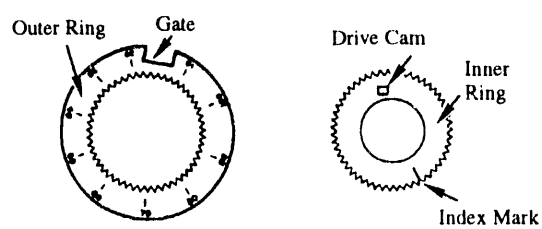

Figure 3-23. Tooth-meshed hand-change wheel

Hole or screw hand-change wheels (shown in Figure 3-24) are found on less expensive locks. In both types, the number of possible positions for the drive pin is greatly reduced, reducing the number of possible combinations.

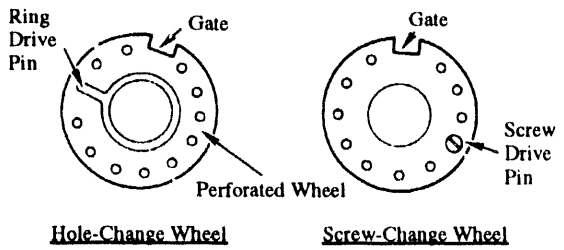

Figure 3-24. Hole and screw hand-change wheels

If the lock combination is key-changeable, changing the combination is a simple task, requiring only a few minutes. The key-change code wheel is similar in construction to the hand-change, mesh-toothed wheel. To change the combination of a key-change lock, the correct combination has to be dialed, aligning each wheel keyhole. A change key is inserted into the rear case cover and outer ring of each wheel. The key is rotated, disengaging the inner and outer rings and allowing the inner rings to rotate while the change key secures the outer rings in position. The new combination is dialed, and each drive pin is moved to a new location with respect to its corresponding wheel gate. The change key is returned to its original position, engaging the wheel rings, and is then removed. A new combination has been set.

Key-change locks are operationally convenient but are often more vulnerable to compromise than hand-change locks. Figure 3-25 shows different key-change wheel designs.

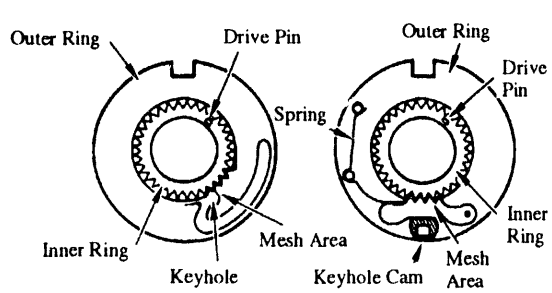

Figure 3-25. Key-change wheels

Another important part of the code wheel is the fly, or limited-motion, pin. Its presence allows 360° rotational use of the code wheel by eliminating any voids or dead spots due to drive-pin thickness. The fly is allowed to travel independently of the wheel, the width of its own "head," and half the distance of the drive pin before it begins to move the code wheel. This keeps the drive pin centered whether the wheel is turning left or right. Each code wheel has a fly by which it is driven and, if it is to drive another wheel, a fixed drive pin. The fly also helps compensate for inertia loading, which causes torque failure (slippage) between the inner and outer rings of the code wheel. Lockouts often result from wheel slippage. Figure 3-26 illustrates the operation of the fly.

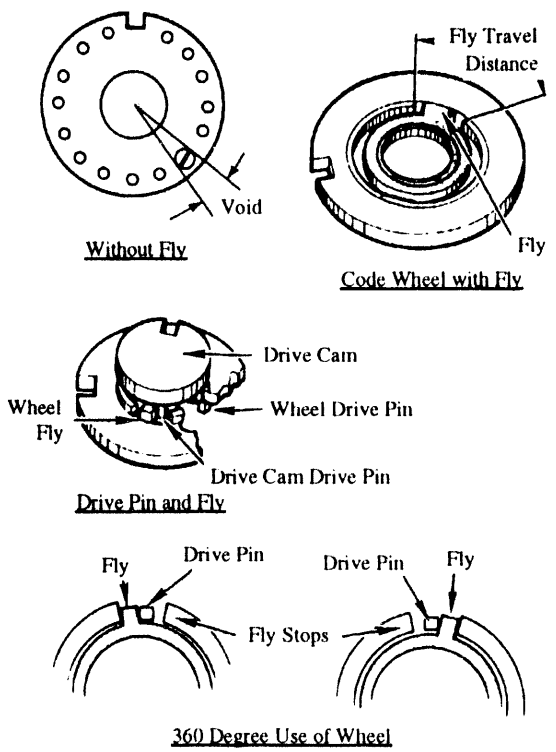

Figure 3-26. Fly operation

Dial Assembly

Door lock dials currently in use are divided into 100 equal parts spread over 360° of the dial. Earlier dial models, some of which are still in use, contain 100 equal parts but are spaced in less than 360°, leaving a blank area on the dial face. This latter design was used to eliminate jamming within the lock during dialing of the last number in the combination. Today, manufacturers' operating instructions request the user to refrain from using a specified area (approximately 20 numbers) when setting the last number of a door lock combination. This problem does not exist in padlocks, which typically contain 50 equally spaced numbers on their dials.

The door-lock ring or padlock case usually has one or two index marks for dialing reference (see Figure 3-27). The index located at the top center of the dial is referred to as the "open index" and is used for unlocking.

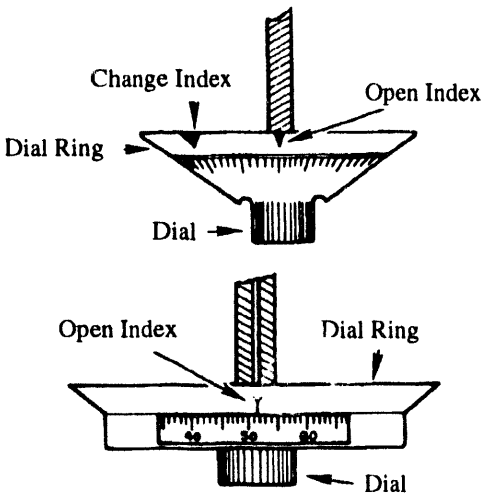

Figure 3-27. Dial

To change the combination, key-change locks often have a second index, called a "change index," which is set to the right or left of the open index. New combinations are entered by dialing the current combination on the change index, which aligns the key-change hole of each wheel with the rear cover key-change hole for change key insertion. If no change index is present on a key change lock, the open index is used by dialing a "change combination." These methods of keyhole alignment prevent unauthorized access while the lock is in the open position.

Spindles are usually fabricated from brass, zinc alloy, or steel. Padlock spindles are part of the dial casting. A door-lock spindle is usually a solid bar attached to the dial.

The dial is connected to the drive cam either directly or indirectly (see Figure 3-28). Padlock dials are directly connected. Directly connected door lock drive cams are usually threaded onto a dial spindle and secured with a spline key; indirectly connected drive cams are attached by a gear arrangement. The drive cam is either placed between the dial and the wheel pack or behind the wheel pack. In addition to providing power for wheel motion, the drive cam serves another important function: it restricts the period of time that the fence can contact the code wheels during rotation. Figure 3-29a shows the nose of the door lock drop lever as it normally rests under spring tension on the circumference of the drive cam. It is allowed to drop below the drive cam diameter once during 360° rotation. When the lever nose drops, the fence touches the wheels (Figure 3-29b). If the correct combination is dialed, the fence drops into the code wheel gates as the lever nose nests into the drive cam gate (Figure 3-29c). This allows the lever to drop below the lock case lever stop. The bolt is then

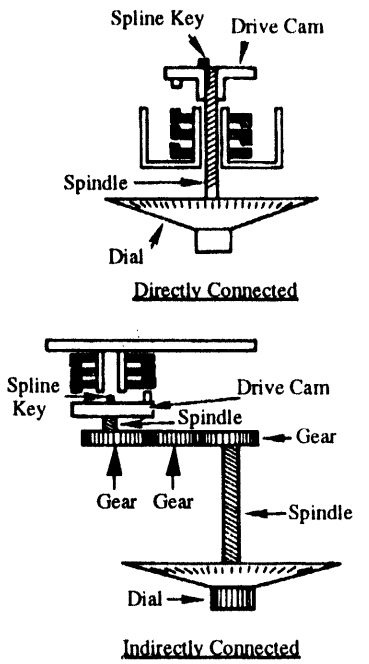

Figure 3-28. Drive cam location

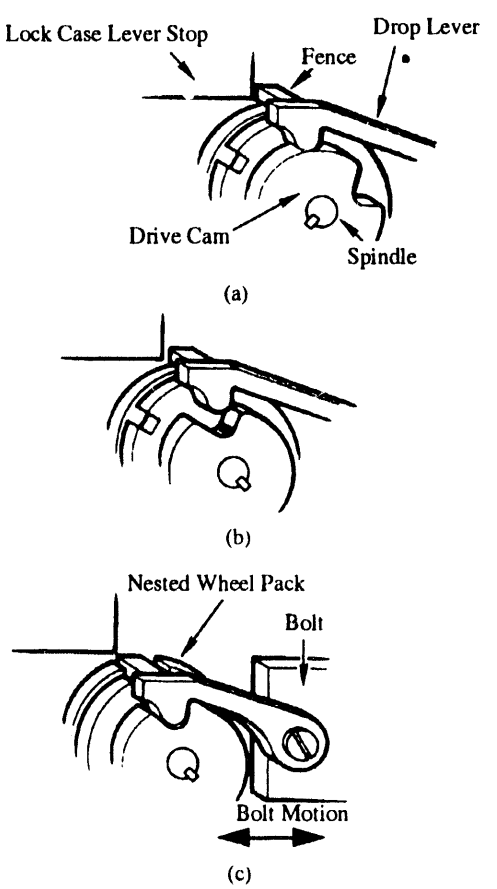

Figure 3-29. Drive cam action (door lock)

retracted by turning the dial in the proper direction. The lever in a combination padlock (shown in Figure 3-30) contacts the drive cam when the shackle is pulled. When the padlock lever enters the drive cam gate, the fence contacts the wheel pack.

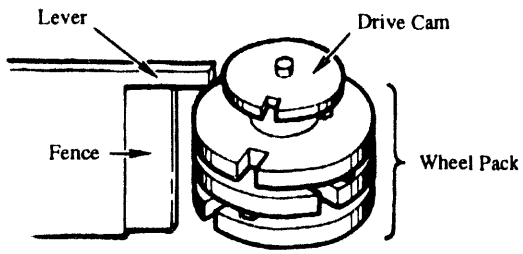

Figure 3-30. Drive cam action (padlock)

Bolt Assembly

The bolt is usually attached to the lever. When the correct combination is dialed, the door lock lever couples the drive cam to the bolt, converting dial rotation into bolt-sliding motion.

The fence is usually an integral part of the lever and is cast, staked, or soldered into place. The entire assembly is normally fabricated from brass, although in older style locks the bolt material is often steel.

The bolt of the combination door lock is used to directly secure the door or to secure a larger mechanism consisting of multi-locking bolts which secure the door to its frame. Most combination door bolts are extended, preventing door movement or multi-locking bolt movement. Bank vault locks are usually of heavy construction and are designed to push/pull a larger mechanism which secures the door.

3.2.2.1 Combination Lock Options and Variations

Manipulation Resistance

Prior to the early 1950s, combination locks were susceptible to unauthorized opening by means of manipulation. Various methods of manipulation can still be used to defeat many present-day locks. For this reason, combination door locks are evaluated and labeled according to their resistance to manipulation. A Group 2 lock is considered "reasonably resistant to unauthorized entry." A Group 1 lock is considered "resistant to manipulation for 20-man-hours." (See ANSI/UL 768.)

One operating feature which makes manipulation possible is the contact made by the fence as it touches the code wheels. If the fence of a combination lock always rested on the code wheels, it would be an easy matter for an individual to rotate the dial and feel or hear each wheel gate as it passed under the fence. However, many present-day locks incorporate options which greatly lessen or completely eliminate fence/wheel contact until an opening is attempted. In a Group 2 lock, the fence is allowed to touch the code wheels only when the lever nose drops into the drive cam gate (once every 360° rotation). The fence is raised when the lever nose slides out of the drive cam gate area. Figure 3-31 illustrates this type of design. However, even though fence/wheel contact occurs infrequently, manipulation is still possible.

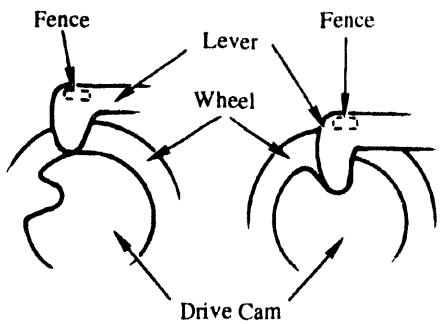

Figure 3-31. Group 2 lock

The resistance to manipulation of combination locks has been greatly increased by the addition of such devices as noisemakers, eccentric rollers, and other features which limit the time of fence/wheel contact.

Noisemakers cover or camouflage authentic fence/wheel contact by means of a spring-loaded detent that rides against the drive cam. It is used in conjunction with a modified spring-loaded drive cam designed to click automatically, thereby eliminating any discernible fence/wheel contact. Figure 3-32 illustrates one type of drive cam noisemaker.

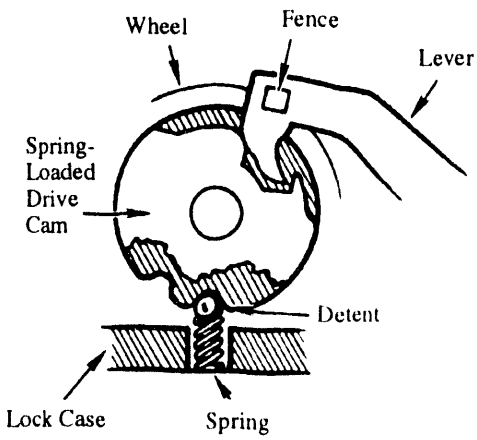

Figure 3-32. Noisemaker

Fence/wheel contact normally occurs at repeatable points in every 360° revolution and can be used as reference points for manipulating a lock. Placing a freely rotating eccentric roller on the nose of the lever changes the lever position as it enters and exits the drive cam gate. This causes the fence/wheel contact area to change each revolution. A lever with an eccentric roller is shown in Figure 3-33.

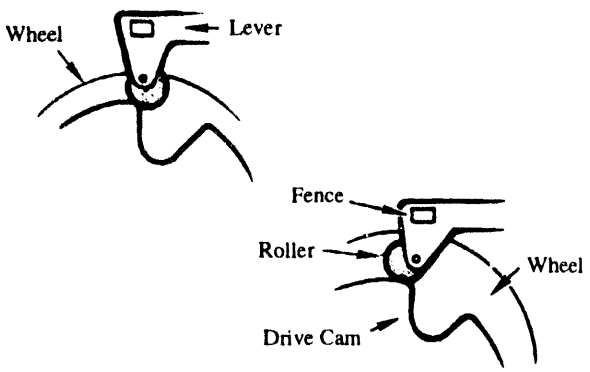

Figure 3-33. Eccentric roller

Another method of impeding manipulation is to eliminate the fence/wheel contact completely until an actual opening attempt is made. One manufacturer accomplishes this by using a sliding drive cam which has no gate opening during normal rotation. During dialing, the lever nose slides along the circumference of the "gate-less cam," keeping the fence from resting on the code wheels. When an attempt is made to open the lock after the combination has been dialed, the dial is turned to the lever/cam engagement position, in this case zero ("0"). The modified cam is then adjusted at the dial, using a knob or "butterfly" attached to an inner spindle assembly. The cam slides apart revealing a gate area. If the correct combination has been dialed, the spring-loaded lever drops into the cam gate, allowing bolt withdrawal. If the combination dialed is incorrect, the wheel gates will not be aligned; consequently, the fence rests on the wheel pack with the lever restricted from withdrawing the bolt. If another opening is attempted, the drive cam gate slides back into concealment while the combination is dialed. The series of illustrations in Figure 3-34 shows two types of concealed drive cam gates.

An older variation of a manipulation-resistant lock is the rotary-fence, gear-driven lock (see Figure 3-35). Dialing in one direction forces the fence away from the wheel pack; dialing in the opposite direction forces the fence against the wheel pack. Some locks of this type are still in use today.

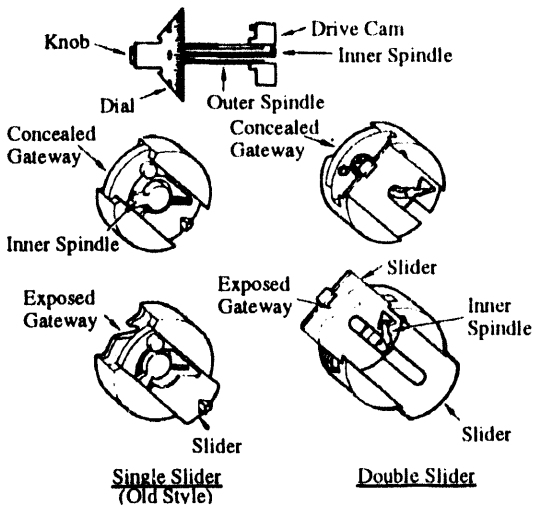

Figure 3-34. Concealed drive cam gates

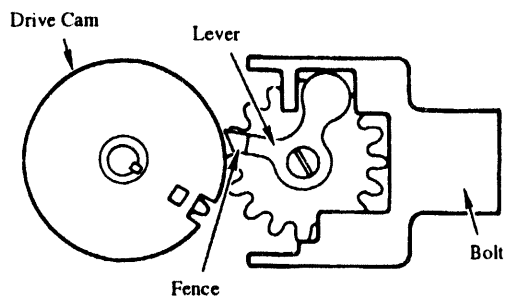

Figure 3-35. Rotary-fence gear-driven lock

Another anti-manipulation design uses spring momentum to force the lever nose into the drive cam gate when an opening is attempted. After a combination has been dialed and the dial returned to zero ("0"), the entire dial is depressed. Depressing the dial, which can only occur with the dial on zero, releases a large, cocked accelerator spring, the moving mass of which momentarily attempts to force the lever nose into the drive cam gate. If the combination dialed is correct, the wheel pack gates will be aligned, allowing the fence to nest into the wheel pack, and lever/cam engagement to occur. If the combination is not correct, only momentary fence/wheel contact occurs, with a second spring pulling the lever back into its original position. If nesting and engagement do not occur, the combination has to be redialed. Recocking the accelerator spring requires no more than one rotation of the drive cam. Figure 3-36 illustrates how this spring-loaded lever action works.

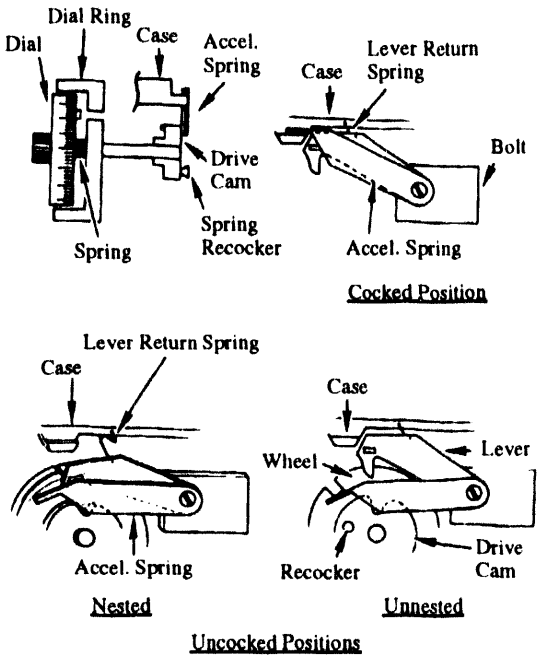

Figure 3-36. Spring momentum

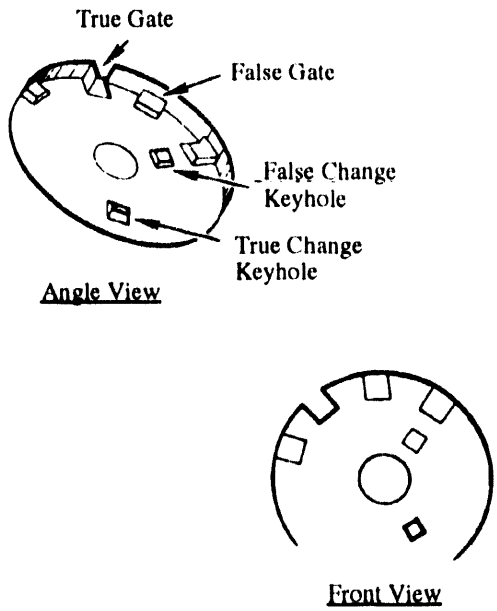

Figure 3-37. X-ray resistant code wheel

Radiographic Resistance

Another option to be considered in selecting a combination lock is its ability to resist radiographic attacks. Combination locks are evaluated and labeled according to their resistance to radiographic decoding. A lock labeled Group 1R is considered resistant to manipulation with the added capability of withstanding 20 man-hours of radiographic attack (see ANSI/UL 768). Wheel design and fabrication material greatly affect the quality of the radiographic pictures an attacker can produce.

Delrin and Lexan are common plastics used to counter an x-ray radiography attack. Simple to highly complex false gates and key-change hole designs are also used in an effort to increase x-ray resistance. Two views of a code wheel which incorporate x-ray resistant designs are shown in Figure 3-37.

Relocking Devices

Relocking devices (or relockers) are incorporated into lock cases and multi-bolt locking systems. These devices are typically designed to react against forcible attacks. Combination door locks are normally equipped with a case cover relocker. If the case cover is forcibly removed, a spring-loaded relocker is deployed, restricting bolt movement. An added feature to counter a thermal attack consists of a low-melt material (such as a Sarrie alloy) which, when melted, releases the relocker. Figure 3-38 illustrates some relocking devices.

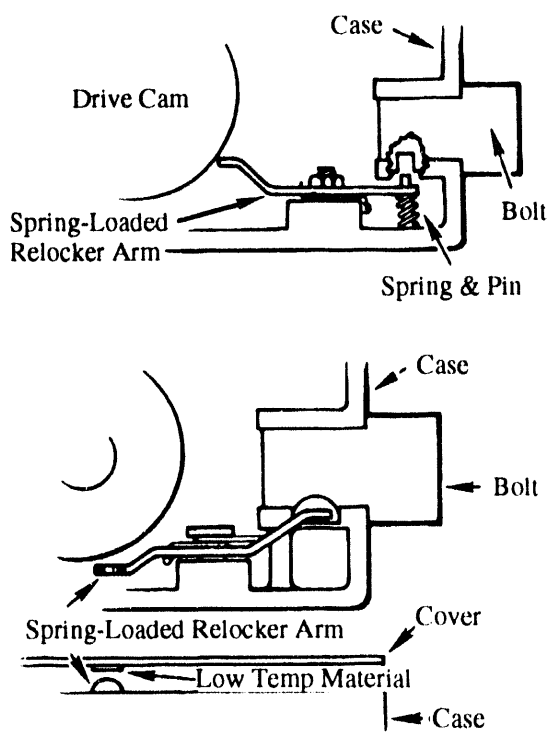

Figure 3-38. Relocking devices

Dial Assembly Design

Several different designs are commonly used to attach the combination dial to the spindle. Usually, the dial and spindle are fabricated as one piece, pressed together, or pinned. Some locks are designed to operate in various positions, making dial positioning adjustable. The drive cam is often splined to provide four hand positions: right, left, up, and down. Spindles are often covered to protect them from fire-insulating materials. Dials and dial rings come in a multitude of designs, and many options are available, including key locks which secure either or both dial and ring; various spy-proof dial and dial ring sets which restrict visual observation of dial settings; and punch-proof spindles.

