

NEMA Standard SB 40-2008

Communications Systems for Life Safety in Schools

Published by

National Electrical Manufacturers Association
1300 North 17th Street
Rosslyn, Virginia 22209

www.nema.org

© Copyright 2008 by the National Electrical Manufacturers Association. All rights including translation into other languages, reserved under the Universal Copyright Convention, the Berne Convention for the Protection of Literary and Artistic Works, and the International and Pan American Copyright Conventions.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

The National Electrical Manufacturers Association (NEMA) standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEMA has no power, nor does it undertake to police or enforce compliance with the contents of this document. NEMA does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety-related information in this document shall not be attributable to NEMA and is solely the responsibility of the certifier or maker of the statement.

CONTENTS

	Page
Foreword.....	ii
Section 1 ADMINISTRATION	1
1.1 Scope.....	1
1.2 Purpose	1
1.3 Application	1
Section 2 REFERENCED PUBLICATIONS	2
2.1 General	2
2.1.1 Normative References	2
2.2 Industry Publications	2
2.3 Other Publications	2
Section 3 DEFINITIONS	4
3.1 General	4
3.2 Standard Definitions:	4
Section 4 RISK ASSESSMENT TO DETERMINE EMERGENCY COMMUNICATIONS NEEDS	7
4.1 Planning and Design	7
4.2 Process.....	7
4.3 Risk Assessment Considerations.....	8
4.3.1 Communications Systems for Life Safety in Schools: Design Considerations	8
Section 5 FUNDAMENTALS OF SCHOOL COMMUNICATION SYSTEMS	17
5.1 Application	17
5.2 Purpose	17
5.3 Equipment and Personnel	17
5.4 System Fundamentals.....	17
5.4.1 Power Supplies	17
5.4.2 Audio Amplifiers	18
5.5 System Functions	18
5.5.1 General.....	18
5.5.2 Initiation of Emergency Calls.....	20
5.5.3 Annunciation of Emergency Calls	20
5.5.4 Lockdown	22
5.5.5 Lockout.....	22
5.5.6 Evacuation.....	22
5.5.7 Reverse Evacuation	23
Section 6 INSPECTION, TESTING, AND MAINTENANCE	24
6.1 General.....	24
6.2 Required Documentation	24
6.2.1 As-Built Drawings (Record Documentation)	24
6.2.2 Owner's Manual	24
6.2.3 Software	24
6.3 Document Accessibility.....	25
6.4 Preventive Maintenance and Servicing	25
6.5 Testing.....	25
Table	
6-1 Testing Methods and Frequencies	26

Foreword

In the preparation of this Standards Publication input of users and other interested parties has been sought and evaluated. Inquiries, comments, and proposed or recommended revisions should be submitted to the concerned NEMA product Subdivision by contacting the:

Vice President, Engineering
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209

Section 1 ADMINISTRATION

1.1 SCOPE

1.1.1 This Standard covers the application, installation, location, performance, and maintenance of school communications systems and their components.

1.2 PURPOSE

1.2.1 The purpose of this standard is to define the means of signal initiation, transmission, notification, and annunciation; level of performance; and the reliability of various types of school communication systems.

1.2.2 The standard also defines the features associated with these systems.

1.2.3 This standard establishes minimum required levels of performance, extent of redundancy, and quality of installation, but does not limit the methods by which these requirements are to be achieved.

1.3 APPLICATION

1.3.1 The standard is intended for all educational facilities.

1.3.2 The standard would apply to single building schools, multi-building campuses, and multi-school districts.

Section 2 REFERENCED PUBLICATIONS

2.1 GENERAL

2.1.1 Normative References

The following normative documents contain provisions, which through reference in this text, constitute provisions of this Standards Publication. By reference herein these publications are adopted, in whole or in part as indicated, in this SP.

National Fire Protection Association (NFPA)
1 Batterymarch Park
Quincy, MA 02169-7471

NFPA 70 *National Electrical Code, 2008 Edition*
NFPA 72 *National Fire Alarm Code, 2007 Edition*
 Glossary of Terms, Spring 2006 Edition

2.2 INDUSTRY PUBLICATIONS

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 1752
Rosslyn, VA 22209

NEMA School Communication Product Guide
SB50-2008 *Emergency Communications Audio Intelligibility Applications Guide*

2.3 OTHER PUBLICATIONS

National Emergency Number Association (NENA)
4350 North Fairfax Drive, Suite 750
Arlington, VA 22203-1695

9-1-1 Report Card to the Nation

U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202

Practical Information on Crisis Planning—January 2007

National Clearing House for Educational Facilities (NCEF)
1090 Vermont Ave., NW Suite 700
Washington, DC 20005

Safe Schools Facility Checklist

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

NCJ 178265
National Institute of Justice

*The Appropriate and Effective Use of Security Technologies in
U.S. Schools—A Guide for Schools and Law Enforcement Agencies,
Mary W. Green Sandia National Laboratories, September 1999*

Section 3 DEFINITIONS

3.1 GENERAL

The definitions contained in this section shall apply to the terms used in this standard. Where terms are not included, common usage of the terms shall apply.

3.2 STANDARD DEFINITIONS:

911 operating authority: The public entity, which operates a 911 telephone system for the public benefit, within a defined 911 service area.

alarm: A signal or message from a person or device indicating the existence of an emergency or other situation that requires immediate attention.

approved: Acceptable to the authority having jurisdiction.

armed intrusion event: Administration is notified there is an unauthorized or unknown person or persons known or considered to be in possession of firearms located either within proximity to or inside the premises.

authority having jurisdiction (AHJ): The organization, office, or individual responsible for approving equipment, materials, installation, or a procedure.

automated notification: The communication system or an external system creates action due to a specific event. Situations requiring this type of notification include, but are not limited to:

- a) 911 phone call from a staff or classroom phone
- b) Entrance/egress access
- c) Fire alarm—secondary notification
- d) Security alarm—secondary notification
- e) Camera system

bomb threat: A threat is received by phone, e-mail, text, letter, or other means indicating there may be an explosive device on the premises.

code: A standard that is an extensive compilation of provisions covering broad subject matter or that is suitable for adoption into law independently of other codes and standards.

community shelter: Where the school facilities are used to shelter residents and/or students and/or staff due to an emergency in the community.

distinctive emergency annunciation: An audible indication of an emergency notification on a device such that users can readily recognize the event as a priority event, and that the indication is unique from routine indications that are utilized by that device.

E911: Enhanced 911 (E911) means the general term referring to emergency telephone systems with specific electronically controlled features, such as ALI, ANI, and selective routing.

evacuation: The withdrawal of occupants from a building or away from an area

extreme weather event: A weather emergency due to an impending severe storm, which could involve extremely high wind, heavy rains, and possible flooding.

fire drill: The action of practicing a building evacuation or relocation as it would be done during an actual fire.

fire emergency: The existence of, or threat of fire, or the development of smoke or fumes or any combination thereof, that demands immediate action to correct or alleviate the condition or situation.

hostage situation: A situation where one or more persons are being held against their will by one or more individuals, through the use force or coercion.

intelligibility: A measure of the proportion of the content of a speech message that can be correctly understood.

internal annunciation: This involves announcing an alarm or call to on-site administrators of the communications system.

labeled: Equipment or materials to which have been attached a distinctive label, symbol, or other identifying mark of an organization, which indicates that the identified equipment or materials are considered acceptable to the authority having jurisdiction concerned with product evaluation. This authority is responsible for the periodic inspection of labeled equipment or materials, and through whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

listed: Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction that is concerned with evaluation of products or services, that also conducts periodic inspections of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

lockdown: A procedure used when there is an immediate and imminent threat to the school building population. School staff and students are secured in the rooms they are currently in and no one is allowed to leave until the situation has been curtailed. This allows the school to secure the students and staff in place and remove any innocent bystanders from immediate danger. Most commonly implemented when building has an intruder.

lockout: Allows no unauthorized personnel into the building. All exterior doors are locked and main entrance is monitored by administrators, security, or school resource officer. This procedure allows the school to continue with the normal school day, but curtails outside activity. Most commonly used when incident is occurring outside school building, on or off school property.

manual notification: Where a teacher, staff member, or student manually initiates an emergency signal via a push button, pull station, or by dialing a code on a telephone. Situations requiring this type of notification include, but are not limited to:

- a) Intruder
- b) Medical emergency of a student or other staff member
- c) Altercation between students and/or staff members
- d) Discipline involving one or more students and staff members that lead to a disturbance requiring assistance to resolve
- e) Any situation in a classroom that requires immediate attention from school administration and/or security

medical emergency: An event where a person or persons on premises have a health-related issue requiring immediate care and summoning of emergency health care providers.

notification: Audible and/or visual display of a call or emergency situation.

remote annunciation: This involves announcing an alarm or call to off-site authorities or administrators responsible for school safety and operation.

reverse evacuation: This situation involves emergency movement of persons from outside a facility or from general locations inside a facility to a designated protected or sheltered location within the complex.

shall: Indicates a mandatory requirement.

shelter in place: Students, faculty, and others within the building remain where they are until given further instructions. Differs from a lockdown in that room doors are not secured and movement within the building is not restricted.

should: Indicates a recommendation or that which is advised but not required.

terrorist event: A premeditated act of violence directed against school occupants for political or personal purposes used to cause fear, exert control, or harm individuals.

Section 4

RISK ASSESSMENT TO DETERMINE EMERGENCY COMMUNICATIONS NEEDS

4.1 PLANNING AND DESIGN.

The planning and design of school communications systems that could be used for emergency purposes should employ a risk assessment methodology to determine the appropriate equipment, level of reliability, operational procedures, and personnel required to fulfill the stakeholder objectives.

4.1.1 A risk assessment is a technique for assessing the current status of a school's threat exposure, preparedness, design, and application of communications systems, and can be used in planning, developing, and strengthening its communications systems objectives.

4.1.2 It is important to establish overall objectives/goals/criteria that can be used in creating the design specifications and the operational procedures. As a result of the risk assessment, the design professional should be responsible for preparing the design specification that will outline the emergency use objectives of the school communications systems and dictate the specific requirements for the school communications systems.

4.1.3 It is crucial that the development of the assessment be in sync with and supportive of the building's emergency response plan (sometimes referred to as the "crisis plan").

4.2 PROCESS

A risk assessment usually involves a systematic multi-step process.

4.2.1 The process should begin with the formation of a team, including a design professional experienced in the application and operations of communications systems used for emergency purposes and of personnel from all pertinent organizational areas. Commonly, either the design professional or the individual responsible for an organization's security serves as team leader.

4.2.2 Once a team leader is identified, the next step involves a characterization of the people and of the buildings, areas, spaces, campuses, or regions to be protected, as well as required equipment and operational procedures, and should consider the type of school environment and the perceived threat to occupants. It includes identification of the people, property, physical features, and operations as well as laws, regulations, and school policies. Likewise, consideration should also be given to the social and political environment, internal activities, after-hour activities, and a review of current site security and safety measures.

4.2.3 The next step is conducting an assessment of potential threats. The process includes identification of potential targets and vulnerabilities. Identification of potential adversarial situations and historical events should be discussed and the lessons learned from those events taken into consideration in the planning process.

4.2.3.1 The risk assessment should consider hazards from natural disaster, accidental hazard, and malicious and terrorist activities. The design of school communications systems should be specific to the nature and anticipated needs of each facility for which it is designed.

4.2.3.2 Identify specific countermeasures such as lockdown, lockout, evacuation, reverse evacuation, community shelter, and shelter-in-place strategies and responses to be applied for each of the potential threats and hazards. Countermeasures should result in mitigating the potential undesired incident from

occurring as well as minimizing the effects stemming from the incident should it occur. The inclusion of trained employees as part of the communications systems should be identified and documented. The design should consider the characteristics or other conditions related to the availability, speed of response, effectiveness, roles, and other characteristics of emergency response personnel.

4.2.3.3 When planning specific countermeasures, also take into account those entities with which you will need to communicate that are outside of the facility such as local police, fire department, parents, etc. For example, if there is an intruder in the building, the building goes into lockdown. Consider how and by what method you will communicate with the local police, parents, and community. This communication is intended to be done in conjunction with the countermeasures taken to immediately address the situation at hand.

4.2.4 Documentation of the risk assessment and resulting actions and subsequent modifications should be recorded and maintained for the life of the facility.

4.3 RISK ASSESSMENT CONSIDERATIONS

4.3.1 Communications Systems for Life Safety in Schools: Design Considerations

The purpose of this section is to guide and create discussion among design professionals and their clients regarding issues that may be relevant to the design of this system, but are not necessarily within the scope of any of the existing standards. These issues may be considered at the discretion of the designers with respect to conducting a risk assessment or evaluation to determine communication needs during emergency situations. Topics reviewed may also be discussed in Referenced Publications (see Section 2). Risk assessment considerations and solutions must be individualized to each facility's needs.

4.3.1.1 Application of 911 Operation

4.3.1.1.1 Interfaces between the emergency communications systems and telephone systems may impact 911 operations in the classrooms. Fundamentally, any operation of a communications system with respect to 911 operation must meet the criteria established by local code, laws, and the 911 operating authority. Also, many states have policies in place for call source area identification for schools of certain sizes. In addition to these regulations, there are other factors to consider as discussed below:

4.3.1.1.1.1 Dialing 9-1-1 is a well understood method of getting help; however, dialing 9-9-1-1 (for an outside line) or 9-1-1#, or any other combination that requires training or a label increases the risk of failure in the event of an emergency. Any phone, classroom or otherwise, will naturally be assumed to be 911-capable in the event of an emergency. Any segregation of this functionality between different classes of phones (e.g., classroom vs. administrative) increases the risk of a failure to obtain help in the timeliest manner possible.

4.3.1.1.1.2 Some systems have historically required dialing 9-9-1-1, or *-9-1-1, or 9-1-1-#. In some instances, phones have been labeled with instructions identifying this. Even if the emergency communication system can process a 911 directly, consider the benefit of the system also being capable of processing the above mentioned 9-1-1 derivations.

4.3.1.1.1.3 Outside telephone lines may be a limited resource. When all outside telephone lines are busy, there is a risk that 911 calls may not be processed unless communication equipment specifically manages resources to ensure that these calls have highest priority. In a general emergency, however, there is the risk of all circuits being occupied by 911 calls, making it difficult for faculty staff to manage telephone communications that may be necessary as part of an emergency plan. Consider the importance of allowing a certain number of 911 to be processed on a priority basis, while still reserving enough outside line capability for staff to effectively manage the emergency response.

4.3.1.2 Intelligibility

The effectiveness of any communication system is always subject to good sound reinforcement design principles. Attention to proper audio design reduces the risk of poor intelligibility during an emergency. Intelligibility can be affected by many factors including the level of background noise in a room, the level (or sound pressure) of an announcement, the size and shape and acoustic properties of a room, and the location, position, and number of speakers. Proper audio design of a facility requires both technical and practical knowledge of sound and acoustical characteristics. Actual methods to accomplish acoustical goals of intelligibility are beyond the scope of this document. However, NEMA SB 50-2008 *Emergency Communications Audio Intelligibility Applications Guide* is an excellent resource, and NFPA 72 *National Fire Alarm Code* provides minimum requirements for audio level and intelligibility. Following are some design factors for consideration:

4.3.1.2.1 Audio Level (sound pressure) of emergency notification should be significantly greater than the ambient noise in a room. This means that the required sound pressure could be different in different rooms or areas. Ambient noise is impacted by the size of the room, the number of people that could be present, and equipment in the room that could be operational (copiers, air handling units, appliances, etc.). The sound pressure of an emergency notification message should be measured in the room as far away from the speaker(s) as possible with typical noise levels encountered in that room. This means for a machine shop, while the machines are running, for a classroom while it is filled with students, or for an outdoor area during a recess or sporting event. A common oversight is to adjust and evaluate sound pressure (audio levels) in empty or quiet rooms.

4.3.1.2.2 Coverage is impacted by both speaker placement and sound pressure. It is more difficult to achieve adequate sound pressures in all areas of a room by using a single speaker located asymmetrically in the room (i.e., the front of a classroom or auditorium). Consider that centrally located or distributed speaker(s) is generally better.

4.3.1.2.3 Another factor to be considered is direct vs. indirect or reverberated sound. Intelligibility is greatly improved when there is a higher ratio of direct sound. Multiple speakers, each operating at lower sound pressure levels, also provides more direct sound and generally better intelligibility than a single speaker.

4.3.1.2.4 Sound that originates from above is usually easier for people to differentiate from other background noise or sound. In other words, it is often easier for people to distinguish and understand emergency notifications that come from speakers in the ceiling.

4.3.1.3 Interface with Fire Alarm Systems

When a fire alarm system interfaces with an emergency communications system, the interface needs to be monitored appropriately. The interface should be such that the primary function of both systems will not be compromised. For further information on this subject, refer to NFPA 72 *National Fire Alarm Code*, chapter on Protected Premises Fire Alarm Systems.

4.3.1.4 Interface with Mass Notification System

When multiple systems are designated to be used as mass notification systems, it is important that they interface properly with each other, in particular, with respect to voice messages and the fire alarm system. In the past, nothing took greater priority than a fire alarm. Today, mass notification inputs are permitted to take priority over the fire alarm, so it is imperative that operational interfacing between systems be considered.

4.3.1.5 National and Regional Input

National and regional emergency services such as FEMA (Federal Emergency Management Agency) and NOAA (National Oceanic and Atmospheric Administration) provide emergency broadcasts of weather and other warnings that are often interfaced with local public address and emergency voice notification systems. Consideration should be given to utilizing these services especially in areas subject to severe weather.

4.3.1.6 Emergency Takeover

Once an emergency condition has been identified, the emergency communications system must prioritize communications so that, to the greatest extent possible, routine communications do not interfere with emergency notification announcements. In the event that a telephone in a classroom is in use, there shall be adequate means to deliver emergency voice notification to all occupants of the room.

4.3.1.7 Visual Notification

Persons with disabilities must be considered when evaluating emergency communications. Audible notification only may be considered insufficient when considering the needs of a person with a hearing disability. Visual indicators including message displays may be considered to reduce risk.

4.3.1.8 Reliability Considerations

School communication systems must be reliable. Reliability must be considered in a multitude of areas such as, but not limited to, equipment, power, installation, infrastructure, operation, physical protection, and remote devices.

4.3.1.9 Operational Integrity

4.3.1.9.1 An emergency communication system may be considered to be part of a larger communication system that is used for routine purposes. This may present a benefit with respect to risk management, because a system that is used regularly for routine purposes is less likely to fall into a state of disrepair or inoperability. It is therefore important to consider the routine communication requirements of a facility to ensure that the communication system is capable of supporting these requirements through an adequate feature set. However, it must be integral to the design of such a communication system that under emergency conditions, the primary functionality be responsive to that situation above all others.

4.3.1.9.2 Some features of a system intended for routine use may interfere with the delivery of emergency communication features. For example, a privacy feature may impede the ability for staff to effectively communicate with a room in an emergency. Such features should be automatically defeated in the event of an emergency.

