UL Compliance

Responses to the UL 1981 document : Standard for Central-Station Automation Systems (Second Edition June 30, 2003)

Unlisted Requirements are believed to be the responsibility of the Central Station, and not the Automation Software.

Installations of stages™ are not considered compliant until a UL site certification evaluation has been completed. Refer to UL Site Certification Bulletin.

Installation Instructions

4.1 A copy of the operating and installation instructions shall be furnished with the automation system submitted for investigation and shall be used as a guide in the examination and test of the system. A final edition is not required for this purpose.

stages™ documentation is provided in an Online Wiki.

4.2 The instructions shall include concise descriptions of the operation, testing, and maintenance procedures for the product(s), and recommended testing frequency. Additional information is not prohibited from being included.

stages™ documentation provides descriptions of all operations of the application.

4.3 The instruction manual shall have a section which specifically describes the system configuration. This section shall include the following equipment requirements for the automation system:
a) Minimum system specifications - 1) Operating system class, minimum revision level and/or kernel type and revision level; 2) For PC-based systems, the most basic microprocessor that the software is designed to work with and the minimum speed of the microprocessor. For systems using minicomputers, the basic system model or family as well as the microprocessor and its speed designation; 3) Minimum disk storage space required; 4) Minimum internal memory size; and 5) Minimum revision level of the alarm-monitoring software. b) Environmental controls - Hardware shall be located in an environment where the temperature is maintained at a level within the temperature rating range of the equipment. c) HVAC standby power - The HVAC system shall have 24 hours of standby power. The standby power for the HVAC shall be provided by the central-station's engine-driven generator(s). When the central-station chooses to do so, it may provide the standby power for the HVAC system by an uninterruptible power supply (UPS), or similar equipment. Exception: When the hardware is rated for use in environments with temperatures between 32°F (0°C) and 120°F (49°C), standby power is not required for the HVAC system. d) Source of power - 1) Hardware shall be powered by a UPS that complies with either the Standard for Uninterruptible Power Systems, UL 1778, or the Standard for Power Supplies for Fire-Protective Signaling Systems, UL 1481. 2) In order to perform maintenance and repair service, a means for disconnecting the input to a UPS and output from a UPS while maintaining continuity of power supply to the automation system shall be provided. 3) When a power conditioner is being used, it shall comply with the Standard for Power Units Other Than Class 2, UL 1012. In order to perform maintenance and repair service, a means for disconnecting the input to a power conditioner and output from a power conditioner while maintaining continuity of power to the automation system shall be provided. e) Supply-line transient protection - Hardware shall be protected by transient voltage surge suppressors that comply with the Standard for Transient Voltage Surge Suppressors, UL 1449. The transient voltage surge suppressors for single-phase, 120/220 V AC systems shall have a marked rating of 330 volts or less. The transient voltage surge suppressors for

3-phase, 480 V AC or higher-rated systems shall have a marked rating of 400 volts or less. f) Signaling-line transient protection - 1) The communication circuits contained within the central-station building and not connected to the telecommunications network shall be protected by isolated loop circuit protectors. These protectors shall comply with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, and shall have a marked rating of 50 volts or less. 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, and shall have a marked rating of 150 volts or less. These protectors shall be used only in the protected side of the telecommunications network. Exception: Equipment connected to telecommunications circuits which has been evaluated to the requirements of the Standard for Control Units for Fire-Protective Signaling Systems, UL 864, are not required to have protection devices evaluated to the requirements of UL 497A. g) Minimum system configuration - List of components constituting minimum system configuration for redundant/non-redundant systems (including CRTs, printers, computers, watchdog timers, and similar equipment). h) Software version - Instructions on how to display the software version. Information on Hardware configuration and Software version is included in the Wiki. All hardware components shall be UL listed. Basic Configuration Diagram

Central Station Staffing

9.1 Central-station staffing shall be such that all alarm signals are acknowledged and verification and/or dispatch actions initiated within 45 seconds of receiver kiss-off to the alarm panel.

Elapsed time is displayed for accounts in alarm on the Alarm Buffer, Dispatch Queue, and stages™ Summary windows.

The Operator Retrieval Time is included in the Alarm History report.

