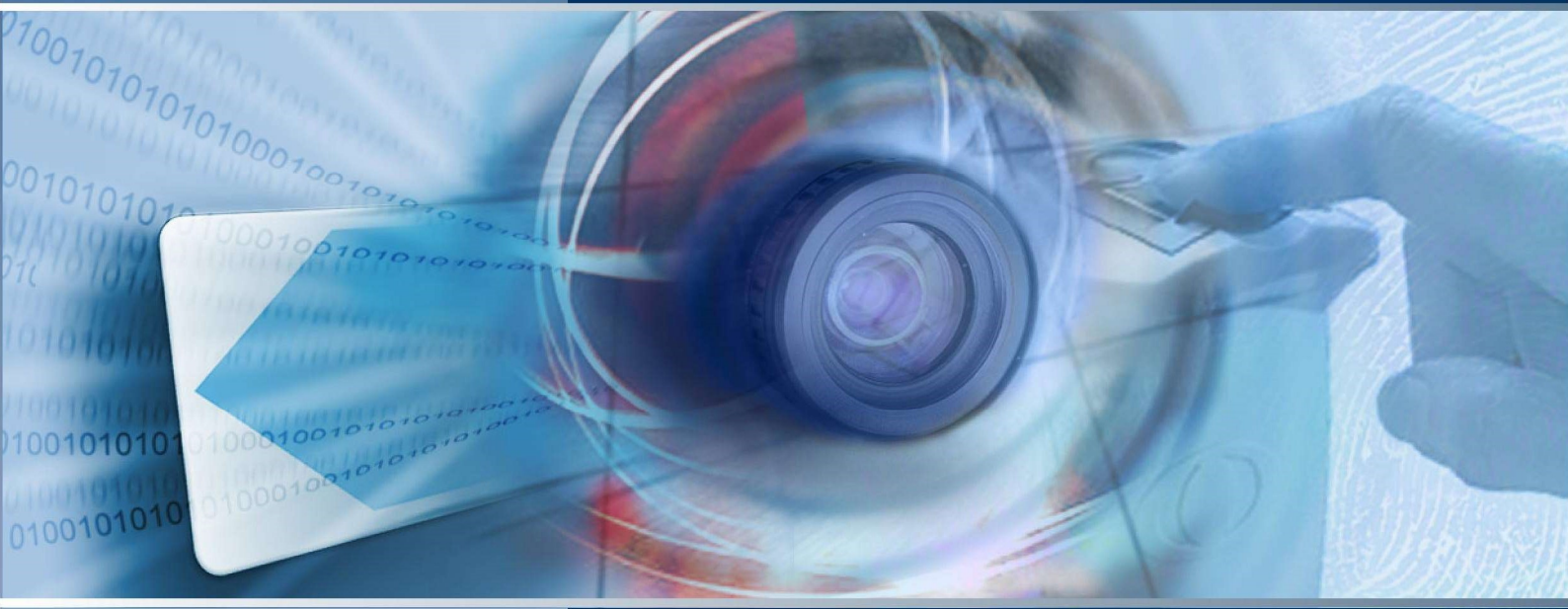


# UL1076 Compliance Guide

**8.0.1.4**

## Symmetry™ Security Management

**9600-0449**

Challenge House, International Drive,
Tewkesbury, Glos, GL20 8UQ, U.K.
Telephone: +44 (0) 1684 850977

**UL1076 Compliance Guide**

**9600-0449**

Issue 8.0.1.4

# *Contents*

**Preface** ..... **ii**
About this Manual ..... ii
Related Documents ..... iii
**Chapter 1: UL Compliance Requirements** ..... **- 1 -**
General Requirements ..... - 1 -
Central Supervisory Stations ..... - 1 -
Environmental ..... - 2 -
Receiving Equipment ..... - 3 -
Data Processing Equipment ..... - 3 -
Transient Suppressors (For Central Station Receiving Equipment). ..... - 3 -
UL Labels ..... - 4 -
Plug-in Transformers ..... - 4 -
Cable Supervision ..... - 4 -
Standard and Encrypted Line Security Equipment ..... - 4 -
Encryption ..... - 5 -
Host Acknowledgement for Arm/Disarm of Protected Areas ..... - 5 -
Misc. Software Default Settings ..... - 6 -
Tamper Switches ..... - 6 -
Passwords ..... - 6 -
Signal Priorities ..... - 6 -
Packet Switched Data Networks ..... - 7 -
Dial-Up Communications ..... - 7 -
Supplementary Systems ..... - 7 -
**Chapter 2: System Configuration** ..... **8**
System Type ..... 8
**Chapter 3: UL2050 (CRZH) Report** ..... **9**

