UL 827

STANDARD FOR SAFETY

Central-Station Alarm Services

UL Standard for Safety for Central-Station Alarm Services, UL 827

Eighth Edition, Dated October 29, 2014

Summary of Topics

This revision of ANSI/UL 827 dated September 28, 2021 includes editorial corrections to the revision in 52.1, published on September 15, 2021.

Text that has been changed in any manner or impacted by UL's electronic publishing system is marked with a vertical line in the margin.

No Text on This Page

OCTOBER 29, 2014
(Title Page Reprinted: September 28, 2021)

ANSI/UL 827-2021

UL 827

Standard for Central-Station Alarm Services

First Edition – September, 1971
Second Edition – October, 1972
Third Edition – October, 1977
Fourth Edition – January, 1982
Fifth Edition – August, 1993
Sixth Edition – October, 1996
Seventh Edition – June, 2008

Eighth Edition

October 29, 2014

This ANSI/UL Standard for Safety consists of the Eighth Edition including revisions through September 28, 2021.

The most recent designation of ANSI/UL 827 as an American National Standard (ANSI) occurred on September 15, 2021. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, and Title Page.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at https://csds.ul.com.

No Text on This Page

CONTENTS

INTRODUCTION

FACILITIES AND EQUIPMENT

FIRE-ALARM SERVICES

BURGLAR-ALARM SERVICES

RESIDENTIAL MONITORING STATION

TEMPORARY OPERATING CENTERS

COMMUNICATION DISRUPTIONS

INTRODUCTION

1 Scope

1.1 These requirements apply to:

a) Central stations providing watchman, fire-alarm, and supervisory services as described in the National Fire Alarm and Signaling Code, NFPA 72;

b) Central-station burglar-alarm systems intended and specifically designated for burglary protection use at mercantile and banking premises, on mercantile safes and vaults, and on bank safes and vaults;

c) Residential monitoring stations monitoring residential alarm systems;

d) Redundant sites; and

e) Remote signal management centers.

1.2 These requirements apply to monitoring stations that are intended to be located in buildings constructed in accordance with building codes, such as the Building Officials and Code Administrators (BOCA) National Building Code, the International Building Code, the Standard Building Code, and the Uniform Building Code.

1.3 The central-station burglar- and fire-alarm or residential alarm systems covered by these requirements are systems in which the operation of electrical protection circuits and devices are signaled automatically to, recorded in, and supervised from a central-station or residential monitoring station having trained operators on duty at all times.

1.4 Requirements covering the construction and operation of burglar-alarm units used in the burglar-alarm systems covered by this Standard are contained in the Standard for Central-Station Burglar-Alarm Units, UL 1610, and the Standard for Digital Alarm Communicator System Units, UL 1635.

1.5 Burglar-alarm protective devices installed on individual properties are classified as to the extent of protection at each location. Requirements covering installation and classification (of extent) of alarm protective equipment at individual locations are contained in the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681.

1.6 Burglar-alarm protective devices installed in residential alarm systems at individual properties are classified as to the extent of protection at each location. Requirements covering installation and classification (of extent) of alarm protective equipment at individual locations are contained in the Standard for Installation and Classification of Residential Burglar Alarm Systems, UL 1641.

1.7 Requirements covering the construction and operation of fire-protective signaling equipment used in the systems covered by this standard are contained in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

1.8 Requirements for the installation of fire-alarm initiating devices and notification appliances installed at individual properties are contained in the National Fire Alarm and Signaling Code, NFPA 72.

1.9 Systems covered by these requirements operate within the limits of the National Electrical Code, NFPA 70, as applied by the local authority having jurisdiction. The Articles of the National Electrical Code that apply are:

a) Article 725, within the limits of Class 2 or Class 3 remote-control and signaling circuits for burglar-alarm systems;

b) Article 760 for fire-alarm systems;

c) Article 800 for outside wiring and protectors;

d) Article 820 for protectors for radio antennas; and

e) Article 830 for Network-Powered Broadband Communications Systems.

1.10 Requirements for software and hardware, and the installation and operation of an automation system in a central station, remote signal management center, redundant site, subsidiary station or residential monitoring station are covered by the Standard for Central-Station Automation Systems, UL 1981, or by the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, and/or the Standard for Central-Station Burglar-Alarm Units, UL 1610.

1.11 A reference made to "station" refers to a central station (burglary or fire), remote signal management center, subsidiary station, or residential monitoring station, depending upon the context in which it is used

1.12 These requirements do not cover the communication channel between the protected property and the station unless the communication company is owned and operated by the station. This includes:

a) The company that provides the communication channel; and

b) The equipment that is used to provide the communication channel.

1.13 The units, devices, and systems covered by the above standards shall operate, and be applied as defined therein, unless this Standard, UL 827, indicates otherwise.

