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;

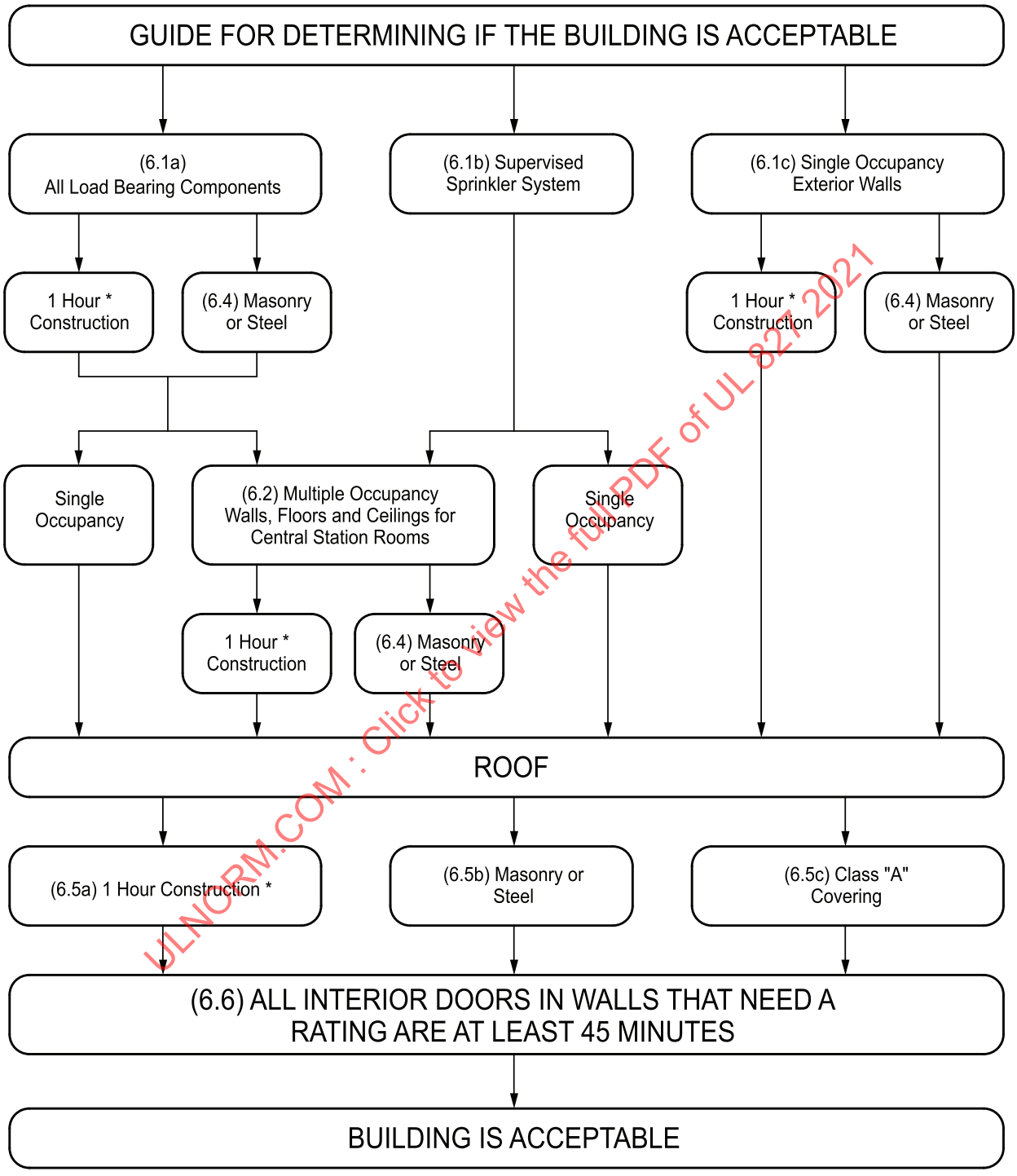
b) A sprinkler system, supervised by the station, installed in all parts of the building except for the operating room and power room; or

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.

8.1.7 A fire extinguisher shall be installed on the hanger or in the bracket supplied, or placed in a cabinet or a wall recess. A hanger or bracket shall be securely anchored to the mounting surface. If a cabinet is used, the door shall not be locked.

8.1.8 Fire extinguishers shall be maintained in accordance with the instructions marked on each extinguisher. Fire extinguishers shall be inspected every 12 months and the date of the inspection recorded in ink on a tag attached to the extinguisher.

8.1.9 The fire extinguisher for a power room, battery room, or engine-driven generator or enclosure described in 11.13.2 shall be located within 3 feet (0.9 m) of the inside or outside of the door or gate. If the engine-driven generator is enclosed as specified in 11.13.6, the extinguisher shall be located within 10 feet (3.05 m) of the enclosure. If the enclosure for the engine-driven generator is provided with a personnel door or gate, the extinguisher shall be located inside or just outside the door or gate, within 3 feet.

8.2 Fire suppression system

8.2.1 If the automation system equipment is located in a separate room or remote signal management center that is not normally occupied by personnel, and it is protected by a fire suppression system using a carbon-dioxide or halogenated or clean agent extinguishing agent, the discharge of the extinguishing agent shall either be automatic and an audible signal shall announce that it has been discharged, or the discharge of the extinguishing agent shall be under manual control. If under manual control, the automation system room shall be equipped with an automatic fire-alarm system that complies with the National Fire Alarm and Signaling Code, NFPA 72, with annunciation in the operating room. Manual discharge is not acceptable in a subsidiary station or redundant site (See 5.2.46).

8.3 Water sheds

8.3.1 A water shed, if not specifically prohibited by the Authority Having Jurisdiction (AHJ), shall be installed over any equipment that is sensitive to water damage if there is a possibility of water damage from overhead, such as the discharging of a sprinkler head. The water shed may be a fixed-in-place deflector, an enclosed rack designed to deflect water from the equipment, or may be a movable waterproof cover or shield installed next to the equipment so that it can be immediately positioned by one person to protect the equipment. A movable waterproof cover shall only be used in a staffed station. Where the staff is not always in the same room as the equipment and the source of the water is a pre-action sprinkler system, the discharge of the sprinkler shall be annunciated to designated personnel trained in the implementation of a written procedure for rapidly positioning the water shed.

8.4 Repeater station fire protection

8.4.1 A repeater station is not required to be provided with fire protection equipment, unless located in a building. A repeater station in a building is not required to be provided with fire protection equipment if it is duplicated at separate sites and signals are able to be relayed through either site.

8.5 Unoccupied area protection

8.5.1 All areas of the station (See 1.11) that are not continuously occupied by alarm service company personnel shall be protected by any of the following systems:

a) An automatic fire extinguishing system,

b) A fire suppression system, or

c) An automatic fire detection system.

8.5.2 Any of the systems referenced in 8.5.1 and used in such areas shall be connected to a fire alarm system installed in accordance with National Fire Alarm and Signaling Code, NFPA 72, and shall annunciate alarm, supervisory, and trouble conditions in the operating room.

9 Standby Lighting

9.1 Fixed standby lighting that is independent of the power source normally used for lighting, and which can be placed into service immediately, shall be provided in:

a) The operating room of a station;

b) Each runner and serviceperson station; and

c) An automation system room or equipment room that is separated from the operating room.

9.2 Fixed standby lighting, or rechargeable flashlights and/or lanterns, that is independent of the power source normally used for lighting, and which can be placed into service immediately, shall be provided:

a) In a power room; and

b) For an engine-driven generator(s).

9.3 Independent battery-powered standby lighting units shall comply with the Standard for Emergency Lighting and Power Equipment, UL 924.

9.4 Rechargeable flashlights and/or lanterns shall comply with the Standard for Class 2 Power Units, UL 1310.

9.5 The standby lighting and rechargeable flashlights and/or lanterns shall be tested for a continuous 5-minute period once per month. A record shall be kept of the test.

10 Clocks

10.1 The operating room or remote signal management center, or redundant site, or subsidiary station shall have the means to display local time by any of the following means:

a) A clock;

b) A date-time stamp that has the means to visually display the time; or

c) An automation system that complies with Section 17, Alarm Monitoring Automation Systems.

10.2 Each date-time stamp powered by 120-volt AC shall comply with the Standard for Time-Indicating and -Recording Appliances, UL 863, or with the Standard for Household Electric Clocks, UL 826.

10.3 One of the following means for recording local time and the day, month, and year shall be provided in each operating room, remote signal management center, redundant site, or subsidiary station:

a) A date time stamp when signals are processed manually or an automation system that is used to process signals and complies with 17.6.1 or 17.6.2.2; or

b) An automation system that is used to process signals and complies with 17.6.3 or 17.6.4.

10.4 The clocks and time stamps in an operating room, remote signal management center, and a redundant site that is staffed at all times shall be checked daily according to standard local time and, if necessary, reset.

10.5 The clocks and date-time stamps in a subsidiary station or a redundant site, unless they are occupied at all times, shall be checked monthly according to standard local time and, if necessary, reset. See 10.4.

10.6 When primary power has been restored after a power failure, any of the equipment listed below that is powered by primary power shall be checked against and, if necessary, reset to standard local time:

a) All clocks that display time in the operating room;

b) All date-time stamps in the operating room; and

c) All components of an automation system that complies with Section 17, Alarm Monitoring Automation Systems, are used to display or record time, and not automatically synchronized with the United States Naval Observatory's Atomic Clock when power is restored.

11 Power Supply

11.1 General

11.1.1 Electrical power for signaling equipment used in a station shall be provided by methods complying with 11.1.2 – 11.15A.6.

11.1.2 Operation of equipment from a secondary power source shall be indicated in the operating room when the switch over to the secondary source is made. This may be done either by an indicator light or by notification via the automation systems.

11.1.3 The configuration of the primary and secondary power sources shall be based on the following:

a) The manufacturer's specifications for power and the use of an uninterruptible power supply (UPS);

b) The results of the monitoring equivalent weight (MEW) calculation (See 5.2.36 and 17.2); and

c) The options for secondary power established in 11.5.1.

11.2 Installation

11.2.1 All power supply equipment (such as batteries, battery-chargers, overcurrent protection, rectifiers, switching facilities, transformers, voltage regulators, power conditioners, emergency generating equipment, uninterruptible power supplies (UPS), engine-driven generator transfer switches, and the like) and wiring shall comply with, and be installed in accordance with, the requirements of the National Electrical Code, NFPA 70, or as required by the local authority having jurisdiction, for such equipment. Where NFPA 70 is not used as the electrical code, power supply equipment shall be installed in accordance with the requirements of a published electrical code, as required by the local authority having jurisdiction, for such equipment.

11.3 Source

11.3.1 Two sources of power shall be provided for operation of the signaling equipment, and other associated equipment necessary for the ongoing operation of the station under all conditions.

11.4 Primary power supply

11.4.1 One primary power supply shall be provided. The primary power supply shall be used to operate the system under any condition except in the case of its failure. The supply shall have the capacity for the intended service and shall consist of:

a) A commercial light and power service; or

b) A permanently-installed, engine-driven generator.

11.5 Secondary power supply

11.5.1 A secondary (standby) supply shall be provided to supply energy to the entire load created by the equipment necessary for the operation of the station in the event of failure of the primary power supply. The secondary power supply shall consist of either:

a) When the MEW calculation is 999 or less, a storage battery or batteries of sufficient capacity to operate the load for a 24-hour period;

b) When the MEW calculation is 49,999 or less, a permanently-installed, automatic-starting, engine-driven generator having sufficient capacity to power the load and a storage battery/batteries or UPS with a 4-hour capacity; or

c) When the MEW calculation is 50,000 or greater, two or more permanently installed engine-driven generators. With the largest capacity engine-driven generator out of service, the remaining engine-driven generator(s) shall be capable of supplying power to operate the load. These generators may be configured in either of the following ways:

1) In a redundant configuration in which only one of the engine-driven generators will start and assume the load when the supply of primary power fails, and the remaining generator(s) will start and assume the load in the event of a failure of the first engine-driven generator. In this configuration a standby battery supply that complies with 11.6.1 shall be provided.

2) In a resilient configuration in which all of the engine-driven generators will start and assume the load when the supply of primary power fails. Once the supply of power to the load has been stabilized, the engine-driven generators that are not required to support the load may or may not continue to operate. In the event of the failure of any of the engine-driven generators that are supplying the load, the remaining engine-driven generators shall supply the needed power to the load. In this configuration, a standby battery supply that complies with 11.6.1 shall be provided. See Table 11.1.

d) When the MEW calculation is 100,000 or greater, a resilient configuration in which all of the engine-driven generators will start and assume the load when the supply of primary power fails shall be used. Once the supply of power to the load has been stabilized, the engine-driven generators that are not required to support the load may or may not continue to operate. In the event of the failure of any of the engine-driven generators that are supplying the load, the remaining engine-driven generators shall supply the needed power to the load. In this configuration, a standby battery supply that complies with 11.6.1 shall be provided. See Table 11.1.

Table 11.1
Secondary power configurations

MEW	# of units	# Auto start	#Assuming load	# Manual start	Capacity of batteries	1st fault	2nd fault
≤999	0	0	0	0	24 hr	Battery supply	None
≤49,999	1	1	1	0	4 hr[b]	Generator	4 hr battery
≥50,000	2	2	1	1	15 min[b]	Generator	Generator
≥50,000	2[a]	2	1	0	15 min[b]	Generator	Generator
≥100,000	2[a]	2	1	0	15 min[b]	Generator	Generator

[a] This is an N+ resilient-configuration in which two or more generators start at the same time with at least one assuming the load.

[b] The battery supply is intended to provide continuity of power during the transition between primary power and the generator(s) assuming the load, or between the first generator and the second generator(s) in the event of a failure of the first generator (See 11.6).

11.5.2 Provision shall be made to restore equipment used to provide secondary power to service within 72 hours by repair of the equipment or by its permanent or temporary replacement. This shall be accomplished by either:

a) Employees of the central station company that have been trained in the servicing of power systems; or

b) Under the terms of a written agreement with a service company that is skilled in the servicing of power systems.

11.5.3 Both the primary and secondary engine driven generators shall be monitored for critical operating functions including but not limited to, low fuel, start failure, over current, high temperature and low oil.

11.5.4 *Deleted*

11.6 Continuity of power supply

11.6.1 Rechargeable batteries of sufficient capacity to operate the maximum normal load of the equipment necessary for the operation of the station for a minimum of 15 minutes shall be provided if signals could be lost due to the transfer of power between the primary and secondary power supplies, or if signal receiving units require more than 30 seconds to reset. The rechargeable batteries shall assume the load in such a manner that no signals will be lost if the secondary power is supplied in accordance with:

a) 11.5.1 (a) or (b) and the transfer is made manually; or

b) 11.5.1(c).

11.6.2 If signals are not lost due to the transfer of power between the primary and secondary power supplies, the transfer shall be accomplished, either manually or automatically, within 30 seconds of loss of primary power. If more than 30 seconds is required, standby power in accordance with 11.6.1 shall be provided.

11.6.3 When the MEW calculation is 999 or less, the rechargeable batteries described in 11.6.1 are not required to be provided by a UPS (See 11.14A) or a UBS (See 11.15A) unless the use of such supplies is required by the specifications of the manufacturer of the equipment being used.

11.7 Storage batteries

11.7.1 Storage batteries shall be designed for stationary commercial or industrial applications in which they are subject to deep discharge or deep cycling and shall be located or enclosed so that signaling equipment cannot be affected by battery gases.

11.7.2 All cells shall be insulated against grounds and crosses, and shall be mounted so as to not be subject to mechanical damage. A rack, frame, or cabinet used to support a battery shall be protected against the corrosive effects of battery gases and liquids.

11.7.3 The concentration of battery gases shall be limited by sealed cell batteries that prevent the venting of gas or venting the power room or each enclosure that houses batteries to the outside atmosphere.

11.7.4 Batteries shall be marked with the date they were manufactured and the date of replacement based on the manufacturer's data for their life expectancy. The marking shall be on the batteries, displayed on the cabinet in which the batteries are housed, or on the control panel of a UPS to which the batteries are connected. Batteries shall be replaced sooner if tests indicate that they should be replaced.

11.7.5 Batteries shall be installed and maintained in accordance with the manufacturer's instructions for safety and continued operation. Local codes that apply to installation and safety concerns related to storage batteries shall be followed in accordance with the local authority having jurisdiction.

11.8 Overcurrent protection for external batteries

11.8.1 Batteries that are external to the equipment they power shall be protected by either:

a) Enclosed fuses or circuit breakers in the main discharging leads. The overcurrent protection shall be installed as close to the battery terminals as practical, or

b) Housed in a vented enclosure that protects the terminals and associated wiring from shorts, grounds or other conditions that could damage the batteries. Wiring between this enclosure and the equipment that is powered shall be housed in conduit, or EMT.

11.8.2 The current rating of the fuse or circuit breaker shall not be less than 130 percent of the current rating of the charging source. The maximum rating shall not be more than 250 percent of the maximum normal operating load or 200 percent of the current rating of the charging source, whichever is greater.

11.8.3 The overcurrent protection provided as a part of the equipment shall be used if it is an integral part of the equipment.

11.8.4 The rating of a fuse or circuit breaker used in the grounded side of a battery, if provided, shall not be less than twice the rating of the fuse or circuit breaker in the ungrounded side.

Exception: The rating of the circuit breaker in the grounded side may be less than twice the rating of the circuit breaker in the ungrounded side, but not less than that rating, if circuit breakers are used in both the ungrounded and grounded side, and they are mechanically linked (ganged) so that both will be opened if either one is operated.

11.8.5 At least two spare fuses and one spare circuit breaker for every rating that is in use shall be available at the station for replacement use.

11.9 Charging method

11.9.1 Provisions shall be made for charging a battery so that it is protected from damage due to any of the following:

a) An excessive rate of charge; or

b) The reversal of the supply current; or

c) The interruption of the supply current.

11.9.2 The spraying of the electrolyte shall be prevented while the battery is being charged by its charging source.

11.10 Trickle- or float-charged batteries

11.10 revised and relocated to 11.10A

11.10A Trickle- or float-charged batteries

11.10A.1 Battery chargers or DC power supplies of sufficient capacity shall be provided to supply power to all direct current circuits without overloading the charging equipment.

11.10A.2 A storage battery of sufficient capacity shall be connected across the line in such a manner that would normally charge the battery, or it shall be in a separate standby condition with an automatic switching means such that the battery would be transferred to operate the system upon failure of the primary power supply. Working circuits shall not be affected by the switchover to standby battery.

11.10A.3 If the DC source used to maintain the charge of the batteries is also used to operate the system to which the batteries are connected, it shall be capable of providing the maximum load with the battery fully discharged.

11.10A.4 The charging current for either a trickle or float-charged battery shall be such that a completely discharged battery is restored to the required operating charge within (See Table 11.2):

a) 48 hours for a battery intended to supply 24 hours of standby power, or

b) 24 hours for a battery intended to supply 4 hours or less of standby power.

Table 11.2
Battery testing and recharging

Supply time	Testing methods	Frequency	Maximum recharge time
24 hr	Discharge 30 min under normal load or tested per 11.14A.9	Monthly or mfr's recommended frequency	48 hr
4 hr	Discharge 5 min under normal load or tested per 11.14A.9	Monthly or mfr's recommended frequency	24 hr
15 min	Discharge 5 min under normal load or tested per 11.14A.9	Monthly or mfr's recommended frequency	24 hr

11.10A.5 Storage batteries that are intended to supply 24 hours of standby power shall be tested either:

a) Monthly by a 30-minute, normal operating load discharge test; or

b) On a frequency established by the battery manufacturer.

In either case, the average voltage per cell shall not be permitted to drop below the manufacturer's recommended level.

