UNDERWRITERS LABORATORIES INC. CERTIFICATION REQUIREMENT DECISION

This Certification Requirement Decision is prepared and published by Underwriters Laboratories Inc. (UL). It is normative for the applicable UL Product Certification Program(s); however, it is currently not part of the UL Standard(s) referenced below.

Product Category (CCN): CRZH & CRZM
Standard Number: UL 2050
Standard Title: National Industrial Security Systems
Edition Date: November 5, 2010
Edition Number: 5
Section / Paragraph Reference: 5.11, 6.3.5, 6.3.6, 6.3.7 – 16, and 6.3.17
Subject: Automation Systems

DECISION:

The additional paragraphs 5.11, 6.3.5, 6.3.6, 6.3.7 – 16, and 6.3.17 provide redundancy for the Government Contracting Monitoring Stations (GCMS) and National Industrial Monitoring Stations (NIMS) when using an automation system.

5.11 AUTOMATION SYSTEM – A computer system that consists of hardware and software components. These components include the alarm-monitoring software supplied by the automation system developer, the operating system, and programming languages, required to make the system operational. An automation system may be configured as a computer system that is directly connected to hardware based central-station receivers, internal software based receivers, or is connected to remote receivers located in central-stations other than the one where the automation system is located. It is used to automatically process change-of-status signals such as alarm, trouble, supervisory, disarming and arming (i. e. opening and closing), and similar signals that it receives from the central station receiving equipment. See the Standard for Central-Station Automation Systems, UL 1981.

6.3.5 A computer system is formed when the equipment includes power supplies, disk drives, processors, data storage devices, and similar components are interconnected to enable the alarm monitoring software to process signals.

6.3.6 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.

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

a) The central station shall maintain a dated diagram or printed description of the current configuration of the alarm monitoring automation system. The diagram or printed description shall be created when the automation system is installed and updated whenever there is a change to the system. The configuration shall be reviewed every 12 consecutive months and the records updated. The following should be included in the diagram or description as a minimum:
    1) All computers that form the automation system;
    2) All components that form a network for the automation system;
    3) All surge protective devices;
    4) All work stations by location;
    5) All network security measures, such as fire walls and the like;
    6) All network communication protocols;
    7) All communications channels that enter into the operating room; and

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

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

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

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

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

6.3.9 An automation system shall be provided with the necessary spare parts, and personnel shall be trained to the necessary expertise to ensure that the system can be placed back in service within 24 hours of failure.

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

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

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

6.3.13 A copy of the operating system shall be kept on-site and at an off-site location. The off-site location is not prohibited from being the software developer’s location, if a copy of the operating system can be delivered to the central station within 24 hours.

6.3.14 Access shall be provided to all back-up data records required and are maintained at an off-site location, this shall be provided at all times.

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

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

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

1) Measure 1 – Physical security of facilities

i) Areas outside of the operating room, in a remote monitoring center, or in a redundant site housing equipment shall comply with physical security requirements.

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

The alarm system shall be monitored in the central station.

2) Measure 2 – Local Area Network (LAN) security measures, as outlined below, shall be applied.. These systems shall be maintained with the latest updates supplied by the manufacturer. .

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

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

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

a2) Evidence of compliance with the latest encryption National Institute of Standards & Technology (NIST) standard shall be provided.

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

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

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

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

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

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

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

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

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

RATIONALE FOR DECISION:

The intent of the additional paragraphs added to section 6 of UL 2050 is to have the monitoring stations equipped with redundancy. This will assure, if at any time the computer system were to fail there is a backup system that will automatically be in place to continue processing signals.

UL has found that the current edition of UL 2050 is silent on the redundancy and maintain operation if a single point were to fail. UL is introducing this concept to reduce and/or eliminate any point the computer system/automation system will be without signal processing.