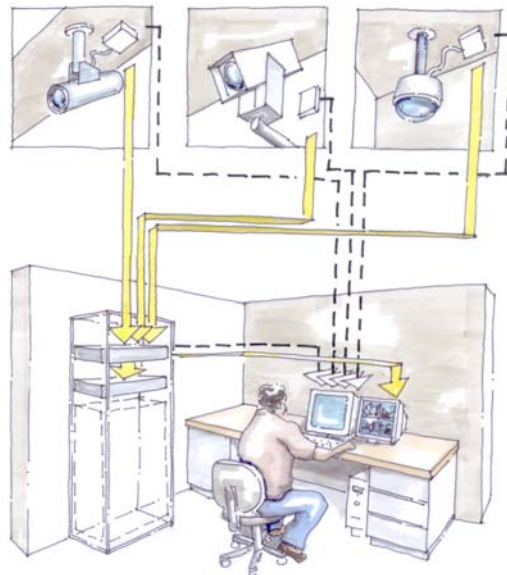


Library Security



This material was created by Mark McComb, RLS Inc., San Francisco. Valuable review and contributions were provided by Edward Dean AIA. Illustrations were done by Michael Bulander, Architect, Los Angeles. The publication is provided through the Libris Design Project [<http://www.librisdesign.org>], supported by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. Any use of this material should credit the authors and funding source.

CONTENTS

1.	INTRODUCTION	1
2.	RISK ASSESSMENT.....	1
2.1.1.	Best Practices.....	1
2.1.2.	Understand the organization and identify the people and assets at risk.....	1
2.1.3.	Specify loss risk events and vulnerabilities.....	2
2.1.4.	Establish the probability of loss risk and frequency of events.	2
2.1.5.	Determine the impact of the events.	2
2.1.6.	Develop options to mitigate risks.	2
2.1.7.	Study the feasibility of actual implementation of options.	2
2.1.8.	Perform a cost/benefit analysis.....	3
3.	PHYSICAL SECURITY (NON-ELECTRONIC)	3
3.1.1.	Architectural Considerations	3
3.1.2.	Security Personnel	8
3.1.3.	Security Hardware	8
3.1.4.	Display Case Protection	10
4.	ELECTRONIC SECURITY	11
4.1.1.	Burglary Protection.....	11
4.1.2.	Collection Security.....	15
4.1.3.	Access Control.....	16
4.1.4.	Video Surveillance.....	17
5.	SECURITY POLICIES, PROCEDURES, AND PLANS	22
5.1.1.	Entry and Exit Procedures.....	22
5.1.2.	Room Registration	22
5.1.3.	Special Collections.....	23
5.1.4.	Entry Key Management	24
6.	GLOSSARY OF TERMS	25
7.	REFERENCES AND ORGANIZATIONS/WEBSITES	25
7.1.1.	References	26

1. INTRODUCTION

The goal of the security system should be to provide a safe and secure facility for library employees, library resources and equipment, and library patrons. At the same time, the security system must perform these functions as seamlessly as possible, without interfering with the library's objective of easily and simply providing patron services.

Security, as the subject is treated in this article, is limited to the physical safety of staff and patrons, and the protection of the library and its collections from theft and vandalism, but does not include a discussion of fire protection or disaster planning issues.

2. RISK ASSESSMENT

2.1.1. Best Practices

The first step in determining the required level of security systems in a library is to conduct a security risk assessment. ASIS International, the leading international organization of security professionals, has published a guideline entitled, *The General Security Risk Assessment Guideline*. The purpose of this publication is "to provide a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions." The following seven steps, which are recommended within the document, apply to the approach to the design of security systems for libraries.

2.1.2. Understand the organization and identify the people and assets at risk.

To understand the organization, the library should ascertain its hours of operation, staffing levels, types of services provided, types of material/collections stored, and the type of clientele. The people at risk include employees, volunteers, patrons, vendors, and others that are directly or indirectly involved with the library.

The assets at risk include all types of tangible property including books, periodicals, archive material, computers, microforms, special collections, artwork, and other valuables. Intangible assets may also be at risk, such as intellectual property and causes of legal action. Other assets at risk include:

- The library's *core business*, that is, the ability to easily provide information as well as the library's reputation and public goodwill.
- The library *networks*, namely, all systems, infrastructures, and equipment associated with data, telecommunications, and computer processing assets.
- The library *information*, including various types of proprietary data.

2.1.3. Specify loss risk events and vulnerabilities.

Risks or threats are those incidents likely to occur at the library, either due to a history of such events or circumstances in the local environment. They also can be based on the intrinsic value of assets and collections housed or present at the facility. A loss risk event can be determined through a vulnerability analysis. The vulnerability analysis should take into consideration any aspect of the building or procedures that could allow a threat to be carried out. This process should highlight points of weakness and assist in the construction of a framework for subsequent analysis and countermeasures.

2.1.4. Establish the probability of loss risk and frequency of events.

Frequency of events corresponds to the regularity of any loss events. For example, if the threat is the loss of books at the library, the frequency would be the number of times the event occurs each day. Probability of loss risk is based upon considerations of prior incidents, trends, warnings, or threats, and the history of such events occurring at the library.

2.1.5. Determine the impact of the events.

The impact is the financial, psychological, and any related costs associated with the loss of tangible or intangible assets of the library.

2.1.6. Develop options to mitigate risks.

Identify options available to prevent or mitigate losses through physical, procedural, logical, or related security processes.

2.1.7. Study the feasibility of actual implementation of options.

The key issue of this study is the implementation of the mitigation options without substantially interfering with the operation of the library.

2.1.8. Perform a cost/benefit analysis.

This final step is a systematic attempt to measure or analyze the value of all the benefits that accrue from a particular expenditure.

The formation of a “security team” to be responsible for the development and implementation of a risk assessment plan is imperative in determining the best security solutions for a specific library, whether it is the design of a new facility, a remodel of an existing facility, or simply assessing and improving security for an existing facility.

The remainder of this article will focus on Step 5, Develop options to mitigate risks. To mitigate the risks specifically associated with library facilities, three aspects should be evaluated:

1. Physical security including architectural considerations, staffing, and hardware such as door and window protection.
2. Electronic systems such as building alarm systems and access control systems.
3. Security policies, procedures, and plans.

3. PHYSICAL SECURITY (NON-ELECTRONIC)

The first step in securing library assets includes physical (non-electronic) deterrents. These include architectural considerations, the use of security personnel, and security hardware.