2 Components

2.1 Except as indicated in 2.2, a component used in a station or a burglar-alarm or fire-alarm installation covered by this Standard shall comply with the requirements for that component. See Appendix A for a list of standards covering components generally used to provide the services covered by this Standard.

2.2 A component is not required to comply with a specific requirement that:

a) Involves a feature or characteristic not required in the application of the component in the product covered by this standard, or

b) Is superseded by a requirement in this standard.

2.3 A component shall be used in accordance with its rating established for the intended conditions of use.

2.4 Specific components are incomplete in construction features or restricted in performance capabilities. Such components are intended for use only under limited conditions, such as certain temperatures not exceeding specified limits, and shall be used only under those specific conditions.

3 Units of Measurement

3.1 Values stated without parentheses are the requirement. Values in parentheses are explanatory or approximate information.

4 Undated References

4.1 Any undated reference to a code or standard appearing in the requirements of this standard shall be interpreted as referring to the latest edition of that code or standard.

5 Glossary

5.1 General

5.1.1 For the purpose of this Standard, the following definitions apply.

5.2 Definitions common to burglar- and fire-alarm systems

5.2.1 ACTIVE SYSTEM – A system that transmits one or both of the following signals to the central-station on a regular basis:

a) A signal that the system has been disarmed and the protection removed (commonly referred to as "opened"); or

b) A signal that the system has been armed and the protection activated (commonly referred to as "closed").

If an alarm system sends opening and closing (disarm and arm) signals, it is considered to be an active system. Supervisory check-in signals transmitted from a system does not make it an active system. (See 5.2.28 Inactive System).

5.2.1A AUTHORIZED PROVIDER – A business which has developed or is provided to provide licensed computer or software-based services or sales to customers.

5.2.2 AUTOMATIC FIRE-ALARM SYSTEM – A fire detection system that will automatically detect and annunciate the presence of fire by the detection of one or more products of combustion. Annunciation is through a fire-alarm system control unit.

5.2.3 AUTOMATION SYSTEM – A computer system that consists of hardware and software components. These components include the alarm-monitoring software supplied by the automation system developer, the operating system, and programming languages, required to make the system operational. An automation system may be configured as a computer system that is directly connected to hardware based central-station receivers, internal software based receivers, or is connected to remote receivers located in central-stations other than the one where the automation system is located. It is used to automatically process change-of-status signals such as alarm, trouble, supervisory, disarming and arming (i.e. opening and closing), and similar signals that it receives from the central station receiving equipment. See the Standard for Central-Station Automation Systems, UL 1981.

5.2.4 BACKUP CENTER – A location that is capable of being staffed in order to process signals in the event the Central Station becomes uninhabitable or inoperable. This center is another location that the operator of the Central Station has chosen to maintain for backup purposes.

5.2.5 BUILDING, MULTIPLE OCCUPANCY – A building that is occupied by two or more independent tenants who do not have control of each other.

5.2.6 BUILDING, SINGLE OCCUPANCY – A building that is occupied by and under the control of the alarm service company only. Any business in the building that is not directly associated with the alarm service shall be the business of, and controlled by, the alarm service company.

5.2.6.1 CALL LIST – Names of individuals, such as authorized representatives, authorized users, and subscriber's representatives, designated by the subscriber to be contacted in association with the receipt of signals or other events in the delivery of central station service. These individuals may be assigned personal identification codes as a means of identification when in contact with the central station.

5.2.7 CENTRAL-STATION – A building, distributed group of buildings, or a distributed group of enclosed areas within a building that is occupied by the alarm service company that operates the central station, other businesses that are owned, and controlled by the alarm service company and which houses an operating room and equipment used to provide central-station service to protected properties.

5.2.8 CENTRAL-STATION SERVICE – The use of a system or a group of systems in which the operation of circuits and devices at a protected property are signaled to, recorded in, and supervised from a central station having trained operators who, upon the receipt of a signal, take such action as required by the nature of the signal received.

5.2.8.1 CERTIFICATE AUTHORITY (CA) – The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy. (The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.)

5.2.9 COMPUTER CLUSTER – High-available clusters or Failover clusters. A group of two or more computers that are connected to form redundant nodes which are used to provide service when system components fail. Such high-availability or failover clusters are designed to use redundancy of cluster components to eliminate single points of failure.

5.2.10 CODE TRANSMITTER SYSTEM – A system that provides for the connection of more than one protection system to a single alarm receiving unit at the station.

5.2.11 DERIVED CHANNEL – A signaling line circuit that uses the local leg of the public telephone company's switched network as an active multiplex channel, while simultaneously allowing the leg's use for normal telephone communications.

5.2.12 DIGITAL ALARM COMMUNICATOR RECEIVER (DACR) – A system component located at the central station that will receive and display signals from a DACT (see 5.2.14).

5.2.13 DIGITAL ALARM COMMUNICATOR SYSTEM – A system that provides for the connection of a protection system to a station through the telephone company's switched network or a wireless communication device utilizing standard industry equipment and licensed for commercial use system.

