Alcatel·Lucent

STRATEGIC WHITE PAPER

Reliable Power for Communications Networks

Understanding and Managing Battery Plant Vulnerabilities

Reliable power is essential for the continuous and successful operation of today's complex communications infrastructures. The equation is simple — no power, no network. Preventing power loss has become more difficult due to the proliferation of communications equipment in remote locations. This white paper summarizes the Eight Ingredient Framework developed at Bell Labs, which is widely used by industry, government and academia to analyze aspects of the communications infrastructure. It then goes on to provide a deeper analysis of the intrinsic vulnerabilities of a fundamental unit of the power system — the battery plant — and how to cope with these challenges.

Bell Labs INNOVATION

Table of contents

Introduction

"Knowledge is power." Today's communications industry requires a slight update to this old saying that's equally true — "Knowledge of power is power." Although today's communications industry equipment bears little resemblance to the telephone equipment of the past, it does share at least one key characteristic — loss of power means loss of communications.

In today's world, reliable power systems are not an option — they are absolutely essential. Failure of critical communications equipment and services due to power failure can have a devastating impact on a country's infrastructure, economy, public safety, national security, and overall stability. Because complex communications equipment is commonly found in remote locations over which the network operator has less control, providing reliable power can be a major challenge.

Meeting today's power challenges

This white paper provides a brief discussion of the eight ingredients of a communications system and the components of a power system, a review of two approaches (threats vs. vulnerabilities) for determining how to defend a system, and a high-level example of intrinsic vulnerability analysis.[1] This discussion is followed by a deeper analysis of the intrinsic vulnerabilities of a foundational unit of the power system — the battery plant.

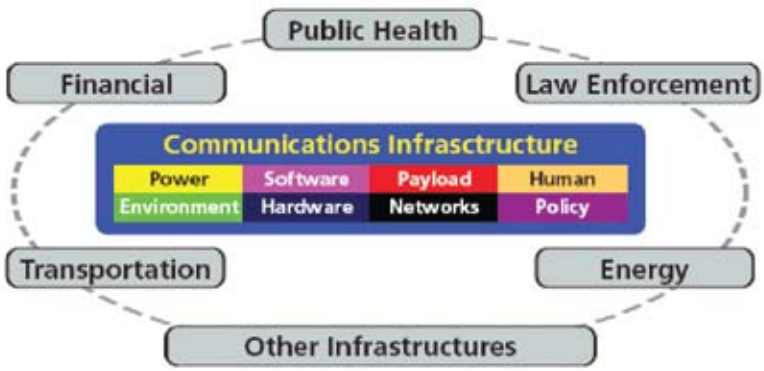
The eight ingredient framework

Modern communications systems are a complex blend of rapidly-changing technologies. Bell Laboratories, the research and development arm of Alcatel-Lucent has developed an Eight Ingredient Framework[2] that has proven to be extremely effective in understanding various critical aspects of the communications infrastructure.

Various high profile industry-government and academic forums have successfully employed this framework in their analysis of aspects of the communications infrastructure.[3] The eight ingredients are:

- Power
- Environment
- Software
- Hardware
- Payload
- Network
- Human
- Policy

Figure 1. Eight ingredient framework



While each ingredient has an impact on the communications network, power is the one on which all the others depend. Without power, the communications network ceases to operate.

Threats versus vulnerabilities

The communications industry defines a threat as "Anything with the potential to damage or compromise the communications infrastructure or some portion of it."[4] Examples of specific threats to power systems include loss of commercial power, a vandal shutting off power to a communications installation, or a technician accidentally shorting out a power supply. Practically speaking, threats are infinite in number. Therefore, while threat knowledge is valuable and certainly has a place in an overall analysis, it generally leaves the defender one step behind the attacker.

The industry has defined a vulnerability as "A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise."[5] Examples of vulnerabilities intrinsic to power systems are battery power limitations, loss of circuit connectivity, and generator dependence on fuel.

