Alcatel·Lucent

STRATEGIC WHITE PAPER

Intrinsic Vulnerabilities of the Power Systems Supporting Communication Networks and Expert Strategies for Defense

Today's communications network is only as safe as it's power system. Recent natural disasters (Hurricane Katrina), intentional acts (the terrorist attacks of 9/11) and unintentional acts (the North East blackout) have underscored the importance of uninterrupted power to our communications infrastructure. When commercial AC is no longer available, the communications systems relies on a DC power infrastructure to maintain critical communications.

Knowing the vulnerabilities of the power system is essential to installing and maintaining a reliable power system. Although it is impossible to anticipate every threat, it is possible to have a thorough understanding of the power infrastructure. Through careful study, identification of potential weak points and the application of industry best practices, one fortifies the power infrastructure that protects the communications system from power interruptions.

This white paper introduces the following concepts: Eight Ingredients framework of communications infrastructure; vulnerability versus threat; basic network power system definitions; network power systems vulnerabilities; and a strategy for mitigating vulnerabilities.

Table of Contents

Executive Overview

Reliable power systems are *vital* to the operation of public communications network infrastructure. During normal operation, power systems serve in the *critical* role of interfacing with commercial electric power to provide high quality electric energy for highly specialized electronic equipment. During extreme events, whether they are natural in origin — such as hurricanes and ice storms, or human in origin — such as power blackouts and terrorist attacks, power systems are *essential*. Without power, communications equipment fails to operate and communications services disappear. The cascading impact of that loss would soon paralyze modern society — threatening national security, crumbling economic stability, and crippling emergency public safety capabilities, to name a few effects. Thus, *the reliability of power systems is crucial.*

To understand the *intrinsic vulnerabilities* of power systems that support today's diverse communications networks, including wireline, wireless, cable, satellite, voice, data and video, Bell Labs has developed a framework of eight ingredients of which the communications infrastructure is built. Power is one of these ingredients. Using this framework, scientific and engineering disciplines are used to establish the *finite nature* of their inherent vulnerabilities. This paper presents a comprehensive list of nine vulnerabilities intrinsic to power systems. By addressing these vulnerabilities, which are the only means that threats can negatively impact power systems, this approach allows for the identification of best practices that protect not only against known threats but also against unknown and unimagined threats.

The power system of a communication network is made up of four basic components: the distribution plant, the battery plant, the generator plant, and the grounding system. It is also heavily impacted by other infrastructures, such as commercial power and transportation, and by other ingredients of the communications system, such as humans, environment, and policy. Mastering knowledge of the finite list of intrinsic vulnerabilities of these components makes it possible to provide *comprehensive coverage* of all the areas of power systems. An example of this type of analysis is provided for generator fuel. Subsequent papers will provide in-depth analysis for other components of the power systems.

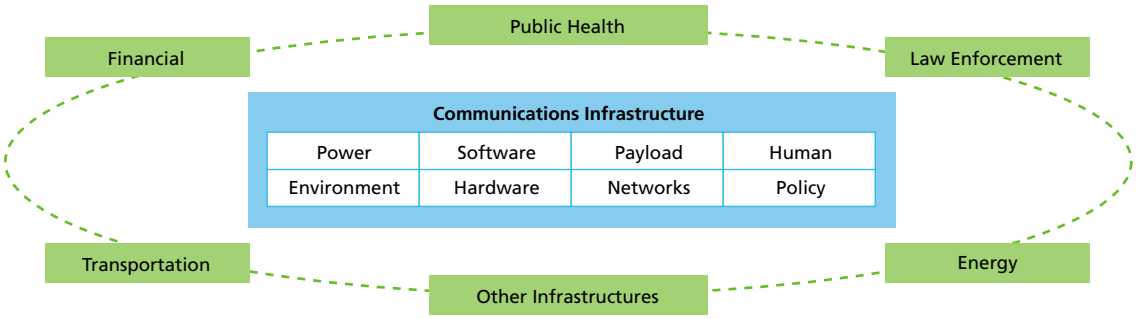
Power systems are an extremely critical piece of today's communications systems. Knowing the vulnerabilities of the power components and the supporting infrastructures is essential to installing and maintaining a reliable power system, which protects both the communications infrastructure and the people who work on it.

Approaching Vulnerabilities

The Eight Ingredient Framework

The communications systems of today are a complex blend of hardware, software, and other components that deliver the wealth of services that have become a part of our daily lives. Analyzing systems as complex as these communications networks is a daunting task. To help with this task, Bell Laboratories developed an Eight Ingredient Framework that has proven to be very useful in better understanding various critical aspects of communications infrastructure, including: intrinsic vulnerabilities, parameters affecting network reliability, and the anticipated impact of emerging trends.[1] Critical industry-government-academia fora have been using the Eight Ingredient Framework for several years and it has proven itself invaluable in numerous analyses.[2]

Figure 1. Eight Ingredient Framework

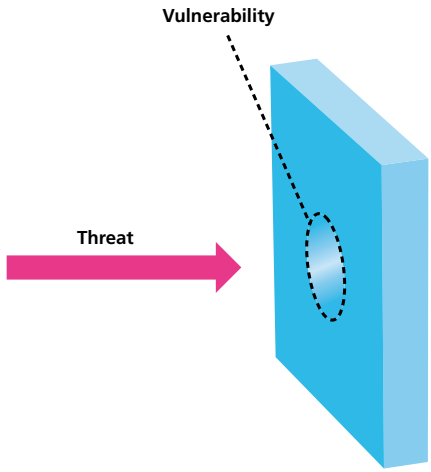


Communications infrastructure is made up of eight basic ingredients (Figure 1). While every one of these ingredients is necessary to the delivery of communications services, power is foundational — the remaining seven are useless without it. When there is no power, hardware is dead, software frozen, networks asleep, payload lost, environments untamed, humans idle and policies meaningless. Without power, there are no communications services. This ingredient-based framework is the context within which this paper explores the vulnerabilities intrinsic to the power ingredient, and offers highly expert approaches to mastering the reliability and security of power systems.

Thinking Vulnerabilities vs. Threats

Threats and vulnerabilities are the two elements that, taken together, allow someone or something to cause harm. Threats exercise vulnerabilities (Figure 2). The communications industry has defined a threat as *"anything with the potential to damage or compromise the communications infrastructure or some portion of it."*[3] Examples of specific threats to power systems include a commercial power voltage spike, an untrained worker being assigned to design a critical circuit, or vandals throwing sand in a generator's oil reservoir. Practically speaking, threats are infinite in number. This is because there are innumerable permutations of a given threat (e.g., use of sugar instead of sand). Because threat knowledge can become quickly outdated, its currency is ever fleeting. Threat knowledge is very valuable, but it is insufficient in protecting critical infrastructure.

Figure 2. Threat & Vulnerability Relationship



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."*[4] Examples of vulnerabilities intrinsic to power systems are battery power limitations, loss of circuit connectivity, and generator dependence on fuel (a complete list is provided later). Unlike threats, the number of vulnerabilities is finite. Because vulnerabilities are fixed, each can be explored in depth, with the value of that knowledge being retained despite the passing of time. The vulnerabilities of power systems can be well known by their designers and builders. Further, because exercising a vulnerability is the *only way* a threat can have a negative impact, a comprehensive vulnerability protection plan can provide a level of confidence that is unachievable with threat-based methods only.

The US National Strategy for Homeland Security states that "terrorism depends on *surprise*."[5] A proactive, rather than reactive, posture is further prescribed by the guidance of the 9/11 Commission Report with its assertion that this historic national tragedy was in a major way caused by ". . . a failure of *imagination*."[6] From a critical infrastructure protection perspective, one of the fundamental lessons of this event *is the need to identify and address vulnerabilities* — independent of threat knowledge.[7] If one addresses all vulnerabilities, "imagining" all possible threats (an impossible task?) is not necessary. This emphasis does *not* mean that one should abandon threat and associated risk analyses; it means one must supplement it, balance it, and integrate it with intrinsic vulnerability analysis.

