UL 1981

STANDARD FOR SAFETY

Central-Station Automation Systems

UL Standard for Safety for Central-Station Automation Systems, UL 1981

Third Edition, Dated October 29, 2014

Summary of Topics

This revision of ANSI/UL 1981 dated November 6, 2019 includes revisions to Remote Access to the Automation System.

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.

The new and revised requirements are substantially in accordance with Proposal(s) on this subject dated June 7, 2019 and August 16, 2019.

No Text on This Page

OCTOBER 29, 2014
(Title Page Reprinted: November 6, 2019)

ANSI/UL 1981-2019

UL 1981

Standard for Central-Station Automation Systems

Prior to the first edition, the requirements for the products covered by this standard were included in the Standard for Central-Station Burglar-Alarm Units, UL 1610.

First Edition – October, 1994
Second Edition – June, 2003

Third Edition

October 29, 2014

This ANSI/UL Standard for Safety consists of the Third Edition including revisions through November 6, 2019.

The most recent designation of ANSI/UL 1981 as an American National Standard (ANSI) occurred on October 18, 2019. 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

FUNCTIONALITY REQUIREMENTS

PERFORMANCE

INSTRUCTIONS

APPENDIX A

APPENDIX B – Informative Operational Tests Work Sheet(s)

APPENDIX C – Informative

INTRODUCTION

1 Scope

1.1 These requirements cover the design, manufacture, implementation, and support of automation system units and accessories intended to be used in central-stations and proprietary stations for the reception, processing, dispatch, responses, and record keeping of property protection and life safety signals. Automated monitoring systems are a combination of computerized automation software and subsystems, including LAN/WAN network communications under control of the central-station. The monitoring system units and accessories and subsystems provide all the monitoring, control, communications audible indications and visual display functions of the system and shall meet all applicable requirements as specified by this Standard.

1.2 These requirements also cover special considerations for proprietary and national industrial security system application software.

1.3 These requirements do not cover hardware receiver units that are evaluated under separate equipment standards such as the Standard for Proprietary Burglar Alarm Units and Systems, UL 1076, the Standard for Central-Station Burglar Alarm Units, UL 1610, the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, and the Standard for Digital Alarm Communicator System Units, UL 1635.

1.4 These requirements do not cover the building needed to house the automation system, the staffing requirements, the power system (s), wiring expectations, spare parts, support policies, the specifics required by the Monitoring Equivalent Weight (MEW) factor, and any other requirement that falls outside the specifics of this automation standard. This information can be found within the latest edition of Standard for Central-Station Alarm Services, UL 827.

2 Components

2.1 Except as indicated in 2.2, a component of a product covered by this Standard shall comply with the requirements for that component. See Appendix A for a list of standards covering components used in the products 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 When 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 For the purpose of this standard the following definitions apply.

5.2 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.

5.3 ALARM-MONITORING SOFTWARE – The sequence of instructions that tells the hardware how to handle the incoming signals and instructions from the keyboard. The alarm-monitoring software controls how the messages are stored in memory and how they are displayed at the operator station and printers.

5.4 ALARM SIGNAL – A signal from an alarm system which requires immediate action. A signal, such as the alarm initiated from a manual box, a water-flow switch, an automatic fire detector, an intrusion detection unit, hold-up initiating device, door contact, or tamper switch, a condition that the software has determined constitutes an alarm, that indicates an emergency, fire or burglary condition requiring immediate action.

5.5 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 Alarm Services, UL 827.

5.6 AUTOMATION SYSTEM HARDWARE COMPONENT – A separate removable/interchangeable section of the system including but not limited to any associated power supply; a supervisory module (watchdog timer) for the disk drive, processor, or primary power, and similar components; operator station; printer; interface equipment; and similar equipment.