# Preface

## About this Manual

This manual details the required steps to install and configure Symmetry intrusion systems to ensure full compliance with all requirements of the UL1076 *Standard for Proprietary Burglar Alarm Units and Systems*.

The information contained in this manual is intended for use by technical staff having a high level of familiarity with Symmetry system configurations, UL standards and applicable government regulations.

It is important that due consideration be given to all applicable codes, statutes, and regulations when planning for UL1076 compliant installations. While every effort has been taken to include all pertinent information at the time this document was published, the installing dealers sales and technical staff should regularly review all applicable regulations at reasonable intervals to ensure ongoing familiarity with the constantly changing regulatory environment of today's security enterprise.

Occasionally you may find conflicting requirements between various agencies and regulations. When in doubt, it is best to seek guidance from the appropriate Authority Having Jurisdiction (AHJ). When clear guidance is not easily attained for reasons beyond your control, the best course of action is to follow the most stringent requirement. It is highly recommended that the installing technicians and project managers have read and thoroughly understand UL681, UL1076, UL2050 and related codes, statutes and regulations prior to embarking on an installation requiring UL1076 compliance. Failure to do so could expose the installing firm to substantial liability if the installation does not meet the project's regulatory requirements.

When this equipment is being installed for alarm service that is UL Certificated it is necessary to determine the category of service. Once that is done, the installation and operation of the equipment is required to comply with the UL Standards used for that category of service. The following are the categories of service in which this equipment may be used:

Proprietary Alarm Systems (CVWX), Relevant UL Standards; UL1076 Proprietary Burglar Alarm Units and Systems and UL681 Installation and Classification of Burglar and Holdup Alarm Systems, National Industrial Security Systems (CRZH), Relevant UL Standards; UL2050 National Industrial Security Systems and UL681 Installation and Classification of Burglar and Holdup Alarm Systems.

Specific features of the service will be determined by an authority having jurisdiction that has an interest in the material that is being protected and who has conducted a threat assessment.

*As just one example, UL1076 does not specifically limit the amount of time that can be set for maximum arm/disarm time from a protected area reader/keypad. However, UL2050 sets the MAXIMUM time at 30 seconds. Any time this equipment is installed in a Government Contractor Monitoring Station (GCMS) under UL1076, the 30 second time period must be observed, and the system must also be configured so that users cannot exceed the 30 second time setting when programming the parameters for the protected areas.*

When additional non-Symmetry equipment is needed to complete an installation, all such equipment must also be UL listed for the intended category, including cable and wire, detection devices, door contacts and the like. It is the installing dealer's responsibility to confirm compliance to all UL requirements.

Other codes, statutes, and regulations that should be considered before beginning a UL1076 installation could include, but would not necessarily be limited to the following:

| Agency | Code, Statute or Regulation | Title |
|---|---|---|
| Underwriters Laboratories | UL681 | Installation and Classification of Burglar and Holdup Alarm Systems |
| Underwriters Laboratories | UL2050 | National Industrial Security Systems, Government Contractor Monitoring Workstation (GCMS) |
| Defense Security Services (DSS) | NISPOM | National Industrial Security Program, Operations Manual |
| Director of Central Intelligence Directive | DCI/D 6/9, Annex B | Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) |
| Homeland Security | HSPD12 | Homeland Security Presidential Directive 12 |

While not specifically a requirement of UL1076, all CRZH (UL2050) GCMS installations require a "System Configuration Diagram" showing all main system devices within the GCMS that make up the security monitoring system. This drawing should include all equipment (servers, workstation, power supplies, etc) contained within the GCMS. The UL certificate services personnel will ask to see this diagram during the yearly CRZH certificate renewal inspections. Dashed lines around the equipment shown on the System Configuration Diagram should indicate all equipment residing within the physical boundaries of the GCMS.