Vibration Resistance

Some factors affecting lock vibration resistance include balanced, lightweight wheels, wheel-pack torque loading, wheelpost tolerance, and lever spring loading (see Figure 3-39). These features are normally controlled by the manufacturer at the factory but vary greatly from one design to another. At present, only one manufacturer is installing an adjustable wave-spring wheel-pack torque washer that is adjustable from the outside of the lock case. The manufacturer recommends maintaining a 14 inch/ounce torque loading throughout the life of the lock.

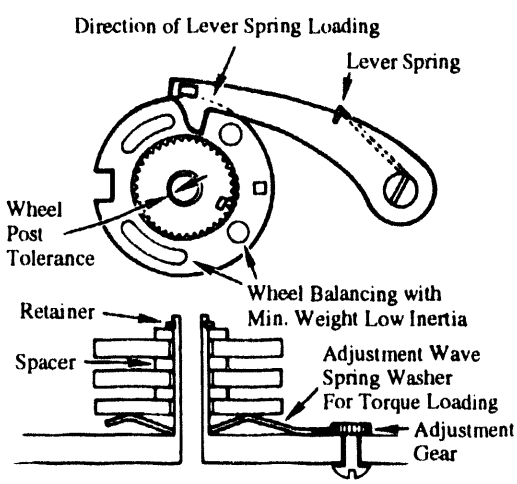

Figure 3-39. Factors affecting vibration resistance

Scrambling Device

The function of a scrambling device is to disrupt the alignment of the code wheels of an open lock when it is closed in order to prevent reopening the lock without redialing. This device is standard in high-quality key-change combination padlocks. When the shackle is inserted into the padlock body to reclose the lock, a spring-loaded metal pawl grabs two grooved wheels and freely spins them, usually from five to 15 numbers. Door locks lack this feature and have to rely upon the individual to secure the lock by spinning the dial in order to scramble the wheels. To scramble the combination completely, the dial needs to be rotated one more revolution than the number of code wheels within the lock.

Key-Change Hole Coverage

An obvious drawback to key-change versus fixed or hand-change combination locks is the presence of a hole in the lock case. Padlock key-change holes are often covered by spring doors or back covers (boots), as shown in Figure 3-40. These can be removed, exposing the keyhole, only when the correct combination is dialed. Key-change holes in door locks are normally exposed when unlocked unless concealed within the container door.

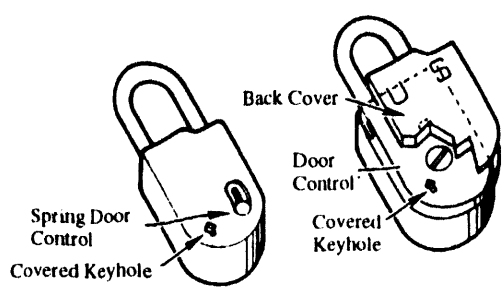

Figure 3-40. Padlock key-change hole

Padlock Shackle Features

Features of padlock shackles are discussed in Section 3.1.3 and are pertinent to combination padlocks as well as key-operated padlocks.

3.2.3 Application Considerations

3.2.3.1 Pros and Cons

Mechanical combination locks have some advantages over key locks. For example, they are less vulnerable to unsophisticated surreptitious attack because the lock mechanism is less exposed. Another advantage is that there is no need for a key, (other than, in some cases, a combination change key). The use of a combination lock also eliminates the need for duplicate keys where multiple access is required. Finally, changing the combination can be far simpler than re-keying a key lock.

If the combination lock is a key change lock, no disassembly of the lock is required.

There are also disadvantages of combination locks compared with key locks. Dialing a combination takes a longer time than inserting and turning a key. Also, traditional combination locks have no "master key" system available. Master keys allow locks to be segregated into groups with mutually exclusive access, but with master access allowed.

Some methods for defeating combination locks are decoding; systematic trial and error; environmental attacks, including heating and cooling; chemical attacks; x-ray radiography; sense manipulation; impact vibration; signature analysis; mechanical probing; and force. These methods are described in the Glossary.

3.2.3.2 General Design Features Which Increase Security

Some specific design features which increase security are included in Section 3.2.2. In this section, we discuss features to reduce vulnerability which apply regardless of the specific design.

- Knowledge of the correct, current combination should be a prerequisite for changing the combination. This prevents unauthorized individuals from installing a combination of their choosing, which would allow access at a later time.

- There should be no openings in the case of the lock through which a probe or other similar device may be introduced into the lock body. This includes change key openings as well as other openings. If a probe can be inserted into the lock body, the positions of the gates in the wheels may be decoded, providing the adversary with the combination.

- The combination should not be able to be determined when the lock is open without knowledge of the existing combination.

- The resistance to systematic trial and error attacks is directly dependent on the number of usable combinations which may be encoded in the lock and the rotational tolerance allowed in dialing a number.

  A permanently mounted, dial type combination lock should have a large number of combinations. UL Standard 768 and Federal Specification FF-L-2740 specify at least 1 million possible combinations. Additionally, Military Specification MIL-L-15596G specifies a minimum of 800,000 theoretical combinations. This may be those that are usable after discounting 20 numbers on the last digit according to manufacturer's directions.

  The rotational tolerance of the lock also affects the number of usable combinations. UL Standard 768 defines three classes of manipulation resistant lock: Group 1, Group 1R, and Group 2. Groups 1/1R have more usable combinations than Group 2. For Groups 1/1R, a number entered may be accepted only if it is within +/- one dial graduation of the true number for a three wheel lock or +/- 1 1/4 graduations for a four wheel lock. Group 2 locks allow the tolerance to be +/- 1 1/4 graduations for a three wheel lock or +/- 1 1/2 graduations for a four wheel lock.

  Requirements for combination padlocks differ from those for permanently installed combination locks. Federal Specification FF-P-110G requires a minimum of 30,000 combinations. Rotational tolerance for acceptance of an entered number is +/- 1/4 dial graduations.

- Permanently installed combination locks should be of high strength, high quality materials which exhibit resistance to wear and corrosion. UL Standard 768 and Federal Specification FF-L-2740 list general materials guidelines for lock construction, while Military Specification MIL-L-15596G lists specific materials and acceptance criteria. Properties of materials used for the construction of combination padlocks are specified in Federal Specification FF-P-110G. Specifications for testing padlocks may be obtained from FF-P-110G and ASTM F 883-90.

- The following features will provide a high level of tell-tale to unauthorized entry:

  The lock finish should be easily marred. If a lock has a finish which is easily damaged, it will provide an excellent indicator of attempted forcible entry. It may also indicate some forms of surreptitious entry.

  The lock construction and materials should be such that any attempt at unauthorized disassembly should permanently distort and mark the components.

  Forcible entry should irreparably damage the lock. This will prevent surreptitious forcible entry except in the case in which a complete replacement lock is available, and can be encoded with the correct combination from the damaged one.

3.2.3.3 Other Factors Which Affect Security

Vulnerabilities can be introduced due to wear and tear, corrosion, and lack of preventive maintenance.

First, a failure can be made credible. If a lock is broken, it could be attributed to the condition of the lock, rather than to

adversary attack. Furthermore, an adversary could forcibly open the lock, then substitute a non-working replacement lock.

Second, an adversary may be able to open the lock if he/she dials a combination close to, but not exactly, the correct combination.

Finally, a poorly maintained lock can be difficult to open by an authorized user. When a lock is difficult to open, it is also difficult to verify that it is locked, introducing another vulnerability.

3.2.4 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

3.2.4.1 Permanently Installed Combination Locks

ASTM F 471-76 - Standard Definitions of Terms Relating to Combination Locks

This document provides a glossary of standard terminology.

This specification may be obtained from the American Society for Testing and Materials.

ANSI/UL 768 - Underwriters Laboratory Standard for Combination Locks

This standard defines requirements for Group 1, Group 1R, and Group 2 combination locks, intended for permanent installation on safes, vault doors, security files, and other security containers. Group 1 locks have a high degree of resistance (20 man hours resistance under certain conditions) to opening by expert or professional manipulation, i.e. by sense of sight, touch, or hearing. Group 1 locks must include advanced design features not found in conventional designs. Group 1R has, in addition, a high degree of resistance to radiographic attack. Group 2 locks have a moderate degree of resistance to unauthorized opening. Combination locks covered by these requirements may or may not have protection against forcible entry.

Specifications cover resistance to unauthorized opening, mechanical construction, number of possible combinations, operational characteristics, endurance, and testing methodology. Non-metallic parts specifications include strength, impact resistance, moisture absorption, and resistance to distortion. For metallic parts, corrosion protection is specified. Also included are specifications for required markings.

This specification may be obtained from Underwriters Laboratories.

FF-L-2740 - Federal Specification, Locks, Combination

This specification covers changeable combination locks intended for permanent installation on safes, vault doors, security files, and other security containers. Locks which meet the requirements set forth in this document are approved by the General Services Administration for use by all Federal agencies.

Locks covered by this specification must meet the requirements for resistance to unauthorized opening of Group 1R in ANSI/UL 768. The Federal specification adds to and elaborates on the requirements of ANSI/UL 768. For example, specific design features, such as mechanical and thermal relock, are required. As another example, the test procedure allows a greater weight of tools to be used than is allowed by ANSI/UL 768. The Federal specification also includes a covert entry requirement not included in ANSI/UL 768.

Other requirements included are the number of possible combinations, complexity of combination change procedures, design, construction, operation, quality assurance responsibilities, testing procedures, environmental specifications, standard marking and packing requirements, and a brief discussion of materials. Other applicable standards and specifications are referenced.

This specification may be obtained from the Defense Printing Service.

MIL-L-15596G - Military Specification, Locks, Combination, for General Services Administration-Approved Security Containers, Vault Doors, and Safe Lockers

This specification covers changeable combination locks intended for permanent installation on safes, vault doors, security files, and other security containers. Locks which meet the requirements set forth in this document are approved by the Department of Defense (DoD) for use by all departments and agencies of the DoD.

There are two notable differences between this specification and FF-L-2740. First, MIL-L-15596G covers materials requirements in detail. Second, MIL-L-15596G covers manipulation and forcible entry, while FF-L-2740 covers surreptitious and covert entry.

ANSI/UL 768 Group 1 or Group 1R is a prerequisite for locks meeting this specification.

Other requirements include physical size and layout; number of possible combinations; complexity of combination change procedure; mechanical design, construction, and operation (including endurance and tolerance); quality assurance responsibilities; testing procedures; environmental specifications; protection time specifications for manipulation and forcible entry; and standard marking and packing requirements. Other applicable standards and specifications are referenced.

This specification may be obtained from the Defense Printing Service.

MIL-HDBK-1013/8 - Military Handbook, Combination Locks

This handbook provides basic instructions for the installation, operation, and maintenance of various permanently installed combination locks and combination padlocks. Also included are instructions for changing and setting combinations for hand-change and key-change locks. Specific models of locks are covered in detail.

This specification may be obtained from the Defense Printing Service.

3.2.4.2 Combination Padlocks

ASTM F 883-90 - Standard Performance Specification for Padlocks

This is summarized in Section 3.1.4.

FF-P-110G - Federal Specification, Padlock, Changeable Combination (Resistance To Opening By Manipulation And Surreptitious Attack)

This specification covers changeable combination padlocks which provide low level resistance to forced entry, and moderate resistance to manipulation and surreptitious entry. In addition, a high level of tell-tale to unauthorized entry is specified. Locks which meet the requirements set forth in this document are approved by the General Services Administration for use by all Federal agencies.

There are two classes of combination padlocks. Class 1 has 30 man-minutes resistance to manipulation, 30 minutes resistance to radiographic techniques, and 10 man-minutes resistance to surreptitious entry. (Note that the definition of surreptitious entry differs between this specification and FF-L-2740.) Class 2 is the same as Class 1 except that it has no requirement for resistance to radiographic techniques. Neither class has any requirement for resistance to forced entry. Detailed test procedures include the following: manipulation techniques, surreptitious attack, radiographic, direct tension, jarring, shackle breaking, and dropping. Other requirements include physical size and layout; number of possible combinations; mechanical design, construction and operation; materials; quality assurance responsibilities; environmental specifications; wear and corrosion; and standard marking and packing. Other applicable standards and specifications are referenced.

This specification may be obtained from the Defense Printing Service.

3.3 Bolts, Strikes, and Latches

This section covers descriptions, illustrations, and discussions of the role of both mechanical and electrical bolts, strikes, and latches in security systems.

In a permanently installed access control system, the most common method of joining the movable barrier (door) to the fixed barrier (wall) is to use a bolt or latch coupled into a strike. This is true whether the system is mechanical or electrical, key or keyless, simple or sophisticated. Figure 3-41 shows a typical mounting configuration of a bolt, strike, and latch.

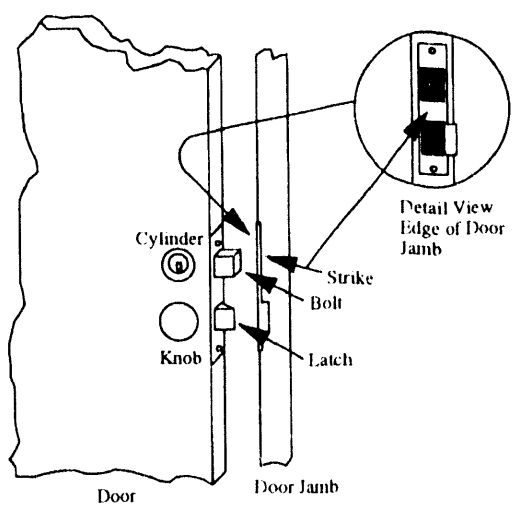

Figure 3-41. Typical mounting configuration of a bolt, strike, and latch

Typically, bolts and latches are mounted on the door. Locking occurs when the door is closed and the bolt or latch projects into a recess in the door jamb. The difference between a bolt and a latch is that a latch will automatically retract as the door is closed, whereas a bolt stays in the same position unless it is intentionally moved. Bolts are typically uniformly thick,

movable devices intended to block motion perpendicular to their direction of travel. Latches are beveled and spring-loaded so they will automatically retract. They are more convenient, and more vulnerable, than bolts.

A strike is used to strengthen the recess into which a bolt or latch projects. Strikes may be active or passive. The only function of a passive strike is to strengthen the recess. Passive strikes are strictly mechanical in nature, but may be used with both mechanical and electrical bolts and latches. An active strike allows the door to be opened when pressure is exerted on the door. Active strikes are generally electrical, and contain moving parts which constrain or release the bolt.

Bolts, latches, and strikes may be either mortise-mounted or rim-mounted. Depending on the design of the hardware, the bolt or latch mechanism may be mounted to either the door or jamb, with its associated strike mounted to the remainder of the two.

Some locking devices are designed to function either mechanically or electrically. An example is a mechanical lock mounted on the door combined with an electrical strike on the door jamb.

3.3.1 Uses

Bolts, strikes, and latches are the actual securing mechanisms in a lock, whether mechanical or electrical. Mechanical bolts, strikes and latches are primarily used in securing portals that do not require remote control operation.

Electric bolts, strikes, and latches are used in security systems where centralized control is required. One application of electric bolts is in prisons to secure cell doors controlled from a central guard station. Electric strikes are often used in security area access control systems, and are actuated remotely by a security officer after identity is verified, for example, by closed circuit television. This allows a centralized location to control access through many portals. Electric bolts, strikes, and latches are also used in electronic access control systems which use devices such as key pads, card readers, and eye scanners for electronic recognition.

The selection of electrical versus mechanical bolts, strikes, and latches is a decision which should be driven by the degree of security needed and by cost-effectiveness. If there is only one entrance to a facility and a guard is needed for continuous monitoring, a mechanical system is probably the right choice. Mechanical locking systems are probably also the right choice if a portal does not need to be continuously monitored, and if unlocking by authorized personnel is relatively convenient. However, if multiple portals have to be continuously guarded, one guard with the ability to remotely monitor and control may be more cost-effective. In this case, an electrical locking system may be the right choice.

3.3.2 Hardware Description: Mechanical Bolts, Strikes, and Latches

Mechanical bolts or latches are generally designed to be integrated with the lock mechanism, with a key or combination lock required to actuate the bolt or latch located in close physical proximity. Sometimes the bolt or latch is contained within the same enclosure as the lock, as in a permanently mounted combination lock (see Figure 3-19). Sometimes the lock is mounted separately with mechanical coupling to the bolt or latch.

A mechanical bolt is constrained in its projected position by interference with a solid obstacle, whereas a latch is projected by a spring. Both types of constraining mechanisms are used in padlocks and door locks, and are activated either by a key or keyless mechanism. The bolt or latch is usually a spring-loaded latch, a dead-locking latch (deadlatch), or a deadbolt.

A spring-loaded latch is shown in Figure 3-42. The convenience of this device is offset by its vulnerability; exerting end pressure on the beveled surface will cause the latch to retract.

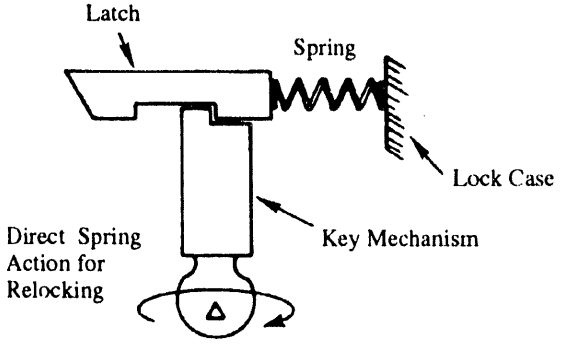

Figure 3-42. A spring-loaded latch

Deadlatches and auxiliary deadbolts are often used to increase security. A deadlatch has a plunger which is depressed as the door is shut, placing an obstacle in the path of the spring latch which restricts its movement. This is shown in Figure 3-43.

A deadbolt has no spring action. Deadbolts are either positively or intermittently coupled (Figure 3-44). When a positively-coupled deadbolt is fully projected, it cannot be unlocked by exerting end pressure. Key locks which are positively coupled require correct

key operation for unlocking. Intermittently coupled key locks can often be defeated by bolt manipulation without operation of the key mechanism.

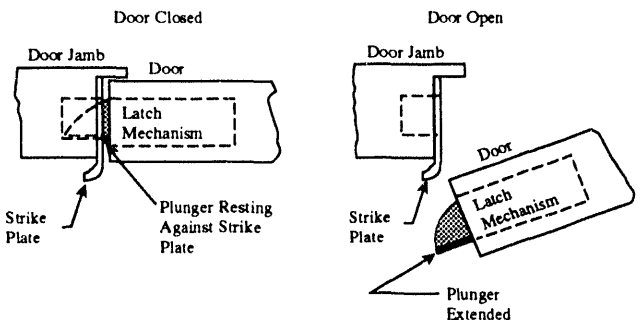

Figure 3-43. Example of dead-locking latch, looking down from top of door

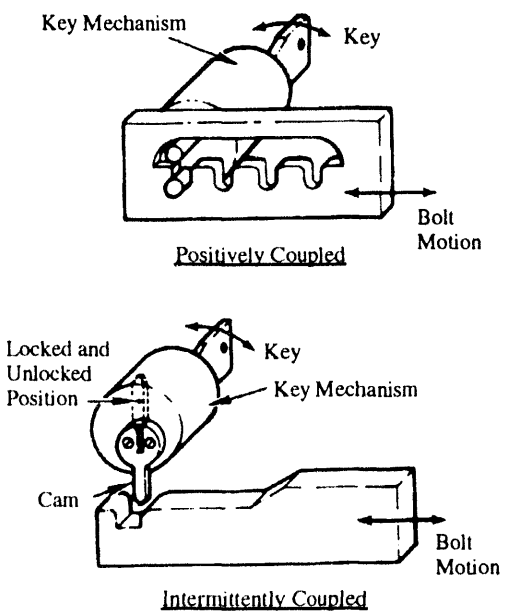

Figure 3-44. Key-operated deadbolt

The bolt and code wheel mechanisms in quality combination locks are intermittently coupled, but bolt movement is usually restricted to when the gate is aligned. In Figure 3-45, the case prevents the bolt from moving to the left until the fence drops into the gate.

A typical passive strike serves as a reinforcement for the recess into which the bolt or latch projects. The simplest passive strike is a formed plate of metal with a hole in the center. The bolt or latch projects into the hole. Some passive strikes have a full enclosure into which the bolt or latch projects. Strikes intended for use with latches typically are beveled to assist the spring latch in retraction.

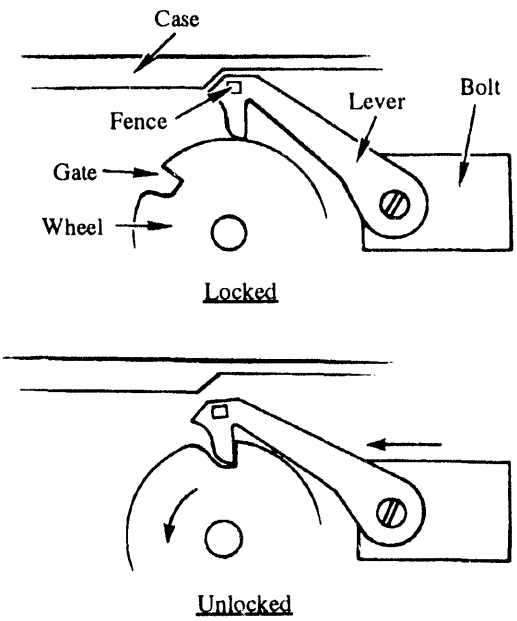

Figure 3-45. Intermittently coupled bolt (combination lock)

3.3.3 Hardware Description: Electrical Bolts, Strikes, and Latches

Electrical bolts, strikes, and latches are often physically removed from the locking circuitry. The locking circuitry usually consists of an electric control system which may be a few feet or a few miles away from the bolt, latch, or strike.

The operation of electric bolts and latches is controlled by application of power to either a solenoid or an electric motor. A solenoid becomes an electromagnet when power is applied. The solenoid then exerts a magnetic force on the appropriate mechanism, which removes a barrier allowing the user to retract the bolt or latch. An electric motor can be used to perform the same function as the solenoid, and while it is more secure, it is also more expensive.

Figure 3-46 shows a simplified drawing of a motor-driven electric bolt. A reversible motor drives a gear train coupled to a lead screw. When the lead screw is rotated in one direction, it threads into the bolt, retracting it. Rotation in the other direction extends the bolt.

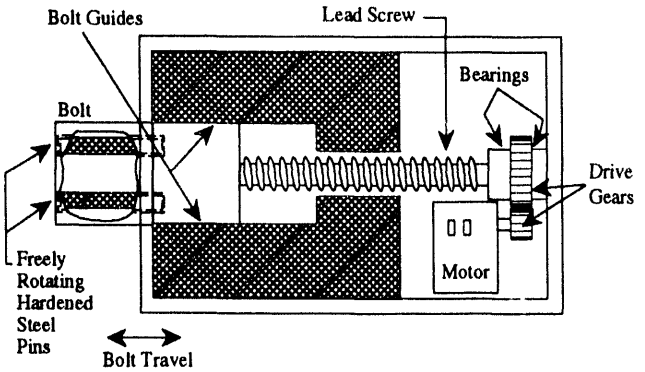

Figure 3-46. Example of electric bolt with motor driven lead screw

Bolts, latches and strikes operate in one of two modes: fail safe or fail secure. Fail safe is usually preferred because it is less dangerous (see Section 7, Safety Considerations of Locks). However, it degrades security because, in the event of a power failure, it automatically unlocks. Auxiliary power supplies are usually required.

Electric strikes are active; i.e. they have moving parts which can be used to lock or unlock the door. Figure 3-47 is an example of a fail secure electric strike. Figure 3-48 is an example of a fail safe electric strike. The difference is that the fail safe device unlocks when power is removed, and the fail secure device locks when power is removed. Both strikes are solenoid operated.