Printer-less Environment 12.1 A central-station is not prohibited from using computer equipment (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 operator/responsible central-station staff. In addition, the central-station staff shall be capable of, and the back-up computer shall be ready for, switching over within 30 seconds so that the back-up computer is energized and connected to the affected receivers. c) The primary and back-up computers shall be isolated from the automation system computer/s (i.e., these computers shall not be configured in such a way that the signals from the receivers that are intended to be transmitted to the automation system computer/s have to first pass through the primary and back-up computers). d) The primary and back-up computers shall have transient protection as required in Electrical Transient Protection, Section 7. e) The communication lines between the computer and the receiver must 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) The captured signals must be retrievable upon demand in maximum 5 seconds. g) Signals must be presented, at a minimum, in the same manner as they would be by receiver printers.

stages™ does not offer a solution. Customers may use third party applications or equipment.

Back-up Components

13.3 In a hot redundant or a fault-tolerant configuration, failure of either the primary or back-up computer system, and switchover to its back-up shall be indicated by an audible and visual signal within 90 seconds of the occurrence of the fault. A visual display condition under which the failure or

switchover condition is obvious to the operator is not prohibited from being used in lieu of both a visual and an audible signal.
Failure of a primary server will result in a specific error message. The failure will be obvious to operators and does not require audio signals. Servers are monitored by tasks and generate an alarm on the Alarm Buffer and auto fed to an operator. Server tasks shall be set up with a Site for alarm generation.

13.5 When the automation system serves more than 25,000 active accounts or more than 125,000 inactive accounts, the primary and back-up computers shall be configured in a hot back-up mode. In addition, the following conditions shall be met:

stages™ uses hot back-ups of all its systems. Redundancy transactions run constantly between the servers and are monitored to ensure their status. Redundancy Status is available at any time and displayed on the stages™ Summary window. If there is a redundancy problem, an alarm will be generated and auto-fed to an appropriate operator.

a) There shall be a second back-up computer that has the same capacity and performance as the primary or the first back-up computer.

For large systems, a second hot back-up server is required.

b) In the event of failure of the automation system's primary and first back-up computers, central-station staff shall be capable of, and the second back-up computer shall be ready for, switching over within 30 seconds so that the second back-up computer is energized and connected to the receivers and other devices required for the system. The second back-up system shall be fully operational within 6 minutes of the loss of the primary or the back-up system. This allows 30 seconds for plugging in the computer and switching the communication lines over to the second back-up system and also allows 5-1/2 additional minutes for the system to boot up, conduct memory tests, file system check, security verifications, and prepare for full operation. The second back-up computer shall have all the capabilities of the primary or the back-up automation system, including capacity and speed. The central-station operators and supervisor(s) shall be trained monthly in making the switchover and bringing the second back-up computer on-line.

The Second back-up server can be on at all times and ready to be switched over. The back-ups are required to have the same minimum specifications of the primary servers. Web Servers are all active and switch over is handled by pointing the application to the URL of the back-up server. Database servers are switched by a Supervisor logging in to the inactive database server and selecting it as active in the Servers window (Utilities | stages™ | Servers)

c) The second back-up computer shall have its own UPS which meets all of the requirements specified in this standard or is configured in such a way that it is capable of being connected to the primary or first back-up computer's UPS in time to meet the requirements of 13.5(b).

Central Station responsibility

d) The alarm system data base on the second back-up computer shall be updated not less than once every 24 hours.

The Second back-up server can be on at all times and participating with the constant redundancy transactions sent between servers.

e) All the network equipment through which signals pass is redundant. Redundancy is capable of being achieved by having a back-up network equipment placed near the on-line unit so that connection to the network is accomplished in 6 minutes.

Central Station responsibility

13.6
In a hot redundant or a fault-tolerant configuration, failure of either the primary or back-up computers, and switchover to their back-up shall be indicated by an audible and visual signal within 90 seconds of the occurrence of the fault. A visual display condition under which the failure or switchover condition is obvious to the operator is not prohibited from being used in lieu of both a visual and an audible signal.

Redundancy issues are tracked on the stages™ Summary window. The Summary window refreshes within 90 seconds and displays if there is a redundancy problem. Switching the database server is done by a supervisor in the Servers window and does not require any action from the operators.