# Related Documents

The following documents provide additional information:

*8DBC MKII Installation Instructions (9600-0658)* (UL294 and UL1076 LISTED)
*4DBC Installation Instructions (9600-0485)* (UL294 and UL1076 LISTED)
*2DBC Installation Instructions (9600-0486)* (UL294 and UL1076 LISTED)
*DBU MKII Installation Instructions (9600-0657)* (UL294 and UL1076 LISTED)
*8DC MKII Installation Instructions (9600-0659)* (UL294 and UL1076 LISTED)
*4DC Installation Instructions (9600-0467)* (UL294 and UL1076 LISTED)
*2DC Installation Instructions (9600-0466)* (UL294 and UL1076 LISTED)
*M2150 EN-DBU MKII Installation Instructions (9600-0660)* (UL294 and UL1076 LISTED)
*M2150 CAB3A Installation Instructions (9600-0418)* (UL294 and UL1076 LISTED)
*M2150 CAB4A Installation Instructions (9600-0419)* (UL294 and UL1076 LISTED)
*M2150 CAB5 Installation Instructions (9600-0483)* (UL294 and UL1076 LISTED)
*AC24/4 Alarm Controller Installation Instructions (24IN-4OUT) (9600-0492)* (UL294 and UL1076 LISTED)
*OC4/24 Output Controller Installation Instructions (4IN-24OUT) (9600-0465)* (UL294 and UL1076 LISTED)
*Power Supply Board Installation Instructions (MN-PSU-6A) (9600-0423)* (UL294 LISTED)
*Power Supply Board Installation Instructions (MN-PSU-KIT MKII) (9600-0610)* (UL294 LISTED)
*NIC4 Installation Instructions (9600-0424)* (UL294 LISTED)
*OC4/8 IO Module Installation Instructions (9600-0468)* (UL294 and UL1076 LISTED)
*AC8/4 IO (MN-I/O) Module Installation Instructions (9600-0326)* (UL294 and UL1076 LISTED)

*SMS Software Installation Manual (9600-0427)* (UL294 and UL1076 LISTED)
*NIC Module Configuration Guide (9600-0402*) (NIC3 and NIC4 sections UL294 and UL1076 LISTED)
*Cluster Installation Manual (9600-0406)* (UL1076 LISTED)
*Threat Level Manager Installation and User Guide (9600-0408)*
*M2150 Intrusion Guide (9500-0540)* (UL1076 LISTED)

This manual should be read in conjunction with the product help, which is also available in printed form as the *SMS Software Reference Manual*.

# Chapter 1: UL Compliance Requirements

## General Requirements

- The system and all components must be installed in accordance with NFPA 70, National Electrical code or as amended by individual states where the work is to be performed.
- All interconnecting devices must be UL listed for the intended use and for the appropriate UL category.
- Power-limited circuits are to be used exclusively for all field device connections unless otherwise indicated.
- Central-Station equipment shall be designed and constructed so that any critical component can be replaced and the system restored to service within 30 minutes. A critical component is one in which a malfunction will prevent he receipt and interpretation of signals by the central-station operator.

## Central Supervisory Stations

**Receiving Equipment:** Central Supervisory Stations are comprised of all necessary equipment required to allow system users to monitor alarm activity within the entire system or partitioned areas as indicated by the users, including servers, workstations, power supplies, and the like. ***All receiving equipment shall be completely duplicated with provision for switchover to the back-up system within 30 seconds. The backup system shall be fully operational within 6 minutes of the loss of the primary system. This allows for 30 seconds for the backup system to be fully energized and connected to the necessary communications lines and other devices, followed by 5 ½ minutes for the system to boot up, conduct memory tests, file system checks, security verifications and prepare for full system operation. The backup computer shall have the capabilities of the primary, such as memory, speed and the like (UL1076 25A.2h)***

Failure of the main computer system, hard disk, and alarm monitor shall result in switch over to the backup system and shall be indicated by an audible or obvious visual indication.

A fault-tolerant system may be used in lieu of complete duplication of the system if every component in the fault-tolerant system, including the software and power supply, is duplicated.

The number of signals (connected premise control units) shall be limited to 1000.