4.3.1.10 Physical Protection

An emergency communication system and its components must not be universally available for abuse or misuse, nor should it be routinely susceptible to damage or tampering. Different levels of physical protection must be considered for different components, appropriate to the risk of failure for all or parts of the system. Equipment or components that present a risk of total emergency communication system failure must be physically protected. Physical protection may include locked rooms, wiring in conduit, tamper proof plates and screws, or direct supervision by facility staff.

4.3.1.10.1 Equipment and Components

Equipment generally refers to main equipment racks. Component generally refers to controls which may include control consoles, and remote devices which may include speakers, call switches, telephones, etc.

4.3.1.10.2 Controls

Controls include, but are not limited to, administrative control consoles and/or administrative telephones and emergency paging devices. While these devices are intended to be accessible, the risk of misuse or tampering increases when these devices are not under constant direct supervision.

4.3.1.10.3 Remote Devices

Remote devices include, but are not limited to, classroom telephones. Classroom telephones are perhaps the most vulnerable elements of an emergency communication system. They are powerful devices that are subject to misuse (e.g., unauthorized paging, inappropriate 911 calls). They are also often provided the least physical protection of any component in the system. They are generally easy to remove, defeat, and damage. Locked cabinets for classroom telephones provide physical protection, but also may reduce accessibility during an actual emergency. Due to these considerations, sole dependence on a room telephone for emergency communication is a risk factor to consider.

4.3.1.10.4 Call-in Switches

Call-in switches are generally rugged and reliable. Tamper-proof screws may be considered to reduce the risk of tampering. Location of call switches is an important consideration for protection from abuse. Switches located at the door can be easily misused by people exiting the room. Misuse, resulting in false alarms, impacts the perceived reliability of the communication system and impacts the staff's ability to respond to real emergencies. Additionally, a clear and separate emergency call-in switch device should be located separately from the routine call-in switch, reducing the risk of physical interference preventing the initiation of an emergency notification.

4.3.1.10.5 Speakers

Speakers can potentially be tampered with and defeated. They should not be physically accessible under routine conditions. Speakers on a desk plugged into a receptacle are vulnerable to abuse or being defeated at any time, which increases the risk of failure. Since under certain emergency situations, they may be used as covert listening devices, speakers should be located unobtrusively, in such a manner as to require significant attention to defeat. Tamper-proof screws may be considered to further reduce risk. Also for consideration, speakers lend themselves well to duplication and distribution. Duplicated speakers can reduce risk should one speaker become inoperable. For further physical protection, separate speaker lines back to the emergency communication equipment may also be considered.

4.3.1.10.6 Vandal Resistant Devices

Remote devices that are located in areas with little or no direct supervision should be vandal resistant. Consideration to reduce risk includes resilient metal enclosures that can significantly resist most common tools; extra guards for speakers that eliminate the ability to puncture a speaker through the grill; resilient tamper-proof buttons with no moving parts; or rugged button travel limitations, tamper-proof screws, no exposed wiring, and no easily compromised wiring enclosures, such as plastic tubing or snap together conduit.

4.3.1.10.7 Weather Resistant Devices

Remote devices that are located in areas that are exposed to the weather must be designed to be weather resistant. Often such devices should also be vandal resistant due to the potential for unsupervised exposure.

4.3.1.10.8 PC and Network-Based Systems

PC networks have proven to be reliable. It is imperative, however, that when setting up the networks that safeguards be put in place. The emergency communication system is a life-safety system. Therefore, the primary application that is supported by the PC, server, and/or network must be considered to be the life

safety, not the conventional computer applications and services. This bears some concern, because in most cases the primary day-to-day concerns of network administrators is the performance of conventional computer applications and network services, not life-safety systems. Care must be taken during the design of emergency communications systems that utilize computer hardware and networks to ensure that over time, the life-safety considerations remain paramount.

4.3.1.10.8.1 Protection

Computers and networks are subject to attack or inadvertent misuse through various avenues. An emergency communications system that depends on computers and their networks for life-safety functionality must be continuously protected against all forms of attack, known or unknown, using firewalls and other measures. In other words, protection for these systems must be continuously audited, evaluated, and enhanced by qualified people and/or other protective mechanisms.

4.3.1.10.8.2 Server-Based Systems

Emergency communications servers must be physically protected with a secure location. Adequate backup and redundancy must be in place to ensure that any failures (e.g., hard drives) are quickly and easily remedied. Server operating systems are frequently patched or updated. Consideration of an update policy is important. Not having an automatic update policy increases the risk of obsolete protection, while automatic updates increases the risk of unintended changes to the operating system. When installing system updates, however, they should be evaluated to make sure they are compatible with the life-safety applications before installing them.

4.3.1.10.8.3 Computer Networks

4.3.1.10.8.3.1 Networks are often a shared resource. Large traffic loads unrelated to life safety, which could occur during an emergency, must be managed with regard for emergency communications requirements. Consider that the delivery of emergency notifications must be assured regardless of other devices and or applications sharing the network at any time. A segregated network (VLAN or otherwise) must be considered during the design of the network.

4.3.1.10.8.3.2 Networks are often distributed with network switches in multiple locations. This introduces the risk of failure to any device that is downstream of a failed switch. Network management should be utilized to alert maintenance of a failed device. Also, network switches, upon which any part of the emergency communications system relies, must be provided power redundancy equivalent to the central equipment.

4.3.1.10.8.3.3 Wired and wireless networks are often accessible (physically or otherwise, for example, network switches in a computer lab, or unused network connections at wall jacks). Keeping the network that hosts the emergency communications equipment functionality physically and electrically separate from other parts of the network that are accessible will reduce the risk that life-safety services could be compromised.

4.3.1.10.9 Wiring

Wiring must conform to all applicable codes and standards. However, often codes and standards are concerned primarily with operational safety and reliability. Risks associated with abuse, or deliberate malicious damage must be considered in the context of system reliability.

4.3.1.10.9.1 Environmental Protection

Wiring should not be exposed to adverse environments or accessible to damage or misuse by unauthorized personnel. In situations where wiring cannot be practicably protected (such as telephone lines or telephone coil cords), the risk of failure must be considered greater, and therefore factored into the overall emergency communications system design. Adding physical protection to the wiring can reduce the susceptibility to malicious damage. Physical protection may include cable trays, conduit, or other approved means of mechanical protection.

4.3.1.10.9.2 Exterior Wiring

In addition to the precautions mentioned previously, exterior wiring, in particular, must be considered a candidate for protection from the weather (high winds, falling trees, standing water, and UV rays) as well as from vandalism.

4.3.1.10.9.3 Transient and Lightning Protection

All wiring, but in particular, exterior wiring, must be considered a candidate for lightning and transient protection, beyond that which is normally provided with the equipment.

4.3.1.10.9.4 Grounding

Correct and proper grounding is mandated by local codes. However, with respect to an emergency communications system, there are additional risks to consider, particularly when the system is distributed with multiple power sources at various locations. A local lightning strike may raise the ground potential difference between equipment connected to the same grounding system to such an extent as to damage system components. In areas where lightning is a common concern, even grounding that exceeds code, coupled with lightning protection, may be insufficient to protect equipment in all cases.

4.3.1.10.10 Power

Reliable power is fundamental to a reliable emergency communications system. Power that is subject to frequent interruptions or brownouts must be considered a risk factor and should be mitigated appropriately.

4.3.1.10.10.1 Primary Power

There may be situations where primary power is intentionally removed from a building. In the context of an emergency communications system, systems that rely on the primary power infrastructure (wiring) and a secondary power source (i.e., backup generator) may inadvertently fail if the backup generator is purposely taken off line. This could be the case for safety in the event of a fire, or police directive during a confrontation. In these cases, the risk of also losing the emergency communications capability must be evaluated.

4.3.1.10.10.2 Secondary Power

4.3.1.10.10.2.1 Secondary power will usually be in the form of batteries, or uninterruptible power supplies (UPS). In the case of a failure of primary power, the risk associated with unexpected failure of the secondary power must be considered. Based on the length of power outage, the secondary power will eventually fail. The exact moment of failure, however, is a risk that should be considered in the emergency response plan. Design of the UPS capacity and current draw of critical communications devices must be determined. Also, the anticipated length of emergency operation must be considered when planning for emergency communications when operating on secondary power. Crucial communications strategy must be considered early in developing the response plan.

4.3.1.10.10.2.2 Secondary power in support of the emergency communication system should not be shared with any other non-critical system. This is especially important when considering distributed equipment. As an example, Internet Protocol (IP) telephones that are part of an emergency communication system must be supported by the secondary power system. Therefore, the network switches that support the IP phones must also be supported by the secondary power system.

4.3.1.10.10.3 Circuits and Circuit Breakers

4.3.1.10.10.3.1 The emergency communications system should not share a common power circuit with non-emergency equipment. A circuit that is used for other or undefined purposes (e.g., a wall outlet) can fail at any time though overload. Also, a shared circuit may be impacted by interference generated by other equipment in non-obvious ways, which in turn may impact the functionality of the emergency communications equipment.

4.3.1.10.10.3.2 Additionally, a circuit may be switched off in order to service other equipment, inadvertently rendering the emergency communications equipment inoperative. Isolating the circuit allows risk to be lowered because the emergency communications equipment may be clearly and specifically identified directly at the circuit breaker. However, with a distributed system, there may be many circuits that are associated with the emergency communications system, all of which should be isolated and identified.

4.3.1.10.11 System Readiness

4.3.1.10.11.1 Constant Use

A system under constant use could be considered more reliable than one under periodic or infrequent use because an operational failure is obvious and repairs must be made to keep the system useable.

4.3.1.10.11.1.1 To the greatest extent possible, the core equipment employed by the emergency communications system should be exercised daily in routine situations. For example, use of microphones, consoles, amplifiers, central equipment, speakers and call switches should be part of the daily routine of school communications. Aspects of the system that are not used routinely should either be incorporated into routine inspection and testing or incorporated into routine drills.

4.3.1.10.11.1.2 Failures occurring during routine operation should be incorporated into the facilities emergency communications equipment maintenance plan, and not just treated as a low-priority routine maintenance issues.

4.3.1.10.11.2 Periodic or Infrequent Use

Facilities having a dedicated emergency communications system that is not used routinely should be electrically supervised. More frequent and rigorous inspection, testing, and drills should be considered to reduce the risk associated with undetected equipment failure.

4.3.1.10.11.3 Electrical Supervision

4.3.1.10.11.3.1 A system that is not used routinely could be electrically supervised to increase awareness of a system failure. All equipment and system wiring should be electrically supervised so that a fault that would negatively impact proper system operation will be promptly identified so repairs can be made in a timely manner. Detection of faults by an electrically supervised system should be prominently annunciated both audibly and visibly. Systems such as those that only provide a computer-generated report of the fault or other similar non-intrusive means to identify a fault and that do not utilize prominent audible and visible trouble signals should be considered inherently less reliable.

4.3.1.10.11.3.2 When constant use principles are not applied for speakers, electronic supervision of speakers can be considered to reduce the risk of undetected failures. However, electronic supervision of speakers must be considered relative to the method of supervision. Some methods of electrical supervision monitor speaker wiring and not the speaker itself. While monitoring the integrity of the wiring is good, it does not eliminate the risk of speakers being inadvertently or intentionally damaged, covered up, or turned down with a volume control. As such, electronic supervision of speaker wiring is not a replacement for routine inspection and testing of each speaker location. Supervision methods that monitor the health of the speaker itself may be considered if the goal is to reduce how often infrequently used speaker are inspected and tested.

4.3.1.10.11.3.3 Call switches may be deemed reliable based on constant use principles. End of line termination will allow a system to monitor the condition of the call-switch wiring, but not the call device itself. If constant use principles are not employed for these locations, periodic visual inspection and functional testing should be performed.

4.3.1.10.12 Testing and Maintenance

For school communications equipment that is used infrequently, testing or drills must be scheduled at fixed intervals to evaluate system functionality. Risk assessment must determine the acceptable risk of system failure based on testing interval. Refer also to Section 6 Inspection, Testing, and Maintenance.

4.3.1.10.13 Emergency Event Consideration

Facilities should have the ability to page to every area of the facility, both inside as well as externally (outdoors) to communicate that the school is in a state of lock out. The communications system should be able to announce at a reasonable decibel level to all areas including classrooms, corridors, offices, restrooms, gymnasiums, locker-rooms, auditoriums, cafeterias, athletic fields, and parking lots.

4.3.1.10.13.1 Lockdown

Schools are placed into "lockdown" during an immediate threat inside or directly outside the school facility. Examples of these types of events include an armed intruder or non-custodial parent inside the building, or an armed intruder on or adjacent to school grounds but not inside the building. In order to adequately perform a facility-wide lockdown where each individual classroom must lock its door, the communications system must provide the ability for hands-free, two-way communications to every room in the facility. This provides the ability to announce the lockdown event and to confirm that every classroom has been able to comply or is receiving assistance.