Remote Connections

17.2 Terminals from which automation system records and/or data can be changed are not prohibited from being connected to the central-station automation system from a location outside the central-station when the following conditions are met:

Conditions A-E and G are Central Station responsibilities.

f) Programmed security: 1) A security sign-on consisting of a minimum of six alpha-numeric characters shall be required.

Security Logins require a minimum number of characters as defined by the user.

2) Each individual shall have a personal security sign-on.

A unique Username/Password is required to log into stages™.

3) The time, date, and identifying characteristic of the individual signing-on shall be recorded.

All current logins are available in the Sessions window and the stages™ Summary window. A history of logins is available in the Session History report.

4) Any modification made to the data base shall be logged with a unique personal identification belonging to the person performing the modification.

The Data Change Log records all edited information with user information. The Event History records all events with user information.

5) Each user's security sign-on shall be required to be changed not less than once every three months. The system shall prompt the user to change the security sign-on at 3-month intervals . The system shall not authorize the user to gain access if the security sign-on is not changed after the prompt.

Password Changes are required by stages™ on a user-defined interval. Access is not allowed until the password is changed.

17.3 With respect to 17.2(f)(4), each area of the system that is modified shall be identified by the personal code. This user/modification information shall be stored on the system for a minimum period of 3 months. However, the central-station is required to keep the information available for retrieval for a minimum of 1 year.

Data Change Logs are stored in stages™ with user information. Data Change Logs do not expire.

17.6 The automation system of a central-station is not prohibited from being used by other central-stations or subsidiary stations of the same company when the following conditions are met:

a) Redundancy is provided for the automation system's primary computer, hard drive, alarm monitor, UPS, and all communication components of the network such as modems, concentrators, and similar equipment when the total number of active and inactive accounts for both the main central-station and remote central-station exceed 200 and 1000 accounts, respectively. Switchover to the back-up automation system shall occur as specified in 13.2(a).

Redundancy is provided for systems using multiple locations. Back-up systems are recommended in the 'remote' locations as well as the 'primary' location.

b) The communication components of the network such as the modems, concentrators, and similar devices shall comply with the requirements for each respective component.
All hardware components are required to have UL Listings and meet the minimum requirement to operate stages™.

c) Each of the central-stations and subsidiary stations that use the automation system are able to generate alarm record information required under 20.8 - 20.10 for the alarm systems (accounts) for which each is responsible.

Reports can be generated at Remote locations.

d) All the signal processing requirements contained in the Normal Operation Test, Section 20, shall be complied with.

Remote locations must follow the same guidelines as the primary location.

e) All ports of the automation system, and all of the networking components, except those connected to the telecommunications network, shall be protected by isolated loop circuit protectors for communication circuits. These protectors shall comply with the requirements in the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B. The transient protectors shall have a marked rating of 50 volts or less. Exception: 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.
All hardware components are required to have UL Listings.

f) 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. Exception: Equipment connected to telecommunications circuits which has been evaluated to the requirements of the Standard for Control Units for Fire-Protective Signaling Systems, UL 864, are not required to have protection devices evaluated to the requirements of UL 497A.
All hardware components are required to have UL Listings.

g) Failure of the primary or the back-up automation system shall be indicated at all of the central-stations and subsidiary stations using the system in such a way that it is obvious to the operators.

Failures of the primary or back-up automation system generate alarm conditions on the Alarm Buffer or result in error messages within the application to inform of the database server or web server disconnection.

h) Provisions shall be made at all of the central-stations using the automation system for operation in a degraded mode as described in the Operation Test - Degraded Mode, Section 21, or the Operation Test - Degraded Mode, Alternate Path, Section 22. The operators and supervisors shall be trained as specified in 13.1(b) and 13.2(b).

Receivers shall be set up to revert to manual mode when disconnected and operators/supervisors trained for degraded mode operations.

17.8 An automation system located at a subsidiary station shall comply with the following conditions:

a) The system shall comply with all requirements of a central-station automation system.

Remote locations are required to comply with all requirements of the primary location.

b) Redundancy is required in all cases.

Redundancy is provided for all stages™ systems.

c) A hot back-up computer shall be provided.