3.1.1. Architectural Considerations

Site Design

Site planning and landscape design issues should be considered when planning for a safe and secure library. Site lighting at vehicular and pedestrian entrances and circulation areas should be continuous and sufficient to support a secure atmosphere as well as support appropriate surveillance.

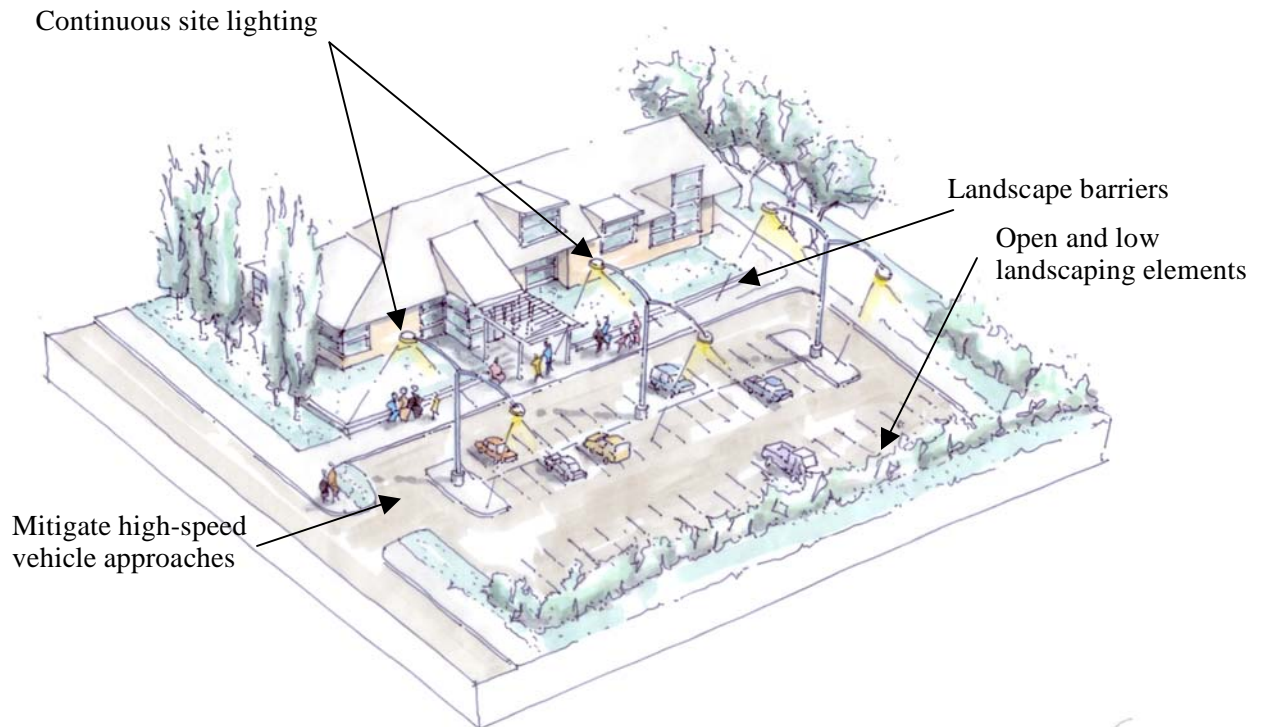


Figure 1. Site design security features.

Appropriate and clear signage should be provided, including off-site and entrance signage as well as on-site signage that should include directional, cautionary, and parking signs for employees, visitors, service vehicles, and pedestrians. Signs should generally not be provided to identify sensitive areas.

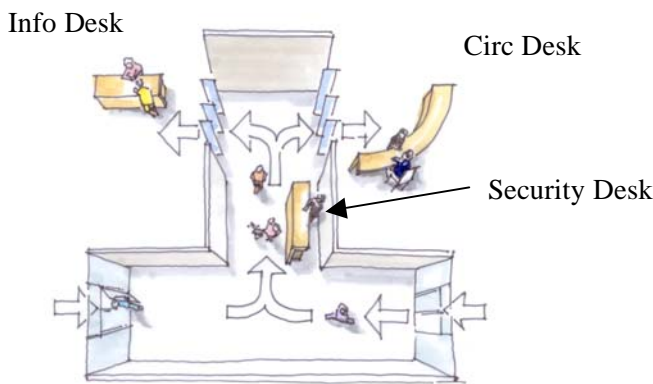
Landscaping elements should enhance security by deterring unwanted entry while not allowing criminals to conceal themselves from security personnel and CCTV systems. Vehicle control is important; a specified distance from the library building to unscreened vehicles and parking should be appropriately set. Various types of buffers and barriers should be evaluated to enhance the landscape design while still providing the appropriate protection. These buffering features could include walls, fences, trenches, plantings, trees, static barriers, sculptures, and street furniture. Vehicular entrances should be designed to prevent high speed approaches.

Building Design

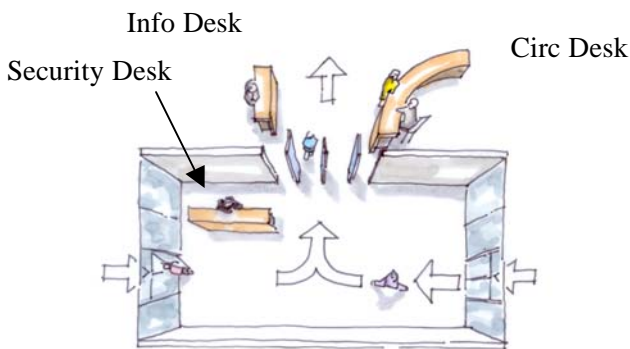
The following areas generally will have security issues that should be appropriately addressed in the design:

- Exterior entrances
- Archive and special collection storage spaces
- Special collection reading areas
- Children’s library area
- Critical building component locations such as electrical switchgear, communication and security equipment, and building control centers
- Public toilets
- Loading docks, mailrooms, and shipping/receiving areas
- Stairwells
- Office locations
- Roof access

Entrances and exits from the library are a particular concern with regard to theft of library materials. When designing a new library, the ideal arrangement is a single point of entry to the secure area of the facility. Magnetic theft detection devices are placed at this location to sound an alarm if unchecked library materials are taken through this point of control.



(a)



(b)

Figure 2. Some alternate methods of handling two points of entry. (a) two sets of book detection devices; (b) one set of book detection devices.