5.2.14 DIGITAL ALARM COMMUNICATOR TRANSMITTER (DACT) – A system component located at the protected premises that will contact a DACR (see 5.2.12) through the public switched telephone network, when there is a change or status in the alarm system, and transmit the necessary data to identify the protected premises and the change of status. The connection to the public switched telephone network may use a wired or wireless path. A DACT is either integral with the control unit that provides alarm or monitoring functions, or interfaces with a control unit that provides these functions.

5.2.15 DIGITAL ALARM RADIO RECEIVER (DARR) – A system component used in a DARS (see 5.2.16) to receive radio signals transmitted from a DART (see 5.2.17).

5.2.16 DIGITAL ALARM RADIO SYSTEM (DARS) – A one-way radio system that provides backup transmission for a DACT (see 5.2.14).

5.2.17 DIGITAL ALARM RADIO TRANSMITTER (DART) – A system component used in a DARS (see 5.2.16) to transmit signals to a DARR (see 5.2.15) via radio signals.

5.2.18 DIRECT-WIRE SYSTEM – A system that provides for the connection of a single protection system to a single alarm-receiving unit at the station.

5.2.19 EMERGENCY COMMUNICATION SYSTEM (ECS) – A system used to communicate with the public that an emergency exists and provide instructions for them (the public) to follow for their safety. There are also systems used to deal with mass-communications that do not qualify as a “life-safety” system. As used within the context of this Standard the ECS systems are the type used in “life-safety” applications.

5.2.20 ENCRYPTION – The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

5.2.21 ENCRYPTION, ADVANCED – A connection with the central station network, that has a certificate of authority (CA), accepted and trusted by the browser(s) and the browser client, or an encryption that is listed in the most recent edition of NIST 800-131 as ‘approved and/or acceptable’.

5.2.22 ENCRYPTION, BASIC – Encryption software that is provided as part of the operating system used by each computer connected to a network.

5.2.23 FAULT-TOLERANT COMPUTER SYSTEM – A computer system containing multiple power supplies, disks, processors, and controllers, each of which backing up and checking on the processes of the others. In the event of a component failure, the other modules take over the job performed by the failed component without affecting the operation of the computer. In addition to the duplicate hardware, a fault-tolerant system includes software components consisting of the operating system, programming languages, and the alarm-monitoring software supplied by the automation system software developer required to make the system operational. See 5.2.45 for the definitions of redundant computer system. A fault-tolerant computer system as defined above is considered to be a redundant system.

5.2.24 HIGH AVAILABILITY COMPUTER SYSTEM – A computer system that has been designed and implemented to ensure the system will be operational 99.9% of every 12 month period. This performance shall include both operational time and any downtime for scheduled maintenance that may occur in the 12 month period.

5.2.25 HUNT GROUP – A group of associated telephone lines within which an incoming call is automatically routed to an idle (not busy) telephone line for completion.

5.2.26 HVAC SYSTEM – A heating, ventilation, and air conditioning system.

5.2.27 IDENTIFICATION CODE – The numeric, alpha numeric, alpha, word(s), or similar device used to identify a subscriber.

5.2.28 INACTIVE SYSTEM – A system that transmits a signal to the central-station only when an unintended condition exists or it is under test. Examples of inactive systems are fire- and holdup alarms, or a burglar alarm system supervising a protected premise without the use of opening and closing signals. Check-in signals transmitted from a system does not make it an active system.

5.2.28.1 INDEPENDENT DEALER – A business that typically sells, installs, and services an alarm system, but contracts with a central-station company to do the alarm system monitoring.

5.2.29 KEY VAULT – An attack resistant container mounted outside of the protected premises that contains the key(s) that will allow entrance into the protected premises. The key vault can be opened with a mechanical key or a card key that is common to several key vaults and which is carried by the runner. Other emergency services, such as the fire department, law enforcement department and authorized private guard service may also have access to the key vault.

5.2.29.1 LOCAL AREA NETWORK (LAN) – The network, that connects computers and peripheral equipment in a building or a cluster of buildings, to the central-station automation system, that is physically secured, managed and under direct control/supervision of the central-station company.

5.2.30 MONITORING EQUIVALENT WEIGHT (MEW) FACTOR – A calculation used to determine the minimum system configuration and hardware for an automation system that is used in conjunction with the delivery of central station services.

5.2.30A MULTIFACTOR AUTHENTICATION – an identification and authentication method in which a user is granted access to an application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).

5.2.31 MULTIPLEXING – A method of signaling characterized by the simultaneous or sequential transmission and reception of multiple signals over a communication channel and the provision of means for positively identifying each signal. The signaling may be accomplished over a communication channel or radio carrier or a combination of both.

