A Separate Network for Control System CyberSecurity

Peter L. Fuhr, Ph.D.1
Oak Ridge National Laboratory
One Bethel Valley Road, Oak Ridge, TN 37831 USA
fuhrpl@ornl.gov

Abstract

The electric utility sector smart-grid definition implies the need for ubiquitous communications and extensive controls to increase reliability, efficiency, flexibility, and cost effectiveness. Smart-grid features include demand-response capabilities, advanced controls, DER integration, increased situational awareness, smart metering, advancement of ancillary services, time-of-use pricing, and peak curtailment, to name a few. The communication technologies at the smart grid’s heart provide the backbone for these features, which risks being exploited by adversaries. Furthermore, adding numerous automated services and devices to support smart-grid objectives risk compromise. In essence, the attack surface of the utility control systems is significantly larger. For example, smart meter and Advanced Metering Infrastructure systems, when implemented incorrectly, could provide injection points to the utility and meters equipped with demand response capabilities introduce the possibility of direct customer power disconnect.

A separate network for control system cybersecurity defines a highly secure, resilient and redundant critical communications, sensing, and technical assistance solution supporting all elements of the electricity enterprise and its supply chain. It is designed to retain national continuity of operations, enable rapid restoration, and facilitate cost-effective protective measures to thwart consequences of cyberattacks, operational and physical threats, and natural disaster. Security and resilience enhancements are not about bolting on a costly, cumbersome exoskeleton. As a nation, we must infuse the grid’s operational architecture digital native attributes (DNA) with modifications resulting in immunity to attack and degradation. Objectives of a project to implement utilization of a separate communication network include:

• Implementing cyber defensive measures beyond what is possible on the public internet.

• Enhancing grid state monitoring with advanced sensing, measurements, escalating alert and situational awareness.

• Using existing buried treasure of infrastructure (e.g., dark fiber) as a cost-effective protective measure, exploiting advanced communications (5G-LTE private wireless) and cybersecurity technologies suitable for the expanding smart grid requirements.

• Using living laboratories to test security functionality and resilience – collaborating with utilities and suppliers for proof of concept.

A review of this concept is presented.

1 Distinguished Scientist, Director, Grid Security, Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA
E: fuhrpl@ornl.gov, M: 1-831-588-7558
1. BACKGROUND AND CHALLENGES

Electricity generated at power plants moves through a complex network of electricity substations, power lines, and distribution transformers before it reaches customers. In the United States, the power system consists of more than 7,300 power plants, nearly 160,000 miles of high-voltage power lines, and millions of low-voltage power lines and distribution transformers, which connect 145 million customers.\(^2\)

Local electricity grids are interconnected to form larger networks for reliability and commercial purposes. At the highest level, the United States power system in the Lower 48 states is comprised of three main interconnections, as depicted at Figure 1, which operate largely independently from each other with limited transfers of power between them. A balancing authority ensures, in real time, that power system demand and supply are finely balanced. This balance is needed to maintain the safe and reliable operation of the power system. If demand and supply fall out of balance, local or even wide-area blackouts can result.

- The Eastern Interconnection encompasses the area east of the Rocky Mountains and a portion of northern Texas. The Eastern Interconnection consists of 36 balancing authorities: 31 in the United States and 5 in Canada.
- The Western Interconnection encompasses the area from the Rockies west and consists of 37 balancing authorities: 34 in the United States, 2 in Canada, and 1 in Mexico.
- The Electric Reliability Council of Texas (ERCOT) covers most, but not all, of Texas and consists of a single balancing authority.
- The network structure of the interconnections helps maintain the reliability of the power system by providing multiple routes for power to flow and by allowing generators to supply electricity to many load centers. This redundancy helps prevent transmission line or power plant failures from causing interruptions in service.
- Resilience, as defined in Presidential Policy Directive 21 (PPD-21) is “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.”\(^{10}\) It includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.\(^{10}\) Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.

As stated in the Energy Sector-Specific Plan published in 2015, cybersecurity is a growing and evolving security challenge for the Energy Sector and more generally for the U.S. economy. Because of the shared responsibility to secure North America’s energy delivery systems against cyber threats, a common vision and framework is needed to guide the public-private partnerships. Both the electricity and the oil and natural gas industries have initiated enhanced approaches to plan for and counter cybersecurity threats to energy infrastructure operations.