All stages™ systems require hot back-ups.

d) Failure of the main or back-up subsidiary station computer shall be indicated at the central-station.Revised 17.8(c) effective June 30, 2005
Failures will result in alarm conditions on the Alarm Buffer and auto fed to an operator or result in error messages within the application to inform of the database server or web server disconnection.

Compliance Verification Chart

18.1 The automation system shall be provided with a compliance verification chart as described in 18.2.

A UL Compliance Chart is provided in the wiki for reports and priorities.

18.2 The compliance verification chart shall include information on the following subjects, explaining the steps to be taken to properly set up the automation system in order to comply with the requirements for installation and operation of the system:

a) Reports: Instructions indicating that reports of the following items for certificated systems shall be up-to-date and kept for a minimum of one year. Items 1 - 5 may be stored on non-volatile memory if they can be retrieved and printed once the automation system is given the account number, date, and time, as appropriate.

1) Alarm tickets. 2) Disarm/arm (Open/close) schedule for each account. 3) Fire alarm signals. 4) Panic / hold-up alarm. 5) Burglar alarm signals. b) Priority Levels: The automation system shall prioritize signals to the operator as follows. 1) Fire alarm. 2) Hold-up or panic alarm. 3) Medical. 4) Industrial supervision if a danger can result (critical process alarm).

5) Burglar alarm. 6) Other. Items 2, 3 and 4 are not prohibited from having equal priority.

Reports are available within stages™ and can be distributed in various ways. Reports can also be

created on demand. Reports can be filtered to show only specific groups of signals using report codes.

Alarms are assigned to Priorities. Stages™ will auto-feed alarms with a higher priority first. The priorities are entered and ordered by the central station.

Normal Operations Test

20.3 The automation system shall have an operator terminal and the capability to generate an audible signal, as a means of alerting the operator to receipt of a change-of-status signal from any receiver. Change-of-status shall include changes to activated, trouble, or restored conditions. Change-of-status signals shall be recorded on non-volatile memory or the equivalent.

Any computer on the network can be used as an operator terminal. An account going into alarm will be auto-fed and locked to an operator and come to the front of the window. Audible signals are generated for additional signals received on an already locked account. All signals are recorded into the Signal Log and the Site History. Changes to the data base are saved at the time the change is made. Power interruption will not cause changes to be lost.

20.4 A minimum of one central-station operator or supervisor shall be logged on at all times. To ensure this, the system shall not allow all alarm-handling users to be logged out at one time. When only one operator or supervisor is logged on, who then attempts to log out, a message informing the operator/supervisor that he/she is the last one logged on is acceptable.

A message will display on attempted logout by an operator when there are no other operators logged in.

20.5 The time, date, type, and location of all signals received by the central station and requiring operator action are to be automatically recorded and displayed in a form that will expedite prompt operator interpretation in accordance with the following. To avoid operator overload, routine signals such as disarming and arming (opening and closing) complying with the schedule shall not be displayed.

Alarm Signals are displayed with time, date, type and location in the Alarm Buffer and entered into Dispatch Queues. Signals are applied EventCodes which are assigned to Priorities and can be identified as Alarms. Only event codes identified as Alarms will appear in the buffer and entered into queues.

a) Signals requiring operator action and acknowledgment shall be both displayed on the operator terminal and recorded on hard disk.

Signals requiring operator action are displayed on the Alarm Buffer window and recorded into Site History. The Alarm Buffer displays only the highest priority alarm signal for the site. When the site is accessed via the Alarm Buffer or Auto Feed, the operator is required to review the Recent History for any other alarm conditions that may apply. Additional signals received after the account has been accessed will generate a Status Change message accompanied by an audible tone.

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

Signals that have been accessed by an operator will display the Operator Initials in the Alarm Buffer.

c) The visual information component shall be either retained on the display, or shall be periodically

repeated at intervals of no more than 5 seconds and remain on for 2 seconds, until manually acknowledged.

The signals are retained on the Alarm Buffer until the Alarm is cleared. The buffer refreshes.

d) Each displayed signal requiring operator action shall be accompanied by an audible indication. Refer to the Exception to 20.3.

The Alarm Buffer refreshes automatically. An audible indicator accompanies the refresh when a new alarm is detected.

e) 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.