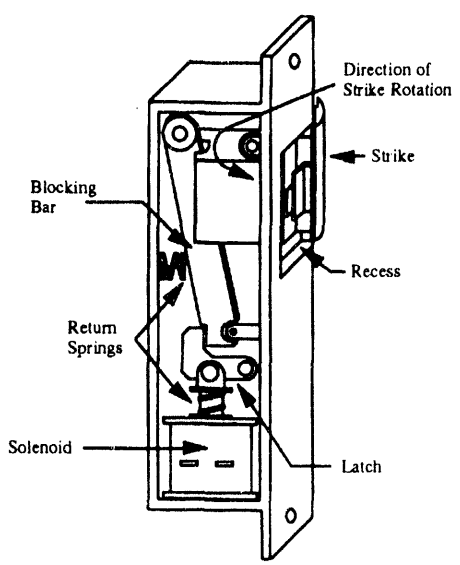

Figure 3-47. Example of a fail secure electric solenoid-operated strike

The fail secure strike operates as follows. When the solenoid is energized, it pulls the latch down. The blocking bar is then free to move, and the strike is free to rotate. A latch (not shown) projects into the recess when the strike is locked. When the door is pushed, it puts pressure on the latch, which puts pressure on the strike. The strike pushes the blocking bar out of the way as the door is opened. When power is removed, the return springs push the blocking bar to the right, and the latch up, preventing the strike from rotating and the door from being opened.

The fail safe strike operates as follows. The solenoid is fixed in place. When power is applied to the solenoid, it pulls an assembly (consisting of the washer, a shaft, and the blocking bar) up. When the blocking bar is up, the strike cannot rotate and the door cannot be opened. When power is removed, the return spring pulls the blocking bar down, allowing the strike to rotate, and the door to be opened.

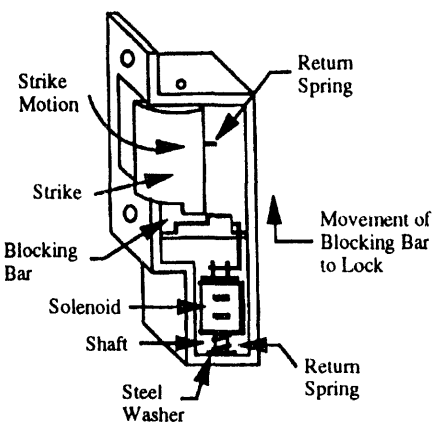

Figure 3-48. Example of a fail safe electric solenoid-operated strike

3.3.4 Application Considerations

3.3.4.1 Pros and Cons

One advantage of mechanical bolts, strikes, and latches is their relatively low cost compared to their electrical counterparts. This low cost includes not only the cost of purchase, but reduced installation cost. For a mechanical system, installation is simpler, and no wiring is required.

Attack methods such as shimming, drilling, sawing, and environmental and chemical attacks can be used to defeat both

mechanical and electrical devices. In addition, electrical devices may be vulnerable to attacks on the power supply or the wiring. Devices which use a solenoid may sometimes be defeated by magnetic attack. Electric motor driven devices do not share this vulnerability. The attack methods are described in the Glossary.

Mechanical devices have fewer types of vulnerabilities than electrical locks. This does not necessarily mean they are more secure. The entire picture should be considered: i.e., the design of the mechanical lock, the design of the electrical lock, continuous monitoring, alarm systems, response to crises, etc.

There are a couple of disadvantages to mechanical devices. One is that they typically have no means of reporting status to a central facility. Another disadvantage is the necessity for the physical presence of an authorized unlocker. Depending on the remoteness of the installation, this can result in significant time delays, both in time to allow access and in time to respond to a crisis.

Electric bolts, strikes and latches have several advantages. One advantage is the ability for one security officer to monitor and control access remotely for multiple portals. This may be cost-efficient when compared to the cost of having multiple security officers, or the inconvenience of reducing the number of portals. Another advantage is that electrical devices can be coupled with electronic recognition systems, such as keypads, card readers, and eye scanners. A third advantage that electrical devices offer is a choice between fail safe and fail secure operation. Caution should be used in making this selection. If a device is chosen to fail secure, then personnel may be placed in danger. If a device is chosen to fail safe, a power failure will provide a breach of security. Fail safe devices should have backup power supplies. Fail secure devices may require emergency exit hardware.

Complexity of installation may be considered a disadvantage of electric devices, especially if a relatively large distance separates the control unit from the lock. Communications, usually wiring, need to be supplied between the control unit and the remote lock. In addition, each lock needs to be supplied with electrical power, and sometimes backup power.

3.3.4.2 Design Features Which Increase Security

Features Common to Mechanical and Electrical Bolts, Strikes, and Latches

- Physical size and strong materials generally make these devices more difficult to forcibly defeat. They provide additional time to allow security forces to respond to a breach of security. Examples are the bolts and latches used in prisons and bank vault doors.

- Monitoring door status (open or closed), either by security personnel or by an automated alarm system, can increase security.

- Construction of exposed areas of the device using case-hardened steel may reduce vulnerability to drilling and other small tools. In addition, case-hardened pins which rotate freely may be installed in the bolt or latch to prevent sawing. Figure 3-46 shows how this is done in a bolt. An attempt to saw through the bolt results in the saw blade resting against the pin, which rotates, and prevents further cutting.

- Latches which incorporate deadlatching devices are more secure than latches without them. Deadlatches block attempts to open the latch by shimming.

- For key locks, positively coupled deadbolts are more secure than intermittently coupled deadbolts.

- The strength with which a device is fastened to the door or jamb may also affect security. For instance, using more fasteners, or fasteners which extend deeper into the door or jamb material may increase security.

Features Specific to Electrical Bolts, Strikes, and Latches

- Motor-operated devices are generally more secure than those operated by a solenoid because solenoids are vulnerable to magnetic attack.

- It is important to protect power sources and wiring. Both should be installed inside the secure area.

- Motor-operated devices which depend on the rotation of a cam or lead screw should use case-hardened materials to fabricate covers and any part of the mechanism used to move the bolt, particularly the lead screw or cam.

3.3.5 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

ANSI/BHMA A156.5-1984—American National Standard for auxiliary locks & associated products, Part II

Part I of this standard covers auxiliary bored and mortise locks, rim locks, and cylinders and includes security tests, operational tests, finish tests, and dimensional criteria.

Part II of this standard establishes requirements for exit alarms, exit locks, electric strikes and indexed key control systems and includes operational and finish tests.

The following is a summary of the portion of Part II concerned with electric strikes. Other parts of this standard are reviewed in the appropriate section of this document.

The standard defines three grades of electric strikes, Grades 1, 2, and 3, with Grade 1 being the best both in operation and security. As a minimum requirement for Grade 3 certification, the standard requires that electric strikes meet ANSI/UL 1034. For Grades 1 or 2, tables are provided which show the enhanced requirements for endurance cycling and force.

The standard also contains finish, corrosion resistance, electrical, and safety requirements.

Descriptions and drawings of different types of electrical strikes are included. Each different strike has a type number which is used to specify strikes which meet this standard. The number refers to this standard, and gives information on material, type of product, specific product function, and grade.

This specification may be obtained from the Builders Hardware Manufacturers Association.

ANSI/UL 1034 - Burglary Resistant Electric Locking Mechanisms

This specification covers a broad spectrum of topics including electromagnetic locks, and electric strikes, bolts, and latches. Security and personnel safety also are addressed.

This specification goes into extreme detail on requirements for electrical enclosures, field wiring, internal wiring, wire sizes and lengths, color of ground wires, insulation thickness, wiring methods, circuit separation, grounding options, splicing, component mounting, insulation, power supplies, overcurrent protection, printed wiring boards, semiconductors, transformers, materials, resistance of terminal connections, and minimum internal spacings required for appropriate voltage holdoffs.

Testing is specified in a wide range of areas. Electrical testing includes normal operations, input and output measurements for the power supply, standby power, over- and under-voltage, leakage current, electric shock current, voltage overload, dielectric voltage withstand, electrical transient, battery replacement, disconnection and reconnection, and terminal assemblies.

Environmental tests check temperature, temperature rise, humidity, and moisture absorption. Resistance to distortion and creeping at temperature is also required.

Mechanical tests for endurance, strain relief, mechanical strength, jarring, sureness of terminal connections, and flexing of wire without breaking are discussed.

Tests for flammability and resistance to ignition from electrical sources are required, and include fire resistance to hot flaming oil, molten PVC, and molten copper. An abnormal operation test is also required to show that the risk of fire or electric shock is not increased.

Tests specific to electric locking mechanisms include a salt spray corrosion test, rain test, dust test, forcing tests, and tool attack tests.

This specification may be obtained from Underwriters Laboratories.

ANSI/BHMA A156.2-1989 - American National Standard for bored and preassembled locks & latches

This standard is summarized in Section 3.1.4.

ANSI/BHMA A156.12-1986 - American National Standard for interconnected locks & latches

This standard is summarized in Section 3.1.4.

ANSI/BHMA A156.13-1987 - American National Standard for mortise locks & latches

This standard is summarized in Section 3.1.4.

3.3.6 Directory of Certified Locks and Latches

This document is published yearly by the Builders Hardware Manufacturers Association. The directory is a listing by manufacturer and model number of devices meeting the requirements of ANSI/BHMA A.156.2 and 156.13. Manufacturers may choose to participate in the certification program whether or not they are BHMA members.

This directory may be obtained from the Builders Hardware Manufacturers Association.

3.4 Mechanical Coded Locks

Mechanical coded locks are briefly described in this section. They are convenience locks which are used in low security applications. However, they are so commonly used that a description is included for purposes of completeness.

3.4.1 Uses

These locks are designed to prevent casual observers and passers-by from entering an area.

3.4.2 Hardware Description

A mechanical coded lock is a self-contained door lock. Push-buttons are used for entry of the combination. Following combination entry, the latch or bolt may be withdrawn. These locks contain up to 10,000 possible combinations.

There are several push-button lock designs on the market which contain a five- or ten-button display for code entry (see Figure 3-49). Code selection varies from a one-number to a seven-number code. Often, the same number can be repeated and different numbers can be pushed simultaneously.

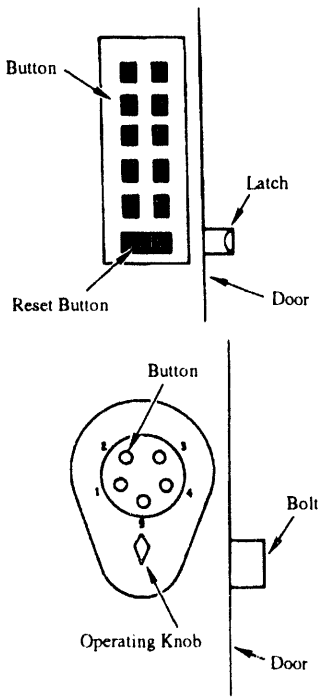

Figure 3-49. Mechanical coded push-button locks

The code mechanism varies among manufacturers. In one design, the spring-loaded latch/bolt is held in the locked position by two coded sliding plates which move up and down each time a button is pushed. Friction between the bolt and the coded plates holds the plates in position. When the correct code is entered, gates located in the plates allow latch/bolt withdrawal. A reset button realigns the coded plates in their initial position. Code combinations can only be changed by replacement of internal parts.

Another push-button design associates each button with a gated gear wheel. When a button is pushed, it rotates its corresponding gated wheel one increment and rotates each previously operated wheel one increment also. Rotation of the door control knob, which is attached to a try bar/fence arrangement, allows latch/bolt withdrawal and/or automatic repositioning of the gate wheels to their initial position. This mechanism is widely used and can be easily recoded.

3.4.3 Application Considerations

Coded locks have one significant advantage over key locks in that they eliminate the potential for breach of security resulting from lost, stolen or impressioned keys. However, they often are designed with bypass key control in case of mechanical failure. Key bypass can also be used by security personnel when it is impractical for them to remember combinations to every lock.

While providing a minimum level of security, these locks have the advantage that they are quick and easy to operate. The combinations are usually shorter and easier to remember than a dial combination lock.

An extensive list of vulnerabilities is not appropriate for this type of lock, since it would not be chosen for its ability to withstand attack by an adversary. However, it should be noted that a systematic trial and error attack by a passer-by has a reasonable probability of success because there are not that many combinations available.

3.5 Electromagnetic Locks

3.5.1 Uses

The primary use of electromagnetic locks is in access control systems. A commercial example is that a receptionist can permit or deny access to the premises without having to walk over to the door. Because of their strength, electromagnetic locks can also be used in security area access control systems. They can be actuated remotely by a security officer after the person desiring entry is identified. This allows a central location to control access to many portals.

An electromagnetic lock can be used in conjunction with an identity verification system, such as a card reader, keypad, fingerprint or hand shape recognition device, eye scanner, or other automated identification system.

By adding additional wiring, it would be straightforward to combine an electromagnetic lock with an automated monitoring or alarm system.

3.5.2 Hardware Description

An electromagnet is made from a coil of wire. When an electric current passes through the coil, it creates a magnetic field, turning the coil into a magnet. The higher the current, the stronger the magnetic field. The magnetic field ceases as soon as the current ceases.

In a standard design, the electromagnet will be surface-mounted on the door jamb, and a strike plate made of a magnetic material, such as steel, will be surface-mounted on the door (see Figure 3-50). When the current is turned on, the electromagnet and the strike plate will be magnetically attracted, locking the door. When the current is turned off, the door is automatically unlocked.

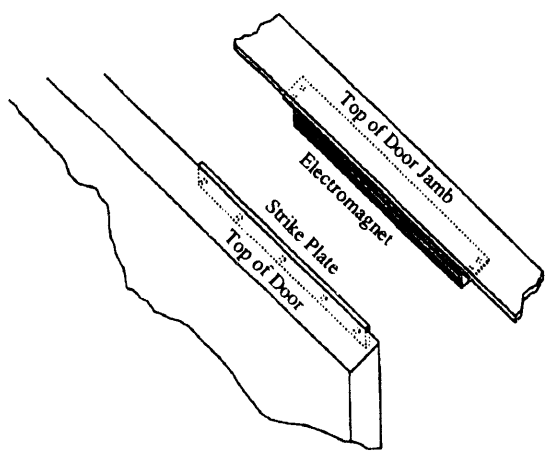

Figure 3-50. Typical electromagnetic lock

An alternative design is the shear-type electromagnetic lock, shown in Figure 3-51. This design mounts into recesses in the door and door jamb, thus hiding the lock from view. The part mounted in the door recess will typically have movable steel "bolts." These are attracted to the electromagnet in the door jamb when the door is closed and the current is applied. They act as deadbolts to strengthen the door against forcible attack.

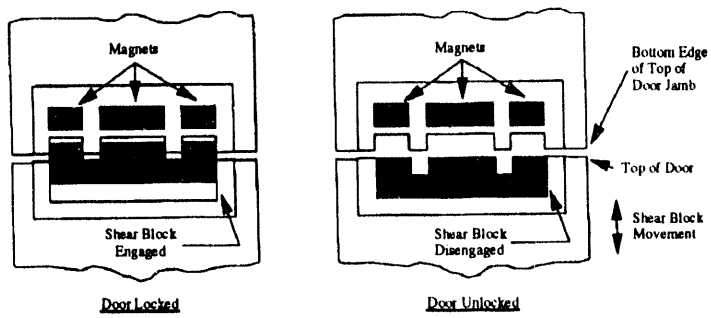

Figure 3-51. Cross section of shear-resistant electromagnetic lock

The strength of commercial electromagnetic locks ranges from approximately 600 to 1,200 pounds. Thus, electromagnetic locks can be made as strong as desired, limited only by such practical matters as size and cost.

3.5.3 Application Considerations

3.5.3.1 Pros and Cons

One advantage of electromagnetic locks is the ability for one security officer to monitor and control access to multiple portals. This is potentially more cost-effective than having multiple officers. However, savings on personnel need to be traded off against the cost of installation.

Electromagnetic locks work well with electronic identification systems, automatic monitoring, and alarms. As a result, electromagnetic locks are extremely well-suited for high security applications.

Electromagnetic locks are intrinsically fail-safe because when power is removed, the electromagnet is no longer attracted to the striker plate. While these devices are safe, the disadvantage is that a simple power failure will provide a breach of the security perimeter. Auxiliary hardware and a backup power supply are required to make such a device fail-secure.

Because there are no moving parts, an electromagnetic lock should require little maintenance.

Complexity of installation may be considered a disadvantage, especially if a relatively large distance separates the control unit from the lock. Communications, usually wiring, need to be supplied between the control unit and the remote lock. In addition, each lock needs to be supplied with electrical power.

Because the electromagnetic lock is so dependent on its power supply, it is vulnerable to attacks on the power supply and the wiring.

Electromagnetic locks, especially those which have a lower holding force, are vulnerable to magnetic attack. An intense magnetic field in close proximity may be able to override the electromagnet, allowing the door to open.

3.5.3.2 Design Features Which Increase Security

- Power sources and interdevice wiring should be protected. Service wiring should always be inside the protected volume, and backup power should be considered.

- The force necessary to open an electromagnetic lock can vary from approximately 600 to 1,200 pounds. The lock should have enough holding force for the intended application.

- Monitoring of door status (open or closed) either by security personnel or by an automated alarm system can increase security. It is straightforward to combine an electromagnetic lock with an automatic monitoring system. This can be done by using a sensor to detect when the electromagnet and the strike plate are joined. Since wiring is needed for the electromagnet anyway, the additional wiring for the sensor can be added at the same time.

- Some electromagnetic locks incorporate mechanical locking devices to allow fail-secure operation. An example is shown in Figure 3-52.

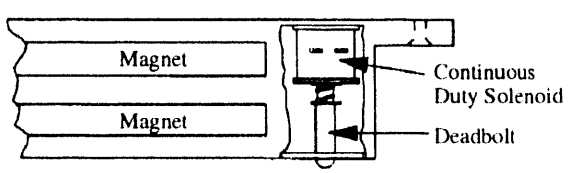

Figure 3-52. Fail secure electromagnetic lock

- The shear-type electromagnetic lock shown in Figure 3-51 may improve security because of the deadbolt action of the steel. However, this type of lock may need the deadbolt action to withstand a level of forcible attack comparable to the standard electromagnetic lock. Which design is more vulnerable depends on the details of the designs being compared.

3.5.4 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

ANSI/UL 1034 - Burglary Resistant Electric Locking Mechanisms

This specification is summarized in Section 3.3.5.

3.6 Self-Contained Electronic Combination Locks

Unlike entry control systems which utilize electric bolts, strikes, and latches, self-contained electronic locks (hereafter abbreviated electronic locks) require no external wiring. Within the lock case are electronics, a power supply, and the locking mechanism. The electronics contains memory to store the combination, and logic to determine whether the correct combination has been dialed. The logic is also used to control security features such as two person control, different combinations for each user, limited try feature, and time delays. Depending on the design, an electronic lock may have significant advantages over its mechanical counterpart.

An understanding of Sections 3.2, Combination Locks, and 3.3, Bolts, Strikes, and Latches, will be helpful in understanding this section.

3.6.1 Uses

Electronic combination locks have been designed to replace their mechanical counterparts in applications requiring medium to high security. This includes safes, vault doors, and other security containers.

3.6.2 Hardware Description

3.6.2.1 Overview

The function of electronic locks is the same as that of mechanical combination locks: to recognize a correct combination and allow retraction of the bolt. The method by which this is accomplished, however, is quite different.

Power Source

Electronic locks may receive power from a generator or a battery. One system has two batteries so that one can power the lock while the other is being replaced. Some locks have external battery compartments which allow rapid battery replacement.

Combination Storage

A feature of some electronic locks is that combinations are stored in non-volatile memory. This type of memory does not require constant power to retain its data. Other lock designs require power to store the combination.

Combination Entry

Some electronic locks use a keypad for combination entry. An alternative design is to use a dial which looks similar to a traditional combination lock, but has an electronic display screen. In yet another design, the dial is marked with numbers, but the number dialed is not electronically displayed.

Electronics Design and Security Features

The electronics package consists of a generator or battery, microprocessor, and other circuit components. The functions of the electronics package are to store combinations in memory, accept entry of combinations, compare entered combinations with stored combinations, recognize changing of combinations, and activate the unlocking mechanism when a correct combination is entered.

Depending on the design, the electronics package may also keep track of and display other information such as the number of opening attempts, the number of failed opening attempts, the dates and times of past openings, and which user opened the lock. This information can potentially be used to determine if the lock has been attacked.

There are many other security features offered by electronic locks. Not all features are offered on any particular design. For instance, each user may be assigned a different combination; a time delay may be required before the lock can be opened; the lock may be able to be opened only at specified times; a limited try feature may prevent the lock from functioning if an incorrect combination is attempted too many times; the lock may be able to recognize an autodialer; and a tamper alarm may be added. All of these features have potential value in security systems.

Methods for Releasing the Lock Mechanism

Once the combination is properly entered, there are several ways to move the bolt. For example, a latch may be closed by spring action, and opened with a solenoid; a motor driven deadbolt is also possible. Still another alternative is for the user to provide the mechanical action to retract the bolt, as is done on mechanical locks.

3.6.2.2 Hardware Description - MAS-Hamilton X-07

Figures 3-53 and 3-54 show the design of the MAS-Hamilton X-07 as viewed from the front and back. This particular electronic lock is the only lock which at this time is GSA-approved; it meets the requirements of Federal Specification FF-L-2740. For this reason, more information is presented on the X-07 than on other electronic locks. In the future other electronic locks may be approved by GSA.

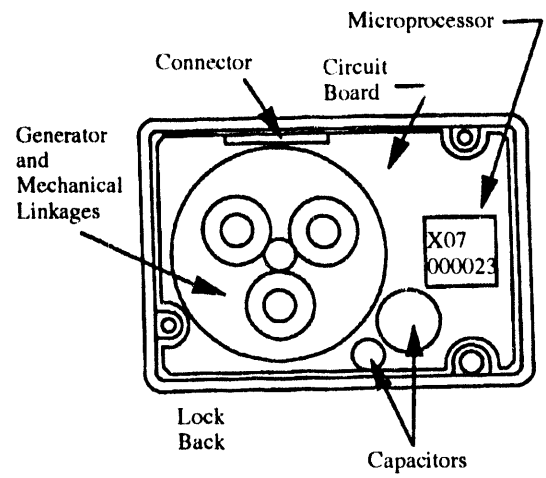

Figure 3-53. X-07 Rear cover/electronics package

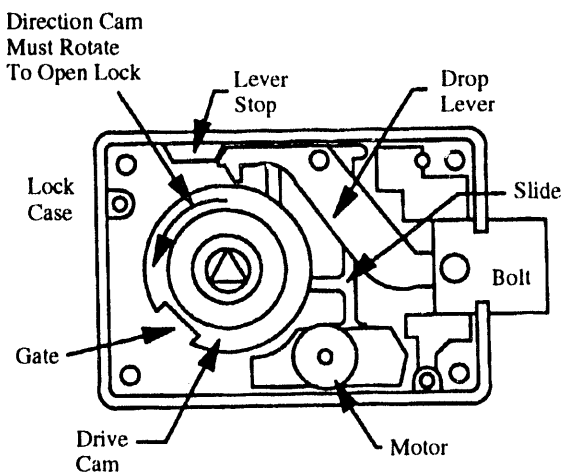

Figure 3-54. Back view of X-07

Power Source

In the X-07, the dial is attached to a spindle which goes through mechanical linkages to drive a small electric generator. Four to six turns of the dial generate sufficient power for the electronics. The power is stored by the capacitors shown in Figure 3-53.

Combination Storage

The MAS-Hamilton X-07 stores combinations in non-volatile memory.

Combination Entry

The X-07 uses a dial without markings; there is no correlation between dial position and the number displayed on the built-in screen. In addition, the limited viewing angle screen is designed to be difficult for a bystander to read. Both features make the lock more secure.

Electronics Design and Security Features

The electronics package consists of a generator, microprocessor, and other circuit components. The electronics package stores combinations in non-volatile memory, accepts combination entry, compares the entered combination with stored combinations, recognizes combination changes, and activates the unlocking mechanism when the combination entered is correct.

The X-07 lock has three modes of operation: single combination mode, dual combination mode, and supervisor/subordinate mode. In the single combination mode, the lock is operated by a three-number combination. This is comparable to the mechanical combination lock. In single combination mode, this electronic lock has a full one million possible combinations. Unlike a mechanical combination lock, the number of usable combinations is not degraded by tolerances and combinations which cannot be used because the lock mechanism may jam.

In dual combination mode, two different three-number combinations have to be entered within forty seconds to operate the lock. This allows two-person control. The X-07 has five hundred billion combinations in dual combination mode.

In supervisor/subordinate mode, the subordinate combination is active only between entries of the supervisor combination. Thus the supervisor can control when a subordinate has access to the safe. The lock has two million combinations in supervisor/subordinate mode.

The X-07 has the capability to detect attempted defeat by autodialer; if the dial is moved continuously with no pauses, moved with short, quick, repetitive turns, or the combination is entered in less than 15 seconds, the X-07 will refuse access.

Dial Assembly

The X-07 has some notable features in its dial assembly. First, there is the liquid crystal display screen and its associated circuitry. The display screen provides all communication between the lock and the user. Second, the dial assembly holds metal tubes in place which in turn provide physical protection for the wiring. These metal tubes also protect against electronic emanations which an adversary might use to defeat the lock through signature analysis.

Methods for Releasing the Lock Mechanism

Once the combination is properly entered, the bolt may be retracted. The X-07 uses a small motor to move a blocking device called a slide. The movement of the slide moves the drop lever below the lock case lever stop and into contact with the gate in the drive cam (see Figure 3-54). The bolt can then be retracted by dialing in the direction shown in the figure. This allows the user to provide the mechanical action to retract the bolt, as is done on mechanical locks.

3.6.3 Application Considerations

3.6.3.1 Pros and Cons - Overview

The electronic combination lock has some advantages over both mechanical combination locks and key locks. It has many features not offered by mechanical locks which can be used to enhance security; these are covered in the hardware description section. A disadvantage is that the electronic locks need power to operate.

Electronic locks may be vulnerable to certain attacks, including decoding and force. These vulnerabilities are described in the Glossary. Potential vulnerabilities are based on descriptions of the locks and not on experimental analysis. Manufacturers may have additional information.

Unlike a mechanical combination lock, an electronic lock is not vulnerable to radiographic attack. Since there is no mechanically stored information, x-rays cannot be used to determine the combination.

3.6.3.1.1 Pros and Cons - MAS-Hamilton X-07

The X-07 allows the combination to be recoded if the serial number of the lock is known. This requires the security container to be open so that the change key receptacle is accessible. In contrast to a mechanical combination lock, the existing combination is not a prerequisite for changing the combination. This feature helps prevent lockout - a situation in which the lock is unusable. While knowledge of the serial

number is not sufficient to open the lock, it may increase vulnerability to adversary attack. Therefore, it is important to protect the serial number of the lock to the same degree as the information the lock is protecting.

3.6.3.2 General Design Features Which Increase Security

These design features are quite similar to those for Combination Locks, Section 3.2.3.

- Knowledge of the correct, current combination should be a prerequisite for changing the combination. This prevents unauthorized individuals from installing a combination of their choosing, which would allow access at a later time.

- There should be no openings in the case of the lock through which a device may be introduced into the lock body. This includes change key openings as well as other openings. For mechanical locks, one concern is that a device could help decode the combination. For an electronic lock, unauthorized operation of the motor or solenoid is a concern.

- The combination should not be decipherable when the lock is open.

- The resistance to systematic trial and error attacks is directly dependent on the number of usable combinations which may be encoded in the lock. Some electronic locks are designed to permit huge numbers of possible combinations, far more than their mechanical counterparts.

- The materials used for the construction of permanently installed combination locks should be high strength and high quality, and exhibit resistance to wear and corrosion.

- The following features will provide a high level of tell-tale to unauthorized entry:

  — The lock finish should be easily marred. If a lock has a finish which is easily damaged, it will provide an excellent indicator of attempted forcible entry. It may also indicate some forms of surreptitious entry. The lock construction and materials should be such that any attempt at unauthorized disassembly will permanently distort and mark the components.

  — Forcible entry should irreparably damage the lock. This will prevent surreptitious forcible entry except in the case in which a complete replacement lock is available, and can be encoded with the correct combination from the damaged one.

3.6.3.3 Specific Design Features Which Increase Security

- The ability to recognize and resist opening by autodialers was one of the original reasons for developing electronic locks. This can be accomplished with a limited try counter, or by detecting dialing speed.

- The use of encryption to store the combination in a different form after each use would make it extremely difficult to determine the combination through emanations.

- Features such as time delays, time locks, and limited try counters help to restrict access to authorized personnel at authorized times.

- The ability to report the number of openings and attempted openings can help determine if unauthorized entry has been attempted.

- Knowledge of when a particular user opened the lock, with time and date, can help both in attack deterrence and detection.

- Dissociation between dial position and displayed number can make it extremely difficult for a bystander to determine the combination. A related factor is limited viewing angle of the display.

- The use of electronics which have low emanations will make electronic locks less vulnerable to a "bugging" attack. Factors which affect emanations are power dissipation, rise and fall times, wiring, and shielding.

- Precision balancing of the lock mechanism helps to increase the difficulty of vibration attack.

- Bolt mechanisms driven by a motor rather than a solenoid are less vulnerable to magnetic attack.

3.6.4 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

The following specifications are summarized in 3.2.4. Though some parts of these specifications were written for mechanical locks, they all contain information which is also applicable to electronic locks.

ASTM F 471-76 - Standard Definitions of Terms Relating to Combination Locks

ANSI/UL 768 - Underwriters Laboratory Standard for Combination Locks

MIL-L-15596G - Military Specification, Locks, Combination, for General Services Administration Approved Security Containers, Vault Doors, and Safe Lockers

The following specification is required for GSA approval:
FF-L-2740 - Federal Specification, Locks, Combination

3.7 Hirsch Electronics Access Control Systems

3.7.1 Uses

Products manufactured by Hirsch Electronics Corporation are not locks since the user chooses and supplies the locking mechanism. Hirsch products are more accurately described as access control systems. The appropriate use is control of access to a secured area.

Though Hirsch products do not include a locking mechanism, this section is included because of DOE interest.

3.7.2 Hardware Description

There are two main product lines produced by Hirsch: the Digi*Trac series and the ScrambleLock series. These two product lines have significantly different capabilities.

Overview

The ScrambleLock is a limited-scope, limited-capability access control system. It controls access through one or two doors by sending appropriate electrical signals to locking mechanisms on the doors. The ScrambleLock has two assemblies: the controller and the keypad (ScramblePad).

The Digi*Trac is a highly configurable access control system. Three distinct product capabilities exist: access control, alarm monitoring, and relay control. This discussion will focus on the access control capabilities, though controllers designed for access control may contain some features of alarm monitoring and relay control.

In its maximum configuration, each Digi*Trac access control system can control access for up to 8 doors, monitor 16 alarm inputs, provide up to 16 relay closures for control applications, provide multi-lingual printer listings of events (accesses, alarms, etc.), and accept programming input from a remotely located or central computer system. To expand these capabilities, Digi*Trac systems programmed with similar user bases may be added. Because of its configurability, the number of assemblies will vary.

For both the ScrambleLock and the Digi*Trac, the locking mechanism is separate, and is added by the user.

Power Source

The ScrambleLock and the Digi*Trac both contain an internal power supply which may be configured to operate from either a 110- or 220-volt power input. Backup power is supplied by an internal rechargeable battery which is charged and monitored by the controller. An AC power-fail indicator is provided.

Combination Storage

Combinations are stored in battery-maintained memory in the controller cabinet. The ScrambleLock can store a maximum of 8 access codes while the Digi*Trac may store from 1000 access codes (minimum configuration) to 16,383 access codes (maximum expanded capability). These codes are chosen from over 110,000,000 possible codes of 3 to 8 digits in length.

Electronics Design and Security Features

The ScrambleLock controller performs the following electronic functions: recognizes the combination, stores the combination, accepts input from the keypads, and sends the appropriate signal to unlock the locking mechanism. The controller also handles several security features, including time delay, time lock, and limited try counter. The most sophisticated version of the time lock allows access according to specific times and days.

The ScrambleLock controller cannot monitor external alarm systems. The only other input device allowed besides the keypad is an exit pushbutton.

In addition to expanding the features above, the Digi*Trac provides a duress digit for codes entered, printer logging of events, computer interface, and the ability to accept input from a wide variety of identification devices rather than only the keypad.

The duress digit is a digit which may be entered after the final digit in the user's code. When entered, operation proceeds as normal, except a "Duress by User at ScramblePad" alarm is logged to the printer, and the "Duress Alarm Relay" is tripped. This relay may be used to notify a central alarm monitoring

facility that the system is being operated under duress, such as the user being forced to allow access.

The identification devices may be card readers, hand geometry scanners, retina scanners, or any other compatible identification device. They may also be used in combination, i.e., hand geometry in addition to code entry. The Digi*Trac controller allows a maximum of 16 external alarm inputs to be monitored.

The keypad is typically located remotely from the controller. The function of the keypad is to accept user input and send it to the controller. A maximum of two keypads may be used as inputs to one ScrambleLock controller, while the Digi*Trac may use a maximum of 16. ScrambleLock system programming may be performed from either keypad, or the system may be configured to accept programming from only one keypad. In addition to keypad programming, the Digi*Trac may be programmed from a serial terminal or a remote computer system.

Although both the ScrambleLock and the Digi*Trac may use keypads other than those manufactured by Hirsch, Hirsch strongly recommends using the Hirsch ScramblePad. This is because of the security features of the ScramblePad.

The primary security features of the ScramblePad are the scrambled digits and the limited viewing angle of the display. Displayed numbers are randomly located, or scrambled, with each access request. These features make it more difficult for an adversary to determine the combination.

Combination Entry

The face of the ScramblePad contains 12 unlabeled keys and one key labeled "Start." The pattern of unlabeled keys is similar to a standard touch-tone telephone keypad.

The keypad is blank when not in use. When the "Start" key is pressed, a random pattern of the digits 0 through 9 appears behind ten of the keys. The user keys in the code, then presses the "pound" key. If the code is valid, the controller will unlock the lock. If three attempts are made to enter an invalid code, the limited try feature, "code tamper alarm," will cause the system to lock out, i.e., stop receiving inputs, for one minute. An audible alarm sounds during lock out.

Methods for Releasing the Lock Mechanism

The ScrambleLock and Digi*Trac are compatible with electric bolts, strikes, latches, and magnetic locks. The output is a relay closure which can switch power to these devices.

3.7.3 Application Considerations

3.7.3.1 Pros and Cons

The Hirsch ScrambleLock and Digi*Trac share the advantages and disadvantages of Self-Contained Electronic Combination Locks (Section 3.6.3.1).

3.7.3.2 General Design Features Which Increase Security

These design features are identical to those for Self-Contained Electronic Combination Locks (Section 3.6.3.2).

3.7.3.3 Specific Design Features Which Increase Security

Features such as time delays, time locks, and limited try counters help to restrict access to authorized personnel at authorized times. The Hirsch ScrambleLock provides programmable time delays and limited try counters in all models, and time zone (i.e., time lock) functions in two models. The limited try counter initiates automatic lock out and an audible alarm with the entry of a third invalid code ("code tamper alarm").

In addition to expanding these features, the Hirsch Digi*Trac includes external alarm monitoring and event logging to printer. If the Digi*Trac is connected to a remote computer, communications are accomplished via proprietary software which makes use of data encryption.

There is complete dissociation between key position and displayed key number on the ScramblePad. Since the number position changes with each operation, pad wear is uniformly distributed.

One potential vulnerability of all combination locks is that a bystander may see the combination entered. The viewing angle of the ScramblePad allows a 26 degree vertical range for viewing, but only a 4 degree horizontal viewing angle. This severely limited viewing angle provided by the ScramblePad makes it extremely difficult for a bystander to determine the combination.

Another advantage of the Hirsch products is that separate enclosures are used for the ScramblePad and the controller. This places the control electronics inside the secured area. Both enclosures are protected by physical tamper alarms. In addition, wiring and power supplies should be inside the secured area.

The controllers contain built-in diagnostics to monitor and verify proper operation.

The large number of possible combinations (over 110,000,000), coupled with the limited try lock out, make guessing the combination or trial-and-error methods of defeat unlikely.

3.7.4 Standards and Specifications

Standards and specifications pertaining to Electronic Access Control Systems are beyond the scope of this document.

3.8 Additional Hardware Issues

The purpose of this section is to briefly mention some hardware issues which are associated with, but not central to, locks. The intent is to make sure that the reader is aware that these issues should be addressed. However, the information is not presented in depth.

The most important topic is the discussion of commensurate levels of security. Other topics include hinges, screws, hasps, hardened barriers, doors, and door jambs.

3.8.1 Commensurate Levels of Security

It is important to match the security of the lock to the security of the rest of the protected container. If the levels of security of different parts of the system vary widely, there will be a weak link for an adversary to attack. For example, a high security deadbolt lock will not enhance the security of a room if the door is hollow core wood.

A typical entry point for burglars breaking into commercial buildings is through a hole chopped through the roof of the building. False facades give good cover for the operation of cutting the hole, and roof entry bypasses all locks and portals.

3.8.2 Hinges

For security applications, hinges should be manufactured from strong materials, such as heavy brass, hardened steel, or stainless steel. In general, the more massive the construction of the hinge, the more secure the installation will be.

Hinges should be mounted with the hinge pin inside the protected area, if at all possible, and hinge pins should be either spot welded or peened to prevent removal.

Locking pins are useful in the installation of hinges. These are pins designed to replace one pair of screws in each hinge. The pin projects from the leaf of the hinge mounted on the door jamb into the mating hole in the moveable leaf, preventing the door from being removed even if the hinge pins are removed.

3.8.3 Screws

Special security screws should be used to mount security hardware located outside the secured area and, depending on application, sometimes those mounted inside the secured area. There are two basic varieties of security screws: those which cannot be removed once installed, and those which may be removed only with a special tool once installed. Adversaries are likely to have access to the special tool.

If screws are used where they are accessible by an adversary, they should be installed with their heads welded to the device they are securing. Screws used for mounting security devices should be hardened. If the hardware is mounted on wood, a higher level of security may be achieved by using screws long enough to embed themselves in the underlying structure.

3.8.4 Hasps

A hasp is a metal fastener with a minimum of two sections. The sections are attached to a movable and a fixed barrier or to two movable barriers. When the barrier(s) is closed, the two sections of the hasp are positioned together in such a manner that the shackle of a padlock can be inserted through both to fasten the two sections together. Only a few varieties of hasps are commercially available. Most are not comparable in quality (in terms of resistance to forcible attack) to the high-security padlocks which might be used in conjunction with them.

Hasp designs usually vary considerably due to different mounting requirements. Hasps can be either mounted with non-removable bolts or welded directly to the door or frame. Not all padlocks and hasps can be combined, but many are universally adaptable. Figure 3-55 illustrates a typical padlock/hasp configuration.

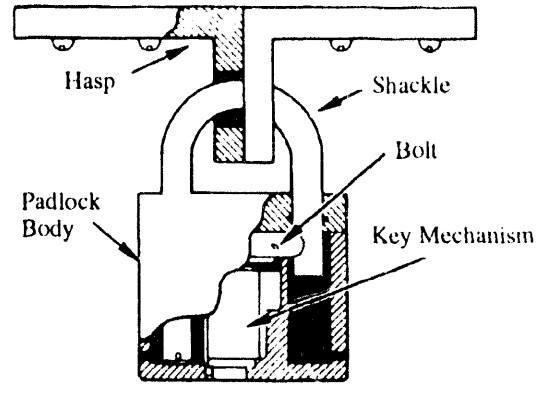

Figure 3-55. Cutaway view of key padlock and hasp

3.8.5 Hardened Barriers

Few locking devices contain hardened barriers to deter the use of force. Key cylinders occasionally contain hardened shields (plates or pins) to resist drilling (see Figure 3-56).

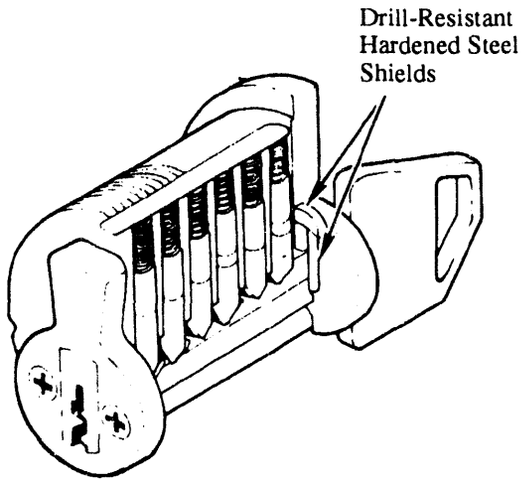

Figure 3-56. Hardened shields

Often padlock bodies and shackles are hardened, with shackle exposure ranging from exposed to totally concealed (see Figure 3-57).

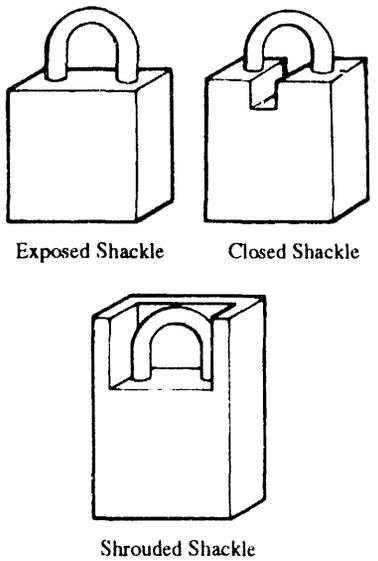

Figure 3-57. Shackle exposure

Almost totally hidden, hardened box-like concealment is obtainable for padlocks (see Figure 3-58).

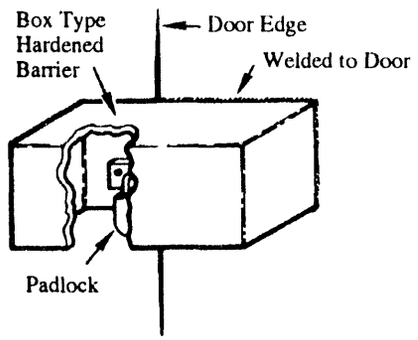

Figure 3-58. Hardened box padlock concealment

Since the amount of key rotation for padlocks is smaller than the key rotation for door locks, the padlock box can often be extended into the key-turning area, providing guard plate protection (see Figure 3-59).

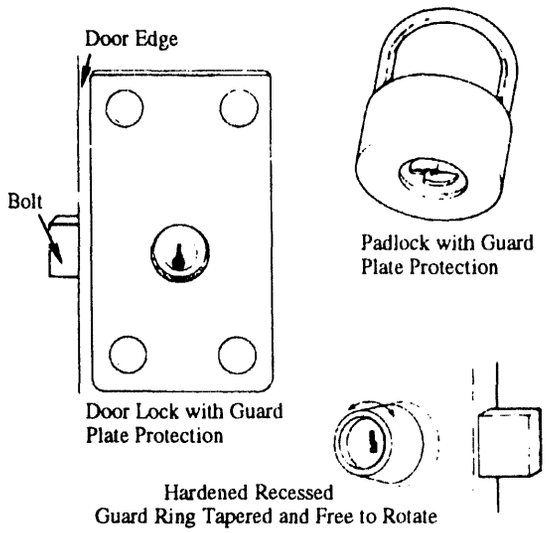

Figure 3-59. Hardened guard plates and rings

Generally, the more removed the lock is from the face of the door, the more protected its position. This protection can also be provided by the use of a guard plate which covers as much of the cylinder as possible while still permitting the key to be turned. Hardened guard rings should be recessed and have sufficient taper and rotation to withstand forcible defeat, as shown in Figure 3-59.

Safe and vault doors are often designed with a hardened plate surrounding the combination lock. The lock is usually embedded in the protected container, with relocking devices such as stressed glass covering vulnerable areas. Figure 3-60 illustrates a hardened combination lock.

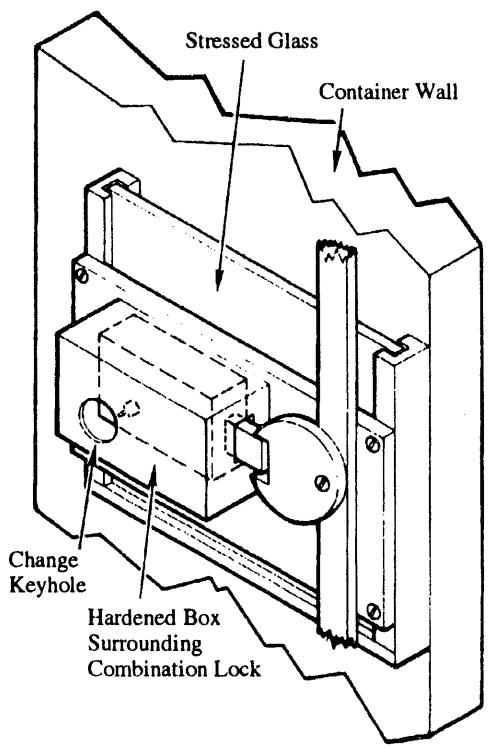

Figure 3-60. Hardened combination lock

3.8.6 Doors and Door Jambs

Doors and door jambs should be of secure construction. Many materials are used in the construction of doors and frames, ranging from glass and aluminum to wood or steel. Doors used as security portals should be manufactured of heavy duty material, preferably steel. If wooden doors are used, they should be of solid core construction. While glass panels in doors are esthetically pleasing, they degrade security considerably. Tough plastics, such as Lexan, are more impact resistant than glass, but suffer other vulnerabilities. For example, plastics typically cannot withstand high temperatures.

If wooden door frames are used in construction, any hardware secured to them should be installed using screws which are long enough to pass through the trim completely and embed themselves in structural members behind the trim. Door jambs manufactured from steel offer more security.

The door and jamb should fit as tightly as possible, while still operating properly. Excessive space between door and jamb may provide attack points for an adversary.

4 Vaults

Vaults are generally large walk-in structures with either single-leaf or double-leaf doors and reinforced concrete and/or steel walls, floors, and ceilings. Vaults are usually located within a larger structure, however, modular vault designs may be free standing or incorporated into a building structure. They may be designed to provide physical security for stored assets or fire protection. The designs for physical security protection and fire protection can be very different. The following discussion is limited to vault designs which provide protection against physical security threats.

4.1 Vault Construction

4.1.1 Uses

The design of a chosen storage vault should reflect the types of threats that may be attacking the vault. The location of the vault within a facility which has its own physical security elements may also influence a vault design. For example, an exterior wall location may provide an adversary with a stealthy penetration path, or permit the use of explosives on the wall or roof with the same impunity with which he could attack an exterior building wall.

When the vault is emplaced within the building, an adversary may be reluctant to use explosives, or may be limited in the amount he could detonate without causing structural building failure. Also, early intrusion detection and rapid security response to intrusion alarms can balance protection provided by the vault.

4.1.2 Hardware Description

A vault is generally composed of four basic structural elements--a floor, walls, a roof, and a door(s)--which should meet specific criteria for containment of material. In addition, some vaults have utility penetrations which should be considered as potential entry paths for adversaries.

An important consideration for any vault is a balanced design. All potential entry paths into the vault structures should be designed to provide approximately the same specified access delay into the interior. A standard, industrial pedestrian door on a vault constructed of 3 foot-thick reinforced concrete is an example of an unbalanced design.

The Bank Protection Act of 1968 (revised 1973), the American Society for Testing Materials (Standard F-1090), Underwriters Laboratories (UL) (Standard 608), and the Department of Defense (DoD 5220.22-M) all have different standards for vault construction which rank the thickness of walls, roof, floors, and doors in several classes with different construction options for walls, roofs, and floors. In general, as the sensitivity of the vault contents increases, the resistance to penetration of walls, doors, and other elements should also increase. The vaults should be constructed of materials that afford at least burglary equivalent resistance.

A design that has been used for some vaults (Figure 4-1) is one having walls, roof, and floor of at least 1/2-inch thick steel with fireproofing, or 12-inch thick, non-reinforced concrete, either of which can be penetrated rather quickly with the appropriate tools.

Table 4-1 shows the range of mean penetration times for typical vault walls. The door, the largest opening in the vault, should provide almost the same delay time as the other major elements. The vaults described above may be penetrated in several minutes.

4.2 Wall Construction

4.2.1 Uses

Reinforced concrete walls are commonly used as a cost-effective material in vault construction for supporting structural loads and for deterrence and delay against security threats. Concrete alone has good mechanical properties in compression, but little strength in tension and flexure, which are approximately 10% and 20%, respectively, of the value for compressive strength. Steel reinforcing resists the tensile and flexural loading.

4.2.2 Hardware Description

Reinforced concrete walls, 8 inches thick or greater, provide substantial resistance to hand, power, and thermal tool attacks. However, against explosives, thicker walls with heavy reinforcing bars (rebar) are generally required. Steel reinforcement can extend the penetration delay time against explosives in most designs. Even though the concrete may be penetrated by the explosion, the reinforcing material usually remains intact to the extent that it needs to be removed before entry can be accomplished. Removing the rebar often requires more time than is needed to remove the concrete; therefore, using additional rebar, increasing rebar size, or decreasing center-to-center rebar spacing can be advantageous.

The amount of explosives necessary to breach reinforced concrete surfaces increases significantly for wall thicknesses greater

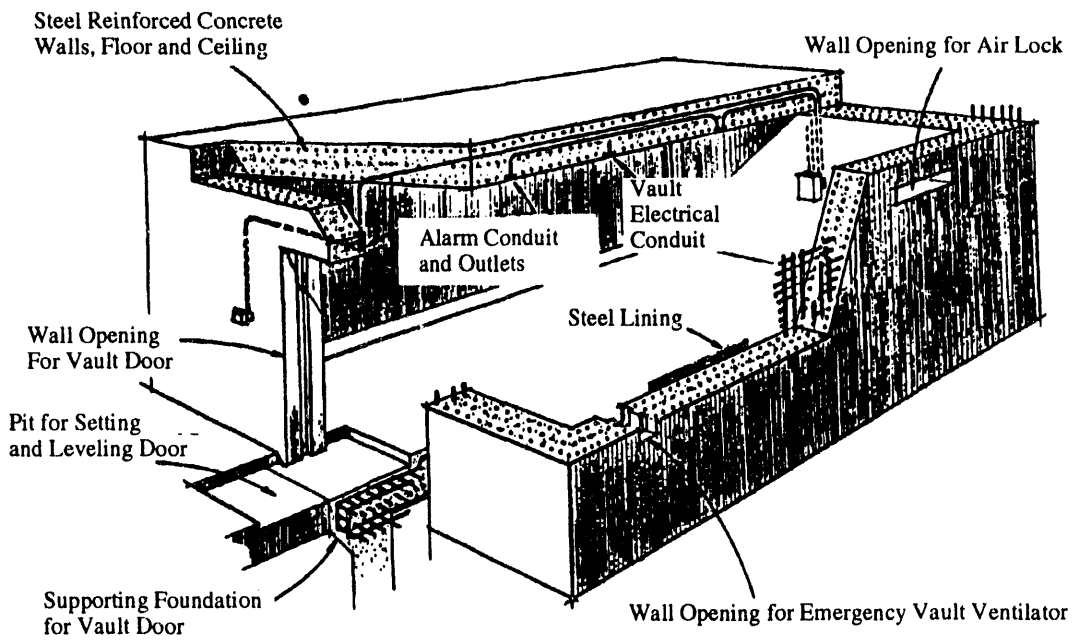

Figure 4-1. Typical vault construction

Table 4-1. Vault penetration mean times (minutes)

Vault Construction	Explosives and Tools	Hand, Power, Thermal Tools
1/2" Steel Plate with 4" Fireproofing	<5	<5 to 10
8" Concrete Block Deformed Bar Reinforcing	<5	<5 to 10's
8" Concrete Block Deformed Bar Reinforcing Cores Filled With Mortar	<5	<5
12" Concrete with Deformed Bar Reinforcing	<5	10's
12" Concrete with Expanded Steel Mesh	<5	10's
Class-5 Vault Door	<5	<5

than 18-24 inches. Also, the vault structure resistance to penetration can be improved by installing steel liner stall plates, spaced walls, standoff barriers, and soil overburden if the structures and location of the vault allow it. The use of steel liners can significantly improve explosive penetration resistance; however, the utilization of these liners does not necessarily allow a reduction in the reinforced concrete thickness of the wall. The liner is relatively vulnerable to thermal tool attack, and consideration should be given to delay times for both explosives and other tools.

Some vault surfaces are constructed with 3.64 lb/ft^2 or 6 lb/ft^2 expanded steel bank vault mesh with embedded steel reinforcing rod in a stacked placement serving as the reinforcing. In some designs, steel weights with this type of reinforcing can be greater than 50 lb/ft^3. Figure 4-2 illustrates an example of expanded metal concrete wall construction.

Finally, steel fiber reinforced concrete can be utilized for wall construction. These materials generally exhibit improved penetration resistance against power tool attacks and have

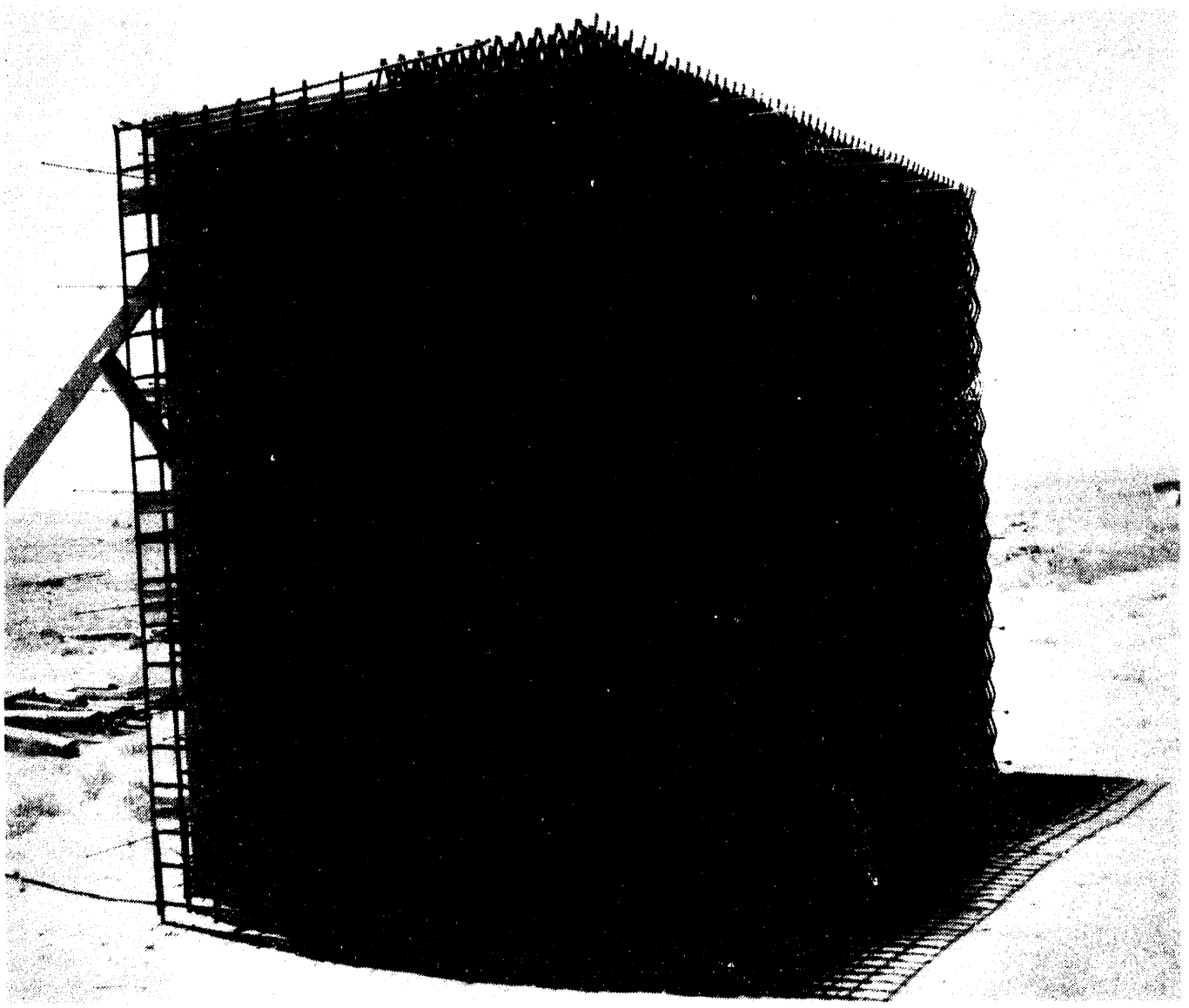

Figure 4-2. Expanded metal-concrete wall construction

penetration resistance comparable to standard reinforced concrete against explosive attack.

4.2.3 Application Considerations

4.2.3.1 Factors Which Affect Security

Penetrations in a vault structure--i.e., ventilation ducts--may provide a weak point in an otherwise hardened structure. These need to be considered in the overall design of the vault. In general, penetrations greater than 96 in^2 require the addition of barriers to provide delay commensurate with the overall vault construction.

4.2.3.2 Design Features Which Increase Security

Increased penetration resistance of a utility port may be achieved by the installation of protective coverings such as grills, bars, expanded-metal mesh, or screens. Similarly, grids and grates constructed of steel mesh, expanded metal, bar stock, tubing, or jail bars can be used to reduce the size of the opening in utility ports to less than crawl-through size.

Grills of 1/2 inch diameter mild steel rebar on 6-inch centers provide nominal delays of approximately one minute against hand tools. Increasing the bar diameter to 3/4 inch improves the delay time as hand tools become ineffective, and tooling of a higher category is required for penetration. Grills should have welded joints and should be constructed with a sufficient number of vertical and horizontal bars so that multiple cutting operations are required to produce a crawl-through opening. The protective grill should be adequately anchored to the wall to ensure that the time required to remove it and the level of difficulty involved are equal to or greater than the wall penetration time and difficulty.

Bar placement is important in the construction of grids and grates, and weight is a limiting factor. If more steel can be placed in an adversary's path, the delay will be greater. Floor grating of 2-1/4 x 3/16 inch steel can provide substantial penetration resistance against hand, power, and thermal tools. Other utility penetration enhancements include barbed tape liners or segmented ducts with rectangular or circular pipe.

4.2.3.3 Modular Vault Construction

Modular vault panels constructed of various combinations of steel, hardwoods, and precast concrete are commercially available. Depending upon specific requirements, these systems may offer construction time and possibly even cost benefits compared to permanent vaults.

Several commercial manufacturers have modular vaults which meet DOE minimum standards for an 8-inch reinforced vault wall. The access delay capabilities of commercial modular vaults are based on Underwriters Laboratories test standard UL608. UL testing of commercial modular vault walls results in ratings based on the net working time to make a 96-square-inch opening in the vault wall. The attacks considered for these ratings use only common mechanical tools, electric tools, cutting torches, or combinations of these. After testing, a modular vault wall panel is UL rated and placed in one of the four categories listed in Table 4-2.

The UL requirements for rating of modular vaults do not consider attacks with burn bars or explosives. The use of commercial modular vaults for any DOE application must be examined with respect to potential attack scenarios which include burn bars and explosives.

Typical commercial modular vaults rated by UL fit two wall types: concrete wall panel construction and laminated wall panel construction. The thickness and weight of individual concrete wall panels depends on the manufacturer's design to meet a specific UL ratings class. Class I wall panels are 3- to 4-inches thick and weigh 500 - 700 pounds; Class II panels are 5- to 6- inches thick and weigh 800 - 1200 pounds; and Class III panels are 8- to 10-inches thick and weigh 1200 - 1500 pounds. Panels are usually approximately 24 inches wide by 102 inches long.

Laminated wall panels offer the same UL rating as concrete panels at a savings in overall weight. Class M and Class I panels range from 3- to 6-inches thick and weigh 300 - 600 pounds; Class II panels are 7- to 10-inches thick and weigh 600 - 800 pounds; and Class III panels are 10- to 14-inches thick and weigh 800 - 1200 pounds.

Laminated panels are made differently by each manufacturer. The walls are usually constructed with a metal skin covering several layers of barrier material such as oak, pine, or expanded screen. Sufficient quantities of each material are used to provide necessary thickness to meet UL ratings. As a result, laminated panels may be up to 40% lighter than equivalent concrete panels. The cost is generally higher than for a cast-in-place concrete wall.

Construction of vaults using modular panels is the same whether the panels are concrete or laminated. Typically, a frame is anchored to the floor and panels are either bolted or welded to the frame. The wall panels are bolted or welded together at the seams, and the process continues until an enclosure, complete with roof, is formed. Finally, a vault door

Table 4-2 Protection classes and delay times

UL 608 Class	Delay Times (minutes)	Construction Specification
M	15	9-inch reinforced concrete, with a minimum of two grids of number 5 rebar, or two grids of expanded steel mesh weighing 6 lbs/ft^2 and having a diamond pattern not more than 3 by 8 inches placed parallel to the face of the slab; or Modular panels, Class M, Burglary-Resistant Vault, UL label; and Vault doors with UL Class M Vault Door label.
I	30	12-inch reinforced concrete with a minimum of three grids of number 5 rebar or two grids of expanded steel, as for M; or Modular panels with UL label for Class I Vault; and Vault doors with UL Class I Vault Door label.
II	60	18-inch reinforced concrete with a minimum of four grids of number 5 rebar or three grids of expanded steel, as for M; or Modular panels with UL label for Class II Vault; and Vault doors with UL Class II Vault Door label.
III	120	27-inch reinforced concrete with a minimum of five grids of number 5 rebar or four grids of expanded steel, as for M; or Modular panels with UL label for Class III Vault; and Vault doors with UL Class III Vault Door label.

is added. The doors may range from a Class V door to a commercial bank vault door. The value or sensitivity of the assets to be protected must be weighed against construction cost to obtain a balanced system.

4.2.4 Standards and Specifications

See Appendix A for addresses and telephone numbers of the ASTM and UL specifications.

There are a number of standards and specifications applicable to secure vault construction.

The ASTM vault construction Standard F-1090 is based on the UL Standard 608 for vault doors and modular vault panels. These standards specify protection classes based on net attack times by two skilled and knowledgeable adversaries. These standards consider only the use of common hand, power, and thermal tools to determine access delay times. Thermal lances and explosives are not considered in the tests.

The protection classes and delay times defined by the UL standard are outlined in Table 4-2. Also included are construction specifications for each of the protection classes as defined by the ASTM.

The Federal Reserve vault specification based on the requirements of the revised Bank Protection Act requires that vaults constructed after November 1, 1973 have walls made of steel-reinforced concrete, at least 12 inches thick.

4.3 Vault Doors

4.3.1 Hardware Description

Vault doors are usually classified according to the thickness of solid steel in the door. Security vault doors were formerly classified by the Insurance Services Office as 1, 3, 4, 5R, 6R, 9R, and 10R, with 10R indicating the greatest thickness (9-1/2 inches).

Classifications 11, 12, and 13 indicate recommended bank vault doors; mercantile vault doors were classified as B, C, E, and G. Although there is no exact correspondence between the bank and mercantile designations, the mercantile door classifications B and G roughly correspond to bank classification 1 and 5R respectively. Underwriters Laboratories and the Bank Protection Act requirements set the comparative ratings for vault doors as well as for other vault construction features.

4.3.2 Standards and Specifications

The Federal Reserve vault specification based on the requirements of the revised Bank Protection Act requires that a vault door be made of steel or other drill- and torch-resistant material at least 3-1/2 inches thick, and should be equipped with a dial combination lock, a time lock, and a substantial, lockable day gate.

Class 5 and 6 vault doors conform to Federal Specification "Door Vault, Security," AA-D-600B.

Class 5 vault doors afford the following security protection:

- 20 man-hours against surreptitious entry
- 30 man-minutes against covert entry
- 10 man-minutes against forced entry

Testing performed in accordance with specification AA-D-600B is limited to no more than two men working simultaneously during each entry attempt. The tools and devices allowed for testing against the class 5 vault door are based on the following entry methods:

Surreptitious Entry. Unlimited tools and devices, except that the total weight of the tools used for a single test shall not exceed 150 lbs.

Covert Entry. Power tools–electrical or battery powered–should be commercially available. Drills should not exceed 5000 rpm. Pressure rigs with a lever arm not exceeding 30 inches may be used. Tools and devices shall be capable of being carried in two bags or cases, each of which shall not exceed 1-1/2 ft^3 in volume. Total tool weight for a single test shall not exceed 150 lbs, excluding the cases. Heat-producing tools shall be limited to single tank propane, butane, or equivalent devices which fall within the weight and volume limits specified above. Acetylene, MAPP (Methyl Acetylene Propadiene Petroleum mixture), electric arc, burn bar, or any oxidizer-assisted products or explosives will not be used.

Forced Entry. Tools and devices will be limited to non-powered tools only.

Class 6 vault doors are intended to meet the following criteria:

- 20 man-hours against surreptitious entry
- 30 man-minutes against covert entry
- no forced entry requirement

Requirements for the class 8 vault door are contained in federal specification AA-D-2757, "Door, Vault, Security." The door may be used as part of a fixed vault structure, or in conjunction with federal specification AA-V-2737, "Modular Vault System," to form a removable vault system.

A class 8 door should provide the following protection:

- 20 man-hours against surreptitious entry
- 30 man-minutes against covert entry
- 15 man-minutes against forced entry

The forced entry test allows a knowledgeable, two-person adversary team to use common hand tools, picking tools, and a wide variety of portable electrical and mechanical power tools to attack the door. Oxy-fuel gas cutting torches are allowed; however, the total gas volume consumed is limited to 2000 ft^3 for any one test. Burn bars and explosives are specifically excluded from the attack threat.

In addition, the weight of tools and devices used in a single test is restricted to 150 lbs. The tools must fit within two cases or bags, each case or bag not exceeding 1.5 ft^3 in volume. There are no limits on the number of methods of surreptitious, covert, or forced entry attempted.

Other door features include the following:

- a permanently installed escape device which requires two unidirectional actions, such as push and turn, to activate the release of the vault door bolts;

- a detent on the locking mechanism to hold the bolts in the open position when the bolts are retracted and the door is swung open;

- the ability to secure the combination lock with the bolts retracted and the door open, and automatically throw the bolts when the door is closed, thereby securing the door.

4.4 Vault-Type Rooms

Vault-type rooms are rooms which are secured by a combination lock on the door, and are protected by intrusion detection devices which will trigger an alarm if the room is penetrated through any wall, the door, the ceiling, utility openings, or the floor. Alarms are also triggered by any motion within the room.

Vault-type rooms may be used for protection of classified documents or material, or for protection of Special Nuclear Material (SNM). However, DOE is moving toward a policy which would prohibit their use for storage of Category I quantities of SNM, attractiveness levels A, B, and C. They would be permissible for attractiveness levels D and E.

Vault-type rooms are often constructed to act as exclusion areas within other protected or limited-access areas. An example of this is an unmanned, classified Automatic Data Processing facility within a limited area.

Although they contain the required intrusion detection systems and the combination lock on the door, these rooms provide little delay to physical attack. Rather, they rely on an efficient response force to provide protection in case of a penetration attempt.

Since they provide limited penetration resistance, the application of vault-type rooms should be evaluated with respect to overall security system performance, including early detection and rapid response.

5 Safes and Security Containers

Significant changes have occurred in the safe industry over the past few years. New barrier materials and locks have increased security compared to previous designs.

5.1 Uses

It is important to use a safe, vault, or security container of the proper level for protection to meet or exceed the value of its contents. The safe or vault is the last line of defense against an attack. Time is a burglar's worst enemy, and the better the safe or vault, the better the chances that the intruder's time will run out.

General Services Administration-approved security containers and safes are available in many styles and sizes to handle a large range of applications.

5.2 Hardware Description

Barrier materials are materials incorporated in the safe's construction as a means to delay an attacker's progress in neutralizing the locking mechanism. They can be positioned to protect only the combination lock, or, as in the case of the ultra high security safes, they can be placed throughout the entire door and body. The latter is referred to as six-sided protection.

Carbide-Included Barriers

There are specific barrier materials for specific duties. Since one of the most common attacks on safes is the drill, the most common barrier material is drill resistant steel, referred to by many in the industry as "hard plate." By placing a hardened piece of steel between the outer portion of the safe door and the locking mechanism, effective protection can be attained against a standard drilling attack.

This type of protection has been used for many years but is easily defeated by carbide tipped drill bits and high speed drill motors. New high-tech, carbide-included barrier plates differ in many respects from old industry standard hard plates (Figure 5-1).

Carbide-included barriers are one of the most effective barriers against drill attack. Carbide is the hardest metal known, but used alone, it is very brittle. Carbide-included barriers have thousands of small, irregularly shaped pieces of carbide in various binding agents, bonded to and enclosed in a steel cladding or envelope. The highly irregular surface of these barriers effectively chews up high speed or cobalt drill bits, and disintegrates carbide-tipped drill bits (Figures 5-2, 5-3).

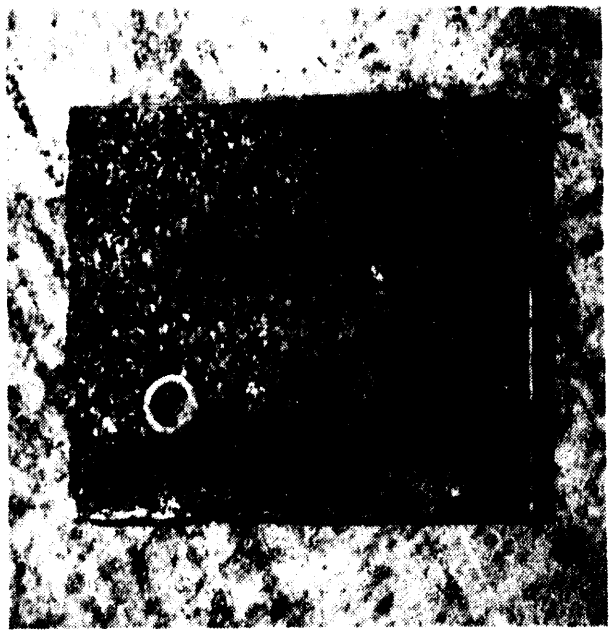

Figure 5-1. Carbide-included barrier plate

Figure 5-2. Plate under attack

Figure 5-3. Defeated drill bit

Some brands of carbide-included barrier plates also offer protection against x-rays. These plates, which are a minimum of 3/8 inch thick, are effective in slowing x-rays due to the denseness of the carbide. While x-rays with sufficient magnitude and exposure time can penetrate almost any substance, in terms of portability, space, power, and working time, x-ray penetration is unlikely.

Other types of carbide-included barrier plates include steel plates with rows of welds laid down by an arc welder using a welding rod containing carbide.

Tungsten carbide and steel powder bonded together form another type of barrier plate. Still another carbide-included barrier uses a process of flame spraying chrome carbide 3/16 inch thick over 3/16 inch thick steel plates. A box made of these plates encapsulates the combination lock on GSA-approved security containers.

Concrete Barriers

Burglary-rated safes and vault doors constructed of heavy steel plates are expensive to produce and offer little protection against the oxy-acetylene cutting torch. Instead, concrete barriers are becoming popular in the safe and vault industry.

Many manufacturers are switching to concrete because of its many advantages. New high-tech cement mixtures have been developed over the past few years that are superior to previous recipes. One manufacturer in Florida has tested some of its samples at over 18,000 psi. These mixtures, which are held proprietary by their manufacturers, are meticulously mixed and cured using precision measuring techniques. This cement offers good protection against the most common form of thermic cutter, the oxy-acetylene cutting torch, as well as drill attacks.

Manufacturers can add various other ingredients to their super cement recipe such as granite chips, chilled iron shot, and diamond-hard proprietary "nuggets" to thwart serious drilling attacks.

Safe design and construction has drastically changed since the development of this high psi concrete. Doors and bodies can now be constructed of more economical, thinner steels to form inner and outer walls. The hollow portion between these walls can then be filled with cement, which is also more economical than steel. Walls can be spaced at varying distances from each other so that more or less concrete can be added for varying levels of protection.

Another advantage of this technology is the additional benefit of fire protection offered by the ultra denseness of the cement. Some manufacturers are now offering one and two hour UL fire ratings on their UL-rated tool-resisting burglary safes. This double rating, coupled with the torch protection of these safes, make them an excellent value.

New high-tech vault doors are built in a similar manner with varying thicknesses for different levels of protection. Most manufacturers cast their doors in steel molds which have all the boltwork, lock, and hinge mounting plates and bosses placed so that when the door comes out of the mold, the slab is simply wrapped with polished stainless steel or painted sheet metal. Locking mechanism and fittings are then installed, and the door is fitted into the steel door jamb. This method of manufacturing is much less costly than the conventional process of machining the door slab out of solid steel. Concrete modular vault panels are cast using the same method as the door except that finish metals are not installed.

Glass Barriers

Glass barriers are one of the most effective deterrents to any penetration attack. Although they are not drill resistant, torch resistant, or explosives resistant, they can offer protection from all of these attacks. Tempered glass plates (Figure 5-4) are mounted between the door slab and lock mechanism with cables connected to them (Figure 5-5). At the other end of these cables are devices called "relockers."

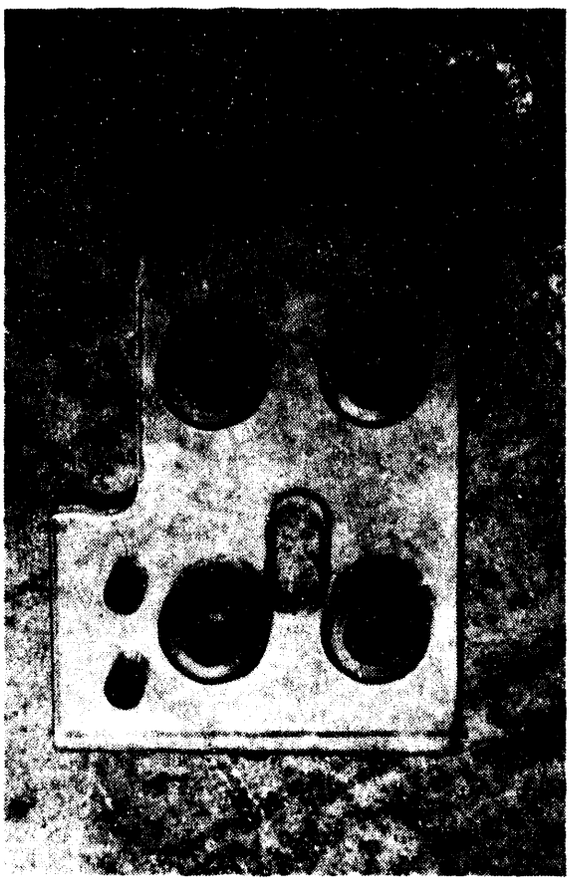

Figure 5-4. Glass plate for keylock

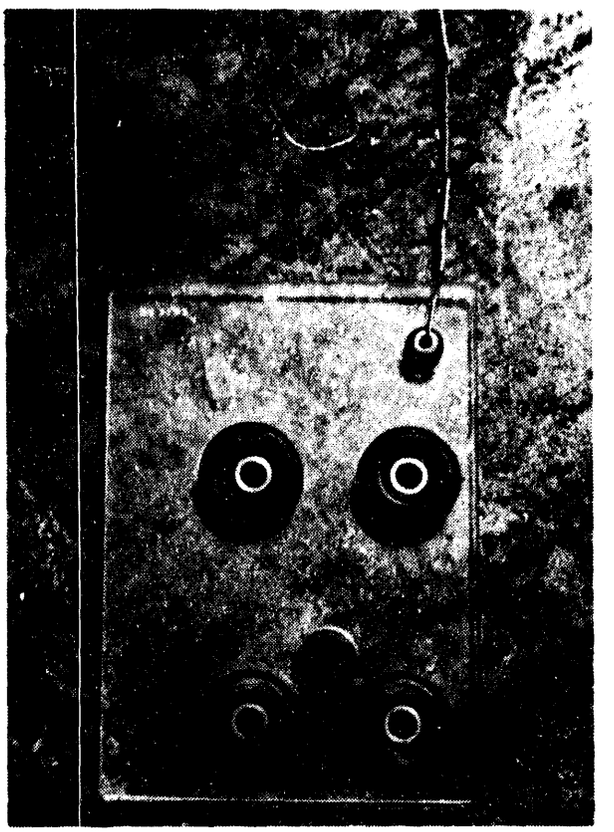

Figure 5-5. Glass plate with cable

The relocker is a secondary spring-loaded or "deadlocking" device. Its job, when released, is to block the movement of the locking bolts. Even if the combination lock were to be blown off the back of the door, the locking bolts would still be held in check by the relocking device. The cables running from grommeted holes drilled through the glass keep these relockers in a cocked position. Any attack would cause the relockers to instantaneously fire into their locked position.

As the use of glass has become known to some of the more sophisticated safe crackers in Europe, they have started attacking the safes from the top, sides, and back, utilizing precision drilling and long boroscopes (inspection lights) to aid in defeating the relockers. Manufacturers have responded by installing multiple glass plates interconnected via the cables so that an attack from any direction would activate the relockers.

5.3 Application Considerations

Class 6 containers are generally good for storage of classified and secret information, documents, small devices, etc. However, different government agencies have varying guidelines concerning selection of a particular class of security containers. Factors such as location, alarms, and security patrols may affect selection requirements. Available class 6 containers are as follows:

- Size I 2-drawer, legal size
- Size II 4-drawer, letter size
- Size III 4-drawer, legal size
- Size IV 5-drawer, letter size
- Size V 5-drawer, legal size
- Size VI 2-drawer, special size (mobile)
- Size VII 1-drawer, special size (mobile)
- Size VIII 1-drawer, special size for field use
- Size IX 2-drawer, letter size

Probably the most common is the class 6 standard legal size 4- or 5-drawer cabinet with single lock (Figure 5-6).

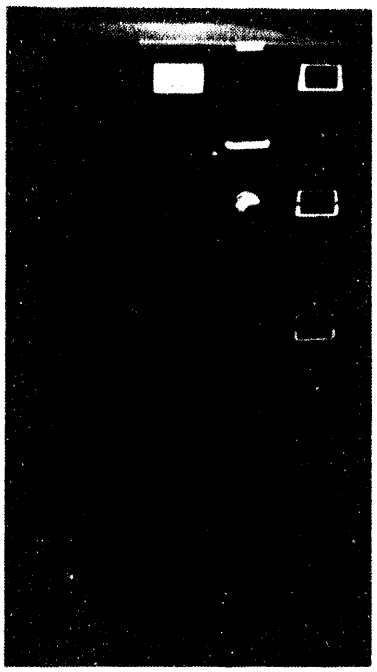

Figure 5-6. Standard 4-drawer single lock cabinet

The class 6 scope of products has the largest choice of options from which to choose. Single lock designs have one drawer (control drawer) equipped with a single combination lock. When this drawer is closed and locked, it secures all other drawers. These cabinets are available with 5, 4, or 2 drawers. Special size 1- and 2-drawer cabinets, designed for mobile applications, are also available. These cabinets should be anchored to the vehicle or aircraft via the pre-drilled holes in the bottom. A single drawer field safe is available that has a steel shield protecting the lock and bolt control handle as well as lifting handles that hinge up for easy carrying.

Another locking design is a dual lock, and has two combination locks (Figure 5-7). This design provides for dual custody of a container which requires the presence of two authorized individuals to gain access. As with the single lock design, one drawer is equipped with the locks and controls all other drawers.

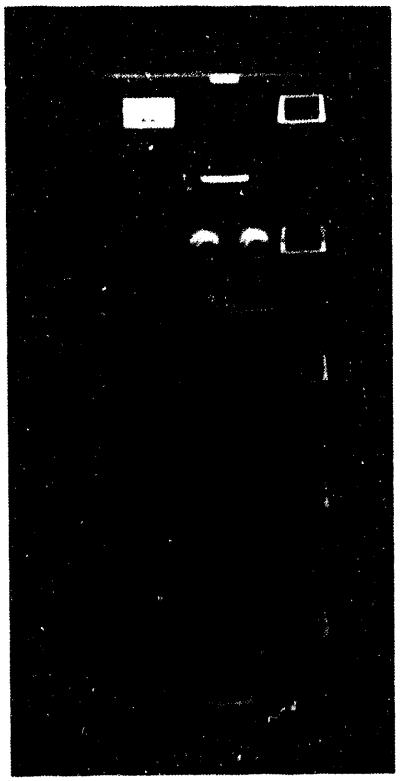

Figure 5-7. A dual-lock cabinet

Dual-multiple lock containers (Figure 5-8) have independently controlled locking drawers with each drawer having one or two combination locks. These containers can be tailored to the user's requirements. For example, the cabinet can have two drawers equipped with dual locks for dual custody and the other three drawers equipped with single locks.

Multiple lock containers (Figure 5-9) have independently controlled locking drawers with each drawer having its own individual combination lock. Multiple lock containers can be used for applications where multiple users, not requiring a lot of storage space, can have their own drawer in a single security container.

Class 5 security containers and safes (Figure 5-10) offer protection against forced entry and may be required by some government agencies and the military in applications of "Top Secret" protection. As in the case of class 6 containers, circumstances may dictate class 5 protection. Class 5 security containers in 2- and 4-drawer legal size are the only file cabinet type containers available at the time of this printing.

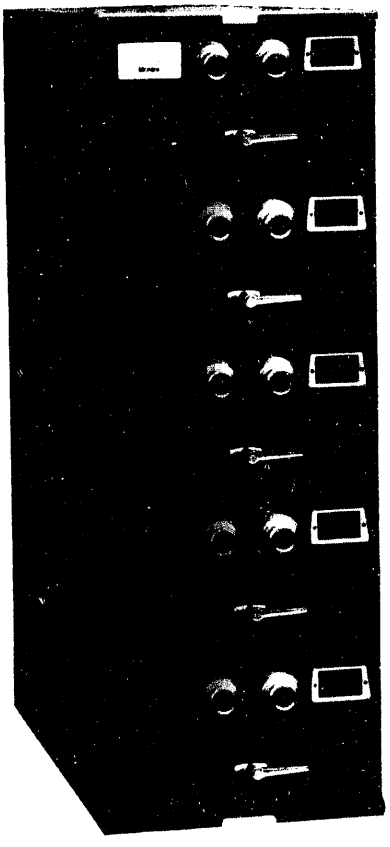

Figure 5-8. A dual-multiple lock cabinet

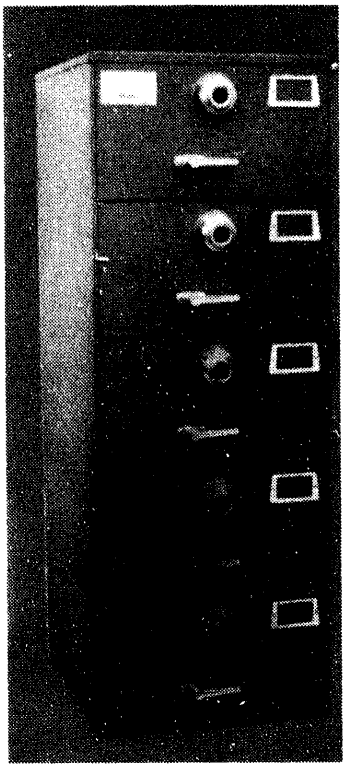

Figure 5-9. A multiple lock cabinet.

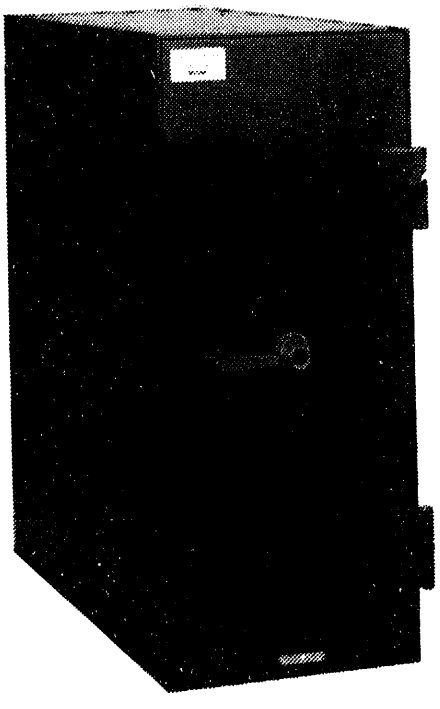

Figure 5-10. Class 5 safe

Class 5 general purpose safes can be used for a wide variety of applications including storage of narcotics, funds, and bulky sensitive items. These safes can be fitted with a wide range of interior equipment to conform to many applications. Class 5 map and plan files (Figure 5-11) can also be custom designed with many interior configurations. Drawers can be added to store such items as computer tapes, microfilm, and filing cards.

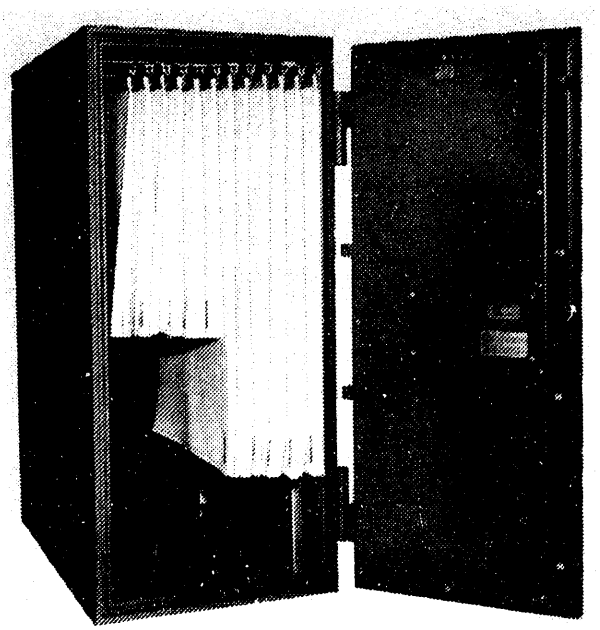

Figure 5-11. Class 5 map and plan

Another common application for these safes is the secure storage of weapons and ammunition. Interior arrangements are available for military rifles and automatic weapons (Figure 5-12). A properly configured weapons safe can store a total of 36 M-16 rifles.

5.4 Standards and Specifications

5.4.1 Specifications of GSA Security Containers

GSA-approved security containers have undergone some notable design changes since the enactment of the new Federal Specification AA-F-358G. This specification superseded the old specification AA-F-358F. (The old specification will be referred to as "358F", and the new specification will be referred to as "358G" from here on.)

In the almost 18 years that passed before 358F was revised, a number of factors contributed to its revision. Availability of

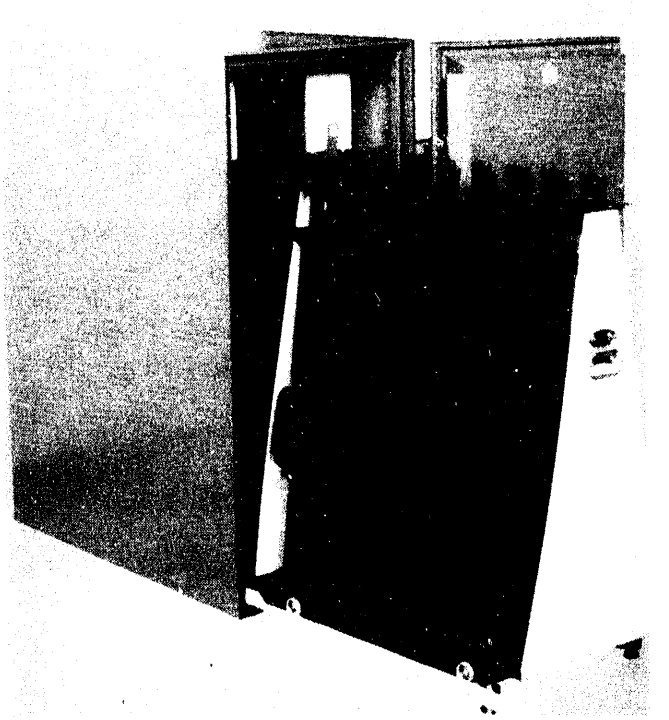

Figure 5-12. Class 5 weapons safe

safe and lock opening equipment, such as drilling rigs, required a reassessment of materials, designs, and construction. Drilling equipment, which had been previously ignored by government testers, has now been included in 358G. As a result, the new barrier plates in the currently manufactured containers are almost impossible to penetrate.

The use of this super barrier material forced another change in design and construction. Since drilling methods of entry are unsuccessful, in the case of a forgotten combination or lock malfunction, the entry method involves totally destroying the drawer head. Therefore, 358G calls for the drawer heads to be removable and replaceable (Figure 5-13).

The locking drawers manufactured under 358 F for class 5 and 6 containers could be drilled and repaired to DoD specifications as outlined in the Industrial Security Manual for Safeguarding Classified Information, DoD 5220.22-M. These 358F drawers had the drawer pan welded to the drawer head, and were expensive to replace in the event that untrained personnel had to destroy a drawer to gain entry. 358G containers can be opened by less experienced personnel (with proper instruction), and can be more economically repaired by replacing only the drawer head.

A new specification has been added to 358G, termed "Covert Entry." Covert entry is defined as "a method of entry which would leave evidence, but would not be detectable by a user during normal use, but would be detectable during inspection by a qualified person." Tools and equipment that are used by professional safe technicians (or illegal safecrackers) have been incorporated into the covert entry testing program.

358G has also increased its "total tools allowed" in testing to 150 lbs which can be carried in two tool cases with a volume of 1-1/2 ft^3 each. 358F allowed 25 lbs of tools that could be carried in one tool case 1-1/2 ft^3/9 in. thick. A typical covert entry would include pulling the dial and drilling a hole to open the lock, then replacing the dial and lock parts with ones identical to the original. The user of the container would not be able to determine that the safe had been compromised. However, a thorough inspection by a professional safe technician would readily determine what had been done.

5.4.2 UL Standards and Specifications

Underwriters Laboratories labels safes according to UL 687, Burglary Resistant Safes.

In the commercial and banking field, safes and vaults are rated by the time it takes to successfully compromise the safe or vault in a battery of tests. Underwriters Laboratories (UL) tests safes and vaults against a stopwatch to ascertain if the given sample is worthy of a particular level of compliance. The UL labeling system lists the qualifying net working time limits on the labels. For instance, a UL TL-15 label signifies that a safe has qualified for resistance against tool (TL) attacks for a net working time of 15 minutes. Net working time is the actual time spent attacking the safe. Time spent setting up drilling equipment, delays encountered because of tool failure, etc., are not counted in the test time. UL offers a total of ten labels for burglary rated safes:

(1) TL- 15
(2) Deposit Safe
(3) TL-30
(4) TL-15x6
(5) TL-30x6
(6) TRTL-30
(7) TRTL-15x6
(8) TRTL-30x6
(9) TRTL-60
(10) TXTL-60

The most common of these labels are the TL-15 and the TL-30. Safes bearing these labels offer protection in the door and front face only. Tools used in the attacks consist of common

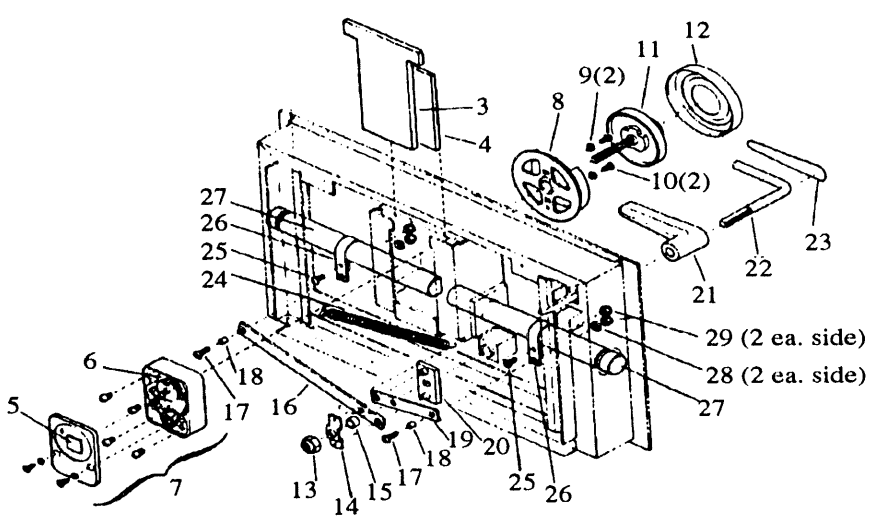

Figure 5-13. New style removable drawer head

hand tools, portable electric tools, carbide drills, and pressure applying drill rigs. The TL-30 must also provide protection against abrasive cutting wheels and power saws.

The Deposit Safe is a type of safe which has a built-in deposit mechanism to receive deposit bags and envelopes. Its test is the same as the TL-15 but also includes testing against fishing and deposit trapping attempts through the deposit mechanism.

All the previously mentioned safes are tested on the door and front face only. TL-15x6 and TL-30x6 afford protection on all six sides (x6) and are the newest labels added by UL. These safes are tested using the aforementioned tools as well as abrasive cutting wheels and power saws. These new labels are a direct result of the new composite and super concrete construction.

The TRTL-30 requires protection from all previously mentioned tools, plus the oxy-gas fuel cutting torch (TR). The TRTL-30 provides a requirement for the body to be encased in a minimum of 3 inches of reinforced concrete. The total weight of safe and encasement is not to be less than 750 pounds and should be equipped with a UL group 1 or 1R manipulation proof combination lock. This safe is tested on door and front face only. The remaining four labels are tested on all six sides.

TRTL-15x6 and TRTL-30x6 safes are attacked by all the previously mentioned tools and cutting torches on all six sides. The last two UL labels are the highest safe ratings offered, but no American manufacturer builds a safe of this magnitude of protection.

The TRTL-60 is the same as the TRTL 30x6 except that it offers an additional 30 minutes of protection on all six sides. Finally, the TXTL-60 offers protection against torch (T), nitroglycerine and other high explosives (X), and all the tools listed for the other labels (TL) for 60 minutes. In addition, it must weigh a minimum of 1000 lbs and be equipped with a UL-approved group 1 or 1R combination lock. At the time of this writing, there are only two manufacturers building these UL-rated safes: one in England and one in Israel. There are even safes built to standards exceeding those of UL.

