www.bcsreports.com

BCS Reports
BUSINESS COMMUNICATION SERVICES

NFPA 731 with Applications to Residential Security Systems

By
Les Baxter, P.E.
BAXTER ENTERPRISES

In 2005, the National Fire Protection Association (NFPA) approved two documents relating to premises security systems: NFPA 730 (Guide for Premises Security) and NFPA 731 (Standard for the Installation of Electronic Premises Security Systems). On Dec. 31, 2007, the 2008 editions of both documents became effective.

This report summarizes the recommendations of those two documents with emphasis on residential systems. Since NFPA 731 specifically excludes single-family dwellings from its scope, Section 4 of this report makes recommendations as to what subset of the requirements of NFPA 731 might be usefully applied to one- and two-family dwellings.

You will be provided with the requirements for "the application, location, installation, performance, testing, and maintenance of electronic premises security systems (EPSS) and their components" for the following seven types of systems:

1. Intrusion detection systems
2. Access control systems
3. Video surveillance systems
4. Asset protection systems
5. Environmental detection systems
6. Holdup and duress systems
7. Integrated systems

Save time and money by putting this report (NFPA 731 with Applications to Residential Security Systems) to work for you.

Published by

BCS
BUSINESS COMMUNICATION SERVICES

Tel: 800-492-8422 • 209-295-3975 • Fax: 209-295-3974

E-Mail: randm@volcano.net • Address: 505-1 So. State Hwy. 49, #242 • Jackson, CA 95642

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

NFPA 731 with Applications to Residential Security Systems

TABLE OF CONTENTS

Page #

FIGURES

TABLES

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

NFPA 731 with Applications to Residential Security Systems

1 Introduction

In 2005, the National Fire Protection Association approved two documents relating to premises security systems:

- NFPA 730 – Guide for Premises Security
- NFPA 731 -- Standard for the Installation of Electronic Premises Security Systems

On December 31, 2007, the 2008 editions of both of these documents became effective.

Sections 2 and 3 of this report provide summaries of NFPA 730 and 731, respectively. The purpose of these summaries is to give a high-level description of the content of these documents and to discuss some of the most important material. This report does not attempt to provide a complete listing of the requirements of these documents.

NFPA 730 covers many types of buildings and facilities. Section 2 gives a brief overview of NFPA 730. A more complete summary is provided in the Annex. In this report, while we will briefly mention non-residential facilities, we will concentrate on the material which is relevant to residential buildings – both single-family dwellings (SDUs) and multi-dwelling units (MDUs).

NFPA 731, which covers installation of electronic security systems, specifically excludes one- and two-family dwellings. Section 3 summarizes the content of NFPA 731. Section 4 of this report makes recommendations as to what subset of the requirements of NFPA 731 might be usefully applied to one- and two-family dwellings.

2 Overview of NFPA 730 – Guide for Premises Security

NFPA 730, as the name implies, provides a guide for selection of a security system in both new and existing buildings. It provides a wealth of information, definitions, and suggestions for implementing security systems. However, it is not a standard and does not provide requirements which can be tested for compliance (such as, the security system shall provide …).

NFPA 730 defines 11 types of buildings plus a twelfth classification for special events. These classifications, and the primary security considerations for each, are summarized in Table 1.

In this report, we will be mainly concerned with residential buildings. Refer to the Annex for a more complete summary of NFPA 730[1].

[1] There were few changes in the 2008 edition of NFPA 730 that affect this document. Most of the 2008 changes were in the Industrial Facilities chapter.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

Category	Type	Primary Security Considerations
Housing	One- and two-family dwellings (SDUs)	Basic precautions Physical security Outdoor lighting Selecting a security provider
	Apartment buildings (MDUs)	Similar to SDUs plus: Security for public/common areas (elevators, etc.) Key management Tenant ID and background check Employment practices
	Lodging	Front desk security Lock and key control Guest room security Access control in non-public areas
Education & Health Care	Educational	Student safety Theft and vandalism prevention
	Health care	Patient and staff safety Visitor control Theft and burglary prevention Employment practices
Retail	Restaurants	Robbery prevention Employee training Burglary prevention
	Shopping centers	Security personnel and law enforcement liaison Emergency procedures Proper lighting
	Retail establishments	Prevention of employee theft Prevention of robbery, burglary, and shoplifting Prevention of workplace violence
Commercial & Industrial	Office buildings	Access control Lock and key control
	Industrial facilities	Prevention of terrorism and sabotage Security of chemicals and hazardous materials Intrusion control Employment practices
	Parking facilities	Lighting Access control
Misc.	Special events	Access control Parking and traffic control Disturbance/incident handling

Table 1. Major NFPA 730 security considerations for each type of facility

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

3 Overview of NFPA 731 -- Standard for the Installation of Electronic Premises Security Systems

3.1 Introduction

Although the title of NFPA 731 emphasizes the installation of electronic premises security systems (EPSS's), it covers much more than just installation. NFPA 731 provides requirements for "the application, location, installation, performance, testing, and maintenance of electronic premises security systems and their components." EPSS's as defined in this document include the following types of systems:

- Intrusion detection systems
- Access control systems
- Video surveillance systems
- Asset protection systems
- Environmental detection systems
- Holdup and duress systems
- Integrated systems

Note that fire alarm systems, which are covered by their own standards, are not covered by NFPA 731. It is required that when an EPSS connects to a fire alarm or other life safety system, the codes and standards applying to that system must also be followed.

This standard covers a very broad area. It is intended to apply to new installations of electronic premises security systems or their components installed for protection of building interiors, building perimeters, and surrounding property. It also applies to non-electronic building and physical security systems when they interface with, or become part of, an electronic premises security system.

There are also a number of areas excluded from coverage by NFPA 731. These include:

- Information technology systems – including data security, software, and computer systems. In other words, it does not address firewalls, anti-hacking provisions, data backups, etc.
- Removal of portable assets
- Finally, NFPA 731 does not apply to EPSS's that are installed in one- and two-family dwellings. We will address this issue in section 4 of this report.

3.2 Fundamentals

3.2.1 General Principles

Chapter 4 of NFPA 731 outlines a number of fundamental principles that apply to all the types of systems and equipment covered by the standard. First and foremost among these principles is the following: ***All equipment shall be listed for the purpose for which it is used in accordance with applicable standards.*** This means that, for example, if a contact is being used in a burglar alarm, it must be listed for use with burglar alarms, not just be compliant with the NEC.

The fundamental requirements that NFPA 731 places on all systems and equipment include:

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

- Comply with all relevant codes and standards (such as NFPA 70, UL 294, etc.)
- Follow requirements of the authority having jurisdiction (AHJ).
- Be listed for the purpose for which they are installed (as discussed above).
- Be installed according to the manufacturer's instructions.
- Be designed and installed by qualified personnel, including, but not limited to:
  - Trained and certified by the equipment manufacturer.
  - Licensed or certified by a federal, state, or local authority
  - Certified by an accreditation program acceptable to the AHJ

3.2.2 Power Supplies

The power supply is a critical element in the reliability of any electronic system. For EPSS's, there are two elements to the power supply – the power source at the common equipment, and the wiring that remotely delivers power to the sensors and actuators. NFPA 731 places a number or requirements on both the power supply and the wiring.