Alarms do not leave the Alarm Buffer until they have been cleared or delayed. The Alarm Buffer can include Alarms that have been delayed. Accounts that require restore can be displayed in the Pending Restorals window (Utilities | Lists | Pending Restorals).

f) When the system provides for continuous retention of the signal on the visual display until manually acknowledged, subsequent recorded presentations shall not be inhibited upon failure to acknowledge, and the visual display shall indicate that additional signals are pending.

Additional signals are not inhibited by a previous signal not being acknowledged. All alarm signals appear in the Alarm Buffer, and are placed into a dispatch queue for auto feed.

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

The Alarm Buffer Buffer is ordered by priority.

h) Multiple function systems shall be configured according to the following functions in descending order of priority:
1) Fire alarm. 2) Hold-up or panic alarm. 3) Medical. 4) Industrial supervision if a danger can result. 5) Burglar alarm. 6) Other. Items 2, 3, and 4 are not prohibited from having equal priority. The signal information content shall be recorded for both alarm and restoration to normal conditions.

Event Codes are assigned to priorities and are handled in order of priority.

20.6 All change-of-status signals shall be recorded on non-volatile memory. The system shall be capable of printing change-of-status signals upon demand when given the account number, date, and time, as appropriate.

Event Codes are logged to the database in site history and constantly sent to redundant systems. A Detailed Activity report can be printed for a site and date.

20.7 All operator actions, such as acknowledgment of signals, dispatch, alarm resolution, and the like, shall be automatically recorded on non-volatile memory with the time, date, and operator's unique personal identification specified. The date is to include day, month, and year; or day of the year and the year. The year is to be recorded in four digits.

Operator Actions are logged to the database in site history and constantly sent to redundant systems. A Detailed Activity report can be printed for a site and date.

20.8 Upon resolution of a fire, hold-up, or burglar alarm incident, the automation system shall

automatically generate an alarm report for certificated accounts and record it on non-volatile memory. The system shall be capable of generating an alarm report upon demand for non-certificated alarm systems. This report shall include the following items, as applicable:
a) The name and address of the subscriber (fire/burglar); b) The type of alarm (burglary, hold-up, fire); c) The designated response time (burglar); d) Whether there is standard or encrypted line security. When provided, it shall be indicated; e) The time the alarm was received by the automation system (fire/burglar); f) The time the police/fire department was notified, and the police/fire department identification number (fire/burglar); g) The time the alarm investigator No. 1 was dispatched, and the investigator's name and employee ID (fire/burglar); h) The time the alarm investigator No. 2 (if any) was dispatched, and the investigator's name and employee ID (burglar); i) The time the alarm investigator No. 1 arrived (fire/burglar); j) The time the alarm investigator No. 2 arrived (if dispatched) (burglar); k) The elapsed time between the receipt of the alarm signal at the central-station automation system and the investigator's arrival at the protected premises; l) The method used to verify the alarm investigator's arrival such as radio, telephone, or other means (fire/burglar); m) Whether the central-station holds keys; n) Whether the keys were used or not used (fire/burglar); o) The time the subscriber was notified, the name of the notified subscriber (2 or 3 lines might be required for multiple notifications) (burglar/fire); p) The disposition of the alarm (fire/burglar); and

q) Whether a sounding device is provided on the alarm system (optional).

Alarm History is created automatically and stored to the database. Alarm History is entered into the Alarm History window and can be printed at any time. The UL Alarm Report can be generated on the operator terminal and printed at any time. UL Certificated Accounts must be properly setup and dispatched.

20.9 The automation system shall be capable of displaying the alarm report on an operator terminal and printing it upon demand.
Alarm History for a specific account can be accessed from the Dispatch window. The UL Alarm Report can be generated on the operator terminal and printed at any time.

20.10 The automation system shall be capable of identifying, sorting, recording, and displaying fire and burglar alarm certificated accounts by type and designated response time (burglar). The automation system shall store one year of alarm history on burglar and fire alarm certificated accounts. The automation system shall be able to display on an operator terminal and print upon demand the alarm reports for all certificated accounts in the automation system's alarm system data base.
Certificated Accounts are applied a UL Code, with a different UL Code for each type and designated response time. Sites can be searched by UL Code. History information does not expire. The alarm history and UL Alarm Report can be generated on the operator terminal and can be printed.