Refer to the *Cluster Installation Manual* (9600-0406) for further instructions regarding automatic system switching from Primary to Secondary servers in the event of a primary server failure, and steps that should be undertaken in the extremely unlikely event that the secondary server does not come on line within the prescribed timeframe.

It is recommended that the dealer and customer both be familiar with UL1076 Sections 89-97.4. Requirements for the central supervising station are outlined there, including items such as area physical protection, lighting, clocks, etc.

**Backup Power and UPS units:** In addition to the main power supply and secondary power supply that are required to be provided at the Central Supervisory Station, the system shall be provided with an uninterruptible power supply (UPS) with sufficient capacity to operate the computer equipment for a minimum of 15 minutes. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the UPS shall be capable of providing input power for at least that amount of time (UL1076 25A.2.k).

UPS equipment used for Central Supervisory Station equipment must conform to the following UL Standards for equipment safety (UL1076 25A.2l):

- UL1778 Standard for Uninterruptible Power Supply Equipment
- UL1481 Standard for Fire Protective Signaling Equipment

In order to perform maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the Central Supervisory Station shall be provided (UL1076 25A.2m).

# Protected Areas

- 24 hour battery backup for the protected areas is required with one exception (UL1076 40.3.3). *"Less than 24 hours standby capacity may be provided if a signal indicating that the protected area is operating on standby power is transmitted to the central supervising station before the capacity of the standby power has decreased below 4 hours*". A minimum of 4 hours run time on batteries is required at all protected area equipment locations.
- When a "Battery Trouble" indication is seen at the Central Supervisory Station, the signal should be considered as the 4 hour warning as indicated above, even though substantially longer run time might be available from the batteries. Battery capacity is affected by many factors including time in use, temperature, charging, and the like. Always follow manufacturers recommended maintenance at regular intervals. It is highly recommended that batteries be load and cycle tested regularly and replaced every 5-7 years. Batteries used must conform to UL1989 Batteries, Standby.
- Maximum reader distance when using 22 AWG cable is 450' for 20mA and 225' for the Wiegand Reader connections. The reason for this limitation is that the reader must continue to operate normally under loss of AC power, and with the battery operating at a maximum voltage of 10.2 VDC.
- Maximum input voltage from the power supply to a fully loaded M2000, M2100 or M2150 board is 13.8 VDC.

# Environmental

The Central Supervisory Station equipment must be installed in a temperature-controlled environment. A temperature-controlled environment is one that can be maintained between 55-95 degrees F (13-35 degrees C) by the HVAC system. 24 hours of standby power shall be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used (UL1076 25A.2g).

# Receiving Equipment

The minimum requirement for the Receiving Equipment must conform to the following UL Standards for equipment safety (UL1076 25A.2b)

**Primary and Back up Server each employ:**
Intel Xeon CPU E2, 1220 v3 @ 3.10 GHz,
Memory 4 GB RAM min.
Hard Drive 40 GB, DVD Drive
Windows Server 2012 R2 Standard SP1, 64-bit OS
NEC Express Cluster X 3.1 for Windows
Microsoft SQL 2014 Express DB software.

**Monitoring Station - Primary and Back Up Workstations:**
Pentium 4 CPU 3.2 GHz,
Hard drive 230 GB min.
Memory 2.0 GB RAM min.
Windows 7 Professional SP1 32-bit OS
DVD Drive
Internet Explorer 11
Monitor
Keyboard
Mouse

# Data Processing Equipment

Data processing equipment, office appliance equipment, and business equipment used for Central Supervisory Station equipment must conform to one of the following UL Standards for equipment safety (UL1076 25A.2a):

- UL114: Standard for Office Appliances and Business Equipment
- UL478: Standard for Information Processing and Business Equipment
- UL60950: Standard for Information Technology

# Transient Suppressors (For Central Station Receiving Equipment).

Transient protection must meet or exceed the following UL Standards for equipment safety:

- Communications circuits & network components; UL497A: Standard for Secondary Protectors for Communications Circuits (UL1076 25A.2f). (Example: APC model PNET1 power line surge suppressor)
- Signal Line Transients; UL497B: Standard for Protectors for Data Communications and Fire Alarm Circuits, maximum rating of 50 volts (UL1076 25A.2e).
- Supply Line Transients; UL1449 Standard for Transient Voltage Surge Suppressors (UL1076 25A.2d).