For intrusion detection and holdup, duress and ambush systems, NFPA 731 specifies that they must be powered by at least two independent power supplies. The secondary power supply must automatically take over without loss of signals or causing transmission of an alarm if the primary supply is unable to supply adequate power. The secondary supply must be able to operate the system under maximum quiescent load for at least 4 hours[2]. The secondary supply must consist of one of the following:

- A storage battery dedicated to the security system.
- A dedicated branch circuit of an automatic-starting generator and storage batteries dedicated to the security system with at least 15 minutes of capacity under maximum alarm load.
- An emergency generating system as defined in NFPA 70, Article 700.

To ensure the reliability of battery-backup systems, requirements for battery, location, charging, over-current protection, and replacement intervals are specified. It is also required that automatic operation of the backup power system be accomplished without interfering with other systems (such as fire alarms, lighting control, elevators, etc.)

3.2.3 Wiring

To ensure the reliability and proper functioning of EPSS wiring, Section 4.5.8 of NFPA 731 gives detailed requirements for copper and fiber wiring. It specifies that all wiring must meet both the requirements of NFPA 70 and the specifications of the equipment manufacturer. All grounding must be in accordance with NFPA 70.

[2] The 2006 edition specified that the switchover to secondary power must take place within 10 seconds and that the secondary supply must operate for a minimum of 2 hours.

Detailed wiring requirements are given, including the following, some of which are illustrated in Figure 1.

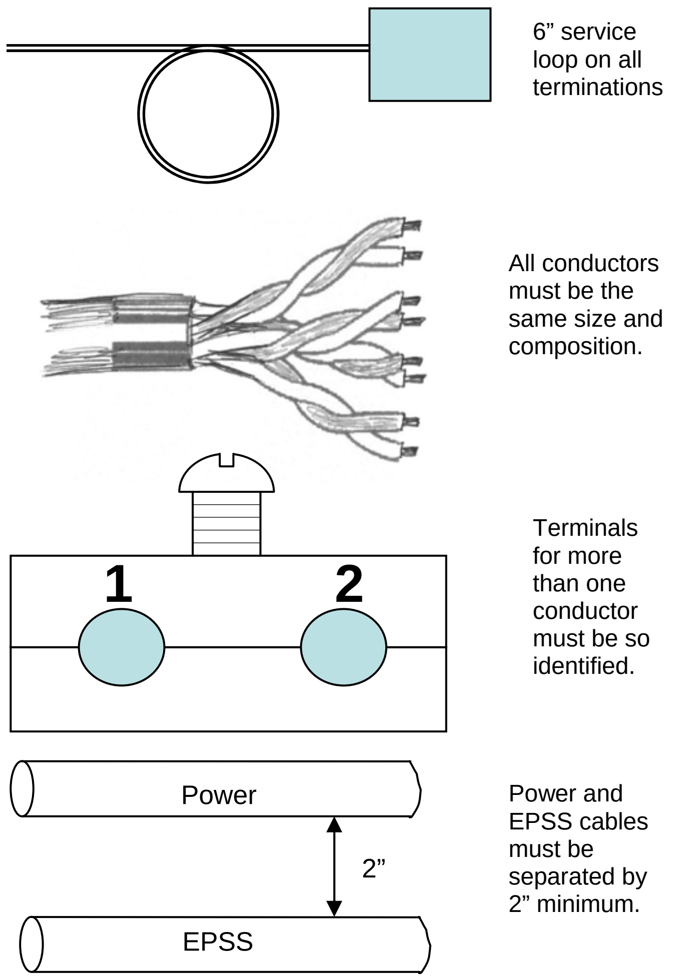
6" service loop on all terminations
All conductors must be the same size and composition.
1
2
Terminals for more than one conductor must be so identified.
Power
2"
EPSS
Power and EPSS cables must be separated by 2" minimum.

Figure 1. NFPA 731 wiring requirements

- The size, construction, and electrical properties of EPSS wiring shall be as specified by the equipment manufacturer.
- Wire termination by means of pressure connectors, screw terminals, or splices to flexible leads.
- All conductors in a cable must be of the same size and composition.
- Provisioning of service loops. A 6 inch (minimum) service loop is required at all copper wiring terminations. For fiber terminations, the service look must be at least 10x the cable diameter, or as specified by the manufacturer.
- Circuit identification is required at all field terminations and within control panels and enclosures. Terminals intended for more than one conductor must be so identified.
- Low voltage EPSS wiring must be separated from power cables by at least 2 inches unless the manufacturer specifically allows for smaller separation.
- Wires and cables must not be placed so that they prevent access to equipment.

Requirements are also given for low-powered wireless systems, including power supplies, alarm signals, monitoring for integrity, and output signals. These monitoring requirements specifically do not apply to EPSS's in dwelling units.

3.2.4 Software and System Requirements

Virtually all modern EPSS's are software controlled. While maintaining the security of the system software is not a primary focus of NFPA 731, it does require that all software provided for use with an electronic premises security system shall be listed for use with the system. Furthermore, a record of installed software version numbers must be maintained and the software must be protected from unauthorized changes.

NFPA 731 specifies a number of environmental, mounting, and location requirements for security system equipment. An EPSS may consist of either integrated systems combining detection, notification and auxiliary functions into a single system or a combination of subsystems.

When multiple control units are interconnected, they must meet all the requirements for monitoring, powering, etc. as specified in this standard.

Systems other than the EPSS may be permitted to share components, equipment, wiring, etc. with the EPSS as long as their operation, maintenance, failure, or removal does not impair the function of the EPSS.

3.2.5 Documentation

It is noted that the AHJ may require the installing contractor to provide a written statement that the system has been installed and tested in accordance with the manufacturer's specifications and the appropriate NFPA requirements.

NFPA 731 specifies what types of documentation must be delivered to the owner of the system upon final acceptance and requirements for training of the system users. Required documentation includes:

- Owner's manuals
- User's instructions
- Record of completion by the system installer
- Contact information for the organizations that maintain and monitor the EPSS

3.3 Intrusion Detection Systems

Chapter 5 of NFPA 731 covers intrusion detection systems, which typically include window and door contacts, glass-break detectors, and motion detectors. A typical intrusion detection system is illustrated in Figure 2.