5.2.32 ONE-WAY RADIO ALARM SYSTEM (OWRAS) – A system in which alarm system signals are transmitted from a RAT (see 5.2.42) through a radio channel to at least two independently powered, independently operating, and separately located RARSRs (see 5.2.40) and which are then relayed to a RASSR (see 5.2.41). Signals may be transmitted through one RARSR provided they are also transmitted directly to the RASSR.

5.2.33 OPERATING ROOM – The physically enclosed area within a station that is secured against unauthorized access and where the operators receive and act on the signals that are transmitted to the station.

5.2.34 OPERATOR – A trained employee of the station whose duty is to provide immediate response to all signals received in the operating room.

5.2.35 PACKET SWITCHED DATA NETWORK (PSDN) – A type of data transmission in which data is divided into packets, each of which has a destination address. Each packet is then routed across a computer network. A packet may travel a different route than packets related to it.

5.2.36 PERSONAL IDENTIFIER – A physical attribute of a person used as a means of verification of personnel identity, such as by retina scan, voice print, fingerprint, hand span, and the like.

5.2.37 POWER ROOM – The area(s) in which the primary and secondary power supplies are housed. This room may or may not include an engine driven generator or uninterruptible battery supply.

5.2.38 PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) – An assembly of communications equipment and telephone service providers that utilize Managed Facilities-based Voice Networks (MFVN) to provide the general public with the ability to establish communications channels via discrete dialing codes. (Source NFPA 72, 2010 edition).

5.2.39 PUBLIC SAFETY ANSWERING POINT (PSAP) – A facility responsible for answering and processing calls for assistance from emergency service organizations such as fire departments, law enforcement departments, and emergency medical service organizations.

5.2.40 RADIO ALARM REPEATER STATION RECEIVER (RARSR) – A system component, used in an OWRAS (see 5.2.32) or a TWRAS (see 5.2.62), consisting of a radio receiver and transmitter located at a repeater station or subsidiary station. This component receives radio signals from a RAT (see 5.2.42) and

retransmits them to another RARSR or to a RASSR (see 5.2.41) in a OWRAS (see 5.2.32), or relays signals between a RATR (see 5.2.43) and a RASSR in a TWRAS.

5.2.41 RADIO ALARM SUPERVISING STATION RECEIVER (RASSR) – A radio receiver or receiver/transmitter located at a station, to receive signals from a RARSR (see 5.2.40), RAT (see 5.2.42), or RATR (see 5.2.43) and either annunciates them or interfaces with an automation system that annunciates them.

5.2.42 RADIO ALARM TRANSMITTER (RAT) – A radio transmitter used in an OWRAS (see 5.2.32) located at a protected premises that will transmit signals to at least two independently powered, independently operating, and separately located RARSRs (see 5.2.40). Signals may be transmitted through one RARSR if they are also transmitted directly to the RASSR. A RAT either:

a) Is integral with a control unit that provides alarm or monitoring functions; or

b) Interfaces with a control unit that provides these functions.

5.2.43 RADIO ALARM TRANSMITTER/RECEIVER (RATR) – A radio transmitter/receiver used in a TWRAS (see 5.2.62) that is located at a protected premises that will transmit and receive signals through at least two independently powered, independently operating, and separately located RARSRs (See 5.2.40) to and from a RASSR (See 5.2.41), or transmits and receives signals directly to and from a RASSR. A RATR either:

a) Is integral with a control unit that provides alarm or monitoring functions; or

b) Interfaces with a control unit that provides these functions.

5.2.44 REDUNDANT ARRAY OF INDEPENDENT DISKS (RAID) – A configuration that provides redundancy and continued performance in the event of a single disk drive failure.

5.2.45 REDUNDANT COMPUTER SYSTEM – Two or more computer systems maintained at a central-station, either of which can quickly be connected and operational for processing alarm signals in the event that the other computer fails to operate. (See 5.2.23). A fault-tolerant computer system is considered to be redundant.

5.2.46 REDUNDANT SITE – One or more physical locations that together can provide all the required functions of a central station should an automated central-station become unable to process signals.

5.2.46A REGIONAL/NATIONAL BUSINESS DISRUPTION – A national, state, or regional declaration, which creates a business disruption event that inhibits the operation of a Central-Station.

5.2.47 RELOCATION CENTER – A location that is acquired and configured when a central station is unable to operate.

5.2.47.1 REMOTE DATA ENTRY FACILITY – Data personnel working at a facility that may or may-not be managed by the central station company, whose only function is to enter data.

5.2.48 REMOTE SIGNAL MANAGEMENT CENTER – A location operated by the central station in which equipment associated with an alarm monitoring automation system, such as operator workstations or tertiary automation system equipment and the like, is housed.

5.2.49 REPEATER STATION – Equipment, such as radio, which is used to relay signals from protected systems installed at other location(s).

5.2.50 RUNNER – A person whose duties are to investigate signals from protected systems that require investigation.

5.2.51 RUNNER OR SERVICEPERSON STATION – A location separate from the central-station, subsidiary station, remote signal management center, or service center, where runners or servicepersons are stationed awaiting instructions to respond to signals received at the central-station. Signals are not to be received at a runner or serviceperson station.

5.2.52 RUNNER SERVICE COMPANY – A company that is independent of the central-station which provides runners to respond to signals received by the station as required by this Standard.

5.2.53 SERVICE CENTER – A location which may be separate from a central-station that provides required installation, maintenance, repair, and alarm investigator service to systems served by the company. Keys (where required) and maintenance records for protected premises are retained at the service center. Maintenance records are not required to be physically kept at the service center if they can be readily accessed at the service center from another location.

5.2.54 SERVICE VEHICLE – A vehicle that is used to provide required alarm investigator, installation, maintenance, and repair service to systems served by the company.

5.2.55 SERVICEPERSON – A person whose duties are to provide service to protected systems.

5.2.56 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) – An Internet-standard protocol for managing devices on IP networks.

5.2.57 SUBSCRIBER – The user of a premise or item protected by a central-station burglar or- fire-alarm system. An authorized representative of the user may also be considered a subscriber. For residential monitoring stations, a subscriber would be an occupant of a residence protected by the alarm system.

5.2.58 SUBSIDIARY STATION – A normally unattended physically secure facility linked by communication channels to a central-station or residential monitoring station. Signals from protected properties are transmitted to the subsidiary station and then relayed to the station. If the communication link between the subsidiary station and the station is out of service, the subsidiary station can be staffed and operated as a central-station or residential monitoring station.

5.2.59 SUPERVISED BURGLAR ALARM SYSTEM – An active alarm system (See 5.2.1) in which the central-station operators initiate follow up actions when an anticipated signal , such as an opening, closing, or check-in is missed or improperly sent.

5.2.60 TEMPORARY OPERATING CENTER – A location that functions as a replacement for an uninhabitable Central Station and/or Redundant Site, when needed.

5.2.61 TERTIARY SYSTEM – An additional computer system to a Redundant Computer System, that may or may not be housed in the central station.

5.2.62 TWO-WAY RADIO ALARM SYSTEM (TWRAS) – A system in which alarm system signals are transmitted and received through a radio channel between a RATR (see 5.2.43) and a RASSR (see 5.2.41). The signals may or may not be relayed through a RARSR (see 5.2.40).

5.2.63 UNINTERRUPTIBLE BATTERY SUPPLY (UBS) – A direct current (DC) generator driven by a combustion engine. The DC output is used to provide the DC power required by an uninterruptible power supply (UPS) or by DC powered units.

5.2.64 UNINTERRUPTIBLE POWER SUPPLY (UPS) – Equipment that will continue to provide alternating current (AC) power to a load in the event of failure of the normal AC power source. A UPS may also provide a more constant voltage and frequency supply to the load. When the normal source of AC fails, the UPS is powered by a DC source from batteries, a UBS, or both.

5.2.65 VIRTUAL PRIVATE NETWORK (VPN) – A private computer network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption.

5.2.66 WIDE AREA NETWORK (WAN) – Any network that is not is described in the definition of a LAN.

5.3 Definitions common to burglar-alarm

5.3.1 ACKNOWLEDGMENT SIGNAL – An audible and/or visual signal that is sent to the subscriber by the station to notify the subscriber that a signal has been received indicating that the protection system has been properly armed. The acknowledgment signal is to be sent manually or automatically.

5.3.2 CENTRAL-STATION BURGLAR-ALARM COMPANY – A company that is engaged in the business of operating one or more central-stations that provide monitoring, record keeping, and reporting for signals received from central-station burglar-alarm systems. The company shall directly provide for equipment installation, inspection, testing, maintenance and repair service of central-station systems, and runners for alarm investigation service, or it may subcontract for these services. In either case the company bears full responsibility the compliance of these services. The company may also operate one or more subsidiary stations or remote signal management centers.

5.3.3 CENTRAL-STATION BURGLAR-ALARM SYSTEM – A system or group of systems consisting of control units, intrusion detection units, contacts, protective wiring, installation wiring, and the like, installed at a protected property in accordance with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681. When the system is armed, detection of an intrusion will cause a signal to be automatically transmitted to a central-station complying with this standard. Arming the system will cause a closing signal to be transmitted and disarming the system will cause an opening signal to be transmitted. The system is to be controlled and operated by a central-station burglar-alarm company.

5.3.4 KEY INSTALLATION – is system for which the central-station holds the keys necessary to permit runners immediate access from the street to the interior of the protected premises or the premises enclosing a protected mercantile vault, safe, stockroom, ATM, or the like.

5.3.5 LINE SECURITY, STANDARD AND ENCRYPTION – Methods of supervising the communication channel used to transmit signals between the protected premises and the central-station or residential monitoring station. This supervision serves to detect compromise attempts on the communication channel that are intended to not cause signals to be annunciated at the station and which would allow entry into the protected premises without initiating a signal at the station.

