
*A NPSTC Public Safety Communications Report*

***The National Public Safety Telecommunications Council is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.***

# Defining Public Safety Grade Systems and Facilities

Final Report 5/22/2014

***Support to NPSTC provided by the U.S. Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC), and the National Protection and Programs Directorate, Office of Emergency Communications (OEC). Points of view or opinions expressed are those of the originators and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security.***

American Association of State Highway and Transportation Officials | American Radio Relay League | Association of Fish and Wildlife Agencies | Association of Public Safety Communications Officials | Forestry Conservation Communications Association | International Association of Chiefs of Police | International Association of Emergency Managers | International Association of Fire Chiefs | International Municipal Signal Association | National Association of State Chief Information Officers | National Association of State Emergency Medical Services Officials | National Association of State Foresters | National Association of State Technology Directors | National Emergency Number Association | National Sheriffs' Association

8191 Southpark Lane, #205 · Littleton, CO 80120 · Phone 866-807-4755 · Fax 303-649-1844 · Website www.NPSTC.org

## Executive Summary

The term "Public Safety Grade" is a conceptual term that refers to the expectation of emergency response providers and practioners that their equipment and systems will remain operational during and immediately following a major natural or manmade disaster on a local, regional, and nationwide basis. The term Public Safety Grade (PSG) in this document is used to refer to network hardening or network sustainability.

This document is intended to provide guidance for the First Responder Network Authority (FirstNet) as it constructs and implements the Nationwide Public Safety Broadband Network (NPSBN). In developing this document, the Public Safety Grade Task Group, operating under the National Public Safety Telecommunications Council (NPSTC's) Broadband Working Group (BBWG), also considered Public Safety Grade requirements and recommendations for Land-Mobile Radio (LMR) communications sites. These recommendations and requirements should be applied to both existing and new LMR sites.

This report expands on previous NPSTC documents that used the term Public Safety Grade (PSG) in an attempt to convey the differences in the way public safety "mission critical" communications systems are designed compared to the typical commercial systems. The PSG term was not defined in prior NPSTC reports, because the conceptual definition is complex and is best rendered with many definitions and best practice design elements in a variety of areas that make up a total communication system. This work is primarily focused on mobile data to assist FirstNet in their design of the NPSBN but can also be helpful to public safety agencies that are designing or specifying new or upgraded public safety LMR systems.

This report is not intended to replace or contradict either the NPSTC *700 MHz Public Safety Statement of Launch Requirements* report or the NPSTC *Push to Talk (PTT) over LTE Public Safety Requirements* report. The best practices and requirements listed in this document describe elements, that when implemented as a whole, create the public safety expectation for reliability and redundancy. It should be noted that this document contains both "Best Practices" and "Requirements." The reference to "Requirements" indicates that the cited information is drawn directly from an existing standard. The PSG Task G roup also recognizes that it will be very difficult to implement all the best practices throughout a nationwide data system. However, the designers of the NPSBN should strive to implement these practices to the greatest extent possible so that system will be considered by users to be a PSG system.

The concept of PSG drives those design choices that result in emergency responders being able to maintain their ability to communicate, as necessary, during mission critical incidents affecting the life, health and safety of the public. PSG is the result of implementation techniques typically used or required by public safety entities to achieve the level of reliability

and resiliency required to support mission critical activities. NPSTC has previously published a PTT over Long Term Evolution (LTE) document detailing many of these issues.

Public Safety Grade also refers to the core best practices, definitions, performance specifications, and the general and featured best practices characteristics necessary for mission critical public safety operations.

A PSG communications system should be designed to resist failures due to manmade or natural events as much as practical. This definition includes descriptions of coverage criteria for public safety systems that must be considered as a component of system reliability and elements of resiliency that ensure a rapid return to optimal performance. PSG communications systems are systems that are used by public safety responders and that have been evaluated by public safety officials to provide reliant and resilient operations in the event of natural or manmade disasters or events.

Communications is vital to both public safety field and command personnel during routine, local incidents and even more so during major incidents covering a larger area. Public safety voice LMR networks today are among the most reliable networks available in the United States. Today's commercial wireless networks are not built to the same standard. The NPSBN must be constructed to meet as many of these PSG requirements as possible. And, since network and cell site sharing with commercial operators may be part of the NPSBN design, those commercial sites which also house NPSBN equipment must be upgraded to meet as many of these requirements as possible. The NPSBN must be relied upon and trusted by the public safety community. It must be a Public Safety Grade network, not a commercial "best effort" network. Emergency responders and their commanders depend upon communications systems to be fully functional at all times and under all circumstances. In order to be successfully adopted by the public safety community, the NPSBN cannot be anything less.

It is important to note that this document <u>is not</u> intended to include the totality of all site requirements. This document is intended to highlight the efforts that must be undertaken above and beyond a typical wireless communication site to make it hardened to Public Safety Grade. In some cases the requirements do go beyond what the PSG Task Group recognizes is common practice for many wireless communication sites; however, the Task Group erred on the side of including what may not be commonly performed at the typical non-public safety site.

NPSTC would like to acknowledge and thank the U.S. Department of Homeland Security, Office of Emergency Communications, for sponsoring the face-to-face meeting in Boulder, Colorado, allowing public safety personnel to collaborate and complete major sections of this document.

# Table of Contents

# 1 Introduction

Hurricane Sandy struck the East Coast in 2012 and all of the commercial wireless communications networks experienced varying degrees of outage. There were several "lessons-learned" reports which showed that 20 percent of all commercial wireless cell sites were out of commission, some for many weeks leaving large areas without any form of cellular communications.

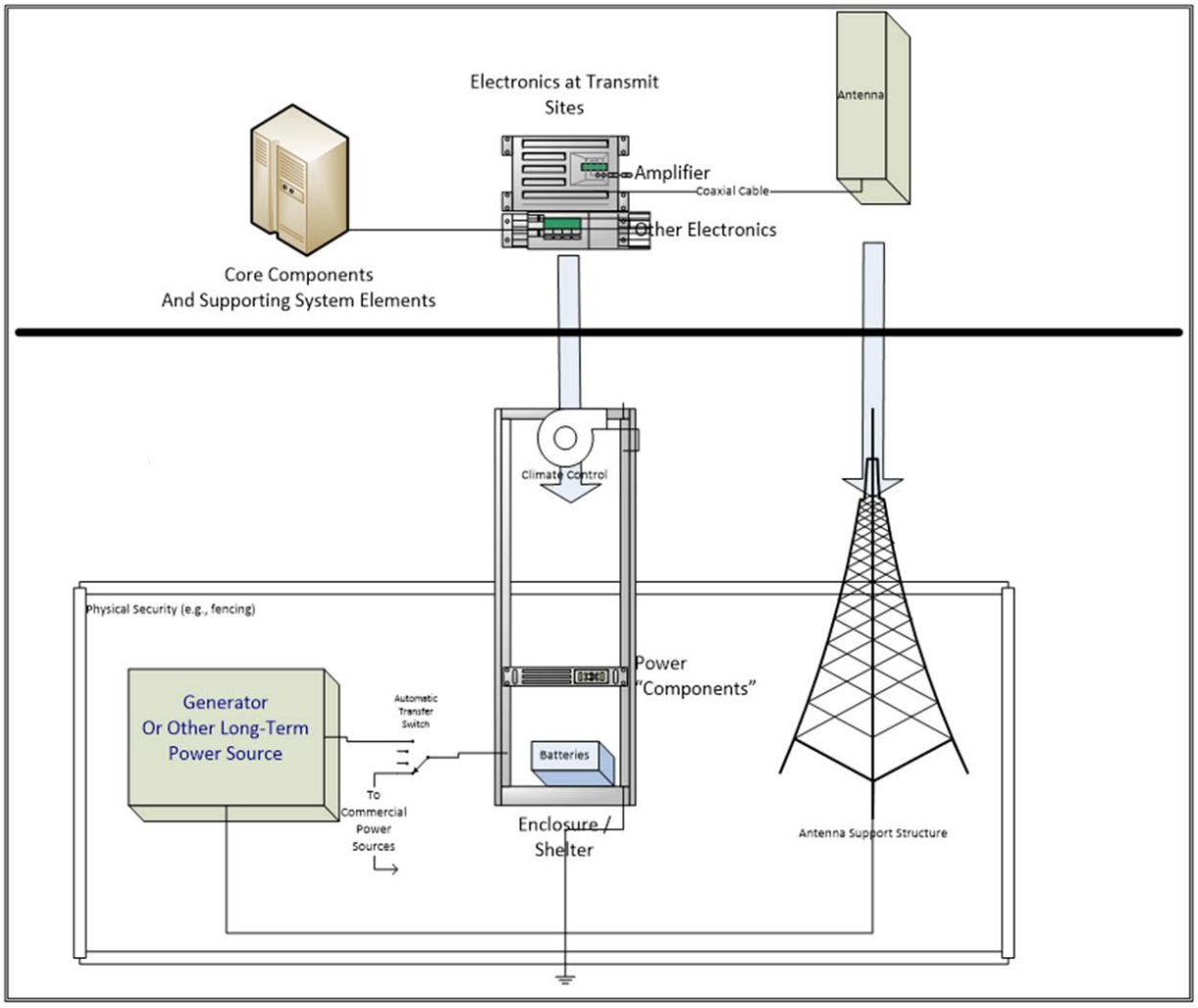
The National Public Safety Broadband Network (NPSBN) must be built to Public Safety Grade (PSG) standards. It is generally recognized commercial broadband networks are designed as "best effort" networks and are more prone to outages during both natural and human caused disasters, power outages, and other events. The NPSBN, as well as existing LMR systems, must be able to withstand more severe natural and manmade disasters and must also be capable of being quickly repaired and/or quickly place into service temporary network components after one of these events.

Today's public safety voice networks and existing LMR systems are built to higher resiliency standards than found in commercial provider installations. They are built to withstand natural and manmade incidents – these events typically correspond to high risk to life and property and are critical moments for public safety communications. They have more resilient systems and substantial communications redundancy. As the LTE network protocol itself lacks the failover mechanisms of a LMR system, the importance of highly available NPSBN core systems and cell sites becomes much more critical. And it becomes paramount to "harden" the NPSBN to achieve PSG service. Therefore, it is critical that public safety establish the requirements to harden the NPSBN to PSG – one that establishes a highly available service during all hazards and events.

The public safety community understands that the entire FirstNet system may not, economically, be built to meet all of the best practices contained in this document. For example, a cell site at a distant or remote portion of the network might not economically be built to meet 100 percent of these requirements. However, a central site that provides links and access to adjoining sites should be considered as a critical site and should be built and operated based on all of these recommendations. FirstNet, in consultation with local jurisdictions, should assess the importance or criticality of each site and determine how to balance cost and risk. In fact, not all of the existing LMR public safety communications sites in service today will meet these requirements. However, a significant number of them will meet the requirements and, as described above, LMR services include communications fallback modes that will not be available on a broadband network built using LTE today.

Congress, in authorizing the construction of the First Responder Network (FirstNet), and the first responder community both recognize that the phrase "public safety" includes a wide variety of governmental and private agencies who respond daily to incidents and larger-scale disasters. Traditional "first responders" are law enforcement, firefighting, and emergency medical services. "Emergency responders" include, as examples, electric, water and gas utilities, transportation, transit, search-and-rescue, hospitals, the Red Cross, and many others.

The requirements in this document apply to sites, including urban, suburban, and rural infrastructure used to provide wireless communication service. These include dedicated public safety communications sites, co-location of the NPSBN on existing or new commercial cell sites, building mounted sites, and any site where either LMR or NPSBN network components are deployed. The figure below identifies the various components covered in this report.



These requirements do not apply to temporary, vehicle-mounted, or mobile sites. Some public safety LMR sites do not, today, meet the requirements spelled out in this document; however, there are some significant differences between today's LMR public safety voice networks and the new NPSBN network.

Any system builder must carefully consider these best practices and requirements. It is acknowledged that some requirements and recommendations may be impossible to meet at a particular site while others may be economically impractical. It is understood that FirstNet (with input from the local jurisdictions) will have to make decisions about each individual site. A determination will have to be made regarding which sites are the most important in each coverage area, which sites are built because of capacity demands, and which sites, if they failed, would not impact other sites within the surrounding area. As new sites are added to the network over time and fill-in sites are constructed improving coverage and capacity, they should meet as many of these requirements as possible.

Even sites which meet these PSG best practices and requirements may not withstand the extraordinary natural or manmade disasters. Therefore FirstNet must take steps to provide temporary network components that can be deployed into an area to replace or augment the failed sites. These temporary network components will not, in most cases meet PSG requirements but will be able to restore minimal communications in a given area until such time as the PSG sites can be restored to full operation.

The best practices and requirements provided in this document are intended to address the steps necessary to make a communication site highly available, even in the event of a disaster. They are intended to capture the typical efforts of public safety network builders to "harden" their communication sites with the objective of achieving this high level of service availability. However, the PSG requirements listed below are not, today, met by all existing public safety LMR sites. Some sites may have constraints that prevent them from achieving these objectives or they may have been constructed prior to the availability of the best practices referenced in this document. It is then a goal of the Task Group that local jurisdictions will follow these requirements when constructing new sites or retrofitting existing sites.

PSG networks are imperative to the continuing ability of the public safety community to communicate at all times. The more robust the network, the more redundancy built into the network, the better it will serve public safety and the better public safety will serve the public in times of both routine incidents and major disasters.

## 1.1 Purpose

This report defines Public Safety Grade (PSG) primarily for use by FirstNet to guide the design and implementation of the NPSBN so the network can accommodate mission critical communications. This report should also be of value to public safety agencies that implement their own LMR systems.

Qualitatively, we define PSG communications simply as the effect of reliable and resilient characteristics of a communications system. The system should be designed to minimize the impact of, or eliminate entirely, equipment or component failures that result in a loss of data throughput or coverage, and be designed in a manner that promotes the system's quick return to optimal performance.

This report seeks to further define the phrase "Public Safety Grade" and to provide measurable characteristics which would differentiate a mission critical communications system from a standard or commercial grade network.

## 1.2 Background

The report covers environmental considerations, service level agreements, reliability and resiliency, coverage, push-to-talk, applications, site hardening, installation, and operations and maintenance. A network or system intended to support mission critical communications and to be considered PSG must address these topics in design and implementation.

The report topics are generally presented in two parts which include a definition and description section and then a listing of best practices. The best practices recommend abbreviated requirements to be considered in the design and implementation of the NPSBN to mitigate those risks.

The PSG Task Group decided to be as comprehensive as possible in listing the best practices.

The use of the words **SHALL** and **SHOULD** are defined below:

- **SHALL**: Best practices that include the word **SHALL** are recommended as mandatory requirements. Adherence to all **SHALL** requirements makes the system PSG compliant.
- **SHOULD**: Best practices that include the word **SHOULD** are optional requirements. They generally indicate areas whereby, if applied, would result in a more robust solution. However, the NPSBN builder will need to factor these requirements against their cost to assess their applicability for any component of the system.

Because this report is so comprehensive, the writers recognize that not every best practice can be followed in all cases for all subsystems in the network. However, the designers and operators of the NPSBN should adhere to the vast majority of the recommendations in order for the network to be considered Public Safety Grade. When economic, environmental, and technology tradeoffs need to occur, FirstNet should consult with the user agencies that will be impacted by the tradeoff. These situations should be reflected in the Service Level Agreement (SLA) between FirstNet and the user agencies.

### 1.2.1 Environmental Considerations Introduction

The environmental considerations section is primarily included to point out risks to the system that can cause outages when the system is most needed to support emergency responder operations. These risks were also considered and addressed by best practices in other sections. The environmental risks were compiled from the collective experiences of the PSG Task Group and all the risks listed have caused failures to public safety communications systems in the past.

### 1.2.2 Service Level Agreements Introduction

For the NPSBN to be successful as a PSG system, user expectations must match the realities of the NPSBN system implementation. No system has ever met 100 percent of every users expectations. The best way to set realistic expectations for the system is through the creation of a Service Level Agreement (SLA). The SLA section defines recommended components of a PSG SLA document. This section is referred to in several of the other sections where precise common best practices cannot be specified for a PSG definition.

### 1.2.3 Reliability and Resiliency Introduction

Reliability and resiliency of the NPSBN are critical to users accepting the NPSBN as a PSG network that can support their mission critical communications needs. The *NPSTC Launch Statement of Requirements (700 MHz Launch SOR)* document refers to the importance of reliability and resiliency in the following statement.

> *Various requirements in this document refer to Public Safety Grade (PSG). While the meaning of this terminology was not defined at the time of this document's completion, the NPSTC Broadband Working Group (BBWG) plans to define the terminology as quickly as possible, for use by FirstNet in system design. For now, the intent of the PSG terminology is to convey the need for design choices that support a greater overall network reliability and resiliency to network disruptions compared to commercial networks.*

The importance of the NPSBN network to be reliable and to be resilient to failures caused by manmade or natural disasters cannot be over stressed.

### 1.2.4 Coverage Introduction

Coverage for public safety communications systems is always a design topic that requires careful consideration and user buy in through a common understanding of expected system performance. Any existing trust relationship is at risk if emergency responders find that the system coverage does not initially meet their needs. Lack of coverage can directly result in loss of life. The PSG Task Group is very aware that 100 percent geographical coverage is too costly to achieve. Therefore the coverage definition and best practices in this section define coverage by measurement. The designers of the NPSBN must define areas they will cover including the type (indoor/outdoor or other) and then measure and document that coverage or lack of coverage as part of a SLA document.

### 1.2.5 Push-to-Talk Introduction

PSG Push-to-Talk (PSG PTT) has performance specifications and definitions that are necessary for mission critical public safety operations. These performance specifications are consistent with or exceed existing PTT communications capabilities that have been identified as critical to public safety operations. The specifications determined for PSG PTT are the result of years of public safety operations and are intended to meet today's expectations in the utilization of tomorrow's technology.

### 1.2.6 Applications Introduction

Because the NPSBN is a data network, PSG data applications will be vitally important to the users. his section defines what makes an application PSG. This section is not intended to address how to program or code an application. t is recognized that further work is needed in this area and that there is not a large amount of publically available research and documentation on public safety data applications.

### 1.2.7 Sites Introduction

Hardening of sites to prevent failure is one of the most critical elements in the construction of a reliable and resilient communications system. This section covers the majority of all systems and infrastructure at a site, including power, security, site hardening, electronics, and other elements. This section was developed by the Association of Public Safety Communications Officials – International (APCO's) Broadband Committee through a working group identified in Appendix B. APCO has expressed interest in the creation of an American National Standards

Institute (ANSI) standard involving site hardening to provide a single source document for use by emergency responder agencies working with broadband or LMR systems.

### 1.2.8 Installation Considerations Introduction

Appropriate installation practices for PSG equipment also contributes to a reliable communications system. For example, incorrect application of weather proofing on coax or waveguide connectors will result in a system failure during a storm (when the PSG system is busy and most needed by emergency responders). This section defines a number of different installation requirements.

### 1.2.9 Operations and Maintenance Introduction

Operations and maintenance occurs following the construction of any system and is critically important to insure reliability of public safety systems. Proven operations and maintenance practices that result in a reliable system are documented in this section.

## 2 Risk Factors and Analysis

There are many risk factors, including dozens of environmental conditions discussed in the next section, which must be taken into account during the design, procurement, installation, and maintenance phases of a PSG system.

When considering the impact of non-functioning communications systems, one must consider the complexities of these systems from the original point of a signal, which could be voice, data, or video, to the end user on the scene of an incident. These complexities may include the need to overcome challenges presented by architectural features and energy delivery systems, communications infrastructure, and computer hardware and software. They can also include a variety of impacts on the end user's equipment on the scene, and the ability to communicate effectively.

As the complexity and design of these systems increases, so do the number of potential failure points, and therefore the potential for failure. There is an increased reliance on cyberspace included in many system designs, which then increases the exposure to potential cyber attacks. These cyber threats are difficult to anticipate; therefore requiring credentialing, authentication, and verification of user's identities and their level of access. Because the NPSBN is a nationwide interconnected network, network security is of paramount importance.

Device operating system evolution means that devices and applications may have different operating systems, and even different versions of those systems, on different devices. This may

cause the devices to become unstable and therefore unusable. One of the many concerns of using more heavily IP-based devices is automatic software updates received by devices while they are in use at the scene of an incident. These updates, if not managed properly, may cause delays in transmitting mission critical information. Heavy usage of devices that rely on applications and other accessories has a significant impact on both the battery life of equipment and the available bandwidth for those devices.

A driver's attention may be diverted by mobile devices while operating a vehicle, which not only puts the operator of the vehicle in danger, but everything in the path of that vehicle as well. Ergonomics and controls that require little or no visual contact are imperative. LCD screens are designed to be viewed directly [e.g., with a straight line of sight], is a concern because mobile devices are almost never positioned directly in front of the driver. Photo sensors that automatically dim displays on these devices can be fooled into dimming the screen's image while inside the vehicle, even though the level of exterior ambient sunlight remains the same.

The intrusion of animals, plants, and foreign substances into sites and vehicles has been shown to have detrimental effects on electronics and other infrastructure. While most communication facilities are built to resist their presence, over time intrusion may occur and create problems with system performance. Animals chew wiring, build nests, and deposit excrement in and around equipment that can have corrosive effects. Vegetation may cause problems to sites resulting in equipment failure and/or security concerns. Environmental factors such as dust, heat, moisture, and salt-laden air are problematic for electronics.

The rise in demand for greater capability, interoperability, and coverage, and the corresponding rise in user expectations for speed, power, and ease of use, has led to a parallel rise in risk to communications systems from natural phenomena, operational error, and planned attack. As these factors impact directly on field user safety, response speed, and success, these factors must be considered when planning these systems.

Some of the most serious risks are derived from environmental conditions that are typically classified as natural disasters including earthquakes, fires, floods, wind, and ice. These all present the potential for system degradation or failure. Similarly, many public safety jurisdictions have geographical areas which include harsh environmental conditions that push systems operations capability to the extreme, not only in terms of temperature, but also in terms of elevation, terrain, and meteorology.

Public safety agencies are constantly improving their systems in response to the ever changing threat, while respecting considerations of training, availability, utility, and fiscal responsibility.

At the same time the goal of maximizing and leveraging these continuing improvements into current technologies which provide services that support our missions remains to prevent, protect against, mitigate, provide a response to, and help recover from the many threats that arrive on our doorsteps, sometimes without warning.

# 3 Environmental Events[1]

Environmental events must be considered during the design, construction, and ongoing operations of a PSG system. There are many variations that must be addressed to ensure that the system can withstand situations which may be local or regional in nature. Depending on their location, some facilities and sites must guard against flooding and earthquakes but not against freezing ice storms. Other areas might require protection from tornado force winds. Each geographic area should be considered unique.

The information contained in this environmental events chapter was developed by APCO as a component of their Site Hardening Best Practices document.

Environmental risk factors are grouped into seven specific "force of nature" threat categories that may compromise the sustainability of a mission critical communications network. The following section identifies and explains the risk factors, analyzes the nature of the risk, and provides recommendations to manage the risk. The section is organized by event type. Each event includes the impact to communication sites as well as recommendations to protect against the event. These recommendations are captured as best practices in the requirements section that follows.

## 3.1 Seismic Events

Seismic events include earthquakes and related events, including mudslides and landslides caused by natural or manmade circumstances.

### 3.1.1 Seismic Events Analysis:

Historically, the risk of earthquakes has been tied to geographical areas, typically California. In the last few years, earthquakes have also struck and impacted other areas of the country, well beyond California. Not all earthquakes are created the same. Much of the damage potential from earthquakes to communication network facilities and equipment can be gauged by the type of soil the network installation rests on. Soil compaction may positively or negatively affect how a facility and equipment "rides out" the event.

[1] NPSTC wishes to acknowledge the work of the APCO Broadband Committee for assistance in the creation of this section.

Ground shaking is the most common hazard of earthquakes. Violent shaking, along with asymmetrical settling of soil beneath a communication structure, can cause an otherwise sturdy structure to be damaged or destroyed. Buildings or radio towers located near a fault are subject to the effects of ground displacement. Ground displacement occurs when soil "tears" causing the ground to move in a different direction on either side of the fault. Buildings or towers built upon a fault can easily be destroyed during a seismic event. The San Andreas Fault Line, which runs through a large part of California, and the New Madrid Fault Line which bisects the states of Illinois, Indiana, Missouri, Arkansas, Kentucky, and Mississippi, are both capable of producing significant magnitude earthquakes and ground displacement.

In recent times, a threat similar to earthquakes, but much more localized has been experienced in the southeast portion of the country. Sinkholes, or areas where unstable land had depressed or shifted in some way, would be a network threat both to buildings, towers, and utility connections. Sinkholes are a specific example of a greater phenomenon known as soil liquefaction. Soil liquefaction occurs when previously stable soil becomes fluid, often as a result of vibrations caused by earthquakes. The risk of liquefaction is more probable on sandy type soil which resides over a high water table. Soil liquefaction may be correlated as a result of an earthquake, but there are also examples of liquefaction occurring outside of a seismic event. Virtually every major earthquake includes liquefaction. Earthen dams and buildings built over reclaimed land would be at a higher risk for damage or destruction resulting from liquefaction.

### 3.1.2 Seismic Event Recommendations:

The potential for network damage, destruction, or interruption resulting from earth movement can be managed, and thus the site hardened through a two-part process. First, a network designer needs to evaluate the site location and quantify the overall risk of an earthquake or soil liquefaction at that location, along with understanding the potential intensity of land movement that may be encountered during an event. Resources to complete this analysis include United States Geological Survey (USGS) seismic charts, soil composition, and stability studies, along with an understanding of prior land uses at that site. The second part of the process is to employ facility construction and equipment installation processes that will allow the network installation some level of resiliency against the potential damage of seismic motion. These measures may include upsizing of structural members that are subject to shearing forces, the use of base isolation techniques, or a minor adjustment in site location to take advantage of more stable soil. Typically, local building codes in areas with a high likelihood of seismic activity will require protection against earthquakes. However, recent events have shown that areas outside the active seismic areas are also susceptible and should be considered.

## 3.2 Wild Land Fires

Wild land fires are those that typically burn in remote areas with forested or grassy regions. These fires are typically fast moving and may be fed by high winds which can disrupt electric transmission lines. This section will not address network hardening to offset the danger of conventional structural fires or exposure to adjacent burning buildings.

### 3.2.1 Wild Land Fires Analysis:

Wild land fires happen not only in forest areas, but also in the urban interface transition areas. Urban interface areas form the boundaries between the primitive forests and more developed or improved populated areas. Wild land fires represent a threat to site equipment buildings, outdoor equipment cabinets, and, to a degree, radio towers. While it stands to reason that network components in direct contact with flames is a major threat to network survivability, the indirect heat transfer from a closely burning fire is equally hazardous to network survivability. Wild land fires frequently are fast moving, very hot, and will burn anything that is made of combustible materials. An example of heat damage is from the 2003 Old Fire in the San Bernardino National Forest--an automobile caught in the fire had the aluminum engine block completely melted. In the same fire, LMR site buildings with wood frame roof and composite roofing shingles had the entire roof burned causing damage to the equipment housed inside in addition to the building itself. A few years later, during a wild land fire in 2009 burning in Los Angeles County, a public safety site burned because it had an older building made of combustible material. The building had been covered in foam with a fire barrier but winter ice damage had exposed the wood in the building's roof. This allowed embers to gather and collect, and then ignite the rooftop and burn the building sometime after the fire had passed by. Wild land fires can pose a serious risk to communications sites and to outdoor equipment not housed in shelters. Communications buildings and shelters provide an extra layer of protection, in some cases sacrificial, to prevent damage from direct fire impingement or radiant heat transfer.

Terrain can also play a large role in influencing the damage potential of a wild land fire. Site installations at the top of a canyon—especially in line with the canyon floor—will be subject to some of the greatest heating potential as a fire progresses up a canyon from a lower elevation. This heat can actually melt radio tower feed lines and antenna systems. Prevailing winds can also influence a wild land fire's direction of travel. Lastly the concentration of vegetation and its proximity to a communications site is also a factor that can place a network at risk.

### 3.2.2 Wild Land Fire Recommendations:

The threat of a wild land fire can be managed through a combination of calculated siting, the utilization of fire resistive construction materials and techniques, and development and implementation of a plan for proactive site area maintenance. Site locations must be chosen with respect for natural fire behavior in a given area. Fire protection experts with a localized knowledge base can be consulted to analyze and rank the relative fire safety of a particular location. Site options where heat may be focused or burning debris may transit are best avoided. Site location options with easy vehicular ingress and egress, close to fire roads, are a desirable attribute. A site with a nearby water supply is also highly beneficial. Firefighters triage areas that are within or threatened by a burning wildfire, and will favor protecting buildings and structures that offer the maximum return on their firefighting efforts while minimizing the risk to their personal safety.