5.7 AUTOMATION SYSTEM SOFTWARE DEVELOPER – A company that develops the alarm monitoring software and specifies the minimum hardware platform specifications required for the combination of hardware and software to process signals from a subscriber's account in accordance with:

a) The National Fire Alarm and Signaling Code, NFPA 72;

b) The Standard for Central-Station Alarm Services, UL 827;

c) The Standard for Proprietary Burglar Alarm Units and Systems, UL 1076;

d) The Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681; and

e) The requirements of this Standard.

5.8 AUTOMATION SYSTEM'S ALARM SYSTEM DATA BASE – The system data base includes alarm system (account) information entered into the computer by central-station personnel. This information includes names and addresses of subscriber accounts; disarming and arming (opening and closing) schedules for individual alarm systems (accounts); dispatch information such as subscribers' phone numbers, police department phone number.

5.9 BANDWIDTH – The data transfer capacity of a network. It is measured in bits per second.

5.10 BATCH ALARM CLEAR – A process or utility that allows blanket clearing of alarms by type, geographical area, and/or priority.

5.11 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.

5.12 CENTRAL STATION PERSONNEL – Any employee of the central station who has the authority and access level to do what is described under specific paragraphs of this Standard.

5.13 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 receipt of a signal, take such action as required by the nature of the signal received.

5.14 CERTIFICATED SYSTEM – A system that is in compliance with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, the Standard for Central-Station Alarm Services, UL 827; the Standard for Proprietary Burglar Alarm Units and Systems, UL 1076; the Standard for National Industrial Security Systems, UL 2050; or the National Fire Alarm and Signaling Code, NFPA 72 and that has a current certificate issued.

5.15 CHECK-IN SIGNAL – A signal that is periodically sent by the alarm system to verify the transmission equipment at the protected property and the communication path are operational. A unique signal that is initiated at a pre-established frequency, or an opening, closing, alarm signal, or any other signal sent by the alarm system that occurs within the pre-established frequency may serve as a check in signal.

5.16 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.

5.17 COLD SYSTEM – A system whose sole purpose is to be available in the event that the main system has experienced a catastrophic failure. The system is only turned on to update the software, the software configuration and the database, and then is turned off until needed. Manual intervention is needed to bring the system online and to make it the active monitoring system.

5.18 CPU (Central Processing Unit) – The active device that fetches machine instructions from memory and executes them.

5.19 DEGRADED MODE OF OPERATION – A hardware or software failure that degrades the operation of the automation system to a point that the operators are required to handle alarm messages directly from the receivers.

5.20 DIAGNOSTICS – Software programs intended to self-test the automation system to determine that the computer hardware and software are operating as intended.

5.21 FAULT-TOLERANT COMPUTER SYSTEM – A computer system containing multiple power supplies, disks, processors, and controllers, each 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 5.25 and 5.43 for the definitions of a hot back-up and redundant computer system. A fault-tolerant computer system as defined above is considered to be a redundant system.

5.22 HARDWARE – Physical computer equipment (computer, disk drive, Video Display, printer, memory boards, and similar equipment) that constitutes the automation system.

5.23 HARDWARE CENTRAL-STATION RECEIVING UNIT – Electrically operated receiving equipment located at a central-station. The receiving equipment connected to an automation system receives signals from alarm systems and transmits them to the automation system.

5.24 HARDWARE VIRTUALIZATION – The partitioning of computer's memory and processor into separate and isolated environments simulating multiple machines within one physical computer. By partitioning the system, multiple copies of the same or different operating systems can coexist without interfering with each other.

5.25 HOT BACK-UP – A continuously energized computer system that is a back-up to the primary system computer and disk drive.

5.26 HVAC SYSTEM – Heating, ventilating, and air conditioning system.

5.27 INCIDENT – One or more alarm signals (i.e., fire, burglary, or holdup) of a related type received from an alarm system that require investigation by an authority having jurisdiction, alarm company, and/or subscriber.

5.28 INTERNET – A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.

5.29 THE INTERNET PROTOCOL (IP) – A set of rules used for communicating data across a packet-switched network using the Internet Protocol Suite, also referred to as TCP/IP.