11.10A.6 The discharge test for a battery intended to supply 4 hours or less of standby power shall be tested either:

a) Monthly by a 5-minute, normal operating load discharge test; or

b) On a frequency established by the battery manufacturer.

The average voltage per cell shall not be permitted to drop below the manufacturer's recommended level.

11.10A.7 Where the batteries are connected to an Uninterruptible Power Supply (UPS) that can conduct a self-test in accordance with 11.14A.8, that test method may be used in lieu of the discharge test methods described in 11.10A.5 and 11.10A.6.

11.10A.8 A record of the test described in 11.10A.5 and 11.10A.6 and the results shall be created and maintained for a minimum period of 12 months.

11.11 Battery chargers and DC power supplies

11.11.1 Battery chargers and DC power supplies shall comply with the Standard for Power Supplies for Fire-Protective Signaling Systems, UL 1481; the Standard for Industrial Battery Chargers, UL 1564; or the Standard for Power Units Other Than Class 2, UL 1012.

Exception: This requirement does not apply to battery chargers used to maintain the starting battery for an engine driven generator. See 11.12A.11.

11.11.2 Preventive maintenance shall be performed on a battery charger or DC power supply as specified by the manufacturer. The maintenance may be provided under a service contract or by trained central station personnel.

11.12 Stationary, engine-driven generators

11.12 revised and relocated as 11.12A

11.12A Stationary, engine-driven generators

11.12A.1 The installation of a stationary combustion engine shall comply with the requirements of the Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines, NFPA 37, as applied by the local authority having jurisdiction.

11.12A.2 The generator units shall be of sufficient capacity to be able to power all of the equipment that is essential to the operation of the station under the maximum normal load conditions. This shall include any necessary heating, air conditioning, ventilation equipment (HVAC), network equipment, uninterruptable power supplies, standby lighting, communication equipment, and the like, needed in support of the monitoring function.

11.12A.3 The station shall:

a) Maintain a current list of all the equipment and facilities that are powered by the engine-driven generator(s) and their loads; or

b) Determine the load by operating the engine-driven generator(s) with all the intended equipment and facilities powered from it (See 11.12A.9).

11.12A.4 Preventative maintenance shall be performed on an engine-driven generator as specified by the manufacturer. The maintenance may be provided under a service contract or by trained central station personnel.

11.12A.5 The central station shall have an operator trained in the use of any engine-driven generators that are used to provide secondary power on duty at all times, unless the requirements of 11.6.1 – 11.6.2 are met.

11.12A.6 The staff in the operating room shall be automatically notified when any engine-driven generator that is used to provide secondary power to the central station is operating. Such notification may be an audible or visual signal, an electronic message displayed by the automation system, or an equivalent means.

11.12A.7 An engine-driven generator shall be located so that the noise, vibration, fumes, heat, and the like, of its operation shall not interfere with the handling of signals and other duties in the operating room and other functions of the station.

11.12A.8 Fuel shall be stored in accordance with local codes or requirements from the local authority having jurisdiction.

11.12A.9 When the fuel source is not natural or manufactured gas that is supplied through utility mains, sufficient fuel shall be maintained so as to provide for 12 hours of operation at full-load provided a reliable source of supply is available at any time on 2 hours' notice. If a source of supply is not reliable or readily available, a supply sufficient for 24 hours of operation shall be maintained.

11.12A.10 If the fuel, such as gasoline, used to power the engine deteriorates with age it shall be frequently replenished, or otherwise maintained to ensure it is always fresh.

11.12A.11 A separate storage battery and an automatic battery charger which maintains the battery charge by cycling between charge mode and stand-by mode shall be permanently installed for starting the engine-driven generator. The charger shall comply with the Standard for Battery Chargers for Charging Engine-Starter Batteries, UL 1236.

11.12A.12 Each engine-driven generator used by a central station, or a remote signal management center that is occupied at all times shall be tested under maximum normal load or through the use of a load bank that has been sized based on the information described in 11.12A.3(a) per one of the following schedules:

a) Operated under maximum normal load for a period of 30 continuous minutes at a scheduled time every 7 calendar days; or

b) Where the installation of the generator complies with the Standard for Emergency and Standby Power Systems, NFPA 110 operated under maximum normal load for a period of 30 continuous minutes at a scheduled time every 30 calendar days.

In either case a record of the test and results shall be created and maintained for a minimum period of 12 months.

11.13 Security of secondary power supplies

11.13.1 Engine-driven generators, power supplies, or batteries that are located in an area of the building not occupied at all times by station personnel, shall be located in a room that is locked and has all movable openings supervised with contacts or the equivalent monitored in the operating room. Openings in the walls, ceiling, or floor that exceed manhole size [96 square inches (619 cm^2) with the smallest dimension exceeding 6 inches (152 mm)] shall be protected with bars or screening as specified in 11.13.2 (a) or (b).

11.13.2 An engine-driven generator, power supply, or battery located in an area of the building that cannot be locked shall be enclosed by one of the following means:

a) A mesh constructed either of expanded sheet steel at least 0.053 inch (1.4 mm) thick, or 10 AWG (0.102 inch diameter) (5.3 mm^2) steel wire, or an equivalent material. Any opening in the mesh shall not be wider than 2 inches (51 mm) when measured in any direction; or

b) A sheet metal enclosure using either steel or aluminum. Sheet steel shall have a minimum thickness of 0.032 inches (0.81 mm) and shall be provided with corrosion protection by painting, plating, or the equivalent. Sheet aluminum shall have a minimum thickness of 0.045 inch (1.14 mm). All removable panels shall be secured by lock and supervised with contacts by the station.

11.13.3 Openings in the sheet metal enclosure described in 11.13.2(b) intended for air flow and the like shall be protected with a mesh complying with the requirements in 11.13.2(a).

11.13.4 Gaps in the perimeter of the mesh barrier shall not exceed 6 inches (152 mm). The space between the barrier and wall, floor, or ceiling shall not exceed 6 inches. The spacing to the ceiling may exceed 6 inches if the mesh barrier extends to a height of 8 feet (2.44 m) and is topped with three horizontal strands of barbed wire or razor ribbon coils, or if the mesh shall be arranged to form a top that extends horizontally across the barriers.

11.13.5 The gate(s) or door(s) into the enclosure described in 11.13.2 shall be locked and supervised with contacts or the equivalent monitored in the operating room.

11.13.6 An engine-driven generator located outdoors shall be housed in a sheet metal enclosure using either steel or aluminum. Sheet steel shall have a minimum thickness of 0.032 inches (0.81 mm) and shall be provided with corrosion protection by painting, plating, or the equivalent. Sheet aluminum shall have a minimum thickness of 0.045 inches (1.14 mm). Openings intended for air flow and the like shall be protected with a mesh complying with the requirements specified in 11.13.2(a). All removable panels shall be secured by lock and supervised with contacts by the station or the equivalent monitored in the operating room.

11.13.7 If the engine-driven generator is located at grade level or on a structure that is below 18 feet (5.5 m) from grade level, it shall be enclosed by one of the following means:

a) A sheet metal enclosure that complies with 11.13.6; or

b) A mesh barrier that complies with 11.13.2(a) – 11.13.5 in lieu of locking and contacting the access panels required in 11.13.6. The barrier shall extend to a height of at least 8 feet (2.44 m) and shall be topped by three horizontal strands of barbed wire or razor ribbon coils, or the mesh shall be arranged to form a barrier that extends horizontally across the barriers. The opening between the bottom edge of the mesh and a surface of concrete or asphalt shall not exceed 6 inches (152 mm). If the surface below the bottom edge of the mesh is not concrete or asphalt, there shall be no opening between the bottom edge of the mesh and the surface.

11.13.8 If the engine-driven generator is located on a roof that is above 18 feet (5.5 m) and not otherwise accessible and defined by the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681 shall be protected as follows:

a) Where access to the roof is not within the central station a sheet metal enclosure that complies with 11.13.6; or

b) Where access to the roof is within the central station but not within notice of the operators, the means of access shall be locked and supervised by contacts in lieu of locking and contacting the access panels described in 11.13.6.

11.13.9 The location of all shut-off valves for the fuel supply to an engine-driven generator that are within 100 feet (30.48 m) of the generator shall be known to the operators and there shall be a written procedure for checking the valves in the case of fuel shut-off. The valves may be electrically supervised by the station with intrusion detection equipment, video surveillance equipment and the like, or housed in a locked enclosure where permitted by local codes.

11.13.10 *Deleted*

11.14 Uninterruptible power supply (UPS) units

11.14 revised and relocated as 11.14A

11.14A Uninterruptible power supply (UPS) units

11.14A.1 When equipment used to receive and process signals in a station is required to have an uninterrupted source of alternating current (AC), a UPS shall be provided. A UPS shall comply with the Standard for Power Supplies for Fire-Protective Signaling Systems, UL 1481, or the Standard for Uninterruptible Power Systems, UL 1778.

11.14A.2 All UPS systems shall be designed to run on engine driven generator power.

11.14A.3 When the MEW calculation is 100,000 or greater, secondary power shall be provided by either a single UPS unit that is constructed so that all components are duplicated, or with multiple UPS units that are arranged so that a single failure of any UPS unit does not interrupt the ability of the alarm monitoring automation system to process signals.

11.14A.4 The UPS capacity shall be configured in accordance with 11.5.1 and 11.6.1.

11.14A.5 The station shall:

a) Maintain a current list of all the equipment and facilities that are powered by the UPS and their loads; or

b) Determine the load by operating the UPS with all the intended equipment and facilities powered from it and then recording the existing load information.

11.14A.6 In order to perform maintenance and repair service, a means for disconnecting the input and output to a UPS shall be provided. One of the following methods shall be employed:

a) A manual bypass switch that does not interrupt continuity of power to the UPS load when operated; or

b) The UPS and any equipment that constitutes the UPS's load shall be duplicated and connected to a separate branch circuit supply. Any automation equipment shall be capable of being brought into service within 5-1/2 minutes; or

c) Any other method that allows a UPS to be taken out of service without interrupting power to the load that it supplies.

11.14A.7 All batteries connected to a UPS shall meet the specifications of the manufacturer of the UPS.

11.14A.8 Unless the UPS system can perform a self-test designed to determine the actual run time when the system is powered by the batteries, the testing of the UPS batteries shall be in compliance 11.10A.5 and 11.10A.6. See Table 11.2.

11.14A.9 Where the UPS system can perform a self-test designed to determine the actual run time the test shall be run at a minimum one every 7 consecutive days. The results of the test shall be verified by either a Simple Network Management Protocol (SNMP) generated by the UPS system, and email generated by the UPS system or similar method that creates a record of the results of the test.

11.15 Uninterruptible battery supply (UBS) units

11.15 deleted

11.15A Alternative secondary power sources

11.15A.1 Where alternative sources of secondary power not described in this standard are utilized they shall be configured in accordance with the following:

a) Installed and maintained as an engine-driven generator where an internal combustion engine such as an uninterruptible battery supply, diesel rotary uninterruptible power supply (DRUPS), and the like is utilized, see 11.12A and 11.13; or

b) Installed and maintained as storage batteries where the charging source is supplied by a renewal energy source such as windmills, photovoltaic cells, and the like are utilized (See 11.7 – 11.10A).

11.15A.2 The station shall:

a) Maintain a current list of all the equipment and facilities that will be powered by the alternate power source and their loads; or

b) Determine the load by operating the alternate power source with all the intended equipment and facilities power from it (See 11.12A.3).

11.15A.3 Where an internal combustion engine described in 11.15A.1(a) is used it shall be tested in accordance with 11.12A.4.

11.15A.4 Preventative maintenance and testing of batteries installed as part of a UBS described in 11.15A.1(a) shall be done in accordance with 11.7.5 and 11.10A.4, or 11.10A.5 respectively.

11.15A.5 Where storage batteries described in 11.15A.1(b) are used they shall be tested in accordance with 11.10A.5 or 11.10A.6 based on the minimum time they are intended to provide power.

11.15A.6 Preventive maintenance of the charging source supplied by a renewal energy source described in 11.15A.1(b) shall be performed as specified by the manufacturer. The maintenance may be provided under a service contract or by trained central station personnel.

11.16 Electrical transient protection

11.16.1 Supply line protection

11.16.1.1 The automation system hardware and other computer based equipment necessary for the operation of the central station shall have their primary power source protected by surge protective devices (SPD) that comply with the Standard for Surge Protective Devices, UL 1449. The SPD shall have a Maximum Continuous Operating Voltage (MCOV) equal to or greater than the normal operating voltage of the system. The SPD Type Designation (Type 1, 2, or 3) shall be suitable for the specified installation application. Where primary power source is protected with an SPD that is a component of the power source, the source shall comply with the Standard for Surge Protective Devices, UL 1449.

11.16.2 Signaling & communication line transient protection

11.16.2.1 Electronic equipment used for the receipt and/or processing signals from protected properties shall be protected against transient surges. These protectors shall comply with the requirements in the Standard for Protectors for Data Communication and Fire Alarm Circuits, UL 497B, or the Standard for Secondary Protectors for Communications Circuits, UL 497A, as appropriate. The transient protectors shall have a marked rating of 50 volts or less.

Exception No. 1: When all of the equipment connected to the automation system is located in the same room as the automation system and is not more than 25 feet (7.62 m) apart, and is not connected to the telecommunications network, isolated loop circuit protection is not required.

Exception No. 2: Transient voltage surge protection is not required for fiber optic circuits.

11.16.2.2 Communication circuits connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A. These protectors shall be used only in the protected side of the telecommunications network. The transient protectors shall have a marked rating of 150 volts or less.

12 Communication Infrastructure

12.1 General

12.1.1 Communication paths such as cables of wire or optic fiber, antennas or other wireless methods, and equipment such as switches, routers, computers and the like through which signals, data or voice communication pass to and from the operating room, a remote equipment room, a remote signal management center, a subsidiary station, or a redundant site shall comply with this Section.

12.1.2 The installation of leased or other cables of wire or optic fiber shall employ standard communication industry operating practices. For requirements pertaining to protectors on each circuit, aerial or underground, refer to the National Electrical Code, NFPA 70, as applied by the local authority having jurisdiction. Where National Electrical Code, NFPA 70 is not used as the electrical code, power supply equipment shall be installed in accordance with the requirements of a published electrical code, as required by the local authority having jurisdiction, for such equipment.

12.1.3 The cables carrying signaling and communication circuits into the station from utility poles or underground routes shall be protected against damage that could impair or prohibit the delivery of central station services by the methods specified in 12.2.1 – 12.4.5.

12.1.4 The cables carrying signaling and communication circuits into the station from antennas and other wireless equipment shall be protected against damage that could impair or prohibit the delivery of central station services by the methods specified in 12.5.1 – 12.5.9.

12.1.4A Areas within the central station, a remote signal management center, subsidiary station, or redundant site through which cables are routed or communication equipment is located shall not be used to house combustible materials or have a known risk of fire.

12.1.5 Communication equipment located at the central station, a remote signal management center, subsidiary station, or redundant site that is used to route signal traffic to or from protected properties and voice communication related to the monitoring, signal processing, retransmission and the like to and from operators shall comply with 12.7.

12.1.6 If the central station receives signals from monitored alarm systems that are transmitted with either a packet switched data network or a managed facilities based voice network the station shall utilize communication services that deliver geographically diverse signal pathways, if possible by:

a) Utilizing two independent internet service providers (ISP) or two independent managed facilities based voice network (MFVN) providers or;

b) Utilizing one internet service provider (ISP) or one managed facilities based voice network (MFVN) provider that provides contracted diverse signal pathways arranged so that the pathways are not likely to be affected by the same natural or man-made disasters or single point of failure.

12.1.7 If the central station utilizes managed facilities based voice network (MFVN) for voice telephone communication, the station shall utilize communication services that deliver geographically diverse signal pathways, if possible, by:

a) Utilizing two independent managed facilities based voice network (MFVN) providers or;

b) Utilizing one managed facilities based voice network (MFVN) provider that provides contracted diverse signal pathways arranged so that the pathways are not likely to be affected by the same natural or man-made disasters or single point of failure.

12.2 Underground entrance

12.2.1 Underground communication cables entering the building housing the station shall be rated for underground service and shall have mechanical protection where necessary to protect against damage that may impair or prohibit the delivery of central station services. The mechanical protection shall be provided by rigid metal electrical conduit, electrical metallic tubing, masonry encasement that is at least 3 inches (76 mm) thick, or shall be at least 18 inches (0.45 m) below the grade surface or under a paved street or sidewalk (concrete or asphalt).

12.2.2 *Deleted*

12.2.3 Manholes, covered cable vaults, and pedestal enclosures, and the like within 50 ft (15.24 m) of the building housing the station, and which provide access to the communication cables entering the station, shall be known to the operators and be protected in a manner that restricts ready access to the cables. Restrictions may be achieved through such methods as:

a) The use of locking mechanisms; or

b) Securing hardware that requires the use of specialized tools which are notreadily available; or

c) Layers of complementary security controls which restrict access to the cablesand which are monitored in the operating room by video cameras or other electronic security means; or

d) Other means that provide notice to the operators when access to the areahousing the cables is made.

12.3 Overhead entrance

12.3.1 Overhead communication cables entering the building housing the station shall be at least 18 ft (5.5 m) above grade. The location of communication cables that enter the building at a point that is less than 18 ft above grade of the building housing the station shall be known to the operators and be protected in a manner that restricts ready access to the cables. Restrictions may be achieved through such methods as:

a) Provided with mechanical protection in the form of rigid metal electrical conduit or electrical metallic tubing; or

b) Covered with a sheet steel guard fixed in place with securing hardware that requires the use of specialized tools which are not readily available; or

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

d) Other means that provide notice to the operators when access to the area housing the cables is made.

12.3.2 Communication cables routed from overhead to underground on a pole or similar fixture that is within 50 ft (15.24 m) of the building housing the station shall be protected by any of the methods in 12.3.1.

12.4 Communication cables inside the building

12.4.1 Communication cables that are not in an area under the control of the station shall not be marked to identify them as serving the station.

12.4.2 Communication cables located inside a multiple-occupancy building housing the station, but outside of areas under control of the station shall be provided with protection by:

a) Any of the methods described in 12.3.1; or

b)Entirely concealed within building walls, floors, or ceilings that are fixed inplace in such a manner that access to the cables cannot be made without breaking or otherwise destroying the enclosing surfaces(s). Lift-out ceiling panels and similar materials are not considered fixed in place.

12.4.3 *Deleted*

12.4.4 *Deleted*

12.4.5 *Deleted*

12.5 Antenna cable – Located at the Central Station

12.5.1 For requirements pertaining to protectors on each antenna circuit, refer to the National Electrical Code, NFPA 70, as applied by the local authority having jurisdiction. Where NFPA 70 is not used as the electrical code, power supply equipment shall be installed in accordance with the requirements of a published electrical code, as required by the local authority having jurisdiction, for such equipment.

12.5.2 An antenna cable connecting a radio antenna to radio receiving and/or transmitting equipment in a station shall be protected against mechanical damage and attack by the methods specified in 12.5.3 – 12.5.11.

12.5.3 An antenna cable that is routed down an antenna tower or mast which is mounted at grade level or on structures that are below 18 ft from grade shall be protected by any of the methods described in 12.3.1.

12.5.3A If the base of the tower or mast facilitates climbing without the use of ladders or other tools the antenna cable shall be housed for its entire length or the base of an antenna tower or mast shall be protected as follows:

a) A barrier constructed of a mesh of either expanded sheet steel at least 0.053 inch (1.4 mm) thick, or 10 AWG (0.102 inch diameter) (5.3 mm^2) steel wire, or an equivalent material, extending to a height of at least 8 ft (2.44 m), topped by three horizontal strands of barbed wire or razor ribbon coils. Any opening in the mesh of the barrier shall not be wider than 2 inches (51 mm) when measured in any direction;

b) The barrier shall not be within 3 ft of the antenna cable that is routed on the tower or mast; and

c) The opening between the bottom edge of the barrier and a surface of concrete or asphalt shall not exceed 6 inches (152 mm). If the surface below the bottom edge of the barrier is not concrete or asphalt, there shall be no opening between the bottom edge of the barrier and the surface; or

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

e) Other means that provide notice to the operators when access to the area housing the cables is made.

