

# System Safety and Security

## Chapter Recommendations

### Nuclear Power Plants

21. Apply relevant findings from the bi-national *Outage Task Force Report* to the operation of nuclear facilities in Illinois.
22. Work with the Nuclear Regulatory Commission and utilities to ensure that nuclear power plants have the policies, procedures and equipment in place to withstand a massive outage.

### Cyber Security

23. Implement the appropriate findings from the bi-national *Outage Task Force Report* and the NERC Critical Infrastructure Protection Advisory Group to ensure that safeguards are in place to protect the integrity of both the generation and distribution systems.
24. Review background check programs for utility employees and contractors to ensure the programs properly correspond to the risk involved for the designated positions.
25. Reconfigure utility computer operating systems to remove remote access and prevent malicious cyber attack.

### Emergency Preparedness

26. Review the state's critical response plan and prepare plans for a worse case scenario.
27. Ensure 24 hours of back-up power for all hospitals and nursing homes.
28. Ensure that all telecommunication systems have at least 24 hours of back-up power.
29. Enhance back-up power for 911 systems and evaluate their capacity to handle a substantial increase in calls during outages.
30. Implement the appropriate safety recommendations offered by parties affected by the August, 2003 blackout.
31. Disseminate information on how to respond to an emergency situation.
32. Develop the appropriate legislation to eliminate potential communication and information problems.

## Background

When the August, 2003 blackout first occurred, there were initial concerns of terrorism. However, the bi-national *Outage Task Force Report* stated there was insufficient evidence to substantiate claims of responsibility by al-Qaeda or any other terrorist agents. The report concluded that a series of equipment malfunctions and human error led to the disturbance.

While nine U.S. nuclear power plants and thirteen Canadian nuclear power plants shut down to protect equipment and systems from the grid disturbance<sup>60</sup>, other U.S. emergency preparedness plans performed short of expectations. At various emergency facilities such as hospitals and police stations, back-up generators became clogged with debris or depleted their fuel supply. Battery back-up systems were unable to maintain lights or communication systems through the duration of the outage. Emergency preparedness plans were geared for limited outages, not a sustained outage.

## Key Issues

The Illinois Special Task Force focused on the safety and security of the state's utility infrastructure, and the safety and security of Illinois residents in case of blackouts. Concerns exist concerning the safety and security of Illinois' nuclear power plants and the cyber security of the electric utility infrastructure.

The safety and security of Illinois residents relies on emergency preparedness and the effectiveness of Illinois Emergency Management Agency, Federal Emergency Management Agency and Illinois Department of Public Health. Emergency communications are provided via the Illinois Emergency Communications Network.

<sup>60</sup> The U.S. nuclear power plants are Fermi 2, Oyster Creek, Perry, Nine Mile 1 and 2, Indian Point 2 and 3, FitzPatrick, and Ginna.

# 1. Nuclear Power Plants

The bi-national *Outage Task Force Report* also focused on nuclear power plants, even though non-nuclear power plants were most affected by the outage. They found no evidence that the shutdown of U.S. nuclear power plants triggered the outage or inappropriately contributed to its spread.

The bi-national *Outage Task Force Report* found:

- All nuclear power plants that shut down or disconnected from the grid responded automatically to grid conditions.
- All nuclear power plants responded in a manner consistent with plant designs.
- Safety functions were effectively accomplished, and the nuclear plants that tripped were maintained in a safe shutdown condition until restart.
- Nuclear power plants did not trigger the outage or inappropriately contribute the outage's spread.

One concern about a nuclear power plant tripping off the grid is ensuring access to an alternative power supply to keep the reactor core cool. The Nuclear Regulatory Commission (NRC) has requirements for the number of off-site power sources and ability to withstand certain transients that cause abnormally high voltages or currents which can severely damage equipment.

Off-site power is the normal source of power to safety systems when a plant's main generator is not in operation. If off-site power is unavailable, the NRC requires emergency generation (typically diesel generators) to provide back-up power to the safety systems.

In addition, the Illinois Emergency Management Agency (IEMA) and the NRC provide oversight of the safety aspects of off-site power issues through inspection programs, monitoring operating experience and performing technical studies.

## A. Illinois Situation

Illinois currently has 11 operating nuclear power reactors at six locations across the state, in or near the towns of Braidwood, Morris (Dresden), Cordova (Quad Cities), LaSalle, Byron and Clinton.<sup>61</sup> These 11 reactors provide over half of Illinois' electric power.