# UL Labels

All UL listing labels are to remain visible after the equipment in fully installed and operational. Do not remove or relocate the factory applied listing labels. When in doubt, contact your Symmetry support representative for labeling requirements (UL1076 83.7 which requires marking permanency).

# Plug-in Transformers

Plug in transformers must not be connected to receptacles that are switched, including multiple outlet power strips. (UL1076 83.1k)

# Cable Supervision

UL1076 does not allow every possible variation of the Symmetry SMS software cable supervision states. See the following table for guidance when connecting initiating devices to a UL1076 listed system. In all cases, the end of line (EOL) resistors should be connected as near as possible to the alarm initiating device. In no event shall EOL resistors be installed at the panel location. (Refer to the M2150 Design Guide, P/N 9600-0420 for the End Of Line Resistor Values/Configurations and Tolerances to be used).

| State Type | UL1076 Compliant | Reason |
|---|---|---|
| 2 State | Conditional | Never allowed for protected area alarm zone initiating devices. *"The protection circuit must respond both to an increase and decrease in the circuit resistance within the limits indicated in the appropriate sections of this standard" (UL1076 1.4).*<br>Allowed *only* for panel connected tamper switches, power supply trouble relays (AC fail and Battery trouble) and the like; provided the wiring from the protection devices to the input terminals is contained solely within the enclosures and connecting conduit.<br>All common functions (i.e. tamper switches for multiple enclosures, etc) may be wired as a common closed loop connected to a single input for all similar notifications at the common panel location. |
| 3 State | Yes | Allowed in all cases without restriction.<br>(Note: 4.7K and 10K resistor configurations only evaluated for UL) |
| 4 State | Conditional | Never allowed for protection zones containing more than one initiating device.<br>Allowed *only* when the initiating zone is comprised of a single initiating device (i.e. door contact, PIR, etc).<br>(Note: 4.7K and 10K resistor configurations only evaluated for UL) |
| 6 State | Conditional | Never allowed for protection zones containing more than one initiating device.<br>Allowed *only* when the initiating zone is comprised of a single initiating device (i.e. door contact, PIR, etc).<br>(Note: 4.7K and 10K resistor configurations only evaluated for UL) |

# Standard and Encrypted Line Security Equipment

In the event a "LAN COMM LOSS" trouble signal is received at the central supervisory station, this trouble signal must be treated as a **compromise attempt** on the system and the appropriate actions must be taken to safeguard the local protected premises panel/central supervisory station.

Each message sent between the premise control unit and the Central Supervisory Station shall be protected with a cryptographic authentication means.

Encrypted Line Security is available by utilizing the NIC4-ENC module on an appropriate DBU/DBC board for network communications.

Standard Line Security is available when using the MN-NIC-4 only. Standard line security is specifically disallowed under UL1076 for communications between premise control unit and the Central Supervisory Station.

# Encryption

UL1076 requires Encrypted Line Security between premise control units and the Central Supervisory Station. For all UL1076 listed installations, only MN-NIC-4-ENC communications devices with encryption enabled are allowed for communications from the premise control unit to the Central Supervisory Station. The MN-NIC-4-ENC employs FIPS 197 256 bit AES Encryption under FIPS 197 CAVP certificate # 1314. For independent confirmation, please see: http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

The following communication methods do not include encryption functionality and therefore cannot be used for communications between the premise control unit and the Central Supervisory Station:

RS232

20 mA (Host Comms A or B)

RS485 (DC Comms)

20 MA Host Comms and RS485 (DC Comms) may only be employed within the secure perimeter room and only when the communications lines remain inside enclosures with tamper switches employed.

