



UL 1981

STANDARD FOR SAFETY

Central-Station Automation Systems



Documents
Document Sharing Hub

*UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL*



Documents

Document Sharing Hub

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

Second Edition, Dated June 30, 2003

Summary of Topics

This revision is being issued to update the surge protection device requirements in 7.1.1.

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. Changes in requirements are marked with a vertical line in the margin and are followed by an effective date note indicating the date of publication or the date on which the changed requirement becomes effective.

The revised requirements are substantially in accordance with Proposal(s) on this subject dated August 19, 2011.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without prior permission of UL.

UL provides this Standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

In no event will UL be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this Standard, even if UL or an authorized UL representative has been advised of the possibility of such damage. In no event shall UL's liability for any damage ever exceed the price paid for this Standard, regardless of the form of the claim.

Users of the electronic versions of UL's Standards for Safety agree to defend, indemnify, and hold UL harmless from and against any loss, expense, liability, damage, claim, or judgment (including reasonable attorney's fees) resulting from any error or deviation introduced while purchaser is storing an electronic Standard on the purchaser's computer system.

The requirements in this Standard are now in effect, except for those paragraphs, sections, tables, figures, and/or other elements of the Standard having future effective dates as indicated in the note following the affected item. The prior text for requirements that have been revised and that have a future effective date are located after the Standard, and are preceded by a "SUPERSEDED REQUIREMENTS" notice.

The following table lists the future effective dates with the corresponding reference.

Future Effective Date	Reference
July 9, 2016	Paragraph 7.1.1



JUNE 30, 2003

(Title Page Reprinted: June 19, 2012)

1

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 30, 2003

This UL Standard for Safety consists of the Second Edition including revisions through June 19, 2012.

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 <http://csds.ul.com>.

UL's Standards for Safety are copyrighted by UL. Neither a printed nor electronic copy of a Standard should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of UL.

COPYRIGHT © 2012 UNDERWRITERS LABORATORIES INC.

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents

Document Sharing Hub

No Text on This Page

*UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL*



Documents

Document Sharing Hub

CONTENTS

INTRODUCTION

1 Scope	5
2 General	5
2.1 Components	5
2.2 Units of measurement	6
2.3 Undated references	6
3 Glossary	6
4 Installation Instructions	10

CONSTRUCTION

5 General	12
6 Power Supply Sources	12
7 Electrical Transient Protection	12
7.1 Supply-line transient protection	12
7.2 Signaling-line transient protection	12
8 Environmental Controls	13
9 Central-Station Staffing	13
10 Power Conditioners	13
11 Uninterruptible Power Supplies	13
12 Printerless Environment	14
13 Back-up Components	14
14 Spare Parts – Maintenance and Service	17
15 Alarm Receiving Equipment	17
16 Back-up Media	18
17 Remote Connections	18
18 Compliance Verification Chart	23

PERFORMANCE

19 General	24
20 Normal Operation Test	24
21 Operation Test – Degraded Mode	28
22 Operation Test – Degraded Mode, Alternate Path	28
23 System Response Time	29
24 Program Access and Control	29
25 Electrical Supervision Test	31
26 Receiver Compatibility Test	31

APPENDIX A

Standards for Components.....	A1
-------------------------------	----

No Text on This Page

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents
Document Sharing Hub

INTRODUCTION

1 Scope

1.1 These requirements cover computerized central-station automation systems intended for use in central-station, proprietary, remote and subsidiary burglar-, and fire-alarm applications for the purpose of automating the signal handling and processing of change-of-status signals generated by receivers. In case of failure of an automation system, the receiving equipment is relied on for receiving and recording change-of-status signals and the provision of an audible and visual signal that identifies the source and type of signal that requires operator attention. These systems are intended to be installed in accordance with the following:

- a) The National Electrical Code, NFPA 70;
- b) The National Fire Alarm Code, NFPA 72; and
- c) The Standard for Central-Station Alarm Services, UL 827.