In February 2013, the President signed Executive Order (EO) 13636, “Improving Critical Infrastructure Cybersecurity,” setting forth policies to address evolving cyber threats. Specifically, EO 13636 directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a cybersecurity framework. To facilitate the Energy Sector’s implementation of the NIST Cybersecurity Framework, DOE and industry partners collaborated to develop the Energy Sector Cybersecurity Framework Implementation Guidance, which relies on existing sector-specific standards, tools, and processes to help industry characterize, enhance, and communicate their cybersecurity posture using the NIST Cybersecurity Framework.

DOE also works with industry to develop new cybersecurity solutions for energy delivery systems through an integrated planning and research and development (R&D) effort. DOE’s Cybersecurity for Energy Delivery Systems is one such program, which emphasizes collaboration among the government, industry, universities, national laboratories, and end users to advance R&D in cybersecurity.\(^4\)

---

\(^2\) Energy Information Administration (EIA), Accessed on 22 July 2016 at https://www.eia.gov/electricity/


The U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability (OE) supports a comprehensive approach to cybersecurity for the grid by:

- Facilitating public-private partnerships to accelerate cybersecurity efforts for the grid of the 21st century;
- Funding research and development of advanced technology to create a secure and resilient electricity infrastructure;
- Supporting the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities;
- Facilitating timely sharing of actionable and relevant threat information;
- Advancing risk management strategies to improve decision making;
- Supporting sector incident management and response; and
- Enhancing and augmenting the cybersecurity workforce within the electric sector.

A key mission of the OE is to enhance the reliability and resilience of the nation’s energy infrastructure. Cybersecurity of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE’s Cybersecurity for Energy Delivery Systems (CEDS) program helps the energy sector by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. Figure 1 illustrates the vast interconnectivity of the U.S. power transmission network.

As a nation, we have made measurable progress in providing assurance that enable resilient next generation smart grid capabilities necessary for improvements in reliability and efficiency of bulk power generation and distribution systems. Efforts and investments range across the cyber-physical systems spectrum and these include the Smart Grid Investment Grant Program and the Smart Grid Demonstration Program. Taken together, these allow a stronger, more agile delivery of energy.

The Cybersecurity for Energy Delivery Systems (CEDS) Project funded industry-led, academia-led, and national laboratory-led research, development, and demonstration projects that lead to improvements in the cybersecurity of communications and control systems of the U.S. energy infrastructure. Although these achievements suggest we are making progress, the specter of a catastrophic cyber event looms large over the energy sector. We need to pursue a comprehensive strategy of robust cybersecurity, operational security and physical security upgrades.

---

Electricity subsector infrastructure components are vulnerable to many tactics. The most likely high profile and potentially consequential tactics, techniques and procedures (TTPs) are targeted shootings, intentional downing of power lines, and bombings. In the past decade, there have been thousands of intentional attacks and incidents in the United States against electricity subsector infrastructure. Targets have ranged from individual power lines to transmission substations and involved a variety of tactics. Effects from these incidents have varied, ranging from damaged components to power outages affecting thousands of customers.

Several incidents—including the April 2013 PG&E Metcalf substation shooting—have indications of insider information or in-depth knowledge of how and what to target to achieve maximum impact. This type of knowledge could be further used to affect electrical infrastructure in ways that could cause larger or longer outages or damage that is harder to repair.

Historically, control systems were physically separated from the internet and other network connections. With the advent of commodity platforms and common internet protocols, control systems can now be built at a much lower cost and can use generally available internet protocols. This results in increased efficiency and significant cost savings, but as the Industrial Control Systems - Computer Emergency Response Team (ICS-CERT) reported, the convergence of closed control systems with open internet-based networks, commodity operating systems, and commodity internet protocols has resulted in increased security risk.\(^6\)


In January of 2016, the DHS stated it was their key judgment that “advanced persistent threat (APT) nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber espionage. The APT activity directed against sector ICS networks probably is focused on acquiring and maintaining persistent access to facilitate the introduction of malware, and likely is part of nation-state contingency planning that would only be implemented to conduct a damaging or disruptive attack in the event of hostilities with the United States.”\(^7\) Given this exposed architecture, what protective measures can help us safeguard the integrity and security of the Supervisory Control and Data Acquisition (SCADA) and ICS communications that operate our infrastructure?