5.3.6 SUBSCRIBER'S BURGLAR-ALARM CONTROL UNIT – Equipment located at the protected premises that controls the protective circuit(s), transmits signals to the central-station or residential monitoring station, and allows the subscriber to arm and disarm the alarm system.

5.4 Definitions common to fire-alarm

5.4.1 CENTRAL-STATION FIRE-ALARM COMPANY – A company that is engaged in the business of operating one or more central-stations that provide monitoring, retransmission of signals, and associated record keeping and reporting for signals from central-station fire-alarm systems. The station shall directly provide for equipment installation, inspection, testing, maintenance and repair service of central-station

systems, runner service, and associated central-station services, or they may subcontract for these services. The company may also operate one or more subsidiary stations or remote signal management centers. The station may also monitor central-station fire-alarm systems installed and maintained by a fire-alarm service – local company. The company operating the central-station may also operate one or more subsidiary stations or remote signal management centers.

5.4.2 CENTRAL-STATION FIRE-ALARM SYSTEM – A system or group of systems installed in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72, in which the operation of circuits and devices are transmitted automatically to, recorded in, maintained by, and supervised from a central-station having trained operators who, upon receipt of a signal, take action as required by NFPA 72. The system is to be controlled and operated by a central-station fire-alarm company.

5.4.3 FIRE-ALARM SERVICE – LOCAL COMPANY – A company that provides protected premises equipment installation, inspection, testing, maintenance and repair service of central-station fire-alarm systems with its own facilities and personnel in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72. The company subcontracts the monitoring, retransmission, and associated record keeping and reporting with a central-station. The required runner service is provided by the company or by the central-station.

5.5 Definitions common to residential monitoring stations

5.5.1 RESIDENTIAL MONITORED ACCOUNT – A single or two family dwelling with an installed alarm system being monitoring by a Central Station, and which does not have supervised openings and closings.

5.5.2 RESIDENTIAL MONITORING STATION – A building or enclosed area within a building that houses an operating room and equipment used to provide residential monitoring station service to protected properties.

5.5.3 RESIDENTIAL MONITORING STATION COMPANY – A company that is engaged in the business of operating one or more residential monitoring stations that provide monitoring, record keeping, and reporting for signals from alarm systems. The company may also operate one or more subsidiary stations or remote signal management centers.

FACILITIES AND EQUIPMENT

6 Building Construction Requirements

6.1 A building that houses a central station, remote signal management center, subsidiary station, or residential monitoring station shall comply with one of the following:

a) All bearing walls, floors, ceilings, columns, beams, girders, trusses, and arches have a one-hour fire resistant rating or are constructed of the materials specified in 6.4;

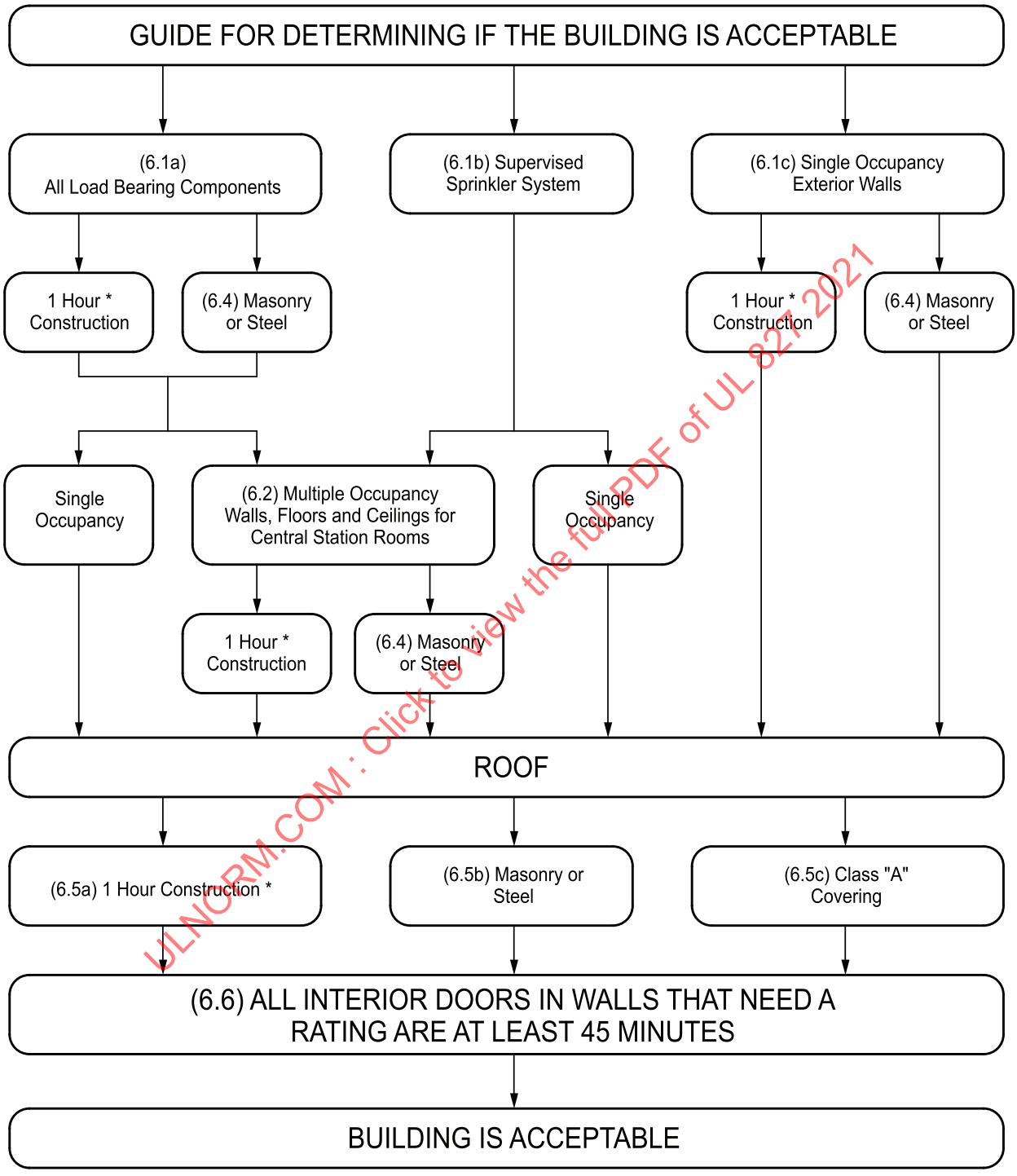
b) A sprinkler system, supervised by the station, installed in all parts of the building except for the operating room and power room; or

c) The building is single occupancy (See 5.2.5) and the exterior walls have a one-hour fire resistant rating or are constructed of the materials specified in 6.4.

See also Figure 6.1.

Figure 6.1

Building construction



su1729

* May be determined by compliance with the local building code, or the Standard for Fire Tests of Building Construction and Materials, UL 263. See 6.3.

6.2 In a multiple occupancy building (See 5.2.5), the walls, floors and ceilings enclosing the station (See 1.10) shall have a one hour fire resistant rating or be constructed of the materials specified in 6.4.

6.3 The fire resistant rating of building construction shall:

a) Meet the requirements of the local building code; or

b) Be determined by the test methods in the Standard for Fire Tests of Building Construction and Materials, UL 263.

6.4 Walls, floors, ceilings, beams, girders, trusses, and arches that are constructed of masonry or steel, or other materials deemed to have similar combustive characteristics are not required to have a fire resistant rating.

6.5 A building that houses a station shall either have a roof:

a) With a one-hour, fire-resistant rating;

b) Constructed of materials specified in 6.4; or

c) Constructed of a combustible deck with a Class A roof covering complying with the Standard for Materials for Built-Up Roof Coverings, UL 55A, and the Standard Test Methods for Fire Tests of Roof Coverings, UL 790.

6.6 Any door in an interior wall that is required to have a fire resistant rating shall have a minimum 3/4-hour fire resistant rating.

6.7 If a repeater station is located in a building:

a) The building shall comply with 6.1; or

b) The repeater station shall be duplicated at separate sites and signals shall be able to be relayed through either site.

7 Physical Protection

7.1 The operating room of a central, subsidiary, residential monitoring station, or remote signal management center shall be completely enclosed within a boundary that is fixed-in-place and shall be protected at all times against attack or entrance by unauthorized persons. Walls enclosing an operating room shall be constructed on a fixed-in-place floor deck and comply with one of the following:

a) Extend to a fixed-in-place ceiling or the underside of the building roof;

b) If a suspended ceiling is used, and the wall construction above the suspended ceiling is not required to serve as a fire stop, the portion of the wall above the suspended ceiling shall be constructed of wire-mesh screening constructed of at least 0.053 inch (1.35 mm) expanded sheet steel or 10 AWG (0.102 inch diameter) (5.26 mm^2) steel wire with openings not greater than 2 inches (51 mm); or

c) The walls extend to a suspended ceiling system and the entire station is configured as follows:

1) Access into and throughout the station is controlled by the company operating the station; and

2) Enclosed by fixed-in-place walls that extend from a fixed-in-place floor to a fixed-in-place ceiling, floor-ceiling assembly, or the underside of the building roof;

3) A burglar alarm system that complies with an Extent Number 3 in the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, shall be installed in the areas surrounding the operating room. The burglar alarm system shall be armed when the areas are unoccupied after normal business hours and shall be monitored in the operating room.