Site structures must be constructed with an emphasis on their resistivity to damage from direct and indirect heating. Buildings constructed in areas with a high likelihood for wild land fire threats must be constructed using non-combustible and self-extinguishing materials to provide maximum protection from heat. Techniques or protective measures need to be considered and employed to prevent the fire from "extending" into the building on combustible cabling or antenna feed line jackets or sheathing. Architectural features that will better shield the building from the collection of heat and embers should be a high priority in network site development. Steel towers, while likely able to survive heating, play host to rather fragile network appliances such as antennas or microwave dishes, feed lines, and sometimes outdoor radio equipment that is attached to the tower. Plumes of radiant heat or blowing embers can easily melt items and equipment on towers, rendering them useless at the onset of fire encroachment. Any active radio equipment mounted on tower structures should be protected from heat damage from a fire that burns over the installation.

Equipment housed in outside cabinets must be protected from heat to minimize damage if the cabinet and site are burned over. Only metal non-combustible tower structures should be used. Wooden poles should not be used for a mission critical installation. A routine schedule of preventative site maintenance should be developed and kept as a high priority in site operation. Site maintenance tactics can begin with pre-emergent weed and brush control. Scheduled brush clearance and removal of debris from the site can occur at regular intervals. A periodic inspection of building safety features should also be on a site maintenance schedule. While local regulation may differ, a basic standard is to remove and haul away combustible materials for a minimum distance of 30 feet around a structure. As noted in the State of Idaho's National Fire Protection Association (NFPA) 1144 Wildfire Checklist, reducing fuel from 30 to

100 feet away from the structure provides additional protection during a wildfire.[2] These practices lead to a communications installation that is highly defendable during a wild land fire threat.

## 3.3 Flooding

Flooding risks stemming from unwanted or uncontrolled water intrusion caused by natural or manmade events that create a barrier to sustained network operations.

### 3.3.1 Flooding Analysis:

Floods are caused when more water flows through the hydrological system than can be absorbed or drawn off through natural process including absorption and evaporation. The hydrological system is the continuous cycle of evaporation of the ocean waters that create rain and eventual drainage back into the ocean.

Quantities of rain exceeding more than 1 inch per hour will begin to cause pooling of water, which may eventually lead to flooding. Flooding is categorized into five different types, generally correlating to where the flood is physically occurring. The types of flooding are flash floods, coastal floods, urban floods, river floods, and ponding. Flash floods are terrain driven and would be prevalent in areas of steep slopes that rapidly concentrate and funnel water and debris along a natural drainage path. Coastal floods occur when the sea, typically from a hurricane's storm surge, distributes the water inland, beyond the typical shoreline. Urban floods occur in developed areas, resulting from natural causes such as poor drainage after a heavy rain or from manmade circumstances such as a damaged water main or a failed water pumping or draining system. River floods occur when rivers or lakes overflow their boundaries and flood the surrounding area. Finally, ponding floods result from extended rainfall over relatively flat land that cannot dissipate the water fast enough. This type of flooding is limited to very shallow water depths, such as an inch or so.

Flooding can interrupt service from a communications facility from the obvious effect of water inundation that causes equipment malfunction or destruction, to less obvious causes such a power grid or fiber transport systems interruption caused by flooded conduits and switch boxes. In severe floods, buildings can be washed away by the force and speed of the water current. Similarly, structural foundations for buildings or radio towers can be undercut by moving water which may cause the foundation to erode or lose its stability, ultimately leading to a massive foundation failure and building/tower collapse.

[2] State of Idaho, NFPA 1144 Wildfire Checklist, http://www.idl.idaho.gov/nat_fire_plan/county_wui_plans/boise/appendix_b.pdf

Flooding may also cause communications sites to become inaccessible for an extended period of time, making it difficult to impossible for personnel to reach the site and conduct repairs or service emergency power generators. Flooding is ultimately a self-limiting phenomenon. Floodwaters will recede, be absorbed, or evaporate. A good quantity of historical flood information has been collected across the United States. Historical flooding trends, coupled with Doppler radar tracking of storms, allows virtually street-by-street monitoring of storms and their intensity of flood-caused damage. A transient weather pattern known as El Nino periodically affects the southwest and southeast portions of the United States. During times of El Nino, very wet winters can be expected in these regions of the country. Urban flooding may result from higher rainfall over developed areas during El Nino weather activity.

### 3.3.2 Flooding Recommendations:

Protecting high importance network facilities and equipment begins first with proper siting of the network node. Avoiding areas of with a history of flooding activity is certainly the best way to protect a communications installation from flood damage. Seeking assistance from local hydrological experts and other knowledgeable sources can identify areas that may have flooded on a prior occasion. These same resources, along with historical flooding records or estimates of probable flood areas can assist with evaluating the relative risk of flood impact on a specific parcel of land. Areas that may be more susceptible to flood water accumulation may have a lower land elevation than the surrounding grade. Areas that are highly developed or improved, such as areas with a proliferation of cement and pavement that seals the ground from absorbing and dissipating water can also be at a higher risk for flood accumulation and damage and thus might want to be avoided. Site locations or terrain that does not allow gravity to drain runoff, or that requires mechanical pumping action to remove water accumulations should be avoided as well.

As a more direct means of protecting a communications network installation from flood damage or water intrusion, architectural and civil features such as installing deeper footings or piers, elevating the building or tower foundation significantly above grade, or installing drainage features such as culverts or water bars that surround the location may be feasible. In flood prone areas the object of flood management is to isolate the installation from the rapidly rising flood water and enable the water drainage to move away from the improvement at a speed or intensity that will not damage the structures.

When evaluating the possibility of flood damage to a communications site and network, the concept of generational floods, for lack of a more descriptive term, is important to understand. Irregular or rare flooding events are known as 50-, 100-, or even 500-year flooding events. These events will produce a magnitude of flood and damage much higher than what can be

expected compared to a typical flood profile in a particular area. The important concept is to realize the interval of generational flooding events is random. It is very possible to have a devastating 100-year flood 2 years in a row. Furthermore, it is likely that 100-year flooding will occur somewhere in the United States in any one year but there is no way to predict where.

## 3.4 Wind Events

Wind events, for the purpose of this document, are classified as abnormally high wind speeds within a given area. Common causes of the increased wind speeds can be attributed to storms, such as a tornado or hurricane, or temperature gradients produced where high pressure and low pressure converges and creates wind. The influence of terrain and temperature difference, such as found in mountainous areas or along coastal areas, can all produce wind speeds that can accelerate the potential for compromise or damage to a network facility.

### 3.4.1 Wind Events Analysis:

The impact of wind on network facilities needs to be thought of and analyzed with three general types of wind: long duration, squalls, and gusts. Each of these winds can affect the stability of network operations in different ways.

Long duration winds are those types of winds and speeds that occur over an extended or up to a nearly continuous period of time. Long duration winds can range in intensity from gentle breezes to devastating hurricanes. Squalls are winds that last for several minutes and can be expected during thunder and hail storms, and are found within tornados. Squalls are responsible for wind shear, where accompanying up and downdrafts can subject small geographical areas to extreme wind velocities. Gusts are very short duration winds. The American Meteorological Society (AMS) defines a wind gust as a sudden brief increase in the speed of the wind.

Wind events of any speed may ultimately create a negative impact on a network facility or component. These can be through direct impacts such as broken or twisted antenna equipment on towers or failed rooftops on buildings, or, for example, indirect or consequential damage caused by a tree blowing over onto a building or tower and causing damage. Another indirect impact of long duration winds can be the erosive damage of exposed equipment caused by the frequent blowing of sand or debris. Amplified wind speeds found in squalls or gusts may stress the structural capability of antennas and dishes including their mounts, transmission lines, or even the tower itself. The effects of these conditions may result in service interruption caused by a loss of antenna alignment all the way to a tower member failure or outright collapse. Long duration winds, even at velocities that are not reasonably believed to be cause damage, can set

up mechanical oscillations or vibrations that can cause equipment on the tower, including the tower proper, to become loose or mechanically unstable. Exaggerated wind speeds caused by squalls or gusts, or more broadly, hurricanes and tornados, obviously pose a lethal threat to a communications network installation. The Enhanced Fujita Scale[3] matches wind speed against the intensity of damage. Wind speeds greater than 65 MPH are predicted to cause minor damage to structures. When 166 MPH wind speeds are realized, extreme damage results, with total structural destruction occurring at 200 MPH.

The Federal Emergency Management Agency (FEMA) denotes four wind speed zones in the United States, ranging from 130 to 250 MPH.[4] FEMA predicts the strongest winds in the mid-United States. Wind speeds are influenced not only by weather, but also terrain. Wind speeds increase as wind travels through narrowing terrain, especially as they travel downhill. In California, regional down canyon winds known as Santa Ana or Sundowners develop in response to seasonal climatic changes. The National Weather Service (NWS) defines these winds as strong down slope winds that blow through the mountain passes. These winds easily exceed 40 MPH. In December 2011, Santa Ana wind speeds in the Mammoth Mountain area of California were measured at 150 MPH.[5] It is important to realize the potential of localized wind events and how they can be detrimental to network operations.

### 3.4.2 Wind Events Recommendations:

Protecting a network installation from the effects of strong winds begins with developing an estimate of the probable wind velocity then building in a safety measure to allow the installation to survive a significantly larger wind velocity. The American National Safety Institute, in the Telecommunications Industry Association (TIA)-222 standard, provides a basic wind speed as a starting point in radio tower engineering.[6] Due diligence in this matter also requires an analysis of terrain and topography as variable factors to further develop the maximum wind potential. Local meteorological experts can be of great assistance in developing "spot" prediction for wind speed.

Moving beyond statistical velocity predictions, actual site location will measure largely in securing a communications installation from damaging winds. An awareness of what might fall

[3] Stormfax Weather Almanac, Enhanced Fujita Tornado Scale (EF scale), http://www.stormfax.com/fujitaenhanced.thm
[4] FEMA, Wind Zones in the United States, http://www.fema.gov/safe-rooms/wind-zones-united-states
[5] Matt Stevens, "Santa Ana Winds: Gusts top 150 mph at Mammoth Mountain", Los Angeles Times, December 2, 2011 (http://latimesblogs.latimes.com/lanow/2011/12/wind-gusts-top-150-miles-per-hour-at-mammoth-mountain.html
[6] Rohn Products, Understanding TIA-222 – Revision G, http://www.rohnnet.com/resourcesmodule/download_resource/id/610/

on the installation or be blown into it, either during a gust or over an extended period of time is of value. This includes being cognizant of nearby trees, power poles, or other buildings that could fail in some way and damage the communications site. Communications installations located on mountain ridge tops or at the base of canyons can be expected to sustain more exposure to higher speed winds than a site in a flat area. Communications installations along the Gulf Coast and in the Tornado Alley areas of the United States will require more structural hardening than required in most other areas. Antennas and other equipment chosen for radio tower installation must be mechanically acceptable for the chosen level of wind resistance. Supplemental bracing and anchoring may be required to insure tower and attachment survivability during an extreme wind event. Buildings will need to employ architectural and structural features that will lower their resistance to wind and allow impacts from flying debris while minimizing damage. Building features that trap wind should not be allowed. Extremely strong winds can create positive and negative pressure differentials within a building and the structure must be able to manage these differences without losing integrity or failing. The potential for the extra damage of driving wind accompanied by rain or hail must also be considered when developing communications sites that must be resilient to natural forces.

## 3.5 Ice Storms

Ice storms include freezing conditions as well as precipitation of frozen hail.

### 3.5.1 Ice Storms Analysis:

Ice storms can negatively impact network reliability and sustainability through several different courses. An ice storm can affect both urban and rural areas alike. Predictions are for at least one major ice storm a year in the continental United States. While freezing rain and the resulting ice storm can occur anywhere, generally the Northeast and Midwest areas of the country are more likely to produce an event.

Ice storms are created by rain that falls when the temperature is below freezing. When the rain hits the ground, trees, power lines, or radio towers, it immediately freezes. Ice storms occur when a convergence of warm and moist air from a higher altitude releases its moisture through lower level, yet freezing air, which cools the rain. When the rain hits any objects that are already at or below a freezing temperature, it immediately forms ice on the object. Over time, this ice will build a thick coating, adding a significant amount of mass and weight to the object.

The thick coating of ice can be detrimental to communication site installations in a number of ways. The ice can create difficulties in accessing the site due to dangerous road and travel conditions, especially in mountain sites.

Power line spans that carry ice may break and fall, interrupting power to the site. Besides a loss of power to the installation, there remains a formidable personnel safety issue due to exposed wires on the ground.

Closer to the site, trees or limbs that have accumulated ice may strain and break under the added weight, fall, and damage equipment or power lines. Depending upon the communications network site location, standing water around the building or tower may have frozen, making it dangerous to traverse.

On the site facility itself, gates and locks may be frozen in position, preventing immediate access and requiring a thawing process to make them operable once again. The feed lines and antennas on a radio tower, in addition to the radio tower itself, will also harbor ice attachment. Ice forming on antenna systems may seriously disrupt the radiation pattern, causing poor radio coverage in otherwise acceptable radio signal coverage areas. The extra weight of the ice can cause the antenna mounts, and sometimes even the tower en masse to fail, causing a catastrophic network outage.

As tower ice begins to release, falling ice can be of sufficient weight and velocity to damage antennas, feed lines, and even building rooftops when it impacts those objects. Damage to feed lines and antenna equipment can render the installation useless until repairs are completed.

### 3.5.2 Ice Storms Recommendations:

As with most environmental catastrophes, there is no way to prevent an occurrence. Efforts must be aimed at protecting the communications network installation from the effects of ice storms by proactively working to configure the facility to avoid the consequential damage of freezing rain.

At ground level, sites should have proper drainage to avoid pools of frozen drainage water. Site managers should consider techniques to insure site or building access is available in a frozen environment. Building entrances and gates should be located on southern exposures, and combination locks should be favored over keyed locks that may be frozen deep within ice. Network facilities including buildings and radio towers should be located so that ice-laden trees will not fall on facility equipment. It may be appropriate to consider specifying trees and vegetation that are resistant to ice storm damage. Where practical, power lines should be routed underground to better protect them from the elements from the point of demarcation with the utility provider.

Radio towers must be constructed to accommodate the icing without impact to their strength or load carrying capacity. Tower attachments including antennas and feed lines must be

properly secured to tower members for assured survivability. Towers must be engineered to protect attached components by deflecting and dispersing falling ice. Towers must also be placed or sited with consideration given to spacing between other buildings so that falling ice does not unnecessarily impact adjacent facilities. While often taken for granted, proper weatherproofing of electrical components on a tower must be insured to prevent water intrusion resulting in signal loss or damage from expanding ice. In geographical regions that are known to be impacted by ice storms, the use of heated antenna or microwave dish assemblies as a means to prevent the formation of ice and thus preserving radiated signal characteristics may be considered.

The ongoing ability to access network sites in ice prone regions is a consideration. It is frequently necessary, especially in mountainous areas, to utilize specialized equipment access and enter a frozen site. Resources such as road graders, snow cats, and, in some instances, helicopters will be required to transport personnel and equipment to the site for emergency repairs. Utilizing standing, in-place agreements to access this type of specialized equipment on a prioritized basis is an important consideration.

## 3.6 Grid Failures

Power outages stem from loss of primary commercial electrical power.

### 3.6.1 Grid Failures Analysis:

The electrical service for a network site is served by the local electrical utility through aerial or underground transmission lines that connect back into a series of higher voltage lines, electrical substations, and, ultimately, all the way back to an electrical power generating facility such as a hydroelectric plant, a wind farm, nuclear plant, or a conventional fired steam generating plant. The term grid is a subjective descriptor. It does not necessarily imply an order of fault tolerance or redundancy. Redundancy occurs when the aerial or underground transmission lines have the ability to be switched over to and then be fed from a different substation. This level redundancy protects more against a substation failure, as opposed to a transmission line failure. A grid failure, or better described as an outage affecting multiple customers, can be the result of weather, excessive power demand, or electrical utility equipment failure. A grid failure can also be caused by an accident or sabotage that damages the electrical service network.

Protecting a network installation requires a strategy that does not rely on grid or electrical network power to sustain operations. The loss of grid power, especially after damaging weather, can last beyond hours into days and weeks.

### 3.6.2 Grid Failure Recommendations:

The potential impact of grid failures on network installations are best managed by insuring a source of redundant power is available with sufficient endurance to remain operational until normal grid operation is restored. Most grid outages will be unexpected. In some cases grid outages may be scheduled and pre-announced when they are a necessary part of electrical network construction or during times when load shedding is forecasted to occur as a management tactic during periods of extreme demand.

Assuring that critical network sites maintain an adequate battery supply and emergency power generating equipment is vitally important as the first step in protection. Depending on the criticality of the facility, a site location that affords electrical service from multiple substations will provide a higher level of redundancy. Frequently electrical utility companies maintain notification lists for their mission critical or high consumption customers. Operators of critical facilities are well served by insuring that they receive such information and can implement response procedures in the event of a predicted or actual grid failure or outage. Extended grid failures will tax emergency power backup systems.

Competition for refueling services and emergency mechanical experts to repair a failed generator or switch gear system can be expected to be high in an impacted area. Multiple days of operational sustainability relying only on fuel stored on site is recommended to manage the risk of network outage resulting from refueling delays. Redundant generators may be indicated for high operational priority sites. Selecting generator fuel options that best match product that is locally and readily available and easy and safe to transport is recommended. In this instance, transporting liquefied propane into a wildfire area might present a greater hazard than transporting diesel to refuel a generator. The ability to preconfigure a network site to allow the connection of trailer-mounted, portable generators as a tertiary power option can provide value to a network operator.

## 3.7 Geographical Specific Events

This is an open-ended topic and is ultimately defined by localized situations and conditions, but is designed to note very specific risks to networks that might include the risk of extreme temperatures, caustic atmospheric conditions, and radio frequency emissions that exceed regulatory exposure levels.

### 3.7.1 Geographical Specific Events Analysis:

Certain network installations may be located in areas where there are extremely high or low temperature extremes. An example of these types of locations are high-elevation mountains,

especially in the Rocky Mountain areas where blizzards are commonplace, and where sub-freezing temperatures nearing -70 degrees Fahrenheit may be experienced, and, conversely, extremely hot areas, such as areas in the Sonoran desert in the states of California and Arizona, where temperatures can exceed 125 degrees. Extreme temperature environments will stress the ability of a building and its climatic control systems to provide a stable temperature to support proper network equipment operation.

There are also locations where the site soil is rich with chemicals or may be more acidic than most areas, to the point that the air tends to be corrosive. Areas where the mining of earth materials occurs may exhibit this condition. While the corrosive environment is not a threat to humans, network equipment installed and operated in that environment—both in buildings and on radio towers—risk early failure due to damage from the destructive forces of corrosion.

A survey of the local environment should be conducted to identify and assess the risk from other geographical specific events that might be present.

### 3.7.2 Geographical Specific Events Recommendations:

Ensuring network survivability in extremely hot or cold climates centers relies on insulating the electronic equipment from temperature extremes. A combination of a well-insulated building and redundant climate control equipment is required to ensure a properly regulated environmental temperature in network equipment rooms. Thermally specified construction materials and the use of heat reflecting or heat absorbing building colors can help in controlling building temperatures.

Frequently, radio communications installations are physically co-located with other like installations. Each installation that emits radio signals will contribute a share to the ambient RF signal level as measured on radio towers, within buildings, and around the exterior areas used for vehicular parking and work staging points. The Federal Communications Commission (FCC), through their Office of Engineering and Technology (OET), in Bulletin OET-65, have set forth a scale of maximum RF signal level that both professionals and the general public may be legally exposed to.[7] Absent the impractical solution of turning an entire communications site complex off for servicing, site locations exceeding these maximum levels require a site-specific plan to allow safe occupancy of the site by service and support personnel or they may impact the feasibility of adding more wireless transmissions to a site altogether.

[7] FCC, Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields, http://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65.pdf

### 3.7.3 Overriding Personnel Considerations:

A network failure caused by environmental events inevitably places technical personnel in a position of elevated risk during their response to and while working to correct the failure. It is important to identify the risk to personnel and then define and implement an appropriate risk management plan to ensure a high margin of safety during these low frequency, high-risk responses. In the event of a network failure or outage during or after an environmental event, technical or support personnel may need to enter an area that others are in the process of, or have already vacated to benefit their own safety. A multitude of hazards will likely exist, and an orientation to and understanding of those hazards needs to be communicated to maximize personnel safety and security.

# 4 Service Level Agreements

This section will describe the role and importance of service level agreements.

## 4.1 Description

A service level agreement (SLA) is a contract between two or more parties, usually a provider and one or more customers, that specifies in measureable terms what commodities or intangible commodities the provider provides to the customer in return for money or other considerations, and at what levels.

For the NPSBN, the services provided will include wireless connectivity to mobile and fixed devices, applications, the devices themselves, management, and operations. The customers will be public safety agencies, local and state governments, federal agencies, and private companies who respond to incidents and disasters.

The levels specified in the agreements may include measures of availability, speed, geographic coverage, and other specifications. In the NPSBN, the initial SLAs will likely be specified using the design required under Title VI of the Spectrum Act[8] for each of the 56 states and territories as part of the state operations plan.[9]

Most SLAs require regular reporting of service levels against the measures specified in the SLA. In commercial contracts there are usually penalties for non-compliance with service levels. The

[8] Middle Class Tax Relief and Job Creation Act of 2012, Public Law 112-96, February 22, 2012, Section 6302, http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

[9] Presentation by FirstNet General Manager Bill D'Agostino and Deputy General Manager T. J. Kennedy to the FirstNet State Points of Contact, January, 2014, slide 25 - http://www.ntia.doc.gov/files/ntia/publications/140115-spoc_webinar_slides.pdf

penalties can be monetary or credit for services rendered and may allow the customer to terminate the agreement.

SLAs are important because they allow the provider (e.g., the NPSBN) to construct, operate, and price its network to achieve the service levels specified in the agreement. SLAs allow the customer (e.g., public safety agencies) to have dependable network services and therefore properly provide public safety services to the citizens and constituents in their service area.

## 4.2 Best Practices

These are the SLA best practices guidelines for the NPSBN to be considered public safety grade.

| | |
|---|---|
| 1. | The NPSBN **SHALL** provide a draft service level agreement in the operations plan presented to each state.[10] |
| 2. | The SLA **SHALL** specify coverage area, availability, reliability, resiliency, and other specifications to measure the services provided by the NPSBN. The SLA **SHALL** include reporting of significant NPSBN outages affecting the customer state or local jurisdiction. |
| 3. | The SLA **SHALL** specify the management services provided by the NPSBN which will allow for local Public Safety Enterprise Network (PSEN) provisioning of devices, applications and services, and local management of features such as the priority of applications, users and devices. |
| 4. | The NPSBN **SHALL** provide regular reports and measurements of the specifications of the SLA with each state. |
| 5. | The SLA **SHOULD** provide descriptions and measurements of other service levels as required or recommended elsewhere in this document. |

# 5 Reliability and Resiliency

## 5.1 Description – Reliability

Reliability is the probability of the NPSBN completing its predefined function during a specified period of time. The NPSBN is further defined as resources or systems include supporting backhaul, data systems/centers, and the supporting connectivity infrastructure and their redundancies. It also includes the operating systems, software, and firmware used by these systems, as well as physical buildings, and sufficient power sources to sustain mission critical equipment. Redundancies are an integral part of public safety communications systems, and

[10] As required by the Spectrum Act: http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf, Section 126 STAT. 213

therefore are required to ensure the wholeness of the definition of reliability. Redundancies may be passive and/or active as the need demands.

Any complex system will have component failures. For the network to be considered a mission critical data communications system for emergency responders, the system must not suffer loss of service availability due to single point failures. Single point failures may cause, on a local geographical basis, some degradation of data throughput as long as that degradation does not prevent essential data communications for the emergency responders. Any failures must be repaired in the shortest possible time to restore normal operations and ensure that additional failures do not cause further degradation to the network. To be considered mission critical, there is an expectation that system coverage and availability is not lost and that limited data losses do not impact mission critical systems.

In a public safety LMR radio system N+1 redundant base station radios are used so that a failure of a single base station radio does not cause total loss of coverage. However, there may be some loss of a voice quality equivalent to degradation of LMR data throughput in the described scenario.

Many of today's public safety LMR radio networks are built to provide a 99.999 probability of service **availability** for a local geographical area. Various system design elements are used to create this performance standard. They include redundant radio base stations, the use of self-healing microwave and fiber networks, backup power supplies, and automatic fail over to redundant critical components.

As an example, Motorola designs equipment such that it has a very low failure rate consistent with system design to 99.999% up time. This is not intended to endorse Motorola products, only to show the design methods of an LMR vendor.

> Six Sigma Quality
>
> A performance standard developed by Motorola and adopted by several other companies to describe a high level of quality. Statistically, it means six standard deviations from a desired result. Allowing for some variation in the mean, this translates into a defect rate of 3.4 parts per million for each and every process step or procedure. That's 99.9997 percent perfect. This is an effective measurement tool which can be applied to both product and services deliverables. It is Motorola's principal measurement for Quality Assurance verification.
>
> The 5-Nines is a corporate-wide initiative to drive 99.999% availability (no more than 5 minutes total downtime per year) as the telephony standard for all Motorola wireless

> systems. By measuring and analyzing data, we are well on the way to improving existing processes to assure that 5 Nines is available within all aspects of our organization. This ensures that customers will receive the highest reliability possible within the industry.

Another example of design to five-nines availability is the new City of Houston 700 MHz LMR system. The City of Houston's 700 MHz trunked radio network includes both five-nines and six-nines availability for specific critical infrastructure:

> 5.2.2J Microwave System Design. Where rings are planned, each ring shall be designed for a minimum of 99.9999% availability.
>
> 5.2.3C All paths in the system, including rings and spurs, shall be designed for a minimum one-way path reliability of 99.9999% per year using the Vigants model in TIA TSB-10.
>
> 5.2.3E All paths in the 11 and 18 GHz band and any band where rain outage is a significant factor, shall be designed for a minimum rain availability of 99.995% per year, using the parameters and methods of ITU-R Rec. P.530-11[11]

The City of Houston document also provides additional quantitative measurement of the systems required coverage reliability:

> Coverage Reliability
>
> 3.1.1D All references to coverage reliability in this document refer to area reliability. For example, the phrase "95% coverage" indicates that 95% of the bounded areas described shall exhibit the specified coverage resulting in a DAQ 3.4 at least 95% of the time. It will not be acceptable to provide a design where two or more adjacent failed grids exist, that is, failed points shall not be unique to any one vicinity, while still meeting the overall coverage reliability goals.

These LMR design elements mean that a single failure will not reduce service availability but may have a limited impact on voice and data throughput.

These limited examples are intended to show that public safety entities design LMR systems to five-nines system availability. This same availability will be needed in the FirstNet system to meet user expectations.

[11] https://www.itu.int/rec/R-REC-P.530-15-201309-I/en

It is recognized that the design and functionality of the FirstNet LTE network will be significantly different that the LMR systems in use today. **This report does not provide guidance on how availability should be measured in an LTE environment.**

- However, public safety would expect the equivalent of five-nines service availability performance from the FirstNet system to match what it receives from its LMR systems today. This is an especially important issue if mission critical voice is to be eventually carried on the FirstNet system.

Therefore, for the NPSBN as a whole, "five nines" reliability as defined for current LMR operations is not the appropriate metric for FirstNet LTE deployment. After careful consideration, this report recommends that FirstNet develop an ability to quantify and report the service level availability and reliability metrics that are being considered for the network. This information will be of critical importance during the state consultation process.

When examining the entire nationwide network as a single system, consideration should be given to the use of a 98 % reliability per year factor for any type of failure. By this it is meant that failures of any individual component are counted as down time, even if that component failure did not result in a system outage. Those failures must be repaired so that the total outage time for components of the NPSBN of no more than 2 percent per year. The intent of this recommendation is to include that measure of risk exposure which occurs during component failures even though the failure did not impact the public safety network. For example, the failure of an emergency generator would be considered a down time incident even if the emergency generator was not needed during the period it was out of service. Regularly scheduled downtime for maintenance activities do not count toward this calculation.

Public safety places a high priority on the operational readiness of redundant or backup equipment as a mandatory ingredient for a mission critical system designation. Redundant equipment must be maintained to the highest state of readiness to insure mission objectives can always be met. Any time a redundant or backup system is not available or has failed outright should be accounted for in the NPSBN's aggregate outage time, regardless of whether the non-availability or failure resulted in a loss of network performance.

An example to illustrate the above is when a backup generator did not start during a routine test. This failure to start would be counted as an outage, even if there was commercial power present and no requirement for generator power at the time of the test.

It is therefore recommended that the best practices of all the sections in this report are considered and followed to the extent possible. It must be recognized that there are unique

environmental, geographical and operational circumstances affecting every public safety agency that prevent a "one size fits all solution" approach.

- Specific service availability for any given jurisdiction will be defined in the SLA between FirstNet and the public safety entity.

In summary, it is not enough to specify an availability number of 99.999%. The measurement of what constitutes availability is also needed. That effort was beyond the scope of the Writing Team and requires highly specialized knowledge of LTE system infrastructure and operations.

- FirstNet will need to define how the availability is measured and applied to each state through an SLA. For example, there may need to be different measurement criteria for urban, suburban and rural areas.
- We recommend more study to be done to examine how public safety LMR systems meet the 99.999% availability criteria and how this translates to measuring availability in a LTE environment.

## 5.2 Description – Resiliency

Resiliency is the ability of the NPSBN to withstand a disruption to the network that would result in loss of coverage and the ability to recover from any such outage within a minimum period of time. The level of response and service can be interpreted differently by agencies. Service response times **SHALL** be defined in a SLA with the PSEN. Resiliency will be built into the system by following the best practices recommended throughout this report.

Deployable systems are a vital component of public safety LMR systems and will be necessary for the NPSBN. When all else fails despite the best design practice and maintenance procedures, deployable resources and off network direct communications are the last resort for emergency responders to maintain essential communications.

## 5.3 Best Practices – Reliability & Resiliency

| | |
|---|---|
| 6. | Every environment event identified in Section 3 **SHALL** be considered when designing the NPSBN. |
| 7. | NPSBN resiliency is achieved by following the best practices in this report, including, if not already defined:<br>• The ability of the NPSBN to continue to function as designed in the event of any circumstances of an all-hazards definition, **SHALL** include: natural disaster, power disruption/loss, directed and/or deliberate attack, and hazmat situations.<br>• In the event of a component failure/system outage, The NPSBN **SHALL** be restored to full functionality as designed, in the minimum possible time. |

| | |
|---|---|
| 8. | Sufficient support personnel **SHALL** be available to respond 24 hours a day, 7 days a week, to any NPSBN failure or outage to meet the response time requirements of the service level requirement. |
| 9. | The NPSBN **SHALL** be designated for federal level restoration priority in incorporating the FCC standards outlined in "CFR-2012, Title47, Volume 3, Part64, Appendix A (TSP)" which outline the programs for "Telecommunications Service Priority." |
| 10. | To ensure deployable systems are able to meet the standards outlined in this document, they **SHALL** be tested monthly and scheduled for maintenance on an appropriate recurring basis. |
| 11. | Deployable resources **SHALL** connect to the existing NPSBN, or, in the event that is not possible, it **SHALL** be deployed in a stand-alone, local area mode. |
| 12. | If deployable resources are part of the redundancy architecture design of the NPSBN, the maximum distance of deployment **SHALL** be calculated into the restoration timelines for NETWORK as described in the previous sections of this document. |

# 6 Coverage

## 6.1 Description

Public Safety Grade coverage differs from commercial coverage. Commercial coverage concentrates coverage (and capacity) where the most demand for service is. This may leave some areas with no coverage (a dead spot) which may be acceptable as customers don't use the service enough to complain and force the commercial company to extend coverage to those dead spots. Public safety agencies however always try to cover 100 percent of their jurisdiction area. While it is not economically possible and extremely hard technically to cover 100 percent of any given large geographical area, public safety systems strive to minimize any large dead spots much more than commercial systems do. They must cover all areas that generate requests for service. Also some areas such as a large high rise or other critical facility may need coverage even if it requires extra cost to provide that coverage.

Coverage is also defined by grade of service. For example, public safety LMR systems generally define their acceptable coverage are as those areas have signal strength high enough provide a Delivered Audio Quality (DAQ) level of 3.4.[12] Any area with a DAQ of less than 3.4 is not considered to be covered. For the data network coverage to be considered acceptable, a minimum data throughput must be specified.

[12] "Reference TIA TSB -88."

This section is not intended to direct the decision of what areas to cover or how to design that coverage. Those coverage decisions will be made during state consultations negotiated by FirstNet with each state and will be incorporated into the SLA. This section is intended to emphasize that when the decision is made to provide coverage that it is done via mutual agreement between FirstNet and each state. Critical buildings or infrastructure **SHOULD** be considered in the design and the agency consulted and made aware of dead spots.

LTE coverage modeling and verification for a public safety system is challenging because of the dynamic nature of the emergency response system. The level of detail required to fully define the parameters and procedures is beyond the scope of this document. This document provides a high-level set of best practices for an envisioned LTE coverage modeling and verification procedure along with representative design parameters. However, additional work across various industry stakeholders is required to fully define the envisioned procedure. An LTE task group has been formed within TIA TR8.18 (Wireless Systems Compatibility - Interference and Coverage) to work on the recommended detailed parameters and procedures.

Public safety users face challenges in the use of communications equipment. In some cases firefighters and law enforcement personnel need to focus on their immediate environment and cannot devote their attention to their communication device. This results in the user device being placed on the body in areas that may cause poor transmission and reception of RF signals. An example of this with current voice portable equipment would be the case where the portable is located on a belt near the waist of the user. This equipment placement must be accounted for in determining system coverage.

## 6.2 Best Practices - LTE Coverage Modeling and Verification

The proposed LTE coverage modeling and verification procedure builds upon the well-established recommendations defined in the TIA TSB–88 series of documents. Specific values are derived from the SLA negotiations defined in Section 5.1.

The key attributes of the procedures are as follows:

| | |
|---|---|
| 13. | The coverage modeling approach **SHALL** be consistent with the coverage verification approach. |
| 14. | The LTE coverage design criterion **SHALL** meet a minimum acceptable user data rate at a prescribed Service Area Reliability. |
| 15. | The coverage design **SHALL** be performed at a specific traffic load level. |
| 16. | The coverage model **SHALL** consider calls for service and incident locations based upon the experience of public safety agencies operating in that geography. |
| 17. | The coverage model **SHALL** consider sensitive and critical infrastructure such as |

| | |
|---|---|
| | schools, shopping malls, event venues, transportation corridors, and other infrastructure which may be subject to major public safety incidents or terrorist attacks. |
| 18. | The coverage model **SHALL** consider UE placement on the body of the user, |

NOTE: Additional details must be specified to create a useful and unambiguous coverage design procedure including defining data rate (i.e., application layer or physical layer, data rate averaging time, etc.), detailed definition of Service Area Reliability, and traffic loading procedures.

The LTE Coverage Verification criterion **SHALL** be defined as follows:

| | |
|---|---|
| 19. | Measured using a data rate, which is consistent with the coverage design criterion in the SLA. |
| 20. | Define a geographic grid of test tiles covering the prescribed service area. |
| 21. | Configure system parameters to emulate design traffic load. |
| 22. | Measure data rate in each tile and compare the measured data rate to the design data rate to determine if the tile is passing or failing. |
| 23. | Calculate the measured Service Area Reliability from the measured tile data rate success and failure results. |

Additional details must be specified to create a useful and unambiguous coverage verification procedure including defining traffic load emulation procedures, procedures for determining the number of test tiles needed to obtain statistically significant measurement results, and procedures for measuring data rate within a given geographic test tile (i.e., duration of throughput measurement and measurement location within test tile).

# 7 Push-To-Talk (PTT)

## 7.1 Description

The concept of PSG drives those design choices that result in emergency responders being able to maintain their ability to communicate, as necessary, during mission critical incidents. PSG is the result of implementation techniques typically used or required by public safety entities to achieve the level of reliability and resiliency required to support mission critical activities. NPSTC has previously published a PTT over LTE document detailing many of these issues.

Public Safety Grade also refers to the core best practices, definitions, performance specifications, and the general and feature best practices characteristics necessary for mission critical public safety operations.

PSG when applied to a public safety service or function (such as PTT) should focus upon what differentiates that service from a similar type commercial network supported service. This shall be an attempt to qualitatively define some elements of the PSG PTT service offering. (The underlying assumption is that the NPSBN supporting this service has its PSG elements defined in other appropriate PSG categories.)

In defining PSG definitions, no intent lays herein to impose these specific network solutions on the NPSBN network. We seek to assist in educating manufacturers and vendors, as to the requirements of the public safety community. The intent is for the NPSBN services to be equivalent in reliability and resiliency to public safety LMR communications systems and specifications that are inherent in supporting law enforcement, fire, and EMS operations, commonly referred to as mission critical systems. The specifications determined for PSG PTT are the result of years of public safety operations and are intended to meet today's expectations in the utilization of tomorrow's technology.

The following table illustrates the time intervals which occur when a P25 unit transmits a message, when another unit receives the message, and when a third unit enters the conversation late. The best practice statements which follow the diagram are intended to reflect maximum time intervals for these activities in order to ensure that a mission critical voice message is communicated as quickly as possible.

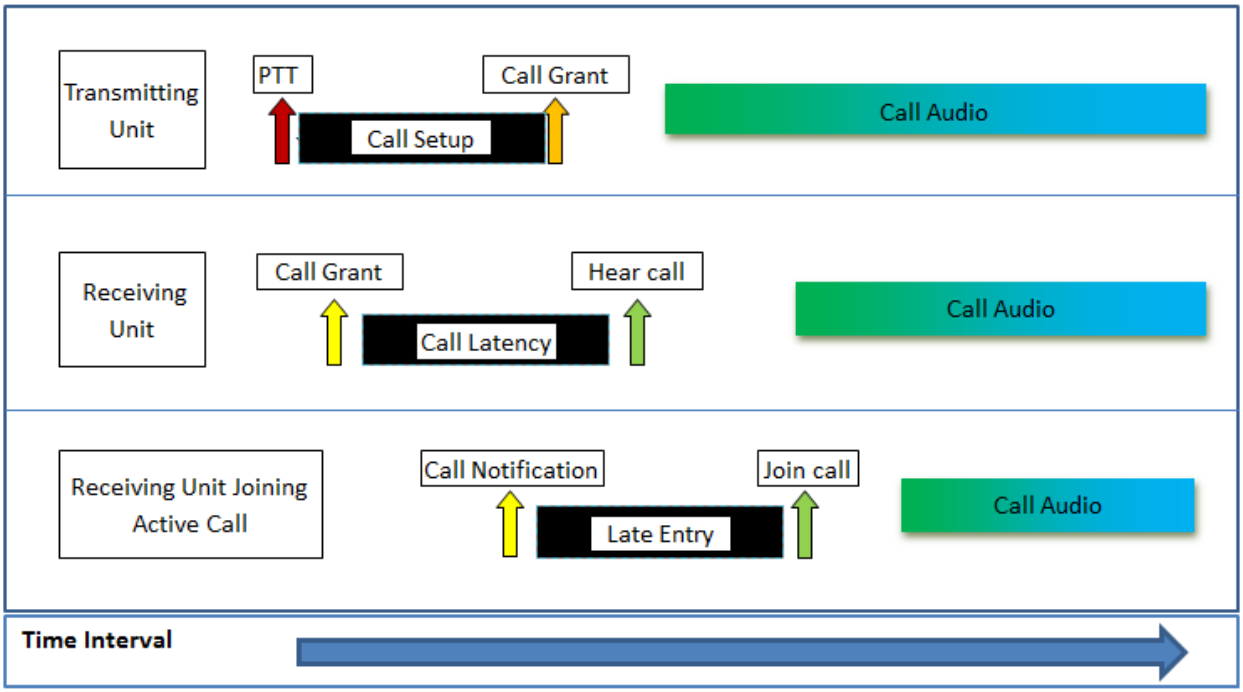



Figure 1: **Diagram of Call time periods**

## 7.2 Best Practices

### 7.2.1 Core Best Practices

| | |
|---|---|
| 24. | Call Setup-Call setup time for group calls and private calls **SHALL** be a maximum of 500 milliseconds but **SHOULD** be no greater than 300 milliseconds when operating "on network" within the NPSBN.[13] This does not include Late Entry (see below). Timing delays are based on a "normal scenario" for pre-registered, on-network LTE devices (no relaying) in a non-roaming scenario with unencrypted voice and no audio transcoding. Call setup is defined as the time from PTT control activation to the time the user is "granted the floor" and can start speaking with no loss of audio. |
| 25. | The call set up time reliability for registered, on-network LTE devices **SHOULD** be 99.9% under uncongested conditions, in a non-roaming scenario. |
| 26. | Call "Mouth to Ear" latency **SHALL** be a maximum of 500 milliseconds but **SHOULD** be no greater than 300 milliseconds when operating "on network" within the NPSBN. Certain configurations of UEs operating "off network" and utilizing relay functionality between UEs back to LTE eNodeB may exceed these values under certain circumstances. Latency is defined as time between an utterance by the talker, and the physical playback of the utterance at the listener's device's speaker after the call has established.[14] |
| 27. | Late Entry-The time associated with late call entry **SHALL** not exceed 150 milliseconds (unencrypted) and 540 milliseconds (encrypted). Late Entry is defined as the time from when the PTT application receives notification of a communication of interest, to when audio from that communication is heard by the user. |
| 28. | Voice Quality-Processing of audio at the source device **SHALL** achieve an average MOS-LQO (Mean Opinion Score-Listening Quality Objective) of no less than 2.7. MOS-LQO scores are the result of the Perceptual Objective Listening Quality Analysis (POLQA), a next generation voice quality testing standard. |
| 29. | Noise Reduction-Processing of audio at the source device **SHALL** minimally achieve the same noise reduction performance as specified in the P25 Vocoder. This does not imply that the P25 vocoder must be used; only that the minimum performance of the vocoder must be equal to or greater than the P25 standard[15] in TIA-102.BABG Table 3-1. |
| 30. | Initial Lost Audio-This is defined as the portion of the talker's utterance that is lost at the beginning of the voice transmission after the user is granted permission to speak |

[13] This performance specification applies to unconfirmed calls. Unconfirmed calls do not attempt to guarantee that required system resources are in place prior to starting the call which would ensure that participants will be able to receive the voice.

[14] This performance specification applies to unconfirmed calls. Unconfirmed calls do not attempt to guarantee that required system resources are in place prior to starting the call which would ensure that participants will be able to receive the voice.

[15] See TIA-102.BABG for P25 performance standards. The TIA standard is not used for LTE vocoders and is noted here for reference only to the required minimum performance level.

| | |
|---|---|
| | by the PTT service. This value **SHALL** be zero milliseconds maximum. |
| 31. | Trailing Lost Audio-This is defined as the portion of the talker's utterance that is lost at the end of the voice transmission after the user is granted permission to speak by the PTT service. This value **SHALL** be zero milliseconds maximum. |
| 32. | Off Network Device-Operationally, User Equipment (UE) off network device functionality and range **SHALL** minimally emulate the performance of a portable unit in the 700 MHz band using the Project 25 standard. (The current accepted standard for public safety communications).[16] |

### 7.2.2 General and Feature Best Practices

| | |
|---|---|
| 33. | High Availability: The application is redundant and **SHOULD** not fail. |
| 34. | The NPSBN **SHALL** maintain synchronization of events, such as emergency activations from UE devices, when the network recovers from an outage. |
| 35. | All public safety UE **SHALL** have device-to-device off network PTT capability.[17] |
| 36. | The NPSBN **SHALL** allow for local management control of certain features and functionality which include, but are not limited to, local control of call participation, security, mission plan, fleet maps, and priority.[18] |
| 37. | The NPSBN **SHALL** provide prioritization mechanisms to all call types, including Immediate Peril and Emergency. |
| 38. | PTT services **SHALL** be authenticated in real-time (e.g., only certain authenticated users can initiate a System Wide Call; only authorized users can cancel group emergencies. In other words, registration-authentication does not allow access to all features.) [19] |
| 39. | The NPSBN **SHALL** support Call setup acknowledgement, as required. |
| 40. | The NPSBN **SHALL** support Emergency calls (which cannot fail, are not dropped, or preempted. |
| 41. | Identities of users in Emergency and Imminent Peril conditions are known by authorized public safety users. |
| 42. | Ruthless and top-of-queue preemption **SHALL** be supported by the NPSBN.[20] |
| 43. | The NPSBN **SHALL** allow local control to set the criteria for cancelling/terminating Emergency Calls/Conditions. [21] |

[16] See NPSTC Push to Talk over LTE Document, Section 7.2, Table 18, Requirements #4 and #5.
[17] See NPSTC Report on Push to Talk over LTE, Section 7.1, Table 17, #4.
[18] See NPSTC document on Broadband Local Control.
[19] See NPSTC document on PTT over LTE, Section 5.2, Table 11, Requirements #1 and #2.
[20] See NPSTC document, PTT over LTE, Section 4.1, Table 8, #1 and #2.
[21] See NPSTC document, PTT over LTE, Section 4.2, Table 9, Requirement #5.

| | |
|---|---|
| 44. | Group communications **SHALL** be afforded an appropriate priority level on the NPSBN which **SHALL** not drop individuals but may drop the entire call if necessary based on network conditions. The network **SHALL** not allow the dropping of a participant from a group call in order to ensure delivery of critical messages to all members of the group. |

# 8 Applications

The primary goal of this document is to detail guidelines for developers and administrators of applications that will operate on the NPSBN.

This document is not intended to be a Statement of Requirements (SoR) for broadband applications, but rather to outline some of the associated risks and best practices that should be followed when developing and/or administering these applications.

The applications-related topics covered in this document are:

- Actionable information
- Availability
- Common data model
- Human-centered interface
- Interoperability
- Operability
- Performance
- Resiliency
- Scalability, adaptability, and portability
- Security and information assurance
- Updates
- Verification and certification

## 8.1 Actionable information

### 8.1.1 Description

Actionable Information is data that can be used by the end user to fulfill their mission. In order to provide actionable information, the application must have access to data of interest and understand the user's situational context. An outcome of providing actionable information is that the user's situational awareness is increased, enabling the user to better fulfill their mission.

### 8.1.2 Best Practices

| | |
|---|---|
| 45. | PSG applications **SHOULD** be able to turn data into actionable information and intelligence in real time, and not burden the user with unnecessary need to sort through data. |
| 46. | Applications **SHOULD** be able to analyze potentially enormous volumes and varieties of continuous data streams to provide decision makers with critical information in near real time. |
| 47. | Applications **SHOULD** include ad hoc analysis, along with easy-to-understand reports to support it, and can drive actionable intelligence and response for all aspects of incident management within and among public safety agencies. |
| 48. | Applications **SHOULD** be able to cache all the retrieved information for a defined period of time. It should be noted that varying degrees of data retention may be necessary depending on the device and the application. This mechanism minimizes queries towards the database and to keep consistency. |
| 49. | PSG applications **SHALL** be provided accurate situational awareness information. |
| 50. | The application **SHOULD** assemble data from various and disparate sources into relevant information for actionable intelligence. |

## 8.2 Availability

### 8.2.1 Description

The NPSBN services and applications need to be ready to serve the needs of the public safety users at all times. Availability is the ability of the public safety community to obtain their required services and applications in all places the public safety community needs to operate. A public safety user considers a service or application to be unavailable whenever they cannot access it or whenever they cannot retrieve or update the desired information in a timely fashion.

### 8.2.2 Best Practices

The following best practices **SHALL**:

| | |
|---|---|
| 51. | Utilize the best practices and procedures for high availability commercial systems. |
| 52. | Implement applications on multiple geographically dispersed servers with automatic rerouting among the servers. |
| 53. | Utilize measurements, statistics, MOS-LQO (Mean Opinion Score-Listening Quality Objective, and Service Level Agreements (SLAs) to monitor and report availability. |
| 54. | Implement critical databases in a fault tolerant manner (e.g., data mirroring, cloud services, abstraction). |

| | |
|---|---|
| 55. | Design for graceful degradation of PSG application with loss of network support capabilities (e.g., a version of useful functionality still available as user moves off of the NPSBN). |
| 56. | Employ techniques such as clustering to reduce application unplanned (fault) downtime. |
| 57. | Employ techniques such as rolling upgrade to reduce planned downtimes. |
| 58. | Isolate PSG applications from non-PSG applications (e.g., separate servers, database managers). |

## 8.3 Common Data Model

### 8.3.1 Definition

A data model (sometimes referred to as a schema) defines the relationships between different data entities within a particular environment, thus establishing the context within which those entities have meaning. Data models can be associated with a single database or span multiple databases.

A "common" data model spans a set of applications and data sources used by a public safety organization. It defines the data relationships and definitions that exist within the public safety organization. This tends to be far from simple to build and so standard data models are not typical.

Generally, a common data model defines the terminology that a public safety agency uses for all of its data sources and the relationships that exist between different data items. Other agency's applications and data views can be mapped to the common data model so that, in effect, the common data model provides a bridge between the different definitions associated with each of the other agency applications. Thus the common data model enables data interoperability between applications. The model should incorporate industry best practices, implementing a layered structure supporting data abstraction that is commonly found in well written systems and applications.

### 8.3.2 Best Practices

| | |
|---|---|
| 59. | The NPSBN **SHALL** have a vetting process to approve all Application Programming Interfaces (APIs). |
| 60. | Databases and data structures **SHALL** have an open API to allow for bi-directional data interoperability as authorized by the PSEN administrator. |
| 61. | As authorized by law, data sharing **SHOULD** be encouraged through the use of common data servers warehousing the data for extraction by authorized users independent of their current location or affiliation. |

| | |
|---|---|
| 62. | Common data model development **SHOULD** include provisions for updating data types and terminology, to allow for adaptability in the future. |
| 63. | NPSBN applications **SHOULD** use industry models available from standards bodies as a guide to developing a common data model. |
| 64. | The NIEM (National Information Exchange Model) **SHOULD** be used[22] during development of the technical layer. |
| 65. | The OASIS model **SHOULD** be used[23] during development of the technical layer. |
| 66. | The Multilateral Interoperability Programme (MIP) Information Model **SHOULD** be used during development of the Semantic layer.[24] |
| 67. | The Universal Core standard **SHOULD** be used during development of the Semantic[25] layer. |
| 68. | The TM Forum – Business Process Framework **SHOULD** be used during development of the Organizational Layer.[26] |

These models allow incorporation of industry best practices, implementing a layered structure supporting data abstraction that is commonly found in well-written systems and applications.

## 8.4 Human-Centered Interface

### 8.4.1 Description

Human-Centered Design is an engineering approach that considers the needs of the end users of the application during the entire product development process. It is fundamentally concerned with understanding the user's context (especially their situational needs) and providing a solution that satisfies fundamental user needs. An outcome of following human-centered design principles is a user interface that is simple and intuitive that meets the user need without distracting them from their mission.

### 8.4.2 Best Practices

| | |
|---|---|
| 69. | The user experience for applications **SHALL** be intuitive. |
| 70. | There **SHOULD** be a Style Guide that establishes a foundation for a common look and feel. |
| 71. | The application development environment **SHOULD** provide a software developer kit that offers a framework for developing public safety applications that includes standard symbology and practices. |

[22] https://www.niem.gov/Pages/default.aspx
[23] https://www.oasis-open.org/
[24] https://mipsite.lsec.dnd.ca/Pages/Default.aspx
[25] https://metadata.ces.mil/ucore/index.html
[26] https://www.tmforum.org/BusinessProcessFramework/1647/home.html

| | |
|---|---|
| 72. | PSG applications **SHOULD** not require extensive training of end users. |
| 73. | PSG applications **SHALL** provide inline contextual help where appropriate. |

## 8.5 Interoperability

### 8.5.1 Description

With respect to public safety communications, the National Incident Management System (NIMS) defines interoperability as "the ability of systems, personnel, and equipment to provide and receive functionality, data, information, and/or services to and from other systems, personnel, and equipment between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together. In addition, it allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real time, when needed, and when authorized."

Additionally, an application should provide operational compatibility with other applications at the API level with backward compatibility.

### 8.5.2 Best Practices

| | |
|---|---|
| 74. | Applications and user meta data **SHALL** adhere to relevant open industry standards that provide for interoperability at the protocol level. NPSBN shall publish an open standards-based API for its applications. |
| 75. | PSG applications and database structure interfaces **SHALL** be tested by the NPSBN in order to demonstrate interoperability with other applications. Applications and database structure interfaces **SHALL** be backward compatible. |
| 76. | There **SHALL** be an "App Store" operated by the NPSBN. |
| 77. | Local PSEN applications **SHALL** be supported on the NPSBN. These local applications may be stored on the NPSBN or on authorized regional or local PSENs as defined by an SLA. |
| 78. | The NPSBN **SHALL** establish a working group to address conflicts in standards, implementations, APIs, and enhancements. |

## 8.6 Operability

### 8.6.1 Description

Operability is defined as the ability of the emergency responder to establish and sustain voice and data communications in support of mission operations.

If the day-to-day operation of the application is not easily understood or difficult to execute, the application will not be used very often and its value to the public safety community diminishes. If an application is not used routinely there cannot be the necessary user familiarity developed and associated user trust in the application results, and this will likely not be a resource that the public safety user can call upon when an emergency incident is occurring. Failure to familiarize on the use of the application can result in miscommunication or misinterpretation of information, compounding a mission critical situation, including risk to life and property.

### 8.6.2 Best Practices

| | |
|---|---|
| 79. | Application operability **SHOULD** be consistent and intuitive, and applications should be easy to install and launch as authorized. |
| 80. | Applications **SHOULD** be able to initiate and maintain reliable communications with other devices/accessories, as applicable, with minimal strain on battery life. |
| 81. | The use of advertisements **SHALL** be prohibited. |
| 82. | There **SHALL** be the ability for FirstNet and the local PSEN to disable or remove their application and associated data. |

## 8.7 Performance

### 8.7.1 Description

Application performance is defined as how an application performs on a client device. Performance would include the responsiveness or speed of an application as realized by the end user, impacts to the UE's battery life, and consumption of NPSBN bandwidth. Application performance must be at a level to serve the needs of the public safety community at all times. Applications that are too slow or "time-out," limit UE battery life, and burden NPSBN bandwidth will be deemed unsuitable by the public safety community. Likewise, an application which repeatedly polls the network and is designed to continuously use bandwidth to verify its online health is also unsuitable for public safety use.

### 8.7.2 Best Practices

Performance of an application is tightly coupled to the capabilities of the user devices. Therefore, some level of minimum device specifications should be stated for application developers to utilize in designing and achieving performance goals.

| | |
|---|---|
| 83. | The NPSBN **SHALL** utilize industry application analysis best practices and application optimizer tools to evaluate the performance of public safety applications. |
| 84. | The NPSBN **SHALL** ensure that all applications are tested to certify conformance with the appropriate NPSBN behavior and performance policies. |

| | |
|---|---|
| 85. | The NPSBN **SHALL** certify UE devices that are authorized to operate on the network. |

## 8.8 Resiliency

### 8.8.1 Description

The Department of Homeland Security (DHS) defines resiliency as the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The mobile environment of the UE is constantly changing. This changing environment could be due to various aspects such as degradation of the local signaling environment, NPSBN congestion, server faults, or other faults. The changing mobile environment could adversely affect the functionality delivered by the application.

While much of this changing condition of the mobile environment is a result of movement of the public safety user's UE, many of these issues may not even be related to actual movement of the public safety user and can affect even the stationary mobile user. For example:

- The cell/sector on which the public safety user is currently affiliated may become overloaded with other user activity demands, potentially reducing the portion of bandwidth available to this user, or reducing the application priority in the NPSBN and thus affecting the potential application functionality.
- The public safety user device may be redirected to another cell/sector due to issues with the current cell/sector, but this new cell/sector has reduced capability, again potentially affecting the potential application functionality.
- A network application server or database becomes unavailable or access becomes bottlenecked.

In a wireless broadband system, resiliency would be the capability of the application to adjust to the changing conditions to continue to provide useful functionality to the public safety user.

### 8.8.2 Best Practices

| | |
|---|---|
| 86. | Applications **SHOULD** be designed to provide maximum operation when connected to the NPSBN offering reliable service. Likewise, when the application is connected to a network with degraded service (i.e., low, lossy, or otherwise challenged bandwidth), there should be some degraded capability that can restore fully when the network recovers. |
| 87. | The application **SHOULD** offer at least some level of operational functionality when off |

| | |
|---|---|
| | NPSBN. |
| 88. | If an application does not intrinsically need NPSBN access or information from the network to fulfill its function, then such applications **SHOULD** provide full operation on and off network equally). |
| 89. | An application designed to work off of the NPSBN **SHOULD** not be hindered in operation when the device is connected to a network. |
| 90. | An application that can function without constant NPSBN access **SHOULD** incorporate a "thick" client at the subscriber device to retain functionality for the user when not connected to the network. |
| 91. | An application that needs NPSTBN support to provide desired functionality **SHOULD** incorporate a "thin" client at the subscriber device to support improved performance and ease of portability. |
| 92. | The application **SHOULD** support graceful performance fall back appropriate to the current NPSBN capacity. |
| 93. | The application **SHOULD** use whatever NPSBN capacity is available and capable of supporting needed operations. |
| 94. | Roaming from the NPSBN to another network **SHOULD** be as seamless as possible, and not interrupt the application's operation. |
| 95. | Users **SHALL** receive explicit notification of degraded application operational conditions. |
| 96. | The application **SHOULD** be able to handle session interruption events without terminating functionality, resuming operation from point of interruption. |

## 8.9 Scalability, Adaptability, and Portability

### 8.9.1 Description

**Adaptability** is the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions.

**Portability** of radio technologies, protocols, and frequencies among emergency management/response personnel will allow for the successful and efficient integration, transport, and deployment of communications systems when necessary. Portability includes the standardized assignment of radio channels across jurisdictions, which allows responders to participate in an incident outside their jurisdiction and still use familiar equipment.

**Scalability** differs from portability in that scalability allows responders to increase the number of users on a system, while portability facilitates the interaction of systems that are normally distinct.

In the public safety application environment these attributes are critical for operational efficiency and mission success.

For example:

- Application optimizes the user experience when operating on a 13" screen or a 4" screen, and adjusts to the devices keyboard/data entry capability. *[Adaptability]*
- When a responder moves from an in-vehicle device to a portable device they require the data to be synchronized between the devices. *[Portability]*
- An incident requires a large number of users each accessing the same application at the same time, without having performance impact to the application being used. *[Scalability*]
- Scalability/Portability/Adaptability for public safety applications can be defined as the ability to optimally adjust to user demand and user device capability to consistently provide actionable information to the user when needed.

### 8.9.2 Best Practices

General public safety impact:

| | |
|---|---|
| 97. | All APIs **SHALL** be open and well documented. |
| 98. | Mobile and desktop applications **SHALL** be able to use the same application database structure. |
| 99. | The application **SHALL** scale to the number of active users without degrading the application functionality to the users. |

## 8.10 Security and Information Assurance

### 8.10.1 Description

DHS defines security from a context of critical infrastructure and resilience. Security shall reduce the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

Applications on the NPSBN need to be secured such that access to the application is controlled, the data used by an application is protected from being inadvertently shared outside of the application, and the application itself is certified and verified to be uncorrupted.

When it comes to data that can be shared, logged, or created by an application on the NPSBN, security is paramount to ensure the protection of that data. Additionally, users must have trust that the data they transmit or receive is secure, and that the integrity of that data has not been compromised during production, capture, or transmission.

Data security and the assurance of information, in the realm of applications, refers to all elements in which the public safety application uses application-level security protocols,

interfaces with network-based security protocols, and ensures all data transmissions are properly verified and tagged.

### 8.10.2 Best Practices

| | |
|---|---|
| 100. | The NPSBN **SHOULD** define specific requirements for hardware based security. |
| 101. | An authentication process **SHOULD** be used (such as an Identity Management System) to verify a user's credentials, so they may access authorized applications. |
| 102. | Authenticated users **SHOULD** have access to all authorized applications resident on the UE without further explicit application sign-on (except those outside the NPSBN requiring additional input). |
| 103. | NPSBN **SHOULD** accommodate multi-level evidentiary standards. Additionally the applications need to follow state/local guidelines on where data can be transmitted. |
| 104. | NPSBN applications **SHOULD** provide a logging and auditing capability for any additions, deletions, and updates to support non-repudiation. |
| 105. | The NPSBN **SHOULD** use industry standard practices to validate application and UE security postures against policies at relevant intervals. |
| 106. | The application **SHOULD** provide automatic tamper-resistant relevant tagging (e.g. device ID, timestamp, geo-location) of captured information on UE. |
| 107. | The NPSBN **SHALL** apply access control measures to applications attempting to access network services and databases. |
| 108. | The NPSBN **SHALL** support secure distinct user profiles. |
| 109. | Public safety applications **SHOULD** be isolated from any non-public safety applications. |

## 8.11 Verification and Certification

### 8.11.1 Description

Verification and certification refer to those activities conducted by the NPSBN or other delegated entities, which independently confirm and warrant that the equipment, applications, and operating systems used on the public safety network are those designed or and authorized for the NPSBN.

In order for the public safety community to be able to meet their primary mission, the public safety community must be able to trust the applications on their UEs. Verification and certification are part of the mechanism for providing application trust for the public safety community. Verification and certification provide the public safety community with a level of confidence that their applications are valid and not detrimental. Tasks associated with this involve testing the application performance on user devices and the NPSBN to ensure performance and that there is no adverse impact to the overall system of introducing the

application into the ecosystem. This includes the code inspection and verification, so that no malicious or unintended source code exists that could later harm the NPSBN.

NOTE: A "user rating" of an application are not part of the verification and certification processes. However, application user ratings may assist the public safety users in selecting which application best meets their needs.

### 8.11.2 Best Practices

The following best practices **SHALL** be followed:

| | |
|---|---|
| 110. | Adherence to Industry best practices for verification and certification of applications **SHALL** occur. |
| 111. | Federal government best practices for verification and certification of applications, including any best practices defined by the National Institute of Standards and Technology (NIST) and DHS **SHALL** be followed. |
| 112. | A test environment **SHALL** be used to evaluate applications prior to public safety use. |
| 113. | Applications **SHALL** be verified as not harmful by utilizing Mobile Device Management (MDM) [27] software that can evaluate the device posture such as being jail broken/rooted or containing malicious code. |
| 114. | Mobile Application Management (MAM)[28] S**HALL** be used to enforce application level security for public safety applications, including user authentication and data encryption. MAM can also be used to distribute applications in an automatic and managed manner to UEs based on policies considering users roles, ensuring no applications are inaccessible to unauthorized users. |

## 8.12 Updates

### 8.12.1 Description

After applications are installed on UEs, they could be updated to correct programming errors, to resolve any detected vulnerabilities, or to add new functions and capabilities. Public safety users must be able to obtain and install newer versions of the applications on their UE whenever these newer versions become available.

### 8.12.2 Best Practices

| | |
|---|---|
| 115. | The user **SHALL** be provided with capabilities to control when and how applications are updated on their UE, as authorized. |
| 116. | Local agency administrators **SHALL** be informed in advance of changes to |

[27] http://www.mobiledevicemanagement.org/mobile-device-management-overview
[28] http://www.cultofmac.com/179828/managing-iphones-and-ipads-dont-forget-mobile-app-management/

| | |
|---|---|
| | application, functions and features caused by updates. This is required in order to ensure that appropriate documentation and training be completed prior to the roll out of the update into the public safety environment. |
| 117. | When an update removes features or functionality that existed in the previous version, or if an update dramatically alters the user Interface, operation, or overall functionality of the app, automatic updates **SHALL** not be available. Instead, the update shall be forced to manual delivery and shall require the user to acknowledge the changes and give the user the ability to learn and adapt to the changes in a controlled environment. |
| 118. | MDM and MAM capabilities **SHALL** be available to enable version control and manage the update of applications on public safety UEs. |
| 119. | Sensitive applications **SHALL** be encrypted whenever they are being downloaded to the UE. |

# 9 Site Hardening

**ACKNOWLEDGEMENT**: Chapter 9 provides a comprehensive analysis of site hardening requirements and was provided by the Association of Public Safety Communications Officials (APCO) International. The original APCO Report, created by their Broadband Committee has been edited here to match the formatting of the NPSTC report.

This chapter represents site requirements with the specific future intention to establish "hardening" standards which create public safety grade sites. The requirements in this document have been developed by a subcommittee of the APCO Broadband Committee representing government communications system operators, communications systems vendors, representatives from commercial service providers, and LMR and broadband consultants.

## 9.1 Scope of Document

This chapter represents public safety requirements regarding various characteristics to make mission critical communications network sites sufficiently robust to meet the service availability requirements of public safety. In other words, what it takes to make network sites "public safety grade" or the extent to which they are "hardened." The document is intended to assist public safety communications network builders with the guidelines necessary to build hardened public safety grade networks. These requirements will be developed with the intention to provide working documents for other APCO working groups to develop public safety hardening standards.

This document addresses hardening for wireless transmission or reception sites. Specifically, it addresses the hardening requirements to provide the appropriate site conditions and characteristics for wireless system electronics (e.g., transmitters and receivers) and wireless passive components (e.g., coaxial cables and antennas). These sites need to withstand the onslaught of natural or manmade conditions and take into account the different requirements for different geographic locations of the United States including their likelihood to be subject to severe storms, earthquakes, tornadoes, and other natural disasters.

This document is intended to address radio sites external to another structure, e.g., stand-alone sites with antennas or sites co-located with but external to an existing fire station or dispatch center. It does not directly address micro-sites located within a building, distributed antenna systems inside a building, stadium, or similar structure, and so forth. Such sites, when implemented, should follow the appropriate practices and requirements specified herein.

## 9.2 Existing Hardening Standards

Industry standards and published recommendations are referred to throughout this document. These standards and publications assist in defining the characteristics required of mission critical communications network sites. In some cases these standards and recommendations are specific to public safety communications site design, development, and deployment. In other cases, the standard is applicable to commercial site design, development, and deployment, with additional "classes," "divisions," or "categories" with more rigorous requirements for critical and/or "life safety" applications. (i.e., TIA-222G: Class 1 vs. Class 2 or Class 3 for communications towers.)

The following table represents key documents used in the creation of these standards as well as the short name used in referencing these existing documents:

| Short Name | Author | Adoption Date | Document Title |
|---|---|---|---|
| **ANSI/TIA-1019A** | American National Standards Institute / Telecommunications Industry Assoc. | 2012 | Standard for Installation, Alteration and Maintenance of Antenna Supporting Structures and Antennas |
| **ANSI T1.313-2003** | American National Standards Institute | 2003 | Electrical Protection of Communications Towers and Associated Structures (Superseded ATIS 0600313, 12/2013) |
| **ANSI T1.334-2002** | American National Standards Institute | 2002 | Electrical Protection For Telecommunications Central Offices |

| | | | |
|---|---|---|---|
| | | | and Similar Type Facilities (Superseded by ATIS 0600334, 05/2013) |
| **ANSI/TIA-222-G** | American National Standards Institute / Telecommunications Industry Assoc. | 2009 | Structural Standard for Antenna Supporting Structures and Antennas |
| **ASCE-7** | American Society of Civil Engineers | 2013 | Minimum Design Loads for Buildings and Other Structures |
| **CLF-SFR0111** | Chain Link Fence Manufacturers Assoc. | Not Provided[29] | Chain Link Fence Manufacturers Institute Security Fencing Recommendations |
| **OET- Bulletin 65** | Federal Communications Commission | 1997 | Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields, Office of Engineering and Technology Bulletin 65 |
| **IEC 61024-1-2** | International Electrotechnical Commission | | Protection of structures against lightning – Part 1-2: General principles – Guide B – Design, installation, maintenance and inspection of lightning protection systems |
| **IEC 61643-1** | International Electro technical Commission | 2011 | Low Voltage Surge Protective Devices, Testing |
| **IEEE C62.45** | Institute of Electrical and Electronics Engineers | 2002 | Surge Protection Device Testing |
| **IEEE STD 1100** | Institute of Electrical and Electronics Engineers | 1999 | Recommended Practice for Powering and Grounding [Revised 2005] |
| **IEEE STD 1159** | Institute of Electrical and Electronics Engineers | 2001 | Recommended Practice for Monitoring Electric Power Quality [Revised 2009] |

[29] The document is available at the following link http://associationsites.com/clfma/collection/CLF-SFR0111Security%20Fencing%20Recommendationsr0611.pdf

| | | | |
|---|---|---|---|
| **NEMA 250** | National Electrical Manufacturers Assoc. | 2008 | Enclosures for Electrical Equipment, 1000V Maximum |
| **NFPA 70 (also the NEC)** | National Fire Protection Association | 2014[30] | National Electric Code |
| **NFPA 780** | National Fire Protection Association | 2011 | Standard for the Installation of Lightning Protection Systems [Revised for 2014] |
| **NFPA 1144** | National Fire Protection Association | 2008 | Standard for Reducing Structure Ignition Hazards from Wild land Fire |
| **Motorola R56** | Motorola Solutions, Inc. | 2005 | Standards and Guidelines for Communication Sites |
| **UL-1449** | Underwriters Laboratory | 2006 | Surge Protective Devices |
| **UL-72** | Underwriters Laboratory | 2001 | Tests for Fire Resistance of Record Protection Equipment |
| **UL-752** | Underwriters Laboratory | 2005 | Standard of Safety for Bullet-Resisting Equipment |
| **UL-96A** | Underwriters Laboratory | 2013 | Lightning Protection Components |
| **UL-1449** | Underwriters Laboratory | 2009 | Standard for Safety for Surge Protective Devices, 3rd Edition |

This table and the requirements in this document represent, except where specifically noted, are thought to represent the most current version of the applicable specification. Many of these standards are updated regularly. Collectively, these underlying standards documents may trigger changes in the underlying specifications if the new standards were adopted.

## 9.3 Organization of Document

This document is organized into four primary sections: The introduction, environmental events, the Public Safety Grade best practices, and carrier hardening practices. The introduction identifies the scope of the document, the authors of the document, and how to use the document. The environmental events section outlines incidents that a PSG site must protect against as well as recommended actions to make sites more resilient to the events. The

[30]The Task Force recognizes that a 2014 version is available from NFPA. However it has not reviewed this 2014 version. The requirements are based on the 2011 version.

requirements section identifies the necessary specifications for sites to achieve PSG. It is organized by functional area. All requirements are contained in tables and numbered sequentially. The requirement tables are surrounded by text that provides additional context and intent.

## 9.4 Economics

The high cost associated with meeting these requirements may not be feasible at all sites. The PSG Task Group understands FirstNet will (with input from the local jurisdictions) have to make decisions about each individual site given the available resources to build the NPSBN. The parties must consider the importance of the site, be it a site that aggregates substantial traffic or the criticality of a facility it serves, against the cost to achieve these requirements. In some cases, sites lack the space or other constraints to meet some of these requirements at any cost. At the same time, the risk of failure must also be assessed for the site. For example, if the risk is high that commercial power will fail, backup power sources become more critical and worth the investment. In fact, in the experience of the Task Group members, power failures represent one of the most common causes for outage in communication networks. Therefore, redundant power solutions are a critical element in achieving PSG system availability. This then underscores the need to assess the cost of each requirement against the risk it protects against and the likelihood of that risk. Likewise, the same risk versus cost evaluation must be conducted for LMR sites. It is important to note that the risk factors must address not only the likelihood of an event that causes unavailable communications; it must also address the impact of the lack of communications. When a risk factor then protects against ice storms, as an example, it must also assess the impact of loss of public safety communication in dealing with the ice storm.

## 9.5 Environmental Events

Environmental issues must be addressed and are fully described in a prior chapter on this topic.

## 9.6 Public Safety Grade Site Requirements

The following sections provide the detailed requirements for establishing PSG communications sites. The requirements are organized by functional area. Each requirement is contained in a table and numbered sequentially. A single requirement occupies one row in the table and is provided a requirement number.

### 9.6.1 General Requirements

The following requirements are general in nature and apply across all requirements sections.

| | |
|---|---|
| 120. | Critical communications sites, such as public safety sites, **SHALL** adhere to all legally applicable local *and national standards and practices as defined by the local and state building, electrical, fire, and other applicable codes.* |
| 121. | In the case where legally applicable codes differ from the standards, practices, and other requirements within this document, the more stringent or rigorous requirements **SHALL** be applied. |
| 122. | In the case where the legally applicable codes are in conflict with the requirements within this document, the legally applicable code **SHALL** be followed. |
| 123. | In the case where the legally applicable code is in conflict with the requirements within this document the site designer/developer **SHOULD** attempt to meet the intent of the requirements of this document without violating the legally applicable code requirement.<br>Alternatively, the site designer/developer may attempt gain an exemption or waiver of the legally applicable code requirement. |
| 124. | If the referenced standards (e.g., TIA 222 Rev G) are updated or amended, the newest revision **SHALL** apply unless otherwise noted. However, sites **SHOULD** only have to comply with the most current standard at the time of construction or site modification.[31] |

### 9.6.2 Physical Security

#### *9.6.2.1 Objectives and Scope*

The overall intent of this section is to provide requirements for public safety communications site physical security. The physical security of the public safety sites is critical to protecting emergency responders and our communities to insure that this vital resource is operational and functioning at the highest level in the greatest time of need.

The scope of this physical security section is to address manmade events (e.g., attacks), as opposed to natural events. Hardening against natural events is covered by other sections of this document. The principal assets that need to be secured are the physical elements comprising a public safety radio communications site, excluding the electronics (i.e., hardware, firmware, and software) and backhaul components. This section considers elements of physical security

[31] The Task Group does not intend for these requirements to imply that the system builders and operators must constantly upgrade their facilities to meet these requirements as these requirements or their underlying references to other standards/specifications change. These requirements are intended to dictate build or retrofit requirements in general.

including asset protection, threat assessment, threat detection, and threat containment. Threats include theft, vandalism, and malicious intent to impair the assets and/or the system. These requirements do not consider operational aspects of physical security, such as asset recovery, event data collection, post-event analysis, and practice/process improvement. These aspects are expected to be covered by the NPSTC PSG document.

Risks do not apply equally to different site types. As an example, sites in rural area are more susceptible to gunfire and sites mounted on other facilities may be more susceptible to an external facility fire. Pole-mounted cabinet sites will have a very different threat profile than full stand-alone shelters. Additionally, the total network impact must be considered with "multi-function" sites, such as master sites, transport aggregation/hub sites, and shared LMR/LTE sites requiring greater protection and hardening than minor fill-in coverage sites. As such, any prioritization of physical security controls or resources should consider the larger impact to multi-function sites.

Demarcation points are identified to delineate assets that are within scope of the physical security subsection. Assets and associated demarcation points are identified in the following illustration:

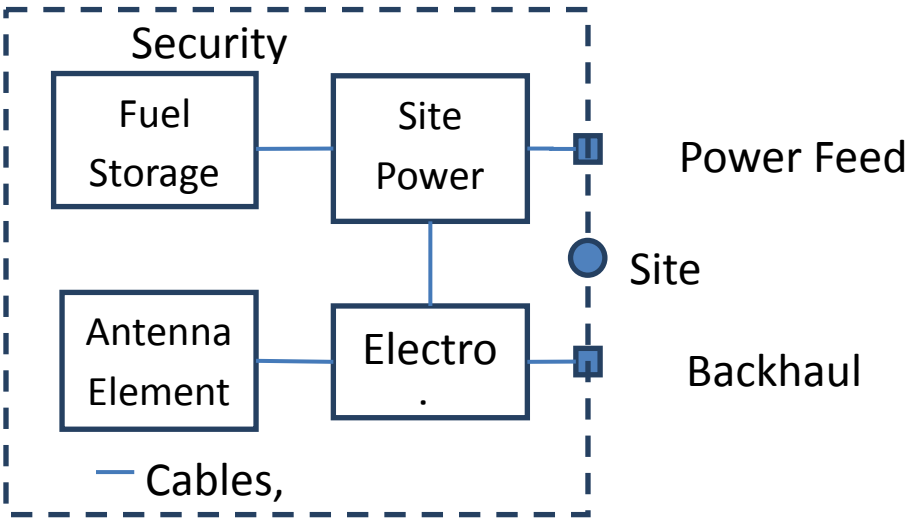



Figure 1: **Security Perimeter – Plan View**

The site must also be secured from ground level to the highest point on any of the structures identified.

### 9.6.2.2 Securing Site Perimeter and Site Access

#### 9.6.2.2.1 Threat Mitigations

1. Provides warning to casual observers of legal boundary of private property.
2. Deters and prevents casual intruders from penetrating restricted and private area.
3. Provides psychological deterrent.
4. Causes delay in obtaining access to the site.
5. Violating of perimeter fencing helps establish criminal intent.

Fencing is only required in areas that have public access. Fencing around site components may be required if the component is outside a restricted access area. There is no intent to require fencing within a fenced area.

Effectiveness of perimeter fencing is materially improved by the provision of clear zones on both sides of the fences. Such clearance areas facilitate surveillance and maintenance of fencing and deny cover to vandals, trespassers, and contraband.

#### 9.6.2.2.2 Threat Controls and Asset Protections

| | |
|---|---|
| 125. | Fencing **SHALL** be required around site components unless they are already restricted from public access (e.g., located on locked roof top or within a secured compound). |
| 126. | Chain link fence fabric **SHALL** be constructed from minimum 9 gauge material with 1290 foot-pounds of tensile strength. |
| 127. | Chain link fence fabric **SHOULD** have a mesh size of 1 inch with anti-cut; anti-climb material with no more than 2 inch mesh SHOULD be used. (The smaller the mesh the more difficult to climb.) |
| 128. | Chain link fence fabric bottom SHOULD be buried to reduce penetration at the base. |
| 129. | Chain link fence fabric **SHALL** have a minimum height of 8 feet. |
| 130. | Chain link fence fabric top section **SHOULD** include razor wire or 1 foot width of 3 strand, 4 barbed, 12.5 gage or better barbed wire angled outward at 45 degrees. |
| 131. | Chain link fence frame **SHALL** consist of line posts, end posts, corner posts, gateposts, and if required top, mid, bottom or brace rail. |
| 132. | Chain link fence frame **SHALL** have a minimum of Schedule 40 pipe of welded pipe and SHOULD be used with a minimum diameter of 2.875 inches. |
| 133. | Chain link fence frame **SHALL** be designed such that posts, bracing, and all other structural members are to be placed on the secure-side of the fencing. |
| 134. | Chain link fence frame **SHOULD** consider eliminating the top rail to eliminate handholds for climbing. |
| 135. | Chain link fence frame **SHOULD** consider weather and wind load when determining frame construction. |

| | |
|---|---|
| 136. | If a chain link fence cannot be used (e.g., due to design ordnances), then an 8-foot high non-scalable wall **SHOULD** be installed. |
| 137. | Gates **SHALL** be similar or higher quality as the fence. |
| 138. | Gates **SHALL** provide limited access for intruders while providing safe passage for operators. |
| 139. | Gates **SHOULD** be securely and robustly lockable (eg, using a ½ inch case-hardened steel chain and a padlock with a ½ inch case-hardened shackle and case-hardened shell, electronic lock). |
| 140. | Clear zones (e.g., 3 foot min) **SHOULD** be designed for deterrence, detection of intruders and for defensible space to protect against wild land fire. |
| 141. | Clear zones **SHOULD** be free of climbable objects, trees, or utility poles abutting the fence line or areas for stackable crates, pallets, storage containers, or other materials. |
| 142. | Vehicles **SHOULD** be prevented from parking along the fence. |
| 143. | Landscaping within the clear zone **SHOULD** be minimized or eliminated to reduce potential hidden masking locations for persons, objects, fence damage, and vandalism. |
| 144. | Signage **SHOULD** contain warnings and law violation information. This is to not only deter crime but to help in showing criminal intent. |
| 145. | Signage **SHOULD** not indicate site ownership or operational purpose. The intent is to avoid governmental targeting. |
| 146. | Signage **SHOULD** be installed at 50-foot intervals maximum. |
| 147. | Signage **SHOULD** be 5 feet above the ground. |
| 148. | Signage **SHOULD** be reflective. |
| 149. | Signage **SHOULD** have 1 inch red lettering minimum. |
| 150. | Signage **SHOULD** have a white background. |

Additional construction information can be found at the Chain Link Fence Manufactures Association website www.associationsites.com document CLF-PM0610.

#### *9.6.2.3 Securing Service Demarcation Points, Antenna Structures, Cables, and Pipes*

##### *9.6.2.3.1 Antenna Structures*

##### *9.6.2.3.2 Threat Scenarios*

The following scenarios could threaten the availability and/or integrity of antenna supporting structures, or the site itself:

1. Removal or damage to structural steel components.
2. Removal or damage to guy wires.
3. Removal or damage to guy wire turnbuckles.
4. Removal or damage to structural bolts.

5. Removal or damage to grounding bars.

#### *9.6.2.3.2.1 Threat Assessments*

The impact of any of the listed scenarios could cause the structure to degrade or collapse that would cause complete operation of the site to fail. Because of the severity of impact to the site, and the time to restore the structure, all identified threats should have controls and protections in-place.

#### *9.6.2.3.2.2 Threat Controls and Asset Protections*

| | |
|---|---|
| 151. | The antenna supporting structure **SHALL** be protected with perimeter fencing per section 11.2.2. |
| 152. | The guy wire anchor **SHALL** be protected with perimeter fencing per section 11.2.2. |
| 153. | The guy wire turnbuckles **SHALL** be protected with safeties installed to protect them from being turned out. |
| 154. | Access points (e.g., gates, doors) **SHALL** be secured at all times. |
| 155. | Detection methods (e.g., video surveillance, ground bar disconnection alarm) **SHOULD** be deployed (e.g., if site is located in area where higher than normal risk of vandalism is expected). |
| 156. | Motion sensing lighting **SHOULD** be installed at base of structure. |
| 157. | Protection and security of transmission lines and cable runs (e.g., via anti-climb gates, underground runs, conduit encasement, tower encasement) **SHOULD** be provided up to 12 feet above ground or roof grade. |

### *9.6.2.3.3 Demarcation Points*

#### *9.6.2.3.3.1 Threat Scenarios*

The following scenarios could threaten the availability and/or integrity of utility transformers, electrical meters, electrical disconnects, and telephone junction boxes, causing site to lose utility power or connectivity.

1. Removal or damage to the site's electrical meters.
2. Damage or manipulation of the site's electrical disconnects.
3. Damage to the site's utility transformers.
4. Removal or damage to the site's telephone junction boxes.

#### *9.6.2.3.3.2 Threat Assessments*

The impact of any of the listed scenarios could cause the site to lose utility power, and / or communications. Loss of utility power would require site to run off its back-up power supply.

Loss of communication may deliver the site inoperable. Because of the severity of impact to the site, and the time to restore the effected components, all identified threats should have controls and protections in place.

#### *9.6.2.3.3.3 Threat Controls and Asset Protections*

| | |
|---|---|
| 158. | The site's electrical meter **SHALL** be protected with perimeter fencing per section 11.2.2. |
| 159. | The site's electrical disconnect(s) **SHALL** be protected with perimeter fencing per section 11.2.2. |
| 160. | The site's electrical disconnect(s) **SHALL** be secured / locked to prevent the manipulation of disconnect if allowed. |
| 161. | The site's utility transformer **SHALL** be protected from vehicle collision. |
| 162. | The site's telephone junction boxes **SHALL** be protected from vehicle collision. |
| 163. | Access points (e.g., gates, doors) **SHALL** be secured at all times. |
| 164. | Site's electrical pedestal/meters **SHALL** be included within a fenced area of the site or within another secured area. |

### *9.6.2.3.4 Cables, Wires, Feed Lines*

#### *9.6.2.3.4.1 Threat Scenarios*

The following scenarios could threaten the availability of site operation if utility feeds, telco lines, or antenna lines are made inoperable.

1. Damage to the site's electrical feeds.
2. Damage to the site's telco lines.
3. Damage to the site's antenna lines.

#### *9.6.2.3.4.2 Threat Assessments*

The impact of any of the listed scenarios could cause the site to lose utility power, and / or communications. Loss of utility power would require site to run off its back-up power supply. Loss of communication may deliver the site inoperable. Because of the severity of impact to the site, and the time to restore the effected components, all identified threats should have controls and protections in place.