Hackers already target the energy sector more than any other part of U.S. critical infrastructure. There are more reported cyber incidents in the energy industry than in healthcare, finance, transportation, water and communications combined — and those are just the intrusion attempts that are detected and reported.\(^7\)

If hackers were to knock out 100 strategically chosen generators in the Northeast, for example, the damaged power grid would quickly overload, causing a cascade of secondary outages across multiple states. While some areas could recover quickly, others might be without power for weeks. The scenario is not completely hypothetical. We had a preview in 2003, when a blackout spread...
from the coastal Northeast into the Midwest and Canada. The 2003 Northeast blackout showed that any extended grid failure could have a large price tag. That multiday blackout, which was attributed to a tree branch in Ohio, not a cyberattack, affected an estimated 50 million people in the United States and Canada and was estimated to cost about $6 billion.\(^7\)

In December of 2015 a blackout caused by hackers came in the form of a coordinated assault, as suspected Russian hackers penetrated Ukraine’s power grid, knocking out electricity for 225,000 people. The hackers flooded the customer service center with calls, causing technical difficulties and slowing the response.

As a case in point, on December 23, 2015, the Ukrainian Kyivoblenenergo, a regional electricity distribution company, reported service outages to customers. The outages were due to a third party’s illegal entry into the company’s computer and supervisory control and data acquisition (SCADA) systems. Seven 110 kV and 23 35 kV substations were disconnected for three hours. Later statements indicated that the cyberattack impacted additional portions of the distribution grid and forced operators to switch to manual mode. The event was elaborated on by the Ukrainian news media, who conducted interviews and determined that a foreign attacker remotely controlled the SCADA distribution management system. The outages were initially believed to have affected approximately 80,000 customers, based on the Kyivoblenenergo’s update to customers. Within the Ukrainian electrical system, these attacks were directed at the regional distribution level. It was subsequently revealed that three different distribution energy companies were attacked, resulting in several outages that caused approximately 225,000 customers to lose power across various areas.\(^10\)

In the Ukrainian incident, the attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the information technology networks of the electricity companies.\(^11\) The attackers demonstrated the capability to harvest credentials and information to gain access to the ICS network. Additionally, the attackers showed expertise, not only in network connected infrastructure; such as Uninterruptable Power Systems (UPS), but also in operating the ICSs through supervisory control system; such as the Human Machine Interface (HMI).

Finally, the adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-Ethernet converters, inoperable and unrecoverable. In one case, the attackers also used telephone systems to generate thousands of calls to the energy company’s call center to deny access to customers reporting outages. However, the strongest capability of the attackers was not in their choice of tools or in their expertise, but in their capability to perform long-term reconnaissance operations required to learn the environment and execute a highly synchronized, multistage, multisite attack.

The following is a consolidated list of the technical components used by the attackers, graphically depicted in Figure 3:

- Spear phishing to gain access to the business networks of the power companies
- Identification of BlackEnergy 3 at each of the impacted power companies
- Theft of credentials from the business networks
- The use of virtual private networks (VPNs) to enter the ICS network
- The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
- Serial-to-Ethernet communications devices impacted at a firmware level
- The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs
- Utilizing uninterrupted power systems (UPS) systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call center.

---


The Ukrainian attack resulted in relatively moderate consequences for the citizens, but it was a chilling reminder of the loss of control of a nation’s critical infrastructure. Here in the United States we have explored the impacts of more widespread and longer duration outages caused by adversarial attacks. In November 2015, over 4,400 participants and 364 utilities, agencies and other organizations participated in the GridEx III tabletop exercise. The tabletop scenario involved simulated physical assaults on key electric and transmission facilities coupled with cyberattacks on grid controls. The exercise after action review no doubt enhances situational awareness and provides additional insights for consequence assessment, but security and resilience require actions and implementation.

2. ROLES, RESPONSIBILITIES AND READINESS

Reliability and resilience are related, but distinct, concepts with different performance goals or metrics. In many cases, the projects and investments being made to improve day-to-day reliability contribute to resilience; however, there is not a one-to-one correspondence. In August 2012, the President’s Council of Economic Advisers released a study on the benefits of investing in grid resilience. The study explained the difference between resilience and reliability as: “A more resilient grid is one that is better able to sustain and recover from adverse events like severe weather—a more reliable grid is one with fewer and shorter interruptions.”