12.5.4 If the antenna tower or mast described in 12.5.3 is located next to a building or other structure that would facilitate passing over the barrier, the cable shall be protected from such an access by either of the following:

a) A mesh of the same material as described in 12.5.3(a) shall be mounted across the top of the barrier in a manner that does not facilitate access to the antenna cable;

b) The cable shall be housed in ridged conduit or electrical metallic tubing to a height of 18 ft (5.5 m) above a point at which the tower or mast may be climbed without the use of ladders or other tools; or

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

d) Other means that provide notice to the operators when access to the area housing the cables is made.

12.5.5 An antenna cable that is routed across a roof or down a roof mounted antenna tower or mast where the roof surface is 18 ft (5.5 m) above grade and not otherwise accessible is defined by the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, shall be protected as follows:

a) Where access to the roof is not within the central-station:

1) The cable shall be housed in ridged conduit or electrical metal tubing to a height of 18 ft (5.5 m) above the roof surface; or

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

3) Other means that provide notice to the operators when access to the area housing the cables is made.

b) Where access to the roof is within the central-station but not within notice of the operators:

1) The means of access shall be locked and supervised.

12.5.6 An antenna cable routed down a pole or the side of a building within 50 ft (15.2 m) of the building housing the station shall be protected by:

a) Rigid metal electrical Conduit, electrical metallic tubing, or a sheet steel guard; or

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

c) Other means that provide notice to the operators when access to the area the cables is made.

12.5.7 An antenna cable that is not in an area under the control of the station shall not be marked to identify it as serving the station.

12.5.8 An antenna cable inside a multiple-occupancy building housing the station, and which is outside of the part of the building housing the station itself shall be provided with electrical or mechanical protection.

12.5.9 Electrical protection shall consist of:

a) A protective circuit surrounding the cable;

b) Motion detection or the equivalent, in the area of the conductors, adjusted to comply with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681;

c) Complete protection of all moveable openings leading into areas containing the cable in accordance with the requirements in UL 681; or

d) Protection of each area through which the cable passes, in accordance with the requirements for Extent No. 3 in UL 681.

12.5.10 An antenna cable that is concealed by the building structure does not require electrical protection or additional mechanical protection, if the building structure must be damaged or destroyed to gain access to the cable. This does not apply to lift-out drop ceiling panels or removable wall or floor panels.

12.5.11 All electrical protection shall be monitored by the station.

12.6 Communication equipment

12.6.1 All communications equipment shall comply with the applicable UL Standard that applies to the equipment in question.

12.6.2 Communication equipment used to route signaling from protected properties and the central station shall be equipped with secondary power in accordance with 11.5 – 11.15A.

12.6.3 Communication equipment shall be configured so that a single point of failure will not prohibit signals or voice communication from being handled by the central station. This shall be accomplished by either of the following:

a) Spare communication equipment of equal size as the failed unit that can be brought into service within 30 seconds; or

b) The communication equipment shall have all key components duplicated within the unit.

Such spare equipment does not eliminate the requirement for the wireless voice communication device in 19.1, 28.1, and 43.1.

12.6.4 The failure of any communication equipment shall be indicated to the operators by audible or visual means.

12.6.5 Voice communication circuits shall be configured so that a failure of a single circuit results in all inbound and outbound traffic to that circuit to be automatically rerouted to an alternate circuit. Voice communication circuits serving central stations with a MEW factor (See 5.2.27) of 100,000 or greater shall have the means of being redirected to a redundant site.

12.7 Disruption of communications

12.7.1 See Section 50, Reaction to Communications Disruptions.

13 Subsidiary Stations

13.1 A subsidiary station shall be connected to a central station or residential monitoring station by:

a) Two or more supervised channels, any one of which can be used to operate the system; or

b) By a supervised channel and a backup channel that is made through a MFVN dial-up network.

c) These channels shall meet the applicable requirements of 17.12.

The connection through the dial-up channel shall be tested weekly by operating through the dial-up channel for 5 minutes or more. A record shall be made of the test.

13.2 The connection between the receiving units at a subsidiary station and the equipment transmitting signals to the staffed central station or residential monitoring station, shall be supervised so that a trouble signal is transmitted to the staffed station if the connection is faulted.

13.3 The switch-over to the standby channel, either supervised or dial-up, shall be made within 90 seconds after the loss of the primary channel.

13.4 If all the channels between a subsidiary station and staffed station are lost, any signals received by the subsidiary station shall be automatically recorded or stored until the subsidiary station can be staffed or the channels restored.

13.5 A subsidiary station shall be equipped so that it can be staffed and operated as a central station or a residential monitoring station.

13.6 The number of individuals required to monitor the alarms systems that send signals to the subsidiary station shall be identified. Sufficient workstations that are equipped with single party telephone communication means and any specialized equipment needed to process signals shall be available to

such personnel. This determination shall be reassessed at least once every 12 consecutive months. If the reassessment determines increase in the number of individuals is needed, there shall be a corresponding increase in the number of workstations.

13.7 A subsidiary station shall be staffed by qualified operating personnel within one hour after the central station or residential monitoring station has determined that all contact has been lost and signals cannot be received from the subsidiary station. The following steps shall be taken to establish operation as a center station:

a) Once staffing has occurred they shall catch-up to handling current signals in "real-time" within one hour of their arrival;

b) Only alarms and trouble signals shall be required to be handled during the staffed period;

c) Signals shall be reviewed to determine the prioritization of response to any alarm signals indicating Life safety, hold Up and burglary to be handled first followed by other types of signals which will be handled on a "first in-first out" basis, including the "catch-up period";

d) Signal handling shall be recorded and available as indicated in Records, Sections 24 and 40.

e) Database availability shall be assured through local physical files or no less than two distinct sources that are immediately available, organized, and not more than one week old;

13.8 Equipment used in a subsidiary station for burglar-alarm service shall comply with the requirements in the Standard for Central-Station Burglar-Alarm Units, UL 1610, or the Standard for Digital Alarm Communicator System Units, UL 1635. Equipment used in a subsidiary station for fire-alarm service shall comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

13.9 A subsidiary station shall be protected by a burglar-alarm and an automatic fire-alarm system whose signals are transmitted to the station it is connected to. The automatic fire-alarm system shall comply with the National Fire Alarm and Signaling Code, NFPA 72. The burglar-alarm system shall comply with the requirements for 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. See 7.9.

13.10 The power and environmental control systems of a subsidiary station shall be monitored by the station to which it is connected.

13.11 A subsidiary station shall be inspected once a month by central station or residential monitoring station personnel or their authorized agents to verify the operation of all equipment, telephones, battery conditions, and, if used, engine-driven generators.

13.12 The subsidiary station shall be equipped with any of the following resources which are to be placed into service if the telephone service described in 13.6 becomes inoperative:

a) An equivalent means of voice communication that is independent of the telephone communication means that are connected between the subsidiary station and the serving telephone company exchange;

b) Wireless voice communication devices that utilize standard industry equipment and licensed for commercial use;

c) Two or more communication lines which can be placed into service within 90 seconds of a failure of the lines that are normally used, and which enter the station at locations that are physically separated and communicate to different telephone company exchanges; or

d) Personnel who staff the subsidiary station shall be so equipped and trained to bring the wireless voice communication devices to the station.

13.13 There shall be a written plan of action for the restoration of service by a subsidiary station. The plan shall include the following;

a) Foreseeable disasters: Possible natural and man-made disaster threats, national and local, that could affect the station;

b) Emergency names list: A notification list that includes the names and the telephone numbers at work, home, vacation home, and the like, and home addresses of management, technical, operators, runners, and other relevant personnel;

c) Equipment vendor contacts: The 24-hour telephone and fax numbers of the vendors, technical assistance providers, and maintenance contractors of the equipment used in the station;

d) Municipal agency contacts: Emergency telephone numbers for local municipal agencies, such as the fire and police departments, to be called for help;

e) Utility contacts: Formalized emergency procedures and 24-hour contact names and telephone numbers of the utility and telephone companies serving the station;

f) If an engine-driven generator(s) is used that requires on-site fuel storage, there shall be a 24-hours a day contact and telephone number for a source of fuel re-supply;

g) Relocation center: If a relocation center is provided for, information on the location of the center, how to get there, how to put the center into operation, and 24-hour emergency management contact names and telephone numbers;

h) The processes, people, and who is responsible for what, in a form easily understandable by those who are required to perform the manual manning procedure(s); and

i) Disruption of communications between either monitored alarm systems or the voice communication to the central station or others.

(See Section 50, Reaction to Communications Disruptions).

13.14 Supervisory personnel and designated employees shall be familiar with the plan and shall know the location of a copy of the plan that is kept at the station or in another location, immediately available, which is clearly noted in the subsidiary station for all to see. The implementation of the plan shall be practiced annually to assure that all personnel know their responsibilities in case of an emergency, thus providing the opportunity to evaluate the current plan, making any changes that are recognized as needed.

13.15 The plan shall be reviewed and updated every six months and current copies shall be kept in designated and accessible locations.

14 Remote Signal Management Center

14.1 A remote signal management center shall meet all of the applicable requirements of the facilities and equipment sections of this Standard except Section 16, Receivers.

14.2 A remote signal management center shall be connected to a central station or residential monitoring station by two or more independent supervised channels that are used to send alarm monitoring data.

a) Each of these channels shall have the capacity to support the full operation of the center;

b) Each of these channels shall meet the applicable requirements of 17.12; and

c) Where possible, these channels shall be provided by independent communication companies or shall enter the building at separate locations.

14.3 The connection used for sending alarm monitoring data between the central station or residential monitoring station and the remote signal management center shall be supervised so that a trouble signal is displayed at both the remote signal management center and the facility to which it is connected if the connection is impaired.

14.4 The switch-over to the standby channel shall be made within 90 seconds after the loss of the primary channel.

14.5 The failure of any of the equipment shall be annunciated at the remote signal management center and the staffed central-station. Switchover to the alternate equipment shall be made automatically within 90 seconds.

14.6 The central station or residential monitoring station from which the remote signal management center receives signals shall have the means to determine that alarm monitoring data is being processed and shall resume processing signals when needed.

14.7 If all the channels between a remote signal management center and staffed station are lost, the central station or residential monitoring station shall resume monitoring all signals.

14.8 When actively processing signals, a remote signal management center shall be staffed by a minimum of two operators.

14.9 Equipment used in a remote signal management center shall comply with the requirements of the same Standard as the alarm monitoring automation system that is used in the central station or residential monitoring station (See 17.1). The display of alarm monitoring data and actions used to process the data shall not be different than the display and actions used in the central station or residential monitoring station.

14.10 The operation of all equipment, telephones, or other voice communication equipment used in conjunction with the processing of signals, battery conditions and, if used, engine-driven generators shall be inspected and tested in accordance with the applicable sections of this Standard.

14.11 A remote signal management center shall be equipped with a wireless voice communication device utilizing standard industry equipment and licensed for commercial use or an equivalent means of voice communication that is independent of the telephone cable that is connected between the remote signal management center and the serving wire center of the telephone company, unless multiple pathways, entering via different physical locations, to multiple wire centers are provided by the telephone company and can be placed into service within 90 seconds.

14.12 There shall be a written plan of action for the restoration of service by a remote signal management center. The plan shall include the following:

a) Foreseeable disasters: Possible natural and man-made disaster threats, national and local, that could affect the station;

b) Emergency names list: A notification list that includes the names and the telephone numbers at work, home, vacation home, and the like, and home addresses of management, technical, operators, runners, and other relevant personnel;

c) Equipment vendor contacts: The 24-hour telephone and fax numbers of the vendors, technical assistance providers, and maintenance contractors of the equipment used in the station;

d) Municipal agency contacts: Emergency telephone numbers for local municipal agencies, such as the fire and police departments, to be called for help;

e) Utility contacts: Formalized emergency procedures and 24-hour contact names and telephone numbers of the utility and telephone companies serving the station;

f) If an engine-driven generator(s) is used that requires on-site fuel storage, there shall be a 24-hours a day contact and telephone number for a source of fuel re-supply;

g) Relocation center: If a relocation center is provided for, information on the location of the center, how to get there, how to put the center into operation, and 24-hour emergency management contact names and telephone numbers;

h) The processes, people, and who is responsible for what, in a form easily understandable by those who are required to perform the manual manning procedure(s); and

i) Disruption of communications between either monitored alarm systems or the voice communication to the central station or others.

(See Section 50, Reaction to Communications Disruptions).

14.13 Supervisory personnel and designated employees shall be familiar with the plan and shall know the location of a copy of the plan that is kept at the center or in another location, immediately available, which is clearly noted in the remote signal management center for all to see. The implementation of the plan shall be practiced annually to assure that all personnel know their responsibilities in case of an emergency, thus providing the opportunity to evaluate the current plan, making any changes that are recognized as needed.

14.14 The plan shall be reviewed and updated every six months, and current copies shall be kept in designated and accessible locations.

14.15 Upon annual inspection, the performance of the remote signal management center shall be included with the central station(s) that the remote signal management center supports. The performance and compliance of a remote signal management center shall be the responsibility of the management central station or residential monitoring station for which it receives alarm monitoring data.

15 Equipment

15.1 Equipment used in a station shall comply with the requirements for that equipment.

15.2 Equipment shall be mounted or installed where it is least subjected to vibration, jarring, and conditions leading to mechanical damage.

15.3 Wiring to protective equipment shall be connected through distribution panels with marked terminals to facilitate rapid transfer of lines from defective units to reserve units when necessary.

15.4 For direct-wire and code-transmitter receiving units, each station shall have two or more audible signal units which may be disabled if the station uses an automation system to process signals. One of the audible signal units may be a reserve, if it can be placed in service within 1 hour.

15.5 Each multiplex receiver, digital alarm communicator receiver, and similar receiver shall have an audible signal that annunciates the receipt of a signal requiring the attention of an operator. The audible signal(s) may be disabled if the station uses an automation system to process signals.

15.6 Wiring connection shall be made to appropriate terminals. Connecting wire shall have the current-carrying capacity and insulation for the service to which it may be subjected. It shall be laced or cabled and protected against physical damage and abrasion by conduit, raceway, or the equivalent.

15.7 If the instructions for alarm-receiving equipment or automation system equipment indicate that it is to be used in a controlled environment where the ambient temperature is to be maintained between 13 and 35°C (55 and 95°F), the area of the station where such equipment is located shall be equipped with a heating, ventilating, and air-conditioning system that maintains that temperature range. The standby power system shall be capable of powering the heating, ventilating, and air-conditioning system for 24 hours or more. The standby power for the heating, ventilating, and air-conditioning system may be supplied by an engine-driven generator alone.

15.8 When required tests of equipment are made, a record of the test shall be made.

16 Receiver Units

16.1 Direct-wire burglar-alarm systems

16.1.1 General

16.1.1.1 Direct-wire burglar-alarm systems shall comply with the requirements for direct-wire alarm units in the Standard for Central-Station Burglar-Alarm Units, UL 1610.

16.1.2 Direct-wire burglar-alarm receiver units

16.1.2.1 Spare direct-wire receiving units shall be kept at each station and arranged so that they can be placed in service within 1 hour.

16.2 Code (McCulloh) transmitter systems

16.2.1 General

16.2.1.1 Code transmitter systems shall comply with the requirements for code transmitter alarm units in the Standard for Central-Station Burglar-Alarm Units, UL 1610. Such equipment used for fire-alarm service shall comply with the requirements for code transmitter alarm units in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

16.2.1.2 Connection between the subscriber's protective wiring and the receiving unit at the station shall be made by means of a code transmitter that is connected to the subscriber's control unit or is an integral part of the control unit.

16.2.2 Receiving units

16.2.2.1 Code signals shall be received at the central-station or residential monitoring station and recorded on a tape register or other recording instrument that complies with the Standard for Central-Station Burglar-Alarm Units, UL 1610, or the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864. Each station line circuit shall include at least one recording instrument.

16.2.2.2 An audible signal shall sound while a code signal is being received. An audible signal connected in common to more than one switchboard unit may be used for this purpose.

16.2.2.3 Each line circuit shall be provided with a visual signal that is activated while a signal is being received from any equipment on its circuit. The circuit from which the signal is being transmitted shall be identifiable under this arrangement.

16.2.3 Burglar-alarm service

16.2.3.1 Not more than 15 active burglar-alarm code transmitters shall be connected to one circuit. Each code transmitter shall send an individual signal readily distinguishable from the signal of any other code transmitter on the same circuit. See Table 16.1.

Table 16.1
Number of code transmitters allowed on a circuit

Normal transmitters		Non-clash transmitters	
active	inactive	active	inactive
15	0	45	0
14	10	42	30
13	20	39	60
0	250	0	250[a]

[a] Excludes fire alarm transmitters

16.2.3.2 Inactive code transmitters (excluding fire-alarm, see 16.2.5.1) may be connected to circuits servicing active burglar-alarm systems.

16.2.3.3 No more than 20 inactive (excluding fire-alarm, see 16.2.5.1) code transmitters may be connected in one circuit serving active burglar-alarm systems. See Table 16.1.

16.2.3.4 For every ten inactive (excluding fire-alarm, see 16.2.5.1) code transmitters connected in one circuit, the number of active burglar-alarm code transmitters that may be connected in the circuit shall be reduced by one, beginning with a maximum of 15 active burglar-alarm code transmitters being permitted (as specified in 16.2.3.1) when no inactive transmitters are connected. For example, if 20 inactive code transmitters are connected in one circuit, the circuit shall not have more than 13 active burglar-alarm code transmitters. See Table 16.1.

Exception: If all of the code transmitters in a circuit (excluding fire-alarm, see 16.2.5.1) are inactive, the total number can be 250.

16.2.3.5 If the equipment is able to operate without signal clash or loss, the maximum number of code transmitters, both inactive and active (excluding fire-alarm, see 16.2.5.1), permitted in 16.2.3.1, 16.2.3.3, and 16.2.3.4, may be multiplied by three but shall not exceed 250 if all of them are inactive. See Table 16.1.

16.2.4 Fire-alarm service

16.2.4.1 A code transmitter circuit that is used for fire-alarm service shall comply with the National Fire Alarm and Signaling Code, NFPA 72, and shall not exceed 250 transmitters or code wheels.

16.2.5 Fire- and burglar-alarm service

16.2.5.1 If a code transmitter circuit is used for fire-alarm service and other service, such as burglar-alarm, industrial processes, and the like, the number of transmitters used for other services shall be limited to 5 or less.

16.2.6 Spare equipment

16.2.6.1 Spare code transmitter receiving units and recorders shall be kept at each station and arranged so that they can be placed in service within 1 hour.

16.3 Multiplex systems

16.3.1 General

16.3.1.1 Multiplexing (See 5.2.32) may be accomplished over a communication channel or radio carrier or a combination of both.

16.3.1.2 The signal may be transmitted from the protection system directly to the central-station or residential monitoring station, or through a subsidiary station or repeater station.

16.3.1.3 Equipment used in a burglar-alarm multiplex system shall comply with the requirements for multiplex alarm units in the Standard for Central-Station Burglar-Alarm Units, UL 1610. Equipment used in a fire-alarm multiplex system shall comply with the requirements for multiplex alarm units in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

16.3.2 Receiving units

16.3.2.1 The number of burglar-alarm systems served by a multiplex receiver shall be limited to 1000.

Exception: The capacity of the system is considered to be unlimited if the station equipment is completely duplicated by standby equipment and a switchover can be accomplished in not more than 90 seconds with no loss of signals during this period.