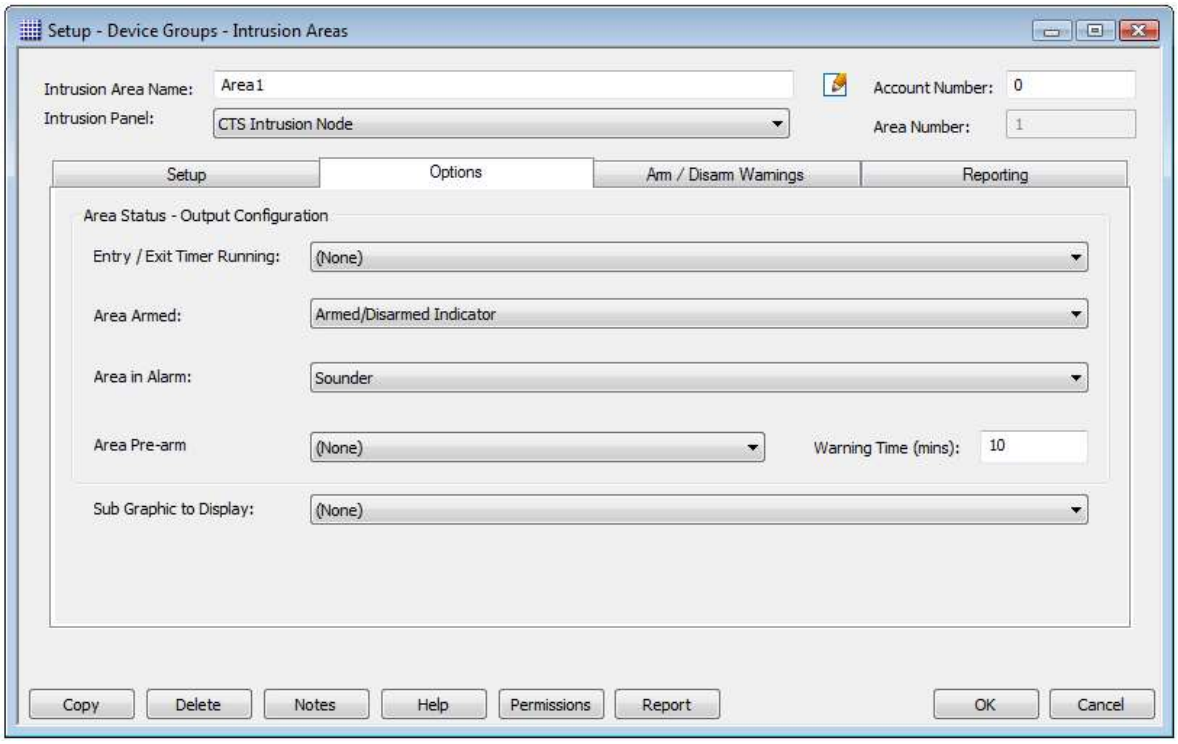
# Host Acknowledgement for Arm/Disarm of Protected Areas

UL1076 section 3.1.1. States "An audible and/or visual signal that is sent to the subscriber by the central supervisory station to notify the subscriber that the protection system has been properly armed".

When arming an area, the user will know that the Receiver (Host) is not available to accept the ARMING request if the user sees the following message: "Not Monitored" or "Present Card". In this condition, alarms will not be monitored from the Receiver (Host) location. If the host acknowledgement signal is received by the premise control unit, the reader display will show "ARMED".

For additional information refer to the M2150 Intrusion Guide, Chapters 4 and 5: Arming/Disarming using S843B-KP, S844-KP and S884-V2 Readers with Keypad and LCD display.

**Note:** Readers used for arming and disarming must either be the S843B-KP or S844-KP or S884-V2 Keypad readers with LCD display.




## Misc. Software Default Settings

The following software changes must be made to the default settings in order to be UL1076 compliant:

- All trouble alarms must have the receiving equipment audible tone enabled.
- All tamper switches must be on 24-hour zones.

## Tamper Switches

Cabinet tamper and reader tamper switches must remain connected at all times.

## Passwords

UL1076 dictates that the user sign-on to this system requires a password with a minimum of four characters. Other codes and regulations may require longer minimum passwords. Contact your Symmetry support representative if the need arises to set the minimum password length to greater than four characters.

## Signal Priorities

A multiplex system that gives priority to signals in the given order below shall annunciate subsequent signals at a rate not less than one every 10 seconds (UL1076 61.13). The order of priority of signals shall be:

1. Burglar alarm (Intrusion Detection Systems – IDS)

2. Watchman tour
3. Burglar alarm supervision
4. Other Supervisory Services, Access control events e.t.c.

## Packet Switched Data Networks

Networks should be constructed with minimum latency. Any loss of connection/signal shall be reported and identified within 200 seconds at the central station receiving unit (UL1076 61A.2).