4.3.1.10.13.2 Lockout (Shelter-in-place)

Schools utilize lockouts when they desire to keep students and staff inside the building and visitors and outsiders out of the building, but still consider it safe for students and staff to move about freely inside the building. Examples of events leading to lockouts are suspects loose in the community, but not directly on or near school grounds, or community-wide emergencies. Shelter-in-place has the same communications requirements as a lockout but is used more often for weather-related emergencies such as a tornado or possibly a chemical leak or other outdoors danger.

4.3.1.10.13.3 Evacuation

Evacuations occur during emergencies such as power loss, fire, earthquakes, gas leak, or bomb threat. The communications system must provide the ability to communicate to all areas of the facility in the event of an intended evacuation. Off-premises (outside) access to paging and intercom features should be considered so that authorities can confirm that the building has been completely evacuated.

4.3.1.10.13.4 Reverse Evacuation

School communication systems shall have the ability to audibly notify all staff and students to perform a reverse evacuation from a building, facility, and/or campus.

A common ploy by a person intending to do harm is to activate the fire alarm system in order to get people out of the building. It is imperative that the person or persons in charge have the ability to override the fire alarm and provide voice and/or visual notification to direct people to initiate a reverse evacuation.

Section 5 FUNDAMENTALS OF SCHOOL COMMUNICATION SYSTEMS

5.1 APPLICATION

The basic function of a complete school communication system shall comply with the requirements of this chapter.

5.2 PURPOSE

The purpose of school communications systems shall be to provide notification of manually or automatically initiated alarms, to allow staff/students to summon aid, and to allow administration personnel to notify staff/students of potential or actual emergency events on a school premises or campus.

5.3 EQUIPMENT AND PERSONNEL

Equipment constructed and installed in conformity with this standard shall be listed for the purpose for which it is used. School communication system components shall be installed in accordance with the manufacturers' installation instructions.

5.4 SYSTEM FUNDAMENTALS

5.4.1 Power Supplies

5.4.1.1 Code Conformance

All power supplies shall be installed in conformity with the requirements of NFPA 70 *National Electrical Code* for such equipment and with the requirements indicated in this subsection.

5.4.1.2 Monitoring of Power Supplies

Both primary and secondary power supplies must be monitored for integrity so that any fault will cause an audible and visible trouble signal to draw attention to the trouble and to initiate corrective action.

5.4.1.3 Primary Power Supply

5.4.1.3.1 Dedicated Branch Circuit

A dedicated branch circuit of one of the following shall supply primary power:

- a) Commercial light and power
- b) An engine-driven generator or equivalent where a person specifically trained in its operation is on duty at all times
- c) An engine-driven generator or equivalent arranged for co-generation with commercial light and power where a person specifically trained in its operation is on duty at all times

5.4.1.3.2 Mechanical protection

5.4.1.3.2.1 The dedicated branch circuit(s) and connections shall be mechanically protected.

5.4.1.3.2.2 Circuit disconnecting means shall have a warning marking, shall be accessible only to authorized personnel, and shall be identified as "SCHOOL COMMUNICATIONS CIRCUIT."

5.4.1.3.2.3 The location of the circuit disconnecting means shall be permanently identified at the school communications control unit(s).

5.4.1.3.3 Overcurrent Protection

An overcurrent protective device of suitable current-carrying capacity that is capable of interrupting the current-carrying capacity to which it can be subjected shall be provided in each ungrounded conductor.

5.4.1.4 Secondary Power Supply for School Communications Systems

The secondary supply shall consist of one or more uninterruptible power supplies (UPS) with dedicated storage batteries arranged in accordance with NFPA 111 *Standard on Stored Electrical Energy Emergency and Standby Power Systems*. The exception to the requirement of an UPS is for the portion of the emergency communication system that is a fire alarm system that complies with NFPA 72 *National Fire Alarm Code*.

5.4.1.4.1 Capacity

The secondary power supply(ies) shall have sufficient capacity to operate the school communication system under a quiescent load (system operating in a non-alarm condition for a minimum of 4 hours and, which at the end of that period, shall be capable of operating all alarm notification appliances used for evacuation or mass notification purposes or to direct aid to the location of an emergency for at least 60 minutes).

5.4.1.4.2 Secondary Power Operation

Operation on secondary power shall not affect the required performance of a school communication system. The system shall produce the same alarm, supervisory, and trouble signals and indications, excluding the alternating current (ac) power indicator when operating from the secondary power source, as are produced when the unit is operating from the primary power source.

5.4.1.4.3 Continuity of Power Supplies

Transition of power for the communications system shall not interrupt operations of the system.

5.4.2 Audio Amplifiers

All independently powered audio amplifiers, not subject to constant use, shall be electrically supervised.

5.5 SYSTEM FUNCTIONS

5.5.1 General

5.5.1.1 In an emergency situation, each classroom/ staff location must have the capability to initiate a manual notification from a dedicated emergency device.

5.5.1.2 The primary manual notification device must be independent of a telephone, distinct from the telephone in location, and should be positioned in a consistent classroom location.

5.5.1.2.1 Routine call-ins may be accomplished by using the telephone or additional buttons but must not use the emergency manual notification device.

5.5.1.2.2 Telephones may be used in addition to a primary manual notification device.

5.5.1.3 The school communication system must have the capability to accept and receive automated notification from other emergency systems located on the facility and/or campus. The school communication system would not be the primary system for the other system. Other emergency systems, include, but are not be limited to:

- a) 911 call from a telephone system
- b) Entrance/egress access
- c) Fire alarm
- d) Security/access control system

5.5.1.4 Each classroom/staff location/area of assembly must have the capability to receive emergency notification, including audible instructions from the school communications system or an administrator. The emergency notification devices must be capable of being heard by all students/staff in a classroom/staff room/area of assembly. Minimum requirements for audio level and intelligibility shall be achieved as specified in NFPA 72 *National Fire Alarm Code*.

5.5.1.4.1 There must be at least one device capable of broadcasting an emergency notification to each schoolroom location on a priority override basis.

5.5.1.4.2 In the event that a notification device is engaged in independent activity, the system must support automatic pre-emption of the independent activity in the event of an emergency notification.

5.5.1.4.3 Subsequent operation of a device in the event of an emergency notification must not be impaired.

5.5.1.4.4 When the school communication system is used as a secondary notification system, emergency notifications of audible instructions must have priority.