20.11 The automation system shall be capable of displaying the software version so it can be easily verified. The software version may be displayed on the main log-in menu screen or on all screens.

The About window accessed from the Help menu displays the Version number of stages™ and its components.

20.12 The automation system shall be capable of displaying, on demand, the number of active and inactive accounts that it has on the data base.

The number of active and inactive accounts is available in the Account Statistics window.

20.13 The automation system shall be capable of displaying active/inactive accounts for each receiver to which it is connected.
The Account Statistics window can be filtered by a range of transmitters. The pre-fix of the xmit number should refer to the receiver.

20.14 The automation system shall be capable of generating a printed record of change-of-status signals for a specific period of time for a specific account when given the account number, initial and final time, and date for that period. For certificated burglar and fire alarm accounts, one year of change-of-status signals shall be resident on the automation system for retrieval upon demand.

The Detailed Activity report shows all activity on a site for a given time frame. Information on the database does not expire.

20.15 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.

In a locked account, Status Changes give an audible signal and must be acknowledged before proceeding with dispatch. Operators can only access one account at a time, a list of other accounts in alarm can be viewed in the Alarm Buffer. The buffer gives an audible tone when a new item is entered into the list.

20.16 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 generate an audible and a visual indication of the signal.

When an operator receives an account through auto feed, the Account comes to the front of the screen regardless of where the user was before.

20.17 When the operation of a switch or a keyboard key prevents proper operation of the automation system, such operation is to be indicated by an audible trouble signal, or by an LED, video display, or other visual annunciator during any operating condition of the automation system.
Errors in the application pull up error messages that are modal and must be acknowledged before proceeding.

20.18 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.

The power source does not alter the operations of the application.

20.19 The automation system shall be able to automatically identify an alarm system as a runaway system when the number of signals from that system exceeds the preprogrammed number within the preprogrammed time frame. It shall immediately and automatically display a message on the operator terminal. The message shall indicate "runaway" system and identify the details of the alarm system such as account number, location, contact person, and similar information.

Runaway conditions are defined in the stages™ Options window. When the conditions are met, a ‘possible runaway’ message displays on the Recent History window bar in the Alarm Dispatch window. The operator can then place the account on test from the Recent History window. Accounts placed on test will not appear in the Alarm Buffer or be auto fed to an operator.

Operations Test - Degraded Mode

21.1 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 revert to their normal operation. Under the degraded mode of operation, the receiver shall automatically print all change-of-status signals and generate an audible signal to alert the operator of the computer failure. There shall be no loss of signal when the system enters the degraded mode of operation. The receiver shall be situated so that operators can easily gain access to the readouts of the receiver.

Receivers are required to revert to manual mode. Tasks are required to be set up for each receiver for signal processing and receiver monitoring. The task will generate an alarm condition it does not receive a poll message from the receiver. A site is required to be set up for each Task to be placed in alarm if a disconnection or failure occurs. The alarm will appear in the Alarm Buffer and auto fed to an operator.

21.2 When an automation system is operating in a degraded mode, change-of-status signals must be processed manually. Whether the automation system is a single or redundant system, the following records shall be maintained at the central-station:
a) The most recent record of the alarm system data base shall be maintained and be readily available for all accounts. This record shall include, as appropriate, dispatch instructions, disarming and arming (opening and closing) schedules, pass card data, holidays observed and schedules , and the time and date that the data file was created. Additionally, record data shall 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. b) A means to permanently record the date and time the action was taken to respond to change-of-status events. c) 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 back in normal operation.

If the application is still running, but not receiving signals from receivers, the signals can be manually entered into the application through the Signal Entry window and will be handled as if they were entered by the receivers.

Operations Test - Degraded Mode - Alternate Path

22.1 Use of a second back-up computer in order to minimize reliance on manual records is not prohibited when the following conditions are met:

a) The primary and first back-up computers are configured in a hot back-up mode and

All servers are configured as hot back-ups and perform constant redundancy checks.

b) The requirements of 13.5 (a) - (d) are met.

Requirements met. 13.5

System Response Time

23.1 The time lapse from the receipt of a signal that is received at the receiver and requires operator action until the signal is displayed and recorded by the automation system shall not exceed 10 seconds. Displaying the signal may be in the form of updating the number of signals in queue.