Network addressing of devices shall not use Public Domain Name Servers. (UL1076 61A.7)

The Security Management System must be protected from the corporate network by a firewall.

IP devices are to be programmed with static IP addresses. DHCP should never be used for IP address provisioning. At a minimum, the following static addressing should be provided:

- IP Address
- Subnet Mask
- Default Gateway
- Preferred and alternate DNS servers

While not mandatory, it is recommended that the "Node Timeout" message should be changed to "Comms Loss" or "Network Loss" to better describe the event to personnel.

## Dial-Up Communications

While the SMS software supports dial-up communications for panel to host communications, UL1076 specifically prohibits this configuration as a primary means of communications. Dial-up communications is allowed only as a back-up means of communications. UL has not investigated dial-up communications for compliance under UL1076.

## Supplementary Systems

Supplementary systems are those for which the software features are not covered within the UL1076 standard, and as such have not been investigated by UL. UL checks to be certain that UL listed devices are utilized and that the supplementary systems do not interfere with normal system operation or circumvent receipt of alarms within the system. Supplementary systems include:

- Badging systems & printers
- DVM video features
- Web Client features
- Card Data Import/Export
- MAPI E-Mail Alarms

# Chapter 2: System Configuration

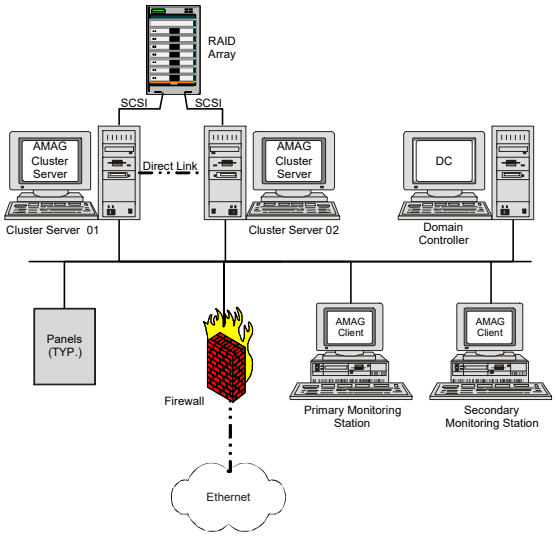
## System Type

The V8.0.1 Symmetry software is designed for use with M2150 controllers, and comes in a variety of prepackaged versions. UL Installations must utilize the redundant server configuration (per UL1076 section 25A.2h) as shown in the following diagram.

**Note:** All computers and their components **must** be listed in the relevant Windows Hardware Compatibility List (HCL).

**Cluster (Redundant) Servers** - A true client/server system suitable for use on a separate security network or customer provided network. This configuration handles UL listed systems as well as larger systems, including global deployment; with the assurance that there is always a standby server ready to be automatically switched into service should the primary server fail for any reason. Reference *9600-0406 Cluster Installation Manual* for additional information on setting up a redundant server configuration.

Typical redundant server configuration:




For cluster servers, use on board NIC card for private sub-net direct link IP communications. Use 2nd IPSec qualified NIC card for public network. NIC cards must be on separate sub-nets.

Typical for all Client Workstations
Windows XP, Vista, 7
SMS v7.0

For details of cluser server minimum computer requirements, please refer to the *9600-0406 Cluster Installation Manual*.

# Chapter 3: UL2050 (CRZH) Report

While UL1076 does not require report preparation and generation, UL2050 does. The requirement is that the user must produce a “UL Report” with 1 hour or the request being made by the UL Certificate Services inspector or other authority having jurisdiction (AHJ). UL Reports only apply to “certificated accounts”, those areas or accounts that carry CRZH UL2050 certificates. UL will be looking for any unscheduled openings and flaws in the report process.