The North American Electric Reliability Corporation (NERC) has the mission of assuring the reliability of the bulk power system in North America. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. In 2014, NERC adopted a new physical security standard for all owners/operators under its authority. CIP-014-1 was designed to identify and protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged because of a physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Each Transmission Owner must perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in the Standard.

NERC Standard CIP-002 R3 requires that Responsible Entities develop a list of Critical Cyber Assets essential to the operation of its Critical Assets, which were identified through a risk-based assessment methodology. The National Institute of Standards & Technology (NIST), Smart Grid Interoperability Panel (SGIP), works closely with DOE and the sector in support of research, design, development, and implementation of cybersecurity measures by providing guidelines for smart grid cybersecurity.

The energy sector faces an increasingly sophisticated and aggressive physical and cyber threat environment. Intelligence reports indicate that cyber adversaries are more persistent and better financed, and their ability to develop and launch new attack tools and techniques could outpace the sector’s ability to develop and deploy new countermeasures. In addition to an evolving threat environment, new vulnerabilities are increasing as the nation transitions to a cleaner, more efficient energy economy. Smarter technologies will significantly increase the number and availability of digital access points to energy communication networks. New threats, business practices, market trends, regulations, and technologies challenge and reshape the security landscape of energy delivery systems.

In 2011, the Energy Sector Control Systems Working Group (ESCSWG) promulgated the “Roadmap to Achieve Energy Delivery Systems Cybersecurity”. The Roadmap provided the framework and a schedule of milestones for a sustaining program that builds a culture of security, assesses and monitors risk, implements new protective risk reduction measures, and manages...
incidents.\textsuperscript{13} The ESCWG Roadmap stated, "cybersecurity is one of the top emerging and standing issues facing the electric sector over the next 10 years."\textsuperscript{14} The ESCWG further noted that among the trends and drivers affecting future energy delivery systems security:

- Increasing system interconnectivity
- Increasing use of Internet Protocol (IP)-based communications
- Increasing reliance on wireless communications
- Increasing use of distributed intelligent devices and controls
- Increasing number of digital access points in delivery communication networks
- The continuing need for remote access.

Each of these attributes of the evolving energy system architecture represents a significant vulnerability to system integrity, security and operational continuity.

Critical elements of the energy system are the industrial control systems (ICS) used in the delivery, transmission, and distribution of electricity, telecommunications, water, oil, and gas. Increasingly, these types of systems are moving away from standalone, physically isolated networks and custom protocols to more general-purpose computers and networks, including the Internet. While this migration results in significant gains in productivity, efficiency, and lower costs, it comes with increased exposure to networked-based attacks resulting from the exploitation of operating system and application software vulnerabilities.\textsuperscript{15} Worse yet, several ICS systems employ antiquated operating systems that no longer maintain ongoing security upgrades to protect vulnerabilities, so these systems are in fact dangerously beyond their safe service life.

Today’s smart grid is essentially a geographically dispersed embedded real-time control application employing thousands of processors synced over a network. Like other such applications, this has a purpose, a topology, networking protocols and, processors. The smart grid topology includes three networks. There are the actual copper wires and switches (or “switchgear”) that carry electricity. There is a control network, including distributed intelligent electronic devices such as circuit breaker controllers, voltage regulators and digital protection relays. These devices are connected to each other, to the switchgear and to supervisory management stations via fiber optic Ethernet. Finally, there is a timing network running over the same fiber optic Ethernet that connects all these other devices to a central clock. All this equipment is located in geographically dispersed substations similar to that portrayed in Figure 4.

![Figure 4: Typical Substation. A substation is the grid interconnect consisting of a switch yard (where voltage conversion, line switching and line protection occur) and a control building housing electronics for substation control and timing. (Source: http://rtcmagazine.com/articles/view/1021908)](image)

Figure 5 depicts the logical connectivity of a typical smart substation. Utilities need to service installed equipment via network connectivity. Today that connectivity is via the increasingly vulnerable Internet. Equipment used in substations today typically employ either DNP3 or IEC61850 protocols for communications with electrical substation automation systems. Figure 5 illustrates the typical communications bus architecture. Regardless of the protocols used, modern gear is IP-addressable, incredibly useful for vendor maintenance, but requiring the risks inherent in general purpose Internet network connectivity.