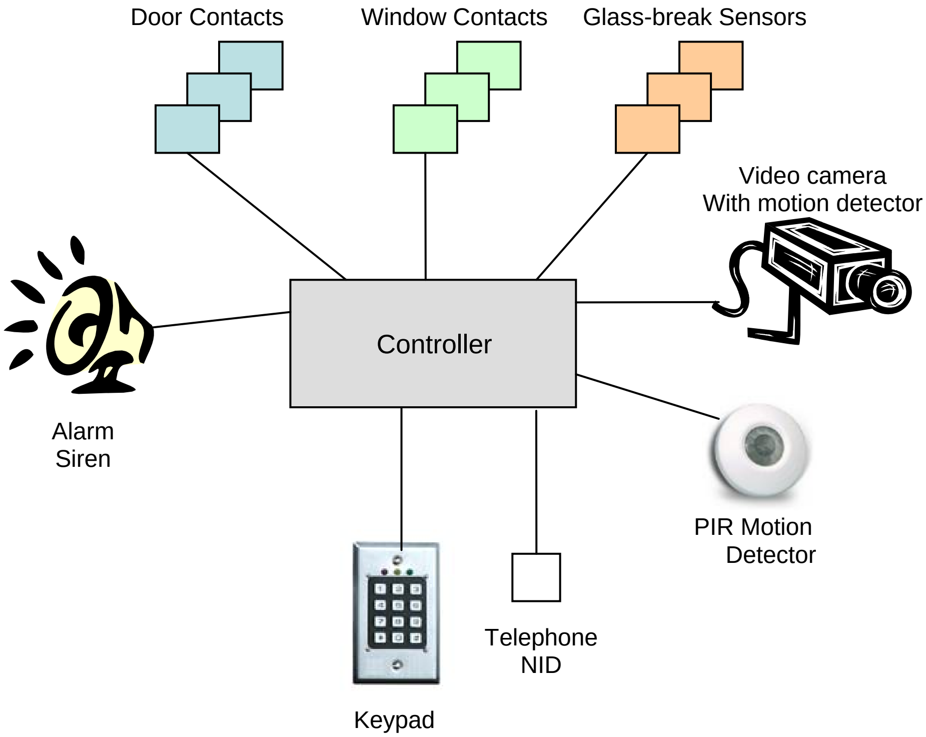

Figure 2. Intrusion detection system

There are a number of general requirements on these systems, including:

- All wiring and interconnections between control units, keypads, power supplies, initiating devices, etc. must be monitored for the integrity of the connection so that a single open or ground-fault can be detected within 200 seconds. Wiring faults must be indicated at the control unit.
- Doors may be provided with an entry/exit delay circuit which gives the user a chance to disarm the intrusion system after entering the premises. The maximum delay time may not exceed 240 seconds.
- Devices shall be installed as per manufacturer's instructions. The coverage and spacing of devices shall be based upon the intended threat.
- Signals from an intrusion detection system must be either sent to a monitoring station and/or activate an alarm at the protected premises.
- Photo electric cells (PEC), motion detectors including passive infrared (PIR), exterior structural detectors, and exterior buried detectors shall meet applicable UL specifications.

NFPA 731 discusses both interior and exterior intrusion detection systems. Types of exterior structural detectors include:

- Audio
- Contacts
- Fiber optic
- Protective cabling
- Proximity
- Shock sensors
- Stress sensors

Exterior buried detectors must be listed in accordance with UL 639 and include the following types:

- Electromagnetic
- Fiber optic
- Leaky coaxial
- Seismic

Interior detection devices shall be installed in accordance with UL 681 and when activated shall annunciate at the protected property and transmit an alarm signal. Interior detection sensors shall be listed as per the appropriate UL specification. Types of interior detection devices used to protect doors and windows include[3]:

- Contacts
- Protective wiring (which includes grooved striping, lacing, open wiring, and screens)
- Traps (devices that are intended to secure a conductor that is used to protect an air conditioner or similar opening so that the circuit is interrupted if the conductor is removed or cut.)
- Shock/vibration sensors

[3] Note – the 2006 edition also included Foil (also known as tape -- a thin metallic strip generally from 1/8 to 1 inch wide which is used around the perimeters of windows. If the glass is broken, the foil breaks and opens an electrical circuit causing an alarm condition) as an interior protection device. Foil has been removed from the 2008 edition.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

- Glass break sensors
- Sound detectors
- Photo electric cell (PEC)
- Motion detectors (including microwave, PIR, and video (VMD))

Interior detection devices may also be applied to walls. Detectors for wall application include:

- Protective wiring
- Shock//Vibration sensors
- Sound detectors
- PEC
- Motion detectors (including microwave, PIR, and VMD)

In addition to sensors on the perimeter as described above, interior space may be protected by pressure-sensitive devices (floor mats, stair treads, and stress sensors), PECs, and motion detectors (including microwave, PIR, and VMD).

Safes and vaults (including ATMs and secure containers) can be protected by a variety of sensors, including:

- Contacts
- Embedded cable
- Foil lining
- Heat detection
- Shock
- Smoke detection
- Sound
- Capacitance

Table 2 lists the UL specifications that these sensors must meet for each area of application.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

Interior Protective device	Window & Door	Walls	Interior Space	Vaults	Safes & ATMs
Contacts	UL 634			UL 634, UL 639	UL 634, UL 639
Protective wiring	UL 606, UL 634	UL 639			
Traps	UL 634				
Shock/vibration sensors	UL 639	UL 639		UL 634, UL 639	UL 634, UL 639
Glass break sensors	UL 639				
Sound detectors	UL 639			UL 634, UL 639	
Photo electric cell (PEC)	UL 639	UL 639	UL 639		
Motion detectors	UL 639	UL 639	UL 639		
Pressure-sensitive devices			UL 634		
Embedded cable					
Heat detection				UL 634, UL 639	
Smoke detection				UL 634, UL 639	
Capacitance					UL 634, UL 639
Embedded cable				UL 634, UL 639	
Foil lining				UL 634, UL 639	UL 634, UL 639

Table 2. Protective Devices and Relevant UL Specifications[4]

3.4 Electronic Access Control Systems

Chapter 6 of NFPA 731 covers electronic access control systems. The overarching requirement is that all access control equipment be in compliance with UL 294, *Standard for Access Control System Units.* In addition to the controller, the major component of access control systems are portals, readers, and locking systems, as illustrated in Figure 3. Access control portals include doors, gates, turnstiles, etc.

[4] See the References section (Section 5) for more details about the UL specifications

A reader is a device that allows an identification credential to be entered into an access control system. When readers are installed on doors, they must be on the latch side. The maximum interval between recognition of valid credentials and unlocking must not exceed 10 seconds.

