



U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.12

GENERAL USE OF LOCKS IN THE PROTECTION AND CONTROL OF FACILITIES AND SPECIAL NUCLEAR MATERIALS

A. INTRODUCTION

Paragraph 50.34(c) of 10 CFR Part 50, "Licensing of Production and Utilization Facilities," requires each application for a license to operate a production or utilization facility and paragraph 70.22(b) of 10 CFR Part 70, "Special Nuclear Material," requires certain applications for a license to possess or use special nuclear material (SNM) to include a physical security plan to demonstrate how the applicant plans to meet the physical protection requirements of 10 CFR Part 73, "Physical Protection of Plants and Materials." Paragraphs 50.54(p) and 70.32(e) require existing licensees licensed under Part 50 and certain licensees licensed under Part 70 who have not submitted a physical security plan to submit such a plan to the Commission for approval. Section 73.40 of 10 CFR Part 73 requires that certain licensees provide physical protection against industrial sabotage and against theft of SNM at the fixed sites where licensed activities are conducted.

Locks are acceptable devices to be used in adhering to the physical protection requirements identified above to assist in controlling access to areas, facilities, and materials through doors, gates, container lids, and similar material or personnel access points, and are considered essential components of a physical barrier. This guide provides criteria acceptable to the Regulatory Staff for the selection and use of commercially available locks in the protection of facilities and SNM.

B. DISCUSSION

Locks are very important components of a physical barrier. Their effectiveness, however, lies in their use in conjunction with other security measures such as intrusion alarm systems and seals. Although some locks

are difficult to pick or manipulate, no lock can claim to be "manipulation proof." Because of the large variety of locks available, it is necessary to subdivide the discussion on locks into the following types: (1) combination, (2) key, (3) electrical, and (4) pushbutton mechanical locks. The discussion of each type includes a general section on advantages and disadvantages, a section on control over the locks, and a section on the applicable standards and specifications.

1. Combination Locks

a. General. It is desirable that a combination lock be designed to afford a choice of a large number of combinations. The number of combinations is determined by the number of tumbler wheels in the lock mechanism and the number of graduations on the dial. High-quality locks usually have 100 divisions on the dial and three tumbler wheels; such a lock is capable of providing a theoretical 10^6 combinations which in practice reduces to tens of thousands. Some combination locks are made with four tumbler wheels, but it is considered that the added number of combinations possible does not proportionally improve the security of the lock and does increase the inconvenience of dialing the combination.

It is desirable for a combination lock to be designed so its combination can be easily changed but at the same time be tamper resistant. The combination of some locks can be changed by disassembly of the tumbler wheel pack and relocation of screws or pins. In this method the effective number of combinations possible is restricted. Another method involves taking apart the wheel pack and resetting an insert in each wheel. This method requires substantial skill on the part of the operator. The most desirable method of changing a combination is by a special key which requires minimal training of the operator and provides a maximum number of combinations. The special key is inserted in

USAEC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the AEC Regulatory Staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Published guides will be revised periodically, as appropriate, to accommodate comments and to reflect new information or experience.

Copies of published guides may be obtained by request indicating the divisions desired to the U.S. Atomic Energy Commission, Washington, D.C. 20545. Attention: Director of Regulatory Standards. Comments and suggestions for improvements in these guides are encouraged and should be sent to the Secretary of the Commission, U.S. Atomic Energy Commission, Washington, D.C. 20545. Attention: Chief, Public Proceedings Staff.

The guides are issued in the following ten broad divisions:

- | | |
|-----------------------------------|------------------------|
| 1. Power Reactors | 6. Products |
| 2. Research and Test Reactors | 7. Transportation |
| 3. Fuels and Materials Facilities | 8. Occupational Health |
| 4. Environmental and Siting | 9. Antitrust Review |
| 5. Materials and Plant Protection | 10. General |

the back of the lock case to release the wheels from their present combination while a new combination is imposed by dialing.

The combination of some locks can be covertly determined by using a radiographic technique. Resistance to this form of attack is designed into certain locks by utilizing materials in the mechanism that are not easily radiographed, e.g., plastics.