The safety of these plants during a major statewide grid outage is obviously a matter of concern. The process of shutting down a nuclear facility, especially the cooling of the reactor, requires the availability of a substantial amount of dependable offsite power for the reactor.



Byron nuclear power plant

Nuclear power plants are designed to shut down upon "loss of off-site power" (LOOP). Fast-starting emergency diesel generators provide the back-up source of power for plant cooling and other essential systems. Studies performed by the NRC revealed that loss of off-site power is a major contributor to the risk of nuclear core damage. The NRC developed criteria for the size and quantity of the diesels to ensure that adequate power and redundancy will be available during a loss of off-site power. The NRC evaluation of Illinois plants resulted in the addition of diesels to reduce that risk.

<sup>61</sup> Illinois Emergency Management Agency, Division of Nuclear Safety

The NRC mandates that reactor designs must adhere to a 1 in 10,000-year core damage frequency. Current operating reactor designs surpass these requirements. Likewise, utility requirements in the U.S. have a 1 in 100,000-year core damage frequency with better plants operating at 1 in 1,000,000. It is likely plants built in the next decade will see a 1 in 10,000,000-year core damage frequency.<sup>62</sup>

The Illinois Emergency Management Agency believes that Illinois nuclear stations are well within accepted risk estimates, and pose no risk to public health and safety during grid loss. It should be noted that during the grid loss of August, 2003, nine U.S. reactors were forced to resort to back-up diesel emergency power without incident. In some cases they were on diesel power for up to fourteen hours and no significant problems occurred during that outage.

### **B. August, 2003 Blackout**

The bi-national *Outage Task Force Report* found that the severity of the power variation caused generators, turbines or reactor systems to reach their protective limit and automatically shut down. All of the U.S. plants tripped in a manner consistent with their plant designs and safely shut down. All safety functions were effectively accomplished with few problems, and the plants were maintained in a safe shutdown condition until their restart.

The nine plants used their emergency diesel generators to power their safety-related systems during the power outage. Off-site power was restored to the safety buses after the grid was energized and the plant operators, in consultation with the transmission system operators, decided the grid was stable.

The plants returned to power operation following a deliberate process controlled by plant procedures and NRC regulations.

Nuclear plants do not have black-start capability allowing them to restart immediately. Therefore, it may require at least a day before the nuclear power plant can restart following a *normal* trip. When a trip is combined with loss of off-site power, additional recovery actions are required that may extend start-up time. The first U.S. nuclear plants came back on line August 17, 2003. The last plant, which needed equipment repairs, returned to service five days later.

#### **Recommendations 21-22: Nuclear Safety**

While the Illinois Special Task Force was satisfied that all of U.S. nuclear power plants operated according to design specifications during the August, 2003 blackout, it does not believe that the industry can rest on its laurels. The Illinois Special Task Force recommends that the Illinois Emergency Management Agency:

21. Review the bi-national *Outage Task Force Report* for any additional findings that may be applicable to the operation of the nuclear power plants in Illinois.
22. Continue to work with the Nuclear Regulatory Commission and Illinois utilities to ensure nuclear power plants have proper policies, procedures and equipment in place to withstand a massive grid outage.

<sup>62</sup> Provided by the University of Illinois at Chicago, [www.uic.com.au/nip14.htm](http://www.uic.com.au/nip14.htm) (visited 6/3/04)

## 2. Cyber Security

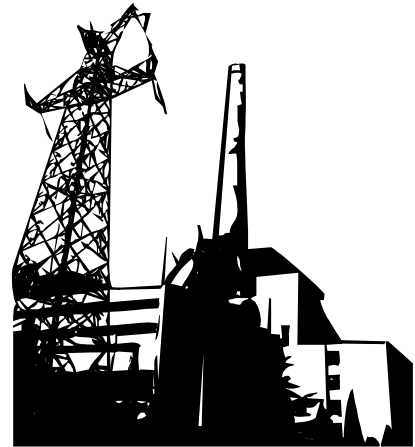
The Security Working Group (SWG) of the bi-national Outage Task Force was asked to investigate whether a malicious cyber event may have caused or contributed to the outage. The SWG found no evidence suggesting that the viruses or worms prevalent across the Internet at that time had any impact on power generation or delivery systems.<sup>63</sup>

The SWG study identified concerns with respect to: the possible failure of alarm software, links to control and data acquisition software, and the lack of a system or process for some operators to adequately view the status of electric systems outside their immediate control. The SWG is working with the energy industry to examine the cyber systems that control power generation and delivery systems, the physical security of cyber assets, cyber policies and procedures, and the functionality of supporting infrastructures (i.e. communication systems and back-up generators).