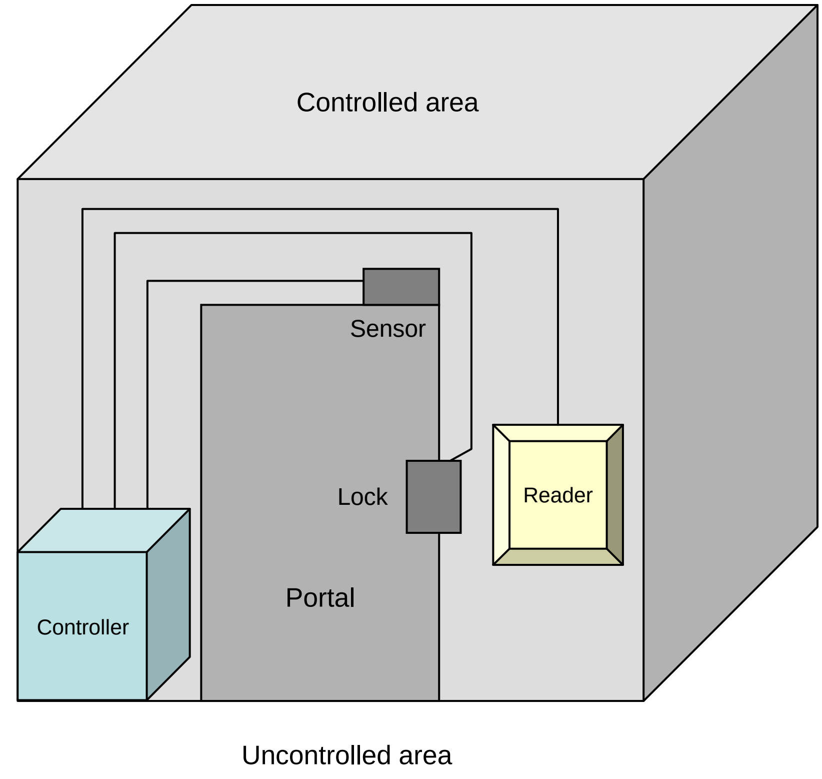

Figure 3. Access control system

NFPA 731 places a number of requirements on locking systems, including:

- Electric locking systems must be used to control portals.
- Portals must automatically close and lock when supervised by the access control system.
- When an exit door has an active lock, a manual means to override the lock must be provided unless specifically not required by the AHJ (in a prison, for example).
- A position sensor which monitors whether the door is open is required on all controlled doors.

There are two methods of authorized egress – free and controlled. Free egress requires the use of a request-to-exit (RTE) device. The RTE device may be either manual or automatic (e.g., a motion detector) and must open the lock on loss of power. Controlled egress requires the user to present credentials to a reader. The system may switch between free and controlled egress on a time-of-day basis.

Controllers and power supplies must be installed in a location that protects them from damage, tampering, and unauthorized access. Figure 3, for example, shows the controller inside the protected area.

Configuration of the system operating parameters must be protected from authorized changes and subject to the approval of the AHJ. If the system includes a NID, the level of encryption must comply with AHJ requirements.

3.5 *Video Surveillance Systems*

Video surveillance systems are an important component of EPSS's. Chapter 7 of NFPA 731 covers the installation of CCTV and analog video systems as well as and digital imaging systems (DIS).

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

Video security systems must be designed to provide visual identification of a person, object, or scene as required by the AHJ. Video equipment must be compliant with applicable standards and installed according to the manufacturer's instructions.

3.5.1 Video environmental requirements

Cameras must be installed so that the image cannot be impaired by vandalism and so that their operation is not adversely affected by environmental conditions such as:

- Rain and fog
- Snow and ice
- Sunlight angles
- Temperature extremes
- Wind loading
- Vegetation (for example, weeds, tree limbs, etc.)
- Animals/insects (for example, bird's nest, spider web, etc.)
- Dust or smoke

Cameras must not have strong backlighting (such as the rising or setting sun, street lights, etc.) behind the main subject.

Camera enclosures, anchoring, and mounting hardware shall be rated for the conditions in which they are used (weight, wind, mounting surface, etc.)

3.5.2 Video cabling requirements

Video cabling has an important effect on both the quality and reliability of video transmission. In addition to transmitting a video signal, the cabling must support control signals and power also. Coaxial cable has historically been the most commonly used video cable, although fiber and UTP may also be used as specified by the manufacturer. UTP usually supports video, control, and power over the same cable, while a separate power and control cable is often needed with coaxial cabling or fiber, as illustrated in Figure 4. Power cabling must comply with NFPA 70.

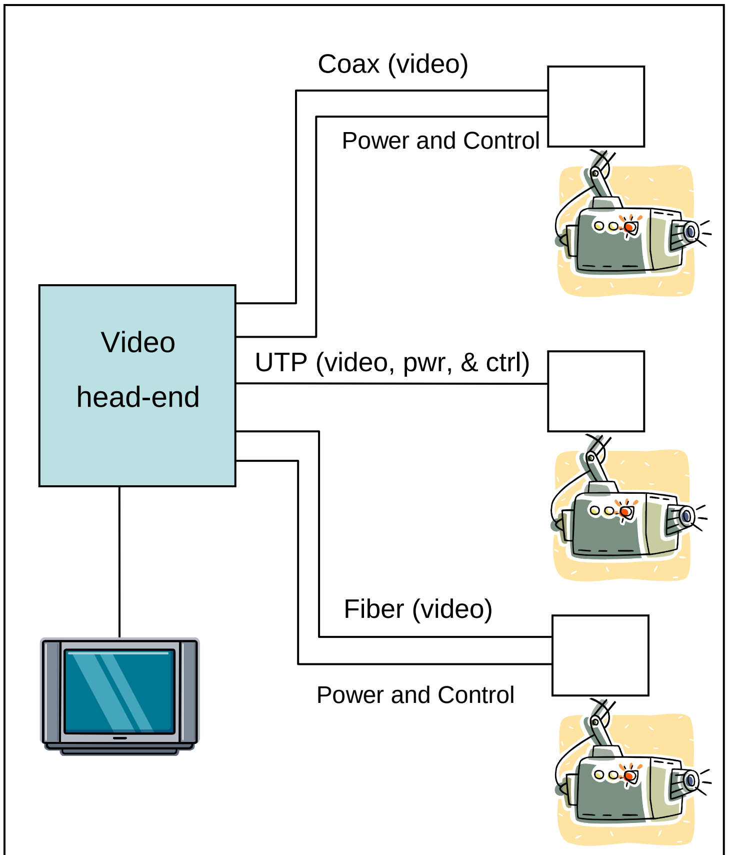

Figure 4. Video cabling configurations

The 2008 edition of NFPA 731 (unlike the 2006 edition) does not provide any specific requirements or guidelines for video cable. Video cable must not exceed the maximum

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

distances specified by the manufacturer.

3.5.3 Video cameras

NFPA 731 contains a couple of informative annexes which are not part of the requirements of the standard but give useful information about camera specifications and selection criteria.

The camera specification material includes equations and tables for calculating the focal length need to insure a required field of view

The annex on camera selection criteria includes information about light level and sensitivity, resolution, back-focus adjustment, format, and sync and phase.

The discussion of light level and sensitivity includes material about:

- Light levels (from quarter moon @ 0.01 lux to full daylight @ 10,000 lux)
- Reflectance
- Lens speed (F stop)
- Usable video
- Automatic gain control (AGC)
- Shutter speed

3.6 Holdup, Duress, and Ambush Systems

Chapter 8 of NFPA 732 gives requirements for holdup, duress, and ambush alarms which are special-purpose alarms that are typically triggered manually by employees when they encounter a hostile situation. There are slight differences between the types of alarms, as noted in section 2.2.3 of this report. These alarms must be in compliance with applicable standards, such as UL 636.

The interconnecting wiring between initiating, annunciating, and control devices must be supervised to that a single open or ground-fault condition will be indicated within 200 seconds.

Initiating devices shall be located so that they are not subject to unintentional operation either by employees, janitors, etc. or by vibration, falling objects, and similar causes.

Initiation of holdup, private duress, or ambush alarms should not be obvious to an attacking or hostile party. Public duress alarm devices may be initiated by the public.

Operation of a holdup or ambush alarm will result in the transmission of a signal to a monitoring station, but shall NOT result in an audible or visual signal that can be observed by an attacking or hostile party.

Operation of a duress alarm will result in an audible or visible signal either at the location of the initiating device or somewhere else on the protected property.

Staff that may be expected to use a holdup, duress, or ambush alarm must be trained in the operation of the alarms and proper emergency procedures.

3.7 Monitoring Stations

This is a new chapter which was added in the 2008 edition. A monitoring station is defined as: A facility that receives signals from electronic premises security systems and has personnel in attendance at all times to respond to these signals.

There are three types of monitoring station defined:

- Proprietary Monitoring Station – owned by the same entity as the property being monitored.
- Commercial Monitoring Station – privately owned by a different entity than the property being monitored.
- Public Safety Monitoring Station – owned by a government body which monitors nongovernmental properties.

This chapter has sections on many aspects of monitoring stations, including: building construction; security; fire protection; access control; standby power; personnel; record keeping, etc. There are also sections on alarm receiving and signal processing equipment and transmission and receiving technologies to assure communications integrity.

3.8 Testing and Inspections

Chapter 10 of NFPA 731 covers requirements for inspection, testing, and maintenance (IT&M) of EPSS's. The owner is responsible for IT&M, however it may be performed by a third party if conducted under a written contract.

Acceptance testing must be done after the system in initially installed. Reacceptance testing must be performed after any of the following:

- Addition or deletion of system components.
- Modifications, adjustments, or repairs to system hardware or wiring.
- Changes to site-specific software.
- Modifications to the structure being protected.

Section 10.4.3 of NFPA 731 contains a 4-page table specifying test methods for each type of device in the system (e.g., lead-acid batteries, fiber optic cable, PIR detectors, etc.) As an example, Table 3 indicates the test methods for metallic conductors. While this seems like a lot of testing for each conductor, except for the supervision test, it is really just a long-winded explanation of the wire map test which is routinely done for UTP installations.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

Parameter	Test
Stray voltage	Measure with a voltmeter – no stray voltages greater than 1 volt ac or dc between conductors to ground or between conductors -- or as per manufacturer's specifications
Ground faults	Test all conductors that are not intentionally grounded for isolation from ground.
Short-circuit faults	Test all conductors that are not intentionally connected together for shorts.
Loop resistance	Measure the loop resistance of each conductor pair and verify that it does not exceed the manufacturer's specifications.
Supervision	Open one connection on at least 10% of the devices and verify that a trouble indication is displayed at the control unit.

Table 3. NFPA 731 test methods for metallic conductors

NFPA 731 also recommends the frequency with which testing should be done, as summarized in Table 4. Almost all components must be tested annually, in contrast with the 2006 edition, where about half of the components were required to be tested either quarterly or semi-annually[5].

In the event that any defects are found during testing or reported during operation, NFPA 731 requires that repairs must begin within 24 hours of the failure indication and that a record of the repair me maintained by the system owner for one year.

Frequency of Test	Intrusion Detection	Holdup, Duress, and Ambush Alarm	Access Control	Video Surveillance	General
Annually	• System • Interior detectors • Exterior detectors	• System • Interior fixed devices • Portable devices • External fixed devices	• System • Readers • RTE devices • Position switches • Electric hardware	• System • Camera enclosures • Recorders	• Batteries • Interface equipment • Sounding devices
Quarterly or by automatic monthly test					• Off-premises transmission equipment

Table 4. NFPA 731 test frequency

[5] Note – the test frequencies have also been changed from a requirement in Chapter 9 of the 2006 edition to a recommendation in Annex A of the 2008 edition.

3.8.1 Inspection and Report Forms

Annex A of NFPA 731 includes several sample test report forms which can be used to document the results of the required inspections and tests. The following forms are included:

- Report of Completion Inspection & Testing Report (1 page)
- Intrusion Detection or Holdup and Duress Systems Inspection & Testing Report (3 pages)
- Access Control Inspection & Testing Report (3 pages)
- Video Surveillance Inspection & Testing Report (2 pages)
- Additional Devices Inspection & Testing Report (1 page)

Each of these forms contains lists of the systems and equipment (controllers, sensors, actuators, etc.) that were tested along with checkboxes for both visual inspection and functional tests. They conclude with a section that lists all the items that did not operate properly and a signature block with spaces for the signatures of both the inspector and owner or responsible party.

3.9 Issues with NFPA 731

NFPA 731 was not initially met with universal acceptance. The National Burglar and Fire Alarm Association (NBFAA) maintained that most equipment manufactured at that time did not meet NFPA 731 and that equipment that does comply will be significantly more expensive. Their position paper on NFPA 731 (issued on May 6, 2005) lists several issues that will cause NFPA 731-compliant security systems to be more expensive, including:

- Most low-cost security equipment is not UL listed. The testing required for the listing process is expensive and time consuming.
- The document does not offer any variances for small or elective installations.
- The maintenance and testing schedule is costly to implement.

Despite the objections of the NBFAA, NFPA 731 was approved on July 29, 2005. However, the NFPA agreed to revise the standard within 2 ½ years to address the NBFAA's concerns. The 2008 edition of NFPA became effective on Dec. 31, 2007 and supercedes the 2006 edition. It contains a number of changes to alleviate the above objections, including the following:

- In a number of cases, the requirements of NFPA 731 have changed from "must be listed according to UL xxx" to "must be compliant with UL xxx."
- The test frequencies (see Table 4) have changed from requirements to recommendations and almost all have been made annual tests rather than quarterly or semi-annually.
- References to a number of UL specifications have been eliminated, including UL 681, Standard for Installation and Classification of Burglar and Holdup Alarm Systems.

This report is based on the 2008 editions of NFPA 730 and 731.

4 Application of NFPA 730 and 731 to SDUs

Having surveyed the contents of both NFPA 730 and 731, we will now look at how to apply these documents to security systems in single- and two-family dwellings.

4.1 NFPA 730 in the Residence

NFPA 730 contains a lot of useful information about residential security systems[6]. The following chapters are particularly relevant:

- Clause 4 – General
- Clause 6 – External Security Devices and Systems
- Clause 7 – Physical Security Devices
- Clause 8 – Interior Security Systems
- Clause 13 – One- and Two-Family Dwellings. The list of "Basic and Environmental Precautions" in clause 13.4.1 is very useful.

4.2 Residential Application of NFPA 731

NFPA 731 specifically excludes single- and two-family dwellings from its scope. Clearly, many of the requirements of the standard are overkill for an SDU. However, let's look through the major sections of the standard and see which might reasonably be applied in an SDU environment.

4.2.1 Fundamental Principles

In section 3.2.1, we listed five fundamental principles that NFPA 731 applies to all types of equipment and systems. Table 5 summarizes their applicability in a residential situation.

NFPA 731 Fundamental Principles	Applicable to SDUs?
Comply with all relevant codes and standards (such as NFPA 70)	Yes.
Follow requirements of the AHJ.	Yes – this is required to get a certificate of occupancy
Be listed for the purpose for which they are installed.	Not necessarily. As pointed out by the NBFAA, listed equipment may be too expensive for SDU applications. Being compliant with the applicable standards is usually adequate.
Be installed according to manufacturer's instructions.	Absolutely.
Be designed and installed by qualified personnel	Yes – typically this would mean someone certified either by the manufacturer or by an industry association like BICSI.

Table 5. Applicability of NFPA fundamental principles to SDUs

[6] See Annex A for a more complete discussion of NFPA 730.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

The only one of these fundamental principles which may not be feasible in residential systems is the requirement that all equipment be listed. As discussed previously, this might be too expensive for residential systems which are typically not required by either building codes or insurance companies.

4.2.2 Power Supplies

The performance of primary and backup power supplies is as critical in a residential system as it is in a commercial building. With the exception of requirements for listing and periodic testing and maintenance, power supplies in an SDU should follow the requirements of NFPA 731.

4.2.3 Wiring

Although NFPA 731 Clause 4.5.8 addresses wiring for EPSS's, the issue of residential cabling is already pretty well covered in TIA/EIA-570B, which includes a section on security system wiring.   There are a number of references available on the subject of residential cabling, including [Baxter 2005] and [BICSI 2002]. Following the requirements of TIA/EIA-570B, as well as NFPA 70, the requirements of the AHJ, and the manufacturer's instructions should be adequate for residential security system wiring.

4.2.4 Intrusion Detection and Access Control Systems

NFPA 731 gives requirements for several different types of security systems. Table 6 summarizes the applicability of these systems requirements in a residential environment.

Type of System	Applicable to SDUs?
Intrusion detection	This is the most commonly installed type of home security system. The NFPA 731 requirements for these systems seem reasonable for SDUs the exception of listing of all equipment. Note that in many cases, the 2008 editions softens this requirement to being "compliant with" rather than "listed to." In any case, local AHJ requirements should be followed.
Access control	Not usually installed in SDUs.
Video surveillance	Often installed as part of a home security system. With the exception of the equipment listing requirement, the NFPA 731 requirements seem reasonable for SDUs.
Holdup, duress, and ambush	Not usually installed in SDUs.

Table 6. Applicability of NFPA 731 System Requirements to SDUs

4.2.5 Monitoring Stations

Residential security systems almost universally use commercial monitoring stations. Selection of a residential security provider is usually done on the basis of reputation and price. It is generally not necessary to demand compliance with NFPA 731.

4.2.6 Testing and Inspection

Testing and inspection is an area where there is a major difference in requirements between commercial and residential installations. The acceptance testing and periodic maintenance specified in NFPA 731 would be very expensive for a residential system. In an SDU installation, it is recommended that the manufacturer's instructions and AHJ requirements be followed instead of the NFPA 731 requirements.

4.3 Conclusion

For the installation of security systems in single- and two-family dwellings, the following practices are recommended:

1. Follow the guidelines in NFPA 730 as they apply to single- and two-family dwellings.
2. Residential wiring should be installed as per TIA-570B as well as NFPA 70.
3. For wiring and equipment, always follow both the manufacturer's instructions and the AHJ requirements.
4. With the exception of equipment listing and testing/maintenance, intrusion detection systems and video surveillance equipment should generally comply with the requirements of NFPA 731.

5 References

[Baxter 2005] *Residential Networks*. Albany, NY: Delmar, ISBN 1401862675.

[BICSI 2002] *Residential Network Cabling*. New York: McGraw-Hill. ISBN 0-07-138211-9.

[NFPA 70] NFPA 70: *National Electrical Code*®, 2005 edition.

[TIA-570B] TIA/EIA-570-B: *Residential Telecommunications Cabling Standard.*

[UL 294] UL 294, *Standard for Access Control System Units*, 1999, revised 2005.

[UL 606] UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems*, 1999.

[UL 634] UL 634, *Standard for Connectors and Switches for Use with Burglar- Alarm Systems*, 2000.

[UL 639] UL 639, *Standard for Safety for Intrusion- Detection Units*, 1997, revised 2002.

[UL 2044] UL 2044, Standard for Commercial Closed Circuit Television Equipment, 1997, revised 2004.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

6 Acronyms

AGC	Automatic gain control
AHJ	Authority having jurisdiction
ATM	Automated teller machine
CCTV	Closed-circuit television
DIS	Digital imaging system
EPSS	Electronic premises security system
IT&M	Installation, testing, and maintenance
MDU	Multi-dwelling unit
NBFAA	National Burglar and Fire Alarm Association
NEC	National Electric Code
NFPA	National Fire Protection Association
NID	Network interface device
PEC	Photo-electric cell
PIR	Passive infra-red
RTE	Request-to-exit
SDU	Single dwelling unit (one- or two-family)
TIA	Telecommunications Industries Association
UL	Underwriters Laboratories
UTP	Unshielded twisted pair
VMD	Video motion detector

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

7 Annex A -- Overview of NFPA 730 -- Guide for Premises Security

7.1 Facility Classification

NFPA 730 classifies buildings and facilities into one of 11 types, as shown in Table A-1. It does not provide specific guidance for a number of types of special-purpose buildings such as stadiums, convention centers, airports, train stations, etc., but covers almost all other common types of buildings. An additional set of considerations for special events is also included. One chapter of the document is devoted to each of these types. For convenience of discussion in this report, the 12 types have been grouped in to five categories, as indicated in the left column of Table A-1.

Mixed facilities include two or more classes of facility within the same building or structure, for example, a resort which includes a hotel, restaurants, and a shopping center.

Category	Type	NFPA 730 Chapter
Housing	One- and two-family dwellings	13
	Apartment buildings	15
	Lodging	14
Education & Health Care	Educational	11
	Health care	12
Retail	Restaurants	16
	Shopping centers	17
	Retail establishments	18
Commercial & Industrial	Office buildings	19
	Industrial facilities	20
	Parking facilities	21
Misc.	Special events	22

Table A-1
Types of facilities in NFPA 730

7.1.1 Concentric Circles of Protection

The recommendations of NFPA 730 are based on the concentric circles of protection methodology which is illustrated in Figure A-1. To protect a critical asset from theft, sabotage, vandalism, terrorism, or other malicious acts, an adversary must either be deterred or defeated. The concentric circles of protection methodology surrounds each critical asset with 4 layers of protection:

- Deter – discouraging an adversary from attacking, usually by making the attack so difficult that success is unlikely.
- Detect – determining as quickly as possible when an attack is occurring.
- Delay – impeding the adversary's actions for as long as possible to give time for an effective response.
- Respond – counteraction against the adversary by either automatic systems or by police and other security forces.