5.5.1.5 All authorized personal must have the ability to initiate an audible mass notification that reaches all classrooms/staff rooms/areas of assembly in the facility/campus simultaneously.

5.5.1.6 Authorized personal must have the ability to silently monitor each classroom/staff room or groups of rooms and/or hallways. This provision is intended for use in hostage or intruder situations. Devices used for monitoring must be permanently affixed.

5.5.1.7 All telephones in a school must have direct dial 9-1-1 access to the 911 operating authority. It must not be required to dial an access code such as 9-, 8-, 9-9, 8-9 to reach the 911 operating authority.

5.5.1.7.1 All 911 calls from staff rooms/class rooms must annunciate and display their location at the designated local administration location(s) in addition to the connection to the 911 operating authority. Typically this should include:

- a) Main receptionist/secretary location
- b) Principal location
- c) Vice principal location
- d) School nurse location
- e) School police officer location

5.5.2 Initiation of Emergency Calls

5.5.2.1 General

Initiating devices fall into two basic categories:

- a) Manually initiated, intended to be selected by a student or staff member and,
- b) Automatically initiated, intended to be actuated from other systems on the premises.

5.5.2.2 Types of Initiating Devices

5.5.2.2.1 Emergency Call Switch—Wired

Installation of emergency call switches must provide:

- a) Ability to communicate the location of an emergency to internal and remote notification
- b) Supervised wiring to call switch to indicate a fault that would impair the ability to place an emergency call

5.5.2.2.2 Telephones

Where telephones are used as part of a life-safety communications system they must:

- a) In the event of an emergency situation, initiate a manual notification and identify the location of the emergency (by use of a specific key or key sequence on the phone)
- b) Maintain the notification regardless if phone is subsequently hung up
- c) Initiate notification after 60 seconds if handset has been knocked off hook

5.5.2.2.3 Emergency Call Switch—Wireless

- a) Emergency wireless call device shall be supervised
- b) An alarm shall be indicated if wireless device is off line for more than 5 minutes
- c) An alarm shall indicate low battery in the wireless device 24 hours before the unit would cease to function

5.5.2.2.4 Confirmation Switch—Wired

School communication system shall have a device in each classroom which can be used to indicate compliance with lockdown order.

- a) This may be a key or key sequence from a telephone
- b) This may be a normal priority call switch, which after a lockdown is initiated, indicates confirmation of lockdown
- c) This device shall be separate from the emergency call switch

5.5.3 Annunciation of Emergency Calls

5.5.3.1 General

5.5.3.1.1 Annunciation for emergency calls must indicate the location of origin of an emergency call and must have a distinctive emergency audible indication to draw the attention of administration personnel to the emergency condition.

5.5.3.1.2 Each campus/facility must have at least one location where emergency calls are annunciated.

5.5.3.1.3 The emergency annunciation tone must silence automatically after call is acknowledged by a single key press or PIN code.

5.5.3.1.4 Canceling of emergency calls must only be performed from the system by using one of the following methods:

- a) Establishing an audio path between the location of the emergency and the answering location and acknowledgement by a single key press or PIN code
- b) Manual intervention requiring an authorization code

5.5.3.1.5 The system must provide the capability for emergency calls to be annunciated at multiple locations including off-site or remote locations.

5.5.3.2 Types of Annunciation Devices

5.5.3.2.1 Speakers

Where speakers are used to annunciate emergency calls:

- a) Annunciation must include voice announcement of location of emergency call if the speaker is not in close proximity with another annunciation device such as a telephone or display that is capable of display of emergency call-ins
- b) Annunciation volume must be such that it conforms with the requirements of NFPA 72 *National Fire Alarm Code* for private mode signaling
- c) Telephone or other device must be accessible for two way communication with location of emergency call
- d) Emergency call annunciation must override any lower priority audio signal to annunciate at designated speaker

5.5.3.2.2 Telephone/Administrative Console

Telephones/administrative consoles are intended for individual users. Where telephones/administrative consoles are used to annunciate emergency calls:

- a) Annunciation must include a distinctive emergency annunciation to indicate to user that an emergency call is pending
- b) The telephone's emergency annunciation must override ringing from inbound telephone calls
- c) Emergency designation and location information should appear on telephone display, or when a call is answered a voice announcement must indicate that it is an emergency call and its location or origin
- d) The telephone must allow for two-way conversation with location of emergency call

5.5.3.2.3 Displays

Displays are intended to alert multiple users in a single location. Where displays are used to annunciate emergency calls:

- a) Annunciation must include a distinctive emergency annunciation to indicate to users that an emergency call is waiting. To achieve this, displays may be used in conjunction with speakers or telephones/administrative consoles
- b) The emergency annunciation volume must be such that it conforms with the requirements of NFPA 72 *National Fire Alarm Code* for private mode signaling
- c) The emergency annunciation tone must override any lower priority audio activity on the display to annunciate the emergency call
- d) Location information as shown on display is intended to be conveniently read by all intended occupants in the room
- e) The telephone or other device must be accessible for two-way communication with the location of origin of the emergency call

5.5.3.3 Emergency Call Escalation

The school communication system must have a call escalation process whereby if an emergency call is not acknowledged within 24 seconds, that call will be escalated and annunciated at an additional location. Care must be used in planning for device(s) for escalation so that a trained user will be available and know how to respond to the emergency call. Typical devices include the following:

- a) Another telephone/administrative console
- b) Overhead speakers
- c) Wall displays
- d) Offsite telephones via public telephone network
- e) Pagers
- f) Email/text messaging
- g) Other interfaced remote notification system

5.5.3.3.1 The escalation sequence should not prevent the emergency call from being acknowledged from any device notified earlier in the escalation sequence.

5.5.3.3.2 The call escalation sequence must have a minimum of three levels of escalation.

5.5.3.3.3 Telephone or other device must be accessible for two-way communication with location of origin of emergency call.