The generation and delivery system has been a target of malicious groups including hackers. The most common methods of cyber corruption are through use of worms and viruses. Infiltration by worms and viruses could be prevented by decreased user access and properly updated protection protocols.

Emerging security concerns apply to the Supervisory Control and Data Acquisition (SCADA) systems. The SCADA systems are the operating programs through which the power facilities are monitored, the Emergency Management Systems (EMS) are controlled, and the means through which power facilities communicate with each other.

SCADA systems were developed to maximize functionality and interoperability, with little attention given to cyber security. In some instances, there may be a need for employees to remotely monitor SCADA systems. Overuse of remote monitoring contributes to the problem of unmanageable size and security risks, and curtailment would reduce the risk of cyber infiltration.



The North American Electric Reliability Council's (NERC) Critical Infrastructure Protection Advisory Group is examining ways to improve the cyber security of the North American power grid. Development of a national program to improve the physical and cyber security of these control systems is now under discussion in the United States by multiple agencies.

### Recommendations 23-25: Cyber Security

Cyber security is an emerging and crucial concern as utility companies become increasingly dependent on information and support provided through vast computer systems. The Illinois Special Task Force recommends:

23. The Illinois Commerce Commission review and, where appropriate, implement the findings from the bi-national *Outage Task Force Report* and the NERC Critical Infrastructure Protection Advisory Group.
24. The Illinois Commerce Commission shall review electric utility company background/security checking programs for new employees and contractors to ensure the programs properly correspond to the risk involved for the designated positions. The program should also be sensitive to the nature of the facility (e.g. nuclear; fossil).
25. The utility companies should reconfigure the Supervisory Control and Data Acquisition (SCADA) system to remove the offsite/remote access units. The computer systems of utility companies should contain adequate measures and protocols, consistently updated, to protect against the potential of a malicious cyber attack.

<sup>63</sup> U.S.-Canada Power System Outage Task Force, *August 14<sup>th</sup> Blackout: Causes and Recommendations*, April, 2004, page 131

### **3. Emergency Preparedness**

There are three primary governmental agencies providing emergency management assistance in Illinois: 1) Federal Emergency Management Agency, 2) Illinois Emergency Management Agency, and 3) Illinois Department of Public Health. Emergency communications are provided via the Illinois Emergency Communications Network.

#### **A. Federal Emergency Management Agency**

The Federal Emergency Management Agency (FEMA) was created in 1979 to reduce loss of life and property as well as protect our nation's critical infrastructure from all types of hazards. Now part of the U.S. Department of Homeland Security, FEMA has more than 2,600 full-time employees and 4,000 standby disaster assistance employees. FEMA often works in partnership with other organizations that are part of the nation's emergency management system, including state and local emergency management agencies, federal agencies and the American Red Cross.

The Federal Emergency Management Agency helps equip local and state emergency preparedness, and provides food, water, mobile kitchens, water purification units and other supplies to support disaster operations and recovery centers. FEMA clears debris, opens transportation routes and restores public utilities, as well as provides mass sheltering and feeding.

The Federal Emergency Management Agency coordinates the federal response to disasters ranging from tornadoes to hurricanes, making federal disaster assistance available to states, local governments, businesses and individuals. It can provide loans and grants to repair or replace damaged housing and personal property. FEMA also has specialized teams for rapid damage assessment, emergency communications, medical assistance and support, urban search and rescue, emergency power restoration, incident management and community relations.

#### **B. Illinois Emergency Management Agency**

After the August, 2003 blackout, the Illinois Emergency Management Agency conducted an analysis of the agencies that participate in the State Emergency Operation Center (SEOC) to determine their readiness to respond in a blackout emergency. The analysis focused on the agencies' communication capabilities, and ability to keep critical infrastructure up-and-running during a blackout.

As a part of the review process, IEMA met with representatives from cities impacted by the August, 2003 blackout. Improvements made by those cities in response to the blackout were also incorporated into the SEOC analysis.

Key findings of the State Emergency Operations Center analysis include:

- The 4-year old critical response plan for Illinois trauma centers and other critical infrastructures appears inadequate.
- The State Emergency Operations Center and Department of Central Management Services need to identify back-up fuel sources for the back-up generators.
- Critical facilities require uninterrupted power supplies (UPS) which generally are good from two to four hours. Back-up generation lasts as long as its fuel supply. The Illinois Emergency Management Agency has nine days of back-up power.
- Critical state agencies have communication capabilities. The agencies either have high frequency radio, cell phone back-up or lines that do not require electric power to operate, as well as satellite communications that can operate on battery power.