1.2 A product that contains features, characteristics, components, materials, or systems new or different from those covered by the requirements in this standard, and that involves a risk of fire or of electric shock or injury to persons shall be evaluated using appropriate additional component and end-product requirements to maintain the level of safety as originally anticipated by the intent of this standard. A product whose features, characteristics, components, materials, or systems conflict with specific requirements or provisions of this standard does not comply with this standard. Revision of requirements shall be proposed and adopted in conformance with the methods employed for development, revision, and implementation of this standard.

2 General

2.1 Components

2.1.1 Except as indicated in 2.1.2, 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.

2.1.2 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.

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

2.1.4 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.

2.2 Units of measurement

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

2.3 Undated references

2.3.1 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.

3 Glossary

3.1 For the purpose of this standard the following definitions apply.

3.2 ACTIVE SYSTEM – Any system that is preprogrammed to send more than 1 signal per day to the central station automation system.

Revised 3.2 effective June 30, 2005

3.3 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 on the operator terminal and printers.

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

3.5 ANSWERBACK – A technique whereby modems contain keywords (not less than eight characters long) that are identical. When one modem "calls" the other, they automatically exchange their keywords and, when there is a match, they stay on-line. This interaction shall happen within three seconds or the called modem goes on-hook.

3.6 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 automated system may be configured as a computer system that is directly connected to central-station 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, disarmings and armings (openings and closings), and similar signals that it receives from the central-station receiving equipment.

3.7 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 terminal; printer; interface equipment; and similar equipment.

3.8 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 Code, NFPA 72;
- b) The Standard for Central-Station Alarm Services, UL 827; and
- c) The requirements of this standard.

3.9 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 numbers, and fire department phone numbers; and graphics.

3.10 CALLBACK – A technique whereby a "called" modem will accept only passwords that it is programmed to accept. Once a match is made, the modem goes on-hook, then off-hook, and dials a predetermined telephone/modem number.

3.11 CENTRAL-STATION – A building, or enclosed area within a building, that houses an operating room and equipment used to provide central-station service to protected properties that are served by the central-station. Refer to the Standard for Central-Station Alarm Services, UL 827, and the National Fire Alarm Code, NFPA 72.

3.12 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.

3.13 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.

3.14 *Deleted June 30, 2003*

3.15 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; or the National Fire Alarm Code, NFPA 72.

3.16 CONTROL UNIT, CENTRAL-STATION (RECEIVING UNIT) – Electrically operated receiving equipment located at a central-station which monitors the status of protected premises. The receiving equipment connected to an automation system receives signals from alarm systems and transmits them to the automation system.

3.17 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.

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

3.19 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 3.21 and 3.33 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.

3.20 **HARDWARE** – Physical computer equipment (computer, disk drive, terminal, printer, memory boards, and similar equipment) that constitutes the automation system.

3.21 **HOT BACK-UP** – A continuously energized computer system that is a back-up to the primary system computer and disk drive. The alarm system (account) information/signal processing is constantly updated in both computers.

3.22 **HVAC SYSTEM** – Heating, ventilating, and air conditioning system.

3.23 **INACTIVE SYSTEM** – An alarm system that transmits a signal to the central-station only when an exception alarm, trouble, or supervisory condition exists or it is under test. Examples of an inactive alarm system are fire and holdup alarm systems, and burglar alarm systems supervising protected premises without the use of disarming and arming (opening and closing) signals. The 24-hour supervisory check-in signal transmitted by a digital alarm communicator transmitter or a one-way radio (RF) transmitter does not make an alarm system an active alarm system. An alarm system is considered inactive when the 24-hour supervisory signal is the only signal normally transmitted on a daily basis.

3.24 **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.

3.25 **LEVEL OF ACCESS** – The privileges associated with the security sign-on to the automation system. This is typically defined as having the ability to do one or more of the following to the automation system database or the alarm-monitoring software:

- a) View only,
- b) View and modify only,
- c) Add,
- d) Delete,
- e) Access alarm-monitoring software,
- f) Access certain segments of the database,
- g) Alter "master" files,
- h) Alter "operating" parameters, and
- i) Stop and start the computer.

These privileges can also be mixed for one security sign-on giving various levels of access to different functions of the system.