![Figure 5: A smart substation with all control and timing elements interoperating over Ethernet. (Source: http://rtcmagazine.com/articles/view/1021908)](image)

\textsuperscript{13} SCWG, Roadmap to Achieve Energy Delivery Systems Cybersecurity, 2011, pages 21-40; accessed on 19 July 2016 at https://www.controlsystemsroadmap.net
\textsuperscript{14} ibid., pg. 20.
In 2016, the available network is the general purpose Internet itself. The wild Internet is rampant with malicious software (malware) and is easily “reachable” by state-sponsored attackers, hackers, or other nefarious actors. This persistent threat is exacerbated by the proliferation of new attack points embodied in the exploding growth of the Internet of Things (IoT).

A secure network is essential to interconnect the substations nationwide with their respective control centers, generation facilities, and authorized analytical collaborators. It is increasingly evident that we can make enormous advances in grid security and resiliency by having the grid components and equipment off the highly vulnerable “public internet” onto a secure, industrial internet.

3. BURIED TREASURE

In fiber-optic communications, “dark fiber” or unlit fiber is the name given to fiber optic cables not in service by a carrier or provider. The cables are not yet connected to any optical device on either end of the fiber run, and the fiber is installed with the purpose of being used at some point in the future. There is no authoritative inventory of the fiber optic cable infrastructure within the U.S. Approvals for installation are typically recorded with state public utility commissions (PUCs) and other state and local government bodies. The subset of unlit or dark fiber within this installed base is not reported in a consolidated format. However, it is important to note that much of the available dark fiber resides within both discrete inactive cables and in many fiber bundles and strands within cables that include active communications services. Thus, the available dark fiber inventory in large measure follows the overall fiber interconnectivity routes.

Dark Fiber Community, a fiber company membership organization, reports over 300 companies control these dark fiber resources in the U.S.10 Broadbandnow.com reports there are 925 fiber optic communications service providers within the U.S.11

During the dot-com bubble in the 1990s, a large number of telecommunications companies built optical fiber networks, each with the business plan of cornering the market in telecommunications by providing a network with sufficient capacity to take all existing and forecast traffic for the entire region served. This was based on the assumption that data traffic would continue to grow exponentially for the foreseeable future. What was not fully appreciated during the buildup is that Moore’s Law holds true with fiber optics. The amount of data coming out of an optical fiber is doubling every nine months. Thus, excluding the transmission equipment upgrades, the cost of transmitting a bit over an optical network may decrease by half every nine months. The availability of dense wavelength-division multiplexing (DWDM) and coarse wavelength division multiplexing (CWDM) is rapidly bringing down the cost of networking. This trend suggests that fiber networks could offer a substantial solution to manage the deluge of data that characterizes the smart and secure grid. Notably, the advanced multiplexing schemes further reduced the demand for fiber by increasing the capacity that could be placed on a single fiber by a factor of as much as 100. As a result, the wholesale price of data traffic collapsed. This led to the bankruptcy of many telecommunications providers and resulted in a glut of unused fiber in the last decade, much of which today remains an available resource. Figure 6 illustrates the distribution of available fiber in the continental U.S.

Our ORNL study team developed this composite map based on the base maps and topology of nearly 20 national networks accessed with the cooperation of major fiber-based broadband providers.

Because dark fiber is merely the medium on which the waves of light travel, it is technology neutral. Many applications and protocols can be transmitted over it, so the investment is protected long into the future, unconstrained by the obsolescence of any particular optical modulation scheme. Available dark fiber offers greater control, cost-savings, scalability and flexibility. Consider that a utility can upgrade service and schedule their own maintenance without waiting for the carrier, upgrade bandwidth and service level options without increased monthly costs, and keep pace with escalating data rates by upgrading from 1 Gb to 10 Gb or beyond simply by changing the optical cards in the equipment, not replacing the fiber “pipes.”

Leveraging the dark fiber base as a physical backbone for a more secure Industrial Internet will of course require augmentation with other communications components (e.g., wireless and/or “last mile fiber”) where necessary, to assure comprehensive and secure connectivity to all grid components.

11 Accessed on 24 July 2016 at: www.broadbandnow.com
3.1 New Threats and Vulnerabilities, New Options for Security

As the Internet of Things (IoT) architecture explodes, industry analysts estimate that some 5.4 billion devices will be connected by 2020.\textsuperscript{13} The opportunities for access to the general purpose Internet by nefarious actors will increase enormously with greater vulnerability to all those critical infrastructure components that share the net. It is imperative that our SCADA and ICS have protective measures consistent with the criticality of those assets. Based on our research and recent proof of concept program activities, we have new opportunities to leverage installed infrastructure, reduce overall costs, and implement a resilient architecture.