### **C. Illinois Department of Public Health**

The Illinois Department of Public Health (IDPH) has created two preparedness teams to respond to disasters within the State. They are the Illinois Medical Emergency Response Team (IMERT) and the Illinois Nurse Volunteer Emergency Needs Team (INVENT).

The Illinois Medical Emergency Response Team was created in 1999 in response to the increased national focus on terrorist threats. The mission of IMERT is to respond and assist with emergency medical treatment at mass casualty incidents in Illinois.<sup>64</sup> There are now 600 medical response team members and four fully-equipped teams on call around the clock. The goal is to have eight fully-equipped teams by the end of 2004.



**INVENT**  
Illinois Nurse Volunteer  
Emergency Needs Team

The Illinois Nurse Volunteer Emergency Needs Team (INVENT) was formed in 2003. The mission of INVENT is to respond to an incident where local resources have been overwhelmed and there is a need for an extended period of time for nursing care. It is anticipated that the first teams will be ready for deployment by 2005.

### **D. Emergency Communications**

The U.S. Department of Homeland Security released its “National Strategy for Critical Infrastructure” in February, 2003, with the aim of promoting reliability, comprehensiveness and resiliency of the nation’s critical infrastructure, including utilities.

Since September 11, 2001, attention has been directed toward assessing the security of critical utility facilities, implementing increased protective measures, and restructuring service plans in the event of a natural or man-made disaster. The August, 2003 outage demonstrated that while some progress may have been made in national emergency preparedness, more work must be done. Balancing the risks and costs of infrastructure security is difficult, and the threats are sometimes unknown.

Illinois utilities maintain Emergency Operation Centers (EOCs) on alert 24 hours a day for problems associated with their networks, systems, or facilities. In February, 2002, the Illinois Commerce Commission created a Task Force of the major energy and telecommunication companies serving Illinois customers to develop a plan to facilitate communications between utilities and government agencies in a disaster situation.

The work of the Task Force resulted in creation of the Illinois Emergency Communications Network (IECN). The IECN is a “virtual command center” that can be activated by a participating utility company or the Illinois Emergency Management Agency (IEMA) in response to a potential or actual emergency. Once activated, participants can exchange information with each other from remote locations while having a direct link to the IEMA Operations Command Center.

The following are examples of benefits derived from the creation of the Illinois Emergency Communications Network<sup>65</sup>:

- Establishment of a mutual assistance program between the private and public sector;
- Prompt, full and effective utilization of available resources;
- Immediate access to outside resources and established clear-cut procedures.

<sup>64</sup> Illinois Medical Emergency Response Team mission statement at [www.imert.org/](http://www.imert.org/) (visited 6/4/04)

<sup>65</sup> A list of the Illinois Emergency Communications Network participants is included in Appendix 9.

The Illinois Emergency Communications Network is a virtual command center to enhance decision-making and cut response time during disasters.

The IECN can be activated under these circumstances:

- A critical event occurred to the infrastructure across at least two industry sectors;
- 50,000 customers are out of service, or affected by the disaster;
- Outage time is expected to exceed 48 hours in duration;
- A major protection or protocol system such as SCADA is lost; or
- A widespread work stoppage transpires affecting a significant portion of a company's service territory.

If a utility believes it is experiencing an emergency situation, it can activate the IECN. The Illinois Emergency Management Agency will then review the situation to determine which members should participate in resolving the problem.

Currently, communication between IECN participants is conducted via e-mail, cellular telephone or landline phones. During the August, 2003 blackout, these forms of communication proved ineffective unless back-up service was available. Preferred communication tools for the IECN are high-frequency radio gateways and satellites. Utilities are reluctant to provide the Illinois Commerce Commission with confidential information. Understanding the various utilities' contingency plans would enable a more thorough analysis.

### **E. Back-up Services**

It was clearly evident during the August, 2003 blackout that back-up generators and batteries were insufficient to withstand a prolonged outage. History shows that major outages generally last from eight to 24 hours, and impact a large geographic area. In some cases, multiple states have been affected.

In Illinois, the Department of Central Management Services (CMS) oversees most state-owned buildings with the majority of these facilities located in Chicago and Springfield. Nearly every facility is linked to the CMS computer network.

The James R. Thompson Center in Chicago has stairwells equipped with battery-powered lighting in the event of a power loss. Lights are programmed to stay on for forty-five minutes, allowing enough time for a complete building evacuation. In addition, a generator would be utilized if the outage continued. The Michael A. Bilandic Building - another Chicago facility which houses state agencies - is also equipped with a battery-powered stairwell lighting system. Emergency phones designed to operate under severe conditions are located in the stairwells.