Unlike threats, the number of vulnerabilities is finite and can be well known to designers and builders of power systems. Because exercising a vulnerability is the only way a threat can have a negative impact, a comprehensive vulnerability protection plan provides a level of confidence that is unachievable with threat-based methods alone. A more detailed description of vulnerability and threat analysis can be found in the first white paper or a number of other documents.[6]

The importance of power

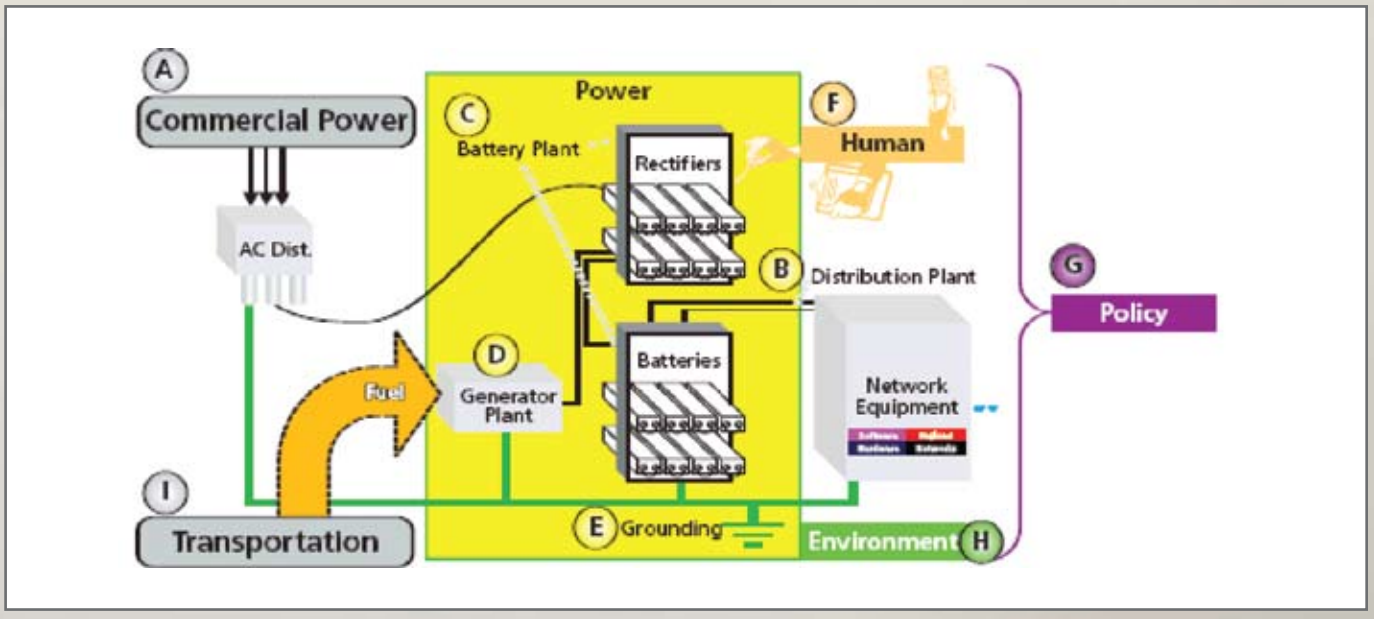
The critical importance of communications network power is underscored by the special attention given to this subject by stakeholder interest groups in recent years. Each of the following bodies has wrestled with the issue of how best to provide reliable power for communications networks:

- The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC)[7]
- U.S. Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI[8] and VII[9, 10, 11]
- The President's Network Security Telecommunications Advisory Committee (NSTAC)
- The U.S. Congress Select Committee on Homeland Security: [cite September 4, 2003 expert panel]
- IEEE CQR and Bell Labs co-sponsored workshops addressing emergency back-up power for commercial networks and for public safety networks
- "Report and Recommendations to the Federal Communications Commission," Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks.
- The European Commission-sponsored Availability and Robustness of Electronic Communications Infrastructures (ARECI) Report identified several key findings related to power

The importance of emergency power was recently re-emphasized by a major government regulatory body, drafting proposed regulations for emergency back-up power for both central offices and remote locations such as cell towers, remote switches and remote terminals.[12]

A SIMPLIFIED, GENERIC POWER SYSTEM

Figure 2. Simplified, generic power system[13]



Four high-level components constitute the power system:

- Distribution plant
- Battery plant
- Generator plant
- Grounding

Figure 2 depicts the components of a simplified power system model and shows that the power plant has direct, critical dependencies on some of the eight ingredients, such as environment, human, and policy, in addition to other infrastructures, such as commercial power and transportation. Commercial power (A) and the four power system components (B, C, D, E) are briefly discussed below, followed by a deeper vulnerability analysis of the battery plant (C) in the next section.