5.30 LOCAL AREA NETWORK (LAN) – A combination of personal computers, servers, and communication devices that are connected to share data files, resources and applications located in close proximity, such as on the same floor or in the same or nearby buildings.

5.31 LEVEL OF ACCESS – The privileges associated with the security sign-on to the automation system.

5.32 MANUAL RECORDS – Records that may be maintained on paper, microfiche, or the non-volatile memory of a computer independent of the automation system. The records include alarm system (account) information that can be referred to in order to decode the signals on the receivers.

5.33 MONITORING EQUIVALENT WEIGHT (MEW) – 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.

5.34 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) – An agency of the U.S. Department of Commerce that works with industry to develop and apply technology, measurements, and standards as needed by industry or government programs such as encryption security.

5.35 NON-VOLATILE MEMORY – The type of memory wherein interruption of power will not result in loss of information content in the storage medium.

5.36 OPERATING ROOM – The physically enclosed area within a central-station that is physically secure and where operators receive and respond to the signals that are transmitted to the central-station.

5.37 OPERATING SYSTEM – The system software responsible for the direct control and management of hardware and basic system operations. Additionally, it provides a foundation upon which to run application software such as word processing programs and web browsers.

5.38 OPERATOR'S STATION – A terminal, consisting of a video display and keyboard, used for displaying and processing alarm, trouble, supervisory signals, and other similar signals.

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

5.40 RANDOM ACCESS MEMORY (RAM) – Computer electronic hardware used to store data on a temporary basis. Unlike a Hard Drive, RAM only stores data as long as the computer has power.

5.41 RECEIVING SOFTWARE – Software residing on a computer or network server that monitors the status of protected premises and stores status changes in memory. The receiving software connects to the automation system and transmits signals received from alarm systems to the automation system.

5.42 RECEIVER-HARDWARE – The physical components of a computer system which monitors the status of protected premises. The server receives signals from alarm systems and transmits them to the automation system.

5.43 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. A fault tolerant computer system is considered to be redundant.

5.44 REDUNDANT SITE – A physical location that is able to assume the complete operation of an automated central-station should the station become unable to process signals.

5.45 RESIDENTIAL MONITORED ACCOUNT – A single or two family dwelling with an installed alarm system being monitored by a central-station, and which does not have supervised opening and closings.

5.46 REVISION LEVEL – A unique version name or number that indicates the state of computer software or firmware. A higher number indicates a more recent iteration of the software.

5.47 RUNAWAY SYSTEM – Any alarm system that transmits a greater number of the same type of signals from a particular device, point of protection, zone or in the absence of the availability of such detail the overall system than the automation system is preprogrammed to receive within a preprogrammed period of time. The number of signals and the time frame which define a runaway system are agreed upon by the central-station and the automation system software provider. For example, a central-station may

define a runaway system as one that transmits more than 20 signals of the same type within 30 minutes. The automation system software developer programs the automation system to this specification. An automation system programmed with the runaway system criteria provided by the central-station meets the requirement of 11.1.9.

5.48 SECURITY SIGN-ON – A technique used to prevent unauthorized access into a computer system.

5.49 SERVER – A computer that provides shared data to multiple users on a computer network.

5.50 SERVICING VIDEO DISPLAY – A video display device used by service personnel. This Video Display is not intended for alarm-monitoring and processing.

5.51 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) – A UDP – based network protocol is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

5.52 SOFTWARE – The automation system computer program that operates on the computer hardware. The alarm-monitoring application(s) shall comply with this Standard.

5.53 SUBSCRIBER – The user of a premise or item protected by a burglar or fire alarm system. An authorized representative of the user is also considered a subscriber.

5.54 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 manned and operated as a central station or residential monitoring station.

5.55 SUPERVISED BURGLAR ALARM SYSTEM – An active alarm system in which operators initiate follow up actions when an anticipated signal, such as an opening and closing, or check-in signal is missed or improperly sent.

5.56 SYSTEM DIAGNOSTICS – A hardware or software supervisory module which supervises all elements of the automation system.