One example of adopting more resilient architecture has yielded impressive results, and defined a new business model that could be replicated across the nation. The EPB, also known as the Electric Power Board of Chattanooga, is an electricity distribution and telecommunications company owned by the city of Chattanooga, Tennessee. In 2010, EPB was the first company in the United States to offer 1 Gbit/s high-speed internet, over 200 times faster than the national average.

On October 15, 2015, Chattanooga implemented the world’s first community-wide 10-gig Internet service, available to all homes and businesses in EPB’s service area. Using a 100% fiber-optic communication network as its backbone, EPB has created a next-generation electric system that includes communication capabilities designed to reduce the impact of power outages, improve response time, and allow customers greater control of their electric power usage. This same fiber optic backbone allows EPB to offer high-speed Internet, TV, and phone service to business and residential customers in the service area. The EPB experience shows that a viable and sustainable business model can improve capital investments in security and contribute to mission assurance and resilience.

When EPB first turned on the fiber-optic network for Internet, customers were getting up to ten times the speed to which they were accustomed. Even those with lower-priced Internet tiers saw their speeds nearly double. The service now has reached up to 10 Gbit/s. Using fiber-optic technology is much cheaper, since the price of Internet access went down almost $300 per month when they started using the new technology. With more than 82,000 fiber optic customers, EPB telecommunications is expected to generate more than $130 million this year and pay more than $30 million into the electric system. More than 130 municipal utilities nationwide offer broadband services. An economic study by the University of Tennessee at Chattanooga said EPB’s fiber optics network in its first three years saved $130.5 million in power outages, boosted business energy efficiency by $234.5 million and spurred $461 million in new business investment.\textsuperscript{14}

The lessons learned from the EPB experience inform the essential cost and benefit analyses that


must be undertaken to validate the case as scalable and feasible. Of note in the Chattanooga effort is the fact that the DOE grant funds were matched by the approval of municipal bonds that created new debt for the City. However, the high value service offering that EPB was able to provide through the fiber implementation yielded unprecedented revenues enabling the early retirement of that debt.

Layered protective measures must safeguard communications between the operational control centers, power generation facilities, and major substations that remain exposed to a range of threats and hazards. A 2008 study performed by the National Infrastructure and Simulation Analysis Center (NISAC) for the Department of Homeland Security (DHS) ranked national energy assets (electric substations and generators). The study developed a consequence-based, national critical asset ranking methodology and associated list of most critical assets within the country based on the application of that methodology. A total of 350 electric assets represent the highest-consequence set of potential asset outages nationwide. The subset includes 65 generators and 285 substations. This highest priority items were identified by a detailed analysis of 35,719 assets, which include all substations and generators reported within the Federal Energy Regulatory Commission (FERC) Form 715 database.25

The NISAC study and the ongoing implementation of the Energy Sector Specific Plan27 prompt us to examine all relevant protective measures, among which we include evaluating the benefits of using available fiber networks to support secure communications with – and control of – critical substations and generator assets.

Overlaying these resources in consideration of fiber network connectivity illustrates the enormous potential of repositioning mission critical communications and control data onto the available, secure and nearly ubiquitous dark fiber networks.

3.2 Next Steps

We have seen that the cost for enhanced protective measures, whether the NERC-CIP physical security upgrades or ongoing cyber security measures, stress the rate-based utilities with unfunded mandates, ever more difficult to offset with ratepayers. We believe that the extraordinary outcomes of the EPB case demonstrate the potential for a new business model, one that enhances the security and resilience of the utility while generating revenue that enables the essential capitalization of equipment upgrades into the future.

The EPB lessons learned are that the concept of leveraging fiber optic networks for connectivity with residential and commercial customers can achieve objectives in both security and sustainability for the greater grid. Looking ahead, we foresee a convergence of infrastructure owners/operators, including electric, gas, water and wastewater utilities, onto available dark fiber to provide secure control, communications and structural health monitoring of their systems.