16.3.2.2 The loading of a multiplex system used to provide fire-alarm service shall comply with the requirements of the National Fire Alarm and Signaling Code, NFPA 72.

16.3.2.3 Spare parts of equipment shall be maintained at the station so that any component whose malfunction prevents the receipt and interpretation of signals can be replaced and the system restored to service within 1 hour. Spare parts are not required if the equipment is duplicated.

16.4 Digital alarm radio system (DARS)

16.4.1 General

16.4.1.1 The signal transmission shall be after the DACT has failed to make successful contact with the DACR, or its transmission shall be simultaneous with the transmission by the DACT. Equipment used in a DARS shall comply with the requirements for such equipment in the Standard for Central-Station Burglar-Alarm Units, UL 1610, and the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

16.4.1.2 Failure of the telephone line connected to the DACT shall result in a trouble signal being transmitted to the digital alarm radio receiver (DARR) within 4 minutes of detection of the fault.

16.4.1.3 A DARS shall have a 90 percent probability of successfully completing each transmission sequence.

16.4.2 Digital alarm radio transmitter (DART)

16.4.2.1 A transmission sequence by a digital alarm radio transmitter (DART) shall be repeated a minimum of five times. The transmissions may be terminated in less than five sequences if the DACT successfully communicates with the DACR.

16.4.2.2 A DART shall transmit a digital code or the equivalent by use of radio transmission to its associated DARR. Signal repetition, digital parity check, or some equivalent means of signal verification shall be used.

16.4.2.3 Each DART shall automatically initiate and complete a test signal transmission sequence to its associated DARR at least once every 24 hours. A successful DART signal transmission sequence of any type within the same 24-hour period shall be considered sufficient to fulfill this requirement if the signals received by the DARR are processed by an automation system which alerts operators of the delinquency of a 24-hour test signal. If no signals are transmitted during a 24-hour period, a special signal for this purpose shall be transmitted. If an automation system with this feature is not used, or if an automation system is not used, the test signal shall be transmitted at the same time every 24 hours.

16.4.3 Digital alarm radio receiver (DARR)

16.4.3.1 A standby DARR shall be provided at the station and shall be capable of replacing a failed unit within 30 seconds after detection of the failure.

16.4.3.2 The following functions shall be supervised at the staffed station:

a) Failure of AC power supplying the DARR equipment;

b) Malfunction of the operating DARR;

c) Malfunction of the receiving antenna and interconnecting cable;

d) Indication of an automatic switchover between the DARR units; and

e) Malfunction of the data transmission line between the DARR and a station which is remotely located from the DARR.

16.5 One way radio alarm system (OWRAS)

16.5.1 General

16.5.1.1 A one way radio alarm system (OWRAS) consists of a radio alarm transmitter (RAT) located at the protected premises which will transmit one way signals to a radio alarm supervising station receiver (RASSR) located at the station. The transmission of the signal shall be through at least two independently powered, independently operating and separately located radio alarm repeater station receivers (RARSR), which shall relay the signal on to the RASSR.

Exception: The transmission may be through one RARSR and also independently sent directly to the RASSR.

16.5.1.2 The OWRAS may be independently owned and operated by the station, or it may be through a company providing an alarm and signal transport service network.

16.5.1.3 The equipment used in an OWRAS shall comply with the requirements for such equipment in the Standard for Central-Station Burglar-Alarm Units, UL 1610, and the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

16.5.2 Signal transmission time and probability

16.5.2.1 The time required to transmit a signal from a RAT to a RASSR shall be as indicated in (a) – (c). There shall be:

a) A 90 percent probability that the time between the initiation of a signal until it is recorded at the central-station or residential monitoring station shall not exceed 90 seconds;

b) A 99 percent probability that the time between the initiation of a signal until it is recorded at the station shall not exceed 180 seconds; and

c) A 99.999 percent probability that the time between the initiation of a signal until it is recorded at the station shall not exceed 450 seconds (7.5 minutes). At that time the RAT shall cease transmitting.

16.5.3 Supervision

16.5.3.1 The following conditions at each RARSR shall be supervised:

a) Failure of AC power supply of the radio equipment;

b) Radio receiver malfunction; and

c) Indication of an automatic switchover to another RARSR (if applicable).

16.5.3.2 In an OWRAS owned and operated by a central-station or residential monitoring station, these conditions shall be annunciated at the station. If the OWRAS service is provided through an independently owned and operated alarm and signal transport service network, the annunciation shall be at one of the stations served by the network or shall be by other means determined to be acceptable.

16.5.4 Protected premises supervision

16.5.4.1 A RAT shall be used with another signal transmission method that provides for the receipt of an acknowledgement signal from the station when the system is armed. See 34.2.1 and Table 34.2. An alarm signal shall be transmitted over both the RAT and the other method of signal transmission. Other signals, such as opening and closing, may be transmitted over only one of the signal transmission methods.

16.5.4.2 A RAT shall automatically initiate and complete a test signal transmission sequence to its associated RASSR at least once every 24 hours. If the signals from the RASSR are processed by an automation system that notifies operating personnel that a RAT is delinquent with its 24-hour test signal, a signal of any type within each 24-hour period meets this requirement. If no signals are transmitted during a 24-hour period, a special signal for this purpose shall be transmitted. If an automation system with this feature is not used, or if an automation system is not used, the test signal shall be transmitted at the same time every 24 hours.

16.5.5 Minimum equipment

16.5.5.1 An OWRAS that is owned and operated by the station shall have a minimum of two independently-powered, independently-operating, and separately located RARSR.

Exception: If the transmission from each RAT can be made directly to the RASSR at the station as well as through one RARSR, the system may operate with one RARSR.

16.5.5.2 If the OWRAS operates through an alarm and signal transport service network provided by an independent company, the network shall have a minimum of three independently powered, independently operating, and separately located RARSRs.

16.5.5.3 The station shall have a standby RASSR that can be put into service within 30 seconds after it has been determined that the operating RASSR has failed.

16.5.5.4 The failure of a RARSR to receive and relay signals from a RAT shall be annunciated at the station in a system that is owned and operated by the central-station or residential monitoring station. In an alarm and signal transport service system, the failure of a RARSR to process signals shall be annunciated at the station supervising the operation of the network.

16.6 Two-way radio alarm system (TWRAS)

16.6.1 A two-way radio alarm system (TWRAS) shall comply with all of the requirements for a one-way radio alarm system (OWRAS) with the exception that the protected premises is equipped with a radio alarm transmitter/receiver (RATR) which is capable of receiving signals as well as transmitting them. The station shall be equipped with a minimum of two radio transmitters capable of transmitting interrogation signals to each RATR in the system either directly or through one or more RARSRs.

16.6.2 The station standby radio transmitters shall be operated once a month to determine proper operation. A record shall be kept of the dates and times that the units are operated.

16.7 Digital alarm communicator system units

16.7.1 General

16.7.1.1 Equipment used in a digital alarm communicator system for burglar-alarm service shall comply with the Standard for Digital Alarm Communicator System Units, UL 1635. Equipment used in such a system for fire-alarm service shall comply with the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864.

16.7.2 Digital alarm communicator receiver (DACR)

16.7.2.1 There shall be spare DACR receivers online or that can be put into service in 30 seconds or less. One spare receiver unit shall be available as a backup for a maximum of five active units. A spare DACR shall have the same or greater capacity as any DACR it is to replace.

16.7.2.2 A DACR shall be provided with a minimum of two telephone lines (numbers) and a maximum of eight. See Table 16.2. Each line (number) shall be supervised so that the operator is alerted by audible and visual signals if any line develops a fault that prevents its use. A fault on any one of the telephone lines (numbers) shall not prevent the receiver from utilizing the remaining lines. All lines (numbers) serving a DACR shall be for digital alarm communicator transmitter signals only and shall be unlisted.

Table 16.2
System transmitters

System loading at a central-station, subsidiary station, or residential monitoring station	Number of lines in hunt group				
	1	2	3	4	5 to 8
With DACR lines processed in parallel:					
Number of initiating circuits		5000	10000	20000	20000
Number of DACTs		500	1500	3000	3000
With DACR lines process serially (put on hold, then answered one at a time):					
Number of initiating circuits		3000	5000	6000	6000
Number of DACTs		300	800	1000	1000

16.7.2.3 The loading capacity of a digital alarm communicator receiver shall be in accordance with Table 16.2 or it shall be demonstrated that there is a 90 percent probability that an incoming call is accepted immediately.

16.7.2.4 For each active alarm system or each suppressed guard tour, the allowable number of DACTs specified in Table 16.2 shall be reduced by:

a) 10 for a 4-line hunt group;

b) 7 for a 5-line hunt group;

c) 6 for a 6-line hunt group;

d) 5 for a 7-line hunt group; or

e) 4 for a 8-line hunt group.

16.7.2.5 For each unsuppressed guard tour, the allowable number of DACTs specified in Table 16.2 shall be reduced by:

a) 30 for a 4-line hunt group;

b) 21 for a 5-line hunt group;

c) 18 for a 6-line hunt group;

d) 15 for a 7-line hunt group; or

e) 12 for a 8-line hunt group.

16.7.2.6 At least one signal shall be received over each of the lines (numbers) connected to a DACR once every 24 hours.

16.8 Other transmission technologies

16.8.1 Other means of transmission technologies shall be permitted if they conform to the National Fire Alarm and Signaling Code, NFPA-72, chapter “Communications Methods for Supervising Station Alarm Systems”, latest edition

17 Alarm Monitoring Automation Systems

17.1 General

17.1.1 For the purpose of these requirements, An automation system is a system that is used to automatically process signals received by the central station receivers. As applicable, an automation system (See 5.2.3) shall comply with:

a) The Standard for Control Units and Accessories for Fire Alarm Systems, UL 864; and

b) The Standard for Central-Station Burglar-Alarm Units, UL 1610; or

c) The Standard for Central-Station Automation Systems, UL 1981.

17.1.2 Automation systems that comply with 17.1.1 (a) or (b) shall be configured in accordance with the manufacturer’s instruction manual.

17.1.3 Automation systems that comply with the Standard for Central-Station Automation System, UL 1981, shall be installed and operated in compliance with this Standard (See 17.2 – 17.11).

17.1.4 Surge suppression for all computer equipment shall be in accordance with The National Electrical Code, NFPA 70. (See 11.16).

17.1.5 The use of optical fiber cables in place of surge arrestors between equipment is allowed.

17.2 Automation installation software

17.2.1 The installation software and the license keys shall be available to the station whenever needed.

17.3 Automation system equipment

17.3.1 A computer system is formed when the equipment described in 17.3.2 and 17.3.3, including power supplies, disk drives, processors, data storage devices, and similar components are interconnected to enable the alarm monitoring software to process signals.

17.3.2 An automation system that complies with 17.1.1 (a) or (b) shall be installed on computer equipment that complies as applicable with the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, or the Standard for Central-Station Burglar-Alarm Units, UL 1610.

17.3.3 An automation system that complies with 17.1.1(c) shall have the alarm monitoring software, subscriber database, and operating system installed on computer equipment that complies with the Standard for Information Technology Equipment – Safety – Part 1: General Requirements, UL 60950-1. Related operator workstations, printers, interface equipment switches, routers, and any other equipment that is interconnected to enable the processing of signals shall also comply with the Standard for Information Technology Equipment – Safety – Part 1: General Requirements, UL 60950-1. Such computer equipment shall also meet any performance specifications established by the software provider.

17.3.4 Computer systems (See 17.3.3) shall be designated, by the manufacturer with the following minimum specifications:

a) Designed for continuous use, 24 hours per day, 7 days per week;

b) Be specified by the manufacturer as a “high-availability” system;

c) Have no less than two cooling fans;

d) Have no less than two power supplies, each of which can supply power for the entire system; and

e) Have no less than two network connections, each of which can service all the system’s needs.

17.4 Monitoring automation system performance

17.4.1 The performance indicators in 17.4.2.1 shall be monitored by software designed for this purpose.

17.4.2 The amount of unused capacity of the central processing unit (CPU) and data storage systems for each computer and the bandwidth of networks shall be stored as a report. If the utilization exceeds 80 percent, an audible and visual notice shall be annunciated in the operating room and the technical support staff shall be notified. The technical staff shall retain a record of the notice.

17.4.2.1 This report shall include the following:

a) The percentage of utilization of the central processing unit (CPU) shall be recorded in at least 20 percent increments, starting at less than 20 percent and going up;

b) The percentage of utilization of the disk drive arrays shall be recorded in at least 20 percent increments, starting at less than 20 percent and going up. When applicable to both:

1) The configured database constraints; and

2) The data-storage constraints.

c) The percentage of the utilization of the bandwidth for any local area networks or wide area networks that are used in conjunction with the automation system shall be recorded in at least 20 percent increments, starting at less than 20 percent and going up. If the utilization of any of these exceeds 80 percent averaged over 15 minutes, an audible and visual notice shall be annunciated in the operating room.

17.4.3 Automation Signal Processing Throughput – An automation system shall make signals, requiring operator action, available to the operator in no less than ten (10) seconds from the receiver making it available to the automation system.

17.5 Monitoring equivalent weight (MEW) calculation

17.5.1 In order to ascertain the needed hardware to support reliable monitoring, a formula as specified in 17.5.2 shall be used. The example worksheet described in Appendix B Site Work Sheet, may be used to record this calculation.

17.5.2 Monitoring equivalent weight, known as the MEW factor shall be calculated as follows:

a) The number of residential monitored accounts x 0.333;

b) The number of inactive commercial monitored accounts x 1.0; and

c) The number of supervised intrusion alarm systems (systems with opening and closings) x 3.0. When an alarm system control unit has been configured with partitions that allow parts of the system to send opening and closings, each partition shall be counted as a separate intrusion alarm system.

See sample calculation in Table 17.1.

Table 17.1
Example of MEW calculation

Category of Account	Number of Accounts	Multiplier	MEW Factor
Residential	2530	X 0.333	842.49
Commercial	1025	X 1	1025
Systems with Openings and Closings	55	X 3	165
Total MEW Factor			2032 (Rounded)

17.5.3 The sum of the 3 calculated amounts in 17.5.2 is the "Monitoring Equivalent Weight" or "MEW factor" used to determine the configuration of the automation system as described in:

a) 17.6.1 (MEW Factor 1 – 999),

b) 17.6.2 (MEW Factor 1,000 – 9,999),

c) 17.6.3 (MEW Factor 10,000 – 99,999), and

d) 17.6.4 (MEW Factor 100,000 or greater).

17.5.4 Based on the Monitoring Equivalent Weight (See 5.2.30), computer systems that comply with 17.1.1(c) shall be configured in accordance with Table 17.2 – Table 17.4.

17.5.5 Table 17.2 correlates automation system characteristics and the maximum MEW factor supported by a system with those characteristics. A central station shall use a system with characteristics that support its calculated MEW or larger. In Table 17.2, “single-failure tolerant” refers to compliance with performance requirements in 17.6.2. “Two-failure tolerant” refers to compliance with performance requirements in 17.6.3.

Table 17.2
Summary of computer system configuration

Maximum MEW	Type of automation system employed	First failure failover accommodation	Second failure failover accommodation	Section reference for details
999	None – Manual Signal Processing	None	None	17.6.1
999	Susceptible to single failure	Manual	None	17.6.1
9,999	Single-failure tolerant	Type of automation system	Manual	17.6.2
99,999	Two-failure tolerant	Type of automation system	Type of automation system*	17.6.3

Table 17.2 Continued on Next Page

Table 17.2 Continued

Maximum MEW	Type of automation system employed	First failure failover accommodation	Second failure failover accommodation	Section reference for details
Unlimited	Two-failure tolerant, with redundant site	Type of automation system	Type of automation system*	17.6.4
* Central Station not required to maintain manual signal handling capability				

17.6 Minimum MEW factor requirements

17.6.1 MEW Factor 1 to 999

17.6.1.1 An alarm monitoring automation system is not required for MEW factor of 999 or less when, as applicable, all of the requirements of fire alarm service (Sections 17 – 26), or burglar alarm service (Sections 28 – 41), or residential monitoring station service (Sections 43 – 49) are met.

17.6.1.2 If an alarm monitoring automation system is used the following shall be met:

a) There is at least one computer system (see 17.3) capable of handling the volume of signals generated from alarm systems within the calculation of this MEW factor;

b) The alarm monitoring automation system shall meet the requirements of 17.3 – 17.4;

c) At least one operator shall be logged onto the alarm monitoring automation system at all times. The logged on operator shall be dedicated to the receipt of incoming signals, and reside within the central station operating room;

d) All of the central station supervisors and operators that use the automation system shall be trained for a period of not less than one hour per month and tested in the use of receivers, UPS units, printers, back-up procedures, emergency call lists, and other procedures in preparation for an automation system failure. Trained staff shall be on duty at all times when the automation system is in use. A log documenting such training and testing shall be maintained and available at the central station;

e) The number of individuals required to monitor the alarm systems that send signals to the station shall be identified. Sufficient workstations that are equipped with single party telephone communication means and any specialized equipment needed to process signals shall be available to such personnel. This determination shall be reassessed at least once every 12 consecutive months. If the reassessment determines an increase in the number of individuals is needed, there shall be a corresponding increase in the number of workstations.

f) The central station shall maintain sufficient current documentation on hand to enable the operators to handle signals directly from the receiver(s) as itemized below:

1) This documentation shall include, as appropriate, notification instructions, disarming and arming (opening and closing) schedules, pass card data, holidays observed and schedules, and the time and date that the documentation was created;

2) A means to permanently record the date and time, the processing of signals, or related actions taken to respond to change-of-status events;

3) A means shall also be provided by the automation system to transfer the data from manually-generated activities into the automation system's permanent record when the automation system is restored to normal operation.

g) Upon failure of the automation system, the receivers connected to the automation system, which may be suppressed, shall revert to their normal operation without loss of any signals. These functions include printing and displaying all incoming signals and providing audible and visual indications of change-of-status signals and generate an audible signal to alert the operator to the failure. The receivers shall be situated so that operators can easily gain access to the receiver displays and printers. If additional operators are required to process the volume of signals that are received provisions shall be established to bring additional staff on duty;

h) Back-up copies of the alarm system database and alarm-monitoring software of automation systems shall be generated once every 30 consecutive days and maintained at a secure off-site location in accordance with 17.10;

i) An operator or shift supervisor using the alarm monitoring automation system shall be capable of displaying the version number of the alarm monitoring software;

j) The central station shall maintain a dated diagram or printed description of the current configuration of the alarm monitoring automation system. The diagram or printed description shall be created when the automation system is installed and updated whenever there is a change to the system. The configuration shall be reviewed every 12 consecutive months and the records re-dated. The following should be included in the diagram or description as a minimum:

1) All computers that form the automation system;

2) All components that form a network for the automation system;

3) All surge protective devices;

4) All work stations by location;

5) All network security measures, such as fire walls and the like;

6) All network communication protocols;

7) All communications channels that enter into the operating room; and

8) All WAN communications channels that penetrate the Central-station company facilities, that connect into the LAN.

k) When other central stations of the same company share database information of the alarm monitoring automation system, but are intended to operate independent of each other in the event of a disaster or the like, then each central station shall be designed and configured in accordance with the backup requirement (redundancy or second backup system) of 17.6.3 based on the MEW Factor.

Exception: A remote signaling management center operated by the company operating the central station is not required to be designed with the backup requirements.

17.6.2 MEW Factor 1,000 to 9,999

17.6.2.1 All requirements of the previous MEW factor are to be met except for those noted in 17.6.2.10. In addition the requirements in 17.3 – 17.4 apply when MEW Factor 1,000 to 9,999 exists.

17.6.2.2 The computer system described in 17.6.1.2(a) shall be capable of resuming signal processing within 90 seconds of a single failure of critical system components. Examples of typical critical components include a power supply, computational/CPU hardware node, data storage hardware component, software/operating system instance, or similar critical component.

17.6.2.2.1 If hardware virtualization techniques are used as part of a method to provide redundancy or failure tolerance:

a) The automation system shall be guaranteed sufficient resources within the system provisioning;

b) Additional partitions shall not have a higher priority than the automation system; and

c) The second or failover automation system shall reside on a separate whole hardware platform that has sufficient capacity to provide the same or greater alarm monitoring performance as the primary hardware.

17.6.2.3 An automation system shall be provided with the necessary spare parts, and personnel shall be trained to the necessary expertise to ensure that the system can be placed back in service within 24 hours of failure (See 17.11 for further details).

17.6.2.4 *Deleted*

17.6.2.5 The system shall be configured so that redundant or failover components are engaged and actively processing signals at least once in every consecutive thirty day period.

17.6.2.6 Upon failure of the automation system's ability to process signals beyond the 90 seconds resumption time noted in 17.6.2.2, the signal handling functions of the receivers connected to the automation system shall revert to their normal operation. These functions include displaying and recording all incoming signals and providing audible and visual indications of change-of-status signals.

17.6.2.7 Back-up copies of the automation system's alarm system database shall be generated every 24 hours for restoring purposes. The most recent back-up copy shall be kept on-site in the event that problems develop with the alarm system data. At a minimum, back-up copies of the current alarm system database and alarm monitoring software shall be transferred to a secure off-site location two times in every seven day period (See 17.10 for a detailed explanation of back-up storage requirements).

17.6.2.8 A copy of the operating system shall be kept on-site and at an off-site location. The off-site location is not prohibited from being the software developer's location, if a copy of the operating system can be delivered to the central station within 24 hours (See 17.10 for a detailed explanation of back-up storage requirements).

17.6.2.9 Access shall be provided to all back-up data records required in 17.6.2.8 and 17.6.2.9 that are maintained at an off-site location shall be provided at all times (See 17.11 for a detailed explanation of back-up storage requirements).

17.6.2.10 Exceptions to the previous MEW requirements – None.

17.6.3 MEW Factor 10,000 to 99,999

17.6.3.1 All requirements of the previous MEW factors are to be met except for those noted in 17.6.3.7. In addition, the requirements in 17.6.3.3 – 17.6.3.7 apply when MEW Factor 10,000 to 99,999 exists.

17.6.3.2 Within 6 hours of the failure described in 17.6.2.2, the computer system shall be returned to a state where it is capable of resuming signal processing within 90 seconds of a second failure in a surviving power supply, computational/CPU hardware node, data storage hardware component, software/operating system instance, or similar critical component that would affect the 90-second switchover.

17.6.3.2.1 System components necessary to meet the requirement of 17.6.3.2 may be kept in an unenergized state and disconnected from all network, power supply, or other systems provided that:

a) The components are engaged and actively processing signals at least once in every consecutive thirty day period;

b) Associated database(s) are updated no less the every twenty-four hours.

17.6.3.3 The facility or facilities housing the automation system shall comply with all local electrical safety code requirements addressing voltage surge and lightning protection.

17.6.3.4 *Deleted*

17.6.3.5 *Deleted*

17.6.3.6 If a central-station company addresses conditions of 17.6.3.2 (2 failures in automation system), by configuring an automation system to allow switch-over of all signal processing to hardware located in another central station, redundant site, or an unstaffed backup center the following shall apply:

a) The remote system shall be energized at all times and the database updated in real time. The other site shall be equipped with a minimum of a single UPS system and a single generator sized appropriately to support the remote automation system hardware;

b) Network infrastructure shall be duplicated and capable of supporting monitoring operations within 90 seconds of the remote system assuming the signal processing.

c) Each of these channels shall meet the applicable requirements of 17.12.

17.6.3.7 The requirements for manual processing of signals in 17.6.1.2 (d), (e), (f), (g), (h), and 17.6.2.6 are not required.

17.6.4 MEW Factor 100,000 or greater

17.6.4.1 All requirements in 17.6.1 – 17.6.3.7 are to be met except for those noted in 17.6.4.7. In addition, the requirements in 17.6.4.2 – 17.6.4.7 apply when MEW 100,000 or greater exists.

17.6.4.2 A central station shall be able to deliver central station services from a “Redundant site” (see 5.2.46) that is located such that it is not likely to be affected by natural and man-made disasters that may disable the central station.

17.6.4.3 The redundant site or sites shall include sufficient communication bandwidth, workstations, computer systems, and the like to provide all of the services normally provided by the central station.

17.6.4.4 The redundant site or sites shall be compliant with Sections 6 – 17 as applicable.

17.6.4.5 The redundant site or sites shall be fully operational within one hour of the failure of the central station. This includes the transferring of phone lines from the central station and having operators available to process signals. Any backlog of signals that are pending handling by an operator shall be completed within one hour of the operators becoming available.

17.6.4.6 The automation system shall be configured so that the system can be operational within six minutes of the failure of the central station or the failure conditions noted in 17.6.2.2.

17.6.4.7 Exceptions to the previous MEW Requirements – None.

17.7 Numbers of computer systems required

17.7 deleted

17.7.1 *Deleted*

Table 17.3
Required tertiary computers
Table deleted

17.8 Redundant site options

17.8.1 *Deleted*

17.8.2 The redundant site shall be operated by any of the following:

a) The central station company that operates the central station (see 5.2.7) from which central-station services are primarily delivered; or

b) A hosted central station services provider with applicable services in compliance with UL 827A, Outline of Investigation for Hosted Central Station Services, with which a contract or written agreement that complies with 17.8.3 exists; or

c) A different central station company with which a contract or written agreement that complies with 17.8.3 exists.

17.8.3 If a central station company chooses to partner with another entity in compliance with 17.8.2 (b) or (c), a contract or written service agreement shall be in place that establishes:

a) How minimum requirements as outlined below will be provided,

b) The specific technical performance levels promised (Service Level Agreement); and

c) Remedies for performance failures.

17.8.3.1 The contract or service agreement shall include a requirement for a written notice of at least 30 calendar days in advance for either party to cancel or amend the contract or agreement.

17.8.3.2 The Service Level Agreement specified in 17.8.3 b) shall address or include, as applicable, provision for:

a) Quantifying and providing sufficient communication bandwidth, personnel, work stations, and related equipment to handle the volume of signal activity typically received by the contracting central-station company;

b) Delivery of a written report to the contracting central-station company at least once every 24 hours summarizing the activity received and any events that require action on the part of the contracting central-station company;

c) Advance notification of unavailability due to scheduled maintenance activities

d) Immediate notification of unscheduled, unplanned unavailability and follow-up notification of availability restoration

e) Current information needed to contact the providers of technical support for the automation system and essential computer equipment

17.8.4 If computer equipment that comprises an automation system is shared with another central station or other organization as described in 17.8.2 (b) or (c), the following shall be met:

a) The contract or agreement in 17.8.3 shall include a requirement for a written notice of at least 30 calendar days in advance of changes to the automation or computer system architecture.

b) The overall shared computer system shall have sufficient capacity to provide required levels of alarm monitoring performance when the overall computer system is supporting alarm monitoring for all parties, under maximum loading conditions

c) If redundant site operating partner processes signals for the contracting central station using the redundant site operating partner's automation system and operator staff:

1) The MEW factor for the overall computer system shall be calculated using the combined account totals of all parties

2) The combined MEW factor shall be used to determine the overall shared computer system MEW dependent requirements

3) When processing signals for more than one central station operating company, the redundant site operating partner shall prioritize signal processing based on signal type (fire alarm, burglar alarm, other), and time of signal receipt without regard for which central station operating company owns the account.

4) Records of signal handling done by a redundant site operating partner shall be committed to a database in a manner such that those records become accessible and part of the contracting central station's database when the contracting central station resumes signal processing for its accounts.

17.9 Site specific data sheets

17.9.1 Site specific data sheets shall be completed as described below and maintained at the central station. An example of the Automation System Check Sheet and Site Data sheets is in Appendix B.

17.9.2 The site specific data sheets shall be completed by trained central station personnel when an automation system is first installed at the central station or related facilities and when the system is changed through the replacement of equipment or the installation of new software.

17.9.3 The site specific data sheet shall be completed by trained central station personal no less than once every 12 consecutive months. Each completed datasheet shall be kept at the central station for five years from the date of its completion.

17.10 Back-up data storage system

17.10.1 General

17.10.1.1 Storage systems for the back-up copies of the alarm monitoring software, the alarm system database, and the operating system required in 17.6.1.2, 17.6.2.7, and 17.6.2.8 shall comply with 17.10.

17.10.2 On-site storage

17.10.2.1 A back-up copy of the alarm system database shall be created once every 24 hours and placed on a storage medium at the central station that is separate from the computer systems that are used for the alarm monitoring automation system and in a manner that permits it to be readily accessed by central station personnel in the event of a failure of the automation system.

17.10.2.2 The back-up copy of the operating system shall be an image of the configuration that is used to operate the automation system. The image shall be held on a storage medium that is separate from the computer systems that are used for the alarm monitoring automation system and in a manner that permits it to be readily accessed by central station personnel in the event of a failure of the automation system.

17.10.3 Off-site storage

17.10.3.1 The back-up copy of the alarm monitoring software shall be stored at a secure off-site location in a manner that permits it to be readily available to central station personnel in the event it is needed for the restoration of the automation system after a failure.

17.10.3.2 The back-up copy of the alarm system database shall be stored at a secure off-site location in a manner that permits it to be readily available to central station personnel in the event it is needed for the restoration of the automation system after a failure.

17.10.3.3 The back-up copy of the operating system shall be an image of the configuration that is used to operate the automation system. The image shall be stored in a manner that permits it to be readily accessed by central station personnel in the event of a failure of the automation system.

17.11 Spare parts

17.11.1 An automation system shall be provided with the necessary spare parts, and personnel shall be provided with the necessary expertise to ensure that the system can be placed back in service within 24 hours of failure. A maintenance contract that provides for restoring operation of the automation system within 24 hours is one method that demonstrates compliance.

17.11.2 There shall be one spare operator terminal and one spare printer for every five being operated. A minimum of one spare operator terminal and printer is required when less than five of each are being used. The spare units are not prohibited from being used in nonessential duties within the central station (See 5.2.7) provided they can be relocated and put into service within 30 minutes.

17.11.3 Where practical, due to the critical nature of the storage array and its data, the following spare parts should be on-site or available to be installed within 24 hours:

a) Spare disk drives that are stored away from the storage array unit and not part of the internal disk drive count;

b) A spare power supply that is stored away from the storage array unit; and

c) Complete spare storage array unit that includes disk drives.

17.12 Connections to the automation system

17.12.1 The central station automation system may include connections to remote locations operated by the central station or to allow other authorized users to access parts of the system.

17.12.2 The type of remote location shall determine the equipment that can be located there, its use, and the security measures that are used to isolate the automation system from unauthorized access. Table 17.4 provides a summary of these conditions. The remote hardware shall meet the requirements listed within Section 17.

17.12.3 When parts of the automation system are located outside of the operating room but within the central station the following conditions shall apply:

a) Opens, shorts, and ground faults on the communication lines between the components of the system shall not adversely affect the operation of the automation system;

b) The operation of any supplementary process such as accounting or data entry shall not adversely affect the change-of-status processing portion of the system, including operation speed;

c) If the primary, back-up, or tertiary computers are located outside of the operating room, they shall be housed in a room composed of fixed-in-place walls floors and ceilings. The room shall be equipped as follows:

1) The doors shall be locked at all times and equipped with automatic door closers;

2) The doors may be equipped with an access control system or the keys shall be under the control of designated personnel; and

3) The room shall be equipped with an automatic fire alarm system that annunciates with audible and visual notification devices in the operating room.

d) Security measures comply with 17.12.6.

17.12.4 When terminals or printers are located in a remote signal management center (See 5.2.48) or a subsidiary station (See 5.2.58), the following shall apply:

a) Opens, shorts, and ground faults on the communication lines between the components of the system shall not adversely affect the operation of the automation system;

b) Surge suppression devices shall be installed in accordance with 17.1.4 and 17.1.5; and

c) Security measures comply with 17.12.6.

17.12.5 When the automation system equipment is located in a redundant site, the following shall apply:

a) Opens, shorts, and ground faults on the communication lines between the components of the system shall not adversely affect the operation of the automation system;

b) Surge suppression devices shall be installed in accordance with 17.1.4 and 17.1.5;

c) The equipment shall be housed in a room composed of fixed-in-place walls floors and ceilings. The room shall be only be available to authorized personnel and equipped as follows:

1) The doors shall be locked at all times and equipped with automatic door closers;

2) The doors may be equipped with an access control system or the keys shall be under the control of designated personnel;

3) The room shall be equipped with an automatic fire alarm system that is monitored by the central station;

4) The room shall be equipped with an automatic fire suppression system; and

5) The room shall be equipped with an Extent Number 3 burglar alarm system that complies with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, and shall be monitored in the central station.

Table 17.4
Logical security measures for communications with the automation system

Type	Location	Equipment	Security measures[a]
A	Within the operating room	Terminals and servers	Program access control
		Software-based receivers	WAN Security
B	Within the central-station company, but outside of the operating room	Terminals, servers, and printers	Program access controls
C	Remote to the central-station location, not operated by the central-station company. (e.g. independent dealer and the like)	Terminals, servers, and printers	WAN Security and program access control
D	Redundant site (central-station)	Workstations, servers, and printers	WAN Security at both sites and program access control
E	Software vendor support connections and applications	Terminals	WAN Security and program access control
F	Central-station company-owned locations	Terminals	WAN Security and program access control
G	Access to Corporate Network	LAN/ WAN	Assignment of Domain Level Access privileges

[a] See Table 17.5 for program access control requirements

17.12.5.1 For WAN security, all communication paths shall employ the use of advanced encryption and other measures as documented (See Appendix C), all of which shall be active at all times. These systems shall be maintained with the latest updates supplied by the manufacturer.

17.12.6 Central station automation security measures over remote access shall comply with the following:

a) The following measures shall be taken to ensure appropriate secure access from sources outside of the central station.

1) Measure 1 – Physical security of facilities

i) Areas outside of the operating room, in a remote signal management center, in a subsidiary station, or in a redundant site housing equipment shall comply with physical security requirements of Section 6, Building Construction Requirements and Section 7, Physical Protection.

ii) Areas housing terminals used to make temporary connections with the automation system by alarm service company managed locations shall be arranged in a manner that limits access and view to authorized employees of the location making the connection. When the area is not occupied, it shall be locked and protected by a Premises Extent 3 alarm system that is compliant with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681. The alarm system shall be monitored in the central station.

2) Measure 2 – Local Area Network (LAN) security

i) If any part of the local area network that is not physically secured, managed and under direct control/supervision of the central-station company, the WAN Security

measures, as outlined below, shall be applied.. These systems shall be maintained with the latest updates supplied by the manufacturer. See Table 17.4.

3) Measure 3 – Wide Area Network (WAN) security

i) All communications shall employ the use of advanced encryption and other measures as documented (See Appendix D), all of which shall be active at all times. These systems shall be maintained with the latest updates supplied by the manufacturer. (See Table 17.4)

a1) Evidence of compliance from a certificate of authority (CA) for the validation of approved communication security functions shall be provided: or

a2) Evidence of compliance with the latest encryption NIST standard shall be provided.

b) Where the connection from the outside source is temporary, such as software vendor support, alarm service company, subscriber, and dealer, and/or from public safety answering points, it shall be made in compliance with Table 17.4 and Table 17.5 and with the program access controls described below:

1) Each individual authorized to access the system shall have a unique personal user name and password;

2) A user name shall consist of a minimum of six characters;

3) A password shall consist of a minimum of six alpha-numeric characters with at least one alpha and one numeric character;

4) After a maximum of five unsuccessful attempts to log on the username or password within 10 minutes, further attempts shall be automatically disabled;

5) The time, date, and identifying sign-on characteristic of the individual signing-on shall be recorded by the automation system at the time of signing-on;

6) The system shall prompt the user to change their security sign-on at intervals of three months or less.

7) A communication session shall be automatically terminated if it is idle for a maximum of 15 minutes; and

8) The ability to modify items within the automation system shall follow Table 17.5.

17.12A Facilities remote from the central-station

17.12A.1 General

17.12A.1.1 The connection at the central-station shall be protected and restricted as identified in Table 17.4 and Table 17.5.

17.12A.1.2 A facility listed in this section shall not handle signals requiring operator action.

17.12A.1.3 Personnel of the central-station shall create and assign the login of remote facility personnel.

17.12A.1.4 Facilities Remote from the central-station shall be provided with physical access security measures.

17.12A.1.5 This section does not address Subsidiary Stations; see Section 13, for further details.

17.12A.2 Independent dealer

17.12A.2.1 The central-station company shall ensure that the data personnel, of the dealer are trained and qualified for automation data entry for the specific dealer accounts and records kept thereof.

17.12A.2.2 At the option of the central-station company, dealer personnel may be permitted to modify data as depicted in Table 17.5.

17.12A.3 Remote data entry facility

17.12A.3.1 If the remote data entry facility is not operated by the central-station company there shall be a contract or service agreement that includes a requirement for a written notice of at least 30 calendar days in advance for either party to cancel or amend the contract or agreement.

17.12A.3.2 The personnel who perform data entry for the central-station shall be trained, qualified and records kept thereof.

17.12A.3.3 The data that may be modified by data entry center personnel shall be in compliance with Table 17.5.

17.12A.4 Service center

17.12A.4.1 A Service center shall be a location or facility that is under the direct control and management of the central-station company.

17.12A.4.2 The personnel shall be agents of the central-station company and typically provide sales, service, installation, and/or data management of alarm accounts for the central-station company.

17.12A.4.3 The data that can be modified by service center personnel are listed in Table 17.5.

Table 17.5
Access and remote functions

Function	Compliant UL 827 c.s. operating room	Service center	Remote data entry center	Independent dealer	Technicians	Subscribers
Security measures	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]	Table 17.4[a]
Minimum User ID and Password “Log On” credentials required	Yes	Yes	Yes	Yes	Yes	Yes
Create and/or commission new accounts	Yes	Yes	Yes	Yes	No	No
Administer, maintain, configure, automation user access	Yes	Yes	Yes/No[c]	No	No	No
Administer, configure, or maintain automation data tables	Yes	Yes	Yes/No[c]	No	No	No
Update customer account records	Yes	Yes	Yes	Yes	No	Yes

Table 17.5 Continued on Next Page

Table 17.5 Continued

Function	Compliant UL 827 c.s. operating room	Service center	Remote data entry center	Independent dealer	Technicians	Subscribers
Permanent schedule changes	Yes	Yes	Yes	Yes	No	Yes
Temporary schedule changes	Yes	Yes	Yes	Yes	No	Yes
Call list updates	Yes	Yes	Yes	Yes	No	Yes
View event history	Yes	Yes	Yes	Yes	Yes	Yes
Signal requiring operator action	Yes	No	No	No	No	No
Initial placed “IN” to Service	Yes	Yes	Yes	No	No	No
Accounts “OUT“ of Service	Yes	Yes	Yes	Yes	No	No
Accounts On/Off Test	Yes	Yes[b]	Yes[b]	Yes[b]	Yes[b]	No/Yes[d]
Remote arming	Yes	No	No	No	No	No
Remote disarming	Yes	No	No	No	No	No
Download panel	Yes	Yes	Yes	Yes	No	No

[a] Security measures for remote access outside of the central-station LAN / WAN or VPN shall be such that access is limited to the allowed actions in the table, that network security, log on user validation and restricted access privileges are in place. (Refer to 17.4).

[b] For defined duration not to exceed 8 hours

[c] Yes, for central-station company personnel, No when contractor personnel

[d] Under conditions set by the Central-Station

17.13 Printer-less environment

17.13.1 A central station is not prohibited from using computer equipment as event loggers to record signals received on receivers, in lieu of printers that are connected to or are part of receiving equipment, when the following conditions are met:

a) Computers used for this purpose shall be redundant;

b) In the event of failure of either the primary or back-up computer, there shall be an audible or visual indication within 90 seconds of the failure. The signal shall be obvious to the operators or responsible central station staff. The central station staff shall switch from the failed computer to the operational one within 30 seconds of the notice of the failure, if the switch-over is not automatic;

c) The primary and back-up computers shall be arranged so that signals from the receivers that are intended to be transmitted to the automation system do not pass through the primary and back-up computers used as event loggers;

d) The primary and back-up computers shall have transient protection as required in Electrical Transient Protection, 11.16;

e) The communication lines between the computer and the receiver shall be supervised so that, within 90 seconds, a distinct audible or visual trouble signal indicates the occurrence of a single break, a single ground-fault condition, or a short circuit that prevents the required operation of the computer;

f) Upon operational request and after data capture by the receiver captured signals must be retrievable and displayed upon demand in a maximum of 5 seconds; and

g) Signals must be presented, at a minimum, in the same manner as they would be by the receiver printers.

17.14 Performance

17.14.1 General

17.14.1.1 Performance of the automation system shall be subjected to the tests specified in 17.14.2 at the time it is initially installed or when the system is changed with the installation of new or replacement of equipment.

17.14.2 Electrical supervision

17.14.2.1 Except as indicated in 17.14.2.4, all interconnecting circuits of the automation system components and the receivers shall be electrically supervised so that within 90 seconds of the occurrence of a single break; a single ground-fault condition; or a short circuit on circuits that prevent the required operation of the automation system a distinct audible trouble signal will be indicated to the operators. When an intermittent trouble signal is used, it shall sound at least once every 10 seconds with at minimum time duration of one-half second. A visual display of a message describing the trouble condition is obvious to the operators is acceptable in lieu of an audible trouble signal.

17.14.2.2 Interruption and restoration of any source of electrical energy connected to the automation system and its connected peripherals or any other malfunction shall not cause a false signal.

17.14.2.3 To determine compliance with the requirements in 17.14.1, the investigation is to start with the representative system combination in the normal supervisory condition. The type of fault to be detected is then to be introduced separately in each circuit conductor.

17.14.2.4 The automation system equipment trouble signal shall be distinguishable from an alarm signal and shall be obvious to the operator. After acknowledgment, the trouble signal shall be indicated in a manner that is obvious to the operators.

17.14.2.5 When an audible signal is used to indicate a trouble condition, it shall be generated once every 10 seconds until silenced. A means of silencing the audible trouble signal is not prohibited from being provided if it does not prevent its operation upon receipt of subsequent trouble signals. The audible trouble signal shall sound when the means of silencing is in its “silence” position and no trouble exists.

Exception: Distinction among alarm, trouble, and supervisory signals received by the automation system may be accomplished by means of a common sounding appliance coupled with a visual indication.

17.15 Cybersecurity Measures

17.15.1 In addition to the cybersecurity measures presented in Section 17, the Central-station company shall implement the following measures specified in 17.15.2 – 17.15.5.

17.15.2 As an ongoing practice, there shall be an effort(s) to detect unwanted activity. The tool(s) to accomplish this shall report and document all unwanted events.

17.15.3 The central-station company shall keep itself aware of the current cybersecurity issues affecting this industry and well as the latest cybersecurity threats.

17.15.4 Precautions shall be taken to ensure “backup” data is not contaminated by any cybersecurity threat. (See 17.6 and 17.10)

17.15.5 Using a form such as shown in Appendix C, and the illustrations in Appendix E, the central-station company shall document the measures it has implemented, to ensure automation/central-station cybersecurity. (See NIST-SP-800-53 for examples of actions that can be taken). See Table 17.6.

Table 17.6
Correlation table for Appendix C

Topic	Individual item	(Yes/No/NA)[a]
i. Personnel Security	1. Background security	(Y or N)
	2. Terminated personnel security measures	(Y or N)
ii. Physical Security	3. Access security	(Y or N)
	4. Workstations secured	(Y or N)
iii. Account and Password Management	5. Access into the automation system(s)	(Y or N)
iv. Confidentiality of Sensitive Data	6. Retention policy(s)	(Y or N)
	7. Archival policy(s)	(Y or N)
	8. Disposing of materials policy(s)	(Y or N)
v. Disaster Recovery	9. Business continuity plan(s) (See 19.2)	(Y or N)
	10. Backup/archival policy(s)	(Y or N)
vi. Security Awareness and Education	11. Staff awareness policy(s):	(Y/N/NA)
	12. Staff alertness to possible breaches, policy(s):	(Y/N/NA)
	13. Password security awareness policy(s)	(Y or N)
vii. Cybersecurity (See Appendix E for communications examples)	14. Exiting communication channels identified (See 17.6.1.2(j)	(Y or N)
	15. Vulnerable channels identified (Y or N):	(Y or N)
	16. Actions to mitigate taken and recorded:	(Y/N/NA)
	17. Actions taken to secured data and recorded:	(Y/N/NA)
viii. Actions Taken on Vulnerable Channels	Based upon the analysis in the above section vii Cybersecurity, and those channels identified as vulnerable, proceed to document any observations and the corrective measures take to protect against cyber-attacks.	
The form shall be updated as elements change, but no less than twice annually		
Numbering corresponds to numbering on the form		
[a] The items that are marked with a "Y or N" shall be addressed and documentation kept thereof. Unmarked items are those that are dependent upon the configuration of the subject central-station.		

FIRE-ALARM SERVICES

18 Type of Service

18.1 Service in accordance with the National Fire Alarm and Signaling Code, NFPA 72, or as specified by the AHJ, is provided in one of the following ways:

a) Full Service – A central station (see 5.2.7) that provides monitoring, retransmission of signals, and associated record keeping and reporting for signals received from central-station fire-alarm systems (see 5.4.2). The station provides for protected premises equipment installation, inspection, testing, maintenance, and repair service of central-station systems, runner service, and associated central-station services, either directly or by subcontracting for these services;

b) Monitoring – A central station that provides monitoring, retransmission of signals, and associated record keeping and reporting for signals from central-station fire-alarm systems. Other services are not provided; or

c) Fire-Alarm Service – Local Company – A company that provides for protected premises equipment installation, inspection, testing, maintenance, and repair service of central-station fire-alarm systems with its own facilities and personnel. Monitoring, retransmission of signals, associated record keeping and reporting for signals from central-station fire-alarm systems is to be subcontracted with a central station. Runner service is provided by the company or the central station.

19 Central-Station Operation

19.1 The central-station shall be equipped with any of the following resources which are to be placed into service if the telephone service becomes inoperative;

a) Wireless voice communication devices that utilize standard industry equipment and licensed for commercial use;

b) An equivalent means of voice communication that is independent of the telephone communication lines that are connected between the station and the serving telephone company exchange; or

c) Two or more communication lines which can be placed into service within 90 seconds of a failure of the lines that are normally used, and which enter the station at locations that are physically separated and communicate to different telephone company exchanges.

19.2 There shall be a written plan of action for the restoration of service by a central station. The plan shall include the following:

a) Foreseeable disasters: Possible natural and man-made disaster threats, national and local, that could affect the station;

b) Emergency names list: A notification list that includes the names and the telephone numbers at work, home, vacation home, and the like, and home addresses of management, technical personnel, operators, runners, and other relevant personnel;

c) Equipment vendor contacts: The 24-hour telephone and fax numbers of the vendors, technical assistance providers, and maintenance contractors of the equipment used in the station;

d) Municipal agency contacts: Emergency telephone numbers for local municipal agencies, such as the fire and police departments, to be called for help;

e) Utility contacts: Formalized emergency procedures and 24-hour contact names and telephone numbers of the utility and telephone companies serving the station;

f) If an engine-driven generator(s) is used that requires on-site fuel storage, there shall be a 24-hours a day contact and telephone number for a source of fuel re-supply; and

g) Relocation site: If a relocation site is provided for, information on the location of the site, how to get there, how to put the site into operation, and 24-hour, emergency management contact names and telephone numbers.

19.3 Supervisory personnel and designated employees shall be made familiar with the plan and shall know the location of a copy of the plan that is kept at the station. The implementation of the plan shall be practiced annually to assure that all personnel know their responsibilities in case of an emergency.

19.4 The plan shall be reviewed and updated every six months and current copies shall be kept in designated and accessible locations.

20 Personnel (Operators and Runners)

20.1 The central station shall have sufficient personnel (at least two persons), trained as operators, on duty at the station, in a remote location that complies with the requirements of the Virtual Operator Workspace, Sections 52 – 54, or a combination of both at all times to provide immediate attention to signals requiring action. No other operator activity shall take precedence over receiving and acting on these signals.

20.2 There shall be a sufficient number of runners and servicepersons available to provide required response to alarm signals, supervisory signals, trouble signals, service requests, and maintenance requests.

20.3 The runners or servicepersons shall be available at all times at any of the following:

a) The central-station;

b) A subsidiary, a remote signal management center, runner or serviceperson station or service center equipped with single party or wireless voice communication device utilizing standard industry equipment and licensed for commercial use or radio communication with the central station;

c) In a vehicle or in an area, and equipped with a wireless voice communication device utilizing standard industry equipment and licensed for commercial use or with a radio that can contact the central station; or

d) At a location acceptable to the local authority having jurisdiction that is provided with a single party or wireless voice communication device(s) utilizing standard industry equipment and licensed for commercial use, or is in radio contact with the central station.

20.4 The runner or serviceperson shall be trained and equipped for the performance of their duties and available for prompt dispatch to provide service to the protected property.

20.5 Runners and servicepersons shall provide service as required by this standard.

21 Runner's Equipment

21.1 Runners shall be equipped with a uniform that identifies their company and shall also be provided with a means of identifying the central station for which they are responding. Runners shall also be equipped with a flashlight, any tools required, and personal identification.

22 Communications with Runners

22.1 A single-party telephone line, wireless voice communication device utilizing standard industry equipment and licensed for commercial use, or radio link shall be used by the fire-alarm central station to dispatch runners by either:

a) Contacting each individual runner that is available for dispatch; or

b) Contacting a local dispatcher, employed by each provider of central station service, who assigns responses to an individual runner from a group of available runners.

22.2 Where a single-party telephone line or wireless voice communication device utilizing standard industry equipment and licensed for commercial use is used as the means of contacting the runner, it shall have call waiting or an equivalent means of interrupting a call in progress.

22.3 An automation system may be used to electronically transmit the required information provided that the automation system provides confirmation to the central station operator that the dispatch has been received and acted upon. The automation system shall provide record keeping as defined in Section 24, Records.

23 Retransmission

23.1 Two independent means, acceptable to the authority having jurisdiction over the property, shall be provided for the retransmission of fire-alarm signals to the appropriate public fire service communication center.

23.2 If public-switched telephone service or managed facilities-based voice networks are used as both the primary and secondary means of retransmission, the central station shall be equipped with a minimum of two telephone paths, each having its own telephone device, connected to the public switched telephone network. A minimum of two telephone numbers shall be available for contacting the Public Safety Answering Service (PSAP) or other facilities used to dispatch the responsible fire department to which the central-station operator may retransmit an alarm signal.

23.3 If the either of the means of retransmission is disrupted the central station shall take the actions in Section 50, Reaction to Communication Disruptions.

24 Records

24.1 Accurate records of the service provided by a central station shall be retained for a minimum of twelve months. The records may be created manually with the use of a date-time stamp (See Section 10, Clocks) or by an alarm monitoring automation system that complies with Section 17, Alarm Monitoring Automation Systems. Records shall include date and time entries and the following information (the date shall include the year which may be recorded using the last digit of the year only):

a) Fire-alarms:

1) Receipt of signal;

2) Signal retransmission to the appropriate public fire service communication center;

3) Dispatch of runners (if required);

4) Arrival of runners (if dispatched);

5) Nature of the alarm (type and disposition);

6) The name or employee identification of the runner(s) (if dispatched) who are representing the alarm company;

7) System identification by number or subscriber's name and address;

8) Identification of the operator who processed the alarm;

9) Identification of the person designated by the subscriber that was notified of the alarm and the time and date of the notification; and

10) Identity of the fire department responding.

b) Supervisory signals:

1) Receipt of signal;

2) Communication of information to person(s) designated by the subscriber;

3) Dispatch of runners (if required);

4) Arrival of runners (if dispatched);

5) Notification of the fire department and/or law enforcement agency, if required;

6) Nature of the signal (type and disposition);

7) The name or employee identification of the runner(s) (if dispatched) representing the alarm company;

8) System identification by number or subscriber's name and address;

9) Identification of the operator who processed the signal; and

10) Identification of the person designated by the subscriber that was notified of the signal.

c) Trouble signals:

1) Receipt of signal;

2) Communication of information to person(s) designated by the subscriber;

3) Dispatch of runners (if required) to arrive within 4 hours to begin maintenance;

4) Arrival of maintenance personnel (if dispatched);

5) Nature of the signal (type and disposition);

6) The name or employee identification of the maintenance personnel (if dispatched);

7) System identification by number or subscriber's name and address;

8) Identification of the operator who processed the signal; and

9) Identification of the person designated by the subscriber that was notified of the signal.

d) For inspection, testing and maintenance, a record shall be made of each specific device inspected, tested or serviced.

24.2 All such entries shall be made in ink on a physical medium or recorded into the non-volatile memory of an automation system from where they can be displayed and, if needed, printed on command. All times and dates shall be entered by date-time stamp or by an automation system.

25 Maintenance and Service

25.1 Contracts and agreements

25.1.1 All installations shall be maintained by the central station company under a service contract or agreement and shall be inspected and tested at intervals in accordance with the National Fire Alarm and Signaling Code, NFPA 72, or the intervals specified by the authority having jurisdiction.

25.1.2 The contract or agreement shall provide for all of the service required by the National Fire Alarm and Signaling Code, NFPA 72, or the authority having jurisdiction.

25.2 Alarm, supervisory, and trouble signals

25.2.1 The monitoring of central station fire alarm systems (See 5.4.2) shall include the retransmission of alarm signals to the communication center (such as a Public Safety Answering Point) serving the protected property, and the dispatch of runners where required, the notification of the receipt of supervisory signals, and response to the receipt of trouble signals that indicate parts of the system are not capable of operating as intended in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72.

25.2.1.1 The monitoring of central-station fire alarm systems (See 5.4.2) and the subsequent receipt of alarm, supervisory and trouble signals, that indicate an alarm condition and/or parts of the system are not capable of operating as intended in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72 shall result in:

a) Alarm Signals: The retransmission of alarm signals to the communication center (such as a Public Safety Answering Point);

b) Supervisory and Trouble Signals: The dispatch of runners where required and the notification of the receipt of supervisory signals, and response to the receipt of trouble signals that indicate parts of the system are not capable of operating as intended in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72.

25.2.1.2 The delivery of monitoring services may be conducted manually or through the use of an alarm monitoring automation system that is configured in compliance with Section 17. The use of an automation system enables the implementation of an automated process that confirms the receipt of the actions described in Table 25.1, when known events such as the receipt of periodic check in signals, or supervisory or trouble signals indicating the system is not capable of operating as intended are received.

Table 25.1
FA Systems
Signals that may be handled by an automated process
(Option to reach an operator shall always be provided)

No.	Signal	Confirmation of receipt, and will attend issue (Y, N)[a]	Confirmation with name and ID code required[b] (Y, N)	Confirmation with rep's name and/or ID code[c] (Y, N)	Additional info required[d] (Y, N)	Answering machine OK, if call list exhausted[e]	Where requirements found
1	FA – Supervisory (AHJ not mandated)	Y	N	Y	Y	NA	NFPA 72
2	FA – Trouble (AC Fail, Late Test, Tamper)	Y	N	Y	Y	NA	NFPA 72
3	Disruption of Communication to PSAP's	Y	N	Y	N	OK[f]	50.1.1 (a) & (b)
4	Disruption of Communication Channel	Y	N	Y	N	OK[f]	50.2.1 (b) & (c)

NOTES:

[a] Y = Distinct Acknowledgement, N = No Answer or Distinct Refusal (See b)

[b] A name and code unique to the answerer and verified to the database

[c] Person gives name and/or code verified to the database

[d] Information is required to complete the transaction irrespective whether or not service is needed)

[e] OK = If no one answers, but a message(s) was left, event is complete (See f)

[f] If only messages were left, another attempt shall be made in 8 hours

25.2.2 The alarm service company shall maintain a means of receiving requests for service at all times and shall keep a record of the time and date that:

a) A service request is received;

b) The service is initiated; and

c) The repairs are completed.

Requests for service shall be received by alarm service company personnel or a method shall be devised that results in the initiation of service in accordance with the National Fire Alarm and Signaling Code, NFPA 72, or the intervals specified by the authority having jurisdiction.

25.2.3 The alarm service company shall provide the alarm service subscriber with written instructions on how to contact the company for service. The method of communication shall allow the subscriber to promptly report trouble conditions.

25.3 Signals from systems other than central-station fire-alarm systems

25.3.1 When an alarm or communication failure signal is received from a system that is armed and that is not a central-station fire-alarm type as defined by this Standard, the central-station shall take the following action:

a) Where the system is a mercantile or bank burglar alarm that complies with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, notify the agency(s)

or person(s) specified in writing by the subscriber. In the absence of a written specification, an operator shall notify the law enforcement agency having jurisdiction over the protected property in a manner that complies with all applicable laws or ordnances; or

b) Where the system does not comply with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, notify the agency(s) or person(s) specified by the subscriber.

25.3.2 The central-station shall notify the alarm service company responsible for the alarm system of the alarm or communication failure signal and the action taken in response to it no later than the next time they are open for business.

25.4 Disruption of communications

25.4.1 If the communication channel that is used to receive signals from protected properties becomes disrupted the central station shall take the actions described in Section 50.2 Disruption of a Communication Channel.

26 Testing and Inspection

26.1 Central-station fire-alarm systems shall be inspected and tested as required by the National Fire Alarm and Signaling Code, NFPA 72, or as specified by the authority having jurisdiction.

27 Protected Premises Control and Transmitter Units

27.1 A fire-alarm control unit and transmitter shall comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864; and shall be installed in accordance with the requirements of the National Fire Alarm and Signaling Code, NFPA 72, or as specified by the AHJ.

27.2 The central-station fire-alarm system at the protected premises shall be provided with standby power that operates the system as intended for 24 hours as required by the National Fire Alarm and Signaling Code, NFPA 72, or as specified by the AHJ.

BURGLAR-ALARM SERVICES

28 Central-Station Operation

28.1 The central station shall be equipped with any of the following resources which are to be placed into service if the telephone service becomes inoperative:

a) Wireless voice communication devices that utilize standard industry equipment and licensed for commercial use;

b) An equivalent means of voice communication that is independent of the telephone communication lines that are connected between the station and the serving wire center of the telephone company exchange; or

c) Two or more communication lines which can be placed into service within 90 seconds of a failure of the lines that are normally used, and which enter the station at locations that are physically separated and communicate to different telephone company exchanges.

28.2 There shall be a written plan of action for the restoration of service by a central-station. The plan shall include the following:

a) Foreseeable disasters: Possible natural and man-made disaster threats, national and local, that could affect the station;

b) Emergency names list: A notification list that includes the names and the telephone numbers at work, home, vacation home, and the like, and home addresses of management, technical, operators, runners, and other relevant personnel;

c) Equipment vender contacts: The 24-hour telephone and fax numbers of the vendors, technical assistance providers, and maintenance contractors of the equipment used in the station;

d) Municipal agency contacts: Emergency telephone numbers for local municipal agencies, such as the fire and police departments, to be called for help;

e) Utility contacts: Formalized emergency procedures and 24-hour contact names and telephone numbers of the utility and telephone companies serving the station;

f) If an engine-driven generator(s) is used that requires on-site fuel storage, there shall be a 24-hours a day contact and telephone number for a source of fuel re-supply; or

g) Relocation site: If a relocation site is provided for, information on the location of the site, how to get there, how to put the site into operation, and 24-hour emergency management contact names and telephone numbers.

28.3 Supervisory personnel and designated employees shall be made familiar with the plan and shall know the location of a copy of the plan that is kept at the station. The implementation of the plan shall be practiced annually to assure that all personnel know their responsibilities in case of an emergency.

28.4 The plan shall be reviewed and updated every six months and current copies shall be kept in designated and accessible locations.

29 Personnel (Operators and Runners)

29.1 The burglar-alarm central-station shall have sufficient personnel (at least two persons), trained as operators, on duty at the station, in a remote location that complies with the requirements of the Virtual Operator Workspace, Sections 52 – 54, or a combination of both at all times to provide immediate attention to signals requiring action. No other operator activity shall take precedence over receiving and acting on these signals.

29.2 There shall be a sufficient number of runners and service persons available to provide the required response to alarm signals, trouble signals, repair service requests, and maintenance requests.

29.3 The runners or servicepersons shall be available at all times at any of the following:

a) At the central-station;

b) At a subsidiary, a remote signal management center, runner or service person station, or service center equipped with single party telephone or wireless voice communication device utilizing standard industry equipment and licensed for commercial use or radio communication with the central station; or

c) In a vehicle or in an area, and equipped with a wireless voice communication device utilizing standard industry equipment and licensed for commercial use or with a radio that can contact the central station.

29.4 The runner or service person shall be trained and equipped in the performance of their duties, to provide prompt service to the protected property.

29.5 Runners and service persons shall provide service as required by this Standard.

30 Runner's Equipment

30.1 Runners shall be equipped with a uniform that identifies their company and shall also be provided with a badge or the like that identifies the central station for which they are responding. They shall also be equipped with a flashlight, identification, and a firearm or night stick.

31 Communication with Runners

31.1 A single-party telephone line, wireless voice communication device utilizing standard industry equipment and licensed for commercial use, or radio link shall be used by the burglar-alarm central station to dispatch runners. Where the communication means has not been used in a twelve hour period during the normal course of business, the central station shall conduct a test of the operability and intelligibility of the means by either:

a) Contacting each individual runner that is available for dispatch; or

b) Contacting a dispatcher, employed by each provider of central station service, who assigns responses to an individual runner from a group of available runners.

A record of the use of the communication link or test in each twelve hour period shall be made and retained for a minimum of twelve months.

31.2 Where a single-party telephone line or wireless voice communication device utilizing standard industry equipment and licensed for commercial use is used as the means of contacting the runner, it shall have call waiting or an equivalent means of interrupting a call in progress.

31.3 An automation system (as defined in Section 17, Alarm Monitoring Automation Systems) may be used to electronically transmit the required information provided that the automation system provides confirmation to the central station operator that the dispatch has been received and acted upon. The automation system shall provide record keeping as defined in Section 40, Records.

32 Retransmission

32.1 A means shall be provided for the retransmission of burglar-alarm signals to law enforcement or other agency(s) or individual(s) designated by the subscriber.

32.2 If telephone equipment is used as the means of retransmission, the central station shall be equipped with a minimum of two telephone lines, each having its own telephone device, connected to the public switched telephone network.

32.3 If the method of retransmission utilizes the public switched telephone network, the correctness of the telephone number of each law enforcement or other agency, or individual designated by the subscriber to be contacted, shall be verified by calling each number at least once every 12 consecutive months if it has not been used in that period. All other methods of retransmission shall be tested every 7 days. A record of all such tests shall be made and retained for a minimum of 12-months.

Exception: The telephone number of an individual designated by the subscriber to be contacted need not be verified if they are a secondary contact.

32.4 If the means of retransmission is disrupted, the central station shall take the actions in 50.1.

33 Burglar-Alarm Protected Premises Control Units

33.1 General

33.1.1 A subscriber control unit for a burglar-alarm system shall comply with the Standard for Central-Station Burglar-Alarm Units, UL 1610, or the Standard for Digital Alarm Communicator System Units, UL 1635, and shall be installed in accordance with the requirements of this Standard and the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681.

33.2 Direct-wire, burglar-alarm subscriber control units

33.2.1 If the subscriber's control unit provides for it, permanent protection shall be supervised when the protection system is disarmed and a signal shall be transmitted to the central station if it is disrupted.

33.2.2 The act of changing the protection mode at the subscriber unit shall cause a signal at the central station.

33.3 Code (McCulloh) transmitter burglar-alarm systems subscriber control units

33.3.1 If a subscriber's protective circuit is disturbed by an intrusion or unauthorized opening, the code transmitter shall send a coded signal to the central station and shall repeat it not less than three times.

33.4 Multiplex burglar-alarm systems subscriber control unit

33.4.1 If the subscriber's control unit provides for it, permanent protective wiring shall be supervised when the protection system is disarmed and a signal shall be transmitted to the central station if it is disrupted.

33.5 Digital alarm communicator transmitter (DACT) subscriber control unit

33.5.1 A burglar alarm DACT shall be supervised in one of the following ways:

a) Two telephone lines shall be used and the transmitter shall be able to switch from one to the other. Both telephone lines shall be monitored so that if a fault develops on either one, the transmitter will contact the receiver through the remaining line to report the fault and identify it as a telephone line trouble. The telephone line used for primary reporting shall be connected to not more than one telephone instrument that has bell-ringing capacitors. The secondary telephone line shall be connected to not more than two telephone instruments that have bell-ringing capacitors. The number of telephone instruments without bell-ringing capacitors are not limited; or

b) If one telephone line is connected to the transmitter, the transmitter shall contact the receiver with an identifiable signal at least once every 24 hours.

33.5.2 If signals are processed by an automation system that notifies operating personnel that a DACT is delinquent with its 24 hour test signal, the normally scheduled opening signal, closing signal, or any other identifiable signal may be used for this purpose. If none of these signals are transmitted during a 24 hour period, a special signal for this purpose shall be generated. If an automation system with this feature is not used, or if an automation system is not used, the test signal shall be transmitted at the same time every 24 hours. The telephone line(s) for (a) and (b) shall be either a wired or wireless connection to the public switched telephone network. The secondary line for (a) may be over a one way digital alarm radio system (DARS). See One Way Radio Alarm System (OWRAS), 16.5.

33.5.3 If the subscriber's control unit provides for it, permanent protective wiring shall be supervised when the protection system is disarmed and a signal shall be transmitted to the central station if it is disrupted.

33.6 Radio (RF) systems subscriber's control unit

33.6.1 Refer to the requirements for radio (RF) systems specified in 16.4 – 16.6 of this Standard.

34 Burglar-Alarm Protection Service

34.1 Alarm response time

34.1.1 The central station shall establish the alarm response time, in 5-minute increments that it will take to respond to an alarm from a protection system as follows:

a) 5 – 45 minutes for a system with standard line security or encryption line security; and

b) 5 – 60 minutes for other systems.

See the requirements for line security in 34.3.

Exception: Response by a runner is optional for a premises or stockroom system designated as having Extent No. 4 protection as defined in the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681. If an Extent No. 4 system does not have runner response, the operator shall notify:

a) The law enforcement agency having jurisdiction over the protected property; or

b) The agency(s) or person(s) specified by the subscriber.

The system shall have no other extent of protection other than Extent No. 4.

34.1.2 An alarm response time of 5 or 10 minutes shall be allowed only for systems that do not require the use of a motorized vehicle on a public road.

34.1.3 The alarm response time that is established shall be calculated by making a minimum of two trial runs during off-peak traffic conditions (not during rush hour) of a business day and noting the time (trial time). For systems assigned response times of 5 or 10 minutes, the trial times shall not exceed 5 or 10 minutes, respectively. For systems assigned response times of 15 – 45 or 15 – 60 minutes, the trial time shall not exceed 80 percent of the stated time. See Table 34.1.

Table 34.1
Maximum trial time for stated response times

Standard and encryption line security systems		Other systems	
Time, minutes		Time, minutes	
Stated	Trial	Stated	Trial
15	12	15	12
20	16	20	16
25	20	25	20
30	24	30	24

Table 34.1 Continued on Next Page

Table 34.1 Continued

Standard and encryption line security systems		Other systems	
Time, minutes		Time, minutes	
Stated	Trial	Stated	Trial
35	28	35	28
40	32	40	32
45	36	45	36
		50	40
		55	44
		60	48

34.2 Signal transmission methods for burglar-alarm systems

34.2.1 Signals shall be transmitted from the protection system by one or more methods. A signal transmission method that does not provide an acknowledgment signal shall not be used alone. If such a method is used, an additional method of signal transmission that provides an acknowledgment signal shall be provided. See Table 34.2.

Table 34.2
Signal transmission methods

Systems that provide an acknowledgement signal	Systems that do not provide acknowledgement signal
Direct wire[a]	One way radio (RF)
Multiplex[a]	Code transmitter
Derived channel[a]	
Two way radio (RF)[a]	
DACT/DACR	
PSDN	

[a] If any equipment used in these types of systems do not provide for an acknowledgement signal, the system that this equipment is a part of shall be used with a method of signal transmission that does provide for an acknowledgement signal.

34.2.2 The following methods of signal transmission may be used alone if they provide for the transmission of an acknowledgement signal to the protected premises:

a) Direct wire;

b) Multiplex;

c) Derived channel;

d) Two way radio;

e) Digital alarm communicator transmitter (DACT) utilizing two separate public switched telephone network paths with 24 hour check-in signal over each path. The primary and secondary paths used for transmission may be over either a wired or wireless connection at the protected property;

f) DACT utilizing two separate public switched telephone network paths with 24-hour check-in signal over only one path. The primary and secondary paths used for transmission may be over either a wired or wireless connection at the protected property;

g) Backed up with digital alarm radio transmitter (DART), with 24 hour check-in signal, transmitting one way signals to a digital alarm radio receiver (DARR), as secondary signal transmission means.

h) DACT, utilizing a single public switched telephone network path with 24 hour check-in signal.

i) PSDN Packet Switched Data Network (See 5.2.35) a type of communications, typically over the Internet that is very similar to “multiplex” systems. (See 16.3 for examples).

34.2.3 The following methods of signal transmission do not provide for the transmission of an acknowledgement signal from the central station to the protected premises. If these methods are used, they shall be used with another method of signal transmission that provides for the transmission of an acknowledgement signal. If equipment connected to the systems specified in 34.2.2 (a) – (d) is used that does not provide for the transmission of an acknowledgement signal, those systems shall be used with another method of signal transmission that provides for the transmission of an acknowledgement signal. These methods are:

a) One way radio transmitter; and

b) Code transmitter.

34.2.4 When more than one means of signal transmission is used, they shall monitor each other's ability to transmit signals. If a fault is detected on any of the signal transmission means, at least one of the other means of signal transmission shall send a signal to the central station to report the fault.

34.2.5 When a DACT with two public switched telephone network paths (see 34.2.2 (e) and (f)) is used, each path shall be monitored. If a fault is detected, a signal shall be transmitted to the central station utilizing the other path.

34.2.6 When a DACT, utilizing a single public switched telephone network path is used with a DART [see 34.2.2(h)], the path shall be monitored. If a fault is detected, the DART shall send a signal to the DARR to report it.

34.2.7 When more than one method of signal transmission is used in an alarm system that provides standard line security or encryption line security on one or more of the methods, alarm signals shall be transmitted over each method. Opening signals shall be transmitted immediately by either:

a) The method of transmission that provides line security; or

b) The method that does not provide line security. If the opening signal is not transmitted within five attempts, the opening signal or a failure to communicate signal shall be transmitted over the method that provides line security.

34.2.8 When more than one method of signal transmission is used in an alarm system that does not provide standard line security or encryption line security, alarm signals shall be transmitted over each method. All other signals may be transmitted over only one of the signal transmission methods.

Exception: A DACT that utilizes two public switched telephone network paths is not required to transmit an alarm signal over both paths.

34.2.9 A burglar-alarm system shall have the option of having an alarm sounding device installed in accordance with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681. Dependent on the mounting location, an alarm sounding device shall comply with the requirements for an outside, or inside alarm sounding device in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL 365.

34.2.10 Burglar-alarm system equipment used to transmit signals to the central station shall comply with the requirements of the Standard for Central-Station Burglar-Alarm Units, UL 1610, or the Standard for Digital Alarm Communicator System Units, UL 1635.

34.3 Line security

34.3.1 Line security may be provided at the following levels:

a) Standard: The signal transmission channel is supervised to detect an attempt to compromise the channel; or

b) Encryption: The signal transmission channel is supervised to detect a highly sophisticated attempt to compromise the channel.

34.3.2 The equipment used to provide standard or encryption line security supervision shall comply with the requirements of the Standard for Central-Station Burglar-Alarm Units, UL 1610.

34.4 Monitoring central station burglar alarm systems

34.4.1 General

34.4.1.1 The monitoring of central station burglar alarm systems (see 5.3.3) includes:

a) The supervision of opening and closing signals (see 5.2.59) as described in Sections 35 and 36;

b) Initiation of alarm verification and/or runner response when alarm signals or communication failures are received as described in Section 37; and

c) Response to the receipt of trouble signals or notifications indicating parts of the system are not capable of operating as intended.

34.4.1.2 The delivery of monitoring services may be conducted manually or through the use of an alarm monitoring automation system that is configured in compliance with Section 17. The use of an automation system enables the implementation of an automated process that confirms the receipt of the actions described in Table 34.3 when known events such as scheduled or properly coded opening and closings, or the receipt of periodic check-in signals, or trouble signals indicating the system is not capable of operating as intended, are received.

Table 34.3
BA Systems
Signals that may be handled by an automated process
(Option to reach an operator shall always be provided)

No.	Signal	Confirmation of receipt, and will attend issue (Y, N)[a]	Confirmation with name and ID code required[b] (Y, N)	Confirmation with rep's name and/or ID code[c] (Y, N)	Additional info required[d] (Y, N)	Answering machine OK, if call-list exhausted[e]	Where requirements found
When BA system is armed							
1	BA – late to open	Y	N	Y	Y	OK	35.3.3
When BA system is disarmed							
2	BA – late to close	Y	N	NA	Y	NA	35.2.3 & 35.3.4
3	BA – late test signal ("check-in")	Y	N	Y	Y	NA	37.4.1 (b)
4	BA – communication fail	Y	N	Y	Y	NA	37.3.1 (b)
5	BA – tamper	Y	Y	NA	N	NA	
6	BA – AC fail	Y	N	Y	N	NA	
7	BA – low battery	Y	N	Y	N	NA	
8	BA – supervisory	Y	N	Y	N	OK[f]	
9	Disruption of communication to PSAP's	Y	N	Y	N	OK[f]	50.1.1 (b) & (c)
10	Disruption of communication channel	Y	N	Y	N	OK	50.2.1 (b) & (c)

NOTES:

[a] Y = Distinct Acknowledgement, N = No Answer or Distinct Refusal (See b)

[b] A name and code unique to the answerer and verified to the database

[c] Person gives name and/or code verified to the database

[d] Information is required to complete the transaction

[e] OK = If no one answers, but a message(s) was left, event is complete (See f)

[f] If only messages were left, another attempt shall be made in 8 hours

34.4.2 BA System is Armed

34.4.2.1 (1) Late to Open

A. Subscriber shall acknowledge the event.

a) The identity of the subscriber can be either name or verified code.

b) The subscriber shall respond with intended action.

c) If no one on the call list answers, but at least one message was left, event is concluded.

34.4.3 BA System is Disarmed

34.4.3.1 (2) Late to Close or (5) Tamper

A. Subscriber shall acknowledge receipt and will attend.

a) The identity of the subscriber shall be verified by name & code.

b) The subscriber shall respond with intended action.

c) If no one on the call list answers, it shall be called again in one hour.

d) When the systems closes or the subscriber intends to stay open, event is concluded.

34.4.3.2 (3) Late Timer Test or (4) Communications Fail

A. Subscriber shall acknowledge receipt and will attend.

a) The identity of the subscriber can be either name or verified code.

b) The subscriber shall respond with intended action, event is concluded.

34.4.3.3 (6) AC Fail, (7) Low Battery, or (8) Supervisory

A. Subscriber shall acknowledge receipt and will attend.

a) The identity of the subscriber can be either name or verified code.

b) The subscriber shall respond with intended action, event is concluded.

34.4.3.4 (9) Communications Fail to PSAP or (10) Alarm Channel

A. Subscriber shall acknowledge the event.

a) The identity of the subscriber can be either name or verified code.

b) The subscriber shall respond with intended action.

c) If no one on the call list answers, and/or only messages left, calling shall restart in 8 hours.

35 Openings and Closing

35.1 General

35.1.1 A burglar-alarm system shall be arranged and operated to reduce the risk of the central station accepting an unauthorized opening (disarming). Systems that are operated without a prearranged schedule shall be operated in accordance with 35.2. Systems that are operated on a prearranged schedule shall be handled in accordance with 35.3. All regular and irregular openings and closing shall be recorded at the central station by an operator or an automation system. The records shall include the information required in 40.1 (b) and (c).

35.2 Openings and closing without a schedule

35.2.1 A burglar-alarm system with or without standard line security or encryption line security may be operated at any time when opening (disarming) and closing (arming) of the system is activated by an authorized user entering a personal identification number (PIN) code of 3 or more digits or characters into the control unit through a key pad or equivalent input device that has 10 or more input buttons or equivalent entry devices.

35.2.2 The code shall be received, automatically recorded, and confirmed by an operator or an automation system at the central station within 1 minute of its receipt.

35.2.3 A central station shall contact an authorized user of an alarm system that does not use a specified closing schedule if the system has not been closed by 9:00 PM or no later than 60 minutes after the time that the user of the alarm system has recorded as their expected closing time. An authorized user may reschedule the closing time in accordance with 35.4.2(d). If the authorized user does not reschedule the closing time, the central station shall contact the authorized user every 60 minutes thereafter until the system is closed.

35.3 Openings and closing with a schedule

35.3.1 A system that opens (disarms) and closes (arms) in accordance with a schedule shall follow a schedule submitted by an authorized person representing the subscriber and kept current at the central station. The schedule shall specify the times at which the burglar-alarm system is expected to be opened (disarmed) and closed (armed), and the days (including holidays) during which the system will remain closed each calendar year.

35.3.2 Every opening that is more than 5 minutes earlier than the scheduled opening time shall be treated as an alarm unless an authorized user of the alarm system has prearranged the opening in accordance with 35.4.1 or it is cleared by alarm verification. See Alarm verification, 37.2.

35.3.3 For systems that use a defined schedule, if, in a 3-month interval, 80 percent or more of the openings for a system occur more than 30 minutes outside of the scheduled time, the schedule shall be amended, with the subscriber's concurrence to reflect the routine opening times. The verification of the receipt of the subscriber's name and identification code shall be part of the record of the change.

35.3.4 A central-station shall contact an authorized user of an alarm system if the system has not been closed within 60 minutes after the scheduled closing time. An authorized user may reschedule the closing time in accordance with 35.4.2(d). If the authorized user does not reschedule the closing time, the central station shall contact the authorized user every 60 minutes thereafter until the system is closed.

35.4 Unscheduled opening

35.4.1 When an opening of a burglar-alarm system not made in accordance with an established schedule (See 35.3.2), then it is an unscheduled opening and shall comply with 35.4.2.