The New Vulnerability Paradigm

The critical importance of communications network power is underscored by the special attention given to this subject by high-profile fora in recent years. Each of these bodies faced the issue of how best to provide reliable power for communications networks:

- The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) chartered several studies on power-related network outages
- Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) focus groups impaneled numerous power experts on various power teams
- The President's National Security Telecommunications Advisory Committee (NSTAC) established a task force to address related national security issues
- The U.S. Congress Select Committee on Homeland Security held expert hearings
- IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR) and Bell Labs co-sponsored workshops addressing emergency back-up power for commercial networks and for public safety networks

During the early 1990s, following several nationally impacting network outages, the FCC chartered the NRIC, an industry advisory group, to make recommendations toward optimizing the reliability of public communications networks[8]. Since its inception, that effort has identified voluntary industry best practices, each of which are already implemented and demonstrated to be effective. Prior to the terrorist attacks of September 11, 2001, most reliability efforts concentrated on developing countermeasures for threats already seen.

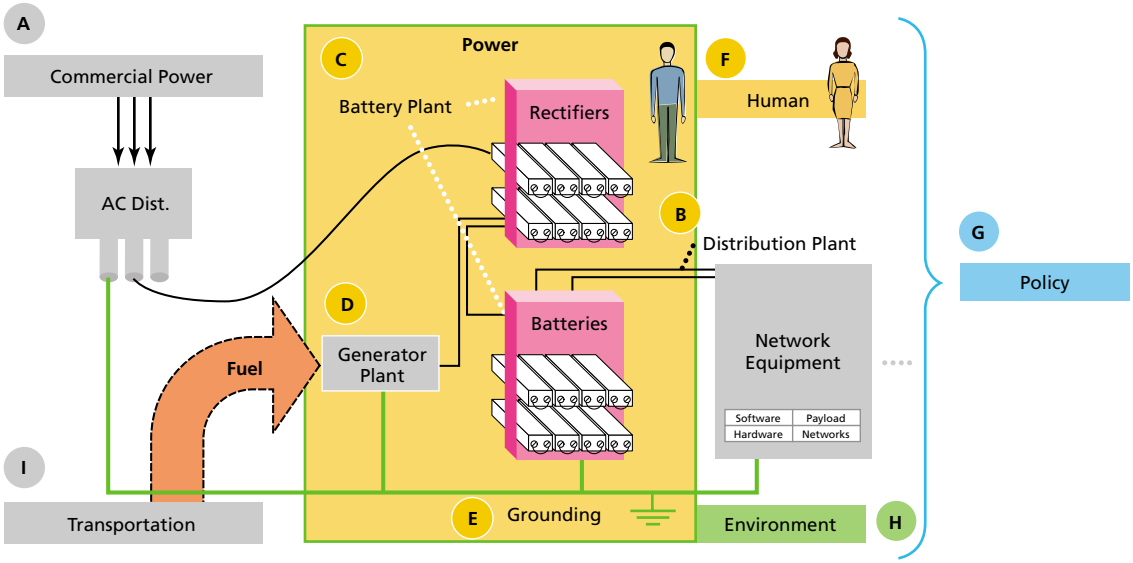
After the September 11 terrorist attacks, the need for vulnerability-based analyses became dramatically evident. What September 11 demonstrated is that new, unimagined threats may manifest themselves with disastrous consequences. It became clear that only protecting against previously seen threats would doom us to always being one step behind the attackers. Applying the thorough and systematic methodologies of the scientific and engineering disciplines, Bell Labs began looking beyond previously seen threats to concentrate on intrinsic vulnerabilities of the building block ingredients.

Advanced power reliability management in the post-9/11 world begins with recognizing that each element of a system has intrinsic vulnerabilities that can be made less susceptible to being exploited by threats. The advantage of the vulnerability-oriented approach is that one need not identify and defend against every threat (i.e., an impossible task), precisely because the underlying vulnerabilities are finite, are well understood, and are being addressed — independent of specific threat knowledge. The necessity of such an approach has been further confirmed by subsequent, previously unseen, events like 2003's Northeast Power Blackout and 2005's Hurricane Katrina and resulting New Orleans flood.

A Simplified, Generic Power System

In discussing vulnerabilities, we consider a simplified, generic power system for a communications network. Figure 3 shows how the components of a power system are supported by the eight ingredients of communications infrastructure and even some of the other critical infrastructures. Four high-level components constitute the power system: Distribution Plant, Battery Plant, Generator Plant and Grounding. However, there are direct, critical dependencies on other ingredients, such as Environment, Human and Policy, as well as other infrastructures, such as Commercial Power and Transportation. At a deeper level, even the remaining ingredients play a role in power systems.[9] The following section reviews each of these areas and compiles the vulnerabilities of the power system components (B, C, D, E). The areas external to the power system also will be discussed, but their vulnerability discussion will be limited, as these are outside the scope of this paper (A, F, G, H, I).

Figure 3. Simplified, Generic Power System



Commercial Power Infrastructure

The dependence of the communications infrastructure on commercial power is an infrastructure interdependency. This dependency recognizes that there are similar vulnerabilities within the other infrastructures, and that the protection and reliability of each critical infrastructure is essential for the operation of all the others.

Commercial power is the "normal" source of power for most communications installations. When commercial power is stable and operating properly, the power room tends to be forgotten, however commercial power is subject to interruption. Because of this, and because it is the component over which the network owner has the least control, the other components of the power system that provide emergency power are necessary.

Distribution Plant

The most basic component of the power system is the electrical connections from the power plant to the network gear. The means by which power is delivered to communications network equipment is connectivity from the power source to the target equipment. The distribution plant includes the cable and wires that bring the power from the power plant to the system and the connections at both ends of the conductor. It also includes the fusing and alarming capabilities.

There are two intrinsic vulnerabilities of the distribution plant: (1) *loss of connectivity*, and (2) *loss of potential*. The former can occur by cables being cut or disconnected (either intentionally or unintentionally), by connections losing continuity due to corrosion or some other chemical or physical action, or by the operation of a fuse that removes power to protect the system from excess current flows. The latter occurs from a short-circuit condition within the distribution plant.

Battery Plant (Short-Term Reserve)

The emergency power source that is always on-line and that provides short-term emergency power is the battery plant. 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. Should the commercial power fail, the battery plant provides "no break" power to the equipment so that there is no disruption of service. In this simplified, generic power system discussion, the rectifiers that charge the batteries are considered part of the battery plant.

There are six vulnerabilities of the battery plant: (1) *critical fuel characteristics*, (2) l*oad limitations*, (3) *interface limitations*, (4) *chemical damage*, (5) *aging*, and (6) *physical damage*. Critical fuel characteristics refer to the batteries' active chemical. Load limitations refer to duration limitations as well as the capacity shortfall, as network gear growth may exceed battery capacity. Interface limitations refer to the allowable window for critical interface parameters for commercial power. The power conditioning (e.g., rectifiers) capabilities have limitations that can be defeated by an unexpected voltage or frequency. Chemical damage encompasses the ability for the chemical make-up of the batteries to be altered. Aging refers to the decreasing performance of a battery over time. Finally, physical damage acknowledges that these physical assets can be destroyed in part or in whole.

Generator Plant (Long-Term Reserve)

When commercial power is lost, batteries provide no-break power and, based on the sizing of the plant, can provide backup power for a finite, relatively short amount of time. Without another power source to replenish them, the voltage drops and the batteries eventually lose their ability to power the communications equipment. Power generators are needed to provide power when commercial power will be out for longer periods of time. These may take the form of generators powered by diesel fuel or natural gas, or some other type of power generator, such as fuel cells. In either case, when supplied with sufficient fuel, the generator can provide power to the network, through the batteries, for an extended period of time, limited only by the availability of fuel and the continued proper operation of the generator. The generator plant includes the starting mechanism, fuel pumps and other supporting materials, such as lubricant.