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

5.58 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.

5.59 UNSCHEDULED OPENING – An opening of a burglar-alarm system not made in accordance with an established schedule.

5.60 VIDEO DISPLAY – An electronic device that presents information in visual form.

5.61 VOLATILE MEMORY – The type of memory wherein any interruption of power will result in loss of information content in the storage medium.

5.62 WATCHDOG TIMER – A hardware or software supervisory module which supervises the disk drives, micro-processors, power supply output, and similar components.

5.63 WIDE AREA NETWORK (WAN) – A WAN differs from a LAN in that a WAN makes data connection across a broad geographic area. Companies use a WAN to connect to various company sites so that information can be exchanged between distant offices.

Functionality Requirements

6 Automation Access Security

6.1 External access

6.1.1 *Deleted*

6.1.1A If the automation system software provides capabilities for remote access from a point outside of the signal receiving center private corporate secure network it shall be through a secure, end-to-end connection that utilizes encryption.

6.1.1B Evidence of a certificate of compliance for the validation of approved communication and stored data security functions shall be provided by the automation system software manufacturer. The certificate of compliance shall be from the National Institute of Standards and Technologies (NIST) cryptographic algorithm validation program (CAVP) and shall be a current valid certificate for the security function used by the system and security function per Appendix C, Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules.

6.1.2 The system shall record the following:

a) User Name;

b) The time access was made; and

c) The date access was made.

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

6.1.4 The system shall record information for the following:

a) Time;

b) Date;

c) Detail of any changes made;

d) Operator number or name;

e) E-mail; and

f) Printouts.

6.1.5 A record keeping system shall be in place to ensure that a user requesting access has the appropriate authority to make the request.

6.1.6 A verifiable record keeping system shall be established for adding and terminating users.

6.2 Sign-on security

6.2.1 Each security sign-on shall consist of the following:

a) Username of at least six characters; and

b) A password which shall consist of a minimum of six alpha-numeric characters with at least one alpha and one numeric character.

6.2.2 Each individual shall have a personal security sign-on, and when signing-on, the system shall create a record including the following:

a) Time;

b) Date; and

c) Identifying sign-on characteristic of the individual.

6.2.3 Any modification made to the database shall be logged with a unique personal identification belonging to the person performing the modification.

6.2.4 The system shall prompt the user to change the security sign-on password at 3-month intervals.

6.2.5 The system shall not authorize the user to gain access if the security sign-on is not changed after the prompt.

6.2.6 The system shall prohibit the following passwords:

a) Repeated passwords, used within the last six changes;

b) Passwords that are a derivative of the users name(s); and

c) Passwords that are simply letters or numbers in order (e.g.: abcd, 1234, etc.).

6.2.7 Once communication of a session has been idle for a maximum of 15 minutes the session shall be automatically terminated.

6.3 Sign-on security levels

6.3.1 The security sign-on shall govern the access level to the automation system.

6.3.2 The automation system shall have a minimum of five levels (or degrees) of security. The ability to handle or acknowledge signals shall be able to be disabled independently by all individual user levels at any security level. All of the privileges of each security level are available at the next higher security level.

6.3.3 Minimum security level:

a) Shall permit processing and acknowledgment of operator actions in response to signals received from alarm systems; and

b) Shall permit printing or electronic copying of alarm system records.

6.3.4 Second security level:

a) Shall permit temporary, 24 hours maximum, suspension of the automation system's designated activity for specific functions of an alarm system;

b) Shall automatically restore the suspended alarm systems within a predetermined time;

c) Shall be restored upon a change of functions; and

d) Shall permit repeated suspensions of an alarm system.

6.3.5 Third security level shall permit permanent record changes to the automation system's alarm system data base such as adding, deleting, or suspending accounts for longer than 24 hours.

6.3.6 Fourth security level:

a) Shall provide the ability to:

1) Create and/or change system users IDs; and

2) Make changes to time and date.

b) The user shall not be able to change the time and/or date of the following status signals:

1) Dispatch information;

2) Arrival information; or

3) Alarm signal information.