An additional benefit of such a repositioning of critical communications assets are the added countermeasures for the adverse effects of Electromagnetic Pulse (EMP), high energy RF (HERF), directed energy weapons (DEW), and the hazards of space weather (e.g., solar storms, coronal mass ejection) that threaten generation, transmission and delivery systems across the continent. Some of these threats are considered in the Joint Electromagnetic Pulse Resilience Study, developed by the DOE and the Electric Power Research Institute (EPRI), and released on 18 July 2016. The Study provides the foundation for the forthcoming DOE Electromagnetic Pulse Resilience Action Plan.

The Joint DOE-EPRI Strategy and pending DOE and industry action plans are intended to drive efforts to reduce EMP vulnerabilities and improve the response and recovery after EMP events, thus minimizing adverse impacts and improving grid resilience. Included among the priorities in the Plan is to “ensure the survivability of interoperable communications systems during and after an EMP”.28 A primary threat of EMP is damage to unshielded digital equipment, including SCADA systems, control systems, protection relays and systems, communications systems, smart meters, intelligent switches and other supporting infrastructure.27 As the concept of using fiber for enhanced security to mitigate the risks of the public Internet is evaluated, its benefits extending to EMP resilience should also be considered. Figure 9 illustrates the multiple uses a fiber backbone can provide to grid security and resilience.

25 National Infrastructure Simulation and Analysis Center, LA-CP-08-0547, Los Alamos National Laboratory, 25 April 2008, Los Alamos, NM.
Enhanced Protection of the Grid: Backbone and Last Mile

The separation of the Industrial Internet from the generic public or general purpose Internet is an objective of the Agile Fractal Grid initiative pursued as part of The SmartAmerica Challenge, a White House Presidential Innovation Fellow project with the goal to bring together research in Cyber-Physical Systems (CPS) and to combine testbeds, projects and activities from different sectors.²⁴

In summary:

- Utilities need to monitor, service, and maintain installed equipment via network connectivity; today that connectivity is via the increasingly vulnerable Internet, a target for nefarious criminal actors, information warfare, and subject to the deluge of vulnerabilities inherent in the unbridled growth of the Internet of Things.

- Regardless of the protocols used, modern gear is IP-addressable, incredibly useful for vendor maintenance, requiring the risks of network connectivity.

- In 2016, the available network is the general purpose Internet itself; it is rampant with malware and “reachable” by the bad actors and data access points are proliferating with the Internet of Things (IoT).

- We can provide the required secure network to interconnect the substations nationwide, using in large measure an installed, but currently unused fiber base.

- We can augment the activated “dark fiber” with other communications segments (e.g., wireless and/or “last mile fiber”) where necessary and in so doing we can achieve measurably enhanced grid security by having the components and equipment off the perilous “public internet” onto an Industrial Internet designed for security.

- A proof of concept program has yielded valuable cost and performance data, now we must dive deeper into the designs and operational concepts that are feasible, scalable and easily replicated, as well as examine alternative business models.

Therefore, we recommend the following critical actions:

- A program consisting of a feasibility study, alternative cost analyses, a proof of concept program plan, and a series of pilot projects – building on the lessons learned from the EPB case – should be expeditiously undertaken to ascertain scalable, repeatable and cost-effective solutions for security and resilience (from cyberattacks, EMP, HERF, DEW, and other threats).

- These efforts should be in partnership with rural cooperative energy utilities, tribal nations, and within large metropolitan areas to validate the operational concepts and

²⁴ Accessed on 21 July 2016 at http://smartamerica.org/about/
business models that will facilitate infrastructure protection and resilience.

Going forward, we must safeguard a considerable portion of the communications and control infrastructure by repositioning it off the exposed terrain of RF pathways, broadband wireless and microwave networks, and the increasingly vulnerable public Internet.

4. REFERENCES


Broadbandnow.com, accessed at http://broadbandnow.com/Fiber-Providers

Carnegie Mellon University, Securing Industrial Control Systems, ICS-CERT, Pittsburgh, PA, 2010


Energy Information Administration (EIA), Accessed on 22 July 2016 at https://www.eia.gov/electricity/


National Infrastructure Simulation and Analysis Center, LA-CP-08-0547, Los Alamos National Laboratory, 25 April 2006.


Personal Exchange with Hunter Newby, Dark Fiber Community on 21 July 2016 and accessed at www.darkfibercommunity.com


Smart America, accessed on 21 July 2016 at http://smartamerica.org/about/


prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf

