8. Communication and Information Systems

8.1. Introduction

PPD-21 identifies "energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." These two infrastructure systems are highly interdependent. Communication and information systems, the focus of this chapter, are increasingly critical parts of our daily lives. For example, the banking system relies on the Internet for financial transactions, documents are transferred via Internet between businesses, and e-mail is a primary means of communication. When Internet is not available, commerce is directly affected and economic output is reduced.

Communication and information systems have seen incredible development and use over the past 20-30 years. In terms of system types, functionality, and speed, some of the most notable changes of communication and information systems over the past few decades are:

- Moving from a society that relies on fixed line (i.e., landline) telephones as the primary means of two-way voice communication to one that relies heavily on mobile devices (e.g., cell phones) and Internet (Voice over Internet Protocol, VoIP) for voice communication, text messages, and e-mail. Many now have abandoned traditional landlines in favor of mobile phones and VoIP.
- Moving from a society where large personal computers were used to communicate via e-mail and access information via the Internet to a society where smaller mobile devices, such as laptops and cell phones, are used for the same purpose
- More and more people now use laptops, smart phones, and tablets to read news on the Internet and watch movies and television shows, instead of using traditional methods such as television
- More recently, businesses have begun to use social networking sites for collaboration, marketing, recruiting, etc.

As in many other developed countries, most people in the United States take these services for granted until they are unavailable. Unfortunately, communication and information systems are often lost in the wake of natural disasters—a time when they are needed most for:

- Relaying emergency and safety information to the public
- Coordinating recovery plans among first responders and community leaders
- Communication between family members and loved ones to check on each other's safety
- Communication between civilians and emergency responders

When addressing resilience, communities must also think about the longer term and improving performance of the built environment in the next hazard event. Intermediate and long-term communications and information infrastructure needs of communities include:

- The ability to communicate with employers, schools, and other aspects of individuals' daily lives
- Re-establishing operations of small businesses, banks, etc., via Internet and telecommunications so they can serve their clients
- Restoration, retrofits, and improvements to infrastructure components so it will not fail in the same way in future events (i.e., implement changes to make infrastructure more resilient).

To address resilience of communication and information infrastructure, service providers should work with other stakeholders in the community to establish performance goals for their infrastructure. Example performance goals for the fictional town of Centerville, USA are provided in this chapter to illustrate the process of setting performance goals, evaluating the state of existing communication and information infrastructure systems, identifying weak links in the infrastructure network, and prioritizing upgrades to improve resilience of the network. The example performance goals tables are for a generic hazard, but can be developed by a community/service provider for any type and magnitude of hazard in rural or urban communities.

The goal of this chapter is to provide guidance for the reader that can be used to understand the potential forms of damage to infrastructure and develop plans to improve communication and information infrastructure resilience. Damage observed in past events and success stories are used to show that service providers have many opportunities to become more resilient. Guidance for planning of logistics and personnel are outside the scope of this chapter. Communities and service providers have their own challenges and solutions to accomplish their goals.

8.1.1. Social Needs and System Performance Goals

As discussed in Chapter 2, the social needs of the community drive performance goals that are to be defined by each community and its stakeholders. Social needs of the community include those of citizens, businesses (both small/local and large/multi-national), industry, and government. Each community should define its performance goals in terms of the time it takes for its critical infrastructure to be restored following a hazard event for three levels of event: routine, expected, and extreme, as defined in Chapter 3.

The community has short (0-3 days), intermediate (1-12 weeks), and long-term (4-36+ months) recovery needs. Specific to communications, communities traditionally think about recovery in terms of emergency response and management goals, which include communication between:

- Citizens and emergency responders
- Family members and loved ones to check on each other's safety
- Government and the public (e.g., providing emergency and safety information to the public)
- First responders
- Government agencies

However, as discussed in the introductory section, communities must think about their long-term social needs when addressing resilience. The community's intermediate goal is to recover so people and businesses can return to their daily routine. To do this, people need to be able to communicate with their employers, their children's schools, and other members of the community. Businesses need to have Internet and telephone service to communicate with their clients and suppliers. In the long term, communities should strive to go beyond simply recovering by prioritizing and making improvements to parts of the communications infrastructure that failed in the disaster.

8.1.2. Availability, Reliability, and Resilience

Availability and reliability are terms often used by industry when referring to communications networks. ***Availability*** refers to the percentage of time a communications system is accessible for use. The best telecommunications networks have 99.999 percent availability, which is referred to as "five 9's availability" (CPNI 2006). This indicates a telecommunications network would be unavailable for only approximately five minutes/year.

Reliability is the probability of successfully performing an intended function for a given time period (Department of the Army 2007). Therefore, though reliability and availability are related, they are not the same. A telecommunications network, for example, may have a high availability with multiple short downtimes or failure during a year. This would mean the reliability is reduced due to incremental disruptions (i.e., failures) in service. Reliability will always be less than availability.

Whether the type of communications system is wireline or wireless telephone, or Internet, service providers market their reliability to potential customers. Service providers think about the communications system itself in terms of the services they provide to the end user rather than the infrastructure (i.e., built environment) that supports the service.

Resilience is closely related to availability and reliability. Like availability and reliability, resilience includes the ability to limit and withstand disruptions/downtime. However, resilience also involves preparing for and adapting to changing conditions to mitigate impacts of future events so disruptions occur less frequently, and, when they do occur, there is a plan to recover quickly. Resilience is also the ability to recover from a disaster event such that the infrastructure is rebuilt to a higher standard. Consequently, by enhancing the resilience of communications infrastructure, availability (amount of downtime) and reliability (frequency of downtime) can be improved. Note that availability will never reach 100 percent because maintenance, which requires downtime, will always be needed.

Capacity. Resilience of communications infrastructure is dependent on the network's capacity. As is often seen during and immediately after disaster events, there is an increase in demand of the communication and information systems (Jrad et al. 2005 and 2006). Section 8.1 points out that, during and immediately after a disaster event, the system is used extensively for communication between family and loved ones, communication with vulnerable populations (e.g., ill or elderly), civilians and first responders, and customers and service providers when outages occur.

Unfortunately, the capacity of a system is not immediately increased for disasters and so cellular phones, for example, may not appear to immediately function properly due to high volume use. This is especially true in densely populated areas, such as New York City, or around emergency shelter or evacuation areas. The latter is an especially important consideration, because some facilities used as emergency shelter and evacuation centers are not designed with that intent.

For example, the Superdome in New Orleans, LA was used as emergency shelter during Hurricane Katrina. Although this was an exceptionally large facility used for sporting and entertainment events, these facilities can be overwhelmed prior to, during, and after disaster events because of the influx of civilians seeking shelter. This results in increased demand on the wireless/cellular network.

With the expansion of technology and the massive growth of cellular phone use, the wireless telecommunications network around emergency shelter facilities will become more stressed in disaster events until augmented by additional capacity.

Jrad et al. (2005) found that for an overall telecommunications infrastructure network to be most resilient, an approximately equal user base for wireline and wireless communications was best. The study found that if one network is significantly greater than the other and the larger one experiences a disruption, increased demand will switch to the smaller network and lead to overload. As a simple example, if landline demand is 1,000,000 users, cellular network demand is 500,000 users, and the landline network experiences a disruption in a disaster event, some landline demand will transfer to the cellular network (Jrad et al. 2005). The increased demand would then stress the wireless network and likely result in perceived service disruptions due to overloading of the network when many calls cannot be completed.

Historically, network connectivity (e.g., reliability or availability) has been a primary concern for communications. However, because of the increased multiuse functionality of mobile communications devices (e.g., cellular phones and iPads), communications network resilience also needs to consider the type of data being used, and hence capacity of the network.

Capacity will become an even greater challenge for communications service providers in the wake of future hazard events. Additional capacity is needed to support service for non-traditional functionality of mobile devices such as sending photographs, watching movies on the Internet, etc. Furthermore, some 9-1-1 centers have the ability to receive photo submissions, which may require more capacity than a phone call. On the other hand, if 9-1-1 call centers can receive text messages, this may also be useful because text messages take up a very small amount of data (i.e., less capacity) and can persist until they get into the network and delivered.

8.1.3. Interdependencies

Chapter 4 provides details of the interdependencies of all critical infrastructure systems in a community. The built environment within communities is continually becoming more complex and different systems are becoming more dependent on one another to provide services. Specific to the communications and information system, the following interdependencies must be considered:

Power/Energy. The communication and information system is highly dependent on the power/energy system. For current high technology and data services, the end user needs external power for telecommunications, Internet, and cable. Loss of external power means loss of communication/information services, except for cellular phones which will likely be able to function until their battery is diminished in the absence of standby power. For use beyond the life of the battery, the cell phone must be charged using an external power source. Furthermore, distribution of communications and power service is often collocated (e.g., wires traveling along utility poles). Failure of these systems can happen simultaneously due to tree fall severing both types of lines. In the wake of a disaster event where external power is lost, communications infrastructure needs continuous standby power to ensure continued functionality.

External power is also critical for cooling critical equipment inside buildings. Air conditioning systems, which keep critical equipment from overheating, are not typically connected to standby power. Therefore, although critical communication equipment may continue to function when a power outage occurs, it may become overheated and shutdown (Kwasinski 2009).

Conversely, emergency repair crews for power utilities need to be able to communicate so they can prioritize and repair their network efficiently. The power provider controls the rights of the utility poles; therefore, the design, construction, routing, and maintenance of telecommunication lines are dependent on the requirements and regulations of the power utility provider.

Transportation. A common problem after disaster events is that roadways and other parts of the transportation system needed in recovery of infrastructure become impassible. Specifically, tree fall and other debris resulting from high wind events (e.g., hurricanes and tornadoes), storm surge/flooding, and ice storms prevent emergency crews from reaching the areas where they need to repair damaged communications infrastructure. Moreover, standby generators cannot be refueled because roads are impassible. Transportation repair crews, including those for traffic signals, need to be able to communicate to ensure their system is fixed. Traffic signals and transportation hubs also rely on communications systems. Traffic signals use communication systems for timing and synchronization of green lights to ensure smooth flow of traffic and transportation hubs use communications system to communicate schedules for inbound/outbound passenger traffic.

Building/Facilities. Buildings and facilities need their communications and information systems to function properly. Buildings used for business and industry communicate with clients, suppliers, and each other via telephone and e-mail. Residential buildings need these services to communicate with employers, loved ones, banks, and services. Currently, money is transferred between businesses, bills are paid to services/businesses and personal banking is completed online or, less commonly, by telephone.

Individuals inside buildings in the immediate aftermath of sudden, unexpected events (e.g., blast events) also need the communications network to learn what is happening.

In large urban centers, service providers often have cell towers on top of buildings. If these buildings fail, an interruption in service may occur due to the loss of the cell tower.

Water and Wastewater. Water and wastewater utilities rely on communications amongst operations staff and emergency workers in the recovery phase. If the communications network, including the cellular network, is down for an extended period of time following a disaster event, the recovery process can take longer since there will be limited coordination in the efforts.

Similar to power/energy, water is needed for cooling systems in buildings that house critical equipment for the communications and information systems. Furthermore, water and wastewater systems are needed in buildings that house critical equipment for technicians.

Security. Security is an important consideration, particularly in the immediate (emergency) recovery after a disaster event. Service providers will not endanger employees. In cases where power and communications systems fail, security becomes an issue because small groups of citizens may use it as an opportunity for looting and violence. Communication and information service providers must be able to work with security to control the situation and begin the recovery process in a timely manner.

8.2. Critical Communication and Information Infrastructure

This section discusses some of the critical components in the communication and information system infrastructure, their potential vulnerabilities, and strategies used in the past to successfully mitigate failures. Figure 8-1 presents components of a telecommunications system.

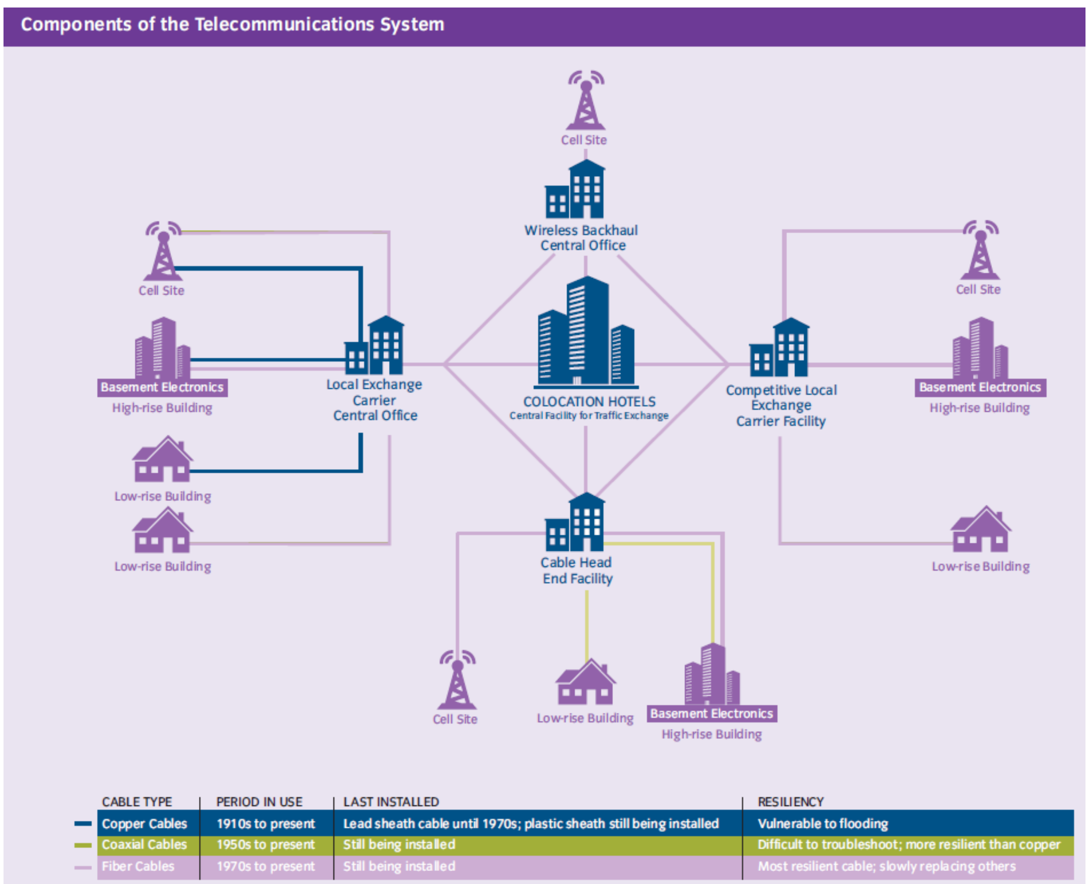

***Figure 8-1. Components of the Communications System** (City of New York, 2013)*

8.2.1. Landline Telephone Systems

Most newer, high technology communication systems are heavily dependent on the performance of the electric power system. Consequently, these newer communication systems are dependent on the distribution of external power to end users, which often is interrupted during and after a disaster. Hence, reliable standby power is critical to the continued functionality of the end user's telecommunications.