Occasionally, however, it may be desirable for external planning reasons to allow patrons to approach and enter the library from opposite directions, resulting in two points of entry to the building. This could result from site features, required location of parking areas versus public transportation locations, or urban design considerations. It is important in these situations to continue to maintain a single point of entry to the secure area of the library. Although this may require special planning and space arrangement within the library, several layouts, as shown in Figure 2, can accommodate this requirement. The key feature of these diagrams is a single point of control at the principal entry to the space.

Special collections spaces, depending on the value of the collections, require a certain level of security design and electronic systems. The risk of theft, particularly for rare books and artifacts, can be high, and both the architectural space planning and the specialized systems should reflect the determined level of risk.

Control of entrance and exit from special collection areas, as well as the design of electronic systems, are discussed below. In general, however, the space planning of special collection areas and their support spaces should be determined as part of the overall security design features.

The arrangement of the special collections service desk with regard to the reading areas and any bookstacks should be planned so that a clear line of sight exists between the desk and the reading tables. Flat open tables are preferred to enclosed furniture or carrels, so that surveillance can be maintained at all times. If bookstacks are located in the special collection reading areas, they should not be positioned so that the visibility of any patron workstation is blocked.



Figure 3. Arrange special collections service desk so that unobstructed view is obtained of all reading tables. Note flat, open tables.

Toilets or other enclosed spaces that cannot be readily monitored should not be located within special collection areas. It may also be desirable to institute a checking procedure for personal belongings and bags before a patron is allowed to enter these sensitive areas. This policy

requires the location of a locker space near the entrance to the special collection room or suite.

Children's library areas are also sensitive with regard to space design and control features, both for protection and monitoring of children's activities. Views in and out of these areas should be through controlled spaces only. Access should also be controlled by positioning the children's area within the secure area of the library, though within easy access of the entry and main security checkpoint.

The building designer should generally try to minimize the number of required staffing locations within the library for reasons of operating economy. Avoiding poor space planning that results in security concerns for certain areas of the building should be part of this design objective, since such concerns could result in the need for a staff monitoring location. For example, relatively isolated areas within the bookstacks that are difficult to monitor are often a problem if this issue is not addressed. Adjacency to circulation, other frequently used spaces, or windows is preferred to remote corners screened by bookstacks.

Finally, large toilet rooms are often placed outside the secure area of the library, primarily for

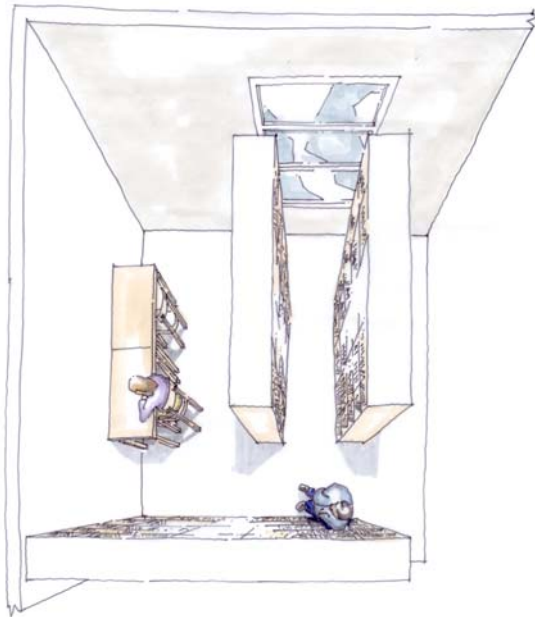


Figure 4. Avoid creating relatively isolated areas within bookstacks. Though desirable by patrons for quiet reading, these areas are difficult to monitor.

after-hours access. If convenient, this location also ensures lack of isolation. Any toilet rooms

internal to the library should be positioned so that entrances are visible from populated areas and not in relatively isolated locations.

3.1.2. Security Personnel

As part of the security plan, the library security team should evaluate the value and need for security personnel, during both normal working hours as well as after the library is closed. Security personnel typically patrol within the facility as well as on the grounds and operate any implemented CCTV system. The security guards may also be used to enforce appropriate library access at the main lobby.

3.1.3. Security Hardware

Physical (non-electronic) protection for libraries is the first level of defense against theft and vandalism. Window protection, door protection, display case protection, and “dummy” security devices all ensure that criminals do not have uncontrolled access to the assets of the library.

Window Protection

There are many types of window security including locks, guards, grilles, bars, screens, and films.

Window locks should be fitted to all windows that can open and are accessible without the means of a ladder. For best control, these windows should be secured by key-operated locks (not just a simple latch). This includes all ground floor windows, windows above garages or other roof tops, windows near to walls or pipes or other structures, which could be used to access the window. Generally, any window over 60 cm. in height (approximately 24 inches) should be fitted with two key-operated window locks to prevent forced opening.

If the security risk assessment investigation determines that the library location has the potential for burglary through windows or vandalism to the windows, then guards, grilles, bars, security screens, or security films should be installed.

Securing the window through the use of guards, grilles, or bars is not always architecturally acceptable, although they can be a cost effective solution in certain circumstances.

A wide range of security screens and films is also available. When using the screens or films, there are no unsightly iron bars, steel mesh, or expanded metal which may not actually protect the glass. Screens and films unobtrusively protect property and glazing by preventing access to windows.

A security screen is made of a durable metal and is mounted in front of or behind existing windows. They can allow over 60% of light and air transmission, which means ample air flow and visibility and no “closed-in” feeling of traditional security methods. From a distance, screens merely give the impression that windows are fitted with tinted glass, but at close quarters it is a visible deterrent to intruders.

Security films can provide a significant improvement over standard or tempered treated glass in its ability to withstand an attack from weapons such as a baseball bat, flying rock, or other blunt weapons. While a criminal may muster enough force to shatter the window, it will require repeated (and attention-getting) blows to break through the virtually impenetrable film. Generally, the burglar cannot risk the time needed to break through, and will abandon the attempted burglary. The film adheres to the window pane and holds the glass together in the event of an attack. These films are also used to ensure the safety of anyone who may fall or be thrown against the glass by holding the glass in one piece in much the same way as laminated glass.

Door Protection

Door protection includes cylindrical locks, deadbolts, mortise locks, and gates.

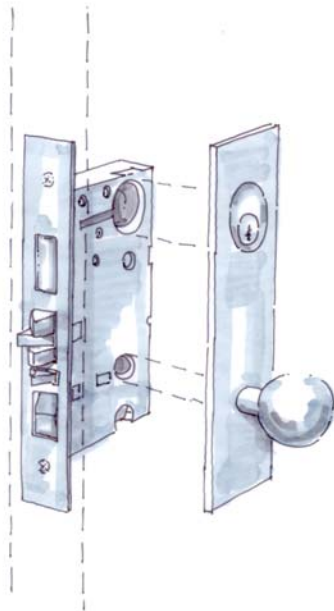


Figure 5. A mortise lockset. A deadbolt is an integrated part of the locking mechanism.

A *cylindrical lockset* fits into a large hole bored into the door's face with the keyhole in the door knob. The latch assembly is locked and provides the securing of the door, though this type of lock provides the least amount of security in door protection. The addition of a *deadbolt* provides enhanced protection by increasing the metal support into the door jam. The throw of the deadbolt should be at least one inch. A *mortise lockset* fits into a rectangular pocket in the door's edge and usually has a deadbolt that is an integrated part of the locking mechanism. When you turn the key from the outside, it releases both the knob and the deadbolt. The mortise lockset is the most secure locking mechanism for a door.

If the security risk assessment investigation determines that the library location has the potential for burglary through accessible doors, then security gates should be considered. Securing doors through the use of gates is not always architecturally acceptable and could require special treatment to allow exiting in case of fire. Normally such security gates should be considered only for high crime environments.

Folding gates are designed to make facilities more secure and still allow frequent, easy access to those who need it. They fold easily back and out of the way when people or equipment need to pass, but provide a lockable barrier when closed. Security gates are excellent for situations where extensive security is desired when the library is closed or at restricted access points (such as rear entries), but visibility and air flow are desired as well. Securing front doors after-hours, shipping and receiving docks, and other restricted areas such as archive storage is sometimes most cost effective with folding gates. Folding gates typically retract to a fraction of their extended width and pivot up to 270 degrees to clear the doorway. They are typically designed to accept padlocks for secure closing.

3.1.4. Display Case Protection

Libraries frequently exhibit valuable collections and artifacts of various kinds in display cases, and the security of these items is a special concern. The display cases themselves need to be made with materials of appropriate strength and should be anchored to the building structure so that the entire case cannot be removed from the premises. The display cases further need to be appropriately locked with cabinet or specialty locks. Finally, the glass used for the case should be laminated with security film as discussed above.

Dummy Security Devices

The security system components within a library are often placed in visible locations so that they become more of a deterrent to thieves or vandals. The deterrence of damage or theft is the important first step in any security arrangement, since it prevents damage or loss when successful, and avoids the possible need of apprehension in the event of an alarm.

Occasionally, dummy security devices can be utilized as part of a deterrence strategy, at a great cost savings to the library.

Inactive CCTV cameras are the most commonly utilized device for this purpose. These cameras are available with long lasting LED's that are powered either by battery or by plug-in. Cameras typically come with a mounting bracket for ceiling or wall mount, cables and connectors, mounting block, and auto iris lens, all of which create a very realistic effect.

Actual CCTV camera housings and ceiling domes are also utilized in this setting. Additionally, inactive EAS (electronic article surveillance) pedestals can be placed at the doorways to create the impression that the books have security tags. To enhance the effect, deactivator pad decals can be placed on the circulation desk so that it appears that the security tags are deactivated when books are checked out.

4. ELECTRONIC SECURITY

The second step in securing a library is the use of electronic security equipment. These components typically provide alarm notification to the appropriate authority, entry control, and site surveillance. The major elements of any electronic security system include burglar protection, collection security, access control, and video surveillance.

4.1.1. Burglary Protection

A burglar protection system includes sensors to detect an intrusion, alarms, and notification to the appropriate authorities.

There are different ways of classifying the types of sensor systems. Sensors can be active or passive, covert or visible, volumetric or line detection. They can also be defined by their mode of application. Active sensors transmit some type of energy and detect a change in the received energy created by the presence or motion of the intruder. Passive sensors detect some type of energy emitted by the intruder, or detect a change of some natural field of energy caused by the intruder. Covert sensors are hidden from view and visible sensors are in plain view. Volumetric sensors detect intrusion in a volume of space, where line detection sensors detect intrusion across a line.

Door and Window Contacts

Door and window contacts are used to trigger an alarm whenever a door or window is opened. They can be attached to, or recessed within, the door or window frame to detect movement. In addition to the standard door and window contacts, there are contacts for outdoor use, for specialty uses, and for high security applications. Most contacts are “normally closed” and consist of two parts: a switch which is mounted on the fixed structure (door or window frame) and a magnet which is mounted on the door or window. When the magnet is in close proximity to the switch, the magnetic field closes the switch. Opening the door or window causes the switch to be opened, triggering an alarm condition.

In addition to magnetic contacts, there are switches that mount in the frame. The action of opening the door or window allows the switch to pop out, opening the switch. When it is normal to leave a window partially open during the alarmed state, the window can be configured with two magnets and one switch. In this configuration, the first magnet is mounted for the window in the fully closed position. The second magnet is mounted for alignment with the switch when the window is in the partially opened position and will trigger the alarm if the window is fully opened.

Contacts should be installed on all doors and windows that are accessible, providing early intrusion notification. Other externally mounted apparatus that can be easily removed may also require protection with security contacts.

Glass Break Protection

There are many security solutions to protect windows and glass. These solutions include the use of acrylic, shatter resistant polycarbonate sheets, as well as wire glass, to discourage breakage. Additionally, vibration detectors and audio discriminators can be added to the alarm system's intrusion detection equipment to detect forced entry. The type of glass to be protected (plate, tempered, laminated) must be considered when selecting glass break detection.

Vibration Detectors

Mounted on the window frame or the glass itself, vibration detectors react to vibrations that are created if someone attempts to break or shatter the glass. Also referred to as shock or vibration sensors, they are adjusted to avoid false alarms by allowing normal vibrations on the glass. Glass-mounted vibration detectors require the use of an attached (visible) wire and are placed about an inch from a corner frame, where acoustic waves concentrate on shock to the glass. Though glass-mounted vibration detectors have less probability of false alarm over frame mounted, their use is restricted to stationary glass where the appearance of the lead wire is not an aesthetic concern.

Audio Discriminators

Frequently, several windows or glass openings can be protected by installing an audio discriminator that will sense glass breaking. Also referred to as acoustical or sound detectors, these security devices can be mounted on the frame, wall, or ceiling. They are tuned to alarm on specific sound frequencies that correspond to breaking glass or excessively loud

noises. Sound detectors are susceptible to loud background noises (music, machinery) and their sensitivity can be reduced by window coverings and other sound dampening materials. The device's sensitivity is adjustable so that ambient noises or normal sounds will not trigger an alarm.