There are five intrinsic vulnerabilities of the generator plant: (1) *critical fuel characteristics*, (2) *load limitations*, (3) *wear*, (4) *aging*, and (5) *physical damage*. Critical fuel characteristics include availability, contamination, and combustion. Load limitations refer to the ability of the generator to support the offered load as that load increases through equipment growth. Wear captures the susceptibility of moving mechanical parts to break down at points of contact and their eventual failure from prolonged stress. Aging encompasses the short- and long-term susceptibility to rust, lack of lubricant, and other deterioration. Finally, physical damage acknowledges that these physical assets can be destroyed in part or in whole, particularly if they are deployed outside, where exposure to the elements is more severe.

Grounding

Grounding provides stability to the communications equipment, maintaining a solid reference potential on which all the equipment operates. In addition, it provides protection for the equipment and the personnel who work on it from voltage spikes.[10] 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.[11] 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.

The grounding circuit has one intrinsic vulnerability: *loss of connectivity.*

Human

The Human ingredient literally touches every aspect of power systems. Ultimately, every power system relies on people to design, install, and maintain it. Considering the inherent danger associated with working with large power sources, and the catastrophic impact a power problem can have on the communications network, the personnel that work on power equipment must be properly trained and experienced. This should include not only the basics of power, but a thorough understanding of the proper procedures and practices that need to be used to help ensure safety and continuity of operation. It often is difficult to find and retain experienced power expertise or to introduce new people into this important field. Human factors also include such things as sabotage, vandalism, and terrorism. These particularly highlight the need to address vulnerabilities rather than threats. Engineers know the vulnerabilities of systems and can design defenses to protect them, but they cannot know all of the threats that other humans can devise. By protecting against the known vulnerabilities, they protect against both known and unknown threats.

Policy

The policy ingredient includes any type of inter-entity agreement on expected behaviors, expanded as: Agreements, Standards, Policies and Regulations (ASPRs). Examples of ASPRs affecting power systems include cell site landlord contracts, the trend for local municipalities to apply building sprinkler code requirements to communications equipment buildings, and requirements for maintaining short-term back-up power reserve on customer premises for lifeline services. Examples of ASPR vulnerabilities include conflicting agreements, misinterpreted standards and outdated regulations.

Environment

The Environment ingredient includes the buildings and remote shelters where equipment is stored, and the ground where the reference potential is anchored. These buildings provide physical security, physical structure on which to be installed, and protection for equipment from weather, as well as stabilization of temperatures in the operating environment. There are numerous vulnerabilities within the Environment ingredient. Of particular interest for power system protection are the security access-related aspects.

Transportation Infrastructure

As the Commercial Power Infrastructure is essential for the normal operation of power systems, the transportation infrastructure is essential for continued long-term power when the commercial power is unavailable. This is because on-site fuel supplies are limited, and therefore new supplies need to be transported to the communications equipment site. Because of this dependency, issues that impact the delivery of fuel (e.g., the ability to pump fuel into delivery trucks, passable roads, authorization of fuel trucks into secure areas) could impact communications power. Recent national disasters have given ample evidence that the transportation sector can be significantly affected during such events. Effects include delays caused by vehicle inspections, immobility due to devastation, and gridlock due to vehicle congestion.

Other Infrastructure Dependencies

The cascading effects of critical infrastructure interdependencies are endless.[12] The best protection will be provided when other critical infrastructures utilize proactive, systematic vulnerability-based approaches toward protecting their critical assets and operations. A network operator may have little control over cross-sector vulnerabilities, but needs to be aware of them and make provisions to protect themselves from them to the extent possible.

Table 1. Comprehensive List of Power System Intrinsic Vulnerabilities

	Power System Component			
Intrinsic Vulverability	Distribution Plant	Battery Plant	Generator Plant	Grounding
Loss of Connectivity	■			■
Loss of Potential	■			
Critical Fuel Characteristics		■	■	
Load Limitations		■	■	
Interface Limitations		■		
Chemical Damage		■		
Wear			■	
Aging		■	■	
Physical Damage		■	■	

Comprehensive List of Power System Intrinsic Vulnerabilities

The previous section reviewed the vulnerabilities of power system components: Distribution Plant, Battery Plant, Generator Plant, and Grounding. Table 1 lists each of these, showing their association with these four components.[13]

As explained earlier, network operators can focus on addressing vulnerabilities, independent of threat knowledge. This comprehensive list, when accompanied by in-depth knowledge of each item, provides critical guidance for optimizing power system reliability.

Addressing Power System Vulnerabilities

At this point, this paper has presented a framework for understanding the vulnerabilities of power systems. In addition, the table above provides a complete list of the vulnerabilities that must be mastered. In this section, the discussion turns to expert-based approaches for mitigating the continuous presence of intrinsic vulnerabilities.

There are four key aspects to an expert-based strategy for addressing ever-present vulnerabilities:

- vulnerability coverage
- vulnerability management
- vulnerability remedies
- vulnerability training

Vulnerability Coverage

The key to vulnerability coverage is to be aware of *all* vulnerabilities. As explained above, this is possible because, unlike threats, the number of vulnerabilities is finite. Also, since it is unlikely that every vulnerability can be completely addressed, the *degree to which they are being addressed* should be known. Poor vulnerability coverage means less complete knowledge of vulnerabilities or lack of awareness of the extent to which protection is being provided. Expert coverage includes 100% identification, detailed knowledge of the degree to which each is being addressed, and *thorough knowledge of where* each vulnerability is manifested. The subject of vulnerability knowledge also will be discussed below under "vulnerability training."

Vulnerability Management

Managing vulnerabilities involves dealing with their constant presence with limited resources. One method of making the best use of limited staff, equipment and time is to learn from historic analogy. Being familiar with relevant past experiences of one's organization, deployed products and

geographic region lays the foundation for this knowledge. Learning from peer network operator experiences can further expand this knowledge base. For example, the ATIS NRSC has conducted special studies on power outages at times during the past decade when data aggregated at the national level across multiple entities suggested statistically significant trends in this area.[14,15] These studies typically provide insights into the major causes of power system outages and the most current voluntary best practices recommended to address these concerns.

Another way to manage always-present vulnerabilities with limited resources is to factor in timely threat information. For natural disaster preparedness, publicly available weather alerts can be tremendously beneficial in planning for snow and ice storms, tornados, hurricanes and other extreme weather conditions. Maintaining good communications with local governments and utilities also can be beneficial for information on such things as planned brown outs. At a national level, U.S. Department of Homeland Security advisories provide alerts regarding possible terrorist threats. Qualified network operators can join government-industry information sharing bodies to benefit from such insights.

Both past and present alert threat knowledge are means of prioritizing limited resources to address vulnerabilities. With such information, protection measures can be bolstered — either temporarily or as part of a long-term strategy. However, it is vital to understand that focusing on vulnerability management without vulnerability coverage can be a *crucial mistake* as it can leave some less familiar vulnerabilities completely unaddressed.

Vulnerability Remedies

There are two objectives when addressing vulnerabilities. The first is to protect against them being exercised by threats. The second is, in anticipation of their eventual exploitation, providing alternate means of providing the anticipated lost capability.

Vulnerabilities in critical infrastructures can be addressed by various means. Regulations are used when government jurisdictions take action to control situations. Standards are used when multiple entities see a need for an agreed-upon measure to be established. Best practices are used when experts share information about highly effective methods of solving classes of problems. For example, to address fire concerns, local governments may regulate acceptable building materials, national standards bodies may define standards characteristics for suppliers of electronic equipment[16], and the industry may assemble its collective wisdom to articulate voluntary best practice guidance regarding training for personnel handling combustible materials.

Best practices have the advantage in that they typically have the fastest process for turning new knowledge into guidance; they are developed by subject matter experts, they are voluntary, and they are generally flexible so as to accommodate a wide range of diverse applications. Examples of the essence of voluntary industry best practices for power systems include:

- *Distribution Plant* – Best practice guidance includes: preventing the loss of connectivity through the use of proper procedures, following industry standards, performing preventative maintenance, and providing diverse paths for critical circuits.
- *Battery Plant* – Best practice guidance includes: providing routine maintenance, predicting eventual failure, and designing battery duration with consideration of the criticality of the service being protected and the ability and time required to provide longer term backup power.
- *Generator Plant* – Best practice guidance includes: minimizing the time interval required to bring up generator units for long-term back-up power, periodically exercising generators, and confirming ability to handle required load, regularly operating under controlled conditions.

Example

As an example of the type of analysis that should be performed for each component, the specific vulnerabilities of generator fuel will be examined in greater depth. The diesel generator is still the most deployed type of generator in public communications networks, although generators that run off of other fuels (such as gasoline or natural gas), and fuel cells (that use hydrogen for fuel) also are being used. Regardless of the type of generator, the common characteristic is the need for fuel, so the lack of usable fuel is the base vulnerability. This can manifest itself in many ways. The fuel tanks may run dry and not be able to be resupplied. The fuel tanks may contain fuel, but the fuel may be contaminated or of the wrong type and therefore unusable. The fuel tanks may be full, but the pumps used to move the fuel from the tank to the generator may be inoperable. These are just three examples related to a single vulnerability: critical fuel characteristics. The three examples cited are all real threats that have occurred, but there are many more specific ways for the lack of fuel to manifest itself. Rather than attempt to identify all those ways and defend against them, we address the basic vulnerability of the need for fuel and find ways to address that.

Fuel also can be used as a force of destruction, damaging or destroying equipment and buildings if it were to ignite in an uncontrolled manner. An attack of this type can be considered to have acted upon several vulnerabilities; it would have deprived the generator of the required fuel, and it may have caused physical damage to the equipment, building or personnel associated with the site. Because of the obvious impact such an occurrence would have, there are best practices that address protecting fuel supplies from unauthorized access. As mentioned earlier, the requirement of the generator for fuel exposes it to dependent vulnerabilities associated with the delivery of fuel. While not directly under the control of the network operator, these dependent vulnerabilities must be accounted for when establishing a comprehensive power plan to assure reliable operation of the network.

- *Grounding* – Best practice guidance includes: training on methods of detecting problems, and conducting periodic verification that grounding is sound and functioning as designed.

Another source of remedies is *emerging technology*. For example, Bell Labs innovations include software-controlled methods of prioritizing communications services during commercial power outages so as to extend the duration of back-of-power supplies.

Vulnerability Training

The most complex interactions related to power systems are human. This includes humans whose job it is to install and maintain the system, humans who may be called upon in an emergency to work with the power system, and humans whose intent is to damage or destroy the system. Training personnel for power systems includes two dimensions. The first includes basic design and operational principles, which can be provided through best practices. The second is just as essential, and it is a working knowledge of the fundamental vulnerabilities of power systems. Training should be ongoing.[17]

Humans make errors, and there are many best practices aimed at reducing those errors through proper procedures, job aids, and training. A mistake when working in the power plant can quickly result in service disruption, equipment destruction, personal injury, or even death. Once viewed as a place to send new employees to keep them out of the way, the power room has shown itself to be a critical asset that requires the attention of well-trained, seasoned professionals. For unintentional human threats, perhaps the best defense is utilizing people trained specifically on power and power equipment.

A working knowledge of power system vulnerabilities distinguishes whether a team is optimally prepared for a wide range of normal and unexpected power system challenges, or relatively unprepared for such and in fact teetering on the verge of causing unnecessary delay during the recovery of a critical outage, triggering a major network outage, or causing an avoidable tragic accident. Power teams should be equipped with a mastery of each of the intrinsic vulnerabilities to the degree where they understand the fundamental scientific and engineering principles behind them. This will provide significant value throughout the power system lifecycle.

Conclusion

For the sake of public safety, socioeconomic stability and national security, it is imperative that communications network reliability be optimized. The power system is the foundation on which today's legacy and emerging next-generation communications networks are built, and the reliability of the power system has a more direct and significant impact on communications reliability than any other factor. This paper presents an approach to understanding power system vulnerabilities within a *systematic framework*, demonstrates how to *master power system vulnerabilities* by producing a comprehensive list, and outlines *expert methods for addressing* them.

Protecting power infrastructure is best accomplished by performing thorough, systematic analysis of its vulnerabilities and implementing processes and procedures to protect those vulnerabilities from being exercised by potential threats — both known and unknown. This paper enumerates the vulnerabilities associated with power systems and provides examples of methods of addressing some of those specific vulnerabilities. Subsequent papers will provide in-depth analysis of other components of the power infrastructure, however analysis without action is meaningless. To be effective, this analysis must lead to a well-developed plan for addressing the identified vulnerabilities. Best practices — already implemented by world-class companies — have been identified by industry experts to address these vulnerabilities. They call for a rigorous program of maintenance, exercise, and testing, performed by people trained specifically in the art of power. The critical nature of the power room demands the attention that only a well-trained workforce, schooled in the scientific approach detailed in this paper, can provide.

About the Authors

Karl Rauscher

Bell Labs Fellow and Executive Director, Bell Labs Network Reliability & Security Office

Karl has provided leadership for numerous critical government-industry fora, 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. He is a formally trained electrical engineer.

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 has led several focus group power teams during NRIC VII. He provided disaster recovery leadership for the Great Hinsdale Fire of 1988 and has since been actively involved in national advisory committees for the President and FCC. He is formally trained as an 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. He is formally trained in the fields of chemistry and computer science.

Peter Hayden
Senior Manager, Network Power Solutions Business Development, Alcatel-Lucent Services

Peter oversees 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 five years, with a concentration in Network Power in the last two. He is a formally trained mechanical and industrial engineer.

Footnotes

1 Rauscher, Karl.F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

2 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.

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

4 Ibid.

5 National Strategy for Homeland Security, Office of Homeland Security, July 2002, Executive Summary, pages viii. [emphasis added]

6 9/11 Commission Repot. 2004. pages 336-339.

7 Rauscher, K. F., Krock, R. E., *The Three Theatres of Security*, Presentation to the IDC IT and Internet Security Conference, Lisbon, Portugal, January 2006.

8 The Great Hinsdale Fire of 1988, The Major Signaling Outages of 1991.

9 For example, power conditioning systems include electronic hardware and software, and are managed remotely over data networks.

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

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

12 For example, a pandemic-stressed health infrastructure could impact the availability of personnel to maintain and operate power systems, or an economic collapse-stressed finance Infrastructure could impair the ability of companies to order supplies and pay bills.

13 The authors acknowledge that while the principle of intrinsic vulnerabilities being finite is established, there are various methods of describing and organizing them.

14 ATIS Network Reliability Steering Committee (NRSC) Northeast Blackout Power Outages Study Group Report, March, 2004. (http://www.atis.org/NRSC/Docs).

15 ATIS Network Reliability Steering Committee Power Outage Study, August 2002.

16 Telecordia GR-63-CORE Network Equipment Building System (NEBS)Requirements April 2002

17 The FCC NRIC VI Homeland Security Physical Security Focus Group Final Report highlights this subject as an Area for Attention: "Power System Competencies Need to Be Maintained Service Providers and Network Operators need adequate levels of competent staff to maintain the power infrastructure. Detailed knowledge and significant experience is required for these special systems. Having these core competencies is a particular concern in the event of a widespread power emergency." Final Report, Issue 3, December 2003, p 46.

Alcatel·Lucent