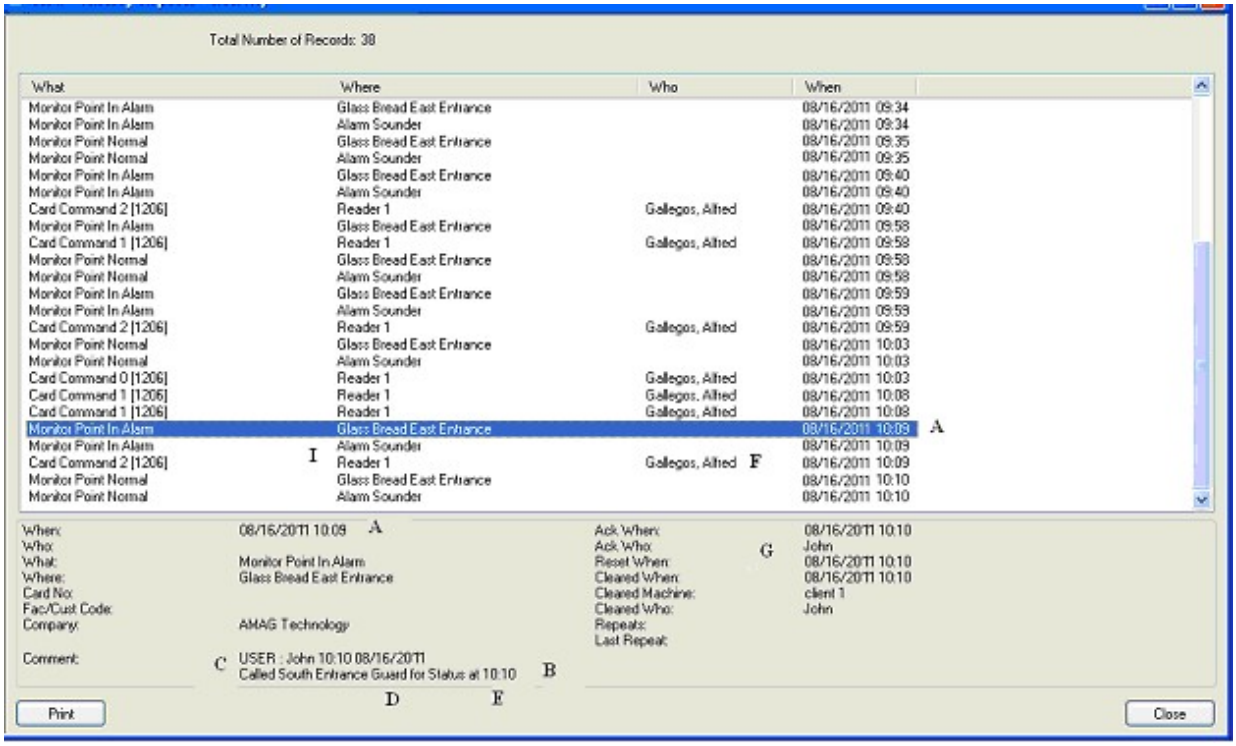
The following information is generally required within the UL Report:

- Time the alarm is received.
- Time that the guard or police were notified of the incident.
- Badge number, employee number, title, etc, that identifies the operator logging the event into the system database.
- Who was dispatched to the area (Guard, Police, other).
- Time when the subscriber was notified.
- Time the respondent arrived at the alarm location.
- ETA from respondent notification time to respondent arrival time.
- Disposition of the alarm.
- Whether or not a sounding device was activated.

To produce a UL Report, follow these steps:

1. Open the "Reports/History/Activity" screen and specify the required dates.
2. Deselect **All Activity**.
3. Under **System Activity**, select **Card Commands** and **User Comments**.
4. Using the **Include** menus, select the arming/disarming reader and the monitor point that activated the sounder.
5. Click **Run**.

The following shows an example of the report.




1. **A** = Time the alarm is received
2. **B** = Time that the guard or police were notified of the incident
3. **C** = Badge number, employee number, title, etc, that identifies the operator logging the event into the system database
4. **D** = Who was dispatched to the area (Guard, Police, other)
5. **E** = Time when the subscriber was notified
6. **F** = Time the respondent arrived at the alarm location
7. **G** = Disposition of the alarm
8. **A, C, F** = ETA from respondent notification time to respondent arrival time
9. **I** = Whether or not a sounding device was activated