The State Capitol in Springfield is equipped with an emergency generator, but the adjoining Stratton Building, home to many state agencies, lacks back-up power. Information on emergency back-up systems in other state facilities is included in Appendix 10.

Following the August 2003 blackout, the *New York City Emergency Response Task Force Report* identified numerous concerns related to emergency back-up power. The New York City Report recommended enhancements to back-up power systems for telephone systems, 911 communications networks and health care facilities.

For example, ever since September 11, 2001, many government agencies had invested heavily in cellular technology which then malfunctioned during the outage. The cellular phone capacity of the general public was also greatly reduced, including the ability to call 911. Even the 911 system itself suffered from immediate overload.

New York City's emergency dispatch operation was still using outdated technology that was overwhelmed by the flood of calls. Even their back-up power systems failed when the outage lasted longer than the batteries in emergency dispatch radio equipment. There was no central repository of evacuation or public transportation options.

The New York City Report found many hospitals and even neighborhood fire stations were dark. Few private or public sector organizations had adequate supplies of water, batteries, flashlights or evacuation plans. In some buildings, lighting failed in stairwells or the public address system crashed. Most high-rise buildings lost power for water pumps, so potable water was unavailable to residents or businesses on higher floors.

A summary of recommendations from the parties affected by the August, 2003 blackout is included in Appendix 6.

<b>Recommendations 26-32: Emergency Preparedness</b>
<p>The Illinois Special Task Force is concerned that current state emergency measures may not withstand a major electric disturbance. The Illinois Special Task Force recommends that:</p> <ol style="list-style-type: none"> <li>26. The Illinois Emergency Management Agency review the state's critical response plan in light of the experiences of August, 2003 and initiate standards for a worse case scenario.</li> <li>27. The Illinois Department of Public Health review the back-up generator guidelines for life support facilities and develops plans to ensure the generators can sustain service for at least 24 hours.</li> <li>28. The Standards of Service for Local Exchange Telecommunications Companies needs upgrading to expand the back-up capability of the batteries and generators in central offices. The back-up should be at least 24 hours with guaranteed sources of batteries or fuel to support the system if an outage extends longer.</li> <li>29. The state's 911 systems need to enhance their back-up power capabilities and evaluate their capacity to handle a substantial increase in calls. Everyone reaches out to 911 during a time of emergency. The system has to be up-and-running with no interruption during the emergency. The 911 system needs to be evaluated to ensure that capacity is available to handle a flood of calls.</li> <li>30. Review, and where appropriate, initiate the safety recommendations from parties affected by the August, 2003 blackout. The Illinois Special Task Force recommends the members of the State Emergency Operation Center carefully review reports released by parties affected by the August, 2003 blackout. The Illinois Special Task Force also recommends that the SEOC continue to dialogue with other cities and states that have experienced blackouts.</li> <li>31. Disseminate information on how to respond to an emergency situation. The U.S. Department of Homeland Security (<a href="http://www.ready.gov">www.ready.gov</a>) and American Red Cross (<a href="http://www.redcross.org">www.redcross.org</a>) offer tips to follow in case of an emergency, including a terrorist threat and a blackout. All utilities within the state should provide links to these websites from their corporate websites as well as develop brochures with safety-related information to be disseminated to their customers.</li> <li>32. The Illinois Emergency Management Agency, in conjunction with the Illinois Emergency Communications Network, develop appropriate legislative and procedural solutions to address the potential communication and information problems identified to date by the bi-national Outage Task Force.</li> </ol>

## Conclusion

To maintain a competitive edge in the global information economy and a high standard of living for our residents, the state of Illinois must have a reliable and secure flow of energy. From the mightiest factory to the smallest personal computer, electricity is the lifeblood of our community.

The extent of the August 14, 2003 blackout that rumbled from Ohio through Canada to New York was a wake-up call for electric utilities, consumers and policy-makers. As the costliest power outage in human history, it offered us an opportunity to examine our own infrastructure here in Illinois.

When Governor Rod Blagojevich created the Special Task Force on the Condition and Future of the Illinois Energy Infrastructure, we became one of only a handful of states to squarely address this problem. The Task Force cast a wide net to generate ideas and positions from diverse voices. The unprecedented dialogue which followed led to the analysis and blueprint found in this report.

The scope of the Illinois Special Task Force's inquiry was comprehensive and the recommendations are balanced. By implementing the Blackout Solutions plan, Illinois will be well prepared for future growth and a safe and healthy environment.