A. Commercial power infrastructure

The normal source of power for most communications installations. When commercial power is operating properly, the power room tends to be forgotten. However, commercial power is subject to interruption. As a result, the other components of the power system are required to provide emergency power when commercial power fails.

B. Distribution plant

The basic component providing the electrical connections from the power plant to the network equipment. The distribution plant includes the cable and wires that bring the power from the power plant to the system, the connections at both ends of the conductor, and fusing to protect from current overloads.

C. Battery plant (short-term reserve)

The emergency power source that is always on-line, and provides short-term emergency power. If the commercial power fails, the battery plant provides "no-break" power to the equipment so that there is no disruption of service. Most systems position a battery plant between the commercial power and the communications equipment so that even under normal operating conditions the battery plant is actually powering the system. In this simplified, generic power system model, the rectifiers that charge the batteries are considered part of the battery plant.

Battery back-up is considered very reliable[14], but plants located at remote sites (for example, cell sites or remote terminals) often provide power for a shorter duration than at a typical central communications hub. Space limitations or local regulations (policy) may mandate remote site locations. Under these conditions, provisions need to be made to quickly supply power from an alternate power source, such as a generator.

D. Generator plant (long-term reserve)

The long term emergency power source. Providing long-term power until commercial power is restored, generators take over when the finite backup of the battery plant loses its ability to support the communications equipment. Power generators may take the form of common generators powered by diesel fuel or natural gas, or other types of generators, such as fuel cells. In either case, the generator can provide power to the network for an extended period of time, limited only by the availability of fuel and the continued proper operation of the generator.

For remote sites, operators may choose to use either fixed or portable generators. When portable generators are used, the battery plant must be sized and engineered to allow for the time required to move the generator into position and connect it to the load. The use of portable generators adds several dimensions to planning that must be considered to maximize their effective deployment and value.[15] The generator plant includes the starting mechanism (which may include batteries), fuel pumps, and other supporting materials such as lubricant.

E. Grounding

Protecting workers and equipment from voltage spikes[16], grounding provides stability to the communications equipment by maintaining a solid reference potential on which all the equipment operates. While the grounding system generally requires little attention, a grounding problem can be very disruptive and is among the most difficult to identify. In addition, care must be taken when working in an environment where common bonding networks and isolated bonding networks exist.[17] A properly grounded system is vital to the continued, proper operation of a communications network and the safety of those that come in contact with it.

Intrinsic vulnerabilities of batteries

The previous paper on intrinsic vulnerabilities of power systems identified six vulnerabilities associated with battery plants. They include:

- Critical fuel characteristics
- Load limitations
- Interface limitations
- Chemical damage
- Aging
- Physical damage.[18]

Examining each of these vulnerabilities, and identifying various methods of defending them is key to a reliable battery plant.

- *Critical fuel characteristics* – All batteries contain active chemicals that react with each other to produce electricity. Over time, the chemicals tend to lose their ability to produce electricity. In a typical lead-acid battery, the lead plates will deteriorate and the electrolyte may lose its sulfuric acid content. When this occurs the battery will be unable to hold a charge, or it may quickly discharge when required to carry the load. In a typical communications installation, deterioration of one or more cells in a battery string would not be obvious as long as commercial power is floating the batteries and providing power to the load. However, when commercial power is disrupted and the batteries are called upon to support the load by themselves, the deterioration will manifest itself by a rapid drop in voltage and the eventual loss of power.

- *Load limitations* – Load limitations are experienced when the batteries are being drained during a power outage and impact how long they can support the load. The battery plant is sized to support an engineered load for a definitive period of time. When that time is exceeded, the voltage will decrease and the battery will eventually fail. This vulnerability that a battery string experiences during a power outage is amplified by load growth. As the load supported by the battery string grows — for example, due to adding equipment at a location — the ability of a battery plant to support the offered load, both in terms of capacity and duration can be strained. Installations that are properly engineered have sufficient battery power (both batteries and rectifiers) to support all of the critical equipment at the site until a longer-term source of power, such as a generator or fuel cell, can be brought on-line. Ideally, that same engineering also planned for additional equipment that is needed to handle future growth. However, experience shows that plans change, loads change, and unauthorized equipment can find its way onto the battery bus. During a commercial power outage, this unanticipated drain on the system may dramatically shorten the time that the batteries can support the load, potentially leading to a service outage.