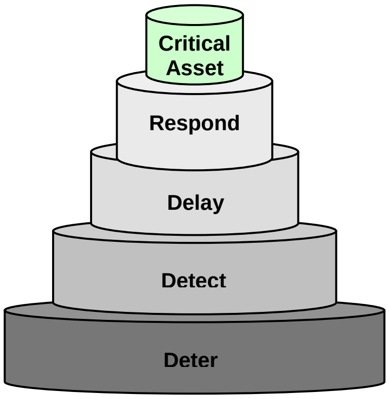

Figure A-1
Concentric circles of protection

7.1.2 Security Vulnerability Assessment

Chapter 5 outlines a fairly standard security planning process which includes the following seven steps:

1) Formation of a security assessment team
2) Organizational/facility characterization
3) Threat assessment
4) Threat vulnerability analysis
5) Define specific security countermeasures
6) Assess risk reduction
7) Document findings and track implementation

7.1.3 Additional Information

Annexes at the end of NFPA 730 include information about a number of other areas, such as the three summarized below.

- **Workplace Violence** -- There is a discussion of workplace violence with particular emphasis on health care facilities. A 27-element checklist is provided to assist in determining the likelihood of workplace violence.
- **Homeland Security Advisory System --** Annex B includes a discussion of the threat levels (Green, Blue, Yellow, Orange, Red) including what actions businesses and homeowners should take.
- **Preparation for Various Kinds of Attacks** – Material is provided about preparing for a whole bunch of different conditions, including:
  - ▪ Terrorism
  - ▪ Cyber attack
  - ▪ Building explosion
  - ▪ Bomb threats
  - ▪ Chemical and biological weapons
  - ▪ Nuclear and radiological attack (including electromagnetic pulse)

The discussion includes information about what to do before, during, and after each type of attack.

7.2 ***Security Systems and Technology***

NFPA 730 addresses a number of different aspects of security systems technology and operations, including:

- External security devices and systems
- Physical security devices
- Interior security systems
- Security personnel
- Security planning

Each of these will be discussed in the sections below.

7.2.1 External Security Devices and Systems

Exterior security systems are used to protect the perimeter of a facility. One of the most common elements of exterior security systems is fencing. NFPA 730 includes an extensive discussion of fencing (especially chain link) including recommendations for:

- ▪ Material
- ▪ Height
- ▪ Posts
- ▪ Top guard
- ▪ Gates
- ▪ Clearances from buildings, parking lots, etc.
- ▪ Illumination levels needed to provide visibility and deter intrusion.

Protective lighting is one of the best and least expensive deterrents to crime and vandalism. The document provides a discussion of many different lighting parameters, including:

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

- Minimum outdoor lighting intensities for exterior areas (ranging from 0.1 foot-candles for inactive entrances to 2.0 foot-candles for pedestrian entrances.)
- Redundancy, reliability, and maintenance of lighting
- Light sources, including incandescent, fluorescent, high-intensity discharge (HID -- mercury vapor, metal halide, and high-pressure sodium)
- Street lighting and search lights

Since the point of illicit entry into a building is normally a window or door, the document makes recommendations for protecting those areas, including the use of ironwork and burglar-resistant and bullet-resistant glazing. Considerations for the security of walls, floors, and ceilings are also discussed, including the use of passive barriers.

Electronic perimeter protection is the final element of exterior security systems. Perimeter systems include fence-mounted or buried sensors, pressure systems, leaky coax, infrared and microwave volumetric detectors, etc.

7.2.2 Physical Security Devices

Locks are the most common means of ensuring physical security. Locks can be divided into three major classifications -- mechanical, electromechanical, and electronic. Use of all three types is discussed.

Since locks are typically opened by either a key or combination, key control and management procedures are of critical importance, especially in commercial environments where a large number of employees may have access to the keys. NFPA 730 makes recommendations on key management, record keeping, and key accountability procedures.

Considerations for locking of doors and windows are covered in detail. Finally, recommendations are made for security vaults, strong rooms, safes and insulated file storage to protect important items and documents.

7.2.3 Interior Security Systems

Interior security systems are designed to provide protection for controlled and restricted areas of a facility. A controlled area is a room or other portion of a facility to which access is monitored or limited in some way. A restricted area is a room or other area to which access is strictly controlled and limited to persons who are specifically authorized to be in that area.

The concentric rings of protection philosophy (as illustrated in Figure A-1) is applied to the areas that are controlled or restricted. Methods of protection include:

- Intrusion detection systems, which include sensors and annunciators and may be either perimeter or volumetric systems.
- Video surveillance and monitoring, including the use of motion detection to trigger an alarm.
- Electronic access control systems which may be either card systems or biometric (fingerprint, hand geometry, handwriting verification, voice recognition, retinal scan, etc.)

When applicable, various types of alarm systems may be provided. The major types of alarm systems are:

- Holdup alarm – enables an employee of a protected premise to transmit a signal indicating that a robbery has transpired. Holdup alarms are normally located at a store cash register or bank teller window.
- Duress alarm – notifies onsite personnel of a potentially hostile civil disturbance or emergency at the protected property and summons assistance to the area of the civil disturbance or emergency.
- Ambush alarm – (sometimes known as a “panic” alarm) sends notification that

The information in this publication has been validated as correct and true to the best of the author’s abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

an “attacking party” has been encountered.

7.2.4 Security Personnel

Security personnel are a key factor in implementing an effective security system. NFPA 730 discusses a number of personnel-related issues, including security duties, cost factors, personnel selection, etc.

7.2.5 Security Planning

NFPA 730 provides in-depth recommendations for the development of a security plan. The key components of such a plan include:

- Security vulnerability assessment (as discussed previously)
- Description of the facility and organizational structure
- Security organization and operations
- Threat assessments and risks
- Employee, visitor, and vendor safety

Planning for terrorism is a key aspect of the security plan. This includes bomb threats and cyber attacks as well as more violent incidents.

Since negligent hiring is a major potential liability for employers, recommendations are also made for pre-employment screening such as criminal background checks.

7.3 Housing Facilities

After the basics of security system philosophy, technology, and operation have been covered, NFPA 730 provides a detailed discussion of security considerations in each of the types of facilities listed in Table A-1. In this report, we will place primary emphasis on housing facilities, but will briefly review the other types as well.

7.3.1 One- and Two-Family Dwellings

One- and two-family dwellings are defined as buildings containing one or two dwelling units which are primarily occupied on a permanent basis. In this report, we will refer to one- and two-family dwellings as single-dwelling units (SDUs).