Combination locks are vulnerable to compromise if the back of the lock is readily available, e.g., when the lockable access is open. Removing the back cover from the lock usually allows the combination to be determined. The combinations of some key-change locks can be changed directly when the lock is in the open position, while other must have the existing combination redialed to a different index when the access is in the open position to permit the combination change. The former type permits an intruder to make a quick change of the combination to one of his own choosing; this would permit him to enter following the closing of the lock and would deny entry to the user. For these reasons it is desirable to protect the back of the lock by back plates or other devices.

High-quality combination locks are designed for use in two basic forms: (1) in a lock case to be mounted on or into a door as a mortise or rim lock and (2) as a padlock.

Protection against forcible attack of a mortise or rim-mounted lock can be increased if the lock is provided with hardened steel plates and if the lock is designed with relocking triggers or devices that deadlock the bolt or bolt-actuating mechanism.

Combination padlocks are not vulnerable to the usual rapping techniques and are usually resistant to manipulation. However, common combination padlocks made of a cast aluminum alloy are without great strength, have little resistance to forcible attack, and are not weather resistant. There are others that are weather resistant but offer little protection against attack.

b. Combination Lock Control. The most important aspect of lock control for combination locks is the protection of the combination. It is desirable to change the combination of a lock every time that a person who knows the combination no longer requires it as a result of termination or reassignment of duties. This would assure that only those individuals actually required to gain access would know the combination.

Losing the combination of a manipulation-proof, well-designed lock in a high-rated door is an expensive situation. This can be prevented by keeping a record of the combination in another location which is as secure as the place protected by the lock.

Combination locks can be set to a single number to simplify the daily chore of opening, but this is a very poor practice since it reduces the security of the lock. Frequently four-wheel locks are set to only three different numbers for ease of opening. This defeats the purpose of the fourth wheel but it is not considered serious since the number of remaining combination choices is considered adequate. It is not recommended that one select combinations in common sequences and multiples of ten. It is also not generally recommended that the last number of a combination be set close to zero because in some cases the lock can jam.

c. Standards and Specifications. A standard for three- or four-tumbler combination locks issued by Underwriters' Laboratories, UL-768, "Combination Locks,"¹ covers "combination locks designed for attachment on doors of safes, chests, vaults, and the like to provide a means of locking the boltwork against unauthorized opening." Quality assurance provisions covering the description, examination, and testing of the product are included through the UL Label Service. A Federal Specification issued for combination padlocks, FF-P-110F, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack),"² includes quality assurance provisions for design, materials, and performance testing.

2. Key Locks

a. General. As in the case of combination locks it is desirable for a key lock to be capable of being set for a large number of different keys. A high-quality six-pin lock with 10 key cutting levels per pin potentially permits 10^6 different keys to be used. However, this large number of key cuts is not as useful as a large number of combinations because less time-consuming techniques for defeating key locks are available. Nevertheless, there is value in specifying at least 10^6 key cuts because it requires careful construction of the lock.

It is important that the key cut required to open a lock (bitting of a lock) be changeable to permit changes whenever keys are lost or an employee having access to a key is reassigned to other duties or

¹Copies may be obtained from the offices and testing stations of Underwriters' Laboratories, Inc. located at the following addresses: 207 East Ohio Street, Chicago, Ill. 60611; 333 Pflingsten Road, Northbrook, Ill. 60062; 1285 Walt Whitman Road, Melville, L.I., N.Y. 11746; 1655 Scott Boulevard, Santa Clara, Calif. 95050.

²Copies may be obtained from business service centers of the General Services Administration Regional Offices located in the following cities: Boston, Mass.; New York, N.Y.; Washington, D.C.; Ft. Worth, Texas; Denver, Colo.; San Francisco, Calif.; Atlanta, Ga.; Chicago, Ill.; Kansas City, Mo.; Los Angeles, Calif.; Seattle, Wash.

terminated. Changing the bitting of a lock can be accomplished usually by changing pins, wafers, or levers. To ease the task of a bitting change, some locks have cores that are removable for replacement by means of a special key called a "control key." If all the locks in a given facility are keyed to the same control key, the locks are virtually master keyed because, with the core removed, the problem of opening the lock is elementary.

Master keying is undesirable from a security point of view because disassembly and inspection of any lock in the system by a competent person provides access to all the other locks in the master-keyed system, and because termination of an employee who had access to a master key would require changing the bitting of all locks set for his master key. The changing of the bitting of a large number of locks can be costly, but the convenience of master systems is such that there is strong pressure for using them. A compromise in this conflict between convenience and security may be to use a nonmastered set of locks for protected areas, material access areas, vital areas, and access to vital equipment and to permit master key sets for other less sensitive areas.

It is necessary for a lock to have some resistance to picking and impressioning (a method used to prepare a key by the impressions of the bitting of a lock on a blank key). In general, this resistance can be provided by precision machining of the mechanisms or by special design features such as side bars, odd-shaped pins or a large number of levers.

Protection of key locks against forcible attack can be enhanced by the use of hardened steel plates in front of the pins or side bars.

It is essential for a bolt of a lock to be retained in the locked position by positive means (dead bolt). In some locks, the bolt is held in a locked position by a spring only. This permits, in the case of padlocks, the use of appropriate rapping or shimming techniques and, in the case of door locks, the opportunity to surreptitiously retract the bolt without the use of force.

b. Lock Control. The security of an access control system based on key locks depends on complete denial of keys to unauthorized persons. It is essential to have a record of each key and the names of individuals to whom keys have been issued and to check all keys at periodic intervals.

A common weakness in mastered key systems is the lack of accountability of lock cylinders. To correct this situation, it would be necessary to require a control system involving the accountability of every mastered lock cylinder having the bitting in present use either for the master or, in the case of removable cores, the control key.

c. Standards and Specifications. A standard for key locks has been issued by Underwriters' Laboratories, UL-437, "Key Locks,"¹ and includes quality assurance provisions through the UL Label Service. Interim Federal Specification FF-P-001480 (GSA-FSS), "Padlock, Key Operated (Resistant to Opening by Force, Pick, and Bypass Techniques),"² covers two types of key-operated dead-bolt padlocks: the exposed shackle and the shrouded shackle. Quality assurance provisions concerning the design, materials, and qualification testing are included.

3. Electric Locks

a. General. In the most popular electric locks, a signal generated by magnetized elements in a plastic card or by sequential activation of buttons is compared with a stored code to activate an electrically operated door strike. In some cases the magnetic card and pushbutton systems are used in coincidence. Combined card and pushbutton systems provide, in general, higher security than card-only systems.

The advantages of the electric lock are isolation of the part containing the code from the exposed part of the lock, versatility of programming, and ease of integration into alarm systems.

Magnetic card systems have some of the problems of common key locks because a lost or stolen card can be used by an unauthorized person. However, reproduction of a card is more complicated than reproduction of a metal key.

Pushbutton systems require memorization of a few digits, usually four, and require more time to operate than the magnetic card system. Although the number of possible combinations usually is smaller than in the combination lock system, quality electric pushbutton systems compensate for this by incorporating devices which prevent trial and error methods of surreptitious attack by activating an alarm after a number of unsuccessful attempts or by introducing a delay after each unsuccessful attempt which prevents operation of the lock for a short period of time.

It is desirable for an electric lock to have the capability for an easy change of combinations. The part of the lock where the combination is set and the housing of the card reader (if the contents of the housing can reveal the combination) should be protected against tampering by tamper switches connected to the alarm system.

Generally, where electric locks are installed, a mechanical lock is also installed as a bypass. This lock should be of a quality as discussed in the part on key locks in this guide.

b. **Lock Control.** The security of an electric lock system depends on strict control of combinations and cards. The magnetic codes in the cards and the combinations need to be changed whenever an employee having had access to them terminates or is reassigned. Strict accountability of cards is strongly recommended.

c. **Standards and Specifications.** There are currently no comprehensive standards or specifications covering electric locks. The reputation of the manufacturer, the specification for his product, and the experience of users must be carefully considered in their selection and use.