#### *9.6.2.3.4.3 Threat Controls and Asset Protections*

| | |
|---|---|
| 165. | The site's utility feed **SHOULD** be buried to prevent damage or disconnection of service. |
| 166. | The site's telco line(s) **SHOULD** be buried to prevent damage or disconnection of service. |
| 167. | The site's antenna feed lines **SHALL** be secured behind fencing per section 11.2.2. |
| 168. | The site's antenna feed lines **SHOULD** be secured "in-side" the tower structure when |

| | |
|---|---|
| | possible (e.g., within a mono pole or inside tower lattice members). |
| 169. | Shelter cable access ports (e.g., for power cables and antenna feed lines) **SHOULD** be protected from external fire ingress into the shelter. |
| 170. | If transmission lines or cables are installed above ground and environmental conditions require an ice bridge, then the site's antenna feed lines and cables **SHALL** be secured to the underneath of an "ice bridge" in all cases to protect the lines (e.g., from ice or dropped tools, etc.) |
| 171. | Access gates, doors, etc. **SHALL** be secured at all times. |

#### *9.6.2.4 Securing On-Site Fuel Storage*

##### *9.6.2.4.1 Threat Scenarios*

The following scenarios that could threaten the availability and/or integrity of the on-site fuel storage, or the site itself:

1. Malicious fuel ignition.
2. Accidental fuel ignition during maintenance check or refill.
3. Malicious fuel theft.
4. Malicious fuel leak and/or loss.
5. Accidental fuel leak and/or loss during to maintenance check or refill.
6. Malicious fuel contamination.
7. Accidental fuel contamination during maintenance check or refill.

##### *9.6.2.4.2 Threat Assessments*

High-risk threats are fuel ignition and fuel theft. The moderate risk threats are fuel contamination and fuel leak and/or fuel loss. None of the identified threats are classified as low risk.

These risks apply equally to various site types, such as shelters, ground-based enclosures, tower-mounted electronics, and rooftop sites. However, there will be larger network impacts to "multi-function" sites, such as master sites, transport aggregation/hub sites, and shared LMR/LTE sites. As such, any prioritization of physical security controls or resources should consider the larger impact to multi-function sites.

##### *9.6.2.4.3 Threat Controls and Asset Protections*

The security controls and protections for each threat scenario identified in the threat assessments are recommended in this section.

Since identified controls are required to mitigate all high-risk threats, all of the controls identified in this section should be implemented.

| | |
|---|---|
| 172. | Fuel tanks **SHALL** be protected from vehicular collisions (e.g., via peripheral bollards). |
| 173. | Bury or encase fuel tanks: Fuel tanks SHOULD be buried or encased in concrete materials (e.g., Concrete Masonry Units). Either method **SHOULD** be designed by a licensed engineer or architect, follow local codes and ordinances, and account for substructures. Burial substructure considerations include local soil composition, stability, and drainage. Encasement substructure considerations include slab, footings, and roof load-bearing capability. |
| 174. | Secure access to fuel fill/drain ports: Fuel fill ports and drain ports (if applicable) SHALL be access controlled. Access controls **SHOULD** be provided by specific port locking controls. A less secure alternative may be provided by other physical site security controls (e.g., site perimeter fencing). |
| 175. | Secure access to vent ports: Fuel tank vent ports (if applicable) SHOULD be protected such that only air or fuel-vapor can pass through the vent port (e.g., per Uniform Fire Codes). Access controls may be provided by specific port controls (e.g., multi-layer mesh shields). A less secure alternative may be provided by other physical site security controls (e.g., site perimeter fencing). |
| 176. | Secure Site Access: The site **SHALL** be access controlled. See Securing Site Perimeter and Site Access, section 11.2.2, of this document. Site access authorizations SHOULD be role-based and adhere to minimum privilege principles. This principle ensures that access privileges are segmented according to role or function, and that minimum privileges are granted in accordance with the need to perform a role or function. |
| 177. | Each fuel tank **SHOULD** be equipped with a fuel level sensor. The fuel level sensor SHOULD be integrated into the site monitoring system so that fuel levels can be remotely monitored from the network operating center (NOC) or systems operating center (SOC). A low fuel level alarm SHOULD be implemented in the site monitoring system so that the fuel level can be remotely monitored from the NOC/SOC. |
| 178. | Each fuel tank **SHOULD** be equipped with fuel fill/drain port open/closed sensors. The fuel fill/drain port open/closed sensors SHOULD be integrated into the site monitoring system so that fuel port open/closed status can be remotely monitored from the NOC/SOC. A port open alarm SHOULD be enabled in the NOC/SOC alarm system. |
| 179. | The site generator **SHOULD** be equipped with a failed start sensor. The failed start sensor SHOULD be integrated into the site monitoring system so that the generator start status can be remotely monitored from the NOC/SOC. A failed start alarm SHOULD be enabled in the NOC/SOC alarm system. |
| 180. | The site **SHOULD** be equipped with one or more remote cameras. The field of view for one or more of the remote camera(s) SHOULD include the fuel storage tank location. The remote camera(s) video feed SHOULD be monitored from the NOC/SOC. |
| 181. | The site **SHOULD** be equipped with a remote video recording system. The video recording SHOULD be motion triggered or triggered from the NOC/SOC. |
| 182. | The site **SHOULD** be equipped with a local site audible siren. The audible siren SHOULD also have capability to be remotely activated/deactivated from the NOC/SOC. |

### 9.6.2.5 Securing On-Site Generator, Battery Plant, and other Power Sources

#### 9.6.2.5.1 Threat Scenarios

The following scenarios could threaten the availability of site operation if the on-site generator, battery plant, or other power sources are made inoperable.

1. Malicious damage to the site's on-site generator.
2. Accidental damage to the site's on-site generator.
3. Malicious damage to the site's battery plant.
4. Accidental damage to the site's battery plant.
5. Malicious damage to the site's alternative power sources.
6. Accidental damage to the site's alternative sources (i.e., solar power).

#### 9.6.2.5.2 Threat Assessments

The on-site generator, battery plant, and other alternative power sources represent the back-up power necessary to keep the site operating should the main utility power be interrupted. The impact of any of the listed scenarios, concomitant with an interruption of utility power could cause the site to shut down completely with a total loss of communications. Because of the severity of impact to the site, and the time to restore the effected components, all identified threats should have controls and protections in place. The specific nature of the protections afforded the power sources will depend upon their location within the site. Separate protection mechanisms, e.g., video surveillance, are not required if the power sources are protected by the same mechanisms used for the shelter or other components in the site.

#### 9.6.2.5.3 Threat Controls and Asset Protections

| | |
|---|---|
| 183. | Access to the on-site generator **SHALL** be limited to authorized personnel. |
| 184. | Generator **SHALL** be completely enclosed in a secure cabinet or enclosure with access limited to authorized personnel.[32] |
| 185. | Batteries **SHALL** be completely enclosed in a secure cabinet or structure enclosure with access limited to authorized personnel. |
| 186. | Batteries and battery connections **SHALL** be protected from accidental contact. (e.g., where tools and other conductive materials cannot accidently be dropped on them). |
| 187. | Alternative power sources such as solar panels **SHALL** be installed in secured locations out of reach to unauthorized persons. |
| 188. | Alternative power sources such as solar panels **SHOULD** be protected from regionally defined hazards and debris (e.g., falling objects from the on-site tower). |

[32] Enclosures may include building or facility.

#### 9.6.2.5.4 Attack Detection, Response, and Recovery

| | |
|---|---|
| 189. | Video surveillance of on-site generator **SHALL** be installed, unless the site is located in a high risk area. |
| 190. | Generator open door sensors **SHALL** be installed. |
| 191. | Access to on-site generator **SHOULD** have a capability to remotely manage access authentication. |
| 192. | Access to site's battery plant **SHOULD** have a capability to remotely manage access authentication. |
| 193. | Video surveillance of on-site alternative power sources such as solar panels **SHALL** be installed. |

### 9.6.2.6 Securing On-Site Electronics Shelters and Enclosures

#### 9.6.2.6.1 Threat Scenarios

The following scenarios that could threaten the availability and/or integrity of the shelters and enclosures, or the site itself:

1. Compromised access
    a. Unauthorized access
    b. Malicious access
    c. Accidental unsecured site
2. Physical attack
    a. Manual (Tools)
    b. Firearms
    c. Vehicle
3. Fire
    a. Malicious Fire

#### 9.6.2.6.2 Threat Assessments

The specific nature of the protections afforded the on-site electronics shelters and enclosures will depend upon their location within the site. Separate protection mechanisms, e.g., video surveillance, are not required if the shelters and enclosures are protected by the same mechanisms used elsewhere in the site, e.g., if the site is physically located on a fire station staffed 24x7 with existing video surveillance and similar mechanisms.

#### *9.6.2.6.3 Requirements for Securing On-Site Electronics Shelters and Enclosures*

The following table summarized threat detection methods for each identified threat.

| | |
|---|---|
| 194. | Bollards **SHOULD** be installed around the site perimeter and/or around site components which are susceptible to vehicular collision (e.g., fuel tanks) |
| 195. | Gate alarm system **SHOULD** be implemented. |
| 196. | Door alarm system **SHALL** be implemented. |
| 197. | Door lock status/operation monitor system **SHALL** be implemented, where feasible. |
| 198. | Security / tamper-proof hardware **SHALL** be used. |
| 199. | Self-closing doors **SHALL** be used. |
| 200. | Motion detector system **SHALL** be implemented in high risk areas as well within the protected compound. |
| 201. | Video monitoring system (Interior/Exterior) **SHALL** be implemented with digital-video-recording systems. |
| 202. | All alarms and monitoring tools **SHALL** be connected and monitored by a NOC or SOC. |
| 203. | Smoke/fire alarm system **SHALL** be implemented and monitored for shelters. |
| 204. | Bullet-resistant materials and hardware **SHOULD** be used. |
| 205. | Audible intrusion siren **SHOULD** be implemented. |

#### *9.6.2.6.4 Attack Detection, Response, and Recovery*

| | |
|---|---|
| 206. | The site **SHOULD** be equipped with one or more remote cameras. The field of view for one or more of the remote camera(s) should include the exterior of the shelter/site; including typical access gate and door and any vulnerable access or hazard views. The field of view for one or more of the remote camera(s) should include the interior of the shelter/site; including the interior of the door, and sufficient view of overall interior. |
| 207. | The remote camera(s) video feed **SHOULD** be monitored (or monitor capable) from the NOC/SOC and/or local law enforcement if applicable. |
| 208. | The site **SHOULD** be equipped with a remote video recording system. The video recording should be motion/event triggered or triggered from the NOC/SOC. Use of constant or loop recording should be considered. |
| 209. | The site **SHOULD** be equipped with a local site audible alarm. The audible alarm should be triggered from the NOC/SOC. |

### 9.6.3 Antenna Support Structure

These antenna support structure requirements address the necessary steps to provide reliable and robust structures to support communications site apparatus above ground level. This generally includes antennas and associated radio frequency cables, but can also include tower mounted equipment such as low noise amplifiers.

### 9.6.3.1 Antenna Support Structure Design

#### 9.6.3.1.1 New Antenna Supporting Structure Design

This section will provide requirements for new antenna supporting structure design. Additional or future loading of such new antenna supporting structure is not a consideration of this section but should be determined by the new antenna structure owner(s) as required. Please note that exposure and topographic categories for each new structure will be determined based on the interpretation of location of the new antenna supporting structure by the design engineer and structure owner(s).

| | |
|---|---|
| 210. | The design of all new antenna support structures **SHALL** comply with the most current revision of ANSI/TIA-222, Class III. |
| 211. | All newly constructed antenna structures **SHALL** comply with all applicable local, county, state, or federal jurisdictional requirements. |
| 212. | Antenna support structures **SHOULD** be elevated as practical to preclude water damage if located within the 100- and 500-year flood plains. |

The ANSI/TIA-222-G specification contains new parameters that significantly affect the magnitude of wind, ice, and earthquake loading for class III structures. Loadings are increased for structures of public safety Class III classification compared to Class II structures by 15 percent for wind, 25 percent for ice, and 50 percent for earthquakes. The earthquake requirements are confined to regions defined as having high seismic activity and are clearly identified in the standard. These requirements do not preclude applicable local, county, state, or federal jurisdictional requirements. Prior to construction of any new antenna structures full compliance with all applicable building standards and zoning laws shall be verified.

1. Whenever any standard such as ANSI/TIA-222 or ANSI/TIA-1019A is referenced it means the latest version including any amendments to that version. As an example there are two amendments for ANSI/TIA Rev G, which came in 2007 and 2009.
2. Antenna support structures types referenced here include self-support, guyed or monopole.

#### 9.6.3.1.2 Existing Antenna Supporting Structures

This section will provide requirements for the structural analysis and potential upgrades of existing antenna supporting structures. A rigorous structural analysis for each existing antenna supporting structure is required prior to the installation of new antennas unless the installation of the new antennas has been determined to fall within section 15.4 of ANSI/TIA-222G. This determination should be made by the engineer performing the rigorous structural

analysis. Please note that exposure and topographic categories for each existing antenna supporting structure will be determined based on the interpretation of location of the existing antenna supporting structure by the engineer performing the rigorous structural analysis and structure owner(s).

| | |
|---|---|
| 213. | A rigorous structural analysis **SHALL** be required for each existing antenna supporting structure prior to the installation of new antennas, lines, or appurtenances unless the installation of such items has been determined to fall within section 15.4 of the most recent version of ANSI/TIA-222 (including all amendments). This determination shall be made by towers owner and properly licensed Professional Engineer (PE) or Structural Engineer (SE) performing the structural analysis. The determination should be in writing and signed off by the tower owner as well as signed and sealed by the jurisdictionally licensed PE or SE who performed the analysis. |
| 214. | All existing antenna support structures **SHALL** be compliant with the most recent version of ANSI/TIA-222 Class II. |
| 215. | All existing antenna support structures **SHOULD** be compliant with the most recent version of ANSI/TIA-222 Class III. |
| 216. | All existing antenna support structures which require upgrades or modifications **SHALL** comply with the most recent version of ANSI/TIA-222 and ANSI/TIA-1019A. |

Towers types include self-support, guyed or monopole.

ANSI/TIA-222 shall govern the structural analysis requirements for modifications and upgrades. While previous revisions of ANSI/TIA-222 allowed the use of existing tower structures, all modifications and upgrades moving forward must be in compliance with the most current version of ANSI/TIA-222 and ANSI/TIA-1019A.Ensuring the structural integrity after modifications and upgrades (or no overstress beyond the safety factor of the original design parameters) of the existing antenna support structure and its foundation are paramount to verify before utilizing it. Additionally ensuring the existing antenna support structure (after modifications and upgrades) meet the twist and sway specifications (thus the five or six nines reliability and/or availability) of the intended end user are also of utmost concern before utilizing it.

#### *9.6.3.1.3 Other Existing Antenna Supporting Structures*

This section will provide requirements for the structural analysis and potential upgrades of other existing antenna supporting structures. A rigorous structural analysis for each existing antenna supporting structure is required prior to the installation of new antennas unless the installation of the new antennas has been determined to fall within section 15.4 of ANSI/TIA-

222 G. This determination should be made by the engineer performing the rigorous structural analysis. Please note that exposure and topographic categories for each existing antenna supporting structure will be determined based on the interpretation of location of the existing antenna supporting structure by the engineer performing the rigorous structural analysis and structure owner(s).

| | |
|---|---|
| 217. | All other antenna supporting structure types **SHALL** comply with the most current revision of ANSI/TIA-222, Class II for structural analysis and ANSI/TIA-1019A for all upgrades and modifications. |
| 218. | All other antenna support structure types **SHOULD** comply with the most current revision of ANSI/TIA-222, Class III for structural analysis as applicable for all upgrades and modifications. |
| 219. | All existing antenna support structures which require upgrades or modifications **SHALL** comply with the most current revision of ANSI/TIA-222 and ANSI/TIA-1019A. |

#### *9.6.3.2 Other Structures (e.g., Billboards, Specialty)*

Use of antenna support structures that cannot be designed to or comply with the most current revision of ANSI/TIA-222 and also do not meet twist and sway requirements of the end user are discouraged.

#### *9.6.3.3 Lightning Protection and Grounding*

This section will provide requirements for lightning protection and grounding, both external and internal, which when implemented will be considered PSG for this category. In order to disperse lightning energy into the earth without causing dangerous over-voltage, the shape and dimensions of the grounding (earthing) electrode system are more important than a specific resistance value of the grounding electrode system. However, a low resistance grounding electrode system is generally recommended (IEC 61024-1-2). Attempts should be made to reduce the grounding electrode system resistance to the lowest practical value (MIL-HDBK-419A, section 2.2.3). Refer to Motorola R56 grounding guidelines, chapter 4, Para 4.7.4.[33]

[33] As a co-author and person responsible for R56 and on behalf of Motorola, I hereby give express permission to the National Public Safety Telecommunications Council (NPSTC) and Association of Public-Safety Communication Officials (APCO) to reference R56 language and diagrams as required for their efforts in completing their respective Public Safety Grade Reports. Robert Batis.

| | |
|---|---|
| 220. | A "single point" grounding concept is required. This includes a single ground point located at all of the outside shelter or equipment room penetrations (RF, AC power, and generator, GPS, tower light controllers, equipment and phone lines. This design will affect the overall equipment layout. DC power systems should also logically be located close to this ground point. Though this uses up some wall and floor space, it permits the systematic growth of communications equipment outward.[34] |
| 221. | External grounding **SHALL** be a common grounding system which complies with NEC Article 250. |
| 222. | Sites **SHALL** achieve a grounding (earthing) electrode system resistance not to exceed 10 ohms. |
| 223. | The sites **SHOULD** achieve a grounding (earthing) electrode system resistance of 5 ohms or less. [35] |
| 224. | Sites in high lightning prone geographical areas, and sites normally occupied (such as dispatch centers), **SHOULD** include enhancements to the grounding electrode system per ANSI T1.334-2002 Section 5.4. |
| 225. | Grounding electrode system enhancements **SHOULD** include.[36]<br>A. Installation of radial grounding conductors.<br>B. Installation of concrete encased electrodes in new construction.<br>C. Installation of longer ground rods. |
| 226. | A lightening arrestor and surge protection system which is compliant with the latest revision of NFPA-780, UL-1449, and UL-96A **SHALL** be required. |
| 227. | All cable tray sections shall be electrically bonded together by an approved method and connected to the building ground system. The cable tray system shall be grounded to the room single point ground position (MGB) only.[37] |
| 228. | Grounding electrodes, conductors, connection devices, and bus bars **SHALL** be listed (UL 467 or equivalent) and installed in compliance for the intended purpose. |
| 229. | External grounding conductors **SHALL** be #2 AWG or coarser, bare, solid, tinned copper. |
| 230. | The radio facility **SHALL** have a common internal and external grounding electrode system. (NFPA 70, Article 250, Grounding, and Bonding and NFPA 780, Article 4.14.1) |
| 231. | Newly constructed radio facilities **SHALL** incorporate a concrete encased electrode (Ufer) in the footer of the building as an integral part of the buildings common grounding electrode system. (NFPA 70, Article 250.52(c); and NFPA 780-2008, section 4.13.3) |

[34] Motorola R56 paragraph 3.3
[35] Motorola R56 paragraph 4.7.4.2
[36] Motorola R56, Section 4.7.4.3 – Supplemental Grounding (Earthing)
[37] Motorola R56 paragraph 3.10.5

| | |
|---|---|
| 232. | The facility **SHALL** have an intersystem bonding termination (IBT) external to enclosures at the electrical service-entrance equipment or metering equipment enclosure and at the disconnecting means for any additional buildings or structures. (NFPA 70, Article 250.94 - Bonding for Other Systems) |
| 233. | The facility **SHALL** have a master ground bus bar (MGB) installed within 24 inches below the primary RF cable entrance to serve as the single point internal ground and provide a convenient grounding location for RF cable surge protection devices. (NFPA 70, Article 250.94 - Bonding for Other Systems)<br>1. The master ground bus bar **SHALL** be bonded to the common external grounding system and **SHALL** be bonded to the intersystem bonding termination at the electrical service-entrance panel. |
| 234. | A subsystem ground bus bar **SHALL** be installed within 24 inches below each secondary RF cable entrance to provide a grounding point for RF cable surge protection devices.<br>1. The subsystem ground bus bar shall be bonded to the master ground bus bar and grounded to the common external grounding system. |
| 235. | For new building construction, vertical structural steel members **SHALL** be "effectively" bonded to a concrete encased electrode. (NFPA 70-2011, Article 250.52(A)(3)) |
| 236. | A telecommunications master ground bus bar (TMGB) **SHALL** be installed near the primary telecommunications service-entrance. The TMGB may be located in the primary telecommunications equipment room where the telecommunication service-entrance is established separate from the electrical service-entrance. |
| 237. | All incoming telecommunication cables, including paired-conductors and optical fiber cable at the telecommunications service-entrance **SHALL** be grounded to the common building grounding system. |
| 238. | Primary surge protection devices (SPDs) for telephone circuits, data circuits, and control circuits **SHALL** be connected to the single point ground with a #6 AWG or coarser grounding conductor using UL 467-listed (or equivalent) grounding connectors. |
| 239. | Lightning protection systems **SHALL** be installed where required by NFPA 780. |
| 240. | If it is determined that a lightning protection system is not necessary, a written document prepared by a qualified engineer justifying why a lightning protection system is not necessary **SHALL** be prepared.<br>1. This document must specifically address the exposure criteria provided below and include appropriate references, results from soil resistivity testing, and elevation measurements used to justify not installing a lightning protection system. |

| | |
|---|---|
| 241. | Building ground rings and tower ground rings **SHALL** be bonded together in at least two points using #2 AWG or coarser, bare, solid, tinned or un-tinned, copper conductor with conductors physically separated to the extent practical.[38] |
| 242. | When multiple radial conductors are used, the conductors **SHOULD** be of different length to help prevent resonant "ringing" of the tower from a lightning strike and facilitate the dissipation of the lightning strike. |

### 9.6.4 Equipment Enclosures

This section will provide requirements for the use and potential upgrades of communications equipment shelters and cabinets which, when implemented, will be considered PSG for this category. A shelter is defined as a structure used to house communications equipment, which is large enough to allow physical entry by one or more support personnel. A cabinet is defined as a structure used to house communications equipment which is not designed for, or large enough to, allow entry by one or more personnel.

#### *9.6.4.1 Shelter Requirements*

| | |
|---|---|
| 243. | Shelter walls, roof, and doors **SHALL** at a minimum have a 150 mph static wind rating in accordance with the latest revision of ASCE-7 Chapter 6. |
| 244. | Shelter roof/top **SHALL** at a minimum have 150 PSF static load rating in accordance with the latest revision of ASCE-7. |
| 245. | All shelters **SHALL** be equipped with a temperature sensing and alarm system. |
| 246. | Shelters **SHALL** be constructed using fire resistant materials designed to keep critical components [39] to below 125 degrees Fahrenheit in order to maintain operational serviceability for at least 2 hours and at a minimum meet the latest revision of UL 72 Class 125-2. |
| 247. | Shelters **SHALL** meet NEMA 3R standards as described in the latest version of NEMA 250.[40] Shelter weather proofing at a minimum SHALL provide protection against the ingress of solid foreign objects (dirt) and protection from the harmful effects on the equipment due to the ingress of water (rain, sleet, snow). |

[38] Motorola 56, Section 4.4.1.6, p 4-22.
[39] This rating is the requirement in enclosures for protecting digital information on magnetic media or hard drives. Temperatures inside the protected chamber must be held below 125 °F (52 °C) with temperatures up to 1700 F (1,090 °C) outside the enclosure for a minimum of 2 hours.
[40] The NEMA X ratings (such as 3X or 4X) should be considered for shelters and cabinets to be located in highly corrosive environments (e.g., chemical plants, industrial plants, or locations in close proximity to saltwater coast lines). It is recommended to consult and collaborate with a professional engineer and cabinet manufacturer(s) for the best way to protect against the corrosive environment and whether a NEMA X-rating is actually required for the cabinet.

| | |
|---|---|
| 248. | Shelter walls, roof, and doors **SHALL** at a minimum meet the latest revision of UL-752 bullet resistance level 4 testing criteria. |
| 249. | Shelters **SHALL** be elevated to preclude water damage if located within the 100 and 500-year flood plains or other areas prone to flooding.[41] |

#### *9.6.4.2 Cabinet Requirements*

| | |
|---|---|
| 250. | All cabinets **SHALL** be equipped with a temperature sensing and alarm system. |
| 251. | Cabinet walls, roof and doors **SHALL** at a minimum have a 150 mph static wind rating in accordance with the latest revision of ASCE-7 Chapter 6. |
| 252. | Cabinets **SHOULD** be constructed using fire resistant materials designed to keep critical electrical circuits to below 125 degrees Fahrenheit in order to maintain operational serviceability for at least 2 hours and at a minimum meet the latest version of UL 72 Class 125-2.[42] |
| 253. | Cabinets **SHALL** meet NEMA 3R standards as described in the latest version of NEMA 250. Weather proofing at a minimum **SHALL** provide protection against the ingress of solid foreign objects (dirt) and protection from the harmful effects on the equipment due to the ingress of water (rain, sleet, snow) and will be undamaged by the formation of external ice. |
| 254. | Cabinet walls, roof, and doors **SHOULD** at a minimum meet UL 752 bullet resistance level 4 testing criteria[43] where circumstances and risks warrant. |
| 255. | Cabinets **SHALL** be elevated to preclude water damage if located within the 100 and 500-year flood plains or other areas prone to flooding. |

[41] It is not recommended to install an enclosure of any kind within a designated flood plain, zone, or areas prone to flooding. If however it is determined that an enclosure must be located in such an area it is recommended to consult and collaborate with design engineers to determine the proper structure or methodology to elevate the enclosure. In addition it is recommended to work with design engineers and jurisdictional authorities to determine the proper ground elevation the enclosure should set at to minimize any flooding risk.

[42] Compliance to the latest version of UL 72 Class 125-2 should be considered for locations where cabinet(s) is likely to be subjected to fire threats. It is recommended to consult and collaborate with design engineers, cabinet manufacturers and jurisdictional authorities to make such determinations. Additionally it is recommended to consult with cabinet manufacturers to understand the viability of manufacturing, direct and indirect costs and timeline of independent verification associated with such compliance and to ensure proper project planning can occur.

[43] Compliance to UL 752 bullet resistance level 4 should be considered for locations where cabinet(s) is likely to be subjected to such threats. It is recommended to consult and collaborate with design engineers, cabinet manufacturers and jurisdictional authorities to make such determinations. Additionally it is recommended to consult with cabinet manufacturers to understand the viability of manufacturing, weight impacts, direct and indirect costs and timeline of independent verification associated with such compliance and to ensure proper project planning can occur.

### 9.6.5 Environmental and Climate Control

This section will provide minimum design requirements for the use and potential upgrades of environmental control systems to include heating and cooling of any structure or enclosure which, when implemented, will be considered PSG for this category.

| | |
|---|---|
| 256. | Climate control systems **SHALL** be able to maintain an optimum operating temperature and humidity level consistent with manufacturer specifications, peak performance and long term reliability of all equipment and batteries[44] installed within an enclosure. [45] |
| 257. | Flooded batteries **SHALL** additionally require "NO SMOKING" signs posted on the interior and exterior of the entry door and provisions shall be made to exhaust gasses produced by flooded cell (wet) batteries. This **SHALL** include changing the rooms total air volume no less than four times per hour or installing a manifold and tubing system designed to vent gases directly to the exterior of the enclosure. |
| 258. | Climate control systems **SHALL** be designed and sized to environmentally control the space inside the enclosure to minimally accommodate the peak heat load of the components inside the enclosure as well as the peak load presented by the external environment surrounding the enclosure. |

### 9.6.6 Power

Clean, reliable electrical power is paramount to highly available wireless communications sites. Availability of power to communications equipment is the fundamental limiting factor regarding the in-service state of the equipment. The causes of loss in commercial power can vary from natural events such as ice storms and high winds to manmade failures such as overload of the power grid. When failures occur, they often persist for several hours or days until downed lines can be restored. As a result, communications systems, to be highly resilient, must have immediate and long-term backup sources. And finally, the power systems themselves must include redundant components to protect against failures as well as include components that protect the power systems from upstream power system deficiencies.

Sites each have different levels of criticality that would affect the operations of the network. Each site must be addressed individually based on the importance in regards to the network

[44] Short term operation of a public safety grade site without climate control on battery power is acceptable in the event of a generator failure where the intent of the battery power is to maintain operations through the transfer from commercial power to generator back-up. Short term defined as a nominal 4 hours to allow for generator repair and/or replacement.

[45] Optimal enclosure temperature should be maintained between 65-75 degrees Fahrenheit and a relative humidity between 45 and 55%.

operation and ability to provide users continuous and reliable connectivity and data throughput. Every site layout shall identify and rectify any single point(s) of failure that would interrupt service affect site availability.