Alarmed Window Screens

Standard window screens can be laced to provide protection in the event they are cut or removed. This provides the added convenience of allowing windows to be open and the security system to remain intact when armed. A special wire is woven into the screening material such that if the screen is cut an alarm is triggered. Existing window screens can be wired and then re-installed on the windows.

Motion Detectors

Motion detectors provide protection by detecting movement within specific areas. They can be used to illuminate an area automatically, or to trigger a silent or audible alarm. These devices are typically located near the openings they are intended to protect. The most

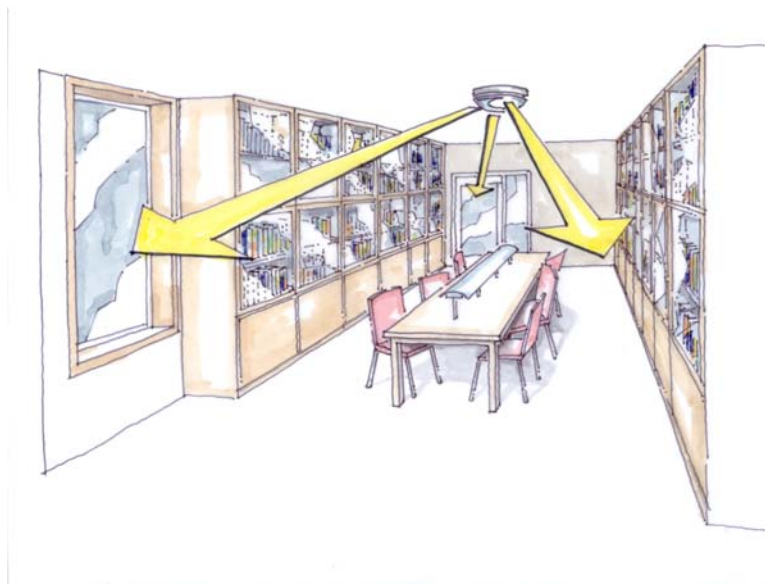


Figure 6. Motion detector should be positioned to have clear view of windows and doors as well as areas within the room.

common motion detectors are ultrasonic, microwave, photoelectric, and passive infrared detectors. Other forms of interior motion detection include floor mats, stress detectors, and magnetic contacts on interior doors.

Ultrasonic and Microwave Motion Detectors

Ultrasonic and microwave motion detectors work by transmitting an ultrasonic or microwave signal and receiving the reflected signal back. The reflected signal frequency is identical to the transmitted frequency if there is no movement. Movement will cause an increase or decrease in the frequency of the signal (known as the Doppler Effect), triggering an alarm. A microwave motion detector uses a higher frequency than ultrasonic, allowing it to detect motion through most interior walls.

Photoelectric Motion Detectors

Photoelectric motion detectors (also referred to as a photoelectric eye or PE) consist of two parts: a transmitter that emits a beam of light (invisible to the human eye) and a receiver that receives the beam of light. If the beam of light is interrupted or broken by motion, an alarm is triggered. PEs can be surface mounted or recessed and require a straight line-of-sight between the transmitter and the receiver.

Passive Infrared Motion Detectors

Passive infrared motion detectors (PIR) detect the heat energy given off by animal or human bodies. If movement of the energy source above a certain velocity is detected, an alarm is triggered. Because PIRs transmit no signal, they can be positioned and adjusted to cover tighter areas. To prevent false alarms caused by an animal, some units have a special lens that prevents the PIR from detecting motion close to the floor. Because they are passive and emit no signal or beam, PIRs generally provide the most economical form of motion detection.

Other Motion Detectors

Floor mats are thin pressure switches that can be placed under rugs, triggering an alarm if enough weight is applied to the mat. Stress detectors are mounted on the bottom of the floor joists, triggering an alarm when stress is created in the joists by movement on the floor. Magnetic detectors are placed on interior doors and trigger an alarm when the door is opened.

Sounders

Sirens alert security personnel and employees of an alarm or emergency condition if they are within the building during an alarm. Indoor sirens are also a deterrent to scare burglars away. Outdoor sirens are designed to call attention to the library during an alarm condition; they

may also have a strobe attached to attract attention visually. Exterior devices should be appropriately housed to provide weatherproofing as well as tamper and vandal resistance.

Notification

Finally, the burglary alarm system should notify the appropriate authorities. This notification may be to on-site security personnel who will provide investigation of the alarm condition and determine the severity of the situation. It may also notify a security dispatch company that will follow library guidelines for appropriate action based on the alarm received; that is, notify security personnel, police, or fire department.

4.1.2. Collection Security

There are many methods of ensuring that no materials leave the library without being checked out. These systems always contain a security device that is placed on the materials (including books, magazines, videocassettes, audiocassettes, CDs, and DVDs) as well as a detection device that is typically located at all library exits. The detection devices must be safe for magnetic media and usually have audible and/or visible alarms. If desired, the audible alarm can be a voice alarm.

There are two major methods currently used for detection: electromagnetic detection and radio frequency identification (RFID).

The demands on today's libraries are both changing and increasing, and circulation rates are rising at the same time that new services are being offered. These changes are placing new demands on staff time. Yet, the number of staff is not increasing, or is actually declining, because of budget constraints. As a result, libraries are looking to technological solutions to minimize the staff handling of library materials so that greater attention can be focused on the patron.

RFID solutions are being designed to improve library operational efficiency. This enhanced capability is provided by RFID tags which do not require line-of-sight to be read, so that books are actually handled less. The tag combines book identification and book security into one label, minimizing labeling time and cost. More than one book can be read at a time, speeding circulation. The tags can be placed on any type of media, including CDs, DVDs, and videocassettes. The RFID tags are read/write, providing flexibility in what is encoded. They can also be put into the patron cards, speeding up the process even more. Library staff can check out and check in several items simultaneously without having to locate and scan individual bar codes.

Patron self-checkout systems are also available to libraries that incorporate RFID technology. Patrons can process several items simultaneously and the security devices can be turned off in a matter of seconds. A portion of the RFID memory can be allocated for theft protection so that no other tag is required. Since the anti-theft device is in the label, the security gates do not need to be attached to a central system or interface with the library's central database.

RFID solutions can also speed up the return process. As library items pass over the RFID check-in antenna, they are automatically checked into the central library database. With the power of the RFID tag, regular inventories can become a reality. Shelf readers allow staff to read the RFID labels easily without having to remove books from the shelves. The shelf reader can also be used to search for a single or specified group of items and alarm the user when an item has been mis-shelved.