6.3.7 Fifth security level:

a) Is intended to be a level only accessible to the software provider's programmers, or end user IT staff; and

b) Shall provide capability for permanent modification of the alarm monitoring software.

6.3.8 Each succeeding level shall have the privileges of the previous level(s).

7 Automation Multiplicity

7.1 Redundancy requirement

7.1.1 The primary system (See Section 9) shall be capable of supporting a "hot back-up" redundant system, that shall be capable of being on-line, monitoring signals, within 90 seconds. This may take the form of:

a) Another "hot" computer system(s);

b) A fault-tolerant system computer system; or

c) A computer cluster.

7.2 Watch-dog timer

7.2.1 If supported by manufacturer, there shall be a watch-dog timer to provide supervision that the automation system(s) are operating as intended. Should one of the automation systems become unable to process signals, an audible and visual signal shall be annunciated.

Exception: A watchdog timer is not required if the automation system meets the following conditions:

a) The automation system monitors the operation of all active computers and receivers;

b) The automation system is capable of generating an audible and visual signal within 90 seconds of the occurrence of a fault; or

c) A visual display condition under which the failure or switchover condition is obvious to the operator may be used in lieu of both a visual and audible signal.

7.3 Tertiary requirement

7.3.1 If supported by manufacturer, the computer systems described in 7.1.1 shall be duplicated in a separate third "Tertiary System" computer system of equal or greater size, including on-line systems use for the storage of alarm monitoring automation system data or a storage system that complies with RAID-1 or higher, with automatic failover capability.

7.4 Memory

7.4.1 A device that uses a memory storage medium that is subject to continuous wear during the course of normal operation and that is not sealed against atmospheric contaminants shall not be used to hold data that is required to perform the alarm-monitoring functions. Such a device is capable of being used for functions such as:

a) Performing initial loading of software and data base information;

b) Database downloading if system operation is not inhibited;

c) Providing enhancement to basic system descriptors; and

d) Making back-ups of software and data base information.

7.5 Hardware virtualization

7.5.1 Virtualization may be used in a central station provided that:

a) The automation system is guaranteed resources within the system provisioning;

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

c) When redundancy is required of the monitoring system and/or software receiver, the redundant system shall reside on a separate whole hardware system that has sufficient capacity to provide the same or greater alarm monitoring performance as the primary hardware.

8 Processing Signals from Monitored Systems

8.1 All signals from fire alarm systems shall be handled in accordance with the National Fire Alarm and Signaling Code, NFPA 72.

8.2 All signals from burglar alarm systems shall be handled in accordance with the Standard for Central-Station Alarm Services, UL 827.

9 Equipment

9.1 Computer systems used in an automation system shall comply with the Standard for Information Technology Equipment – Safety – Part 1: General Requirements, UL 60950-1 and the Standard for Central-Station Alarm Services, UL 827.

9.2 Computer systems 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.

10 Reports and Records

10.1 General

10.1.1 All recorded data shall be recorded on non-volatile memory.

10.1.2 The system shall be capable of printing change-of-status signals upon demand when given the account number, date, and time, as appropriate.

10.1.3 Upon resolution of any incident resulting in an alarm signal being received, the automation system shall record the following information about all accounts which shall include the following items, as applicable:

a) The name and address of the subscriber;

b) The type of alarm;

c) The designated response time;

d) If the alarm system has line security whether it is standard or encrypted line security;

e) The time the alarm was received by the automation system;

f) The time the alarm signal was acknowledged;

g) Alarm Verification (if used);

h) The time the police/fire department was notified;

i) The identification of the police or fire department personnel that were notified;

j) The time the alarm runner No. 1, if any, was dispatched and the investigator’s name and employee ID;

k) The time the alarm runner No. 2, if any, was dispatched, and the investigator’s name and employee ID.

l) The time the alarm runner No. 1 arrived (if dispatched);

m) The time the alarm runner No. 2 arrived (if dispatched);

n) The elapsed time between the receipt of the alarm signal at the central-station automation system and the arrival of the runner at the protected premises;

o) The method used to verify the alarm arrival of the runner such as radio, telephone, or other means;

p) Whether the Central Station holds keys;

q) Whether the keys were used or not used;

r) The time the subscriber(s) was notified;

s) The name of the notified subscriber;

t) The alarm resolution;

u) Identification of the operator who processed the alarm.