#### *9.6.6.1 General Electrical Requirements*

| | |
|---|---|
| 259. | AC power systems **SHALL** be designed installed and maintained adhering to the current NFPA 70/NEC[46] codes and/or local jurisdictional codes utilizing the most stringent. |
| 260. | Future expansion of the site **SHALL** be considered during the electrical systems design. |
| 261. | Operating loads **SHALL** not be more than 80% of the electrical systems capacity. |
| 262. | The current edition of NFPA 70- Article 220 and Article 310-15 or the local jurisdiction's code, whichever is more stringent **SHALL** be considered for circuit / feeder design and conductor selections |
| 263. | At all sites, there is either or both a main service disconnect and a fused disconnect. A main service disconnect may be located at a meter location away from the building. A main disconnect located within the shelter, equipment room, or area may be fed by a feeder circuit originating at a main service disconnect located in an electrical room in a different location in the building or even a separate building. Typically, the neutral and ground conductors are bonded in the main service disconnect. When the main service disconnect is located remotely from the equipment room or area, a separately derived system **SHOULD** be installed in the equipment room. (See NFPA 70, Article 250.30 and 250.32 for additional information.) One of the reasons for the separately derived system is to reestablish the neutral/ground bond, thereby improving the effectiveness of normal mode suppression. See figure 6 below within this section. |
| 264. | Circuit breakers **SHALL** be sized to protect the conductor attached to them and not the load (Current edition of NFPA 70, Article 240.4) |
| 265. | A panel schedule **SHALL** be filled out. (Current edition of NFPA 70, Article 408.4) |
| 266. | All branch conductors **SHALL** be copper to reduce corrosion and impedance due to dissimilar materials. |
| 267. | Branch conductors **SHALL** have an allowable ampacity equal or greater to the non-continuous load plus 125% of the continuous load. (Current edition of NFPA 70, Article 210.19(A)(1) |
| 268. | A ground conductor of the same size as the current conductor **SHALL** be installed in all branch circuits. |
| 269. | Extension cords **SHALL** not be used to power permanent equipment. |
| 270. | All interior surface mounted building wiring **SHALL** be in rigid electrical metallic |

[46] In all cases, unless otherwise specified, the most current (as of buildout of the communication site) version of NFPA shall apply.

| | |
|---|---|
| | tubing (EMT) or raceways. (Current edition of NFPA 70, Article 358) |
| 271. | Conduit **SHALL** not be used as the AC equipment ground (ACEG) conductor. |
| 272. | A fused disconnect **SHALL** always be installed before all other panels and equipment, including a generator transfer switch. |
| 273. | The following are required thresholds when testing AC power quality in most single-phase and three-phase configurations (IEEE STD 1100-1999). The actual thresholds used **SHALL** be based on the installation requirements of the connected equipment, as the connected equipment may have more stringent requirements. See IEEE STD 1159-R2001 for additional information.<br>Phase Voltage Testing Thresholds<br>• Frequency Deviation **SHALL** not exceed ± 0.5 Hz<br>• High Frequency Noise **SHALL** not exceed approximately 1% of the phase-neutral voltage<br>• Voltage Sags **SHALL** be less than –10% of nominal supply voltage (108 V for a 120 VAC circuit)<br>• Voltage Swells **SHALL** not be more than +5% of nominal supply voltage (126 V for a 120 VAC circuit)<br>• Transients **SHALL** not exceed approximately 100 V over the nominal phase-neutral voltage<br>• Distortion **SHALL** not be more than 5% Total Harmonic Distortion (THD) – the voltage distortion level at which loads may be affected<br>Neutral-ground Voltage Testing Thresholds<br>• High Frequency Noise **SHALL** not exceed 2-3 peak volts<br>• Voltage Swells **SHALL** not exceed 1% to 2.5% of nominal phase-neutral voltage |
| 274. | Diverse and redundant power feeds delivered from a minimum of two different power systems from the utility **SHOULD** be considered for locations with extreme criticality affecting the operation of the network to ensure 99.999% availability of the network and applications. |

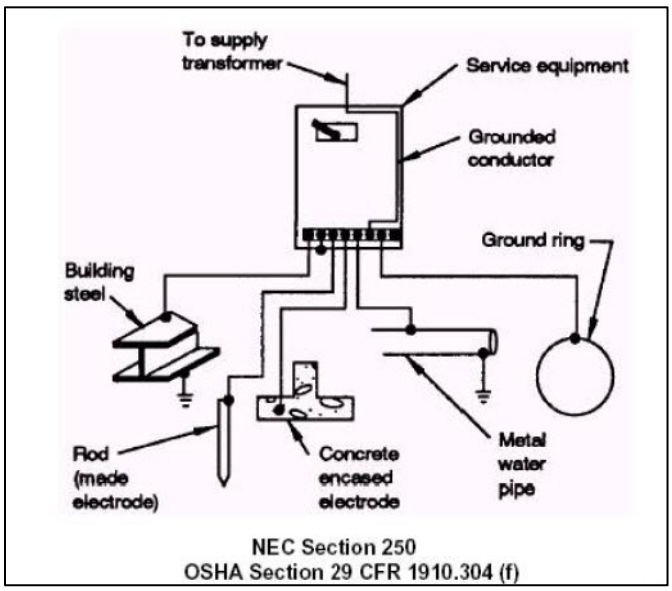



Figure 2: **General Communication System Electrical Diagram**[47]

### *9.6.6.2 Alternative Power Sources For Primary and Backup Power*

Sites without access to commercial AC power utilities can use solar and/or wind-generated power. The solar panels and/or wind generated charges batteries that provide power to site equipment. Propane or liquid natural gas (LNG) generators can be used, especially in colder climates, to back up the solar/wind system.

Because solar/wind systems provide limited power, it is important when planning the power system to calculate the predicted power usage for the site. Solar power is best suited for small sites with low power requirements where physical size and cost of the standalone power system does not become impractical. The site's transmitter duty cycles shall be planned so as not to exceed the maximum average current requirement.

"Wind generators can be used to back up a solar panel system. If there are sunless days with wind then battery charging can still take place. Such a system could take advantage of more sun in the summer and more wind in the winter. Wind generators should be mounted higher than buildings or other obstructions where wind flow is more efficient."[48]

Hydrogen fuel cells are a potentially viable option for backup power, particularly in the telecommunications sector. Traditional backup power technologies use batteries and generators that operate on diesel, propane, or gasoline. Most backup-power communication

[47] NFPA Section 250
[48] Motorola Standards and Guidelines for Communications Sites 9/1/05-UP), p 6-25.

and control systems use a combination of generators and batteries to provide redundancy and avoid service disruptions. Although these systems are reliable and well established, growing concerns about batteries and generators are motivating many customers to seek alternatives that provide high reliability and durability at reasonable cost. Compared with batteries, fuel cells offer longer continuous runtime and greater durability in harsh outdoor environments. And with fewer moving parts, they require less maintenance than generators or batteries. They can also be monitored remotely, reducing maintenance time. Compared with generators, fuel cells are quieter and have no harmful emissions. On a lifecycle basis, fuel cells can offer significant cost savings over both battery-generator systems and battery-only systems when shorter runtime capabilities of up to 72 hours are sufficient (fuel cell system costs for longer runtimes can be higher than incumbent technologies due to the cost of hydrogen storage tank rentals).[49]

| | |
|---|---|
| 275. | For solar or wind system battery storage **SHALL** be designed to supply adequate power to the site for sites without an additional alternative source (e.g., generator) of power to replace the primary power generation to deliver 99.999% availability given the expected weather conditions (i.e., as a function of the expected availability of sun and wind resources). |
| 276. | Solar panels **SHALL** be oversized by minimum 10% of calculated load. |

#### *9.6.6.3 Long-Term Backup Power Source*

There are a number of long term fixed and mobile backup power sources. This section addresses these units and fuel types available.

| | |
|---|---|
| 277. | Each site **SHALL** have ~~a~~ backup power generation with a power supply duration sized to power the site until it can be refueled to maintain 99.999% availability. |
| 278. | The fuel source for the generator **SHALL** be chosen to provide reliable generator operation given the site's climate and other environmental factors.[50] |
| 279. | Fixed generators with onsite fuel storage **SHALL** have an adequate sized storage to allow for the unit to operate at full load for the longest expected runtime given distance from supplies and the potential for transportation disruption during a disaster or power outage. |

[49] See http://www1.eere.energy.gov/hydrogenandfuelcells/applications.html

[50] Propane fuel is a clean independent fuel source. Liquid Propane Gas (LPG) is a good all-around fuel. Use of propane vapor must take into account fuel demand, ambient temperature, and tank size. These must be addressed due to the liquid to vapor conversion required and properties of the fuel based on the container and environment. Diesel and gaseous propane are not well suited for colder environments; however, they may be the most appropriate fuel for other climates. Gasoline is a poor fuel due to the high flammability and limited storage life.

| | |
|---|---|
| 280. | System(s) **SHALL** have adequate capacity to carry ALL loads at full capacity when sizing the long-term power source equipment. |
| 281. | System(s) **SHOULD** have adequate capacity to carry ALL loads at full capacity plus 30% expansion factor when sizing the long-term power source equipment. |
| 282. | When sizing long-term power source equipment, derating per manufacturer's specifications **SHALL** be calculated for altitude, installation location, voltage/phase configuration, and fuel and load type. |
| 283. | Based on the environmental characteristics of a site, generators and fuel storage **SHALL** be located in an area protecting it from flooding and should address other physical hazards: blowing derbies, falling ice, and frequent extreme weather. |
| 284. | In areas prone to seismic activity fuel lines and connections **SHALL** meet local seismic codes for the fuel type utilized. |
| 285. | Generators **SHALL** be equipped with an engine high temperature and low oil pressure alarm/shutdown. |
| 286. | The capability to view oil pressure and engine temperature **SHALL** be installed on generator. |
| 287. | Voltage, amperage, and frequency meter(s) **SHALL** be installed either at the generator, transfer switch or both. |
| 288. | Any additional alarms or indicators **SHOULD** be considered to provide early detection of impending issues. |
| 289. | Engine, stator, control panel, and battery heaters **SHOULD** also be considered on the location of the unit. |


Figure 3: **Power System with Automatic and Manual Transfer Switch**

### *9.6.6.4 Transfer Switch*

Transfer switches utilized in the network will be automatic for fixed auto start generators and manual for generators that deploy to a site.

| | |
|---|---|
| 290. | **SHALL** have a rating equal or greater to the circuits being transferred. |
| 291. | Surge protection **SHALL** be installed to protect the automatic transfer switch. |
| 292. | A manual transfer switch **SHALL** be utilized for supplying standby power as a primary backup source at non-fixed generator sites and **SHALL** be installed as a secondary source to the fixed automatic start generator system. |
| 293. | A secondary electrical connection **SHALL** be installed with manual transfer switch applications on the exterior of the shelter. An “Appleton” type power connection **SHALL** be included at every site that is physically capable of utilizing a transportable generator to facilitate safe, effective, and efficient secondary backup power. |

Figure 4: Appleton Style Power Connection[51]

### 9.6.6.5 *Uninterruptible Power System (UPS)*

Uninterruptible Power Systems (UPS) are defined as those that produce alternating current (AC) output and include backup battery power. UPS systems are not required in all sites (alternative architectures could be used whereby the power system remains in direct current (DC) and does not include the additional conversion back to AC. However, when employed the following requirements define public safety grade sites. UPS systems are typically intended to provide short-term power to specific loads when there are transient disruptions or short-term power outages. Thus UPS system(s) are typically intended to provide transition power between power loss and generator online.

| | |
|---|---|
| 294. | When utilizing a UPS system(s), two distinct power panels **SHALL** be utilized, an equipment panel (UPS Panel board) and Utility Power Panel. |
| 295. | UPS system **SHALL** deliver a true sinusoidal output. |
| 296. | Since units are typically used for "short-term" operation backup time is usually less than what a rectifier system typically is designed for. The unit(s) ability to perform in an "extended run-time" scenario **SHOULD** be considered in the design. |
| 297. | The UPS **SHALL** be capable of dry contact alarms as well as SNMP to identify the following alarm conditions: minor, running on inverter, pre-low battery, pre-low runtime, internal temperature, major, low batter, and low runtime. At a minimum minor and major **SHALL** be available. |
| 298. | Recharge time for fully a fully discharged battery array **SHALL** be no more than 12-16 hours for sealed lead acid. |
| 299. | A bypass shall be installed for UPS systems in the event of equipment failure, power maybe restored to the system(s) by bypassing the equipment. A make-before-break **SHALL** be utilized unless it is not approved by UPS manufacture due to power configuration |

[51] Image provided by Chris Kindelspire with permission.

Figure 5: **Bypasses: Make-before-break (left) and Online Double Conversion (right)**[52]

### *9.6.6.6 Rectifier System*

The following section addresses the rectifier requirements for public safety grade sites. These requirements apply to "DC only" sites, whereby a UPS is not used. In other words, these requirements apply in those situations where Alternating Current is converted to Direct Current by the Rectifier System and the power is not inverted back to Alternating Current to power the electronic systems. Therefore, these rectifier requirements do not apply to the rectifiers that would be part of a UPS system.

| | |
|---|---|
| 300. | All direct current (DC) equipment **SHALL** be powered via n+ 1 redundant rectifier whereby one additional rectifier beyond the required number to meet the load is included. |
| 301. | UL-listed General Use or battery cable **SHALL** be used in DC systems. |
| 302. | Overcurrent protection **SHALL** be 50% larger than calculated load but not larger than the conductors rating. Conductors **SHALL** be based on their calculated load requirements and current carrying capacity. |
| 303. | DC systems incorporating a battery backup **SHALL** be equipped with a Low Voltage Load Disconnect (LVLD). A Low Voltage Battery Disconnect (LVBD) **SHALL** not replace or be substituted for the LVLD. |
| 304. | The rectifier system **SHALL** be capable of dry contact alarms and/ or SNMP to identify the following alarm conditions: Over and under charging alarms. |

[52] Images provided by Chris Kindelspire with permission.

### 9.6.6.7 Batteries

These battery requirements do not apply in situations where a UPS is used. They apply in situations whereby once power is converted to DC via a rectifier system, it remains in DC to power the electronic systems. Batteries used fall into two categories: flooded cell (wet) and valve regulated (sealed). Wet cell batteries pose a greater hazard vs. sealed batteries due to hydrogen gas being emitted during operation. Sealed Absorbed Glass Mat (AGM) batteries are preferred however, if wet cell batteries are utilized the following must be addressed.

| | |
|---|---|
| 305. | Battery system **SHALL** be designed to allow technicians to respond to the site after an outage. Running on battery operation at 100% load **SHALL** be utilized for calculating the runtime to maintain 99.999% availability when designing the battery system. Systems are typically designed for a technician response of 2 hours for urban locations, 4 hours or more for rural location and 8 hours are typical for private cellular carriers. |
| 306. | Batteries having been discharged bellow full charge **SHALL** be fully recharged within 24 hours. |

### 9.6.6.8 Grounding Requirements

| | |
|---|---|
| 307. | Master Ground Bus (MGB) **SHALL** be the focal point for all grounds systems of the building or cabinet(s). Connections to the MGB **SHALL** be arranged utilizing the configuration in the figure below within this section. |

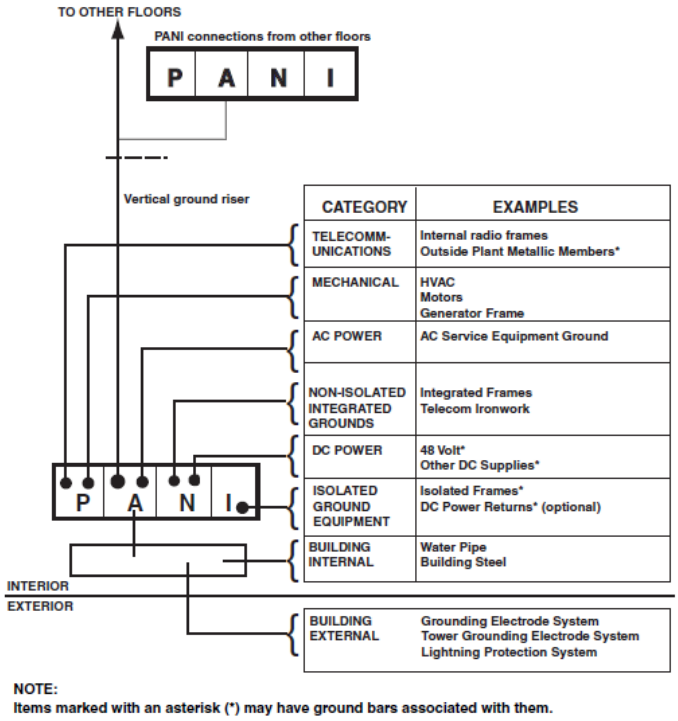



Figure 6: **Typical MGB Connection Configuration**[53]

### *9.6.6.9 Surge Protection Devices*

| | |
|---|---|
| 308. | Six major performance characteristics that **SHALL** be considered when selecting the proper surge device are: response time, voltage protection level (VPL), power dissipation, disturbance-free operation, reliability, and operating life. |
| 309. | SPDs **SHALL** be required on all power feeders to and from communications facilities. |
| 310. | All devices **SHALL** be installed per the manufacturer's installation instructions. |
| 311. | The facility grounding and bonding systems **SHALL** be properly implemented to help ensure that the electrical service, all surge suppression devices, and the communication system components within the equipment area are at the same ground potential. This is critically important to help ensure maximum safety of personnel and maximum effectiveness of the SPDs. |
| 312. | The SPDs **SHALL** be installed within the equipment shelter, room, or area to achieve maximum effectiveness. |
| 313. | Installation at locations away from the equipment area **SHALL** NOT be performed, as it reduces the effectiveness of the SPD. |
| 314. | SPDs **SHALL** be mounted as closely as possible to point of protection. Lead lengths shall be as short as possible and direct to avoid an increase in a |

[53] Source: Standards and Guidelines for Communications Sites, Motorola Solutions, Inc., 9/1/05, p 5-37

| | |
|---|---|
| | suppressor's response time and protection level. |
| 315. | Multiple surge protection devices **SHALL** be installed to reduce transient overvoltage. |
| 316. | The SPD **SHALL** include a set of form "C" dry contacts, rated at a minimum of 250 VAC, and a minimum of 2.0 amperes, with a power factor of 1.0, for remote alarm reporting capability. This set of contacts **SHALL** operate when there is an input power failure or the integrity of any module has been compromised. This contact set **SHALL** be isolated from the AC power circuitry to safeguard the alarm circuit or reporting device should there be a catastrophic event. Connection to the remote monitoring contacts of the SPD shall utilize 0.34 mm2 (#22 AWG) or coarser conductors. |
| 317. | All sites **SHALL** have a Type 1[54] SPD that provides protection for the service entrance, and all branch panel locations within the same equipment room. |
| 318. | If a generator and transfer switch is used, a Type 2[55] SPD **SHALL** be installed on the panel board before the transfer switch and a Type 1 SPD **SHALL** be installed on the panel board after the transfer switch. |
| 319. | Type 3[56] SPDs **SHALL** be utilized when equipment is at a distance of greater than 10 conductor feet from the panel board. |

#### *9.6.6.9.1 Types 1, 2, and 3 Surge Protection Devices*

The following requirements provide the unique requirements for Type 1, Type 2, and Type 3 Surge Protection Devices. These requirements are provided courtesy of Motorola Solutions, Inc.[57]

##### *9.6.6.9.1.1 Type 1:*

Type 1 SPD provides protection for the service entrance, and all branch panel locations within the same equipment room. The requirements are as follows:

| | |
|---|---|
| 320. | The SPD **SHALL** be a permanently connected, one-port, or parallel configuration. |
| 321. | The suppression components **SHALL** be voltage limiting type. Voltage switching components **SHALL** not be utilized as a suppression element in the SPD. |
| 322. | All suppression modules **SHALL** be installed from each phase conductor to the neutral conductor (L-N, Normal Mode). |

[54] Specific Type 1 SPD requirements are provided below.
[55] Specific Type 2 SPD requirements are provided below.
[56] Specific Type 3 SPD requirements are provided below.
[57] See Motorola 56 from pp 7-29 through 7-31

| | |
|---|---|
| 323. | Suppression modules or devices of any type **SHALL** NOT be connected between any phase conductor and the equipment grounding conductor or ground (L-G, Common Mode Neutral to Ground). |
| 324. | The primary module(s) **SHALL** consist of a SAD module(s) providing 20KA per phase, per polarity, minimum energy absorption. |
| 325. | The secondary module(s) **SHALL** consist of a Metal Oxide Varistor (MOV) module(s), with sufficient energy handling capability to meet the maximum discharge current requirement of 160 kA per mode. |
| 326. | The minimum pulse life or durability requirements and the voltage protection level **SHALL** be as specified in Table 7-4 for the respective Maximum Continuous Operating Voltage (MCOV) listed. |
| 327. | SPD **SHALL** be properly selected based on the operating voltage and number of phases of the circuits to be protected. |
| 328. | Each module or subassembly **SHALL** be modular in design to allow for easy field replacement. |
| 329. | The SPD **SHALL** use integral over-current protective devices, and the SPD **SHALL** have a short circuit current rating of 25,000 amperes or larger, as defined by UL 1449, second edition, Section 39. |
| 330. | The SPD **SHALL** have a nominal discharge current of 10,000 amperes, as defined, and tested by IEEE (IEEE C62.45-2002) waveform characteristics (Category C high 10 kA 6kV minimum) SPD tested in accordance with IEEE C62.45-2002. |
| 331. | The SPD **SHALL** have a voltage protection level (at the nominal discharge current of 10,000 amperes) of 600 Vpk or less from each phase-to-neutral mode, when tested in accordance with IEEE C62.45-2002. Test points are measured using specified conductor size at a distance of 150 mm (6 in.) outside of the enclosure. |
| 332. | The SPD **SHALL** have a Suppressed Voltage Rating (SVR) of 330 Vpk, as determined by testing in accordance with UL 1449, second edition, Section 34. |
| 333. | The SPD **SHALL** have a maximum discharge current of 160 kA per mode, as tested in accordance with IEC 61643-1 |
| 334. | The enclosure rating of the SPD **SHALL** be NEMA 4. |
| 335. | The maximum dimensions of the enclosure **SHALL** be 406 mm × 406 mm × 228 mm (16 in. × 16 in. × 9 in.) for single-phase, 3W+G configurations, and 508 mm × 508 mm × 228 mm (20 in. × 20 in. × 9 in.) for three-phase wye. |
| 336. | 4W+G configurations. The maximum weight of the SPD **SHALL** be 13.6 kg (30 lb.), and 18 kg (40 lb.) respectively. |

| | |
|---|---|
| 337. | The environmental parameters of the SPD **SHALL** be as follows:<br>Operating temperature range: -40 °C to +65 °C<br>Storage temperature range: -40 °C to +65 °C<br>Operating humidity range: 0-95%, non-condensing<br>Altitude range: -152.4 m to 4572 m (-500 ft. to +15,000 ft.) |
| 338. | Connection to the SPD **SHALL** be conducted with a wire range of 16 mm2 csa (#6 AWG) or coarser. |
| 339. | Per NFPA 70, Article 110, the conductor size **SHALL** match the breaker size. |
| 340. | Each SPD **SHALL** have indicator lamps on or visible from the front of the device showing that power is applied and that the protection integrity has not been compromised. |
| 341. | The SPD **SHALL** be UL 1449, 2nd Edition listed, and tested to clause 7.10. A test report from a Nationally Recognized Testing Laboratory (NRTL), NAVLAP or A2LA, or a Certified UL client testing data laboratory detailing the procedures used, and the results obtained **SHALL** be made available. |

#### *9.6.6.9.1.2 Type 2:*

Type 2 SPDs provide protection for the service entrance locations within the same equipment room. The requirements are as follows:

| | |
|---|---|
| 342. | The device **SHALL** consist of primary modules using MOV technology. |
| 343. | The SPD **SHALL** be a permanently connected, one-port or parallel configuration. |
| 344. | The suppression components **SHALL** be voltage limiting type. Voltage switching components **SHALL** not be utilized as a suppression element in the SPD. |
| 345. | All suppression modules **SHALL** be installed from each phase conductor to the neutral conductor (L-N, Normal Mode). |
| 346. | Suppression modules or devices of any type **SHALL** NOT be connected between any phase conductor and the equipment grounding conductor or ground (L-G, Common Mode Neutral to Ground). |
| 347. | The primary module(s) **SHALL** consist of a Metal Oxide Varistor (MOV) module(s), with sufficient energy handling capability to meet the maximum discharge current requirement of 160kA per mode. |
| 348. | The minimum pulse life or durability requirements and the voltage protection level **SHALL** be as specified in Table 7-4 for the respective Maximum Continuous Operating Voltage (MCOV) listed. |
| 349. | SPD **SHALL** be properly selected based on the operating voltage and number of phases of the circuits to be protected. |
| 350. | Each module or subassembly **SHALL** be modular in design to allow for easy field replacement. |

| | |
|---|---|
| 351. | The SPD **SHALL** use integral over-current protective devices, and the SPD **SHALL** have a short circuit current rating of 25,000 amperes or larger, as defined by UL 1449, second edition, Section 39.3. |
| 352. | The SPD **SHALL** have a nominal discharge current of 10,000 amperes, as defined, and tested by IEEE C62.45.2-2002 waveform characteristics (Category C high 10 kA 6 kV minimum) SPD tested in accordance with IEEE C62.45-2002. |
| 353. | The SPD **SHALL** have a voltage protection level (at the nominal discharge current of 10,000 amperes) of 800Vpk or less from each phase-to-neutral mode, when tested in accordance with IEEE C62.45-2002. Test points are measured using specified conductor size at a distance of 150 mm (6 in.) outside of the enclosure. |
| 354. | The SPD **SHALL** have a Suppressed Voltage Rating (SVR) of 400 Vpk, as determined by testing in accordance with UL 1449, Second Edition, Section 34. |
| 355. | The enclosure rating of the SPD **SHALL** be NEMA 4. The maximum dimensions of the enclosure **SHALL** be 406 mm × 406 mm × 228 mm (16 in. × 16 in. × 9 in.) for single-phase, 3W+G configurations, and 508 mm × 508 mm × 228 mm (20 in. × 20 in. × 9 in.) for three-phase wye, 4W+G configurations. The maximum weight of the SPD shall be 13.6 kg (30 lb.), and 18 kg (40 lb.) respectively. |
| 356. | The environmental parameters of the SPD **SHALL** be as follows:<br>Operating temperature range: -40 °C to +65 °C<br>Storage temperature range: -40 °C to +65 °C<br>Operating humidity range: 0-95%, non-condensing<br>Altitude range: -152.4 m to 4572 m (-500 ft. to +15,000 ft.) |
| 357. | Connection to the SPD **SHALL** be conducted with a wire range of 16 mm2 csa (#6 AWG) per NFPA 70-2005, Article 110 the conductor size must match the breaker size. |
| 358. | Each SPD **SHALL** have indicator lamps on or visible from the front of the device showing that power is applied and that the protection integrity has not been compromised. |
| 359. | The SPD **SHALL** be UL 1449, 2nd Edition listed, and tested to clause 7.10. A test report from a Nationally Recognized Testing Laboratory (NRTL), NAVLAP or A2LA, or a Certified UL client testing data laboratory detailing the procedures used, and the results obtained shall be made upon request. |

#### *9.6.6.9.2 Type 3:*

Individual equipment SPDs are available in many varieties. These may be wire-in receptacle outlet replacement types, plug-in adapters, or receptacle outlet panels or strips. General requirements are as follows:

| | |
|---|---|
| 360. | All individual equipment devices **SHALL** provide Normal Mode (L-N) circuit protection. |

| | |
|---|---|
| 361. | Common Mode (L-G) circuit protection **SHALL** NOT be permitted. |
| 362. | Individual devices with the plug manufactured as a combined part of the device **SHALL** be designed to be plugged into a single simplex receptacle outlet and shall incorporate a single simplex receptacle outlet for the load connection. Individual plug-in units with a duplex receptacle outlet **SHALL** NOT be used. |
| 363. | Multi-receptacle outlet strip devices, if used, **SHALL** incorporate an independent ground point on the exterior of the device. This attachment point or stud shall be suitable for attachment of a lug sized for a 16 mm2 csa (#6 AWG) conductor. |
| 364. | Multi-receptacle device housings, if used, **SHALL** be metallic and **SHALL** be provided with mounting ears, tabs, or brackets. Devices may be suitable for standard EIA 483 mm (19 in.) rack mounting. |


Figure 7: **Surge Protection Devices: Type I (left), Type II (right), and Type III (bottom)**

### *9.6.6.10 Power Redundancy*

| | |
|---|---|
| 365. | Each major piece of equipment **SHALL** have its own dedicated individual branch circuit with proper over current protection. |
| 366. | Power system **SHALL** be designed as a redundant N+1 – Parallel (System) to ensure that an uninterruptible power supply (UPS) or rectifier system is always available. N+1 stands for the number of modules that are required to handle an adequate supply of power for essential connected systems, plus one more. |
| 367. | Automatic Transfer Switch power strip / power distribution unit. The ATS **SHALL** have two power cords, allowing it deliver a dual-circuit power supply. This makes it possible to keep the devices running by automatically switching over to a second power supply system if a fault occurs with the first power supply system. Input cords support connection to separate primary and secondary power sources providing redundant power for single-corded device(s). |

## 9.7 Carrier Hardening Practices

### 9.7.1 Objective and Scope

The major commercial cellular carriers were surveyed to determine their practices related to site hardening. This was done in order to understand the level of hardening generally provided by the carriers at commercial sites that might become target sites for the NPSBN and to determine the differences between the common hardening practices used by the commercial carriers and the hardening requirements established by public safety.