4. Pushbutton Mechanical Locks

a. **General.** This is a type of combination lock utilizing mechanical-pushbutton-activated linkages that connect a gate with an external knob to permit opening of the lock. In this lock it is difficult to design in penalties for punching a wrong combination as is done in electric locks. Therefore, it is important to have a large number of possible combinations.

Provisions for easy change of combinations are desirable. Some locks permit a new combination to be dialed in utilizing an Allen wrench when the lock is open, a procedure similar to that for some combination locks. Others require the replacement of internal parts to change the combination.

The mechanical locks appear to be fairly resistant to concealed attack; however, more information is needed on their resistance to forcible attack.

b. **Lock Control.** Similar to other combination locks, the combinations need to be changed when employees having access to the combination terminate or are reassigned.

c. **Quality Assurance.** There are currently no comprehensive standards or specifications for mechanical pushbutton locks.

C. REGULATORY POSITION

The following guidelines are acceptable to the Regulatory staff for the selection and use of locks in the protection of facilities and SNM:

1. **Combination locks** installed in solid doors such as those in vaults or vault-type rooms in protected areas should be three- or four-position dial-type changeable-combination locks meeting the Underwriters' Laboratories Standard UL-768, "Combination Locks," for Group I locks.¹

2. **Combination padlocks** should be used when practicable on doors or gates to material access areas, in

protected and vital area perimeters, and for access to vital equipment in preference to key padlocks. Combination padlocks should be used on closed vehicles or containers holding SNM that are required to be locked. Combination padlocks should be three-position-dial type changeable-combination padlocks meeting Federal Specification FF-P-110F, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)."²

3. **Key locks** used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should provide a high degree of resistance to opening by force and tamper techniques and should meet Underwriters' Laboratories UL-437, "Key Locks."¹

4. **Key padlocks** used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should be of rugged and sturdy construction and designed for outdoor use if necessary, and should meet Interim Federal Specification FF-P-001480 (GSA FSS), "Padlock, Key Operated (Resistant to Opening by Force, Pick, and Bypass Techniques)."²

5. **Electric locks** should be used inside the protected area as a means of access control only if a magnetic card key system is coupled with a pushbutton system and integrated into the alarm system. This lock combination should have features that resist tampering with the combination-changing mechanism and that alarm after a set number of errors in punching the combinations is made.

6. **Pushbutton mechanical locks** are not recommended for use at this time because of the lack of comprehensive standards and specifications against which the locks can be evaluated.

7. **Mechanical locks** used as panic locks on emergency exit doors within protected area perimeters should be operable only from the inside.

8. **Combinations, keys and locks** should be controlled, protected and changed in accordance with the following requirements:

a. **Combinations of locks or padlocks** on repositories containing SNM or used to secure gates or doors to material access areas, in protected and vital area perimeters, and for access to vital equipment should be known only to those authorized access to the material or to the area. They should be changed when repositories or areas are first placed in use, whenever a person knowing the combination no longer requires it as a result of reassignment of duties or termination, whenever the combination may have been compromised, or at least twice every year. A record of the combinations of locks should be kept in a location that is secured by a combination lock.

b. Keys and cards to locks or padlocks on containers holding SNM or used to secure gates or doors to material access areas and in protected and vital area perimeters should be issued only to persons authorized access to the material or to the area. Keys or cards in use should be checked in at the end of each shift or workday, and a log should be maintained showing keys and cards, users, in and out times, and other pertinent information. Keys and cards should be recovered from reassigned or terminating personnel. Locks should be immediately changed or cores replaced and an inventory conducted whenever a core, key, or card is lost or missing; the lock, core, key, or card has been compromised; or unrecorded keys or cards are found. In

a mastered system, a complete remastering of the system should be conducted whenever a core, card, master or control key, or a lock is lost or compromised.

c. A record of all locks, cores, keys, and cards should be maintained and kept in a location secured by a combination lock. A physical inventory of locks, cores, keys, and cards should be conducted semiannually when the locks are used for protection of facilities and bimonthly when the locks are used for the protection of SNM. Unused locks, cores, keys, and cards should be stored in a location secured by a combination lock. A specific individual at each site should be named and placed in charge of all locks, cores, keys, and cards.