5.5.4 Lockdown

In the event of a lockdown occurrence, the school communication system must be able to:

- a) Send an audible and voice emergency notification to all classrooms/ staff locations/ areas of assembly
- b) Send a lockdown signal to an access control system, if one is in use. This notification can be manual, or pre-recorded
- c) Each call switch shall have the ability to send a manual notification confirming lockdown status during a lockdown event
- d) Each call switch shall retain the ability to send an emergency manual notification during a lockdown event

5.5.5 Lockout

In the event of a lockout occurrence, the school communication system must be able to:

- a) Send an audible and voice emergency notification to all classrooms/ staff locations/ areas of assembly
- b) Send a lockout signal to an access control system, if one is in use. This notification can be manual or pre-recorded

5.5.6 Evacuation

In the event that the school facility is to be evacuated, the school communication system must be able to:

- a) Send an audible and voice emergency notification to all classrooms/staff locations/areas of assembly and outside grounds including, but not limited to, playgrounds, parking lots and athletic fields
- b) Override any prerecorded voice emergency notification with live voice notification to all classrooms/staff locations/areas of assembly and outside grounds including, but not limited to, playgrounds, parking lots and athletic fields in case of any changes in evacuation routes
- c) Send evacuation signal to an additional notification system, including but not limited to, the fire alarm system and mass notification system

5.5.7 Reverse Evacuation

In the event that a school must perform a reverse evacuation, the school communication system must be able to:

- a) Send an audible and voice emergency notification to all classrooms/staff locations/areas of assembly and outside grounds including, but not limited to, playgrounds, parking lots, and athletic fields
- b) Override any prerecorded evacuation notification with reverse evacuation notification to all classrooms/staff locations/areas of assembly and outside grounds including, but not limited to, playgrounds, parking lots, and athletic fields
- c) Override fire alarm system and mass notification system in order to halt an ongoing evacuation
- d) Send reverse evacuation signal to an additional notification system including, but not limited to, the fire alarm system and mass notification system

Section 6 INSPECTION, TESTING, AND MAINTENANCE

6.1 GENERAL

6.1.1 Communications systems for life safety in schools require initial acceptance and periodic validation testing, inspection and preventive maintenance.

6.1.2 System documentation must be maintained and be available for the purpose of updating information and for use by technicians for testing and maintaining the system.

6.1.3 Manufacturer's software and equipment testing and maintenance agreements are recommended in order to keep current with system software revisions and to ensure reliable system operation.

6.2 REQUIRED DOCUMENTATION

6.2.1 As-Built Drawings (Record Documentation)

6.2.1.1 As-built drawings must be completed by the installer and turned over to the facility prior to acceptance of the installation.

6.2.1.2 As-built drawings must be updated whenever changes or modifications are made to the communications system(s).

6.2.1.3 When any changes or modifications are made to the system(s), the date of the change (revision date) must be clearly marked on any associated documentation.

6.2.2 Owner's Manual

6.2.2.1 The installer must turn over an owner's manual to the facility.

6.2.2.2 The owner's manual must include a complete set of operations and maintenance manuals, manufacturer's published instructions, and product technical data sheets covering all system equipment.

6.2.3 Software

6.2.3.1 For software-based systems, a copy of the current revision of the site-specific software and where applicable, software licenses must be provided by the supplier of the system or by the servicing company.

6.2.3.2 The copy of the software must be readily available in case of equipment failure or corruption of the existing software in use.

6.2.3.3 The purpose of the copy of the site-specific software is to minimize potential system downtime.

6.3 DOCUMENT ACCESSIBILITY

6.3.1 As-built drawings, owner's manuals, software and other record documentation must be maintained on site and available only to authorized personnel.

6.3.2 Documents must be physically protected by means such as a lockable cabinet, sized to contain all system documents in 6.3.1 as well as copies of inspection, test, and maintenance reports.

6.4 PREVENTIVE MAINTENANCE AND SERVICING

6.4.1 Preventive maintenance must be performed in accordance with the equipment manufacturer's recommendations.

6.4.2 Preventive maintenance reports must be saved in the same location as the required documentation in 6.2.

6.4.3 Service reports for system repairs or routine service must be saved in the same location as the required documentation in 6.2.

6.4.4 Preventive maintenance and other service documentation must be maintained for a period of three years.

6.5 TESTING

6.5.1 Periodic testing shall be performed to validate correct system operation.

6.5.2 Testing must be performed in accordance with methods and the frequency in Table 6-1.

6.5.3 At a minimum, the communications system(s) must be tested prior to the start of each school year, and after any extensive shut down of the facility.

6.5.4 Components of the system that are not used on a regular basis or that are not supervised must receive more frequent testing.

6.5.5 Testing reports must be saved in the same location as the required documentation in 6.2.

6.5.6 Testing reports must be maintained for a period of three years.

**TABLE 6-1
TESTING METHODS AND FREQUENCIES**

Component	Acceptance Test	Periodic Test Constant Use or Supervised	Periodic Test Infrequent Use or Non-Supervised	Test Method
Control Equipment	YES	Annually	Semi-Annually	At a minimum, control equipment must be tested to verify correct receipt of call inputs; operation of notification signals and other functions (outputs); circuit supervision, including detection of open circuits and ground faults; and power supply supervision for detection of loss of ac power and disconnection of secondary batteries or UPS. All emergency communications and security features must be tested.
Annunciation	YES	Annually	Semi-Annually	The correct operation and identification of calling stations shall be verified. If provided, the correct operation of annunciator under a fault condition shall be verified.
Amplifiers	YES	Annually	Semi-Annually	Correct switching and operation of backup equipment shall be verified.
Secondary (Standby) Power Supply	YES	Annually	Semi-Annually	All primary (main) power supplies must be disconnected and the occurrence of required trouble indication for loss of primary power shall be verified. The ability of batteries to meet standby and operational requirements shall be verified. Voice communications systems must be tested for a minimum of 15 minutes. Primary (main) power supply must be reconnected at end of test.
Batteries/UPS	YES	Semi-Annually	Quarterly	Check for functionality and that system configuration will support the schools required emergency communications plans during power outage.
Interface Equipment	YES	Semi-Annually	Quarterly	Interface equipment connections and throughput shall be tested by operating or simulating the connected equipment. Signals required to be transmitted shall be verified.
Peripheral Devices				
Call Switches	YES	Annually	Semi-Annually	Call switches must be operated to verify the signal is sent to the appropriate location and annunciate the location of the emergency call.
Telephones	YES	Annually	Semi-Annually	Test key pad functions and speaker and handset voice quality as well as phone display and message waiting and ringer functionality.
Locking Devices	YES	Annually	Semi-Annually	Activate the means of initiating locking devices to ensure proper locking.
Speakers	YES	Annually	Semi-Annually	Audible information shall be verified to be distinguishable and understandable.
Textual Displays	YES	Annually	Semi-Annually	Test that text message displays are functional, including LEDs and display brightness.
School LAN and WAN	YES	Annually	Semi-Annually	Verify that no changes in the LAN/WAN have been made that would impact voice quality of service or any other system operation.

§