35.4.2 An unscheduled opening may be performed by an authorized user of the system without investigation if it is prearranged in one of the following ways:

a) The authorized user may use a PIN code in accordance with 35.2.1;

b) The authorized user may appear at the central station or at a staffed central station service center prior to the opening to personally specify the time for the opening. The identification and signature of the authorized user shall be verified during the visit. Any opening that actually takes place at a time differing by more than 5 minutes before or 45 minutes after the prearranged opening time shall be considered to be an alarm (with or without the use of alarm verification, 37.2);

c) The authorized user may send a letter by mail or fax or by other written, clearly legible communication that specifies the time for the opening and bears the signature of the authorized user. The communication shall be typed or hand written in ink. It shall be received at the central station before the time specified for the opening. Any opening that takes place at a time differing by more than 5 minutes before or 45 minutes after the prearranged opening time shall be considered to be an alarm (with or without the use of alarm verification, 37.2);

d) The authorized user may telephone, radio, or otherwise communicate with the central station to notify it of the intended time of the opening and to identify themselves by their identification code and name. The identification code and name shall be checked against the record of authorized users filed by the subscriber. If a copy of this record is provided to the subscriber, it shall not show the identification code. If cards are issued to an authorized user showing the identification code, the card shall not identify the protected premises.

35.5 Control unit programming

35.5.1 The maximum time that a control unit may be programmed to delay the transmission of a signal to the central station or the energizing of a local alarm sounding device, in order to permit the alarm system user to either enter and disarm the system, or arm the system and exit, shall not exceed 60 seconds.

35.5.2 The use of a universal service code or any other code other than that uniquely tied to an authorized user, or a runner or serviceperson responding to a trouble or alarm signal when the system is in the closed (armed) condition, shall result in the immediate transmission of an alarm signal.

36 Closing and Malfunctions During Closing

36.1 The central station shall return an acknowledgement signal to the control unit when a proper closing signal is received. (See 16.5.1 and 34.2.1).

36.2 If a malfunction of the burglar-alarm system is reported by the subscriber or authorized user at the time of closing, made apparent by the arming of the system, or a result of the subscriber's or authorized user's exit, then the central station shall dispatch a serviceperson who shall initiate service within one hour plus the designated response time for the system. (See 41.2.3).

36.3 If the burglar-alarm system cannot be returned to operating condition so that the system can be armed, the central station shall take the following action:

a) If the subscriber or an authorized user of the system is at the protected premises, the serviceperson shall inform them of the result and obtain the signature the individual on the service record; or

b) If the subscriber or an authorized user of the system is not at the protected premises, the central station shall notify the subscriber or an authorized user of the system of this condition by telephone or similar means that assures receipt of the message. If the subscriber agrees to come to the premises or sends a representative to guard the premises, the central station shall provide a runner or serviceperson to remain on the premises for up to 60 minutes after the agreement by the subscriber or until the subscriber or representative arrives at the premises. If the runner or serviceperson is still at the premises when the subscriber or representative arrives, the runner or serviceperson shall record the arrival time of the subscriber or representative and obtain their identification and signature. The signed record shall be held with the service records for the system.

36.4 If the subscriber or authorized user mentioned in 36.3(b) declines to come to the premises or to arrange to have it guarded, the runner may leave after determining that the premises is physically secure. The central station shall make a record of the time and date of the subscriber's instruction that the premises may be left unguarded, identifying the subscriber by name and identification code. This record shall be held with the service records for the system.

37 Alarms and Unauthorized Openings

37.1 Alarm investigation

37.1.1 A burglar-alarm signal, communication outage, or unauthorized opening of a protected property that has been closed and the protection system armed, shall be investigated as an alarm condition. When such a signal is received, the central station operator shall:

a) Record the time and date that the signal was received (this may be done automatically when an automation system is used);

b) If applicable, initiate the verification procedures in 37.2.1 – 37.2.7;

c) Dispatch runners to investigate if verification procedures do not determine that the alarm signal is acceptable as an opening or if verification procedures do not apply (see 37.1.2);

d) Notify the subscriber if keys to the protected premises are not held; and

e) Record the date and time of the arrival of the runner(s) representing the central station when the runner(s) arrive at the entrance to the protected premises.

37.1.2 The investigation shall be conducted by:

a) A runner, with or without keys, representing the central station and a member of the law enforcement agency having jurisdiction over the property;

b) Two runners with keys representing the central station and a member of the law enforcement agency having jurisdiction over the property;

c) Two runners with keys representing the central station: or

d) When keys are held, at least two persons consisting of the individuals mentioned in (a), (b) or (c) shall enter the protected premises (see 37.1.5).

37.1.3 An improper opening signal shall be investigated by at least one runner who is a representative of the central station if the opening occurs within the subscriber's customary opening time period. Investigation is not required if central station operators identify the person at the premises through the means of Alarm verification, 37.2.

37.1.4 A runner shall carry a card, electronic device, or shall be given oral instructions, indicating the address of the premises, the floor on which the premises are located, instructions regarding the use of keys, and other information necessary to enable efficient investigation of the alarm.

37.1.5 Alarms from an alarm system in which keys to the protected premises are held shall result in a complete search of the interior of the premises covered by the alarm system, including vaults, safes, stockrooms, ATMs, and the exterior of the premises that is accessible from adjacent locations.

37.1.6 Alarms from an installation for which runners do not possess keys shall result in a complete search of the outside of the premises and the surrounding area by the runners. A runner representing the central station shall remain at the premises if the subscriber, upon being notified, agrees to arrive at the premises within 1 hour of being notified to allow an interior search.

37.1.7 If the subscriber declines to come to the premises to allow an interior search, the runner may leave if there is no physical evidence of unauthorized entry and the premises appears physically secure. The central station shall make a record of the time and date, identifying the subscriber by name and identification code, indicating that the subscriber has declined to come to the premises.

37.1.8 For a key or no-key system, if there is evidence of unauthorized entry or the premises is not physically secure, the subscriber shall be notified. The runner shall remain at the premises for up to 1 hour if the subscriber agrees to come to the premises or arrange to have it guarded.

37.1.9 If, after the investigation of an alarm, the system cannot be rearmed by the runner or subscriber, the central station shall dispatch a service person to arrive within 1 hour plus the stated response time , unless arrangements have been made to guard the protected premises until such time that the system is repaired. See Repairs, 41.2.

37.1.10 The runner making the investigation of the alarm and who represents the central station shall leave a notice at the premises for the subscriber reporting that there has been an alarm investigation. The notice shall record the time and date of the investigation.

37.1.11 Following a burglary attack, the alarm system shall be inspected and any damages repaired. The system shall be given a complete operational inspection and returned to service. A record of the inspection and service performed shall be kept by the central station.

37.2 Alarm verification

37.2.1 The central station may attempt to verify that the cause of an alarm signal is due to the improper use of the alarm equipment by personnel that have authorized access to the premises for the following systems:

a) A premises alarm system that complies with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681; and

b) From equipment installed to protect a stockroom, vault, safe, night depository or automated teller machine connected to the premises system described in (a) if the presence of authorized personnel has been established by the receipt of a valid opening signal or by alarm verification procedures described in this section for the premises system surrounding the area or object being protected.

Successful verification in accordance with the steps outlined in 37.2.2– 37.2.7, shall eliminate the need for dispatch and investigation by runners representing the central station and the law enforcement agency having jurisdiction over the protected property.

37.2.2 Alarm verification for a system without standard line security or encryption line security shall be performed by the operator as follows:

a) Immediately after the receipt of the alarm signal, attempt to establish intelligible voice communication with the protected property through the use of a single-party telephone or alarm equipment that can provide two-way voice communication and that complies with the Standard for Central-Station Burglar-Alarm Units, UL 1610;

b) If intelligible voice communication cannot be made with authorized personnel at the protected premises within 6 rings or 1 minute (whichever comes first) or there is no answer on the first call to the protected premises, a second call or calls may be made to alternate phone numbers such as a second premises or cellular number;

c) If the attempt to contact the premise is met with a busy signal, the operator may attempt a second call to the same protected premise telephone number if no alternate contact telephone number is listed;

d) If intelligible voice communication cannot be made with authorized personnel on or off the premises within a maximum of 2 minutes from the receipt of the signal at the central station, runners and/or law enforcement personnel shall be dispatched to the premises;

e) If contact is made within 2 minutes, an authorized subscriber shall be identified by their name and identification code, which may be transmitted orally or electronically, such as a signal which can only be received as a result of an authorized subscriber, entering their code into the alarm control unit; and

f) If the person(s) contacted cannot be identified by a valid identification code within 2 minutes after the contact, runners and/or law enforcement personnel shall be dispatched to the premises.

The intelligible voice communication in (a) may be initiated by an authorized person at the protected premises.

37.2.3 Alarm verification for a system with standard line security or encryption line security shall be performed by the operator as follows:

a) Immediately after the receipt of the alarm signal, attempt to establish intelligible voice communication with the protected property through the use of a single-party telephone or alarm equipment that can provide two-way voice communication and that complies with the Standard for Central-Station Burglar-Alarm Units, UL 1610;

b) If intelligible voice communication connection cannot be made with authorized personnel at the protected premises within 6 rings or 1 minute (whichever comes first) or there is no answer on the first call to the protected premises, a second call or calls shall be made to alternate phone numbers such as second premises or cellular number;

c) If contact cannot be made with authorized personnel on or off the premises within a maximum of 2 minutes from the receipt of the signal at the central station, runners and/or law enforcement personnel shall be dispatched to the premises;

d) If contact is made within 2 minutes, an authorized subscriber shall be identified by their name and identification code, which may be transmitted orally or electronically;

e) An authorized subscriber shall then also be identified by a separate electronically transmitted personal identifier;

f) The personal identifier of (e) may be a restore or cancel signal to the central station generated as a result of the entry of a personal numerical identifier code into the subscriber control or the equivalent, or may use a physical attribute of the person to make the identification; or

g) If the person(s) contacted cannot be identified by a valid identification code and an electronically transmitted personal identifier within 2 minutes after the contact, the investigation team of runners or runner(s) and law enforcement personnel (See 37.1.2) shall be dispatched to the premises.

The intelligible voice communication contact in (a) may be initiated by an authorized person at the protected premises.

37.2.4 If alarm verification is used, the declared alarm response time for the system shall not be extended by the amount of time necessary to perform the verification attempt.

37.2.5 If the runner(s) and the law enforcement agency having jurisdiction over the protected property have been dispatched and alarm verification is then properly obtained, they may be recalled. This is acceptable if the verification is obtained after the time limits specified in 37.2.2 and 37.2.3.

37.2.6 If a central station uses alarm verification, the information required in 40.1(a) shall be recorded.

37.2.7 The alarm verification record shall be a part of the alarm record.

37.3 Investigation of a compromise attempt

37.3.1 A signal that indicates the possibility that an attempt is being made to compromise the installation or the means of communication with a system having standard line security or encryption line security shall be treated as:

a) As an alarm signal in accordance with 37.1 and 37.2, if the alarm system is armed and if an alternate communication channel that provides the same level of line security as the channel that has been affected is not brought into service within the check-in time of the affected communication channel; or

b) A trouble condition if the system is open and the protection is disarmed. Such an indication can be a signal that indicates a compromise attempt, a momentary alarm, or any communication channel outage.

37.3.2 The subscriber shall be notified no later than the next working day and a record of the receipt of the notification shall be made, and/or by a written report within two working days of the compromise attempt.

37.3.3 If possible, the source and cause of the compromise attempt shall be determined. In any case, the system shall be returned to normal operating condition (See 41.2.3). A record of the service performed shall be kept by the central station.

37.4 Investigation of a missing check-in signal

37.4.1 A missing check-in signal from any alarm transmission device that is required to send a check-in signal, shall be investigated if the system is:

a) Open (disarmed), the missing signal shall be treated as a trouble signal and an authorized user of the system shall be contacted and instructed to cause the transmitter to send a signal to the central station.

b) Closed (armed), the missing signal shall be investigated by a runner or service person or may be treated as a communication outage. See 37.1.1.

Exception: If the signal is not received, and the equipment provides for it, the central station may contact the premises control and cause it to send a signal to the central station whether the system is armed or disarmed.

37.4.2 The reasons for the missing check-in signal shall be determined and corrected, and a record of the results made.

37.5 Alarm response overruns

37.5.1 Not more than 20 of every 100 alarm investigations of signals received from systems that comply with this Standard shall exceed the maximum elapsed time specified in 34.1.1. The following shall be used in calculating this performance:

a) As a minimum, the most recent full month, in which 100 or more alarm investigations have occurred, shall be used;

b) At a maximum, the alarm investigations that occurred in the most recent six months shall be used; and

c) Alarms for which a runner was required but not dispatched or did not arrive shall be included in the calculation.

37.5.2 Elapsed time shall be determined by using the difference between the time recorded for the receipt of the alarm signal (See 37.2.4) at the central station, and the time recorded at the central station as a result of a signal given by the runner representing the operating company upon arrival at the entrance of the subscriber's premises. See 37.1.1.

37.6 Unwanted alarms

37.6.1 An alarm is a signal received at the central station that requires immediate verification or investigation as defined in 37.1.1, and was caused by:

a) Attempted burglary;

b) Actual burglary; or

c) Vandalism.

Other apparent alarm signals are unwanted alarms.

37.6.2 The central station shall provide instructions to each authorized user of the alarm system on the proper operation of the system.

37.6.3 If an alarm system has more than four unwanted alarms caused by subscriber error in a 12-month period, the users of the alarm system responsible for the unwanted alarms shall be re-instructed on the proper operation of the alarm system. A record of the retraining shall be kept by the central station.

37.6.4 If the cause for each unwanted alarm cannot be determined, a complete operational inspection shall be conducted by a service technician on the next day the protected premises is open for business to determine if any mechanical, electrical, or environmental problems exist, and the system shall be restored to operating condition. A record of the inspection and any repairs shall be kept by the central station.

37.7 Signals from systems other than central-station burglar-alarm systems

37.7.1 When an alarm or communication failure signal is received from a system that is armed and is not a central-station burglar-alarm-type as defined by this Standard, the central station shall take the following action:

a) Where the system is a mercantile or bank burglar alarm that complies with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, notify the agency(s) or person(s) specified in writing by the subscriber. In the absence of a written specification, an operator shall notify the law enforcement agency having jurisdiction over the protected property in a manner that complies with all applicable laws or ordinances; or

b) Where the system does not comply with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, notify the agency(s) or person(s) specified by the subscriber.

37.7.2 The central station shall notify the alarm service company responsible for the alarm system of the alarm or communication failure signal and the action taken in response to it no later than the next time they are open for business.

37.8 Disruption of communication

37.8.1 If the communication channel that serves more than one protected property becomes disrupted, the central station shall take the actions described in 50.2.

38 Identification of Subscribers

38.1 During an investigation of an alarm or in response to an unscheduled opening (see Unscheduled opening, 35.4) runners shall obtain satisfactory evidence of the identity and authority of the subscriber, their employees, or others found on the premises, and shall obtain the signatures of such persons. If such persons will not provide such information, the law enforcement agency having jurisdiction shall be notified.

38.2 If a law enforcement agency is involved with the investigation, the runner or the central station operator shall obtain and record the identity of law enforcement personnel by:

a) Name and badge (or other) number;

b) Squad number; or

c) Car number.

39 Handling of Subscriber's Keys

39.1 General

39.1.1 Each key or set of keys that provides access to a subscriber's premises shall be maintained in a locked container. The locked container shall be located in an operating room, subsidiary station, runner station, a remote signal management center, runner's vehicle, in a key vault that is attached to the protected premises, or in a service center independent of a central station or subsidiary station. Only authorized personnel shall have access to the means of unlocking the container or key vault.

39.1.2 The name and address of the premises for which the keys provide access shall not appear on anything that is attached to or contains the keys.

39.1.3 Each key shall be maintained under a key management system that provides an accurate record of when the keys were last used. Keys that have not been used for 12 consecutive months shall be functionally tested in the locks that they are intended to operate at the premises. Any key that does not function shall be returned to the subscriber the next day that they are open for business and a correct key requested. If a correct key is not obtained within 10 business days, the system shall be classified as a no-key system. Written notification of such reclassification shall be sent to the subscriber by mail, messenger, or similar means.

39.1.4 When a key is used, the runner or other central station representative that used the key shall leave a notice at the premises for the subscriber reporting that the key was used. The notice shall record the time and date that the key was used.

39.2 Key vaults

39.2.1 A key vault complying with the Standard for Antitheft Alarms and Devices, UL 1037, used to house keys to a subscriber's premises shall be securely attached to the building in which the protected premises is located. The opening of the key vault with or without the key, or its removal from its mounting shall result in the transmission of an alarm signal to the central station when the system is armed. When the system is disarmed, either a trouble or alarm signal shall be transmitted.

40 Records

40.1 Accurate records of the service provided by a central station shall be kept for at least 12-consective months. The records may be created manually with the use of a date-time stamp (See Clocks, Section 10) or by an alarm monitoring automation system that complies with Alarm Monitoring Automation Systems,

Section 17. Records shall include date and time entries and the following information (the date shall include the year which may be recorded using the last digit of the year only):

a) Burglar-alarms signals:

1) Receipt of alarm;

2) Alarm verification (if used);

3) Dispatch of runners (including notification of the law enforcement agency having jurisdiction over the property);

4) Arrival of runner;

5) Nature of the alarm;

6) The name or employee identification of the runner(s) who are representatives of the alarm company;

7) Identification of the law enforcement personnel involved (see 37.2);

8) The designated response time;

9) System identification by number or subscriber's name and address;

10) Identification of the operator who processed the alarm;

11) Identification of the subscriber notified of the alarm;

12) Whether or not keys were used; and

13) Identification of the subscriber or their employee(s) as specified in 37.1.

b) Openings and Closing:

1) Scheduled opening and closing time; and

2) The actual opening and closing time.

c) Irregular openings and closing:

1) The arranged irregular opening and closing time;

2) The actual irregular opening and closing time; and

3) The name of the subscriber or subscriber's representative making an irregular opening and closing.

d) The use of the keys held or controlled by the central station;

e) Inspection, testing and maintenance:

1) Nature of service,

2) Specific equipment inspected, tested, or serviced, and

3) Name of central station representative performing service.

f) Any follow-up or additional action taken on unwanted alarms.

40.2 All such entries shall be made in ink on a physical medium or recorded into the non-volatile memory of an automation system from where they can be displayed and, if needed, printed on command. All times and dates shall be entered by time stamp or by an automation system.

41 Maintenance and Service

41.1 Contracts and agreements

41.1.1 All installations shall be maintained under a service contract or agreement with the alarm service company.

41.1.2 Each alarm installation shall be inspected at intervals that will maintain the system in its intended operating condition. The interval between regular maintenance inspections shall not exceed 12 consecutive months. The regular maintenance inspection may be done in parts throughout the 12 month period. A record of all inspections shall be maintained (See 40.1(e)).

41.2 Repairs

41.2.1 The alarm service company shall maintain a means of receiving requests for service at all times and shall keep a record of the time and date that:

a) A service request is received;

b) The service is initiated; and

c) The repairs are completed.

Requests for service shall be received by alarm service company personnel, or a method shall be devised that results in the initiation of service within the time interval indicated in 41.2.3.

41.2.2 The alarm service company shall provide the alarm service subscriber with written instructions on how to contact the company for service. The method of communication shall allow the subscriber to promptly report trouble conditions.

41.2.3 Repair services for a central-station burglar-alarm system shall begin, not later than:

a) One hour plus the designated response time for the system after the scheduled closing time for the system if the request for service is received while the protected property is open for business;

b) One hour plus the designated response time after the request for service is received if the request for service is made as a result of trouble that has developed:

1) At closing time;

2) After the property has been closed and armed; or

3) After an alarm investigation.

Exception No. 1: The beginning of repair service may be extended to the time that the protected property is next open for business if the subscriber to the alarm service provides written or oral authorization. Authorization shall be given to alarm service company personnel when the subscriber makes the decision to delay service. If authorization is given, the alarm service company shall make a record of:

a) The time and date of the authorization;

b) The name and identification code of the person giving the authorization; and