Conventional analog landlines (i.e., not digital telephones) operate on a separate electric supply that may be impacted by the event, but service providers often use their own standby power to minimize disruption at end user locations. Hence, landline telephones are generally a more resilient option for telephone communication if commercial power loss is the only impact from a disaster event.

The American Lifelines Alliance (ALA 2006) recommends that landline systems should be retained or reinstated for standby service to reduce vulnerability. However, failure of utility poles or trees onto wires can result in lines for power, cable, and telecommunications being cut, resulting in loss of service.

8.2.1.1. Central Offices

Central Offices, also known as telephone exchanges, are buildings that house equipment used to direct and process telephone calls and data. Maintaining the functionality of these facilities is critical to the timely recovery from an event. These facilities are designed as occupancy Category III (in some cases IV) buildings in ASCE 7 and, consequently, are expected to be fully functional after an expected event.

The primary resiliency concerns for Central Offices are:

- Performance of the structure
- Redundancy of Central Offices/nodes within network
- Placement/protection of critical equipment
- Threat to/from interdependent services

Performance of the Structure. The design of Central Offices is extremely important for continued service of the telecommunications system. These buildings are to be designed as an Occupancy Category III building per ASCE 7, and consequently the design of equipment and standby power must be consistent with that of the building design.

Depending on the location of the community, the design considers different types and magnitudes of disasters. For example, the design of Central Offices in California may be mainly concerned with earthquake loading, whereas Central Offices on the east coast may be concerned mainly with hurricane force winds and/or flooding (especially if it is located in the floodplain as are many Central Offices in coastal communities). In place of providing redundancy of Central Offices, these structures should be designed to resist more severe environmental loads. In cases where Central Offices are located in older buildings that were built to codes and standards that are less stringent than current day standards, it is important to bring these buildings up to modern standards or harden the sections of the building containing critical telecommunications equipment to achieve the desired performance level.

Partial failure of a Central Office can result in the loss of switches and other critical equipment, which results in damage to the communications infrastructure network and loss of functionality. On September 11, 2001 (9/11), four switches were lost in the Verizon Central Office located at 140 West Street (Jrad et al. 2006).

Complete collapse of a Central Office or other building containing a node/exchange in the network would result in loss of all switches and critical equipment. On 9/11, two switches were lost in the World Trade Center Buildings that collapsed (Jrad et al 2006). Though these were not Central Offices, the loss of the nodes could not be recovered. The loss of an entire Central Office would bring the service provider's network to a halt, particularly if no redundancy or backup/restoration capability was built into the network of Central Offices.

Since communities are ultimately responsible for updating, enforcing, and making amendments to building codes, it is important that the most up-to-date building codes be used in the design of new buildings that are used as a part of the communication network. In cases where existing buildings house Central Offices, these buildings should be evaluated and hardened as needed to ensure the critical equipment within the structure is protected.

Redundancy of Central Offices. As learned after the 9/11 terrorist attacks on the World Trade Centers in New York City, redundancy of Central Offices is vital to continued service in the wake of a disaster. On September 11, almost all of Lower Manhattan (i.e., the community most immediately impacted by the disaster) lost the ability to communicate because World Trade Center Building 7 collapsed directly onto Verizon's Central Office at 140 West Street, seen in Figure 8-2 (Lower Manhattan Telecommunications Users' Working Group, 2002). At the time, Verizon did not offer Central Office redundancy as part of its standard service. Furthermore, customers of other service providers that leased Verizon's space lost service as well since they did not provide redundancy either.

Figure 8-2. Damage to Verizon Building on September 11, 2001 (FEMA 2002)

Verizon made a significant effort to restore their services rapidly after the attacks and have since improved their system to use multiple Central Offices for additional reliability. AT&T also endured problems as they had two transport nodes located in World Trade Tower 2, which collapsed and was restored in Jersey City, NJ with mobilized recovery equipment. Overall, almost $2 billion was spent on rebuilding and upgrading Lower Manhattan's telecom infrastructure after 9-11 (Lower Manhattan Telecommunications Users' Working Group, 2002).

Although this was an extremely expensive venture, it is an example that shows building a telecom system with redundancy can eliminate expensive upgrading/repair costs after a disaster event. However, this magnitude of expense is likely not necessary for many other communities.

Placement/Protection of Critical Equipment. Although construction of the building is important, placement and protection of equipment is also an essential consideration if functionality is to be maintained. For example, any electrical or standby power equipment, such as generators, should be placed above the extreme (as defined in Chapter 3) flood level scenario. They should also be located such that it is not susceptible to other environmental loads such as wind. Flooding produced by Hurricane Sandy exposed weaknesses in the location of standby power (e.g., generators). Generators and other electrical equipment that were placed in basements failed due to flooding (FEMA 2013).

Figure 8-3. Large Standby Portable Power Unit Used when Basement Generators Failed (FEMA 2013)

In recent events where in-situ standby power systems did not meet the desired level of performance and failed, portable standby power was brought in to help bring facilities back online until power was restored or on-site standby generators were restored. For example, Figure 8-3 shows a portable standby generator power unit used in place of basement standby generators that failed due to flooding of Verizon's Central Office at 104 Broad Street in Manhattan, NY after Hurricane Sandy (FEMA 2013).

After 9/11, the Verizon Central Office at 140 West Street (i.e., the one impacted by the collapse of WTC 7) was hardened to prevent loss of service in a disaster event (City of New York, 2013). Between 9/11 and Hurricane Sandy, the 140 West Street Central Office:

- Raised their standby power generators and electrical switchgear to higher elevations
- Used newer copper infrastructure (i.e., encased the copper wires in plastic casing)
- Provided pumps to protect against flooding

The City of New York (2013) compared the performance of this Central Office to the one at 104 Broad Street (also affected by Sandy) that had not been hardened. The 104 Broad Street Central Office positioned its standby power generators and electrical switchgear below grade (i.e., in a basement) and had old copper infrastructure in lead casing (City of New York 2013). While the 140 West Street Central Office (i.e., the hardened Central Office) was operational within 24 hours, the 104 Broad Street Central Office was not operational for 11 days.

The success story of the 140 West Street Central Office during and after Hurricane Sandy illustrates that making relatively simple changes in location of equipment can significantly improve infrastructure/equipment performance following a disaster event. This example shows careful planning of critical equipment location and protection is essential to achieving the performance goal of continued service in the wake of a disaster event.

An alternative to raising all critical equipment is to protect it so water does not enter the Central Office during a flood event. Sandbags are often used in North America to protect buildings or openings of buildings from flooding. However, these sandbag barriers are not always effective. After the 9.0 magnitude earthquake and tsunami in the Great Tohoku, Japan Region in 2011, Kwasinksi (2011) observed that watertight doors performed well in areas that experienced significant damage and prevented flooding of critical electronic equipment in Central Offices. Watertight doors, such as that shown in Figure 8-4, can be used in the United States to prevent water from entering a Central Office due to inland (riverine) or coastal (storm surge, tsunami) flooding. Note that other openings, such as windows, may also be vulnerable to flooding and need to be sealed effectively so other failures in the building envelope do not occur (Kwasinski 2011).

Figure 8-4. Watertight Door Used on Central Office in Kamaishi, Japan (Kwasinski 2011)

Placement and protection of critical equipment should be considered for all types of natural disasters a community may experience. As illustrated by the Hurricane Sandy example, different hazard types warrant different considerations. Equipment stability must be considered for earthquakes. Figure 8-5 shows an example of failure inside a telecommunications Central Office in the 1985 Mexico City Earthquake (OSSPAC 2013). The building itself did not collapse, but light fixtures and equipment failed. Critical equipment in earthquake prone regions should be designed and mounted such that shaking will not lead to equipment failure.

As indicated in Chapter 3 and presented in Table 8-1 through Table 8-3 (see Section 8.3), the desired performance of the communications system in the routine, expected, and extreme event (as defined in Chapter 3) is little or no interruption of service. These Central Office buildings are considered Risk Category III buildings in ASCE 7 and, consequently, should be designed to remain functional through the 1/100 year flood elevation + 1 ft, or the design-based elevation (whichever is higher), the 1,700 year wind event (based on ASCE 7-10), and the 0.2 percent earthquake. In the case of Hurricane Sandy, the desired performance with respect to flooding was not achieved.

***Figure 8-5. Light Fixture and Equipment Failure inside Central Office in Mexico City 1985 Earthquake** (Alex Tang, OSSPAC 2013)*

Although these facilities are less vulnerable to wind than flood, in the case of routine, expected, and extreme events it is critical that the building envelope performs as intended since failure of the building envelope can allow significant amounts of water to enter the building and damage components. Historically, few building envelopes actually meet anticipated performance levels.

Threat to/from Interdependent Services. As discussed in Section 8.1.3 and Chapter 4, interdependencies play a big role in the overall performance of communications infrastructure. Central Offices rely on external power for critical equipment and electrical switchgear. The transportation system is needed for workers to maintain and monitor the functionality of equipment. Functioning water is needed for technicians to enter a building, meaning that if water the water system is not functional, repairs cannot be made to critical equipment.

Electric power is the most obvious and important dependency of the communication and information system. For Central Offices, external electric power is needed to ensure the air conditioning system is functional so it can serve as a cooling system for critical electrical equipment. Although critical equipment is typically connected to backup batteries and/or standby generators, air conditioning systems are not connected to these standby systems. When there is a loss of electric power, critical telecommunications equipment can overheat and shut down as a result (Kwasinski 2009).

Intra-dependencies with the rest of the communications infrastructure network must be considered. A Central Office serves as a switching node in the network and if its functionality is lost, stress is put on the network because the links (distribution system) are not connected as intended.

8.2.1.2. Transmission and Distribution

While the Central Offices of the telecommunications systems play a key role in the functionality of the system, the transmission and distribution system must also be maintained and protected adequately for continued service. There are several components that must be considered for continued functionality:

- First/last mile transmission
- Type of cable (copper wires, coaxial cables, fiber optic cables)
- Overhead vs. Underground Wires
- Distributed Loop Carrier Remote Terminals (DLC RTs)
- Cable Television (CATV) Uninterruptible Power Supply (UPS)

First/Last Mile Transmission. The "first/last mile" is a term used in the communications industry that refers to the final leg of delivering services, via network cables, from a provider to a customer. The use of the term "last mile" implies the last leg of network cables delivering service to a customer, whereas "first mile" indicates the first leg of cables carrying data from the customer to the world (e.g., calling out or uploading data onto the Internet). Although the name implies it is one mile long, this is not always the case, especially in rural communities where it may be much longer (WV Broadband 2013).

As learned from the 9/11 attacks, the first/last mile is a key to resilience for telecommunications and information infrastructure, especially for downtown business telecom networks. In urban settings, service providers typically connect Central Offices in a ring, which connects to the Internet backbone at several points (Lower Manhattan Telecommunications Users' Working Group, 2002). Although the first/last mile is beyond this ring of Central Offices, the redundancy results in a resilient method that improves the likelihood that service providers will achieve their systems performance goal of continual service. Path diversity is built into the infrastructure system often using nodes that connect to the network backbone. However, as learned during workshops used to inform this framework, part of the last mile typically does not connect to the network backbone and, thus, is vulnerable to single-point failures. Furthermore, the location of the node failure also impacts service. If the failed node is between a Central Office and the buildings/facilities it services (i.e., first/last mile) the first/last mile customers will be of service.

There is likely to be less redundancy in the telecommunication and information network cable systems in rural communities. Historically, rural and remote communities have not used these services as frequently or relied as heavily on them as urban communities. This has been the case because:

- In the past, technology to send large amounts of data over a long distance had not been available
- The cost for service providers to expand into remote communities may be too high and have a low benefit-cost ratio

As a result of the lack of redundancy in rural and remote communities, a failure of one node in the service cables (single point of failure) may be all that is necessary for an outage to occur. Therefore, it may not be practical, currently, for rural and remote communities to expect the same performance goals as urban communities. As communications technology continues to grow and change, the level of redundancy (or path diversity) in communications infrastructure delivering services to rural/remote communities is likely to increase. In the case where the reason for loss of telecommunication services in the loss of external power rather than failure of the communications system itself, restoration of services may be quicker for rural communities. As learned in stakeholder workshops held to inform this framework, it was observed in Hurricanes Katrina and Sandy that power can be easier to restore in rural areas because in densely populated areas, components tend to be packed in tightly and other systems need to be repaired first before getting to the power supply system.

Copper Wires. Copper wires work by transmitting signals through electric pulses and carry the low power needed to operate a traditional landline telephone. The telephone company (i.e., service provider) that owns the wire provides the power rather than an electric company. Therefore, the use of traditional analog (i.e., plain old telephone service or POTS) landlines that use copper wire lessens the interdependency on external power (ALA 2006). As a result, in a natural hazard event resulting in loss of external power, communication may still be possible through the use of analog landlines (though this is not guaranteed).

Although copper wires perform well in many cases, they are being replaced by fiber optic cables because copper wires cannot support the large amount of data required for television and high-speed Internet, which has become the consumer expectation in the 21st century (Lower Manhattan Telecommunications Users' Working Group 2002).

Some service providers are interested in retiring their copper wires. Keeping both fiber optic and copper wires in service makes maintenance expensive for service providers and, hence, for customers (FTTH Council 2013). Copper wire is an aging infrastructure that becomes increasingly expensive to maintain. Verizon reported its operating expenses have been reduced by approximately 70 percent when it installed its FiOS (fiber optic) network and retired its copper plant in Central Offices (FTTH Council 2013).

Despite the advantages of traditional copper wire, there are also well-documented problems. As seen during and after Hurricane Sandy, copper wire is susceptible to salt water flooding. Once these metal wires are exposed to salt water, they fail (City of New York 2013). One solution to this problem is to ensure the copper wire is encased in a plastic or another non-saltwater-sensitive material. Furthermore, copper wires are older and generally no longer installed.

Coaxial Cables. Coaxial cable is a more modern material and commonly used for transmission. It offers more resistance to water and is, therefore, not as susceptible to flood damage as copper wires. After Hurricane Sandy, these coaxial wires generally performed well with failures typically associated with loss of power to the electrical equipment to which they were connected (City of New York 2013). Coaxial cable has been and continues to be primarily used for cable television and Internet services. However, coaxial cables are being replaced by fiber optic cable since fiber optics can carry all types of services.