Some of these features are also available on an electromagnetic detection system when used in combination with a barcode. This type of system is limited, however, since the barcode must be visible to the detector to identify the material, and the electromagnetic device with a barcode system does not allow for any additional information to be stored in the tag if desired.

4.1.3. Access Control

Electronic access technology is the best system for controlling access to library buildings, facilities, and rooms. Authorized people are allowed to enter a controlled area by automatic unlocking of the door. Plastic access cards are inexpensive and software can be programmed to restrict access to certain areas while recording the time, date, and location of authorized and unauthorized access attempts.

For extra security, access control can be used in conjunction with video surveillance to control and monitor large facilities. Access cards can be integrated as photo ID cards for library employees and can be used as temporary “keys” for library clientele to have access to restricted areas. The access system also can be used for monitoring employee time and attendance, security patrols of the property, and can limit access to sensitive areas, information, or equipment. Electronic access control systems enhance safety and protect valuable library assets.

When combined with central monitoring, versatile design, and online report capabilities, the system can become a valuable management tool. Access control solutions range from simple authorized access systems to advanced closed-circuit monitoring and exception reports delivered through secure Internet connections.

The most popular type of card is the magnetic stripe card, which looks like a credit card and carries two or more tracks of information on the magnetic stripe. These can be used for access control and other services. The security level is low and the magnetic stripe cards are prone to corruption of the data if placed near a magnetic field. The cards can also have user identification photos and information printed on them.

The proximity card is more expensive but is also more durable and easier to use. For internal use, a close-range type is used; for car parking entrances, a longer range of up to one yard or so is possible. Proximity card readers can be hidden behind a wall surface for aesthetic purposes, with just a marker on the wall. Other available card readers include barcode readers and RFID readers. Entry keypads can also be included within an access control system for entry without a card, or in addition to the card. Biometrics entry systems are available including fingerprint recognition, palm recognition, and iris scanning systems for high security areas.

All types of readers are connected to a local controller which supervises a number of doors local to it. The controller contains a database of users and their rights of access at certain times. The information is downloaded from a central computer and if communication with the computer is lost, most controllers will continue to operate their local doors without any adverse effect. Controllers also provide the power supply for the locks or this may be local to each door.

4.1.4. Video Surveillance

Video surveillance and closed-circuit television (CCTV) systems serve as a way to monitor and record security, deter crime, and ensure safety. Advances in CCTV technology and reduction in costs have also made video surveillance a cost-effective management tool for library facilities.

Libraries can use CCTV to identify visitors and employees, monitor work areas, deter theft, and ensure the security of the premises and other facilities. The system can also be used to monitor and record evidence on clientele and employee misconduct.

CCTV systems are quickly becoming one of the most important and economical security and safety tools available to libraries.

The key steps when considering or designing a CCTV security system include:

- Determine the primary application of the CCTV system
- Define the layout and characteristics of the controlled area(s)
- Decide on camera type and features

- Determine the best location for viewing monitors
- Determine the best method of signal transmission
- Decide on the type of recording/archival equipment for the system

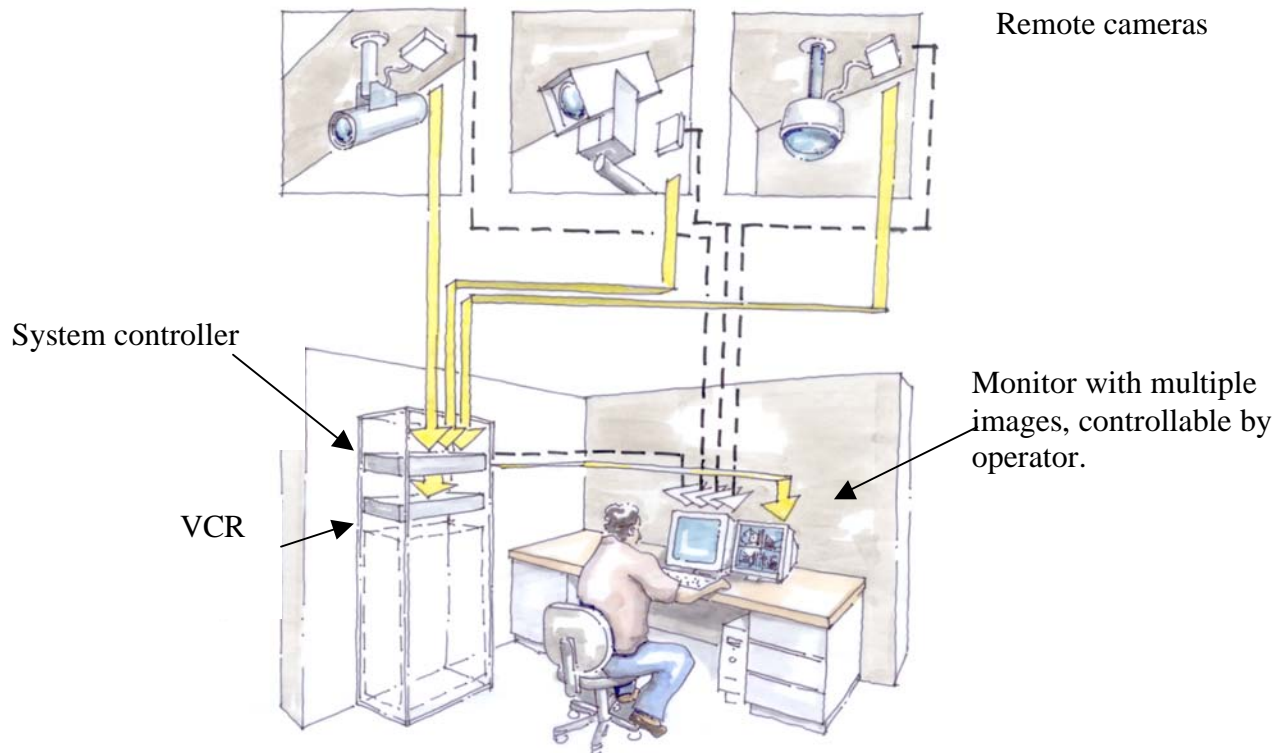


Figure 7. Diagram of components of typical library CCTV system.

When used for video surveillance and monitoring, the primary purposes of a CCTV system are detection, assessment, and identification. In all applications a CCTV system must provide the ability to visually observe, monitor, and record. Observation provides real-time information for detection and identification. Recording provides after-the-fact material for assessment, analysis, and review, usually with overlaid time, date, and location information.