Several factors should be taken into consideration when planning a security system for an SDU, including:

- Type of residence
- Demographics
- Lighting
- Pedestrian and vehicular traffic
- Activity in the area

Clause 13.4.1 gives an extensive list (29 items) of basic and environmental precautions that can be taken to deter crime by reducing the perception of opportunity, such as:

- Make sure the home looks lived-in when you are away (arrange for lawn mowing and/or, snow removal, don’t let newspapers accumulate, put the lights on a timer, etc.)
- Don’t hide a key outside the house.
- Change the code on radio-operated garage door openers which are usually set to a default code when manufactured.)
- Keep shrubbery trimmed back away from doors and windows to eliminate hiding places for burglars.

Most of these are common-sense items, but failure to observe them can negate an otherwise well-planned security system.

Key elements of physical security in the home are discussed in some detail, including:

- Deadbolt locks

The information in this publication has been validated as correct and true to the best of the author’s abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

- Doors
- Garage doors
- Windows

Outdoor lighting is also an important consideration, including the use of photoelectric and motion-detection sensors. Recommendations for selecting a security provider are also provided, including advice on selecting a reputable company and on the type of system to be installed.

7.3.2 Apartment Buildings

Apartments are defines as buildings containing three or more dwelling units with independent kitchen and bathroom facilities. The security of the individual rental units in apartment buildings is very similar to the considerations for SDUs which were discussed in the previous section. However, there are a number of additional areas which must be addressed in a security plan for apartment buildings, including the following.

- Key management is very important. As tenants move into and out of apartments, the keys must be accounted for and locks must be re-keyed as necessary.
- Tenant identification and background verification are also very important.
- The neighborhood crime history should be considered.
- Apartment buildings normally include a number of public accessible and common areas such as stairwells, elevators, lobbies, hallways, laundry rooms, storage facilities, recreational facilities, parking lots, etc. Adequate security provisions must be provided for these areas.
- An apartment complex normally employs maintenance and security personnel who have access to both the common areas and the rental units. Employment practices, such as training, screening and background checks, and drug testing are very important. When outside contractors and vendors are used, proper screening and identification should also be applied.

7.3.3 Lodging Facilities

Lodging facilities includes many different types of structures including hotels, motels, inns, resorts, conference centers, etc. They often provide restaurants, meeting rooms, recreational facilities and other services. Among the key security considerations are:

- Front desk security
- Lock and key control
- Guest room security
- Access control in non-public areas such as kitchens, mechanical rooms, electrical distribution facilities, etc.

7.4 Educational and Health Care Facilities

7.4.1 Education

Educational facilities include both primary and secondary schools as well as college and university campuses. In addition to the requirements discussed in other sections for housing (dormitories and apartments), restaurants, and parking facilities, there are a number of special considerations for educational facilities. Maintaining student safety is one of the primary considerations. Prevention of theft and vandalism are also very important in the educational environment. NFPA 730 devotes more than five pages to a discussion of these issues.

7.4.2 Health Care Facilities

NFPA 730 defines a health care facility as a facility that provides medical services or treatment simultaneously for at least four persons who (for reasons of age, illness, disability, anesthesia, etc.) are unable to take action for self-preservation under emergency conditions. Some of the major considerations for the security of health care facilities are:

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

- Security of patients is obviously a major concern since, by definition, they are not able to take care of themselves in any type of emergency situation.
- Security of the staff is also a major consideration since they are vulnerable to assault both by disoriented patients and by unhappy relatives of patients.
- Visitor control is important due to the large number of visitors and delivery personnel that are often present at health care facilities.
- Health care facilities generally contain medications and other controlled substances as well as expensive equipment. Theft and burglary prevention are therefore very important.
- To provide patient security and prevent theft, access to uniforms, medicines, equipment, etc. must be tightly controlled.
- In a health care facility, employment practices (including background checks, drug tests, etc.) are obviously extremely important.

7.5 ***Retail Facilities***

The three types of retail facilities are restaurants, retail establishments (i.e., stores), and shopping centers. For all of them, proper employment practices are a major component of the security plan. This includes pre-employment screening, criminal background checks, drug testing, and proper identification.

7.5.1 Restaurants

For purposes of NFPA 730, the term restaurants includes both fast-food and table-service types of establishments. Major security concerns for restaurants include:

- Robbery prevention including control of cash.
- Employee training, including procedures for handling robberies, disturbances, health problems for guests, etc.
- Burglary prevention, including intrusion detection systems.

7.5.2 Retail Establishments

Retail establishments are businesses that are primarily engaged in the sale of products directly to consumers. The major security considerations are the prevention of employee theft, robbery, burglary, shoplifting, and workplace violence.

7.5.3 Shopping Centers

A shopping center is a group of retail establishments which is managed as a single property. In addition to the considerations for retail establishments and restaurants which are mentioned above (and parking facilities which are discussed in a later section), the main additional considerations for shopping centers are:

- Security personnel, patrols, and law enforcement liaison.
- Emergency procedures for natural and man-made disasters, criminal acts, and mechanical failures.
- Proper lighting

7.6 ***Commercial and Industrial Facilities***

7.6.1 Office Buildings

Office buildings include facilities used for office, professional, or service-type transactions including the storage of records. It does not include government or law-enforcement buildings which are covered by a Department of Justice publication. The major security considerations include:

- Access control is a particular problem for office buildings because large numbers of office employees must come and go with minimal inconvenience but unauthorized personnel must be excluded.
- Lock and key control is a critical element due to the large number (and frequent) turnover of tenants and employees with access to controlled areas.

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.

7.6.2 Industrial Facilities

Industrial facilities include facilities where products are manufactured, processed, assembled, or repaired or where operations such as mixing, finishing, and packaging are conducted. The key security considerations for industrial facilities are:

- Because industrial facilities often make use of chemicals and explosives or other hazardous materials, prevention of terrorism and sabotage are major issues.
- Security of chemicals and hazardous materials is important, both to prevent deliberate harmful acts as well as accidental environmental damage or injury to employees.
- Industrial facilities are often large and provide many places for intruders to hide, so access control and intrusion detection are very important.
- Employment practices, particularly background checks, are once again of critical importance.

7.6.3 Parking Facilities

A parking facility is a building or space that is primarily used for the storage of vehicles. Prevention of crime in the parking facility is the major security concern -- both the theft of vehicles and crimes against occupants of the vehicles. Two of the main methods of addressing crime prevention in parking facilities are proper lighting and access control, including minimizing the number of entrances and exits to the facility.

7.7 Special Events

Special events include things like athletic events, concerts, exhibits, and visitors who will draw a large crowd. In addition to the normal everyday security concerns of the facility, the following are of key importance when hosting special events:

- Access control
- Parking and traffic control
- Disturbance/incident handling

The information in this publication has been validated as correct and true to the best of the author's abilities. The author and BCS provide no guarantee and disclaim all liability stemming from the use of any information herein, and assume no responsibility for statements/opinions expressed or implied in the body of this document.