Fiber Optic Cables. Fiber optic cables are more resistant to water damage than either coaxial cable or copper wire (City of New York 2013). Fiber optic cables are now commonly used to bundle home services (television, high-speed Internet, and telephone) into one system, and provide ultra-high speed Internet. The use of fiber optic cables allows for transmission of large amounts of data on a single fiber. These cables are fully water resistant (City of New York 2013). Unfortunately, these services rely more heavily on power provided by a power utility instead of the communications provider itself for the end user. Consequently, during and after a natural hazard event where power is frequently interrupted, landline communications using fiber optic cables are lost in the absence of end user standby power equipment (ALA 2006). In fact, some communities turn off the power prior to the arrival of hurricane force winds for safety purposes. This prevents "live" electric lines from falling on roads, homes, etc., but it also eliminates the external power source for telecommunications of the end user. Some service providers provide in-home battery backup for cable and telephone.

Overhead vs. Underground Wires. Distribution wire can be strung overhead using utility poles, or run underground. There are advantages and disadvantages for both options.

Overhead wire failures are relatively easily located and repaired in the wake of a natural hazard event. However, their exposure makes them especially susceptible to high wind (e.g., hurricanes and tornadoes) and ice hazards. In high wind events, overhead wires may fail due to the failure of poles by the direct action of wind acting on poles and cables, or trees falling onto the cables. Figure 8-6 shows an example of a failed cable television (CATV) line due to the direct action of wind during Hurricane Katrina.

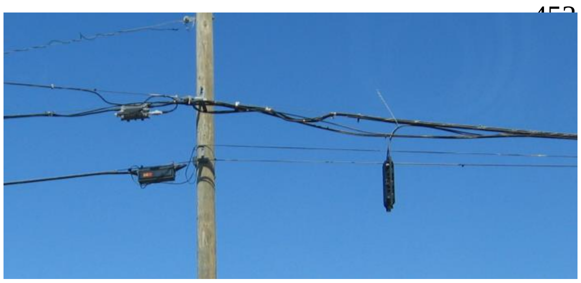

Figure 8-6. Failure of CATV cable due to the direct action of wind (Kwasinski 2006)

Widespread failure of the aboveground system in high winds and ice storms is common and often associated with the effects of tree blow-down and falling branches. This is difficult to mitigate without removing trees. Some improvement in performance can be achieved with continued trimming of branches, to reduce both the likelihood of branches falling on lines and wind-induced forces acting upon the trees, which reduces the blow-down probability. The electric utility that owns the poles performs the tree trimming. Chapter 7 discusses challenges associated with tree removal and trimming.

Ice storms can also result in failure of aboveground communication infrastructure. For example, in January 2009, Kentucky experienced an ice storm in which long distance telephone lines failed due to loss of power and icing on poles, lines, and towers (Kentucky Public Service Commission 2009). Similar to wind hazards, accumulation of ice seen in Kentucky, paired with snow and high winds, led to tree falling onto overhead telephone and power lines. However, unlike power lines, telecommunication lines that have limbs hanging on them or fall to the ground will continue to function unless severed (Kentucky Public Service Commission 2009). Since long distance telecommunications depend on power from another source (i.e., power providers), communication with those outside the local community was lost during the storm. Following the 2009 Kentucky ice storm, many communities became isolated and were unable to communicate their situation and emergency needs to regional or state disaster response officials (Kentucky Public Service Commission 2009). However, as learned in workshops held to inform this framework, long distance communications do have standby power capability.

Emergency response and restoration of the telecommunications infrastructure after a hazard event is an important consideration for which the challenges vary by hazard. In the cases of high wind and ice/snow events, tree fall on roads (Figure 8-7) slows down emergency repair crews from restoring power and overhead telecommunications. Ice storms have their own unique challenges in the recovery process. In addition to debris (e.g., trees) on roads, emergency restoration crews can be slowed down by ice-covered roads, and soft terrain (e.g., mud) in rural areas. Emergency restoration crews also face the difficulty of working for long periods of time in cold and windy conditions associated with these events. Communities should consider the conditions under which emergency restoration crews must work in establishing realistic performance goals of telecommunications infrastructure.

Figure 8-7. Trees Fallen Across Roads Due to Ice Storm in Kentucky Slowed Down Recovery Efforts (Kentucky Public Service Commission 2009)

Although installation of underground wires eliminates the concern of impacts from wind, ice, and tree fall, underground wires may be more susceptible to flood if not properly protected, or earthquake damage and liquefaction.

Communities in parts of the United States have debated converting their overhead wires to underground wires to eliminate the impacts from wind, ice, and tree fall. However, converting overhead to underground wires is both challenging and expensive (City of Urbana Public Works Department 2001). The main challenges/issues associated with converting from overhead to underground wires noted in the City of Urbana's Public Works Department Report (2001) are:

- Shorter design life of the underground system
- Lack of maintenance and repair accessibility of the underground facilities
- Aboveground hardware issues
- Converting all customers' wiring to accommodate underground in place of aboveground services

Service providers, like electric utility providers, would pass the cost associated with converting from overhead to underground wires to their customers (City of Urbana Public Works Department 2001). As discussed in Chapter 7 (Energy Systems), electric utility companies have tree trimming programs (and budgets) to reduce the risk of tree branches falling and damaging their distribution lines. The power utility is also reimbursed by telecommunications service providers since their services also benefit from the tree trimming program. The cost associated with maintaining a dedicated tree trimming program is significantly less than converting from overhead to underground wires because converting to an unground network involves many expensive efforts, including removing the existing system, lost cost resulting from not using the existing system for its design life, underground installation costs, and rewiring each building to accommodate underground utilities (City of Urbana Public Works Department 2001). Since telecommunications service providers and electric power utilities share infrastructure, they should work together to decide what is best for their distribution system.

Loop Digital Carrier Remote Terminals. Loop Digital Carrier Remote Terminals (DLC RTs) are nodes in the landline and Internet network that allow service to be distributed beyond the range for a given Central Office or exchange. Historically, copper wires provide service from a Central Office to a customer within approximately 4 kilometers of that Central Office (Kwasinski et al. 2006). The use of fiber optic cables and curbside DLC RTs can extend this range of service to approximately 10 km (Kwasinski et al. 2006). Therefore, DLC RTs provide a possible solution for service providers to reach customers further from their existing Central Offices or exchanges without having to invest in the construction of additional Central Offices. However, these nodes will not always allow sufficient capacity to replace the demand of a Central Office or node. Therefore, the service provider should consider how many customers it needs to serve (i.e., demand) with the node and if that number will grow (e.g., due to expansion of developments in area) or shrink (e.g., customers leave and do not come back as was the case after Hurricane Katrina).

DLC RTs can be used to rapidly replace smaller Central Offices or nodes as was done after Hurricane Katrina when less capacity than before the event was needed (Kwasinski 2011). This can help limit downtime of the network, but appropriate planning is needed to ensure the DLC RTs do not fail after the next hazard event. Perhaps the two most important things for service providers to consider when implementing DLC RTs are construction to limit vulnerability to hazards and standby power, which is a crucial consideration for any communications infrastructure.

A key lesson learned for DLC RTs from Hurricane Katrina was that nodes should be elevated in storm surge areas so they are not impacted in future hazard events (Kwasinski 2011). The former BellSouth in New Orleans implemented this practice in New Orleans and the surrounding region after Hurricane Katrina. Figure 8-8 shows a DLC RT elevated on a platform. The building in the background of the figure was a small Central Office in which all equipment was damaged during Hurricane Katrina, but never replaced (Kwasinski 2011). When the next set of storms (i.e., Hurricanes Gustav and Ike) passed through the region in 2008, many of the DLC RTs were not physically damaged due to storm surge.

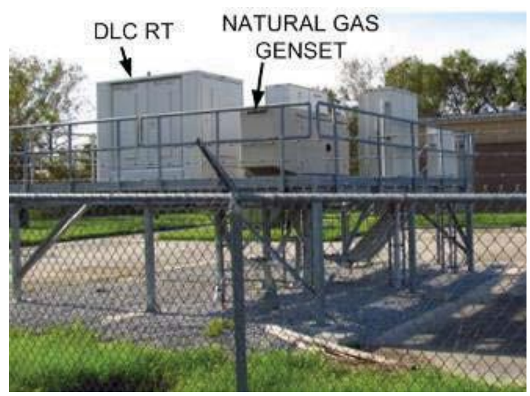

Figure 8-8. Elevated DLC RT with Natural Gas Standby Generator Installed After Hurricane Katrina (Kwasinski 2011)

Like cell towers, DLC RTs, need standby power to function when external power is disrupted as often occurs in a hazard event (see Section 8.2.3.1). Standby power generators can either be installed permanently, or deployed after a disruption in service. There are challenges associated with both options.

Waiting until after an event to deploy standby generators can be difficult because:

- It can require significant labor support and logistics to mobilize a large number of standby generators
- Fuel-operated standby generators require refueling during extended outages, which can be problematic due to access to fuel
- Transportation routes to reach nodes may be impassible due to debris

In contrast, permanent generators can be expensive to install and maintain for a large number of sites, and require periodic testing to ensure they will function when needed. Furthermore, permanent generators should also be placed such that they are less vulnerable to the hazards that face the community (e.g., raised above anticipated storm surge levels). The installation of permanent standby generators (and raising the DLC RTs) after Hurricane Katrina (see Figure 8-8), helped reduce the amount of telecommunications outages during the 2008 Hurricanes (Gustav and Ike) that struck the same region (Kwasinski 2011).

As discussed in other chapters of this document (e.g., Chapter 7), there are several energy options for standby generators. The most common is liquid fuel. Fuel is generally widely available, but may not be immediately after a disaster event which may make refueling challenging if outage times of external power extend for a long period of time. Permanent natural gas standby generators have also been used in the past. Natural gas standby generators performed well during Hurricane Gustav (Kwasinski 2011). However, natural gas generators are not the best option in general because natural gas distribution lines are often shut down prior to an anticipated hazard event to prevent fire and explosions. As a result, natural gas may not be the best option for standby power at critical nodes in the communications network.

Cable Television (CATV) Uninterruptible Power Supply (UPS). Many people receive landline telephone, Internet, and cable television through the same service provider. These services are bundled and distributed to the customers in a similar manner to the typical landline using coaxial cable. UPS systems are used to inject power into the coaxial cable so CATV service can be delivered to customers (Kwasinski et al. 2006). UPS systems are placed on a pedestal on the ground or on a utility pole. Kwasinski (2011) documented several of the challenges associated with this infrastructure, including the placement of UPS' on the ground or on utility poles, and providing adequate standby power. Like all of other critical equipment discussed in this chapter, it is important to place UPS systems such that their vulnerability to hazards is minimized. Figure 8-9 (left) shows two UPS systems after Hurricane Katrina: one that was mounted on a pedestal at ground level was destroyed due to storm surge, and another that was mounted to a utility pole was not damaged. However, Figure 8-9 (right) also shows that placing UPS systems too high on utility poles can interfere with regular maintenance (Kwasinksi 2011). As previously mentioned, providing adequate standby power is a challenge, particularly for a pole-mounted UPS, because the additional load on a utility pole to provide sufficient standby power may be more than the pole can withstand.

Figure 8-9. Placement of UPS Systems is an Important Consideration for Resilience and Periodic Maintenance (Kwasinski 2009)

8.2.2. Internet Systems

The Internet has become the most used source of communication over the past couple of decades. It is continually used for e-mail, online shopping, receiving/reading the news, telephony, and increasingly for use of social networking. Businesses rely heavily on the Internet for communication, sending and receiving documents, video conferencing, e-mail, and working with other team members using online collaboration tools. The Internet is heavily used by financial institutions for transferring funds, buying and selling stocks, etc. Connectivity is becoming more important in the healthcare industry as it moves towards electronic medical records.

High-speed Internet is often tied in with telephone and cable by service providers through coaxial or fiber optic wires. The Internet depends on the electric power system, and loss of power at any point along the chain from source to user prevents data reception. As a result, Internet dependency on the electric power system makes it vulnerable to the performance of the power system in a natural hazard event. A concern for Internet systems, as is the case for landlines, is single points of failure (i.e., an individual source of service where there is no alternative/redundancy).

8.2.2.1. Internet Exchange Points (IXP)

Internet Exchange Points are buildings that allow service providers to connect directly to each other. This is advantageous because it helps improve quality of service and reduce transmission costs. The development of IXPs has played a major role in advancing development of the Internet ecosystem across North America, Europe, and Asia (Kende and Hurpy, 2012). IXPs now stretch into several countries in Africa and continue to expand the reach of the Internet. IXPs facilitate local, regional, and international connectivity.

IXPs provide a way for members, including Internet Service Providers (ISPs), backbone providers, and content providers to connect their networks and exchange traffic directly (Kende and Hurpy 2012). Similar to Central Offices for landlines, this results in IXPs being a potential single point of failure.

The buildings housing the IXPs would be expected to meet the ASCE 7 requirements for critical buildings (Occupancy Category IV) and, consequently, would be expected to perform with no interruption of service for the “expected” event, or hazard level. The facilities would be expected to have sufficient standby power to function until external power to the facility is brought back online.

Location of Critical Equipment in IXPs. Another similarity to telecommunications Central Offices is that the location and protection of critical equipment is important. Critical equipment should be protected by placing it in locations where it will not be susceptible to expected hazards in the community. For example, inevitably some buildings are in floodplains because many large urban centers are centered around large bodies of water or on the coast. The owner, engineers, maintenance, and technical staff must all be aware of potential hazards that could impact the equipment within the structure. As should be done for telecommunications Central Offices, the following considerations should be taken into consideration for the critical equipment of IXPs:

- Electrical and emergency equipment should be located above the elevation of an “extreme” flood, which is to be defined by the community (see Chapter 3). Alternatively, tools such as Sea, Lake, and Overland Surges from Hurricanes (SLOSH) maps could be used to define the minimum elevation for electrical and critical equipment.
- Rooms housing critical equipment should be designed to resist extreme loads for the community, whether it is earthquake, high wind, blast, other hazards, or a combination of hazards. Remember that fire is often a secondary hazard that results from other hazard events.
- Where possible, redundancy and standby power for critical equipment should be provided.

All too often, communities see the same problems and damage in the wake of a natural hazard event (e.g., loss of power, loss of roof cover and wall cladding leading to rain infiltration in high wind events). Fortunately, many problems can be mitigated by sufficient planning and risk assessment (as previously discussed in the comparison of two telecommunications Central Offices in New York City after Hurricane Sandy). Careful placement and protection of critical equipment can help achieve performance goals of the Internet’s critical equipment. For example, in flood prone regions, critical equipment should be placed above the extreme flood level for the area. In earthquake regions, critical equipment should be designed and mounted such that shaking from earthquake events does not cause failure.