The responses from the carriers have been analyzed and will be reported as common trends and practices. No specific carrier practices are identified and no comparison among the carriers has been performed.

### 9.7.2 Physical Security

#### *9.7.2.1 Identify Physical Assets and Demarcation Points*

Carrier physical assets are designed based on site type (outdoor ground, roof-top, building enclosed) and usually demarcated by carrier. For outdoor compound-type sites, individual carrier assets are often denoted through explicit lease or ownership areas on the compound ground that include poured or pre-formed concrete pad or raised-steel/aluminum grid platforms for enclosed equipment. Other carriers utilize various forms of enclosed, walk-in shelters that contain only the carrier's equipment.

Demarcation points, other than physical separation, are usually related to utilities, grounding, and RF cable runs. Power and telephone utilities prefer to use a common "distribution" system for the site and are best envisioned as a star configuration from the single utility access at the site to each carrier. Individual power meter bases in multi-base "H posts" distribute power and unique telephone demarcation points for each carrier. Space constraints at rooftop and inside-building installations sometimes force utility sharing of single power and telephone. In this configuration, a lead carrier or agency at the site sometimes assumes all utility costs and then sub-charges each "co-locator."

#### *9.7.2.2 Securing Site Perimeter and Site Access*

Site perimeter security configurations are highly dependent on site type and local jurisdictional restrictions; i.e., some locales won't allow razor wire or even barbed wire on top of fences. Outdoor ground sites most often utilize varying styles and height of chain-link fence; some with top barb wire. Variations of fencing, sometimes required by ordinances or property owners,

may include screening for limited visibility and shrubs outside the fence. Depending on location, some sites are enclosed by brick, block, or aggregate concrete walls. Rooftop and inside sites often have less secure perimeters but the building or rooftop access itself provides a level of site perimeter away from normal building occupants.

Sites are more often being monitored electronically with cameras and motion-sensing devices. A site leasing company may purchase service-based monitoring or individual carriers with high-speed connections and network operations centers may monitor their own assets within the compound.

Access to sites is tempered between security and ease of access to equipment for maintenance and repairs. Outdoor ground sites typically use a master gate, most often sized and located for vehicle access into at least a portion of the compound. A chain or bar lock system allows installation of individual locks and access to each carrier into the site. For inside and rooftop sites, access may be restricted by security doors, locks, lockout steps, and ladders and may include escort by security guard.

#### *9.7.2.3 Securing Service Demarcation Points, Antenna Structures, Cables, and Pipes*

Securing these points and devices are challenging as they are both individual to each system but essentially shared by all carriers on site. Utility demarcations at outdoor ground sites are often achieved with underground conduits from the utilities to each carrier. Some level of security for inside and rooftop sites are achieved by conduit and waterproof protection.

Antenna structures and cables are most susceptible by the nature of their location in the open, be it outdoor or internal antenna systems. They are especially vulnerable to influences outside of the site that can be minimally controlled. Cable theft is prominent. Carriers are beginning to use alternative dielectric cables to deter theft while maintaining acceptable conductivity characteristics. Cables and chases are also being enclosed and locked to reduce potential theft. The added benefit is protection from accidental damage by others working on site.

#### *9.7.2.4 Securing On-Site Fuel Storage*

Many carriers traditionally have not utilized power plants utilizing fuel, which eliminates the need for fuel storage. Changes in philosophy for longer-term power backup and affordability for on-site generators drive the need for development or modification of fuel storage. Fuel storage security is primarily driven by the design of the site equipment. Carriers mention inside and rooftop owners rarely allow or accommodate fuel storage because of fire and life hazards. For ground sites, the most secure configuration desired by carriers is a generator integrated into a

hardened shelter that also includes the fuel storage in the shelter, reducing the possibility of tampering and theft. Outside fuel storage poses a more significant security risk simply by exposure to outside influence. Affordability, storage space, ordinances, or site requirements and vendor access are mentioned as challenges for outside storage of fuel.

#### *9.7.2.5 Securing On-Site Generator, Battery Plant, and other Power Sources*

As with fuel storage for generators, significant storage battery plants and alternative/backup power sources are not the mainstay for many carriers; primarily for cost reductions in extremely competitive markets. Small, equipment-enclosure-only sites usually have some battery backup to accommodate up to 8 hour primary power disruptions with connection capabilities for non-dedicated deliverable generators. Other carriers, primarily those using larger shelters, commit space for larger uninterruptable power supply (UPS) arrays as well as generators/fuel storage. These sites can be self-sustainable for days to weeks depending on the size of on-site fuel storage. Inherently stored inside the shelter, the backup power plants have essentially the same site security as the RF system electronics.

A new trend is to locate generators and fuel storage on top of a hardened shelter building. This reduces the lease "footprint" that results in lower lease costs. The downside is less secure equipment that is exposed to the elements, theft, and less visual appeal of sites. Nonetheless, carriers view the cost of lease ground space as a very real and sometimes unaffordable systemic cost that inhibits generators or any significant means of backup or alternative powering. They are finding unique solutions like this to enable capabilities for backup powering but some fall short of PSG best practices for power plant robustness, diversity, and longevity of operation.

Lastly, some carriers are investigating the possibility of alternative power sources including solar and wind power plants to charge battery arrays. Most carriers are at a significant advantage to public safety systems as their equipment typically uses less power. This leads to more options and relatively smaller power plants than most public safety systems. They also reason that (more) modern carrier electronics consume even less power and can be served by alternative power plants that are becoming more affordable. Lower total cost of ownership over the equipment life with less maintenance than fossil fuel power sources are cited. One carrier sites the transition to "green energy" as a corporate culture influence. Carriers report the most likely "hardened" alternative/backup power is solar.

#### *9.7.2.6 Securing On-Site Electronics Shelters and Enclosures*

Securing electronic equipment enclosures is admittedly a carrier weakness. Enclosure security is often limited to a single "equipment" style key that is common among the industry's

enclosures. This would be akin to a common public safety radio equipment key in hand by a plethora of individuals. Carriers have contracted with equipment enclosures to utilize carrier-specific key locks but still, keys are common, can be easily duplicated, and locks are still easy to pick. Enclosures, while known for being waterproof, have no significant, system-locking mechanisms.

Carriers using hardened shelters use much more robust and elaborate systems to security electronics. Some use door keys while others utilize alphanumeric combination or credentialing card access systems. Access cards systems are sometimes tied into the site security electronics, which report back to the carrier network operations center for real-time credential or logging.

A notable observation is some carriers using equipment level security. As systems become more reliant on software operating systems, access controls for electronics are embedded with user logins and various levels of access based on specific users. While this security is more about access control for known users and does not prevent the proverbial "pulling the plug" by a would-be system assailant, the concept does provides a new type of electronics "hardening" for the inadvertent, errant configuration change that can render a site inoperable.

### 9.7.3 Antenna Support Structure Design

#### *9.7.3.1 New Antenna Support Structure Design*

When designing a new antenna support structure, the factors that must be considered by any system operator include: the load to be carried by the antenna support; the amount of wind the antenna support will be exposed to; whether the antenna support will be exposed to icy conditions and to what degree; and whether the antenna support will be exposed to earthquake conditions and to what degree.

With the most recent revision to the antenna support structure standard TIA-222-G: "Structural Standard for Antenna Supporting Structures and Antennas," recommendations for these factors are well defined. The factors are based on the region of the country in which the antenna support will be built and also a number of characteristics to be chosen or defined by the designer. The primary characteristics are tower classification, exposure category, and topographic category.

#### *9.7.3.2 Antenna Support Structure Classification*

The classification of the structure is the most important of these. The classification of the tower results in specific adjustments to be made to the wind, ice, and earthquake loading of the tower based on the reliability requirements of the application. Three classifications have been

established based on the type of service provided and on the structure's potential hazard to human life and property. Class I is the lowest class level and it is used for structures that either, because of the use or location, represent a low hazard to human life and damage to property in the event of failure and/or are used for services that are optional and/or where a delay in returning the services would be acceptable. Class II is considered the default classification and is used for structures where the use or location represent a substantial hazard to human life and/or damage to property in the event of failure and/or are used for services that may be provided by other means. Finally, Class III is the highest class level and is used for structures where the use or location represent a high hazard to human life and/or damage to property in the event of failure and/or are used primarily for essential communications.

Wind, ice, and earthquake loading progressively increase from Class I to Class III levels. Specifically, Class I loading characteristics do not apply any ice loads or earthquake analysis and reduce the applied wind load by 13 percent. Class II loading does include ice loads and earthquake considerations and uses the nominal wind loads for its region. Class III loading characteristics are the most severe and specify an increased ice thickness of 25 percent, 15 percent more wind load applied to the structure, and a 50 percent increase in the earthquake load in the regions subject to this hazard.

#### *9.7.3.3 Antenna Support Structure Exposure Category*

A structure's exposure category reflects the amount of "ground surface irregularities" in the vicinity of the planned structure. Exposure categories are used to adjust wind loading based on the type of terrain surrounding a site. Reduced wind loads are associated with rougher terrains that tend to slow the wind down. Three exposure categories have been defined based on terrain variations. Wind loading is increased as the exposure designation changes from Exposure B (roughest terrain) to Exposure D (smoothest terrain). Specific definitions of these exposure categories are provided in the standard. The default exposure category is C.

##### *9.7.3.3.1 Topographic Categories*

Topographic categories are used to determine increases in wind loading for sites located on hills and other elevated locations (other than buildings). The shape and relative height (topography) of an elevated site determines the increase in wind load. The intent of the standard is to allow the structure designer to classify the structure site into one of the standard four topographic categories (1 – 4), with a fifth category (Topographic Category 5), which can be used for specific wind speed-up criteria. The default topographic category is 1, which refers to no abrupt changes in general topography.

#### 9.7.3.4 Approach to Structure Design

Based on the organization of TIA-222-G, today's approach to the design of antenna support structures generally consists of defining the intended use (class) and specifics related to its planned site location as described above. The parameters and guidelines defined with the standard are then used to establish specific design criteria. The resulting process defined by the standard also takes into account regional considerations and the various types of environmental hazards that a structure may be subject to in different parts of the country.

Commercial service providers generally define their antenna support structures to be Class II structures, which is the default classification. However, when public safety or emergency services installations are added to commercial towers, this justifies the reclassification of the structure to the more stringent Class III.

With respect to the exposure and topographic categories, commercial service providers generally specify the exposure and topographic categories based on the specifics of the location. However, some carriers include the exact latitude and longitude of the proposed tower and require the tower vendors to review the location and confirm or revise the exposure, topographic categories, and also determine if any uplift (wind speed-up) is needed before submitting their quote.

#### 9.7.3.5 Existing Antenna Support Structures

For existing structures, commercial service providers will perform a structural analysis to analyze the structure similar to public safety agencies. Most state and local codes require that the structure be analyzed according the antenna support structure standard TIA-222-G, as discussed above. The standard states that, as a minimum, existing structures shall be analyzed in accordance with this standard, regardless of the standard used for the design of the original structure, under any of the following conditions:

a) A change in type, size, or number of appurtenances such as antennas, transmission lines, platforms, ladders, etc.
b) A structural modification, excepting maintenance, is made to the structure;
c) A change in serviceability requirements;
d) A change in the classification of the structure to a higher class.

#### 9.7.3.6 Other Structure Types

Where practical, commercial service providers will utilize antenna support structures other than towers, such as water tanks; billboards; smokestacks; power line support structures, etc.

These items are typically handled by performing a structural analysis whenever possible, similar to existing tower structures.

#### *9.7.3.7 Guidelines for Communications Sites Construction*

Most commercial services providers follow their own standards for grounding and local building codes for construction. One carrier interviewed uses a typical ground ring with multiple grounding rods, all connected together. The fencing around the site is also grounded.

#### *9.7.3.8 Lightning Protection and Grounding*

One carrier that was surveyed uses in-line surge arrestors on hybrid cables but grounding only on coax cables.

### 9.7.4 Equipment Enclosures

#### *9.7.4.1 Shelters*

The practices for the use of equipment shelters vary among the commercial carriers. Some of the carriers generally use concrete aggregate buildings similar to public safety shelters. Others have fewer specific requirements for shelter design and in some cases only use shelters when they have a site with a large installation. These carriers tend to use outdoor equipment cabinets where possible.

#### *9.7.4.2 Cabinets*

As stated above, some carriers prefer to use equipment shelters whenever possible. These shelters are generally provided by the equipment manufacturer and are designed to commercial environmental standards.

### 9.7.5 Environmental and Climate Control

#### *9.7.5.1 Structure Type: Ground-Based Shelters*

Environmental and climate control systems for ground-based shelters typically consist of two units configured for redundant operation. Each unit is sized to handle the entire anticipated cooling and/or heating requirements. Reserve capacity is not stated, but is believed to be between 25 percent and 50 percent of initial requirements.

#### 9.7.5.1.1 Structure Type: Cabinets

Environmental and climate control systems for cabinets are typically provided by the vendor as a component of the cabinet mounted site equipment. Reserve capacity is not stated, but is thought to be minimal.

#### 9.7.5.1.2 Structure Type: Rooftop Shelters (Lightweight)

Environmental and climate control systems for rooftop shelters typically consist of two units configured for redundant operation. Each unit is sized to handle the entire anticipated cooling and/or heating requirements. Reserve capacity is not stated, but is believed to be between 25 percent and 50 percent of initial requirements.

#### 9.7.5.1.3 Structure Type: Building Room Build-out

Carriers typically prefer to use the same standard environmental and climate control systems for the build-out of interior rooms of existing facilities, if possible.

### 9.7.6 Power

Power systems for carriers, tower companies, or integrators are being surveyed to identify their power requirements, specifications, and best practices. Additionally, we want to understand if they treat sites and zones across the nation identically. Specifically, do they have different power requirements for high-traffic sites, critical geographic areas, or areas that are more susceptible to severe weather conditions? One carrier has indicated that it does not have different requirements on a site-by-site basis but provides battery backup and generators wherever possible.

#### 9.7.6.1 Power Loads

Carriers will be surveyed to determine if they have any specific mechanisms or analysis to determine what types of loads they assume for each site. One carrier reported that it typically specifies 120/240V (or 110/280V), single phase, 3 wire, 200 Amp service with a load of approximately 150A (37KVA).

#### 9.7.6.2 Long-Term Back-up Power Sources

Carriers often use batteries in addition to generators for backup sources. These generators are to keep the site running for indefinite periods until power is restored. Since a generator requires fuel, carriers need to define any deployment strategies or service level agreements to ensure sufficient fuel is available at sites to keep the generators running.

One carrier stated that it has provisioned generators at all sites in Virginia unless space or access is an issue. They indicated that they nominally run generators as long as required until power is restored but have no specific duration. Also, they have service providers that are contracted to refueling generators as needed but do not have any firm service level agreements to meet any stringent outage requirements.

Another carrier indicated that it generally does not provision generators at every site, but will transport generators to the more important sites during extended outages such as those resulting from hurricanes or other major disasters.

#### *9.7.6.3 Generator Specifications*

Carriers must be surveyed to determine the specifications and requirements for generators including power output, fuel tank and monitoring requirements.

One carrier stated that generators used are sound attenuated 50-80KW diesel (LP and Natural Gas are options) "genset" with double-walled 225 Gal fuel tank integral to genstand. Generators can be placed either indoor or outdoor based on the specific shelter used. The generator's status and conditions are electronically monitored and alarmed to on/off, operating temp, battery condition, fuel status, etc. Where generators are used, they are typically "exercised" once a week at a set time and day. Carriers also have suppliers to ensure that generators are fueled as needed but do not have any specific service level agreements. Suppliers have to coordinate access or have agreements on how to access the generators for service.

Suggested specifications:

a. 120/240 VAC, Single-Phase, Three –wire, 60 Hertz (HTZ).
b. Full single-phase output @ 1.0 Power Factor (PF).
c. Voltage regulation +/- 2% of rated voltage for constant load between no-load and full-load.
d. Frequency regulation 0.5 % from steady CBP no-load to steady CBP rated-load.
e. Single Step Load Pick up 100% of rated output power, less applicable derating factors, with the engine and generator at operating temperature.
f. Integral Underwriters Laboratories listed, thermal-magnetic type rated, main output circuit breaker.
g. Gauges and meters: The unit shall be equipped with the following: Oil pressure gauge, Temperature gauge, Charge rate ammeter, run time meter, Output-frequency meter.
h. Condition indicators: The unit shall be equipped with the following: Oil pressure gauge, Temperature gauge, charge rate ammeter, run time meter, Output-frequency meter.

i. Remote Monitoring capabilities from a central Network management system (e.g., SNMP or NO/NC): The unit shall be equipped with the following alarms: Low oil pressure indicator, Low oil level, Low fuel tank, High temperature, shutdown conditions (Over Crank, Over Speed, Under Speed, Low oil/pressure, High temperature, Oil pressure, fail to start.

j. Remote activation/deactivation (Run/Stop, Fault reset and Over Crank shutdown).

#### *9.7.6.4 UPS/Battery and Rectifier*

Carriers must be surveyed to determine how long a site can run with just battery backup and requirements for batteries and chargers and rectifiers.

One carrier reported that they provide for 8-hour minimum operation with battery backup.

Another carrier indicated that they research the typical power outage duration for a particular site and size their battery backup to meet that typical timeframe. This is generally just a couple of hours, but could be up to 12-15 hours.

Battery conditions are monitored (on site and remotely) through the battery charger and rectifier. The battery charger/rectifier can be serviced without interruption to load and equipped with fuses, circuit breakers and disconnect hardware. The system should provide both visual indications and remote management for rectifier failure, AC fail, fuse alarms, and low voltage disconnect.

#### *9.7.6.5 Transfer Switch*

Transfer switches allow switching between power sources (e.g., battery, generator and utility based power).

One carrier reported they use the transfer switch to switch between power sources. The general type of transfer switches are Automatic Transfer Switch with integrated loads. Bypass and isolation switchgear will be used to allow the system to be serviced and tested without disrupting power to the critical loads.

#### *9.7.6.6 Surge Protection*

The carriers surveyed have stated that they use surge protection for each site, although specifications were not generally available.

# 10 Installation

The installation section will provide guidance and best practices for installing equipment, equipment racks, equipment grounding, coaxial cables, and data cables into the site-hardened facilities and vehicles.

This document is intended to provide a top-level overview of equipment installation standards and practices for PSG communication sites utilized with the NPSBN. Wherever possible, reference shall be made to existing documents, standards, and codes applying to the installation of communications equipment within the shelter, building, cabinet, or other enclosure used to provide the desired environment for such equipment.

## 10.1 Antenna Systems

The purpose of the antenna system best practices is to set minimum requirements for antenna and sub-system installation on hardened antenna mounting structures. With the current state of the art moving toward Fiber-to-the-Antenna (FTTA), the general scope of antenna systems has been expanded to include support devices. As every facility has unique requirements, these practices should be considered a minimum requirement.

All installations shall be designed to the highest industry standard for quality and reliability. Manufacturers' installation recommendations shall be considered a minimum requirement. The installation of RF feed lines, fiber optic cable, DC power, and grounding will all be done with the highest quality of workmanship and materials. These statements have been incorporated into the Best Practice tables listed below.

### 10.1.1 Cable Installation

#### *10.1.1.1 Description*

Cable installation refers to the placement of cables either in an enclosure or from the enclosure to the antenna system. Cable installation practices are designed to ensure the highest reliability and prevent damage caused by weather and other physical hazards.

### 10.1.2 Best Practices

| | |
|---|---|
| 368. | The cable entrance **SHALL** enter the communications shelter through an "entrance panel" adjacent to the ice bridge, designed to be weather proof at the cable entrance per the manufacturers specifications. |
| 369. | All cabling **SHALL** be installed in such a manner that it is not bundled together. Each cable **SHALL** be supported separately with an appropriate mounting clamp assembly. |

| | |
|---|---|
| 370. | Antenna cable assemblies attached directly to antennas **SHALL** have an appropriate "drip loop" to discourage the migration of water into junction points. |
| 371. | All coax cable assemblies **SHALL** be cut to the appropriate length. |
| 372. | Rigid coax **SHALL** not directly connect to antennas or RF equipment. A flexible jumper **SHALL** be used to interconnect devices. |
| 373. | Critical communications sites, such as public safety sites, **SHALL** adhere to all legally applicable local and national standards and practices as defined by the local and state building, electrical, fire, and other applicable codes |
| 374. | Grounding kits **SHALL** be installed<br>• At the top of the tower where the waveguide transitions from a flexible waveguide jumper to the vertical waveguide section.<br>• At intervals not exceeding 50 feet along the vertical section.<br>• At the bottom of the vertical waveguide section, within 10 feet of the transition and continuation of the waveguide run across the ice bridge to a communications vault or transition to the flexible waveguide jumper in the case of a tower mounted microwave terminal.<br>• All grounding kits to be bonded to the site ground system. |
| 375. | To ensure the most reliable installation, vertical plant **SHALL** be done in one contiguous piece, without junctions. |

## 10.2 Fiber Optic Cable for Antenna Systems

### 10.2.1 Description

Many modern systems use fiber optic cable to send and received RF signals to power amplifiers and low noise pre-amps located near to the antenna systems on towers. For the fiber system to be considered PSG at a minimum the below best practices must be followed.

### 10.2.2 Best Practices

| | |
|---|---|
| 376. | Fiber optic cable **SHALL** be installed in accordance with the manufacturers' recommended practices. |
| 377. | A hybrid cable design **SHOULD** be used as it provides both power and fiber conductors in one assembly. |
| 378. | DC power cabling **SHALL** be terminated into enclosure per manufacturers' specifications. |
| 379. | Any fiber cable ground and the fiber enclosure **SHALL** be grounded to the site master ground system. |
| 380. | Supporting hangers that isolate the fiber optic cable, from the tower structure, **SHOULD** be used, as this provides some vertical movement to minimize structural stressors such as vibration. Hangers shall be installed at intervals of no more than 3 ft. |

| | |
|---|---|
| 381. | All vertical plants **SHOULD** be one contiguous piece between cable management enclosures at the top and bottom of the tower[58] structure. |
| 382. | Fiber optic cable **SHALL** be routed into manufacturer's approved termination enclosure with all weatherproof seals installed per specifications. |
| 383. | Bending radius **SHALL** not exceed the manufacturer's specifications. |
| 384. | The fiber entrance **SHALL** enter the communications shelter through an "entrance panel" adjacent to the ice bridge, designed to be weather proof at the entrance per the manufacturers specifications. |
| 385. | Data and RF cables **SHOULD** be separated as per manufacturer's recommendations. |

## 10.3 Transmission Line - Waveguide

### 10.3.1 Description

Many microwave communications systems use waveguide cable to send and received RF signals to the antenna systems on towers. For the waveguide cables to be considered PSG at a minimum the below best practices must be followed.

### 10.3.2 Best Practices

| | |
|---|---|
| 386. | Waveguide **SHALL** be installed in accordance with the manufacturers' recommended practices. |
| 387. | Supporting hangers that isolate the fiber optic cable, from the tower structure, are recommended. This provides some vertical movement to minimize structural stressors such as vibration and physical damage to the waveguide. Hangers **SHALL** be installed at intervals of no more than 3 ft. |
| 388. | Grounding kits **SHALL** be installed:<br>• At the top of the tower where the waveguide transitions from a flexible waveguide jumper to the vertical waveguide section.<br>• At intervals not exceeding 50 feet along the vertical section.<br>• At the bottom of the vertical waveguide section, within 10 feet of the transition and continuation of the waveguide run across the ice bridge to a communications vault or transition to the flexible waveguide jumper in the case of a tower mounted microwave terminal.<br>• All grounding kits to be bonded to the site ground system. |
| 389. | To ensure the most reliable installation, vertical plant **SHALL** be done in one contiguous piece, without junctions. |

[58] For purposes of this document, tower is defined as the antenna mounting structure and may be a lattice style tower or mono pole design.

## 10.4 Transmission line – Coaxial Cable

### 10.4.1 Description

Many communications systems use coaxial cable to send and received RF signals to the antenna systems on towers. For the coax cables to be considered PSG at a minimum the below best practices must be followed.

### 10.4.2 Best Practices

| | |
|---|---|
| 390. | Coaxial cable **SHALL** be installed in accordance with the manufacturers' recommended practices. |
| 391. | Supporting hangers that isolate the coaxial cable, from the tower structure, **SHOULD** be used. This provides some vertical movement to minimize structural stressors such as vibration and physical damage to the coaxial cable. Hangers **SHALL** be installed at intervals of no more than 3 ft. |
| 392. | Coaxial surge protection - Each coaxial line **SHALL** have a lightning suppressor installed and bonded to the site master ground system |
| 393. | Grounding kits **SHALL** be installed:<br>• The top of the tower, within 10 feet of the transition from "hard line" coaxial cable to the flexible coax jumper, to the antenna.<br>• At Intervals not exceeding 50 feet along the vertical plant.<br>• At the bottom of the vertical plant, within 10 feet of the transition and continuation of the coax run across the ice bridge to a communications vault. An additional grounding kit shall be installed before the coaxial cable enters the communications vault. |
| 394. | All grounding kits to be bonded to the site ground system. |
| 395. | All direct current (DC) cabling **SHALL** be run in a metal conduit unless otherwise specified. When the DC power cable is an integral part of a fiber assembly designed for outside mounting, no conduit will be required. |
| 396. | Surge protection **SHALL** be used with all DC cabling. |

## 10.5 Shelters, Equipment, and Internal Cabling

This document is intended to provide a top-level overview of equipment installation standards and practices for PSG communication sites utilized with the NPSBN.

### 10.5.1 Description

Like existing mission critical LMR equipment, the NPSBN system equipment and infrastructure will be housed in shelters and cabinets that must meet specific requirements to ensure the safety, security and operability of these systems.

### 10.5.2 Installation of Equipment Racks and/or Cabinets within New or Existing Shelters

Equipment and infrastructure systems will frequently be installed in equipment racks and cabinets within new or existing storage shelters. These installations must conform to appropriate standards and best practices to ensure an appropriate level of operability, reliability, and readiness.

#### *10.5.2.1 Best Practices*

| | |
|---|---|
| 397. | Equipment installations **SHALL** conform to the manufacturer's specifications (to include all manufacturers of the equipment, racks and/or cabinets, and hardware used for installation). |
| 398. | In addition or where individual manufacturer's guidance is lacking or insufficient to direct the installation of the equipment, the installation[59] **SHOULD** minimally conform to the guidelines set forth in the Motorola document[60] titled, "Standards and Guidelines for Communication Sites (R56 Issue B)." |
| 399. | The installation procedures **SHALL** conform to all applicable OSHA standards and manufacturers guidelines for the safe lifting and moving of equipment racks and cabinets.[61] |
| 400. | All installations **SHALL** be evaluated for environmental hazards listed in Section 3, which are applicable to the specific geographic area, and **SHALL** take mitigating actions as required. |
| 401. | Procedures to verify compliance: An installation audit **SHALL** be performed by one or more of the following: A manufacturer's representative familiar with the installation standards for such equipment, a building inspector familiar with local codes and regulations governing the installation of equipment in occupied or unoccupied buildings within the inspector's jurisdiction; and/or a competent project engineer assigned to the installation project. |
| 402. | The environment hazards and issues identified in Section 3 **SHALL** be considered during the construction, installation, and maintenance phase of the project. |

[59] References: Motorola, Inc. Standards and Guidelines for Communication Sites, Issue B, 2005. Chapter 9: Equipment Installation, Sections 9.5-9.8 (Equipment Mounting Plumb and Squareness, Equipment Anchoring, Equipment Installation Within Racks or Cabinets, Ancillary Equipment Mounting)

[60] Motorola Solutions has developed an internal document titled "Standards and Guidelines for Communication Sites (R56 Issue B)." This document covers site design and installation practices. While this document is not a recognized standard document, it is used by many public safety entities to guide them in those areas. The consensus of the working group is that R56 is a valuable document to use in site development and equipment installation.