10.1.4 Opening and closing record

10.1.4.1 Where the system is operated in accordance with Section 35.2, Openings and Closings without a Schedule, of the Standard for Central-Station Alarm Services, UL 827, records of opening (disarming) and closing (arming) a system shall include the following:

a) The name associated with the personal identification number (PIN) of the authorized user of the system making the opening or closing; and

b) The actual time of the opening or closing.

10.1.4.2 Where the system is operated in accordance with Section 35.3, Openings and Closings with a Schedule, of the Standard for Central-Station Alarm Services, UL 827, records shall include the actual time of the opening or closing.

10.1.5 Irregular openings and closings

10.1.5.1 Records of any Irregular Openings and Closings shall include the following:

a) The time the unscheduled opening or closing was arranged;

b) The actual time the unscheduled opening or closing occurred; and

c) The name of the subscriber or subscriber's representative scheduling and/or making an unscheduled opening or closing.

10.1.6 If supported by the manufacturer, records of any Inspection, Testing, and Maintenance action shall include the following:

a) Nature of service;

b) Specific equipment inspected, tested, or serviced;

c) Name of central-station representative performing service; and

d) Any follow-up or additional action taken on unwanted alarms.

10.1.7 Account specific reports

10.1.7.1 The automation system shall be able to output the information contained in 10.1.3 – 10.1.6 by account number or account number range.

10.2 System wide reports

10.2.1 The automation system shall be able to output the following standardized statistical reports both by certificated accounts, non-certificated accounts and both combined as indicated below:

a) If the central station has multiple locations then the totals must also be broken down by each central station location that is responsible for delivering monitoring services.

b) Certificated account activity shall include the statistics as specified in 10.2.2 (a) – (g).

10.2.2 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;

c) Alarms for which a runner was required but not dispatched or did not arrive shall be included in the calculation;

d) All statistics shall be broken down by certificate type, such as fire alarm systems, central-station burglar alarm systems, proprietary burglar alarm systems, national industrial burglar alarm systems, mercantile burglar alarm systems, or residential burglar alarm systems, and account number;

e) Total number of events, requiring operator action, that occurred in certificated accounts;

f) Operator acknowledgement time shall be listed by longest time, average time, and shortest time; and

g) Runner response elapsed time shall be listed by longest time, average time, and shortest time. Elapsed time shall be determined by using the difference between the time recorded for the receipt of the alarm signal [See 10.1.3(e)] 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 10.1.3(l).

10.2.3 The automation system shall be able to process signals that are able to be displayed by a receiver to which it is connected.

11 Human Interface

11.1 General

11.1.1 Each operator station that displays change-of-status signal shall have an audible or visual means of alerting the operator to the receipt of a change-of-status signal. Unless operators are dedicated to handling change-of-status signals and stationed at operator stations dedicated to this purpose, the alerting means shall be audible.

11.1.2 The following change-of-status signals shall be indicated to the operators:

a) Alarm conditions;

b) Supervisory conditions;

c) Trouble conditions; or

d) Restoral conditions.

11.1.3 A minimum of one central-station operator or supervisor shall be logged on at all times.

11.1.4 When only one operator or supervisor is logged on, who then attempts to log out, a message shall inform the operator/supervisor that he/she is the last one logged on.

11.1.5 The time, date, type, and location of all signals received by the central-station and requiring operator action shall be automatically recorded and displayed in a form that will expedite prompt operator interpretation in accordance with the following:

a) Routine signals such as disarming and arming (opening and closing) and periodic check-in signals complying with the schedule shall not be displayed.

b) A status change signal that is acknowledged shall be displayed differently from a status change signal that has not been acknowledged.

c) When an audible signal that alerts the operator to receipt of a change-of-status signal is silenced, it is to be re-energized upon receipt of a subsequent change-of-status signal with higher priority from the same account or a change-of-status signal requiring operator action from another account.

d) There shall be means provided for the operator to redisplay the status of signals that have been acknowledged and not yet restored to the normal condition.

e) When the system provides for continuous retention of the signal on the visual display until manually acknowledged:

1) Subsequent recorded presentations shall not be inhibited upon failure to acknowledge; and

2) The visual display shall indicate that additional signals are pending.

f) When only a single display is provided, fire alarm signals shall be given priority status on the common visual display.

g) Multiple function systems shall be configured according to the following functions in descending order of priority:

1) Fire alarm;

2) Emergency call system;

3) Hold-up or panic alarm;

4) Medical, including carbon monoxide;

5) Industrial supervision if a danger can result;

6) Burglar alarm (with line security);

7) Burglar alarm (without line security);

8) Supervisory signal;

9) Trouble signal;

10) Other.

Items 2, 3, and 4 are not prohibited from having equal priority.

h) The signal information content shall be recorded for both alarm and restoration to normal conditions.

11.1.6 When the operator is working from a menu other than the alarm processing menu, and a change-of-status signal requiring operator action occurs, the automation system shall either:

a) Generate an audible and a visual indication of the signal; or

b) Generate an audible signal that continues until the operator resumes alarm processing.

11.1.7 When the operation of a switch or a keyboard key prevents proper operation of the automation system, such operation shall be indicated by one of the following:

a) An audible trouble signal; or

b) An LED, video display, or other visual annunciator.

11.1.8 The operation of an automation system from a standby power source under normal and abnormal conditions is to produce the same signals as when the unit is connected to its primary power source.

11.1.9 The automation system shall be able to automatically identify an alarm system as a runaway system (See 5.47) when the number of signals from that system exceeds the pre-programmed number within the pre-programmed time frame. The following shall occur:

a) It shall immediately and automatically display a message on the operator terminal; and

b) The message shall indicate "runaway" system and identify the details of the alarm system such as type of signal, account number, location, contact person, and similar information.

The automation system supplier shall ensure that the "runaway" counter minimum threshold is more than the "swinger-shut-down" maximum of ANSI/SIA CP-01-2010 count (standard six trips).

11.2 Automation software components

11.2.1 One or more program screens shall display the alarm type signal received with the necessary data required to notify the authorities and the subscriber(s) as needed.

11.2.2 The operation of the automation system shall:

a) Be easily understood and laid out in an orderly fashion;

b) Be alerted by audible annunciation when a new signal is received (See 11.1); and

c) Log the date and time of each action performed by the operator to history. (See Section 10, Reports and Records, for greater detail)

11.2.3 Upon receiving a signal from a receiver, the system shall time and date stamp within the record and shall:

a) Prioritize alarms in the order required by 11.1.5(g);

b) Deliver the new signal to the next available operator in the alarm queue;

c) Move certificated system alarms to the top of each respective priority queue; and

d) Cause an alert when events at given priorities exceed specified wait times (See 11.2.5)

11.2.4 If supported by manufacturer, batch alarm clear shall be done by an authorized individual with a third or fourth sign-on security level. The batch alarms shall have an option to exclude fire alarms and certificated systems.

11.2.5 An alarm pending in the automation alarm queue that goes unprocessed in excess of 90 seconds shall generate an alarm at the central-station signifying there is an alarm pending for handling at the remote site that has not been claimed in over 90 seconds.

12 System Connections from Outside the Central-Station

12.1 The central-station software shall provide for security verification for remote user access that is at least equal to security standards for personnel having access internal to the system location as found in Section 6, Automation Access Security.

12.2 If supported by manufacturer, when access to the system is not over a secure access point and there is no means of verifying the user, there shall be no access.