8.2.2.2. Internet Backbone

The Internet Backbone refers to the cables that connect the "network-of-networks." The Internet is a system of nodes connected by paths/links. These paths run all over the United States and the rest of the world. As a result, many of the same challenges identified for the landline cables for fiber optic cables exist for Internet, namely that it requires power to function. The heavy reliance on power impacts the performance and recovery goals of Internet service for service providers and their customers.

Path Diversity. Path diversity refers to the ability of information to travel along different paths to get to its destination should there be a failure in its originally intended path (i.e., path diversity is synonymous with redundancy). The more diversity that exists, the more reliable the system.

8.2.3. Cellular/Mobile Systems

The cellular telephone system has most of the same vulnerabilities as the landline system, including the local exchange offices, collocation hotels, and cable head facilities. Other possible failure points unique to the cellular network include the cell site (tower and power) and backhaul switches at Central Offices. Figure 8-1 (page 5) shows how the cellular phone network fits within the telecommunication network. At the base of a cell tower is switchgear (also known as Cell Site Electronics) and standby power. Damage of switchgear at the base of the tower prevents switching to standby power when commercial power fails.

8.2.3.1. Cell Towers

Virtually all natural hazards including earthquake, high wind, ice and flood affect the ability of an individual cell tower to function through loss of external power or failure of cell phone towers themselves.

Loss of External Power. Large scale loss of external power occurs relatively frequently in hurricanes (mainly due to high wind and flooding), large thunderstorm events (such as those associated with derechos and tornadoes), ice storms, and earthquakes. Some cell towers are equipped with batteries designed to provide four to eight hours of standby power after loss of external power (City of New York 2013). In the past, the FCC has attempted to mandate a minimum of eight hours of battery standby power, but the requirement was removed by the courts. However, adequate standby power should be provided for cell towers, particularly in areas that serve critical facilities. The functionality of the tower can be extended through use of permanent or portable diesel generators. Portable generators were used in New York following Hurricane Sandy in 2012. The installation of permanent diesel generators has been resisted by the providers due to the high cost and practicality (City of New York 2013).

Recalling that buildings and systems should remain fully functional during and after a routine event (Chapter 3), all cellular towers and attached equipment should remain operational. There is an expectation that the 9-1-1 emergency call system will remain functional during and after the event. Considering the poor performance of the electric grid experienced during recent hurricanes (which produced wind speeds less than the nominal 50 to 100-year values as specified in ASCE 7 [93, 95, 02 and 05]), external power is unlikely to remain functional during the expected, or even routine (as defined in Chapter 3) event. Consequently, adequate standby power is critical to ensure functionality. Recent experience with hurricanes and other disaster events suggest the standby power needs to last longer than the typical current practice of four to eight hours (City of New York 2013).

In flood prone areas, the standby power needs to be located, at a minimum, above the 100-year flood level to ensure functionality after the event. Similarly, the equipment must be resistant to the 50-year earthquake load.

The use of permanently located diesel electric standby power poses significant difficulties due to the initial and ongoing required maintenance costs. Diesel generators are often (though not always) loud and may generate complaints from nearby residents. In the case of events such as hurricanes and major ice storms where advanced warning is available, portable generators can be staged and deployed after the storm. However, for widespread hazard events, such as hurricanes and ice storms, the need often exceeds the ability to deploy all of the portable generators needed. When they are deployed, the portable generators usually require refueling about once per day so continued access is important. Permanent generators also require refueling, but the frequency is variable due to the different capacities of permanent generators. In events where there is little to no warning, such as earthquakes and tornadoes, staging of portable generators cannot be completed ahead of time. However, for localized events that are unpredictable and short duration (e.g., tornadoes, tsunamis), portable generators may be the best approach for quick recovery of the system's functionality.

In highly urbanized areas, such as New York City, cell towers are frequently located on top of buildings, preventing the placement of permanent diesel standby generators and making it difficult to supply power from portable generators because of impeded access.

Improvements in battery technology and the use of hydrogen fuel cell technologies may alleviate some of the standby power issues. Furthermore, newer cellular phone technologies require less power, potentially leading to longer battery life. Standby battery technology is a key consideration in establishing the performance goals of cellular phones in the wake of a hazard event.

Failure of Cell Phone Towers. Collapse of cell phone towers due to earthquake, high winds, or flooding should not be expected to occur when subject to a natural hazard event of magnitude less than or equal to the expected event. This was not the case in Hurricane Katrina (2005) where cell phone towers were reported to have failed (DHS, 2006), although many failed after being impacted by flood-borne debris (e.g., large boats, etc.), whose momentum was likely well beyond a typical design flood impact. After an event, failed towers can be replaced by temporary portable towers. Similarly, the January 2009 Kentucky ice storm had cell phone tower failures due to the combination of ice accumulation and winds over 40 mph (Kentucky Public Service Commission 2009).

Cell towers may be designed to either ASCE Category II or ASCE Category III occupancy requirements. The latter is used when the towers are used to support essential emergency equipment or located at a central emergency hub. Consequently, in the case of wind and flood, the towers and equipment located at the base of the tower should perform without any damage during both routine and expected events (Chapter 3).

More commonly, cell towers are designed to meet the criteria of TIA/EIT-222-G. Prior to the 2006 version of this standard (which is based on the ASCE 7 loading criteria), it used Allowable Stress Design (ASD) rather than Load and Resistance Factor Design, wind loads used fastest mile wind speeds rather 3-second gust, and seismic provisions were not provided. The ice provisions differ from version to version, but no major differences in methodology have been noted. Therefore, cell towers designed to meet the criteria of TIA/EIT-222-G should perform well in an expected wind, ice, or earthquake event. However, older cell towers that have not been retrofitted/upgraded to meet the 2006 version of TIA/EIT-222-G may not perform as well. Specifically, cell towers in earthquake-prone regions may have been designed and built without guidance on the loading, which may have resulted in either over- or under-designed cell towers in these regions.

Backhaul Facilities. Backhaul facilities serve a purpose similar to that of the Central Offices and consequently should meet the same performance goals, including proper design of the standby power system.

8.3. Performance Goals

Although the goal of communities, infrastructure owners, and businesses is to have continued operation at all times, 100 percent functionality is not always feasible in the wake of a hazard event given the current state of infrastructure in the United States. Depending on the magnitude and type of event, the levels of damage and functionality will vary. Most importantly, performance goals of the communications infrastructure will vary from community to community based upon its needs and should be defined by the community and its stakeholders. As discussed in Section 8.2, there are many examples of service providers and other infrastructure owners who have successfully made changes to their infrastructure system such that their downtime has been shortened or even eliminated after a hazard event.

This section provides examples of performance goals for the fictional town of Centerville, USA. Communication infrastructure stakeholders and communities can use performance goals tables to assess their infrastructure and take steps in improving their resilience to hazard events. Note that performance goals are specified in terms of recovery time. However, mitigation techniques, including improving design and code/standard enforcement, play significant roles in accomplishing performance goals. Therefore, both mitigation strategies and recovery plans can be used to achieve performance goals.

Before establishing performance goals, it is imperative to understand who the owners, regulatory bodies, and stakeholders of the communications infrastructure are and how they operate. All groups should be involved in establishing performance goals and working together to narrow gaps in resilience.

Infrastructure Owners, Regulatory Bodies, and Stakeholders. Ownership and regulation of communication and information infrastructure systems adds a layer of complexity for resilience. Governments typically do not own communication infrastructure other than in their own facilities. However, Federal, State, and Local government agencies are involved in the regulation of communications infrastructure. The Federal Communications Commission (FCC) has an advisory committee called the Communications Security, Reliability, and Interoperability Council (CSRIC) that promotes best practices, although there are limited requirements for compliance with the practices. However, best practices are often implemented by service providers (despite not being standards) because they help mitigate risks, which is a good idea in a competitive industry.

The FCC has authority over wireless, long-distance telephone, and Internet services, whereas state agencies have authority over local landlines and agencies at all levels have regulatory authority over cable (City of New York 2013). Within these three levels of government, there may be multiple agencies involved in overseeing infrastructure. State and local Departments of Transportation (DOTs) control access to roadway rights-of-way for construction. The local Department of Buildings (DOB) regulates the placement of electrical equipment, standby power, and fuel storage at critical telecommunications facilities as specified in their local Building Codes (City of New York 2013).

Service providers own communications infrastructure. The Telecommunications Act of 1996 was established to promote competition in the communications industry (FCC 2011), which would result in lower prices for customers. This has resulted in a growing number of industry players who share infrastructure to offer options for their services to customers more efficiently. Service providers can sometimes share infrastructure to provide their services. However, their infrastructure cannot always be shared because different providers use different technology that is not compatible.

Telecommunication and Cable/Internet Service Providers, such as AT&T and Verizon, often share infrastructure with providers in the energy industry. For example, utility poles for overhead wires typically serve to transport electric energy, telecommunications, and cable. It is, therefore, essential that key members from these service providers are involved in establishing, or agreeing to, the performance goals for the communications infrastructure. Improved performance of their infrastructure, much like the power industry, will result in improved service in the wake of a hazard event. Moreover, improvements made to achieve performance goals may result in better performance on a day-to-day basis. A service provider may benefit from excellent performance following a hazard event because customers frustrated with their own service may look for other options that are more reliable. Service providers may also experience different damage levels for the same quality infrastructure due to poor fortune, which can provide an inaccurate perception that it is not as reliable as another service provider. However, this may not always be true because some service providers share infrastructure and thus, failures may occur due to interdependencies. Moreover, in a competitive cost-driven industry, the cost to make a system more resilient, which is passed down to customers, may result in losing business. Therefore, including service providers in the group of stakeholders is key because their industry is quite complex.

After the AT&T divestiture of 1984, the end user became responsible for the voice and data cabling on its premises (Anixter Inc. 2013). Therefore, building owners are responsible for communications infrastructure within their facilities. As a result, standards have been developed by the American National Standards Institute/Telecommunications Industry Association (ANSI/TIA) for different types of premises, including:

- Commercial buildings (e.g., office and university campus buildings)
- Residential buildings (e.g., single and multi-unit homes)
- Industrial buildings (e.g., factories and testing laboratories)
- Healthcare facilities (e.g., hospitals)

Communications infrastructure has owners and stakeholders from multiple industries that must be included in establishing the performance goals and improving resilience of system components. For resilience of the distribution communication systems, service provider representatives, including designer professionals (engineers and architects for buildings owned by service providers such as Central Offices/data centers), planners, utility operators, and financial decision makers (i.e., financial analysts) for power service providers must be included in the process. Owners of buildings that are leased by service providers to house critical equipment and nodes in their system are important stakeholders. Additionally, representatives of end users from different industries should be included to establish performance goals and improve resilience of communications system transfer from provider to building owner. Specifically, transfer of telecommunications and Internet to a building is often through a single point of failure. Those involved in building design, such as planners, architects, engineers, and owners need to be aware of potential opportunities to increase redundancy and resiliency.

Performance Goals. Performance goals in this document are defined in terms of how quickly the infrastructure's functionality can be recovered after a hazard event. Minimizing downtime can be achieved during the design process and/or recovery plans. Example tables of performance goals for communications infrastructure, similar to the format presented in the Oregon Resilience Plan (OSSPAC 2013), are presented in Table 8-1 through Table 8-3. These tables of performance goals are examples for routine, expected, and extreme events, respectively. Note that these performance goals were developed based on wind events using current ASCE (ASCE 7-10) design criteria, performance seen in past high wind events, and engineering judgment. Thus, these goals can be adjusted by users as necessary for their community to meet its social needs, consider their state of infrastructure, and the type and magnitude of hazard. For example, an earthquake-prone region may have different performance goals because the design philosophy is for life safety as opposed to wind design which focuses on serviceability.

The performance goals tables (Table 8-1 to Table 8-3) are intended as a guide that communities/owners can use to evaluate the strengths and weaknesses of the resilience of their communications systems infrastructure. As previously discussed, the performance goals may vary from community-to-community based upon its social needs. Communities/owners and stakeholders should use the table as a tool to assess what their performance goals should be based on their local social needs. Tables similar to that of Table 8-1 to Table 8-3 can be developed for any community (urban or rural), any type of hazard event, and for the various levels of hazards (routine, expected and extreme) defined in Chapter 3 of the framework.

Representatives of the stakeholders in a given community should participate in establishing the performance goals and evaluating the current state of the systems. The City of San Francisco provides an excellent example of what bringing stakeholders together can accomplish. San Francisco has developed a lifelines council (The Lifelines Council of the City and County of San Francisco 2014), which unites different stakeholders to get input regarding the current state of infrastructure and how improvements can be made in practice. The lifelines council performs studies and provides recommendations as to where enhancements in infrastructure resilience and coordination are needed (The Lifelines Council of the City and County of San Francisco 2014). Their work has led to additional redundancy being implemented into the network in the Bay Area.

Granularity of Performance Goals. Table 8-1and Table 8-3 present examples of performance goals for different components of the communications infrastructure when subjected to each hazard level. The list of components for this example is not intended to be exhaustive. These lists vary by community based on its size and social needs. In terms of granularity of the performance goals table, the communications infrastructure system is broken down into three categories (see Table 8-2): 1) Core and Central Offices, 2) Distribution Nodes, and 3) Last Mile.

The Core and Central Offices could be split into two different functional categories by nationwide service providers. The Core refers to the backbone of service provider's network that includes facilities that store customer data and information. For larger service providers, these facilities may be geo-redundant and run in tandem so one widespread event, such as a hurricane or earthquake, cannot disrupt the entire network. Central Offices, discussed throughout this chapter, are regional nodes whose failure would result in widespread service disruptions. For this example of performance goals, the Core and Central Offices are treated as one functional category because the performance goals for Centerville, USA are the same (i.e., no failure of Central Offices or Core facilities).

Distribution nodes include the next tier in the communications network that collect and distribute communications at a more local (e.g., neighborhood) level. For Centerville, USA, this includes cell towers. For other communities, this may include DLC RTs and other local hubs/nodes.

The last mile refers to distribution of services to the customers. For landline, Internet, and cable, this is impacted by the performance of the distribution wires in a given hazard event. Wireless technology, such as cellular phones, operates using signals rather than physical infrastructure for distribution. Therefore, the last mile distribution is not needed. Although the system's components (e.g., underground cables, overhead cables, etc.) are not specifically included in the performance goals, they must be considered to achieve the performance goals specified by the community or service provider.

Developing Performance Goals Tables. The community/owners should work to establish their own performance goals. In the example tables (Table 8-1 to Table 8-3), performance goals are established for three levels of functionality. The orange shaded boxes indicate the desired time to reach 30 percent functionality of the component. Yellow indicates the time frame in which 60 percent operability is desired and green indicates greater than 90 percent operability. A goal is not set for 100 percent operability in this example because it may take significantly longer to reach this target and may not be necessary for communities to return to their normal daily lives. The performance of many of the components in the communication network, such as towers and buildings housing equipment are expected to perform according to their design criteria. Recent history, however, suggests this is frequently not the case.

The affected area of a given hazard can also be specified, which is often dependent on the type of hazard. For example, earthquake and hurricanes typically have large affected areas, whereas tornadoes and tsunamis have relatively small affected areas. The affected area is important for a community to consider because it will impact how much of the infrastructure may be damaged, which in turn will impact the duration of the recovery process. The disruption level based on the current state of the communications infrastructure system as a whole should be specified as usual, moderate or severe.

An "X" is placed in the each row of Table 8-1 through Table 8-3 as an example of how a community can indicate anticipated performance and recovery of the infrastructure in their evaluation. As seen in the tables, the hypothetical "X" indicates there is a significant gap between what is desired and what reality is for all of the components. This is a resilience gap. If the community decides that improving the resilience of their Central Offices is a top priority after its evaluation of their infrastructure, the next step would be to determine how to reduce this resilience gap. For Central Offices and their equipment, there are a number of solutions that can help narrow the gap in resilience, including hardening the building to resist extreme loads and protecting equipment from hazards such as flooding by elevating electrical equipment and emergency equipment above extreme flooding levels.

These lessons have been learned through past disasters, including the 9/11 terrorist attacks, Hurricanes Sandy and Katrina, etc. Section 8.6.1discusses potential methods to evaluate the anticipated performance of existing communications infrastructure. Sections 8.6.2 and 8.6.3 provide mitigation and recovery strategies that can be used to achieve the performance goals set by the community or service provider. The strategies in these sections also recognize it will take communities/owners time and money to invest in solutions, and provides possible long and short term solutions.

Emergency Responder Communication Systems. The performance goals include distribution infrastructure to critical facilities such as hospitals, fire and police stations, and emergency operation centers. However, the example performance goals for communication infrastructure do not include communication systems between emergency responders (fire/police/paramedics), which have their own communications networks and devices. Community emergency response providers should ensure their networks and devices remain functional in the immediate aftermath of a disaster event (i.e., there should not be any downtime of emergency responder communication networks). After a disaster event, functionality of critical services communication networks is essential to coordinating response to people who are injured, and fire or other hazard suppression.

Table 8-1. Example Communications Performance Goals for Routine Event in Centerville, USA

Disturbance		
(1)	Hazard	Any
	Affected Area for Routine Event	Localized
	Disruption Level	Minor

Restoration times		
(2)	30%	Restored
	60%	Restored
	90%	Restored
(3)	X	Current

Functional Category: Cluster	(4) Support Needed	(5) Target Goal	Overall Recovery Time for Hazard and Level Listed								
			Routine Hazard Level								
			Phase 1 – Short-Term			Phase 2 -- Intermediate			Phase 3 – Long-Term		
			Days			Wks			Mos		
			0	1	1-3	1-4	4-8	8-12	4	4-24	24+
Nodes/Exchange/Switching Points		**A**									
Central offices			90%		X						
Buildings containing exchanges			90%		X						
Internet Exchange Point (IXP)			90%		X						
Towers		**A**									
Free standing cell phone towers			90%		X						
Towers mounted on buildings			90%		X						
Distribution lines to …											
Critical Facilities		**1**									
Hospitals			90%		X						
Police and fire stations			90%		X						
Emergency operation center			90%		X						
Emergency Housing		**1**									
Residences			90%			X					
Emergency responder housing			90%			X					
Public shelters			90%			X					
Housing/Neighborhoods		**2**									
Essential city service facilities			60%	90%		X					
Schools			60%	90%		X					
Medical provider offices			60%	90%		X					
Retail			60%	90%		X					
Community Recovery Infrastructure		**3**									
Residences			60%	90%		X					
Neighborhood retail			60%	90%		X					
Offices and work places			60%	90%		X					
Non-emergency city services			60%	90%		X					
Businesses			60%	90%		X					

Notes: These performance goals are based on an expected wind event (using current ASCE design criteria) and performance seen in past high wind events.

Footnotes:

1 Specify hazard being considered
Specify level -- Routine, Expected, Extreme
Specify the size of the area affected - localized, community, regional
Specify severity of disruption - minor, moderate, severe

2 | 30% | 60% | 90% | Restoration times relate to number of elements of each cluster

3 | X | Estimated restoration time for current conditions based on design standards and current inventory
Relates to each cluster or category and represents the level of restoration of service to that cluster or category
Listing for each category should represent the full range for the related clusters
Category recovery times will be shown on the Summary Matrix
"X" represents the recovery time anticipated to achieve a 90% recovery level for the current conditions

4 Indicate levels of support anticipated by plan
R Regional
S State
MS Multi-state
C Civil Corporate Citizenship

5 Indicate minimum performance category for all new construction.
See Section 3.2.6

Table 8-2. Example Communications Performance Goals for Expected Event in Centerville, USA

Disturbance		
(1)	Hazard	Any
	Affected Area for Routine Event	Localized
	Disruption Level	Moderate

Restoration times		
(2)	30%	Restored
	60%	Restored
	90%	Restored
(3)	X	Current

Functional Category: Cluster	(4) Support Needed	(5) Target Goal	Overall Recovery Time for Hazard and Level Listed								
			Expected Hazard Level								
			Phase 1 – Short-Term			Phase 2 – Intermediate			Phase 3 – Long-Term		
			Days			Wks			Mos		
			0	1	1-3	1-4	4-8	8-12	4	4-36	36+
Nodes/Exchange/Switching Points		**A**									
Central Offices			90%			X					
Buildings containing exchanges			90%			X					
Internet Exchange Point (IXP)			90%			X					
Towers		**A**									
Free standing cell phone towers			90%			X					
Towers mounted on buildings			90%			X					
Distribution lines to …											
Critical Facilities		**1**									
Hospitals			90%			X					
Police and fire stations			90%			X					
Emergency Operation Center			90%			X					
Emergency Housing		**1**									
Residences					60%	90%		X			
Emergency responder housing					60%	90%		X			
Public Shelters					60%	90%		X			
Housing/Neighborhoods		**2**									
Essential city service facilities					30%	90%		X			
Schools					30%	90%		X			
Medical provider offices					30%	90%		X			
Retail					30%	90%			X		
Community Recovery Infrastructure		**3**									
Residences					30%	90%		X			
Neighborhood retail					30%	90%			X		
Offices and work places					30%	90%		X			
Non-emergency city services					30%	90%			X		
Businesses					30%	90%			X		

Footnotes: See Table 8-1, page 22.

Table 8-3. Example Communications Performance Goals for Extreme Event in Centerville, USA

Disturbance		
(1)	Hazard	Any
	Affected Area for Extreme Event	Regional
	Disruption Level	Severe

Restoration times		
(2)	30%	Restored
	60%	Restored
	90%	Restored
(3)	X	Current

Functional Category: Cluster	(4) Support Needed	(5) Target Goal	Overall Recovery Time for Hazard and Level Listed								
			Extreme Hazard Level								
			Phase 1 – Short-Term			Phase 2 -- Intermediate			Phase 3 – Long-Term		
			Days			Wks			Mos		
			0	1	1-3	1-4	4-8	8-12	4	4-36	36+
Nodes/Exchange/Switching Points		**A**									
Central Offices			90%			X					
Buildings containing exchanges			90%			X					
Internet Exchange Point (IXP)			90%			X					
Towers		**A**									
Free standing cell phone towers				90%		X					
Towers mounted on buildings				90%		X					
Distribution lines to …											
Critical Facilities		**1**									
Hospitals			90%			X					
Police and fire stations			90%			X					
Emergency operation center			90%			X					
Emergency Housing		**1**									
Residences					30%	90%			X		
Emergency responder housing					30%	90%			X		
Public shelters					30%	90%			X		
Housing/Neighborhoods		**2**									
Essential city service facilities					30%	60%	90%		X		
Schools					30%	60%	90%		X		
Medical provider offices					30%	60%	90%		X		
Retail					30%	60%	90%		X		
Community Recovery Infrastructure		**3**									
Residences					30%	60%	90%			X	
Neighborhood retail					30%	60%	90%			X	
Offices and work places					30%	60%	90%			X	
Non-emergency city services					30%	60%	90%			X	
Businesses					30%	60%	90%			X	

Footnotes: See Table 8-1, page 22.

8.4. Regulatory Environment

There are multiple regulatory bodies at the various levels of government (Federal, State, and Local) that have authority over communications infrastructure. There is no one regulatory body that oversees all communication infrastructure and is responsible for enforcement of the various standards and codes. The rapidly evolving technologies over the past 30 years have led to changes in regulatory jurisdiction, which adds complexity to the regulatory environment. This section discusses regulatory bodies of communications infrastructure at the Federal, State, and Local levels.

8.4.1. Federal

The regulatory body of communication services and, thus, infrastructure is the FCC. The FCC is a government agency that regulates interstate and international communications of telephone, cable, radio, and other forms of communication. It has jurisdiction over wireless, long-distance telephone, and the Internet (including VoIP).

As previously discussed, the FCC has an advisory group called the Communications Security, Reliability, and Interoperability Council (CSRIC) that promotes best practices. The council performs studies, including after disaster events (e.g., Hurricane Katrina), and recommends ways to improve disaster preparedness, network reliability, and communications among first responders (Victory et. al 2006). The recommended best practices are not required to be adopted and enforced since they are not standards. However, as learned in the stakeholder workshops held to inform this framework, industry considers best practices voluntary good things to do under appropriate circumstances. Furthermore, implementing best practices allows service providers to remain competitive in business.

8.4.2. State

State government agencies have authority over local landline telephone service. Most commonly, the agency responsible for overseeing communications infrastructure at the State level is known as the Public Service Commission (PSC). However, other State agencies have jurisdiction over telecommunications infrastructure as well. A prime example is the State DOT. The State DOT has jurisdiction over the right-of-way and, therefore, oversees construction of roads/highways where utility poles and wires are built. Utility poles and wires are commonly placed within the right-of-way of roads, whether it is aboveground or underground. The DOT has the ability to permit or deny planned paths of the utilities.

8.4.3. Local

Local government has jurisdiction over communication infrastructure through a number of agencies. The Department of Buildings (DOB), or equivalent, is responsible for enforcing the local Building Code. Therefore, the DOB regulates the placement of electrical equipment, standby power, and fuel storage at critical telecommunications facilities such as Central Offices (City of New York 2013).

Large cities, such as New York City, Chicago, Los Angeles, and Seattle have their own DOT (City of New York 2013). These local DOTs oversee road construction and the associated right-of-way for utilities (including communications infrastructure). Many smaller municipalities have an Office of Transportation Planning, which serves a similar function.

8.4.4. Overlapping Jurisdiction

Due to the complex bundling packages that service providers now offer customers, a number of regulatory bodies have jurisdiction over the various services provided in said bundle. For example, a bundled telephone, Internet and cable package functions under the jurisdiction of both Local (cable) and Federal (Internet and VoIP) agencies (City of New York 2013). Furthermore, changing from traditional landlines to VoIP shifts a customer's services from being regulated by State agencies to Federal agencies. As technology continues to evolve, jurisdiction over services may continue to shift from one level of government to another. Following the current trend of more and more services becoming Internet based, the shift of services may continue to move toward being under Federal agency regulations.

8.5. Standards and Codes

Codes and Standards are used by the communication and information industry to establish the minimum acceptable criteria for design and construction. The codes and standards shown in Table 8-4 were mainly developed by the American National Standards Institute/Telecommunications Industry Association (ANSI/TIA). This organization has developed many standards that are adopted at the state and local government levels as well as by individual organizations. In fact, many of the standards presented in Table 8-4 are referenced and adopted by universities, such as East Tennessee State University (ETSU 2014), in their communication and information systems design guidelines. Individual end users, such as a university campus or hospital, and levels of government may have additional standards/guidelines.

Table 8-4. Summary of Communication and Information Codes and Standards

Code/Standard	Description
ANSI/TIA-222-G Structural Standards for Antennae Supporting Structures and Antennas	Specifies the loading and strength requirements for antennas and their supporting structures (e.g., towers). The 2006 edition of the standard has significant changes from its previous editions including: changing from ASD to LRFD; change of wind loading to better match ASCE-7 (i.e., switch from use of fastest-mile to 3-second gust wind speeds); updating of ice provisions; and addition of seismic provisions (Erichsen 2014)
ANSI/TIA-568-C.0 Generic Telecommunications Cabling for Customer Premises	Used for planning and installation of a structured cabling system for all types of customer premises. This standard provides requirements in addition to those for specific types of premises (Anexter Inc. 2013)
ANSI/TIA-568-C.1 Commercial Building Telecommunications Cabling Standard	Used for planning and installation of a structured cabling system of commercial buildings (Anexter Inc. 2013)
ANSI/TIA-569-C Commercial Building Standard for Telecommunication Pathways and Spaces	Standard recognizes that buildings have a long life cycle and must be designed to support the changing telecommunications systems and media. Standardized pathways, space design and construction practices to support telecommunications media and equipment inside buildings (Anexter Inc. 2013)
ANSI/TIA-570-B Residential Telecommunications Cabling Standard	Standard specifies cabling infrastructure for distribution of telecommunications services in single or multi-tenant dwellings. Cabling for audio, security, and home are included in this standard (Hubbell Premise Wiring, Inc. 2014)
ANSI/TIA-606-B Administration Standard for Commercial Telecommunications Infrastructure	Provides guidelines for proper labeling and administration of telecommunications infrastructure (Anexter Inc. 2013).
ANSI/TIA-942-A Telecommunications Infrastructure Standard for Data Centers	Provides requirements specific to data centers. Data centers may be an entire building or a portion of a building (Hubbell Premise Wiring, Inc. 2014)
ANSI/TIA-1005 Telecommunications Infrastructure for Industrial Premises	Provides the minimum requirements and guidance for cabling infrastructure inside of and between industrial buildings (Anexter Inc. 2013)
ANSI/TIA-1019 Standard for Installation, Alteration & Maintenance of Antenna Supporting Structures and Antennas	Provides requirements for loading of structures under construction related to antenna supporting structures and the antennas themselves (Anexter Inc. 2013)
ANSI/TIA-1179 Healthcare Facility Telecommunications Infrastructure Standard	Provides minimum requirements and guidance for planning and installation of a structured cabling system for healthcare facilities and buildings. This standard also provides performance and technical criteria for different cabling system configurations (Anexter Inc. 2013)
ASCE 7-10 Minimum Design Loads for Buildings and Other Structures	Provides minimum loading criteria for buildings housing critical communications equipment. Also provides loading criteria for towers.
IEEE National Electrical Safety Code (NESC)	United States Standard providing requirements for safe installation, operation and maintenance of electrical power, standby power and telecommunication systems (both overhead and underground wiring).