Layout and Characteristics of the Controlled Areas

Before a CCTV system can be designed, specific information must be gathered regarding the layout of the controlled areas. This information will facilitate camera location and selection. Information must be assembled to determine the height or width, and direction of view for each camera location.

Issues to consider include whether a fixed-mount camera or a camera with pan/tilt/zoom capability is required, as well as the lighting characteristics of the controlled areas. To determine the best solution, consider the objects or area to be observed and the environment in which they exist. Different areas contain different colors, surfaces, and materials that reflect varying levels of light. To select proper equipment, it is necessary to determine the minimum lighting level (day and night) that will arrive from the area to the camera. The available light will affect picture clarity and focus. The better the light, the better the picture quality.

Camera Types and Features

Cameras are selected based on sensitivity, resolution, and features. A camera's sensitivity is the amount of light that is needed to produce a quality video image. A camera's resolution determines the quality of the video. Some cameras can be programmed to patrol an area or respond to movement. Factors such as distance from the scene, focal length, desired field of view, lighting, and format affect the size and clarity of the video.

Lenses play an important role in the design of a CCTV system. Some cameras have powerful zoom lenses which can be focused at far distances. Choose the proper lens for each camera by the format size of the camera, distance from the camera to the scene, and the required size of the viewing field for adequate identification. When both wide scenes and close-up views are needed from the same camera, a zoom lens is preferable.

Where the level of available light can change dramatically, a camera equipped with automatic iris control can help provide consistent video quality. Automatic iris control enables cameras to open or close the lens to adjust the amount of light passing through it. In bright light an auto iris camera will close the lens to prevent strong light from distorting the video. In low light, the camera will open the iris to allow a greater amount of light in and sharpen the video.

Cameras can be fixed or have pan, tilt, and zoom capability. Fixed cameras are mounted on a fixed bracket and cannot be automatically adjusted to different angles of the viewing area. Pan/tilt/zoom cameras are motor driven and can pan left and right, tilt up and down, and zoom in and out for close-up or wide-angle viewing.

Color cameras usually require a higher level of lighting than monochrome (gray tone) cameras. Color produces a more natural, richer image than monochrome and makes it easier to identify subjects. With a color system one could more easily distinguish a red from a green object, while on a monochrome system both objects would appear a similar shade of gray. However, monochrome cameras continue to offer some advantages. Monochrome cameras

are better suited for extremely low light situations. In any event, the ability to capture good quality video images in low light situations increases the cost of both monochrome and color cameras.

A camera's housing protects the camera and lens from the environment and potential vandalism. It can also enhance the appearance of the camera installation and conceal the equipment from observation. All outdoor cameras require a housing of some type. Protection from cold, heat, dust, and other elements is needed to ensure optimum performance and extend the life of the camera. Where aesthetics are a concern, dome cameras are a common choice. Dome cameras are covered by a dark colored Plexiglas housing that hides the camera and wires.

Viewing Monitors

The viewing monitor receives the video signal from the camera and displays it for viewing. A CCTV monitor provides higher lines of resolution than a TV and accepts only video signals. Lines of Resolution is the total number of horizontal lines the camera or monitor is able to reproduce. The more lines of resolution, the better or sharper the video picture will appear.

Several factors should be considered when selecting and placing a monitor: the size of the monitor, its positioning and viewing angle, monitor resolution, viewing station growth, and adequate ventilation. CCTV systems use both dedicated monitors and switchable monitors. A dedicated monitor displays the video from just one camera. A switchable monitor enables a viewer to switch between different cameras. A multiplexed monitor gives a viewer the ability to view the images from multiple cameras simultaneously.

Signal Transmission

Signal Transmission is the method by which the video signal gets from the camera to the monitor. Several video transmission technologies exist, each with its own advantages and disadvantages. It is not uncommon to find several video transmission technologies in use within the same CCTV system. The choice of signal transmission depends on factors such as distance, environment, cost, and area layout. Nearly all methods of transmission suffer from various forms of signal interference or loss. Good system design works to minimize signal interference and loss. Examples of video signal transmission include the following:

A twisted pair wire provides a physical connection or closed circuit between the camera and the monitor. A twisted pair of wires can transmit a video signal for distances up to one kilometer without a signal boost. An example of a twisted pair wire is a dedicated telephone

line that connects the camera with the monitor. Specialized equipment makes it possible to use public telephone lines for video signal transmission.

A coaxial cable provides a physical connection or closed circuit between the camera and the monitor. The cable is shielded to minimize interference from any other electronic devices or circuits. Copper braided coaxial cable is recommended to maximize conductivity and minimize potential interference. For traditional CCTV systems this is the most common method of signal transmission over relatively short distances.

A fiber optic cable provides a physical connection or closed circuit between the camera and the monitor. Fiber optic technology changes an electronic signal into pulsed laser light and transmits it through a fiber optic cable, changing the pulsed light back into an electronic signal capable of being displayed on a monitor. Fiber optic transmission is resistant to electrical or environmental interference. Fiber optic transmission is the most common method of signal transmission over extended distances.

Wireless signal transmission uses radio frequency to transmit video signals. It is cost effective and reliable for short distances with line-of-sight video transmission. It is practical where hardwiring methods are either impossible or cost prohibitive. However, wireless transmission is susceptible to adverse environmental conditions and other radio frequency signals in the area.

Microwave can be an efficient and cost-effective method of transmitting video signals. Microwave converts the video signal into high frequency radio signals that require no wire or cable, providing good quality transmission over a line-of-sight path. Though microwave technology requires line-of-sight transmission and is affected by environmental conditions, it offers a large bandwidth to carry video and is a practical option when a wire path between the camera and monitor locations cannot be established or is prohibitively expensive.

Recording Equipment

Recording equipment is used to record events for later review. Recordings make it possible to view events that may have gone unnoticed at the time they occurred or that may require closer scrutiny. It is possible to record all the cameras all of the time or some cameras some of the time. Multiplexers make it possible to record all cameras in the system onto a single videotape. Some multiplexers also have a motion detection feature that enables the system to record more video from cameras with motion than from those without motion.

Digital video recorders (DVRs) provide the ability to record perfect quality pictures and replay them at the touch of a button. Digital recording also makes it possible to record video on a computer disk. DVRs are able to record much more information in either real-time or time-lapse mode. Real-time mode produces higher quality recordings that approximate the ability of the human eye to easily distinguish moving images. Time-lapse mode records more video over longer periods of time on less videotape. Since the number of pictures recorded per second in time-lapse mode decreases significantly as the recording time increases, video movement may appear jerky. Alarm recording combines these two modes, recording in time-lapse mode until an event occurs (operator selected or alarm) that switches the recorder to real-time mode.