5.5 Management of Security Containers and Safes

Although management systems will differ from one government agency to another, standard basic practices should be followed. GSA-approved security containers should be used for safeguarding all "Classified Information" (top secret, secret, and confidential). Security officers should maintain a current list of all classified storage containers by serial number and their locations (the building and room number where each container is located). Containers will bear no external markings indicating the level of classified material authorized to be stored therein.

Good security practices are that security containers and safes should be located in non-congested areas and should be free of any clutter or items stored on top of them. No calendars or pictures should be hung on any security container.

6 Management of Lock Systems

The purpose of this section is to describe some of the important aspects of managing locks. Policy and procedures play a major role in lock effectiveness. An organization which does not have a systematic method of lock selection, maintenance, key and combination control, and access authority will not have a secure locking system. Effective policy and procedures should also cover other issues, including security objectives, trade-offs between security and convenience, and responsibilities of management and staff.

The ideas presented below apply primarily to companies or organizations in which security is both crucial and complex. The ideas are not by any means exhaustive. As is appropriate for this document, locks are covered in more detail than other aspects of security.

6.1 Management Issues Common to All Types of Lock Systems

6.1.1 Management Policy

As discussed in Section 2, locks are an important part of a physical protection system. A management policy is needed to ensure a systematic approach to all aspects of security, including locks. Such an approach can increase effectiveness and reduce cost, particularly in complex systems.

Only the high level management of a company can determine the priority of security compared to other important matters. Consequently, management needs to make policy decisions on security. Subordinates can present options and implement the policy, but management needs to make the difficult decisions on how much security the company needs and can afford.

In organizations where security is important, the policy needs to be effectively communicated. Management and staff need to understand their responsibilities. If employees are to be held accountable for certain aspects of security, such as lock keys and combinations, and reporting of irregularities, this accountability needs to be made clear.

Objectives

To keep things in perspective, the management policy needs to state the credible threats to a physical protection system. Possible threats may include terrorists, competing companies, insiders, and burglars, and attacks may be forcible or surreptitious.

The policy also needs to state what assets and information are most important to protect. Different levels of protection are appropriate, depending on the consequences of losing particular assets and information. The most valuable items may need sufficient protection to stop an attack while it is occurring. For less valuable items, it may be sufficient to have knowledge of an attack after it has occurred.

Security and convenience need to be traded off in a conscious manner. For example, master-keyed locks provide convenience, but reduce security. Combination locks take longer to operate than key locks, but they can increase security. It is not appropriate for the policy to specify which locks to use. However, the policy needs to contain enough guidance that such decisions can be made by knowledgeable lock experts.

Access Authority

In any physical protection system, it is fundamental to allow access only to those who need it. One person, or at most, a small number of people, should have the authority to determine who needs to have access to each area. The need for access should be reviewed periodically.

Changing the Lock or Combination

The policy should state under what conditions locks need to be rekeyed, replaced, or have the combination changed. This should clearly be done if there is evidence or suspicion that the security barrier may have been breached. However, there are less threatening circumstances in which it may be useful to limit access. Such circumstances include an employee who no longer needs access; one who has retired or left the company; a disgruntled employee; or one under suspicion.

Keys and combinations should be changed periodically if important assets or information are being protected. This should be done even if there is no specific event to trigger the change.

6.1.2 Implementation—Turning Policy Into Action

Designated Control Officer or Security Organization

In companies where security is important, it is crucial that someone have the primary responsibility for making sure the management policy is implemented. Whether it is a part-time job for one person or a full-time job for a whole organization depends on the size of the task, and how much can be delegated to line organizations. If one person has the responsibility, it will probably be necessary to train an alternate. For the remainder of this section, the term Designated Control Officer will be used with the understanding that more than one person may be needed.

The Designated Control Officer is responsible for planning, operating, and maintaining an access control system to meet management policy. This person should be responsible for making decisions such as the types of access control, including locks, alarms, and monitoring devices, to be used in each area. This person needs to have technical expertise, but may need help from other experts. The Designated Control Officer should not be a dictator; instead, he/she should regard it as his/her duty to provide viable options to meet the needs of the company.

The Designated Control Officer should have the ultimate responsibility and authority to ensure that procedures are followed and reflect policy.

Procedures

If the security system is complex, procedures need to be established which implement management policy.

The primary danger of procedures is that they can become lengthy and bureaucratic. When this happens, they lose their value. It is crucial that procedures do not camouflage the critical issues in their desire to be complete.

The most valuable procedures are written by the people who are responsible for following them. Guidance should be provided on what is important. However, people responsible for implementation are best able to decide what to do, when to do it, and what records are appropriate to keep.

Suggested lock areas to be covered by procedures include Key Lock Control, Combination Lock Control, Lock Monitoring, Compensatory Action (what to do in case of lock failure or suspected attack), and Auditing. Some topics to include are covered in Sections 6.2-6.6. Depending on the complexity of the security system, other areas may be appropriately covered by procedures.

6.1.3 Maintenance and Inventory

Vulnerabilities can be introduced due to wear and tear, corrosion, and lack of preventive maintenance. These vulnerabilities can cause several problems. First, a failure can be made credible. If a poorly-maintained lock is broken, it could be attributed to the condition of the lock, rather than to adversary attack. Furthermore, an adversary could forcibly open the lock, then substitute a non-working replacement lock. Second, an adversary may be able to open the lock if he dials a combination or uses a key which is close to, but not exactly, correct. Finally, a poorly maintained lock can be difficult to open by an authorized user. When a lock is difficult to open, it is also difficult to verify that the lock is locked, introducing another vulnerability.

Maintenance operations should be done in-house. Using outside contractors to maintain the security system can significantly increase vulnerability.

Regular maintenance on key locks will help to avoid mechanical failures. If management policy requires cylinders to be periodically rekeyed, some maintenance will be done in conjunction with rekeying. Maintenance for key locks which are one part of a high security system may only be necessary if a lock fails. When a lock is part of a security system which includes guards, alarms, and fences, this may be acceptable.

Combination locks should be regularly inspected for signs of attempted defeat, including insertion of devices which would assist in decoding the combination. This may conveniently be done whenever the combination is changed.

Maintenance records should include lock failures, especially "fail safe" failures in which the failure compromised security. In this type of failure, a post mortem should be performed to provide information about which component of the lock failed. Lock-out failures should also be noted, to determine if higher than expected rates of failure are occurring.

The inventory required will depend on several factors: the number of locks to be maintained, the availability of replacement parts for the locks selected, and the skill level of the individual or individuals performing the maintenance. If the maintenance personnel are highly skilled, and there is a ready availability of parts for the locks used, the inventory required will be small. On the other hand, if the maintenance personnel merely replace entire locksets, or if the locks selected are non-standard in some respect--e.g., a proprietary keyway design--the inventory needs to be correspondingly larger.

The inventory of replacement parts may be broken down into two classifications: sensitive parts, such as keyed cylinders and cut keys, and non-sensitive parts, such as bolts, latches, and strikes. It is acceptable to lock non-sensitive items in cabinets providing lower security than that necessary for sensitive items. Keyed cylinders and cut keys should be protected at a security level commensurate with the items they will eventually protect. Master keys should be protected at the highest security level of any item they may protect. Master keys issued to personnel, such as security forces, should be inventoried often, perhaps daily.

The Designated Control Officer should be the only individual authorized to purchase, or permit the purchase of, replacement parts.

6.2 Issues Specific to Key Lock Systems

This section discusses some of the management issues which are important to key lock systems. Depending on the application, some or all of these issues should be addressed in any procedure written for key lock control.

- Key and lock inventory should be done periodically under normal circumstances, and if any breach of security occurs or is suspected.

- Each key should be clearly marked "DO NOT DUPLICATE."

- Keys should have an identifying number stamped on them for inventory purposes. The number should not indicate which locks can be opened with the key.

- Keys should be stored in a protected facility.

  —Protection should be at the same or higher level as the highest level of information or material to be protected.

  —Only the Designated Control Officer should have access to key storage.

  —Storage should be systematic to enable rapid inventory of keys.

- Up-to-date records should be maintained which list all keys, locks, identifying numbers, and personnel having access to keys, including dates of access. It may be helpful to include cross references which allow determination of all of these records starting from any one. For a large system, this is particularly important.

6.3 Issues Specific to Combination Lock Systems

This section discusses some of the management issues which are important to combination lock systems. Depending on the application, some or all of these issues should be addressed in any procedure written for combination lock control.

- The combination should be entered in a way that prevents bystanders from observing the combination.

- The combination should not be written in an unsecured place, such as a Rolodex file or on a slip of paper in a desk drawer.

- Avoid use of obvious combinations, such as birthdays, phone numbers, organization numbers, social security numbers, etc.

- Keep track of previous combinations used for a lock, and do not use them again. Also make sure there is no pattern.

- Up-to-date records should be maintained which include lock identifiers, lock location, people who know the combination, and the dates of changes. A cross reference of people who have the combination of various locks may be useful. If combinations are recorded, records should be protected to at least the highest level of protection that the combination lock provides.

- A fundamental principle of security is to allow access only to those who need it. For combination locks, people who need the combination should memorize it, and access to the combination should be denied to all others.

  Recording the combination potentially provides access to people who do not have the need. The main reason for recording a combination is so it can be retrieved, especially in an emergency. Storing combination records in a separate secure container decreases the vulnerability if access to the separate secure container is limited to those who need access to the original lock.

- It is more secure to select the combination using random numbers to avoid patterns, obvious combinations, and previous use.

- All combination locks should be examined periodically for insertion of devices which would aid in decoding.

6.4 Lock Monitoring

This procedure should cover the details of checking that locks are secured, typically at the end of the work day. It is important that personnel be trained to know exactly how the lock should be monitored. For instance, combination locks without scramblers need to be turned at least one more rotation than the number of wheels, in order to scramble the combination.

Lock monitoring is typically covered as part of a general security procedure.

6.5 Compensatory Action—What to Do in Case of Lock Failure or Suspected Attack

- This procedure should detail immediate actions to be taken if a suspected breach of security occurs. The information should include, at a minimum, whom to contact and how.
- Short-term solutions for plugging the suspected security breach should be included. It may be important for the discovering individual to keep guard until reinforcements arrive.
- Determining the probable cause of lock failure will help to avoid taking unnecessary and costly action. The failure may be due to normal causes or obvious adversary attack. In cases of suspected surreptitious attack, it will probably be necessary to contact knowledgeable experts.
- After the cause has been determined, it is important to determine if the failure could be avoided in the future. It may be appropriate to change policy or procedures to avoid recurrence.

6.6 Auditing

The purpose of an audit procedure is to make sure that management policy is being implemented. However, there are effective and ineffective ways to accomplish this.

No one likes to be audited because there is intrinsic suspicion on both sides. The one being audited quite rightly suspects that the auditor is compelled to put down something on the report to justify the auditor's existence. The auditor, on the other hand, may run into people who are not concerned with security, but just want to do enough to pass the audit.

To have an effective auditing procedure, the auditor should be regarded as an expert helper, and those who are being audited should believe that what they are being asked to do is important for their organization and their career. One way the auditor can be regarded as an expert helper is by being willing and able to communicate ahead of time what he/she is looking for, by understanding and communicating the logic behind security procedures, and by doing "pre-audit audits" with no penalty. The issue of importance to organization and career should be established by management.

Another way to make an auditor effective is to give him/her authority to change, or at least influence, policy and procedures. When an auditor performs an audit, he/she will discover practices in an organization that could benefit the whole company. If these practices become widespread, the company improves, the organization which originated the practices is justifiably proud, and the auditor is more likely to be regarded as an expert helper.

7 Safety Considerations of Locks

This section addresses safety considerations of locking systems.

7.1 Conflicting Needs

To protect human life in an emergency, the Uniform Building Code and the Life Safety Code, along with most local building codes, stipulate that a door which may be used for an emergency exit should not be locked or otherwise secured in a manner that prevents emergency egress when the area they serve is occupied.

When both safety and security are at issue, there is an intrinsic conflict: the measures which add safety will often degrade security.

Emergency egress should be carefully considered in determining the types of locks to be used in a security system. Locked doors present two specific hazards:

(1) They prevent egress of personnel from the emergency.

(2) They prevent immediate access to the area by personnel assigned to mitigate the emergency.

On the other hand, devices installed to provide emergency ingress and egress increase vulnerability. Typically, it will be easier to successfully attack a door which has such a device. In addition, the device allows an intruder to freely leave the building. The door may also be left open for unauthorized individuals.

Safety and security should therefore be balanced. The installation of a high cost, high security system may not be justifiable if the system will be degraded because of safety requirements.

7.2 Emergency Exit Devices

Safety requirements are typically met by installing emergency exit devices on doors which should usually remain locked. These devices allow doors to be readily opened from the inside during an emergency. The Life Safety Code requires the emergency exit device operation to be obvious, even in darkness. Some devices degrade security more than others. If an appropriate emergency exit device is chosen for a given application, safety needs will be served, and security will be degraded as little as possible.

There are many emergency exit devices in the commercial market. They fit different types of doors, with different ancillary hardware. There are also several different mounting styles, including rim, mortise, surface vertical rod, concealed vertical rod, and combination.

Different actuating devices include a panic bar, push pad, and paddle. Some use latches, some use deadbolts, and some are alarmed. Most are mechanical, but some are electrical. The Directory of Certified Exit Devices lists the devices which meet specific standards. A summary of this directory can be found in Section 7.2.4.

Even though many options are available, emergency exit devices all have a common function: to allow an able-bodied person on the inside to open the door in an emergency situation, even if the person is in a panicked state of mind.

Emergency exit devices should satisfy their own safety requirements. They should fail safe, and should not be dangerous to people using them. These requirements are detailed in Section 7.2.3, Standards and Specifications.

7.2.1 Hardware Description

The most common method of providing safe exit through a door which is normally locked is the use of a panic bar (Figure 7-1), also known as a crash bar or cross bar. When a force is applied to the panic bar in the direction the door opens, the bar releases a latch, allowing the door to open.

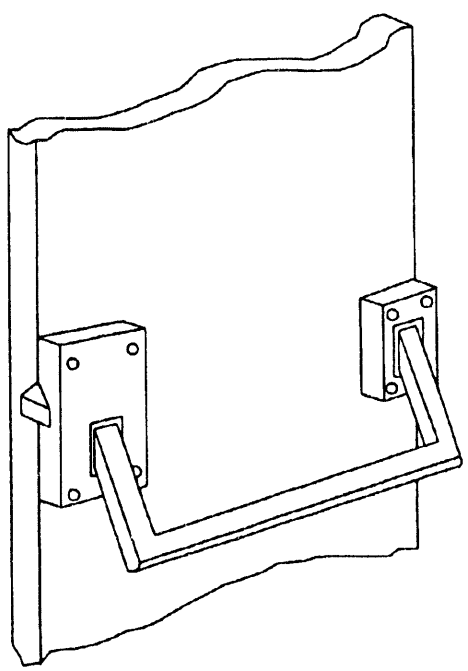

Figure 7-1. Rim-mounted panic bar

A push pad with an alarm is shown in Figure 7-2.

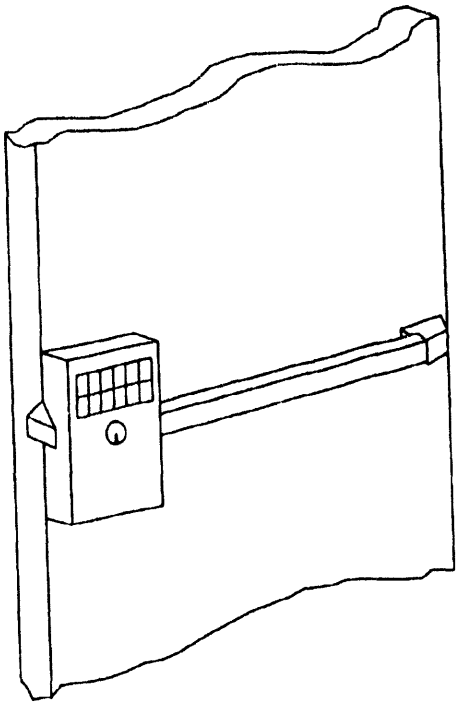

Figure 7-2. Push pad with alarm

A method of providing both emergency ingress and egress is the use of electrically operated bolts, strikes, or latches which are designed to be fail safe. A further option is to use an electromagnetic lock, which is intrinsically fail safe. These devices allow an operator to release the door in an emergency. They release automatically when they lose power, and can be designed to release when a sensor, such as a fire or radiation sensor, trips an alarm.

To meet the Life Safety Code, the electrically operated devices should also have some means by which a person on the inside can release the lock. One method is to install a mechanical panic bar. The mechanical panic bar also has an electrical equivalent: the motion of the bar actuates an electrical switch, which releases the door. Care should be taken to insure that if the panic bar is pushed at the same time as electrical release, the mechanism does not jam.

There is another type of electrical panic bar which has no moving parts. It operates using body capacitance to actuate the electronics. It is adjustable to be sensitive enough to operate properly through gloves or heavy clothing. However, to guarantee that this device is fail safe, it must also be equipped with a mechanical switch which can release the latch.

In buildings which are protected by an approved automatic fire detection system or automatic sprinkler system, the Life Safety Code may allow the installation of a time release mechanism to improve security. When the emergency exit device is actuated by a person wishing to exit, an irreversible process is initiated which will release the lock within 15-30 seconds. The time delay may allow security personnel to arrive before the individual activating the alarm can leave.

There are several conditions which must be satisfied by a time-delayed system. First, the door must unlock without delay when the fire detection or automatic sprinkler system is activated. Second, the door must unlock without delay whenever there is loss of power. Third, the Life Safety Code allows this type of system to be used only in low or ordinary hazard areas.

7.2.2 Application Considerations

7.2.2.1 Pros and Cons

Panic bars do not increase access to an emergency area. Other methods, such as readily available keys, should be added to allow authorized personnel access to mitigate the emergency.

An electrical release mechanism increases access to the emergency area as well as allowing personnel to exit.

Alarm systems are subject to false alarms. These are not simply a nuisance, but degrade security in two ways. First, security personnel may regard a real emergency as just another false alarm. Second, security personnel responding to a false alarm are not available to respond to a real emergency.

One vulnerability of emergency exit devices is that an adversary may use them to gain access. For example, the adversary could use a stiff wire to apply sufficient pressure to the device, causing it to operate. This may be accomplished if the tolerances in door fit are sufficiently large to admit the wire, or if the adversary has sufficient time to drill through the door.

Another vulnerability is that a person on the inside could leave the door unlocked for unauthorized personnel.

Electromagnetic locks and electric bolts, strikes, and latches may be vulnerable to attacks on wiring and power supplies. Some are vulnerable to magnetic attack. These vulnerabilities are described in the Glossary.

7.2.2.2 Design Features Which Increase Security

- Doors should fit their frames with very close tolerances. No space should exist which will allow a shim or wire to be inserted past the door and into proximity with the emergency exit device.

- It is important to select a locking device which allows no more access than is actually needed. For instance, suppose a particular door is used only as an exit. In this case, there is no reason to install a lock which can be opened from the exterior. If such a lock is installed, it degrades security.

- Status monitoring and alarms should be installed to give indication of the position of the latch or bolt, and the door. If only the position of the door is detected, the door may be left closed but unlocked.

  A simple method is to install a sensor which will not allow an electric bolt to extend unless the door is shut. For an electric strike, a sensor can detect if the latch is in the recess. While these sensors do the job for which they are designed, they would be quite easy for an adversary to defeat.

- For electrically-operated devices, status monitoring should include whether the lock is on backup power, as well as whether the door is secured.

- Design features which increase security of electrically operated locks are presented in Sections 3.3.4 and 3.5.3.

- Astragals are devices which mount to the edge of a door and extend over the outside of the door jamb. They are designed to cover the space between the edge of the door and the door jamb, to prevent anything from being inserted to actuate the emergency exit device. Astragals are also used on double doors to cover the space between the doors.

- Doors equipped with emergency exit hardware should not open into areas of higher security.

7.2.3 Standards and Specifications

See Appendix A for addresses and telephone numbers of the organizations from which these standards and specifications may be obtained.

ANSI/BHMA A156.3-1989 American National Standard for exit devices

This standard provides operational and security testing and grading for exit devices. All hardware described in this specification should, at minimum, meet all requirements of UL 305, Panic Hardware. Eleven types of exit devices and six types of ancillary hardware are named. Twelve possible functions of the different types of hardware are described. The simplest function is exit only. The other functions include how entrance from the exterior side is accomplished.

The requirements for Grade 2 hardware (the lower grade) are approximately the same as UL 305. The differences are that this standard adds a cylinder test, and is slightly more specific on the other tests. The cylinder test requires that the hardware meet all requirements of ANSI/BHMA A156.5-1984. The only additional test is a torque test to insure that excessive force is not required to open the latch with a key.

The requirements for Grade 1 hardware are significantly increased over UL 305. Grade 1 must pass the same cylinder test as Grade 2. Grade 1 must be cycled 250,000 times, instead of 100,000 for Grade 2 (and UL 305). In addition, Grade 1 requires a security test in which the device must function properly after an attempt is made to forcibly open the door from the outside. Grade 1 also requires an inside pull test and a push test, which make sure the device functions if unusually large forces are applied to the exit device from the inside.

Finish testing includes salt spray, humidity, pencil hardness, and perspiration. The standard does not describe these tests, but does provide references to the appropriate standards and specifications.

A list of definitions for panic device hardware is supplied.

This specification may be obtained from the Builders Hardware Manufacturers Association.

ASTM F 571-87 Standard Practice for Installation of Exit Devices in Security Areas

This standard provides information for the installation of exit devices used in security areas with the goal of achieving the greatest security possible without violating safety requirements. High level security is not always possible if exit devices are required, but some types of devices are more secure than others. This standard gives information on what exit devices to choose if both security and safety are important factors.

This standard also offers installation guidelines for doors and frames, associated hardware, exit devices on single and double doors, and exit locks. Pertinent information is provided concerning exit device functions, optional security features for exit devices, and fasteners used in installations.

The following information on exit device functions provides an example of the type of information contained in this standard. Functions of exit devices range from those having no operation on the exterior side of the door, to those which can be operated by a knob, lever, or thumbpiece on the exterior side. The most secure devices are those which cannot be operated from the exterior side. These are called "exit only devices." The second most secure are those operated only by key from the exterior side. Least secure are those which can be left unlocked, and can be operated by a knob, lever, or thumbpiece on the exterior side.

This specification may be obtained from the American Society for Testing and Materials.

UL 305 Panic Hardware

This specification covers exit devices actuated by a panic bar for outward-opening doors, designed to facilitate the egress of people from buildings in the event of emergency.

Exit devices are required to operate properly and be maintainable. Materials must be corrosion resistant, and must not melt at temperatures less than 1000 degrees Fahrenheit.

Safety requirements for exit devices specify that the ends of the panic bar must be designed to preclude catching on clothing; the mechanism must not depend on springs to open the latch; no locking or dogging devices may be installed which prevent the release of the latch; if a deadbolt is used, it must be operated by the panic bar; and the panic bar must not unduly restrict the exit opening when the bar is depressed. The panic bar must not be deformed by the tests, and must always allow a spacing of at least 1 inch between the bar and the door face, to prevent fingers from being smashed.

A 100,000 cycle endurance test is required at a rate of 30 cycles per minute.

The exit device must operate with a horizontal force of 15 lbs or less. If a horizontal force of 250 lbs is applied to a latched door in the direction of opening the door, the exit device must operate with a horizontal force of 50 lbs or less.

For double doors, a horizontal force of 250 lbs is to be applied against the midpoint of the outer stile of each door. The exit device must operate with a horizontal force of 50 lbs or less.

This specification may be obtained from Underwriters Laboratories, Inc.