8.5.1. New Construction

The standards listed in Table 8-4 are used in new construction for various parts of the communications infrastructure system. As discussed in Section 8.2.1.1, new Central Offices are designed using ASCE 7-10 Occupancy Category III buildings. Consequently, the design of equipment and standby power for Central Offices must be consistent with that of the building design. As discussed in Chapter 5 (Buildings), buildings (e.g., Central Offices) must be designed in accordance with ASCE loading criteria for the applicable hazards of the community, which may include flooding, snow/ice, earthquakes, and wind. Wind loading criteria used by ASCE 7-10 has been developed using hurricane and extratropical winds. Other natural loads that can cause significant damage such as wildfire, tsunami, and tornadoes are not explicitly considered in ASCE 7-10. However, as discussed in Chapter 5, fire protection standards are available and are used to mitigate potential building fire damage.

The ANSI/TIA-222-G standard is used for the design of new cell towers. This version of the standards, released in 2006, included the biggest set of changes since the standard's inception (TIA 2014). Some major changes include:

1. Using limits states design rather than allowable stress design
2. Changing the design wind speeds from fastest-mile to 3-second gust, as is done for ASCE 7, and using the wind maps from ASCE 7
3. Earthquake loading is addressed for the first time in the ANSI/TIA-222 standard (Wahba 2003)

Note that wind, ice, and storm surge are the predominant concerns for towers. However, earthquake loading was added so it would be considered in highly seismic regions (Wahba 2003).

Communication system distribution lines are subject to the design criteria in the National Electric Safety Code (NESC). As discussed in Chapter 7, Rule 250 contains the environmental hazard loading on the communication and electric power lines as well as their supporting structures (e.g., utility poles). Specifically, these criteria address combined ice and wind loading, which are provided in Rule 250B for three districts of the United States defined as: 1) Heavy; 2) Medium; and 3) Light. Rule 250C addresses "extreme" wind loading and Rule 250D provides design criteria for "extreme" ice with concurrent wind.

Use of the term "extreme" by NESC does not correspond to that used in this document. Rather, use of "extreme" by the current version of NESC-2012 indicates the use of the ASCE 7-05 maps for the 50 year return period, which, if used with the appropriate ASCE 7-05 load and resistance factors, corresponds to an expected event as defined in Chapter 3 of this document. However, the NESC "extreme" loads only apply to structures (in this case distribution lines) at least 60 feet above ground. Since most communication distribution lines in the last mile are below this height (i.e., 60 feet), the lines would be designed for Rule 250B, which has lower loading requirements than Rules 250C and D.

For communication distribution wires, the designer could use either the NESC or ASCE 7. Malmedal and Sen (2003) showed ASCE 7 loading of codes in the past have been more conservative than those of NESC, particularly for ice loading. Using ASCE 7 will provide a more conservative design, but a higher cost that is not desirable to utilities/service providers. When considering resilience, a more conservative design should be considered, particularly for communication distribution lines in the last-mile to critical facilities.

In the communications industry, codes and standards provide the baseline loading and design for infrastructure. However, the industry heavily relies on the development and implementation of best practices, rather than regulations, to improve their infrastructure resilience. The FCC's CSRIC provides an excellent example of a body that develops and publishes best practices for various network types (Internet/data, wireless and landline telephone) and industry roles, including service providers, network operators, equipment suppliers, property managers, and government (CSRIC 2014). Service providers often adapt these and/or develop their own best practices to help improve the infrastructure of which their business relies. The best practices developed by the CSRIC cover a wide array of topics ranging from training and awareness to cyber security and network operations. For the purposes of this document, only a handful of the best practices developed by the CSRIC (see Table 8-5) that relate to physical communications infrastructure are listed.

As shown in Table 8-5, the best practices list many suggestions discussed in this chapter, including:

- Adequate standby power for critical equipment and cell towers
- Backup strategies for cooling critical equipment in Central Offices
- Limiting exposure of distribution lines and critical equipment to hazards (important for standby equipment too)
- Minimizing single points of failure in Central Offices, and distribution network

The best practices (CSRIC 2014) have an emphasis on ensuring adequate power supply because the communications system is dependent on power systems to function. Innovative technologies and strategies for maintaining external power infrastructure continue to be developed and are discussed in Chapter 7.

Table 8-5. Best Practices for Communications Infrastructure

Best Practice Description (CSRIC 2014)	**Applicable Infrastructure**
Network Operators, Service Providers, Equipment Suppliers, and Property Managers should ensure the inclusion of fire stair returns in their physical security designs. Further, they should ensure there are no fire tower or stair re-entries into areas of critical infrastructure, where permitted by code.	Central Offices, nodes, critical equipment
Network Operators and Service Providers should prepare for HVAC or cabinet fan failures by ensuring conventional fans are available to cool heat-sensitive equipment, as appropriate.	Critical equipment
Network Operators and Service Providers should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-destructive systems.	Central Offices, nodes, critical equipment
Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, expected load, and reliability of primary power.	Cell sites and DLC RTs
Network Operators and Property Managers should consider alternative measures for cooling network equipment facilities (e.g., powering HVAC on generator, deploying mobile HVAC units) in the event of a power outage.	Central Offices, nodes, critical equipment
Network Operators, Service Providers, and Property Managers together with the Power Company and other tenants in the location, should verify that aerial power lines are not in conflict with hazards that could produce a loss of service during high winds or icy conditions.	Distribution lines
Back-up Power: Network Operators, Service Providers, Equipment Suppliers, and Property Managers should ensure all critical infrastructure facilities, including security equipment, devices, and appliances protecting it are supported by backup power systems (e.g., batteries, generators, fuel cells).	Central Offices, nodes, critical equipment
Network Operators, Service Providers, and Property Managers should consider placing all power and network equipment in a location to increase reliability in case of disaster (e.g., floods, broken water mains, fuel spillage). In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels.	Central Offices, nodes, Cell sites, DLC RTs, critical equipment
Network Operators, Service Providers, Equipment Suppliers, Property Managers, and Public Safety should design standby systems (e.g., power) to withstand harsh environmental conditions.	Critical equipment
Network Operators, Service Providers, Public Safety, and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).	Distribution lines
Service Providers, Network Operators, Public Safety, and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). Emergency/Backup power generators should be located onsite, when appropriate.	Critical equipment
Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).	Distribution
Back-Up Power Fuel Supply: Network Operators, Service Providers, and Property Managers should consider use of fixed alternate fuel generators (e.g., natural gas) connected to public utility supplies to reduce the strain on refueling.	Central Offices/nodes, cell sites, DLC RTs, critical equipment.
Network Operators and Public Safety should identify primary and alternate transportation (e.g., air, rail, highway, boat) for emergency mobile units and other equipment and personnel.	Cell sites, DLC RTs, critical equipment

8.5.1.1. Implied or Stated Performance Levels for Expected Hazard Levels

As discussed in Chapter 5, the performance level for an expected hazard event depends on the type of hazard and the design philosophy used for the hazard.

For wind, buildings and other structures are designed for serviceability. That is, in the expected wind event, such as a hurricane, the expectation is neither the building's structure nor envelope will fail. The ability of the building envelope to perform well (i.e., stay intact) is imperative for high wind events, because they are typically associated with heavy rainfall events (e.g., thunderstorms, hurricanes, tornadoes). Therefore, even if the building frame were to perform well, but the envelope failed, rain infiltration could damage the contents, critical equipment, and induce enough water related damage such that the building would have to be replaced anyway. The expectation is that a Central Office would not have any significant damage for the expected wind event, and would be fully operational within 24 hours. The 24 hours of downtime should only be required for a high wind event to allow for time to bring standby generators online if needed and ensure all switches and critical electrical equipment are not damaged.

Similarly, for an expected flood, a Central Office should not fail. There is likely to be some damage to the building and its contents at lower elevations, particularly the basement. However, if the critical electrical and switchgear equipment and standby power are located well above the inundation levels, the Central Office would be expected to be fully operational within 24 hours of the event.

For earthquakes, buildings are designed for life safety. Therefore, for Central Offices in highly seismic regions, some damage to the building is likely for the expected earthquake. As a result, it is likely that there will be some loss of functionality of a Central Office following the expected earthquake event. If the critical equipment and switchgear were designed and mounted, downtime would be expected to be limited (less than one week). However, if the critical equipment and switchgear were not mounted to resist ground accelerations, it could be weeks before the Central Office is fully functional again.

For cell towers, the primary hazard that is considered for design in ANSI/TIA-222 is wind. However, ice and earthquake are also considered. ANSI/TIA-222 provides three classes of tower structures (Wahba 2003):

- ***Category I Structures:*** Used for structures where a delay in recovering services would be acceptable. Ice and earthquake are not considered for these structures, and wind speeds for a 25-year return period using the ASCE 7-02/7-05 methodology are used.
- ***Category II Structures:*** This is the standard category that represents hazard to human life and property if failure occurs. The nominal 50-year return period wind, ice, and seismic loads are used.
- ***Category III Structures:*** Used for critical and emergency services. The nominal 100-year return period loads.

For the expected event, failures would only be anticipated for a small percentage of cell towers (e.g., less than five percent). It is noted that, as discussed in the previous section, the loading in ANSI/TIA-222-G is based on that of ASCE 7.

Communication distribution wires will likely experience some failures in the expected event, particularly for wind and ice storms. As discussed in the previous section, most distribution lines in the last-mile are below 60 feet above the ground and, hence, are not even designed to meet what Chapter 3 defines as the expected event if Rule 250B in NESC is followed for design. For lines that are designed to meet the NESC Rules 250C and 250D, it would be anticipated that only a small percentage of failure of the overhead wire would fail in an expected ice or wind event. However, as discussed earlier in this chapter and in Chapter 7, tree fall onto distribution lines causes many failures rather than the loading of the natural hazard itself. Therefore, service providers should work with the electric power utility to ensure their tree-trimming programs are adequately maintained.

8.5.1.2. Recovery Levels

As discussed in the previous section, Central Offices and cell towers should not have an extended recovery time for the expected event. Given that the earthquake design philosophy is life safety (rather than wind which is designed for serviceability), Central Offices may have some loss of functionality due to damage to the building envelope and critical equipment if it is not designed and mounted to resist adequate ground accelerations.

With respect to cell sites, wind, storm surge, and fire are the predominant hazards of concern for designers. Ice and earthquake are also considered, though not to the same extent in design. Given that the ANSI/TIA-222-G loads are based on ASCE 7 loading, it is anticipated that only a small percentage of cell tower structures would fail during an expected event. Cell towers are configured such that there is an overlap in service between towers so the signal can be handed off as the user moves from one area to another without a disruption in service. Therefore, if one tower fails, other towers will pick up most of the service since their service areas overlap.

For distribution lines, a key factor, more so than the standards, is location of the cables. For example, if the distribution lines are underground for a high wind or ice event, failures and recovery time should be limited. However, even if the distribution lines are underground it is possible for failure to occur due to uprooting of trees. For flooding, if the distribution lines are not properly protected or there has been degradation of the cable material, failures could occur. For earthquake, failures of underground distribution lines could also occur due to liquefaction. As discussed in Section 8.2.1, although underground lines may be less susceptible to damage, they are more difficult to access to repair and failures could result in recovery times of weeks rather than days. However, for an expected event, some damage to the distribution lines would be expected.

If the distribution lines are overhead, high wind and ice events will result in failures, largely due to tree fall or other debris impacts on the lines. The debris impacts on distribution lines is a factor that varies locally due to the surroundings and tree trimming programs that are intended to limit these disruptions. Although these lines are more likely to fail due to their direct exposure to high winds and ice, recovery/repair time of the lines for an expected event would be expected to range from a few days to a few weeks depending on the size of the area impacted, resources available, and accessibility to the distribution lines via transportation routes. Note that this only accounts for repair of the communications distribution lines itself. Another major consideration is the recovery of external power lines so the end user is able to use their communications devices. Chapter 7 addresses the standards and codes, and their implied performance levels for an expected event.

8.5.2. Existing Construction

Although the standards listed in Section 8.2 are used for new construction for communications infrastructure, older versions of these codes and standards were used in the design of structures for the existing infrastructure.

Central Offices designed and constructed within the past 20 years may have been designed to the criteria ASCE 7-88 through 05. Prior to that, ANSI standards were used. There have been many changes in the design loading criteria and methodology over the design life of existing Central Offices. For example, ASCE 7-95 was the first time a 3-second gust was used for the reference wind speed rather than the fastest mile for the wind loading criteria (Mehta 2010). Over the years, reference wind speeds (from the wind speed contour maps) have changed, pressure coefficients have been adjusted, earthquake design spectra, ground accelerations, and other requirements have changed. Overall, codes and standards have been added to/changed based on lessons learned from past disaster events and resulting research findings.

As discussed in Section 8.5.1, ANSI/TIA-222-G is the current version of the standard used for cell towers and antennas. However, prior to 2006, versions of the code include (TIA 2014):

- ANSI/TIA/EIA-222-F established in 1996
- ANSI/TIA/EIA-222-E established in 1991
- ANSI/TIA/EIA-222-D established in 1987
- ANSI/TIA/EIA-222-C established in 1976
- ANSI/TIA/EIA-222-B established in 1972
- ANSI/TIA/EIA-222-A established in 1966
- ANSI/EIA-RS-222 established as the first standard for antenna supporting structures in 1959.

The 1996 standard, ANSI/TIA/EIA-222-F, was used during the largest growth and construction of towers in the United States (TIA 2014). As noted in Section 8.5.1, earthquake was not considered in this version of the standard, allowable stress design was used rather than limit states design, and reference wind speeds used fastest mile rather than 3-second gust (Wahba 2003). Note that the use of fastest mile for the reference wind speed is consistent with ASCE 7 prior to the 1995 version (of ASCE).

Historically, communication distribution lines, like the new/future lines, have been designed to NESC standards. The following lists some of the most significant changes to NESC rule 250 that have occurred over the past couple of decades (IEEE 2015):

- Prior to 1997, NESC did not have what is now referred to as an “extreme” wind loading. Rule 250C adapted the ASCE 7 wind maps after the wind speed changed from fastest mile to 3-second gust as is used today.
- In 2002, Rule 250A4 was introduced to state that since electric and telecommunication wires and their supporting structures are flexible, earthquakes are not expected to govern design.
- In 2007, Rule 250D was introduced for design of “extreme” ice from freezing rain combined with wind.

These changes and their timeframe indicate older distribution lines, if not updated to the most recent code, may be more vulnerable to failures from wind and ice events than the current code. However, the NESC adopting these new standards should help lead to improvements of overhead distribution line performance in the future.

8.5.2.1. Implied or Stated Performance Levels for Expected Hazard Levels

Existing Central Offices designed to an older version of ASCE 7 or ANSI criteria should have similar performance to those of new construction for an expected event. However, it is possible that these structures may have varied performance depending on the design code’s loading criteria. Nonetheless, an existing Central Office should have similar performance to that of a newly constructed Central Office (see Section 8.5.1.1).

As discussed in the previous section, the ANSI/TIA/EIA-222-F 1996 standard was in effect when the largest growth and construction of cell towers took place (TIA 2014). For wind and ice, the towers would be expected to only have a small percentage of failures for the expected event as discussed in Section 8.5.1.1. However, earthquake loading was not included in any of the standards prior to ANSI/TIA-222-G (Wahba 2003). Although earthquakes do not typically govern the design of cell towers, highly seismic regions would be susceptible to failures if an expected earthquake occurred. For existing towers designed to standards other than ANSI/TIA-222-G in highly seismic regions, the design should be checked to see if earthquake loads govern and retrofits should be implemented if necessary. Existing towers that have electronics added to them are updated to meet requirements of the most up to date code (ANSI/TIA-222-G). Note that despite no earthquake loading criteria in ANSI/TIA/EIA-222-F, and older versions of this standard, designers in highly seismic regions may have considered earthquake loading using other standards, such as ASCE 7. However, this was not a requirement.

As discussed in Section 8.5.1.2, some communication distribution lines are anticipated to fail during an expected event. Given that "extreme" ice loading was not included in the NESC standard until 2007, distribution lines adhering to prior codes may be particularly vulnerable to ice storms.

8.5.2.2. Recovery Levels

As discussed in the previous section and Section 8.5.1.2, Central Offices and cell towers should not require a long time for full recovery after an expected event. However, given that older standards of ANSI/TIA/EIA-222 did not include earthquake loading criteria, a large number of failures and, hence, significant recovery time may be needed to repair or replace towers after an expected event in a highly seismic region. To replace a large number of towers would take weeks, months, or even years depending on the size of the impacted area. As discussed in Section 8.6.3, service providers have the ability to provide cell on light trucks (COLTs) so essential wireless communications can be brought online quickly after a hazard event in which the network experiences significant disruptions (AT&T 2014). However, the COLTs are only intended for emergency situations. They are not intended to provide a permanent solution. The best approach for cell tower owners in these earthquake prone regions is, therefore, to ensure the cell towers can resist the earthquake loading criteria in the new ANSI/TIA standard.

With respect to performance of distribution lines, performance and recovery time is largely dependent on the placement of the cables (i.e., overhead versus underground) as discussed in Section 8.5.1.2.

8.6. Strategies for Implementing Community Resilience Plans

Section 8.2 discusses critical components of communication and information infrastructure. The discussion includes examples from different types of hazards to encourage the reader to think about the different hazards that could impact the communication and information infrastructure in their community. The number, types, and magnitudes of hazards that need to be considered will vary from community to community.

Section 8.3 discusses the performance goals of the communication and information infrastructure strived for by the community. Section 8.3 does provide example performance goals for the routine, expected, and extreme event. However, the performance goals should be adjusted by the community based on its social needs, which will vary by community.

Sections 8.4 and 8.5 outline some regulatory levels and issues, and codes and standards the reader should keep in mind when planning to make upgrades/changes to existing structures as well as building new structures for their communications network. The objective of this section is use the information from Sections 8.2 through 8.5 to provide guidance on how a community or service provider should work through the process of assessing their communications infrastructure, defining strategies to make its infrastructure more resilient, and narrowing the resilience gaps.

8.6.1. Available Guidance

Recall that in the Section 8.3 discussion of setting performance goals of the communication and information infrastructure, there was also an "X" in each row corresponding to an example of what a community actually found its infrastructures' performance to be given a level of hazard. The question then becomes: How does the community/service provider determine where the "X" belongs for the various types of infrastructure in our community?

At this point, the community should have convened a collection (or panel) of stakeholders and decision makers to approach the problem and establish the performance goals for each type and magnitude of hazard. To assess the infrastructure, this panel should have the knowledge, or reach out to those in the community who have the knowledge to assess the state of the infrastructure. The panel of stakeholders and decision makers will have to assess the infrastructures' performance relative to the type and magnitude of event that the community may face because different types of hazards will result in different types of failure modes and, consequently, performance. In some communities, it may only be necessary to make assessments for one hazard (such as earthquake in some non-coastal communities in California or Oregon). In other communities, it may be appropriate to complete assessments of the performance for multiple types of hazards such as high winds and storm surge in coastal communities in the Gulf and east coast regions of the United States.

There are three levels at which the infrastructure can be assessed:

Tier 1. A high level assessment of the anticipated performance of the components of the communications infrastructure can be completed by those with knowledge and experience of how the components and system will behave in a hazard event. For Central Offices, this may include civil and electrical engineer/designers. For wires (both overhead and underground), and cell towers, this may include engineers, utility operators, service providers, technical staff, etc. As a minimum, each community should complete a high level (Tier 1) assessment of its infrastructure. The community can then decide whether additional investment is warranted in completing a more detailed assessment. The SPUR Framework (Poland 2009) took this high level approach in assessing their infrastructure for the City of San Francisco, and is highly regarded as a good example for the work completed to date.

Tier 2. A more detailed assessment can be used, based on an inventory of typical features within the communication infrastructure system, to develop generalized features for various components of the infrastructure. To do this, the community would have to use or develop a model for their community to assess the performance of common components of their infrastructure system for a specific type and magnitude of event (i.e., model a scenario event and its resulting impacts). Alternatively, the community could model a hazard event scenario to compute the loads (wind speeds/pressures, ground accelerations, flood elevations) to be experienced in the community and use expert judgment to understand what the performance of various components of the communications infrastructure would be as a result of the loading.

A Tier 2 communication and information infrastructure assessment would include the impact on typical components of the infrastructure system independent of the intra-dependencies. The Oregon Resilience Plan (OSSPAC 2013) provides a good example of modeling a hazard event to assess the resulting impacts of the current infrastructure. It used HAZUS-MH to model and determine the impacts of a Cascadia earthquake on the different types of infrastructure and used the losses output by the HAZUS tool to back-calculate the current state of the infrastructure.

Tier 3. For the most detailed level of analysis, a Tier 3 assessment would include all components in the communications infrastructure system, intra-dependencies within the system, and interdependencies with the other infrastructure systems. Fragilities could be developed for each component of the communications infrastructure system. A Tier 3 assessment would use models/tools to determine both the loading of infrastructure due to the hazard and the resulting performance, including intra- and interdependencies. Currently, there are no publicly available tools that can be used to model the intra- and interdependencies.

8.6.2. Strategies for New/Future Construction

For new and future construction, designers are encouraged to consider the performance goals and how to best achieve those goals rather than designing to minimum code levels, which are sometimes just for life safety (e.g., earthquake design). It is important to consider the communication and information infrastructure as a whole because it is a network and failure in one part of the system impacts the rest of the system (or at least the system connected directly to it). Therefore, if it is known that a critical component of the infrastructure system is going to be non-redundant (e.g., a lone Central Office, or a single point of entry for telephone wires into a critical facility), the component should be designed to achieve performance goals set for the extreme hazard.

Throughout this chapter, there are examples of success stories and failures of communications infrastructure due to different types of hazards (wind, flood, earthquake, ice storms). Designers, planners, and decisions makers should think about these examples, as well as other relevant examples, when planning for and constructing new communications and information infrastructure. There are several construction and non-construction strategies that can be used to successfully improve the resilience of communications infrastructure within a community.

Construction Strategies for New/Future Central Offices. With respect to Central Offices that are owned by service providers, the service provider should require the building to be designed such that it can withstand the appropriate type and magnitude of hazard events that may occur for the community. It is imperative that all hazards the community may face are addressed because hazards result in different failure modes. Designing for an extreme earthquake may not protect infrastructure from the expected flood, or vice versa. However, as was discussed during the workshops held to inform this framework, not all Central Offices or other nodes housing critical communications equipment are owned by service providers.

Sections of buildings are often leased by service providers to store their equipment for exchanges or nodes in the system. In this case, service providers typically have no influence over the design of the building. But, if a building is in the design phase and the service provider is committed to using the space of the building owner, the service provider could potentially work with the building owner and designers to ensure their section of the building is designed such that their critical equipment is able to withstand the appropriate loading. In a sense, the goal would be to "harden" the section of the building in the design phase rather than retrofitting the section of the structure after a disaster, as is often done. Adding the additional protection into the design of the building would likely cost more initially, and the building owner would likely want the service provider to help address the additional cost. However, the service provider would be able to compute a cost-to-benefit ratio of investment for paying for additional protection of their critical equipment versus losing their equipment and having to replace it.

Non-Construction Strategies for New/Future Central Offices. Although the design and construction of buildings that house critical equipment for Central Offices, exchanges, and other nodes in the communications network is an important consideration, non-construction strategies can also be extremely effective. For example, service providers who own buildings for their Central Offices should place their critical equipment such that it is not vulnerable to the hazards faced by the community. For example, Central Offices vulnerable to flooding should not have critical electrical equipment or standby generators in the basement. Rather, the critical electrical equipment and standby generators should be located well above the extreme flood levels. As shown by the success story of the Verizon Central Office after Hurricane Sandy described in Section 8.2.1, placing the critical equipment and standby generators above the extreme flood level can significantly reduce the recovery time needed. Similarly, for Central Offices in earthquake prone areas, service providers can mount their critical equipment to ensure it does not fail due to the shaking of earthquakes.

Service providers planning to lease space from another building owner should be aware of the hazards faced by the community and use that information in the decision making process. For instance, a service provider would not want to rent space in the basement of a 20-story building to store electrical and critical equipment for an exchange/node.

Construction Strategies for New/Future Cell Towers. New/Future Cell Towers should be designed to the latest TIA/EIT-222-G standard. As discussed in Section 8.2.3, the 2006 version of the TIA/EIT-222-G standard was updated to reflect the design criteria in ASCE 7 for wind, ice, and earthquake loading. For wind and ice, if the towers are designed and constructed in accordance with the appropriate standards, only a small percentage of cell towers would be anticipated to fail in an "expected" event. With respect to earthquake, where the design philosophy is life safety, towers should be designed beyond the code loading criteria. Since cell towers are becoming more numerous, they should be designed for the "expected" event.

Non-Construction Strategies for New/Future Cell Towers. Historically, the predominant cause of outages of cell towers has been the loss of electrical power. As discussed in Section 8.2.3, the FCC's attempt to mandate a minimum of eight hours of battery standby power to overcome this problem was removed by the courts. However, service providers should provide adequate standby power to maintain functionality following a hazard event.

As is the case for standby generators in Central Offices, standby generators for cell towers must be placed appropriately. Standby generators for cell towers in areas susceptible to flooding should be placed above the "expected" flood level. Similarly, in earthquake regions, standby generators should be mounted such that the ground accelerations do not cause failure on the standby generator.

Additional protection should be implemented for cell towers when appropriate and feasible. As discussed in Section 8.2.3, during Hurricane Katrina debris impacts from boats in flood areas resulted in failure of cell towers. Impacts from uprooted trees or branches during high wind events and tsunamis could also result in failure of these towers. Therefore, the topography and surroundings (e.g., relative distance from trees or harbors to cell towers) should be considered to ensure cell towers are protected from debris impact.

Strategies for New/Future Distribution Line to End User. As discussed in Section 8.2.1, there are several different types of wires (copper, coaxial, and fiber optic) that carry services to the end user. Each of the types of wires has advantages and disadvantages. More and more, service providers are installing fiber optic wires to carry services to the customer.

There is ongoing debate regarding whether underground or overhead wires are the best way to distribute services to the end user. For new/future distribution lines, several factors should be used to decide which method of distribution of services is best. The factors should include:

- Building cluster to which the services are being distributed
- Potential hazards to which the community is susceptible
- Topography and surroundings of distribution lines
- Redundancy or path diversity of distribution lines

The first three items can be considered together. The building cluster to which the services are being delivered (1st bullet) is a key consideration. As seen in Section 8.3, performance goals for transmission of communications services to critical facilities reflect a desire for less recovery time (i.e., better performance) than the clusters for emergency housing, housing/neighborhoods, and community recovery. The hazards the community faces (2nd bullet) can be used to determine how to best prevent interruption of service distribution to the building (i.e., end user). For example, in regions that are susceptible to high winds events (i.e., 2nd bullet), it may be appropriate to distribute communication services to critical services (and other clusters) using underground wires rather than overhead wires. The use of overhead wires would likely result in poorer performance in wind events because of failures due to wind loading or, more likely, debris (i.e., tree) impact (3rd bullet).

Redundancy or path diversity (4th bullet) of communications distribution lines to end users is an important consideration. As discussed in Section 8.2.1, building redundancy in the communications network is essential to ensuring continuation of services after a hazard event. For example, single points of failure in the last/first mile of distribution can be vulnerable to failure causing long term outages. Redundancy (i.e., path diversity) should be built into in the distribution network, especially the last/first mile, wherever possible.

8.6.3. Strategies for Existing Construction

Similar to new/future communication and information infrastructure, there are several construction and non-construction strategies that can be used to successfully improve the resilience of existing communications infrastructure within a community. However, unlike new/future components of the communications infrastructure system, existing components must be evaluated first to understand their vulnerabilities, if they exist. If it is determined that a component is vulnerable to natural loads, strategies should be used to improve its resilience.

Given that the communication and information infrastructure system is extremely large and much of the existing infrastructure is owned by service providers or third party owners (e.g., building owners) with competing needs for funding, it is not reasonable to expect that capital is available for service providers (or third parties) to upgrade all infrastructure immediately. However, prioritization can address the most critical issues early in the process and develop a strategy to address many concerns over a longer time period. Moreover, by evaluating the inventory of existing infrastructure and identifying weaknesses, service providers can use the data to implement strategies for new/future infrastructure construction so the same weaknesses are not repeated.