7.2 Entrances into the operating room shall be kept locked at all times and arranged so that positive identification can be made by vision and voice of any person seeking admittance. If the person is unknown to the personnel, they shall be identified by an identification card or the like. If a closed circuit television camera is used, a second means shall be provided and consist of either;

a) A second closed television camera with the same field of view as the first camera; or

b) A manual means of visual identification such as a peephole or the equivalent.

7.3 A door into the operating room of a station shall be one of the following:

a) A recognized fire-resistant door and door frame;

b) A solid or hollow metal door;

c) A solid wood, or solid wood core door with wood, plastic, or composition cladding a minimum of 1-1/2 inches (38 mm) thick; or

d) Where the door is located in an area that is controlled by the station such that only authorized persons have access to it, the door may be of glazing that complies with local building codes.

7.4 The entry door shall be equipped with an automatic door closer without a hold open feature, and a locking means that cannot be changed to an unlocked condition.

7.5 If the door is locked with an electromagnetic lock or similar device that requires electrical power to maintain the locking of the door, standby power or a backup mechanical lock shall be provided to maintain the locking of the door. The standby power shall be provided from the secondary power supply (see 11.5).

7.6 The operating room shall be arranged so that a person that is outside of the operating room in an area that is controlled by the station, cannot view the signal processing equipment to obtain information about an alarm system served by the station.

7.7 Any transparent window or panel that provides a view of the operating room from a location that is not under the control of the station shall be made translucent or opaque by painting, screening, blinds, curtains, drapes, or similar coverings. Mirrored, tinted, and one-way glass shall not be used for that purpose unless they are under the control of the Central Station in such a manner as to prevent a potential inversion of the one-way viewing functionality.

7.8 Any exterior opening, other than a door, that leads into the operating room from an area that is not controlled by the station, and which is:

a) Greater than 96 square inches (619 cm^2) with the smallest dimension exceeding 6 inches (152 mm); and

b) Is within 6 feet (1.82 m) of grade level or a working surface that may be reached through the use of fixed-in place ladders, stairs, or similar fixtures that facilitate climbing,

c) Shall be protected in manner that restricts ready access through the opening.

d) Restrictions may be achieved through such methods as the use of;

1) Heavy metal bars or screening installed over openings; or

2) Reinforcement of glazing with framed impact resistant polymeric film or sheet materials designed and installed for such purpose; or

3) Layers of complementary security controls which restrict access to the opening and which are monitored in the operating room by video cameras or other electronic security means; and the like.

7.9 A subsidiary station, a repeater station that is located in a building and does not comply with 6.7(b), a remote signal management center or redundant site that is not staffed at all times shall be equipped with a burglar-alarm and automatic fire-alarm system connected to the central station or residential monitoring station. The automatic fire-alarm system shall comply with the requirements in the National Fire Alarm and Signaling Code, NFPA 72. The burglar-alarm system shall comply with Extent No. 3 in the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, and shall be armed when the station is unattended. Equipment used to form the burglar-alarm and fire-alarm system shall comply with the applicable standard for such equipment (See Appendix A).

8 Fire Protection

8.1 Portable fire extinguishers

8.1.1 Each station operating room shall be equipped with a minimum of two multipurpose fire extinguishers rated 2-A:10-B:C or two portable fire extinguishers rated 2-A or greater and two portable fire extinguishers rated 10-B:C or greater.

8.1.2 Where an automation system or receivers are located in a separate room within or outside of the operating room a fire extinguisher rated 2-A:10-B:C and complies with 8.1.6 shall be located outside of the room and within 3 feet (0.9 m) of the door or in compliance with 8.2. One of the fire extinguishers required in 8.1.1 may fulfill this requirement provided it is readily accessible and immediately available for use in the operating room. Such rooms shall be provided with an automatic smoke and fire detection system that complies with the National Fire Alarm and Signaling Code, NFPA 72, and annunciates in the operating room.

8.1.3 Each power room, battery room, and engine-driven generator room or enclosure shall be equipped with a minimum of one multipurpose fire extinguisher rated at 2-A:10-B:C or one portable fire extinguisher rated 2-A or greater and one portable fire extinguisher rated 10-B:C or greater.

8.1.4 Portable fire extinguishers shall comply with the applicable Standards below:

a) The Standard for Water Fire Extinguishers, UL 626

b) The Standard for Carbon-Dioxide Fire Extinguishers, UL 154

c) The Standard for Dry Chemical Fire Extinguishers, UL 299;

d) The Standard for Halocarbon Clean Agent Fire Extinguishers, UL 2129.

8.1.5 A fire extinguisher intended to be used on electronic equipment, such as an automation system or receiver, shall be of the carbon dioxide or halogenated agent type and shall be located next to the equipment it is to protect if there are other types of extinguishers in the same room.

8.1.6 Fire extinguishers shall be located where they are readily accessible and immediately available. If they are mounted in a location that is not visible from any point in the operating room, their location shall be marked by a sign or similar notice.