- *Interface limitations* – Interface limitations primarily affect the rectifiers because they are the interface point of the battery plant to AC power (both commercial and generators) and remote human interaction. Unexpected voltages or frequencies on their input side may negatively impact the operation of these power conditioning devices and the batteries. In addition, rectifiers are also the general contact point for remote power maintenance. This makes them susceptible to both accidental and intentional human interactions that can reduce or eliminate their ability to condition AC battery power.

- *Chemical damage* – When the chemical make-up of the batteries changes, their ability to produce electricity may be affected. These changes can occur naturally over time, or be caused intentionally, for example, by sabotage.

- *Aging* – The chemical reaction that occurs in batteries causes changes to the chemicals and the batteries themselves. As batteries age, they typically lose their ability to hold a charge and can lose voltage faster when sustaining a load. Deterioration of the battery case may occur as the battery ages. The effects of aging can also accelerate under various conditions, such as the operation of batteries at elevated temperatures.

- *Physical damage* – Physical damage can be the result of human interaction, including accident or sabotage, environmental occurrences such as earthquake, building collapse, flood, and fire, or failure of the materials that make up the battery. In these instances, the battery plant may be partially damaged and still be able to provide some power, or totally destroyed, resulting in loss of communications services.

Influence of other selected ingredients on the battery plant

As shown in Figure 1, selected ingredients of the Eight Ingredient Framework directly impact the battery plant. The environment in which the battery plant exists substantially affects its performance. Cold temperatures tend to reduce battery output over time while elevated temperatures accelerate aging, and proper ventilation is essential to prevent the buildup of hydrogen gas given off by the chemical reaction that occurs in typical lead-acid batteries. Policy can also have an effect on the battery plant, manifested in local regulations or building codes that may impact battery installations, other back-up power systems, or fire sprinkler requirements.

Including the rectifiers as part of the battery plant brings the hardware ingredient into play. Rectifiers convert AC power received from commercial power or generators to DC power, which charges the batteries and carries the load. These rectifiers are sophisticated pieces of equipment, monitoring inputs and outputs and providing an interface for remote monitoring and maintenance. Failure of hardware in a rectifier can disable these remote maintenance capabilities or disable the rectifier entirely. Most installations have a series of rectifiers to eliminate single points of failure, but the loss of one or more rectifiers may drive the remaining rectifiers into overload and ultimately prevent the power plant from supplying the power required by the offered load.

The operation of rectifiers also requires software to support hardware functionality and to enable their advanced capabilities. These units are susceptible to not only hardware failures, but software failures, as well. The series of rectifiers at most installations are often of the same type and vintage, and in all likelihood, are running on the same software. For this reason, a generic software bug in one unit will likely be found in other units at the site, creating the potential for a cascading failure.

While the factors above can threaten a battery plant, the human element creates the largest potential for impact. Intentional attacks on a battery plant in the form of sabotage, vandalism, and/or theft are the most commonly considered threats that humans pose. Although these types of attacks are difficult to predict, preventing physical access to the battery plant location and cyber access to remotely-controlled rectifiers by unauthorized personnel are effective deterrents.

Network operators spend considerable time and effort protecting against intentional human threat, but unintentional human threats are by far the most insidious and challenging to defend against. Battery plants require maintenance in order to function properly, so completely eliminating human access, either physical or cyber, is not an option, The problem is that allowing human access introduces the possibility of human error. Because batteries are considered "low tech," maintenance tasks are often assigned to "the new guy," or just not done at all. This may be expedient in the short term, but can be very costly in the long run. Failure to perform routine maintenance jeopardizes the battery plant, and consequently the communication services that are powered by it. Allowing untrained personnel to work on the battery plant invites such common mistakes as shorting across power leads, disconnecting live power feeds, inadvertently turning off power supplies, or disabling alarms. These actions can result in loss of power to critical communications services, and even personal injury or loss of life.

Less obvious mistakes, but equally dangerous to the reliability of communications systems, include improperly taken measurements or readings, or failure to notice physical signs of battery deterioration. These signs are often the only indication of potential battery failure, and missing them by having an untrained person in the power room exposes the communication services to unnecessary and preventable failures. The single biggest countermeasure to protecting against unintentional human threats is to employ properly trained technicians on all work involving battery plants and power systems. Improperly or untrained technicians pose a threat to both the communications systems and themselves.