Construction Strategies for Existing Central Offices. Existing buildings owned by service providers and used as Central Offices should be assessed to determine if the building itself and sections of the building containing critical equipment and standby generators will be able to meet performance goals (see Section 8.3). As stated for the case of new/future construction, if the Central Office is a non-redundant node in the service provider's infrastructure network, the Central Office should be evaluated to ensure it can resist the "extreme" level of hazard. However, if the Central Office is a node in a redundant infrastructure system, and failure of the Central Office would not cause any long-term service interruptions, the Central Office should be assessed to ensure it can withstand the loads for the "expected" event.

If the service provider finds that its Central Office will not be able to withstand the loading for the appropriate level of hazard event, it should take steps to harden the building. Although this is likely to be expensive, if the Central Office is critical to the service provider's performance following a hazard event in both the short and long term, a large investment may be necessary and within a reasonable cost-benefit ratio.

For nodes, exchanges, or Central Offices located in leased (existing) buildings, the service provider does not have control over retrofitting or hardening the building. However, the service provider could attempt to work with the building owner to have the sections of the building housing critical equipment hardened. Alternatively, there are also several non-construction strategies that could be used to protect the critical equipment.

Non-Construction Strategies for Existing Central Offices. Critical equipment in Central Offices or in other nodes/exchanges in the communications infrastructure network should be assessed to determine whether it is likely to fail during hazard events faced by that community. Whether the building is owned by the service provider or leased from a third party, relatively easy and inexpensive changes can be made to protect the critical equipment.

As was demonstrated by the example of the Manhattan Verizon Central Office at 140 West Street discussed in Section 8.2.1, non-construction strategies can be used to successfully improve performance of critical equipment in hazard events. Recall that the 140 West Street Central Office was hardened after 9/11. What may have been the most successful change was elevating the standby generators and critical equipment to higher elevations such that they would not fail in the case of flooding (City of New York 2013). Compared to another Central Office located at 104 Broad Street in New York City that had critical equipment and standby generators stored in the basement, the Verizon Central Office performed much better. The 104 Broad Street had an outage of 11 days, whereas the Verizon Central Office was operational within 24 hours. The 104 Broad Street did not meet the performance goals for the expected event in Section 8.3. With the singular change of elevating critical equipment and standby generators, the Verizon Central Office met the performance goals presented in Section 8.3.

Construction Strategies for Existing Cell Towers. Existing cell towers should be evaluated to determine whether they can resist the loading from the "expected" event the community faces (wind speed/pressure, earthquake ground accelerations, ice storms). Versions older than the 2006 ANSI/TIA-222-G did not include earthquake design criteria. Therefore, design loads for existing cell towers, particularly in earthquake-prone regions, should be assessed to understand the loading that the towers can withstand. It is assumed that a designer in an earthquake-prone region would use loading based on other codes and standards, but it is possible that the loading used in the original design may not be adequate. If it is found after assessing the cell tower for earthquake loading that it was not designed to resist adequate loads, retrofits such as the addition of vertical bracing can be constructed to ensure the loading can be resisted. Similarly, since there have been changes in the wind and ice loading in ANSI/TIA-222-G to better match the loading criteria in ASCE, cell towers should be assessed to ensure they will resist the appropriate loads, and retrofitted if needed.

Non-Construction Strategies for Existing Cell Towers. Existing cell tower sites should be assessed to determine whether adequate standby power supply is available given the criticality of the site and whether the standby generator and switchgear are protected against loading from the appropriate magnitude (expected) of natural hazard. Although it may not be economically feasible to provide standby generators for all cell towers immediately, a program can be developed to accomplish this over time. The immediate surroundings of cell sites should be assessed to determine vulnerabilities to airborne and waterborne debris. If the cell site is located such that it is vulnerable to tree fall or other debris in a high wind or flood event, additional protection should be provided to protect the cell tower.

Strategies for Existing Distribution Line to End User. For existing distribution lines to the end user, an inventory of wires, including the type, age, and condition should be recorded. When wires are damaged or have deteriorated due to age, they should be retired and/or replaced.

As discussed for new/future distribution lines, overhead versus underground wires is an ongoing debate in the industry. Distribution lines, particularly to critical buildings, should be assessed to determine whether overhead or underground wires are best for the communications infrastructure system. If a service provider is considering switching from overhead wires to underground wires to avoid possible outages due to ice storms or high wind events, a cost-benefit ratio should be computed as part of the assessment and decision making process. If cost is much greater than projected benefits, the service provider may want to consider other priorities in making their infrastructure more resilient. In fact, rather than switching the distribution lines from overhead to underground wires, the service provider may find it more economical to add redundancy (i.e., path diversity) to that part of the infrastructure network. Thus, the service provider would not be reducing the risk to the existing overhead distribution wires, but reducing the risk of service interruptions because it is not solely reliant on overhead distribution lines.

Non-Construction Strategies for Critical Facilities/Users. As previously discussed, communications network congestion is often seen during and immediately after a hazard event. The following programs have been implemented to help critical users have priority when networks are congested due to a disaster event (DHS 2015):

- Government Emergency Telecommunications Service (GETS)
- Wireless Priority Service (WPS)
- Telecommunications Service Priority (TSP)

GETS works through a series of enhancements to the landline network. It is intended to be used in the immediate aftermath of disaster events to support national security and emergency preparedness/response. Cell phones can also use the GETS network but they will not receive priority treatment until the call reaches a landline. Rather, the WPS is used to prioritize cell phone calls of users who support national security and emergency preparedness/recovery when the wireless network is congested or partially damaged. WPS is supported by seven service providers: AT&T, C Spire, Cellcom, SouthernLINC, Sprint, T-Mobile, and Verizon Wireless (DHS 2015). The GETS and WPS programs are helpful in coordinating recovery efforts in the wake of a disaster event. However, note that the main goal of these programs is to provide priority service when there is congestion due to limited damage. If a significant amount of the infrastructure fails, these services may not be available.

TSP is an FCC program that enables service providers to give service priority to users enrolled in the program when they need additional lines or need service to be restored after a disruption (FCC 2015). Unlike the GETS and WPS programs, the TSP program is available at all times, not just after disaster events. For all of these programs, eligible entities include police departments, fire departments, 9-1-1 call centers, emergency responders, and essential healthcare providers (e.g., hospitals).

Short-Term Solutions for Restoring Service. Service providers and other stakeholders (e.g., third party building owners) responsible for infrastructure cannot make all infrastructure changes in the short term due to limited resources, a competitive environment driven by costs, and competing needs. Therefore, as part of their resilience assessment, service providers should prioritize their resilience needs. Service providers should budget for necessary short-term changes (0-5 years), which may include relatively inexpensive strategies such as placement and security of critical equipment and standby generators. For the long term (5+ years), service providers should address more expensive resilience gaps that include hardening of existing Central Offices and replacing overhead distribution lines with underground lines.

Although not all resilience gaps can be addressed in the short term through investment in infrastructure, service providers should use other strategies to address these gaps. Ensuring there is a recovery plan in place so service to customers is not lost for an extended period of time helps minimize downtime. AT&T's Network Disaster Recovery (NDR) team provides an excellent example of using temporary deployments to minimize service disruption. The AT&T NDR was established in 1992 to restore the functionality of a Central Office or AT&T network element that was destroyed or in which functionality was lost in a natural disaster (AT&T 2005).

The NDR team was deployed after several disaster events to minimize service disruption where the downtime would have been long term, including after 9/11, the Colorado and California wildfires in 2012 and 2013, the 2013 Moore, OK tornado, 2011 Joplin, MO tornado, 2011 Alabama tornadoes, Hurricane Ike in 2008, and 2007 ice storms in Oklahoma (AT&T 2014). The AT&T NDR team completes quarterly exercises in various regions of the United States and around the world to ensure personnel are adequately trained and prepared for the next hazard event (AT&T 2014). Training and field exercises for emergency recovery crews are essential to helping reduce communications network disruptions and, hence, the resilience gaps.

After the May 22, 2011 Joplin tornado, the NDR team deployed a Cell on Light Truck (COLT) on May 23, 2011 to provide cellular service near the St. John's Regional Medical Center within one day of the tornado (AT&T 2014). The cell site serving the area was damaged by the tornado. Satellite COLTs can be used to provide cellular communications in areas that have lost coverage due to damage to the communication infrastructure system (AT&T 2014).

Using satellite telephones can be an alternative for critical facilities or emergency responders in the immediate aftermath of a hazard event. Satellite phones are almost the only type of electronic communications system that will work when cell towers are damaged and Central Offices or exchanges/nodes have failed (Stephan 2007). Unfortunately, satellite phones are used infrequently, especially with the continuing growth of cellular phones. In 1999, the State of Louisiana used Federal funds to provide the state's parishes with a satellite phone to use in the event of an emergency, but the state stopped providing the funding to cover a monthly $65 access fee one year before Hurricane Katrina occurred (Stephan 2009). As a result, only a handful of churches kept the satellite phones. However, even for those parishes that did keep their satellite phones, they did little to alleviate the communications problem because nobody else had them when Hurricane Katrina occurred. In general, people do not own satellite telephones so this is not the best solution for an entire community. However, for critical facilities and communications between emergency responders, satellite telephones may be a viable option to ensure the ability to communicate is preserved.

8.7. References

Anixter Inc., (2013). *Standards Reference Guide.* Glenview, Illinois.

American Lifelines Alliance (2006). *Power Systems, Water, Transportation and Communications Lifeline Interdependencies – Draft Report.* Washington, DC.

American Society of Civil Engineers (ASCE 2010). *ASCE 7-10, Minimum Design Loads for Buildings and Other Structures, Second Edition.* New York, New York.

AT&T (2014). Viewed August 28, 2014. < http://www.corp.att.com/ndr/deployment1.html>.

AT&T (2005). *Best Practices: AT&T Network Continuity Overview.*

The City of New York (2013). *A Stronger, More Resilient New York.* New York City, NY.

City of Urbana Public Works Department (2001). *Overhead to Underground Utility Conversion.* Urbanaa, Illinois.

Centre for the Protection of National Infrastructure (CPNI 2006). *Telecommunications Resilience Good Practice Guide Version 4.* United Kingdom, March 2006.

Communications Security, Reliability, and Interoperability Council (CSRIC 2014). <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm>. *CSRIC Best Practices. Viewed* December 16, 2014.

Department of the Army (2007). *Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities.* January 19, 2007.

Department of Homeland Security (DHS 2015). *GETS/WPS Documents.* < http://www.dhs.gov/publication/getswps-documents#> . Viewed January 13, 2015.

East Tennessee State University Office of Information Technology (ETSU 2014). *Telecommunications Design and Installation Standards Policy.*

Erichsen, John R. *Slideshow Presentation: ANSI/TIA-222-G Explained.* Viewed July 5, 2014.

Federal Communications Commission (FCC 2015). <*Telecommunications Service Provider. http://www.fcc.gov/encyclopedia/telecommunications-service-priority*> . Viewed January 13, 2015.

Fiber-to-the-Home Council (FTTH Council 2013). *Comments of the Fiber-to-the Home Council on Request to Refresh Record and Amend the Commission's Copper Retirement Rules.* Washington, DC.

Hubbell Premise Wiring Inc. *Structured Cabling Standards and Practices.* Viewed July 5, 2014.

Institute of Electrical and Electronics Engineers (IEEE 2015). *History of the National Electrical Safety Code ANSI C2.* < http://standards.ieee.org/about/nesc/100/> . Viewed January 26, 2015.

Jrad, Ahman et al. (2005). *Wireless and Wireline Network Interactions in Disaster Scenarios.* Military Communications Conference. Washington, DC.

Jrad, Ahman et al. (2006). *Dynamic Changes in Subscriber Behavior and their Impact on the Telecom Network in Cases of Emergency*. Military Communications Conference. Washington, DC.

Kende, Michael, and Hurpy, Charles (2012). *Assessment of the Impact of Internet Exchange Points – Empirical Study of Kenya and Nigeria.* Analysys Mason Limited. Washington, DC.

Kentucky Public Service Commission (2009). *The Kentucky Public Service Commission Report on the September 2008 Wind Storm and the January 2009 Ice Storm.*

Kwasinski, Alexis (2009). *Telecom Power Planning for Natural Disasters: Technology Implications and Alternatives to U.S. Federal Communications Commission's "Katrina Order" in View of the Effects of 2008 Atlantic Hurricane Season.* 31st International Telecommunications Energy Conference (INTELEC).

Kwasinski, Alexis (2011). *Effect of Notable Natural Disasters from 2005 to 2011 on Telecommunications Infrastructure: Lessons from on-site Damage Assessments.* 2011 IEEE International Telecommunications Energy Conference (INTELEC).

Kwasinski, Alexis; Weaver, Wayne; Krein, Philip; and Chapman, Patrick (2006). *Hurricane Katrina: Damage Assessment of Power Infrastructure for Distribution, Telecommunication, and Backup*. University of Illinois at Urbana-Champaign. Urbana-Champaign, IL.

Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations (2002). *Building a 21st Century Telecom Infrastructure.* Ney York City, NY.

Mehta, Kishor (2010). *Wind Load History ANSI A58.1-1972 to ASCE 7-05.* Structures Congress, American Society of Civil Engineers.

Oregon Seismic Safety Policy Advisory Commission (OSSPAC 2013). *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami.* Salem, Oregon.

The Lifelines Council of the City and County of San Francisco (2014). *Lifelines Interdependency Study Report I.* San Francisco, California.

Federal Communications Commission (FCC 2011). <www.fcc.gov/telecom.html>. Viewed on July 5, 2014. *Telecommunications Act of 1996.*

Federal Emergency Management Agency (FEMA 2002). *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations.* New York, New York.

Federal Emergency Management Agency (FEMA 2013). *Mitigation Assessment Team Report: Hurricane Sandy in New Jersey and New York.* Washington, DC.

Malmedal, Keith; Sen, P.K. (2003). *Structural Loading Calculations of Wood Transmission Structures.* IEEE Rural Electric Power Conference.

Stephan, Karl D (2007). *We've got to Talk: Emergency Communications and Engineering Ethics.* IEEE Technology and Society Magazine.

Telecommunications Industry Association (TIA 2014). *TR-14 Structural Standards for Communication and Small Wind Turbine Support Structures.* Viewed September 22, 2014. <http://www.tiaonline.org/all-standards/committees/tr-14>.

Wahba, John et al. (2003). *New Standards for Broadcast Structures ANSI/EIA/TIA-222-G.*

West Virginia Broadband (2013). Viewed July 5, 2014. <http://www.westvirginia.com/broadband/mediaroom/BroadbandGlossary.pdf>.

The White House. *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience.* February 5, 2013. Office of the Press Secretary. Washington, DC.

Victory, Nancy et al. (2006). *Report and Recommendations of the Interdependent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks.* Washington, DC.