Additional features of a CCTV recording system include a video printer that can produce a hard copy printout of a video scene, a time and date generator that can annotate the video scene with chronological information, and a camera identifier to identify the selected camera.

5. SECURITY POLICIES, PROCEDURES, AND PLANS

All libraries should create and implement security policies, procedures, and plans. These should, at least, include entry and exit procedures, room registration procedures, personal belonging restrictions, special collections use policies, and entry key management procedures.

5.1.1. Entry and Exit Procedures

Libraries should determine the type of personal property visitors are allowed to bring into the library. Persons entering a library should do so with the understanding that all property in their possession can be inspected by the library security personnel upon entry and exit.

Normally, however, there is no comprehensive screening at library entries.

At the exit, all individuals must pass through a theft detection device, which will sound an alarm if a targeted collection item is carried through it. In special security library environments, all individuals should present for inspection any property in their possession at the exit.

5.1.2. Room Registration

If the library has public reading rooms, study rooms, computer catalog centers, or multimedia rooms, security procedures for utilizing the rooms should be defined. Requirements for

proper identification may be required before using these types of spaces, and should be defined within the library policies and procedures. Particular requirements for different types of rooms should also be defined.

5.1.3. Special Collections

The Association of College and Research Libraries (ACRL) Rare Books and Manuscripts Section (RBMS) has published a set of excellent guidelines for dealing with special and rare collections. These guidelines identify important items that collection administrators should address in developing adequate collection security. While directed primarily toward rare books, special collections, and manuscripts, the topics are also applicable to general collections. The RBMS Security Committee also recommends the unique identification marking of materials and the appointment of a Library Security Officer.

The guidelines include the following:

- The special collections building or area should have a single entry and exit point for both researchers and staff.
- Fire and emergency exits, which should be strictly controlled and provided with alarm coverage, should not be used for regular access.
- Within the facility itself, the public should have access only to public areas, not to work areas or stack space.
- Researchers should be received in a separate reception area where a coat room and lockers should be provided for researchers' personal belongings and outer wear.
- A secure reading room where researchers can be continuously monitored at all times by staff trained in surveillance should be identified as the only area in which material may be used.
- A security guard should check researchers' research materials prior to their entering the secure area as well as when they depart.

Keys and their equivalents, such as keycards, are especially vulnerable items. A controlled check-out system for all keys should therefore be maintained. Keys to secure areas should be issued to staff only on an as-needed basis, and master keys should be secured against unauthorized access. Combinations to vaults also should have limited distribution and should be changed each time there is a staff change involving a position with access to the vault. Strong consideration should be given to installing proprietary keyways in locks in the special collections area.

5.1.4. Entry Key Management

The library should have a policy pertaining to the custody and control of keys and access cards to all doors within the facility. Procedures and policies should be defined and should include:

- Process for issuing keys and access cards.
- Identification of various areas which are included within the access and who should have access to each type of area.
- Required refundable or non-refundable deposit for keys and access cards.
- Nature and type of appropriate forms.
- Determination of the quantity of keys allowed per person.
- Assignment of who can authorize the release of keys and access cards.
- Nature of the policy to grant visitors or contractors keys and access cards.
- Statement of the master key policy.
- Nature of the change of access or door hardware procedure.
- Prescription of penalty for any breach of key management policies.

6. GLOSSARY OF TERMS

<i>Alarm Monitoring Facility</i>	Central station where security, fire, or other emergency alarms are monitored and persons are dispatched to investigate the alarm.
<i>Assets</i>	Refers to what the library has or owns and considers valuable, including human life, collections, structures, properties, even the good name and operations of the library.
<i>Perimeter Security</i>	Protection concept of designing a three-dimensional ring around objects of value, often one inside another, such as a property line perimeter, building shell perimeter, non-public area perimeter, and high value area perimeter.
<i>Secured Area</i>	An area whose perimeter security has been reviewed and usually reinforced, with entries and exits locked or under observation, and generally alarmed when not occupied.
<i>Security Manager</i>	Library/archives staff person who is responsible for library security and protection issues.
<i>Security Personnel</i>	Staff who are dedicated to performing security duties most of their working time, usually staff of a security office or security department.

7. REFERENCES AND ORGANIZATIONS/WEBSITES

ASIS International, www.asisonline.org

Association of College and Research Libraries, www.ala.org/ACRLTemplate.cfm

International CPTED Association, www.cpted.net

Library Administration and Management Association, www.ala.org

National Burglar and Fire Alarm Association, www.alarm.org

National Crime Prevention Council, www.ncpc.org

National Crime Prevention Institute, www.louisville.edu/a-s/ja/ncpi/

7.1.1. References

ASIS International 2002 The General Security Risk Assessment Guideline, Alexandria, VA.

Crowe, Timothy D. (2000) Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts, Second Edition, Butterworth: Stoneham, MA and National Crime Prevention Institute.

The Facilities Standards for the Public Buildings Service, P100-2003 (March 2003), General Services Administration (GSA).

Garcia, Mary Lynn (2001) The Design and Evaluation of Physical Protection Systems, Butterworth: Stoneham, MA.

Guidelines for the Security of Rare Books, Manuscripts, and Other Special Collections (Final version approved July 1999), Prepared by the ACRL Rare Books and Manuscripts Section's Security Committee.

CONTRIBUTORS

Mark McComb, Security Consultant
RLS Inc., San Francisco, CA
mmccomb@rls.com

Edward Dean, AIA
edward.dean@sbcglobal.net

About the Author:

Mark McComb is a Principal of RLS, San Francisco. He has been the Sr. Technology Consultant on many corporate and academic projects including the Telecommunications Infrastructure Upgrade at University of San Francisco, Helen Wills Neuroscience Institute at UC, Berkeley, Microsoft Silicon Valley Campus, Campbell Union H.S. District, and the San Francisco State University / Sutro Library. A graduate from Cal Poly, SLO, Mr. McComb holds a Bachelor of Science degree in Electrical Engineering with additional study in Computer Science and a Minor in Music. He is a Registered Communications Distribution Designer (RCDD) and a member of ASIS International (formerly the American Society of Industrial Security) and IEEE (Institute of Electrical and Electronics Engineers). For more information, please visit RLS on the Internet at www.rls.com.