12.3 If supported by manufacturer, security measures shall be implemented to limit data access to information needed based on the user type or device type. Limitations shall be based on:

a) Geography;

b) Customer type;

c) Business type; or

d) Service type.

12.4 If supported by manufacturer, service technicians shall utilize field equipment that is registered within the monitoring system's database to view data and/or conduct system testing functions including:

a) On test;

b) Off test; and

c) Test results.

12.5 If supported by manufacturer, forms of communication between the technicians and the system include but are not limited to:

a) Voice automation;

b) Dual tone multi-frequency signaling (DTMF); or

c) Smart device.

12.6 If supported by manufacturer, all employees capable of changing data shall provide user security sign-on codes as found in Section 6, Automation Access Security.

12.7 The automation system shall be capable of immediately sending electronic notifications to the designated end user any time a data change is made to a subscriber account.

12.8 Forms of connectivity between the system and the subscriber include but are not limited to:

a) Voice automation;

b) Text messaging;

c) Electronic mail;

d) Smart devices; or

e) Internet.

12.9 The ability to change data shall not include the capability to change a user account.

12.10 Violations of rules stated in this Section shall create an alarm condition for response by the central-station.

13 Hardware Receiver Requirements

13.1 The automation software developer shall provide an information screen that will list all compatible receivers.

PERFORMANCE

14 System Performance

14.1 General

14.1.1 Except as otherwise indicated, the performance of an automation system shall be investigated by subjecting a representative sample in commercial form to the tests described in Sections 14 through 16 (The chart in Appendix B may be used as an example for documenting the performance check).

14.2 Performance Monitoring

14.2.1 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% 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.

14.2.2 The report shall include the following:

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

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

1) Any constraints to the database resulting from its configuration shall be recorded.

2) Any constraints of the data storage system shall be recorded.

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% increments, starting at less than 20% and going up. If the utilization of any of these exceeds 80% averaged over 15 minutes an audible and visual notice shall be annunciated in the operating room.

14.3 Signal processing throughput

14.3.1 An automation system shall make signals, requiring operator action, available to the operator within ten (10) seconds of the receiver making it available to the automation system.

15 Normal Operation Test

15.1 An automation system shall be capable of operating for all conditions of its intended performance as indicated in the user's instruction manual when used in conjunction with the equipment indicated by the installation wiring diagram and information supplied with it.

15.2 To determine compliance with 15.1, the compatible receiving and transmitting equipment is to be connected to an automation system as specified by the installation wiring diagram to form a typical combination. The system is then to be operated for each condition of its intended performance as stated in the user's manual. An example of a worksheet for recording data is shown on the Automation System Check Sheet found in Appendix B.

16 Operation Test – Degraded Mode

16.1 Upon failure of the automation system - whether redundant or non-redundant - the required functions of the receivers connected to the automation system which may be suppressed shall:

a) Revert to their normal operation;

b) Automatically print all change-of-status signals and generate an audible signal under the degraded mode of operation; and

c) Not cause a loss of signal when the system enters the degraded mode of operation.

16.2 When an automation system is operating in a degraded mode, change-of-status signals shall be processed manually.

16.3 Whether the automation system is a non-redundant or redundant system, all of the following records shall be maintained and readily available at the central-station.

Exception: The maintenance of records requirements shall be superseded by the requirements of the Standard for Central-Station Alarm Services, UL 827, Section 17, Alarm Monitoring Systems.

a) Dispatch instructions;

b) Arming and disarming, (opening and closing) schedules;

c) Pass card data;

d) Holidays observed and schedules, and the time and date that the data file was created;

e) Meet the requirements specified in the Records sections (fire alarm, and burglar alarm) in the Standard for Central-Station Alarm Services, UL 827, as appropriate;

f) A means to permanently record the date and time the action was taken to respond to change-of-status events; and

g) A means to transfer the data from manually-generated activities into the automation system's permanent record when the automation system is back in normal operation, shall be provided.