Life Safety Code Handbook

This handbook is an annotated version of the National Fire Protection Association's publication 101, the Life Safety Code, 1988 edition.

Section 5 of the Life Safety Code establishes criteria for door hardware and emergency exit devices. Some of the criteria follow.

- A door shall be readily opened from the egress side whenever the building is occupied.
- A latch or other fastening device on a door shall be provided with a knob, handle, panic bar, or other simple type of releasing device having an obvious method of operation under all lighting conditions (including darkness). Doors shall be openable with no more than one releasing operation.
- No lock, padlock, hasp, bar, chain, or other device shall be installed on any door on which panic hardware is required if the device prevents egress.

Locks on doors in buildings with approved, supervised, automatic fire alarms or automatic sprinkler systems may be equipped with approved locking devices which shall

- unlock upon activation of approved fire alarm system or fire extinguisher system;
- unlock upon loss of power controlling the locking device; and
- initiate an irreversible process that will free the latch within 15 seconds whenever a force of 15 lbs is applied to the release device. The authority having jurisdiction may approve a delay not to exceed 30 seconds provided that reasonable life safety is assured.

This special type of locking device is allowed only in low and ordinary hazard areas.

Sections 14 and 15 of the Life Safety Code deal with provisions for detention and correctional facilities. While the functions of such facilities differ dramatically from the functions of other facilities, the safety requirements are in some ways similar. The requirements provide some insight into methods applied to problems associated with locked doors under emergency conditions.

- Detention and correctional facilities must be provided with 24-hour staffing. Staff must be within three floors or 300 feet of the access door of each resident housing area.
- The arrangement shall be such that the staff can start release of locks for emergency evacuation within two minutes of alarm.
- Provision shall be made so that residents can readily notify staff of an emergency.
- A plan for the protection of all persons in the event of fire must be written. All employees shall be instructed and drilled with respect to their duties under the plan.
- Doors from areas of refuge (areas where people can gather within the detention facility, but removed from the emergency) to the exterior may be locked with key locks in lieu

of remote locking devices. The keys to unlock such doors shall be maintained and available at the facility at all times, and the locks shall be operable from the outside.

- Any remote release used for egress shall be provided with a reliable means of operation, remote from the resident living areas, to release locks on all doors. An exception is that the requirement for remote locking and unlocking may be waived, provided not more than 10 locks must be unlocked to move all occupants. However, the unlocking must be done as promptly as required for remote unlocking devices. The opening of all necessary locks shall be accomplished with no more than two separate keys.

- All remote release operated doors must be provided with a redundant means of operation.

- Doors remotely unlocked under emergency conditions shall not automatically relock when closed unless specific action is taken at the remote location to enable doors to relock.

- All keys necessary for unlocking doors shall be individually identified by both touch and sight.

- Standby emergency power shall be provided for electrically operated locks. Power shall be arranged to automatically operate upon failure of normal power within 10 seconds and to maintain the necessary power for at least 1 1/2 hours.

The Life Safety Code and the Life Safety Code Handbook may be obtained from the National Fire Protection Association, Inc.

ANSI/BHMA A156.5-1984 American National Standard for auxiliary locks & associated products

Part I of this standard covers auxiliary bored and mortise locks, rim locks, and cylinders. Security tests, operational tests, finish tests, and dimensional criteria are included.

Part II of this standard establishes requirements for exit alarms, exit locks, electric strikes, and indexed key control systems, and includes operational and finish tests.

The following is a summary of the portion of Part II concerning exit alarms and exit locks. Other parts of this standard are reviewed in the appropriate section of this document.

- Exit alarms must pass a cycle test to meet this specification. The number of cycles is 10,000.

- Exit locks must pass a humidity test, cycle test, and operations test. A latch bolt must be cycled 100,000 times, and a deadbolt 5000 times. The operations test is similar to one of the tests in UL 305. The exit lock must operate with 15 lbs of force applied at the center of the actuating mechanism.

- Descriptions and illustrations of a few types of exit alarms and locks are given. The part numbering scheme describes how to specify what you want to purchase: material, type of product, product function, and grade.

This specification may be obtained from the Builders Hardware Manufacturers Association.

Uniform Building Code

The Uniform Building Code may be obtained from the International Conference of Building Officials.

7.2.4 Directory of Certified Exit Devices

This document is published yearly by the Builders Hardware Manufacturers Association. The directory is a listing by manufacturer and model number of devices meeting the requirements of ANSI/BHMA A156.3. Manufacturers may choose to have their hardware listed whether or not they are BHMA members.

This directory may be obtained from the Builders Hardware Manufacturers Association.

Appendix A

Addresses for Specifications

The American Society for Testing and Materials
1916 Race St.
Philadelphia, PA 19103
(215) 299-5400

Builders Hardware Manufacturers Association, Inc.
355 Lexington Ave.
New York, NY 10017
(212) 661-4261

Defense Printing Service (for both military and federal specifications)
700 Robbins Ave.
Building 4, Section D
Philadelphia, PA 19111-5094
(215)697-2000

International Conference of Building Officials
5360 Workman Mill Rd.
Whittier, CA 90601
(310) 699-0541 ext. 501

National Fire Protection Association, Inc.
P.O. Box 9146
Quincy, Massachusetts 02169
(800) 344-3555

Underwriters Laboratories, Inc.
333 Pfingsten Rd.
Northbrook, IL 60062
ATTN: Publications
(708) 272-8800

Appendix B

Standards and Specifications

Standard No.	Date of Issue Reviewed in this Document	Bolts, Strikes, and Latches	Combination Locks	Emergency Exit Devices	Key Locks	Electromagnetic Locks	Safes and Security Containers	Self-Contained Electronic Combination Locks	Vaults	Page No.
	Subject									
A-A-1927C	1989				X					17
A-A-1930A	1982				X					13, 17
A-A-1932A	1982				X					16
AA-D-600B	*								X	50
AA-V-2737	*								X	50
AA-D-2757	*								X	50
AA-F-358F	1971						X			58, 59
AA-F-358G	1989						X			58, 59
ANSI/BHMA A156.2	1989	X			X					14, 33
ANSI/BHMA A156.3	1989			X						67, 69
ANSI/BHMA A156.5	1984	X		X	X					14, 16, 33, 67, 69
ANSI/BHMA A156.11	1991				X					15
ANSI/BHMA A156.12	1986	X			X					15, 33
ANSI/BHMA A156.13	1987	X			X					15, 33
ANSI/UL 768	1984		X					X		2, 22, 24, 26, 27, 40
ANSI/UL 1034	1987	X				X				33, 36
ASTM F-1090	*								X	45, 49
ASTM F 471-76	1976		X					X		27, 39
ASTM F 571-87	1987			X						67
ASTM F 883-90	1990		X		X					16, 17, 26, 28
Bank Protection Act	1973								X	45, 49, 50
DoD 5220.22-M	*								X	45, 58
FF-L-2740	1989		X					X		26, 27, 28, 37, 40, 77
FF-P-110G	1987		X							17, 26, 28, 77
Life Safety Code	1988			X						2, 65, 66, 68, 69
Life Safety Code Handbook	1988			X						68, 69
MIL-HDBK-1013/8	1989		X							28
MIL-L-15596G	1988		X					X		26, 27, 40
MIL-L-2898D	1968				X					13, 15
MIL-P-43607G	1986				X					13, 16, 17
MIL-P-43951A	1989				X					13, 16
UL 305	1979			X						67, 68, 69
UL 437	1986				X					13,15
UL 608	*								X	45, 48, 49
UL 687	1991						X			59
Uniform Building Code	1988			X						65, 69

* Information taken from previously-written document. Specification not available. Please use latest issue.

GLOSSARY

This glossary includes words having specialized meanings, technical terms, and acronyms as they are used in this document. Because the primary subject matter of this document is locks, most of the terminology is specific to either combination locks or key locks.

ANSI – American National Standards Institute.

ASTM – American Society for Testing and Materials.

autodialer– a device which systematically attempts all possible combinations for a combination lock. An autodialer may be computer-driven.

auxiliary lock – a lock having a latch bolt or a deadbolt operated by a key or a thumb turn or both. An auxiliary lock is often used in addition to another lock.

BHMA – Builders Hardware Manufacturers Association.

bitting or key cut – the pattern of cuts, consisting of both location and depth, which must be machined on a key blank to correctly operate a particular lock.

bolt – the part of a lock which locks or blocks another mechanism from operating until it is retracted.

bolt manipulation – manual retraction of a bolt without operation of the lock mechanism. This is effective only for intermittently coupled bolts.

bolt track – the machined area within the lock case in which the bolt moves.

boltcutters – a cutting tool comprised of long lever-like handles providing closing force to short, hardened cutting jaws.

bored lock – a lock fitting round bored openings in the face and edge of a door.

breakaway line – a line scored or etched on the rear cover of a combination lock along which the cover will break if force is applied from the front. The purpose is to avoid defeat by punch attack.

cam stop – combination locks using a "butterfly" to lock the dial permit the butterfly to engage only when the dial is set to zero. Cam stops cast in the back cover of the lock prevent attempts to engage the butterfly if the dial is not set to zero.

case – see lock case.

chemical attack – the use of corrosive chemicals to degrade lock materials to the point of lock failure.

combination lock – a locking device which does not require a key. Instead it relies on entry of a single or ordered series of digits or letters to permit opening.

core removal/pulling – the forcible removal of a lock cylinder core to defeat the lock.

covert entry – a method of entry which would leave evidence which is not detectable by a user during normal use, but would be detectable during inspection by a qualified person.

cylinder – the portion of the pin-tumbler or wafer lock containing the locking mechanism.

cylinder plug or core – the tubular portion of the cylinder which may rotate within the cylinder body upon insertion of a correct key.

deadbolt – a lock component having an end which protrudes from or is withdrawn into the lock by action of the lock mechanism. A deadbolt is part of the barrier.

deadlatch – a spring-actuated latch bolt with a beveled end and incorporating a plunger which, when depressed, automatically locks the projected latch bolt against return by end pressure.

decoding – the use of special tools and techniques to determine the bitting for the correct key. For a combination lock, decoding is the use of special tools and techniques to determine the combination.

drilling attack – drilling a hole into a lock, safe, or vault for either direct defeat or to provide access to the interior for other defeat methods.

door stile – the vertical portions of a frame around the glass portion of a door.

electromagnetic lock – a lock comprised of an electromagnet and strike plate made of ferrous material. Application of electric current creates a magnetic field, which holds the electromagnet and strike together, securing the portal.

environmental attack – the application of extreme heat or cold to cause the materials used in fabrication to degrade to the point of failure.

exit alarm – an alarm triggered by actuation of an emergency exit device.

fence – the portion of a combination or lever lock which engages the gates and translates rotational motion to linear motion to withdraw the bolt.

forcible entry – a method of entry which leaves evidence which is detectable during normal use. Examples include sawing, grinding, chemical, and environmental attacks.

gate – the cutout in the wheel of a combination lock or the lever of a lever lock which the fence must engage to allow bolt retraction.

grinding attack– removal of material by grinding, allowing a lock, safe, or vault to be dismantled and defeated.

index mark – a mark engraved on a combination lock dial ring to which combination numbers are aligned during entry or change of a combination.

impact vibration attack – striking a spring-loaded padlock may cause vibration which momentarily releases the shackle, thus opening the padlock.

impressioning – creation of a correct key by copying an impression of the original key, or by impressioning the pins or levers within the interior of the lock cylinder using a key blank.

indexed key control system – a system of records used to control issue of access keys. Cross references are maintained to quickly determine who possesses keys, how many are outstanding, etc.

interconnected lock – a mechanically interconnected locking mechanism having a separate latch bolt or dead-locking latch bolt and deadbolt designed for installation in round bored openings in the edge and face of a door.

key blank – an uncut key which fits the keyway in a lock.

key-change hole – the keyway in a combination lock providing access for the combination change key.

key lock – a locking device operated by a key.

keyway – the cross section of a keyhole. The profile of the keyhole is designed using wards or obstacles to restrict the profile of keys capable of entering.

latch – a lock component which is part of the barrier. A latch has a beveled end which projects from the lock in its extended position, but may be forced back into the lock case by end pressure or drawn back by action of the lock mechanism.

lever lock – a lock which requires one or more levers to be moved into proper position by the key bitting before permitting bolt withdrawal.

lever stop (as applied to a combination lock) – a barrier machined or cast into a combination lock case to prevent the lever from moving when the fence and gates are not aligned. This prevents bolt manipulation.

lock case – the exterior housing of a lock.

magnetic attack – the use of a magnet or electromagnet to override the magnetic field of an electric bolt, latch, or strike or an electromagnetic lock. This allows operation of the device without authorization.

manipulation – opening a lock, safe, or vault in a way it was not intended to be opened without alteration of the physical structure or disarranging or substitution of any parts.

master-keying – to combine a group of locks or cylinders such that each is operated by its own change key as well as a master key for the entire group.

mechanical probing – the use of a small probe to aid in opening a lock.

mortise lock – a lock designed to fit into a rectangular cavity cut in the edge of the door.

NFPA – National Fire Protection Association.

pawl – a hooked arm assembly used to translate linear motion into rotational motion, but only in one direction.

physical manipulation – see manipulation, sense manipulation.

pin-tumbler lock – a lock requiring the key to correctly position a series of pins with respect to a shear line before allowing key rotation.

picking – the unlocking of a key-operated lock by the use of various tools which simulate the action of a key.

punch attack (as applied to a combination lock) – an attack in which hammer blows are applied to the spindle. This will cause the back of the lock to break away. A lock design to counter this attack has a breakaway line in the back of the case and a relocking device.

radiographic attack – the use of a radiation source to produce an image of the interior of the lock to aid in defeating the locking mechanism.

relocking device – a device separate from the primary locking mechanism which functions to block withdrawal of the bolt if the lock, safe, or vault is forcibly attacked.

removable core – a method for re-keying a lock in which the entire core is removed and replaced with one operated by a different key.

rim lock – a lock mounted on the surface of a door.

rotational tolerance – the tolerance within which a combination must be entered, i.e., the numbers must align with the index mark within plus/minus 1 digit, or 1-1/2 digits, etc.

sawing attack – use of specialized cutting tools to cut through a barrier in a lock, safe, or vault.

scrambling device – a device installed in a mechanical combination lock which scrambles the position of the wheels after the lock has been opened or closed to prevent decoding. Electronic combination locks may perform automatic combination scrambling as part of their programming.

self-contained electronic lock – an electronic combination lock requiring no external source of energy in order to function.

sense manipulation – reliance on the senses of touch, hearing, and sight to assist in a manipulation attack.

shackle – that portion of a padlock which secures the movable barrier to the non-movable barrier and is then secured into the padlock body.

shimming–inserting a thin material, such as a credit card, between a latch and strike plate to retract the latch.

signature analysis attack– analysis of audible or electronic signals for patterns which will help decode and open a locking mechanism.

spindle (as applied to a combination lock)– the rod connecting the combination lock dial to the wheel pack.

strike – a metal plate or box attached to, or mortised into, the door jamb to receive and reinforce the lock bolt.

surreptitious entry – the definitions from FF-L-2740 and FF-P-110G differ slightly. Both specifications agree that surreptitious entry is a method of entry which leaves no evidence which would be detectable during normal use. FF-L-2740 in addition requires that surreptitious entry not be detectable during inspection by a qualified person.

systematic trial and error – an attempt to open a combination by systematically attempting all possible combinations.

thermal sensor – material installed in a lock, safe, or vault which melts at relatively low temperatures. The sensor is used to trigger a relocking device. The purpose is to avoid defeat by environmental attack.

thumb turn – a device used in place of a knob or key to retract a latch or bolt.

UL – Underwriters Laboratories.

wafer (or disk) lock – a lock which requires several disks to be correctly positioned by insertion of the key before permitting key rotation.

warded lock – a lock requiring cuts in the key to match permanent barriers in the keyway (wards) in order to permit key rotation.

x-ray radiography – see radiographic attack.

Distribution:

2 U. S. DOE, DP-68
Office of Field Security Oversight
Attn: William Hensley, Director
Washington, DC 20585

1 U. S. DOE, SA-10
Office of Safeguards and Security
Attn: Edward J. McCallum, Director
Washington, DC 20585

1 U. S. DOE, SA-14
Headquarters Operations Division
Attn: Marshall O. Combs, Director
Washington, DC 20585

1 U. S. DOE, SA-121
Physical Security Branch
Attn: William J. Desmond, Chief
Washington, DC 20585

1 U. S. DOE, SA-121
Physical Security Branch
Attn: Darryl Toms
Washington, DC 20585

1 U. S. DOE, SA-123
Technical and Operations Security Branch
Attn: Larry D. Wilcher, Chief
Washington, DC 20585

1 U. S. DOE, SA-131
Assessment and Integration Branch
Attn: G. Bowser, Chief
Washington, DC 20585

1 U. S. DOE, SA-132
Weapons Safeguards and Security
Operations Branch
Attn: Donald J. Solich, Chief
Washington, DC 20585

1 U. S. DOE, SA-133
Production/Energy Safeguards/Security
Operations Branch
Attn: Avitus J. Heysel, Chief
Washington, DC 20585

2 U. S. DOE, SA-134
Planning and Technology Development
Branch
Attn: G. Dan Smith, Chief
Washington, DC 20585

1 U. S. DOE, SA-134
Planning and Technology Development
Branch
Attn: Carl A. Pocratsky
Washington, DC 20585

1 U. S. DOE, SA-141
Headquarters Physical Protection Branch
Office of Safeguards and Security
Attn: Charles C. Coker, Chief
Washington, DC 20585

1 U. S. DOE, SA-142
Technical/Information Security Branch
Attn: Floyd McCloud, Chief
Washington, DC 20585

1 U. S. DOE/Abuquerque
Central Training Academy
Attn: Don Jewell, Asstistant Director
PO Box 18041
Albuquerque, NM 87185

1 U. S. DOE/SNSD/AL
Security and Nuclear Safeguards Directorate
Attn: Donald A. Gurule, Director
PO Box 5400
Albuquerque, NM 87185

1 U. S. DOE/Amarillo
Safeguards and Security Management Branch
Attn: John E. O'Brien, Chief
PO Box 30030
Amarillo, TX 79120

1 U. S. DOE/BP
Attn: Robert L. Windus, Security Manager
PO Box 3621
Portland, OR 97208

1 U. S. DOE/CH
Safeguards and Security Division
Attn: Harold W. Kelley, Director
9800 South Cass Avenue
Argonne, IL 60439

1 U. S. DOE/CH
New Brunswick Laboratory
Attn: Charleton Bingham
9700 South Cass Avenue
Argonne, IL 60439

1 U. S. DOE/ID
Special Services Division
Attn: R. Green, Director
785 DOE Place
Idaho Falls, ID 83402

1 U. S. DOE/KC
Security Section
Attn: Roger Teska, Chief
PO Box 202
Kansas City, MO 64141

1 U. S. DOE/LLNL
Safeguards and Security
Attn: Don Wentz, Deputy Manager
PO Box 808, MS L556
7000 East Ave.
Livermore, CA 94550

1 U. S. DOE/NV
Safeguards and Security Division
Attn: E. Wayne Adams, Director
PO Box 98518
Las Vegas, NV 89193-8518

1 U. S. DOE/OAK
Safeguards and Security Division
Attn: Douglas A. Ash, Director
1301 Clay Street, Suite 700N
Oakland, CA 94612

1 U. S. DOE/OR
Safeguards and Security Division
Attn: William G. Phelps, Director
PO Box 2001
Oak Ridge, TN 37831-8570

1 U. S. DOE/PNR
Safeguards and Security Division
Attn: J. A. Bullian, Director
PO Box 109
West Mifflin, PA 15122

1 U. S. DOE/RF
Safeguards and Security Division
Attn: Richard J. Levernier, Director
PO Box 928
Golden, CO 80402-0928

1 U. S. DOE/RL
Safeguards and Security Division
Attn: J. L. Spracklen, Director
PO Box 550, MS A6-35
Richland, WA 99352

1 U. S. DOE/SPRO
Security Division
Attn: Donald J. Ornick, Director
900 Commerce Road East
New Orleans, LA 70123

1 U. S. DOE/SR
Safeguards and Security Division
Savannah River Operations
Attn: Larry Brown, Director
PO Box A
Aiken, SC 29802

1 U. S. DOE
Safeguards and Security Division
Schenectady Naval Reactors Office
Attn: George G. Stefani, Jr., Director
PO Box 1069
Schenectady, NY 12301

5 Albuquerque Safe Company
Attn: Steve Highland
3204 Candelaria Blvd. N.E.
Albuquerque, NM 87107

1 BE Inc.
P.O. Box 381
Barnwell, SC 29812

1 Brookhaven National Laboratory
Attn: Joe Indusi
53 Bell Ave., Bldg. 197C
Upton, NY 11973

1 EG&G Idaho
Safeguards and Security
Attn: Roger O. Cook, Manager
PO Box 1624
Idaho Falls, ID 83402-3126

1 EG&G Mound Applied Technologies
Attn: Daniel Baker, Security Manager
PO Box 3000, Bldg. 99
Miamisburg, OH 45343-0987

1 EG&G Rocky Flats
Safety and Health Division
Attn: Shirley C. Olinger, Director
PO Box 464, Bldg. 116
Golden, CO 80402-0464

1 Los Alamos National Laboratory
Attn: Robert Wagner
PO Box 1663, MS G728
Los Alamos, NM 87545

1 Martin Marietta Energy Systems
Paducah Gaseous Diffusion Plant
Attn: A. K. Yancy
PO Box 1410
Paducah, KY 42001

1 Martin Marietta Energy Systems
Attn: E. R. Smith
PO Box 628, MS 1233
Piketon, OH 45661

1 Martin Marietta Energy Systems
Y-12 Safeguards and Security
Attn: W. O. Clements, Manager
Bldg. 9706-1, MS 8212
Oak Ridge, TN 37831-8213

1 Mason & Hanger-Silas Mason Company, Inc.
Pantex Plant, Safeguards and Security
Attn: James J. Hallihan
PO Box 30020
Amarillo, TX 79177-0001

1 Westinghouse Hanford Company
Safeguards and Security Division
Attn: W. R. Brooksher, Manager
PO Box 1970, MS L4-01
Richland, WA 99352

1 Westinghouse Idaho Nuclear Company
Safeguards and Security Division
Attn: E. L. Goldman, Manager
PO Box 4000
Idaho Falls, ID 83403

1 Westinghouse Savannah River Company
Safeguards, Security, & Emergency Preparedness
Attn: J. W. Dorrycott, Manager
PO Box 616
Aiken, SC 29802

1	MS	0769	D. S. Miyoshi (5800)
1	MS	0768	R. W. Moya (5804)
2	MS	0762	Safeguards and Security Library (5805)
1	MS	0768	J. W. Kane (5806)
1	MS	0781	D. J. Gangel (5831)
1	MS	0780	D. S. Fitzgerald (5838)
1	MS	0780	S. Ortiz (5838)
1	MS	0759	I. G. Waddoups (5845)
1	MS	0782	J. F. Chapek (5848)
1	MS	1131	B. J. Steele (5849)
1	MS	0570	C. W. Childers (5900)
1	MS	0571	R. L. Ewing (5914)
5	MS	0847	M. G. Wilde (5931)
10	MS	0815	K. T. Gee (5932)
6	MS	0815	J. V. Williams (5932)
5	MS	0899	Technical Library (7141)
1	MS	0619	Technical Publications (7151)
1	MS	0173	J. D. Martin (7400)
10	MS	0100	Document Processing for DOE/OSTI (7613-2)
1	MS	9018	Central Technical Files (8523-2)
1	MS	0766	J. R. Kelsey (9600)
5	MS	0783	S. H. Scott (9611)

Sandia National Laboratories

DATE
FILMED
5/10/94
END