BONNEVILLE POWER ADMINISTRATION

February 2007

Physical Security Technology Roadmap

The Enigma was a portable cipher machine used to encrypt and decrypt secret messages

TECHNOLOGY INNOVATION OFFICE

PHYSICAL SECURITY TECHNOLOGY ROADMAP

In the aftermath of 9/11, the electrical industry, like many other critical infrastructure sectors, has been under considerable pressure to improve the security of its facilities. The Department of Homeland Security and the Department of Energy have levied numerous protection requirements on an industry where staffing resources and budgets have been reduced. This creates an opportunity where technology innovation may offer effective low-cost solutions that will enhance a utility's ability to manage its facilities during crisis conditions.

The Bonneville Power Administration (BPA) intends to pursue this opportunity. For this reason, BPA is seeking state-of-the-art electronic systems and tools that can be integrated and mutually shared between system operations staff and security staff to enhance the security of high voltage facilities. Such systems will need to:

- improve transmission system monitoring/assessment capabilities,
- provide for more secure facilities, and
- improve personnel protection.

The objective is improved system reliability across a broad spectrum of threat. These systems should feature improved designs and afford expanded application of technology to augment power system and security operations in a manner that helps mitigate risks to BPA's mission.

There is a need across the electrical power industry for the design and development of operations and physical security systems that function effectively within a high voltage electrical environment, which includes remote and unmanned facilities. Such systems must be robust and able to operate effectively in adverse weather conditions.

These security systems should provide features that are useful for both power system operations personnel and security staff. A dual purpose system will provide valuable tools that can be used to monitor routine operations, as well as providing assessment capability for security operations. The end products should be commercially available and applicable to the high voltage electrical substation industry at large, whether public or private.

BPA operates one of the most critical infrastructures in the region. Therefore, under this technology development initiative, BPA must consider the emerging security threats to its critical infrastructure. BPA has faced long-standing operational and security challenges in monitoring and securing its system due to the complexity of the BPA system, its geographical spread and the remote location of many of its facilities. State-of-the-art tools that enhance real-time monitoring, assessment and timely response are needed to improve BPA's capability to manage the power system across multiple hazard scenarios. In addition, tools that protect critical components and provide adequate delays for perpetrators, while also affording rapid response, are needed for both security and operations functions. These attributes must be key ingredients of the protection sets needed. Improvements in these technologies can improve risk management of emergency events on a real-time basis, whether the events are natural disasters or human caused.

In terms of operations and cost, a multi-purpose approach will best serve when applying any new technology.

BPA will help define the desired technological features and capabilities and provide an environment to facilitate the design and testing of the technology to ensure compatibility with the actual power system. BPA also will work within the region to encourage sharing of new security and operations technologies within the electrical power industry.

Historical challenges and considerations:

Historically, the public and private sectors of the high voltage electrical utility industry have done very little research and development (R&D) on security systems for the high voltage electrical utility environment. Instead, the utility industry has tended to adapt existing technologies that were designed and developed for non-electric environments. While some of these systems were adaptable, many presented significant operational and maintenance issues when subjected to high voltage environments and adverse weather conditions. The remoteness of many electrical facilities and the fact that many sites are unmanned contributed to these problems.

On the positive side, the Department of Homeland Security (DHS) is supporting some funding for security system initiatives that are managed by national laboratories, particularly where the end state is intended to provide value to both the government and private critical infrastructure sectors. Although this funding may not be targeted toward the electrical utility industry, future opportunities may be available if the electrical utility industry can clearly demonstrate some self-initiative. This industry also will have to justify any funding augmentation in competition with other non-revenue generating governmental critical infrastructure organizations.

BPA has enjoyed a long association with a number of the national laboratories on a number of different industry and national security subjects. As a result, BPA Security is often approached by national laboratory representatives and other vendors interested in partnering with BPA to collaborate on the mutual development of new security technologies. Such a partnership could provide strong incentives to labs and vendors for providing viable proposals to the nation's utility industry that will provide cost effective and reliable security solutions that address common security system needs. Given the current climate, there is heightened interest across the electrical utility industry in new security technologies.

The current DHS funding for the labs has provided the necessary resources for what is called "lab directed research and development." This has opened up the labs to ideas from outside their organizations as well as encouraging them to take a new look at existing R&D projects and applied technologies that may have application in other arenas. As an example, current sensor technology developed for Department of Defense (DOD) requirements is being modified for transmission line and tower sensor application that would measure system health.

A procedural and substantive list of new security standards is evolving from the North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC), as well as reliability guidelines and requirements relative to electrical utility physical

and cyber security systems. In addition, there is a growing realization that adversarial disruption of distributive systems – electrical, oil and gas, and water supply – could be catastrophic, and the impact of such events mandates serious consideration. Issues include potential service disruption costs and challenges in replacing equipment or shifting high voltage equipment production capabilities to areas outside the United States. Because of these and other risk factors, the U.S. owners and operators of critical electrical system infrastructure have a compelling interest in better protecting the nation's workforce and vast capital investments.

BPA is continuing to:

- Encourage other utility partners to focus on and share new technology ideas or developments with broad application across the industry.
- Collaborate with NERC, Edison Electric Institute (EEI), individual utilities and the national laboratories on recommended solutions and/or technological innovations that may provide solutions to common security concerns.
- Engage security system providers/vendors with security requirements to encourage private industry R&D to explore new product development.
- Encourage creative solutions with security system design/install contractors to explore and take advantage of available technologies that might be applied to protecting critical facilities.
- Offer BPA's security expertise, including facilities and technical engineering support, to labs for system testing.
- Provide feedback on lessons learned to help drive technological improvements.
- Work with Federal Columbia River Power System (FCRPS) partners in assessing available security system technology and explore the sharing of systems to maximize efficiencies and reduce operational costs.
- Encourage continued prudent development of security system standards among the regulatory authorities and industry partners, as well as maximum adherence to those system standards by the industry. An interconnected power system is only as secure as the weakest link. Therefore, it is hoped that all utilities will adopt similar security standards and utilize similar security equipment and procedures to help to maximize the security of the whole power system.
- Work with the federal Technical Support Workgroup (TSWG), a federally funded R&D security solution coordination group based in Washington, D.C. BPA has tentatively encouraged TSWG to earmark limited funds for physical security R&D activities.

Specific project proposal supported by TSWG:

Protective barriers with Integrated Intruder Detection System

Design, develop, demonstrate and commercialize a low-cost blast/ballistic barrier and intrusion detection system for critical assets at electrical substations, such as transformers, breakers, reactor banks, switch gear and control houses. The blast/ballistic protection should mitigate the effects of high-power rifle shots from approximately 50 yards, and of approximately 100 pounds of explosive material, such as C4 type explosives, placed close to the barrier. The intrusion detection system must provide early detection of intruders out to at least the perimeter. It must also communicate an alarm securely and wirelessly to a remote monitoring station.

The detection systems should include integrated distributed sensors for classifying and reporting the nature of the threat. Detection systems should also support a broad range of standardized configurations for infrastructure assets. The system must operate 24/7 in 500-kilovolt environments, at remote locations and in all weather conditions. The design should allow field crews to easily inspect, repair and restore facilities. And, ultimately, the system must be affordable for commercial energy companies.

Deliverables include: 1) a near-production-ready prototype; 2) monthly reports; 3) program reviews including a detailed preliminary design review and conceptual design review covering the design and commercialization efforts; 4) data for life expectancy under extreme environmental conditions; 5) a demonstration and training session for government personnel (two-to-three days); and 6) support during testing at a government facility (30-to-60 days). The program should have defined phases with clear deliverables, test procedures and exit criteria. It could have optional phases for expansion, integration or improved capabilities. Required government support or resources should be clearly indicted.

Future plans include:

- Forging stronger partnerships with TSWG, labs and other progressive utility partners, including the Federal Columbia River Power System partners.
- Establishing formal partnerships with selected labs and or vendors where appropriate.
- Participation as a prototype site for beta testing of new or improved security concepts/systems.
- Providing labs and or vendors involved with R&D with new ideas and concepts, along with lessons learned from existing systems used by BPA or other utilities.
- Encouraging constructive budget participation from Department of Energy and Homeland Security, as appropriate, for strategic planning technology targets
- Incorporating Continuity of Operations strategies and resiliency features into technology developments.

- Working with other utilities in support of a national standard for security design and systems application protocols leading to improved operating postures for critical electrical infrastructure facilities.

- Ensuring actual testing of technologies developed by Idaho National Labs relative to tower and transmission line sensor application to monitor, detect and assess natural or man-caused conditions.

Technology gaps:

- The use of bio-metrics to be integrated with system operations and access control.

- Improved barrier technologies: defensive countermeasures to harden systems; physical denial systems compatible with maintenance and operational requirements; critical substation physical hardening (e.g. new fencing technology, pumice and epoxy or Kevlar applications for barrier technology).

- Use of mobile assessment systems such as unmanned aerial vehicles or stand-alone remotely controlled mobile security systems designed for rapid deployment

- Application of wireless detection and assessment sensors for closed-circuit television (CCTV) applications and intrusion detection systems used in high voltage environments without unacceptable nuisance alarms. This includes testing and application of satellite imagery, night vision capability and improved CCTV for remote and unmanned sites.

- Passive automated denial systems for unauthorized attempts to enter or sabotage critical BPA systems or specialized facilities; i.e., control houses, control cable tunnels, etc.

- Self-repairing high voltage equipment and transmission lines, resistant to vandalism and other human-perpetrated acts.

- A physical barrier technology that complements the TSGW project but is tailored for individual coverage of high voltage components in substation yards.

- Development of nonmetallic grounding cables that withstand high voltage conditions, yet are not attractive to metal thieves.

Desired functionality:

Substations should have real-time CCTV wireless assessment capabilities that are free of unacceptable interference caused by electromagnetic forces from high voltage substation equipment. Wireless intrusion systems should also function without the unacceptable false and nuisance alarms generated from surrounding high voltage equipment. The utility industry would want physical security barriers that do not interfere with operations and maintenance activities

and that are cost effective for controlled utility rates under competitive markets. Also, interoperable communications systems that afford continuity of telecommunications in the event of either natural disasters or other events would add value to the reliability of the systems.

Consistent with this initiative, the desired state would include a resilient security communications and response network that will incorporate a next-generation computing and communications network, with security designs integrated in all initial key segments, nodes and links. This system would feature self-diagnosing responders and enunciators, as well as self-repairable physical and cyber infrastructure systems.

What it will take to attain the ideal functionality:

- Improve sensor performance for physical and cyber systems that use monitoring and detection systems. Sensors will need to be faster, more sensitive and more accurate. They must have reduced power requirements, increased durability, lower cost, and use robotic platforms (e.g., unmanned aircraft) for assessment/pursuit activities.

- Use common inputs and assumptions. Apply standardized vulnerability analysis and risk analysis of critical infrastructure sectors to develop the foundations for quantitative and economically based security solutions. Accordingly, develop enhanced monitoring and interpretation systems for automated protection, notification and alarming, intrusion deterrence, prevention and detection, and surveillance in both the physical and cyber domains.

- Broaden the application of integrated operations and security modeling, simulation and analysis for real-time decision support and planning.

- Improve prevention, detection and protection by developing new, low-cost physical perimeter and area defense systems, and develop methods for hardening critical physical infrastructures.

- Improve insider threat assessment capabilities, including technologies such as intent determination and anomalous behavior monitoring for insider threat detection. Developments should build toward integrated methods of personnel surety and improved document authentication and access authorization.

- Improve large-scale situational awareness for critical infrastructure from an insider and outsider threat standpoint.

- Define the communication and computing system architecture needed to create a national common operating picture (COP).

- Use pilot studies and test beds to begin integrating network architectures consisting of sensors, controls, real-time data and advance systems to have uniform structures, common language, interoperability, compatibility and scalability.

- Develop next-generation designs and architecture for devices and systems to include designed-in and built-in security. These systems must be reliable, autonomic, resilient and survivable.

- Develop a human interface with application of the technology that allows better comprehension and decisions.

BPA's priorities for internal support

- Enhanced critical electrical component design which provides inherent hardening characteristics that reduce risks of damage from natural or human-caused events.

- Technological solutions for theft deterrence for high value metal electrical components without reduction in physical properties.

- Technological developments in electronic solutions that address wireless capabilities for detection and assessment systems and interoperable communications with internal and external connectivity across the BPA service area. Also includes sensor technology that can be adapted to electrical transmission operations enabling tower and conductor health to be measured and transmitted over long distances.

- Personnel protection technology, such as duress systems that communicate with control centers to inform the agency that a lone employee has been injured, abducted or otherwise incapacitated. Such a system must provide location and automatic notification if activated.

- Adaptation of existing barrier technology or development of new state of the art barriers that afford a significantly improved protection characteristic for critical assets. Must be low cost, easily maintained, and not an access impediment to critical electrical components requiring routine inspection and maintenance.

Sources include:

S-1: The National Plan for Research and Development in Support of Critical Infrastructure Protection (2004).

S-2: EPRI, 2004 Annual Report (2005)

S-3: Grid Works Multi-Year Plan, Office of Electric Transmission and Distribution, US Department of Energy (March 2005)

S-4: http://gridwise.pnl.gov/vision/

S-5: http://gridwise.pnl.gov/vision/how.html

S-6: http://electricity.doe.gov/about/boxstory2.cfm?section=about&level2=box2

S-7: http://www.energetics.com/meetings/electric/pdfs/electric_roadmap.pdf (U.S. DOE, National Electric Delivery Technologies Roadmap, November 2003)

S-8: Electric Distribution: Multi-Year Research, Development, Demonstration, and Deployment Technology Roadmap Plan: 2005-2009, Office of Electric Transmission and Distribution, US Department of Energy (December 2004)