[61] US Dept. of Labor Occupational Safety and Health Organization guidelines on materials handling and storage: https://www.osha.gov/SLTC/etools/electricalcontractors/materials/heavy.html

### 10.5.3 Installation of Power, RF and Data Cabling within New and Existing Shelters

The proper installation of power feeds, RF transmission lines and data cabling is essential in order to ensure an appropriate level of operability, reliability, and readiness.

#### *10.5.3.1 Best Practices*

| | |
|---|---|
| 403. | Installation of cables **SHALL** conform to the cable manufacturer(s)' guidelines for the proper preparation installation and securing of that manufacturer(s)' cabling and connectors including but not limited to recommendations on bend radius proper sizing of conductors and strain relief. |
| 404. | The installation **SHALL** conform to all applicable local and national codes for the installation of power cabling.[62] |
| 405. | The installation procedures **SHALL**[63] conform to all applicable OSHA standards for the installation of cabling within telecommunication spaces. In the case of power cabling, the installation **SHALL** conform to all applicable local and national codes for the installation of power cabling. |
| 406. | In addition or where individual manufacturer's guidance is lacking or insufficient to direct the installation of the cabling the installation **SHOULD** conform to the guidelines set forth in the Motorola,[64] Inc. document "Standards and Guidelines for Communication Sites" (R56 Issue B) |
| 407. | Periodic inspections of the grounding system **SHALL** be conducted. |
| 408. | A written safety plan **SHALL** be required. |
| 409. | Procedures to verify compliance: An installation audit **SHALL** be performed by one or more of the following: A manufacturer's representative familiar with the installation standards for such cabling an electrical inspector and/or licensed electrician familiar with local and national codes and regulations governing the installation of electrical cabling in occupied or unoccupied buildings within the inspector's jurisdiction; and/or a competent project engineer assigned to the installation project. |
| 410. | In addition, installed cabling **SHOULD** be tested, when practical before initial turn-up to verify operating parameters such as return loss/VSWR, insertion loss, system gain/loss, passive intermodulation conformity correct polarity voltage drop, cross-talk proper pin outs, and any other operating parameter which is critical to the functionality of the installed cabling. |

[62] National Fire Protection Association: NFPA 70: National Electrical Code: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=70

[63] U.S. Dept. of Labor Occupational Safety and Health Organization Standard Publication 1910.268: Telecommunications.https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_id=9867&p_table=STANDARDS

[64] Motorola, Inc. Standards and Guidelines for Communication Sites, Issue B, 2005. Chapter 9: Equipment Installation, Section 9.9, (Equipment Cabling).

### 10.5.4 Interior Grounding and Bonding of Installed Equipment

Electronic equipment is required to be electrically bonded/grounded to the site/enclosure ground system. Proper interior and exterior grounding and bonding of systems, cables, and other equipment is essential in order to ensure an appropriate level of operability, reliability, safety, and readiness

#### *10.5.4.1 Best Practices*

| | |
|---|---|
| 411. | The installation **SHALL** conform to the manufacturer(s)' guidelines for the grounding and bonding of the equipment. Additionally the installation **SHALL** conform to a nationally recognized standard for the grounding and bonding of communications sites. At this time the recommended standard is "Standards and Guidelines for Communication Sites" (R56 Issue B) published by Motorola Inc.[65] |
| 412. | Procedures to verify compliance: A grounding and bonding audit **SHALL** be performed by one or more of the following: A manufacturer's representative familiar with the grounding and bonding requirements of that manufacturer's installed equipment; an electrical inspector and/or licensed electrician familiar with local and national codes on the grounding and bonding of electrical service; or a competent project engineer assigned to the installation project. |
| 413. | A grounding and bonding audit **should** be performed by a person or persons certified by the Electronic Technician's Association, or a similar professional organization in the grounding and bonding of communication sites according to a nationally recognized standard such as "Standards and Guidelines for Communication Sites" (R56 Issue B).[66] |

## 10.6 Vehicles

A wide variety of vehicles are used by public safety agencies and generally all require data and voice communications equipment to be installed in them. Proper installation of these systems and devices is essential in order to insure an appropriate level of operability, reliability and readiness.

#### *10.6.1.1 Description*

Communications equipment is defined as the electronic equipment that is installed in the vehicle that supports voice and data communications with the NPSBN. This equipment also

[65] References: Motorola, Inc. Standards and Guidelines for Communication Sites, Issue B, 2005. Chapter 5: Internal Grounding (Earthing).
[66] References: Motorola, Inc. Standards and Guidelines for Communication Sites, Issue B, 2005. Chapter 5: Internal Grounding (Earthing).

includes terminals, devices, cameras, sensors and computers. Communications equipment contains sensitive electronics susceptible to voltage drops and power supply interference.

#### *10.6.1.2 Best Practices*

| | |
|---|---|
| 414. | All work **SHALL** be conducted according to OSHA/FCC/Manufacturer standards |
| 415. | All wiring **SHALL** be continuous runs free of splices and butt connectors. |
| 416. | All power supply wiring **SHALL** initiate at or near the battery, fused as close as possible to the source. |
| 417. | A secondary battery, isolation and/or load management system **SHOULD** be considered for communications equipment if vehicle starter or high demand appliance (Telma retarder, mechanical siren, etc.) drops the voltage in primary battery. |
| 418. | Antenna installations **SHALL** follow manufacturer's separation and installation recommendations. |
| 419. | External antennas and modems **SHOULD** be used to provide appropriate coverage and reliability. |
| 420. | Special procedures recommended by the manufacturer **SHALL** be followed when installing or working on electric/hybrid/specialty vehicles. |

### 10.6.2 Driver Safety

#### *10.6.2.1 Description*

Driver safety can be impacted by the installation of equipment in vehicles. Installing mobile devices intended to be used by the driver shall consider the safety effects.

#### *10.6.2.2 Best Practices*

| | |
|---|---|
| 421. | For devices intended to be operated by the driver, device **SHALL** be installed with the display angled square to the driver's line of sight |
| 422. | The device **SHALL** be installed within driver's reach without requiring them to lean. |
| 423. | The device photocell/dimming control **SHALL** sample outdoor ambient light instead of in-vehicle light. This relates to mobile devices only, and does not include portable devices unless other specified. |
| 424. | Tactile controls, such as volume and brightness, **SHOULD** be provided and **SHALL** be designed for ease of use in the public safety environment |
| 425. | Devices **SHALL** be designed to minimize driver distractions. |
| 426. | Devices **SHALL** not interfere will vehicle Supplemental Restraint Systems (SRS) or other required safety devices. |

### 10.6.3 Equipment Environment

#### *10.6.3.1 Description*

Public safety vehicles operate in harsh environments and often experience rapid changes in vehicle temperature. When installing equipment in vehicles the heat, cold, dust, moisture, and vibration must be controlled. (More and more communications components are being added to emergency response vehicles. The placement of these components have been added to vehicles as place can be found and not in a planned process.

#### *10.6.3.2 Best Practices*

| | |
|---|---|
| 427. | Installation of vehicle electronics **SHOULD** consider temperature extremes and other environmental issues. |
| 428. | Serviceable components **SHOULD** be easily accessible. |
| 429. | Antenna installations **SHALL** have an engineering study of frequencies in use and the radiated power anticipated. Place antennae in an arrangement to minimize their effects on each other. |
| 430. | An analysis of all frequencies in use and their radiated power **SHALL** be conducted to ensure effective device operation. |
| 431. | Sheet metal **SHALL** be installed on fiberglass surfaces to maximize the ground plane. |

### 10.6.4 Data Centers

This section describes best practices for installation of equipment in data centers that have been constructed to site hardening specifications as described in other sections of this document

The TIA-942 standard identifies four tiers of installation standards for redundancy and uptime.

- Tier 1 – Basic data center with no redundancy
- Tier 2 – Some redundancy
- Tier 3 – Multiple distribution paths with only one active
- Tier 4 – Multiple active distribution paths

Data Centers for public safety grade communications shall be Tier 4 rated.

#### *10.6.4.1 Description*

Data centers may house specialized equipment for the NPSBN excluding equipment located in a site as defined in Chapter 9 (Site Hardening). This could include the aggregation site for the RAN infrastructure. Core equipment should be housed in hardened secure data centers and configured to ensure no single failure from disrupting the NPSBN.

#### *10.6.4.2 Best Practices*

| | |
|---|---|
| 432. | The Data Center **SHALL** be rated at Tier 4. Multiple distributed aggregation sites, which are geographically distributed, may achieve the required redundancy and resiliency through the use of multiple Tier 3 sites. |
| 433. | Data Center installation **SHALL** follow the ANSI/TIA-942 Telecommunications Installation Standard for Data Centers, ANSI/NECA/BICSI-002 Data Center Design and Implementation Best Practices, and local and national building codes. |
| 434. | If redundant data centers are used, they **SHALL** be geographically separated to minimize a single manmade or natural event from disabling both primary and backup data centers. |
| 435. | Data centers **SHOULD** be located in areas that are least likely to be affected by environmental conditions (see Section 3 on Environmental Events), commercial power issues, civil unrest, or other risks. |
| 436. | All communication paths between data centers **SHALL** have redundant self-healing connectivity. |

### 10.6.5 Sensitive Electronics

#### *10.6.5.1 Description*

Sensitive electronic equipment is used throughout the public safety network. This equipment is susceptible to voltage drops, power supply disruptions, and other interference issues.

#### *10.6.5.2 Best Practices*

| | |
|---|---|
| 437. | Power **SHALL** be conditioned for noise suppression, transient impulse protection and general voltage stabilization. |
| 438. | Sensitive equipment **SHALL** have redundant power sourcing. |
| 439. | UPSs or DC battery systems **SHOULD** be utilized to protect equipment during power transfer, power spikes, or brown outs. |
| 440. | UPS devices **SHALL** be sized to provide power as a result of primary power, through generator start and transfer with a reserve to allow for graceful shutdown if required. |

### 10.6.6 Data Center Security

#### *10.6.6.1 Description*

Public safety data centers require additional physical and cyber security measures to protect them from natural and manmade disruptions

#### *10.6.6.2 Best Practices*

| | |
|---|---|
| 441. | NPSBN data centers **SHALL** conform to Tier 4 criteria as designated by the TIA-942[67] standard. |
| 442. | Data center cabling **SHALL** conform to TIA/EIA 568 standard. |
| 443. | Employees and technicians working in Data Centers **SHALL** be subject to appropriate criminal justice background check. |
| 444. | The Security requirements listed in the Site Hardening Section **SHALL** be applied regardless of unique NPSBN data center or shared data center. |
| 445. | Shared space data centers require special considerations including the caging of equipment. |

## 11 Operations and Maintenance

This document references maintenance from the perspective of prevention. It assumes corrective maintenance will occur once failure is detected and under the terms of the agency's SLA. Upgraded maintenance is not addressed as each agency must decide to upgrade based on their respective operational needs.

During maintenance, efforts shall be made to avoid service interruption. Such efforts shall include a level of fallback appropriate for the work being conducted. (e.g., if a generator is being repaired, a trailer-mounted generator shall be available onsite). If service interruption is necessary for the maintenance, it shall be coordinated with the agency's operations personnel.

All operations and maintenance work will be conducted according to NIOSH/OSHA, FCC, FAA, ANSI/TIA 1019A, 222G, and manufacturer's standards.

This section covers RAN, backhaul, core, and sites (generators batteries, etc.)

[67] http://www.te.com/content/dam/te/global/english/industries/enterprise-network-solutions/knowledge-center/documents/enterprise-white-paper-tia-942-data-center-standards-overview-102264ae.pdf

## 11.1 Description

Public safety communications facilities that are designed and constructed to meet the PSG best practices will need periodic maintenance in order to maintain proper operations. It is important that periodic inspection, preventative maintenance, and event-based inspection be implemented to ensure that the systems maintain an appropriate level of operability, reliability, and readiness.

## 11.2 Best Practices

### 11.2.1 Sites & Backhaul

| | |
|---|---|
| 446. | Quarterly visual inspection **SHALL** be conducted to look for evidence of vermin, ventilation restriction, water intrusion, security breach, fuel leaks, corrosion, mandated lighting, vandalism, and other issues, or whenever the site is accessed. Grounding shall be visually checked and **SHALL** include a periodic grounding test. |
| 447. | Visual and electronic inspection of batteries, **SHALL** be conducted quarterly. |
| 448. | Quarterly visual inspection **SHALL** be conducted to include a general overview of site/tower/pole for misaligned components, lighting system, and other evidence of wear and tear, or whenever the site is accessed. |
| 449. | Manufacturers' recommended maintenance requirements **SHALL** be followed for all HVAC equipment. |
| 450. | Visual inspection of all electronic equipment located at the site **SHALL** be conducted quarterly or whenever the site is accessed. |
| 451. | Manufacturers recommended preventative maintenance procedures **SHALL** be performed. |
| 452. | Quarterly visual inspection **SHALL** be conducted to look for evidence of vermin, ventilation restriction, water intrusion, security breach, fuel leaks, corrosion, mandated lighting, vandalism, and other issues, or whenever the site is accessed. |
| 453. | If the backhaul network includes a microwave path, a visual inspection **SHALL** include assessment for path obstructions. |

## 11.3 Generators and UPS Maintenance

### 11.3.1 Description

Generators and UPS exist at sites to ensure uninterrupted operation of the communications infrastructure.

### 11.3.2 Best Practices

| | |
|---|---|
| 454. | At staffed facilities, **SHALL** conduct weekly generator run test under load. |

| | |
|---|---|
| | Transfer switch operation shall be checked. A 1-hour run time is suggested to assure staff is familiar with conditions imposed by backup power (partial lighting, reduced HVAC, etc.). Each shift should be exposed to the generator run test. Tests **SHALL** also be conducted at off-peak times. |
| 455. | At unstaffed facilities, generators **SHALL** be run monthly under load. Run time shall be long enough to validate fuel flow and to adhere to manufacturers minimum run time based on fuel type and other factors. |
| 456. | The quarterly check of the generator **SHALL** include compliance with manufacturer's preventive maintenance to assure all wear components are addressed. (e.g, fluids, batteries, belts) |
| 457. | A quarterly visual assessment **SHALL** be conducted of fuel supply for quantity and leaks and lines for leaks. |
| 458. | Site and data center power systems **SHALL** be monitored. Low fuel level alarms **SHALL** be monitored. |
| 459. | Prior to any preplanned or environmental events, site inspection **SHALL** occur to determine that the site is appropriately readied for ongoing operations. This includes a check of all critical systems, electronics, fuel supply, and other components required by the event. |

# Appendix A—NPSTC Broadband Working Group, Public Safety Grade Task Group Participants

NPSTC wishes to thank the following members of the Public Safety Review Team who helped conduct the final editing and review of the document:

David Buchanan, Chair
Steve Devine, State of Missouri
Bill Schrier, State of Washington
Mike Barney, State of Texas
Tim Trager, San Bernardino County-ISD
Chris Kindelspire, Grundy County, Illinois 9-1-1
Brad Stoddard, State of Michigan
Bill Agee, City of Hampton, VA
John Chaney, Harris County, Texas
Mark Grubb, State of Delaware
John Lenihan, Los Angeles County Fire
Larry Schaefer, U.S. Capitol Police

NPSTC also wishes to thank all of the public safety, commercial, and industry participants who helped create this report. NPSTC wishes to note that the appearance of anyone's name on this list is meant to acknowledge their participation in the process and does not automatically indicate their support, or absence of support, for the entire contents of this report.

Scott Agnew, AT&T
Pat Amodio, EchoStar
Rick Amweg, State of Ohio
Stephen Anderson, DHS Joint Wireless
William Andrle, Advanced Networks
Daniel Biglin, AT&T
James Blocker, Federal Engineering
Kimberlyn Bouler, Shelby County, VA
Richard Coupland, General Dynamics C4
Damon Darsey, Mississippi MEDCOM
Charles Dionne, Aviat Networks
Tewfik Doumi, Alcatel-Lucent
James Downes, DHS-OEC
William Drew, State of New Jersey
Robert Ehrlich, TeleCommunication Systems
David Eierman, Motorola Solutions
Jeremy Elder, Harris Corporation
Gerald "Jay" English, APCO
John Evans, Harris Corporation
Charles Fair, Sedgwick County, Kansas
Joseph Farnan, Good-Will FD, DE
Bob Fredericks, Motorola Solutions
Brian Gottschall, Berks County, PA
Ron Gronneberg, Fargo, ND
Timothy Haynie, Harris Corporation
Mark Hoppe, Blue Wing Services
Neil Horden, Federal Engineering
Dr. Clive Horn, Tait Radio
Brenda Jackson, Thales Communications
Bill Janky, Harris Corporation

Gerald "Jerry" Jaskulski, DHS-OEC
Tom Jenkins, Rogers FD, Arkansas
Al Jette, Nokia Siemens Networks
Brad Kaupp, Sprint Corporation
Farrokh Khatibi, Qualcomm
Brett Kilbourne, Utilities Telecom Council
Phil Kirmuss, Icom America
Frank Korinek, Motorola Solutions
Sridhar Kowdley, BAH for CBP
Shawn Lapinski, DHS CBP
Paul Levitsky, Deloitte Consulting
Kenneth Link, Monroe Twn FD, NJ
Jennifer Lord, Wisconsin DNR
Claudio Lucente, Ctr Security Science/CAN
Russell Luedecker, Cranford, NJ PD
Joseph Madzelan, Manchester Twn Fire
Melissa Marshall, RCC
Ric Martin, Federal Engineering
Frank Marum, TSS Partners
Andrew Maxymillian, Blue Wing Services
Michael Mazzitello, Sr., MPS LLC
Timothy McHood, Tennessee Hwy Patrol
John McLemore, Motorola Solutions
Kathy McMahon, MCP
Mick McQuilton, Eagle County, CO
George Molnar, State of Nevada
Tim Morrow, Memphis TN PD
Peter Musgrove, ATT
Adam Nelson, Federal Engineering
Steve Nichols, Thales
Rich Nowakowski, RCN Consulting
Sean O'Hara, SRC Incorporated
Gene Oldenburg, SE Wisconsin Regional IO
Stu Overby, Motorola Solutions
Shane Palmer, Evergreen CO Fire
Tim Pierce, Dane County, WI
Mark Raczynski, General Dynamics C4
Patrik Ringqvist, Ericsson
Dr. Doug Roberts, San Bernardino, CA
Joe Ross, Televate
Tom Rubinstein, Motorola Solutions
Penny Rubow, State of Arkansas
Mark Ryckman, Corning, New York
Mel Samples, AT&T
Charlie Sasser, State of Georgia
Michael Sasuta, MDS
Frederick Scalera, State of New Jersey
Brian Scarpelli, TIA
DeWayne Sennett, AT&T
Thomas Sharp, Federal Engineering
Scot Smith, Sprint
Karl "Andy" Spanhak, Sprint
William "Don" Speights, DHS
Ken Swanson, Shasta County CA FD
Tina Tapuai, American Samoa DHS
Ramiz Taqi, Sprint
John Toone, Motorola Solutions
Mark Uncapher, TIA
David Vander Staay, Thales
Nick Waddell, Harris Corporation
Nate Walowitz, IMT Communications LLC
Bill Waugaman, LR Kimball
Chris Wilson, Motorola Solutions
Scott Wiggins, Federal Engineering
Jeffrey Wobbleton, Washington DC SWIC
Paul Wright, NW Fire District, Tucson AZ
Larry Zamora, Coconino County AZ SO

NPSTC also wishes to acknowledge the work by the Association of Public Safety Communications Officials (APCO)-International and their Broadband Committee's Site Hardening Working Group, which created the site hardening content used in this document. The following APCO members participated in the project:

| **Co-Chairs** | |
|---|---|
| Joe Ross | Sr. Partner, Televate |
| Andy Seybold | Principal Andrew Seybold, Inc, |
| **Committee Members** | |
| Bill Agee | Hampton City, VA |
| Dominick Arcuri | RCC Consulting |
| Bob Batis | Motorola Solutions |
| David Buchanan | NPSTC |
| Billy Carter | Illinois Department of Public Health |
| Ferdinand Cedeno | PREMS |
| Daniel Devasirvatham | Director / Program Manager, WNUF. INL |
| Neil Horden | Federal Engineering, Inc. |
| John Johnson | State of Tennessee |
| Jim Junkins | Harrisburg-Rockingham ECC |
| Tom Kadunce | State of Delaware |
| Chris Kindelspire | Grundy County 911 |
| Sridhar Kowdley | BAH for CBP |
| Morton Leifer | Clarkstown PD |
| Barry Luke | NPSTC |
| Dick Mirgon | Mirgon Consultants |
| Mel Samples | AT&T |
| Bill Schrier | Office of the CIO, State of Washington |
| Gino Scribano | Motorola Solutions |
| Theron Shinew | State of Michigan |
| Mike Stanley | Mindbank Consulting Group |
| Ted Sumners | Mindbank Consulting Group |
| Tim Trager | San Bernardino County-ISD |
| **Executive Sponsors** | |
| Terry Hall | Past President, APCO |
| John Wright | First Vice-President, APCO |

NPSTC is grateful for support provided by the U.S. Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC), and the National Protection and Programs Directorate, Office of Emergency Communications (OEC). Facilitation support for the task team was provided by the following individuals:

Jackie Bayless
MarySue Brown
Barry Luke
Debby Replogle

# Appendix B—Glossary of Terms

| | |
|---|---|
| **1:1 PTT Call Also 1 to 1** | A private push-to-talk call between only two devices that are actively affiliated. |
| **1:N (1 to Many)** | A one-to-many push-to-talk call. Also known as a group call. "N" is identified as the number of users required in that particular group call and/or the number of UEs authorized for that group call by the agency's System Administrator. |
| **Actionable Information** | Data that can be used by the end user to fulfill their mission. In order to provide actionable information, the application must have access to data of interest and understand the user's situational context. An outcome of providing actionable information is that the user's situational awareness is increased, enabling the user to better fulfill their mission. |
| **Announcement Call** | A special type of group call wherein the group is composed of the users who have selected a group that is part of the announcement group.<br>An Announcement Call is a call sent to user devices based on either: The selected user device personality is slaved to a particular announcement voice resource. Or, the user device has selected a voice resource that belongs to a multi-voice resource group. |
| **Availability** | The ability of the public safety community to obtain their required services and applications in all places the public safety community needs to operate. |
| **Availability check** | Request sent to a subscriber polling the device to see if it is actively registered on the network. |
| **Call** | A series of one or more push-to-talk transmissions. |
| **Caller** | A user of a fixed or mobile device placing a call on the network. |
| **Call-Setup or Access Time** | The time that the talker presses his PTT control, and the time that he is able to speak. These values include elements associated with some of the following characteristics: The amount of time required from PTT to voice resource grant, mouth-to-ear latency, public safety grade audio fidelity, trailing lost audio, initial lost audio, among other values. |
| **Emergency Call** | Group calls with preemptive priority due to their association with a life-threatening condition being experienced by a responder and automatically routed to the related/appropriate administrative authority for immediate response or action. |
| **Encoder/Decoder (CODEC)** | A codec is a device or computer program capable of encoding or decoding a digital data stream or signal. |

| | |
|---|---|
| **Encryption** | Client-server encryption: Client initiates a connection request and establishes a connection to a server. The client stores a list of known hosts locally and uses this list to authenticate the server each time a connection is made.<br><br>Pre-positioned "shared" key(s): A common key(s), called a Pre-Shared Key (PSK), must be pre-loaded into the subscribers.<br><br>Key distribution: Remotely transfer key management messages to radios to update a radio's keys, poll the radio, inhibit the radio, and erase the radio's keys. Radios can also send key management messages to the Server to acknowledge events or to request a key update.<br><br>Key negotiation: Authenticates the device(s) before establishing a connection to the NPSBN. |
| **Full Duplex** | Two or more one parties can talk simultaneously. |
| **Group Call** | A one-to-many (1:N) push-to-talk call made to N devices that have selected a particular resource. |
| **Half Duplex** | Only one party can talk at a time. |
| **Human-Centered Design** | An engineering approach that considers the needs of the end users of the application during the entire product development process. It is fundamentally concerned with understanding the user's context (especially their situational needs) and providing a solution that satisfies fundamental user needs. An outcome of following human-centered design principles is a user interface that is simple and intuitive that meets the user need without distracting them from their mission. |
| **Imminent Peril Call** | A call, which is automatically routed to the related/appropriate administrative authority and surrounding associated users for immediate response or action.<br>A type of group call with elevated priority of an urgent nature impacting human life safety and/or incident operation. |
| **Initial Lost Audio or Late Call Entry** | Powering up the device or selecting voice resource while a call is in progress. |
| **Live Time in Queue** | Active time a PTT transmission is being processed by the PTT service. |
| **Monitor** | The act of observing something (and sometimes keeping a record of it). |
| **Personality Programming** | The ability to program a subscriber unit with characteristics indicative of a specific agency's user(s) with particular access to talkgroups associated with that agency. |
| **PTT Service** | Push-to-talk voice service using user equipment (UE). |

| | |
|---|---|
| **PTT Transmission** | A single continuous push-to-talk communication from a talker to zero or more listeners. |
| **PTT User** | Someone that uses a push-to-talk subscriber. |
| **PTT Subscriber** | A device that has a subscription to the push-to-talk service, or an "Application User" that has such a subscription. Herein, the term is used generally when a requirement applies to both Fixed and Mobile PTT Subscribers. |
| **PTT Fixed Subscriber or Fixed PTT Subscriber** | A wireline push-to-talk subscriber (e.g., a console) that accesses the PTT service from a PSEN. PTT Fixed Subscribers include dispatchers and dispatch supervisors.<br>Console devices are typically hardwired to the NPSBN. However, in mobile command posts, the network connection could be over the air. |
| **PTT Mobile Subscriber or Mobile PTT Subscriber** | A wireless push-to-talk subscriber (e.g., a handheld device) that accesses the PTT service over the air. PTT Mobile Subscribers include responders in the field. |
| **Prioritization** | A scale of urgency of need for an active talk path. Subscriber and talkgroup each have their own respective level of priority. |
| **Private Call** | Push-to-talk call only heard by two specific users. |
| **PSE** | Public Safety Entity. PSE is synonymous with a public safety agency responsible for operations and maintenance (O&M). For example, procedures may be negotiated to permit NPSBN users (NPSBN-Us) needing to roam onto commercial networks so they receive consistent treatment of their assigned priority classifications, such as through admission control (AC), allocation and retention priority (ARP), and/or quality of service class identifier (QCI), commensurate with their PSE identity. |
| **PSEN** | Public Safety Enterprise Network. A PSEN is a communications network that serves one or more public safety agencies. A PSEN can serve an entire state or a single agency. |
| **Public Safety Grade** | Refers to components such as, coverage calculations, tower construction, equipment installation, environmental controls, and many other requirements. |
| **LMR Subscriber** | A land mobile radio subscriber is a user communicating from an LMR system. |
| **Reliability** | The ability of a system to perform and maintain its functions in both routine and hostile or unexpected circumstances. |
| **Resiliency** | The ability of a component or system to continue to function satisfactorily under adverse circumstances and to quickly recover from a failure and/or return to its original form. |
| **Ruthless Preemption** | The lowest priority user is forced off a call to provide resources for an emergency call. |
| **Scanning** | Monitoring multiple voice resources simultaneously. |

| | |
|---|---|
| **Services** | Common network applications authorized users can use. |
| **System Call** | A dispatch-originated high-priority call that is received by all units in a designated geographic area without regard for jurisdictional boundaries. |
| **Talk Group** | Subscribers organized by agency and/or functionality to conduct PSE operations/business. |
| **Talker ID** | Identification of calling subscriber. |
| **Top of Queue** | Call is routed to top of waiting call list. |
| **UE** | User Equipment |
| **User** | The user is the person that is utilizing the NPSBN Subscriber device. |