Protecting vulnerabilities

It isn't enough to simply identify vulnerabilities. Once they have been identified, vulnerabilities need to be protected from being accessed by a threat. Proper maintenance procedures, such as reacting to load readings, can mitigate load limitations. Limiting access can prevent a saboteur from causing damage. Intrinsic vulnerabilities are always present, but addressing them can prevent threats from taking advantage of them, effectively neutralizing the threat's potential impact.

The four primary means of safeguarding a battery plant's vulnerabilities have been identified in Figure 3 below. They include:

- Limited access
- Trained technicians
- Routine maintenance
- Alarms

Figure 3. Battery plant vulnerabilities and safeguards

	Safeguards			
Intrinsic vulnerability	**Limited access**	**Trained technicians**	**Routine maintenance**	**Alarms**
Critical fuel characteristic		■	■	
Load limitations		■	■	■
Interface limitations	■	■		
Chemical damage	■	■		
Aging		■	■	
Physical damage	■	■	■	■

- *Limited access* – This entails restricting both physical and remote access to the battery plant to properly-trained personnel with a legitimate need for access. Locking building doors is one obvious means of preventing physical access. Limiting access of untrained power technicians who are otherwise authorized to be in the building, and multiple companies co-located in a common space introduce additional complexity. Possible solutions include deploying electronic key systems that restrict access to the power room to properly trained personnel[19] and using locking cabinets or cages in shared spaces. Limiting remote access may include requiring strong authentication[20] for operational support systems and restricting access to remote power commands to those technicians properly trained in power procedures.

- *Trained technicians* – Limiting access eliminates intentional attacks by outsiders, and also helps reduce unintentional human attacks. However, people still need access to the battery plant — installation, growth, maintenance, and replacement activities all require technicians to be working in and around the battery plant, both on-site and remotely. As with any work on a communications system, the technician should be properly trained for the work to be done.

An untrained person in the power room is a threat to the power plant, the communications services, his co-workers, and himself. For this reason, only power trained technicians should be used. This is especially true in emergency situations where a wrong move can significantly delay restoration or even cause an outage. As one power expert noted, "Experienced and trained power personnel are your most valuable assets during a power emergency."[21]

Errors of "commission," such as an untrained technician shorting out a terminal, can harm a battery plant. Equally as damaging, but less obvious, are the errors of "omission," such as an untrained technicians failing to take readings properly, missing tell-tale signs of battery aging or damage, or ignoring indicators that load limitations are being reached. These errors often do not show up immediately, but they position the battery plant for a potentially catastrophic outage in the near future.

- *Routine maintenance* – Batteries are generally quite reliable, so there may be a tendency to ignore them; however, as many outage analyses have reported, an ignored battery plant is a ticking time bomb. Skipping or ignoring scheduled power plant maintenance is often found to be the root cause of communications outages associated with power failures. A report on the effects of Hurricane Katrina noted, "… not all locations were able to exercise and test the backup equipment in any systemic fashion. Thus, some generators and batteries did not function during the crisis."[22] The same situation occurred during the Northeast Power Blackout of 2003. Of the eight communications outages caused by failed power plants during that event, "lack of routine maintenance/testing" was a contributing factor to four of the outages. [23]

  Latent problems can often be uncovered and corrected before they cause a problem if battery readings and inspections are conducted regularly by qualified personnel. While routine maintenance needs to be performed, simply going through the motions with untrained personnel reduces the benefit and misses the opportunity to find problems before they cause service interruptions.

  An important aspect of routine maintenance is load testing. The battery plant must be capable of bridging the gap between the time commercial power fails and when an alternate source of power such as a generator or fuel cell takes over. If no alternate source of power is located at a site, the batteries must carry the load for the duration of the power outage or until a portable power generating unit can be delivered and brought on-line.

  In 2004, the median duration of a central office power outage was 5.5 hours.[24] Longer durations, on average, can be anticipated for remote locations. These factors should have been taken into consideration during engineering and the battery plant sized accordingly; however even a properly engineered battery plant may support the load for a shorter time than the calculated duration due to load creep and the effects of battery aging. Overloaded or undersized power plants were a contributing factor to 25% of the FCC reported failures during the 2003 Northeast Power Blackout.[25] Routine load testing can help identify these conditions and afford the network operator time to remedy them before they contribute to a service outage. There may be a tendency to defer load testing the battery plant for fear of encountering a problem and needlessly disrupting power, however it is much more desirable to encounter a problem under the controlled conditions of a test than during an actual emergency. Non-invasive testing and analysis techniques are available that predict battery capacity without the risks associated with discharge testing.

- *Alarms* – The majority of communications installations are unmanned for most of the day. This is especially true of remote locations, which may not be visited for days or weeks at a time. These locations depend on alarms to provide the network operator with a view of the power situation. According to the NRSC, "The classic cause of battery plant outages is failure of the alarms or failure to react to the alarm."[26] Properly monitored alarms can indicate that a plant is reaching its load limit and provide a reliable view of the status of the power plant.

  Under normal circumstances the network operator is aware of a power failure and takes steps — such as bringing a generator on-line — to carry the load and re-charge the batteries. However, there have been instances when power alarms were not operating properly and the operator was not aware of a power failure, or the failure of the generator to start. The batteries discharged and ultimately failed, resulting in an extended communications outage. For this reason, installing and maintaining proper alarms in the power room, and especially on the battery plant, is essential. A discharge alarm on the battery plant is a sure indication of power problems, and is therefore considered one of the most critical. [27] As stated in an ATIS NRSC power study, "The importance of power alarms can hardly be overemphasized if catastrophic power failures are to be driven to zero."[28]

Conclusion

The battery plant is the backbone of the communications power plant, as it is the only component that provides power that must always be up. Commercial power and generators may fail, but the battery plant must always be on-line.

Although viewed by some as low tech, it is certainly high impact. Communications outages that occur because of battery plant failure are statistically the longest outages due to the length of time it takes to restore the battery plant. Recovering from a battery outage is costly, both in terms of maintenance expense and impact to service, and is potentially dangerous to the people affecting the recovery.

There are a limited number of vulnerabilities associated with a battery plant and understanding these vulnerabilities is the first step towards safeguarding them. While understanding these vulnerabilities at a high level may appear somewhat straightforward, there are nuances associated with individual locations and specific equipment characteristics that must be studied and understood.

Although implementing a plan to address each vulnerability is the first step toward preventing battery plant outages, achieving the desired goals is always limited by resources and cost. Countermeasures may effectively address vulnerabilities, but still not completely close a vulnerability. For example, restricting access to battery plants will discourage most intruders, but a determined person may still gain access to the batteries and damage them. Therefore, every emergency power plan should have a provision for replacing batteries should they become inoperable.

The human element has the potential to exercise almost every vulnerability in the battery plant, and yet the major difficulty in protecting against unintentional human errors is that humans must be allowed to access the batteries. The only reliable approach to minimize these errors is to only allow properly trained technicians to perform installation and maintenance procedures. Improperly installed or maintained, the battery plant is the Achilles' heel of the critical infrastructure on which all other infrastructures depend. Properly installed and maintained, it is the unseen, secure foundation upon which today's communications services are built.

About the authors

Rick Krock
Member of Technical Staff
Bell Labs Network Reliability & Security Office

Rick has been actively involved in the development of numerous NRIC Best Practices and led several focus group power teams during NRIC VII. He provided disaster recovery leadership for the Great Hinsdale Fire and has been actively involved in national advisory committees for the President and FCC on power issues. He chaired the IEEE CQR conference on Emergency Power in Washington DC and the IEEE CQR Workshop on Power in Rome. Rick is formally trained as an electrical engineer.

Karl Rauscher
Bell Labs Fellow and Executive Director
Bell Labs Network Reliability & Security Office

Karl has provided leadership for numerous critical government-industry forums, including IEEE CQR, NRSC, WERT, NRIC and NSTAC. He has been an advisor for network reliability issues on five continents and has served as an expert witness for the U.S. Congress Select Committee on Homeland Security regarding the Power Blackout of 2004. Karl is a formally trained electrical engineer.

Jim Runyon
Technical Manager
Bell Labs Network Reliability & Security Office

Jim has led numerous industry studies on national network outage trends, including several in the area of power. He has been actively involved in the development of hundreds of industry best practices and oversees an expansive best practice implementation program involving hundreds of subject matter experts. Jim is formally trained in the fields of chemistry and computer science.

Peter Hayden
Senior Manager, Network Build and Integrate Business Unit
Alcatel-Lucent
Services Business Group

Peter manages Alcatel-Lucent's re-entry into the Telecommunications Power business. He has been actively involved in Alcatel-Lucent's Maintenance and Deployment offers for the past 7 years, with a concentration in Network Power in the last four. Peter is a formally trained mechanical and industrial engineer.

Patrick McGuan
Solution Manager, Network Build and Integrate Business Unit
Alcatel-Lucent
Services Business Group

Patrick manages the Network Power Solution. He has been a member of Alcatel-Lucent's Services Business Group for 10 years. Patrick is a formally trained mechanical and manufacturing engineer.

Notes

1 For a more comprehensive discussion of these topics, see: Karl F. Rauscher, Richard E. Krock, James P. Runyon, and Peter Hayden, "Intrinsic Vulnerabilities of the Power Systems Supporting Communication Networks and Expert Strategies for Defense, " 2007. *http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334*

2 Karl F. Rauscher, Richard E. Krock, and James P. Runyon, "*Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security*, Bell Labs Technical Journal, Vol. 11, No. 3

3 The IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR), Proceedings of the 2001 CQR International Workshop, May 2001; The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC), The NRSC 2002 Annual Report; The Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, NRIC VII Wireless Network Reliability Focus Group Final Report, Issue 3, October 2005, NRIC VII Public Data Network Reliability Focus Group, Issue 3, October 2005; The President's National Security Telecommunications Advisory Committee (NSTAC) Next Generation Networks Task Force Report, 2006; The European Commission Availability and Robustness of Electronic Communications Infrastructures, The ARECI Study, Final Report, March, 2007.

4 FCC NRIC VI Homeland Security Physical Security Final Report, December, 2003.

5 Ibid.

6 For a more detailed discussion of threats and vulnerabilities, see: Karl Rauscher, et al, "Annex B, *Communications Infrastructures Vulnerabilities*," *Availability and Robustness of Electronic Communications Infrastructure*, Report to the European Commission Information Society and Media Directorate-General, March 2007

7 *Power Outages Study Group*, August, 2002, and *Northeast Blackout Power Outages Study Group Report*, March, 2004.

8 Network Reliability And Interoperability Council VI – Homeland Security &Physical Security (FOCUS GROUP 1A)

9 Network Reliability And Interoperability Council VII – Focus Group 2A, Homeland Security – Infrastructure

10 Network Reliability And Interoperability Council VII – Focus Group 3A – Wireless Network Reliability

11 Network Reliability And Interoperability Council VII – Focus Group 3B - Public Data Network Reliability

12 FCC *Order on Reconsideration*, FCC07-177, October 4, 2007

13 Rauscher, Runyon, Krock, Hayden, *Intrinsic Vulnerabilities of the Power Systems Supporting Communications Networks and Expert Strategies for Defense*

14 IEEE Emergency Power Workshop held in 2004: "56% of the attendees rated battery as the most reliable source of back-up power, with 39% voting generators as the most reliable," "Survey Question Results", *http://www.comsoc.org/~cqr/PowerConf.html* slide 3

15 IEEE CQR Emergency Power Workshop: "74% identified generators the most cost efficient source of 8 hours of backup power, whereas only 5% identified batteries", Survey Question Results", *http://www.comsoc.org/~cqr/PowerConf.html* slide 4

16 A. F. Kirk, *Engineering and Validating Electronic Switching Systems To Withstand the Effects of Lightning Strikes*, Published at INTELEC, 1999

17 A. F. Kirk and S. V. Natale, *A Proposal for Hardware Compatibility in the Telecommunications Ground System Environment*, Presented at International Telecommunications Energy Conference, September, 2004

18 Ibid page 4

19 NRIC Best Practice 7-6-5012

20 NRIC Best Practice 7-7-8022

21 Charles Romano, "Power Blackout of 2003: Lessons Learned", slide 6, *http://www.comsoc.org/~cqr/PowerConf.html*

22 *Report and Recommendations to the Federal Communications Commission*, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, June 12, 2006

23 *NRSC Northwest Blackout Power Outages Study Group Report*, March 10, 2004 slide 5

24 *Network Reliability Steering Committee Annual Report 2004*, Alliance for Telecommunications Industry Solutions, October 2005 *http://www.atis.org/NRSC/Docs/2004_Annual_Report.pdf*

25 *NRSC Northwest Blackout Power Outages Study Group Report*, March 10, 2004 slide 5

26 NRSC *Analysis of Power Related Network Outages*, August 29, 1996

27 NRIC Best Practice 7-7-0689

28 1996 NRSC Power Study: "Analysis of Power Related Network Outages", August 29, 1996

Alcatel·Lucent