Signals are processed continuously and entered into alarm queues if applicable. In the event of Signal Processing failure, an alarm is generated.

23.2 When the central-station automation system is duplicated, either manual or automatic switchover shall be accomplished as described in 13.2(a).

stages™ constantly has redundancy transactions between the servers. Switchovers can occur at any time.

Program Access and Control

24.2 The central-station staff shall not be able to change the time and date when change-of-status signals are received and processed, including dispatch, arrival, and similar information.

Logged times and dates are not editable within the application.

24.3 The automation system shall have a minimum of four levels (or degrees) of security. In order to operate the automation system, a security sign-on code consisting of not less than six alpha-numeric characters shall be required. The security sign-on shall govern the access level. The levels of security shall be as follows:

a) Minimum security level - Shall permit acknowledgment of operator actions in response to signals received from alarm systems. It shall also permit printing or electronic copying of alarm system records. This level shall not affect the ability of the automation system to perform its alarm system monitoring functions. b) Second security level - Shall permit temporary (24 hours maximum) suspension of the automation system's designated activity for specific functions of an alarm system. The preprogrammed condition shall automatically be restored within a predetermined time of change of function. Suspension may be repeated at the discretion of the central-station staff with this security level. c) 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. d) Fourth security level - Shall provide the ability to change central-station operator IDs, or changes to time and date. The user shall not be able to change the time and/or date of change-of-status signals that are received and processed, including dispatch, arrival, and similar information. e) High security level - Shall provide capability for permanent modification of the alarm-monitoring software. This is intended to be a level only accessible to the software provider's programmers.

stages™ provides customizable permissions and permission groups to apply to the application users. There is no limit on the number of permission groups. SGS retains access to change the monitoring application for support and updates.

24.5 An audible trouble signal shall activate within 90 seconds of any occurrence of the following malfunctions:

a) The automation system does not execute its program cycle.

stages™ will generate an alarm if one of its processes or Tasks is not functioning.

b) A power-supply output upon which the operation of the automation system relies (such as a micro-processor, memory, disk drive, or similar equipment) ceases to operate.

The included backStage™ Manager can alert on system component failure.

c) Rotation ceases, or fails to start when required, in an automation system that incorporates permanent memory-storage devices having rotating elements.

stages components do not rely on rotating memory-storage devices. The included backStage™ Manager can alert on the status of memory-storage devices.

24.6 The alarm-monitoring capabilities of the automation system shall not be affected when it executes or fails to execute any supplementary program.

The Alarm Monitoring capabilities of the application are self contained and not affected by supplementary programs.

24.7 The automation system shall have a non-volatile, reliable storage device (hard disk, optical disk, or similar device).

stages™ is configured on redundant hard disk servers

24.8 The back-up copies of the operating system and the alarm-monitoring software shall be stored on removable media. The alarm system data base shall be saved on removable media daily. The automation system shall have provisions for connection to equipment that is able to reload the operating system, alarm-monitoring software, and the alarm system data base.

Back-ups of the database are maintained on all back-up servers. A back-up can be stored in the SGS Network Operations Center and can be reloaded remotely.

Receiver Compatibility Test

26.1 The receiver shall automatically transmit to the automation system the signals that it receives. This transmission shall be in such a manner that the time lapse from receipt of a signal that is received at the receiver and requires operator action until the signal is displayed and recorded at the automation system does not exceed 10 seconds. Displaying the signal may be in the form of updating the number of signals in queue.

Approved for the following Receivers:

```
Bosch Security Systems Inc., Model D6600

Digital Security Controls (SurGard Security Systems), Model System III

Ademco Model MX8000

ITI, Model CS4000

FBI, Model CP220

Silent Knight by Honeywell, Model SK9000
```

26.2 The receiver to be used with the automation system is to be programmed in such a manner that it detects failure of the automation system within 90 seconds of its first attempt to send a signal (a "heartbeat") to the automation system and then operates in the degraded mode of operation. Upon detection of the computer failure, the receiver is to generate an audible signal and store in memory or print all incoming signals. In addition, it shall print a message indicating the computer failure. There shall be no loss of signal when the system enters the degraded mode of operation.

Tasks are required for Receivers to detect polling messsages and alert on failures. The receivers are required to revert to manual mode upon failures to communicate with the automation system.