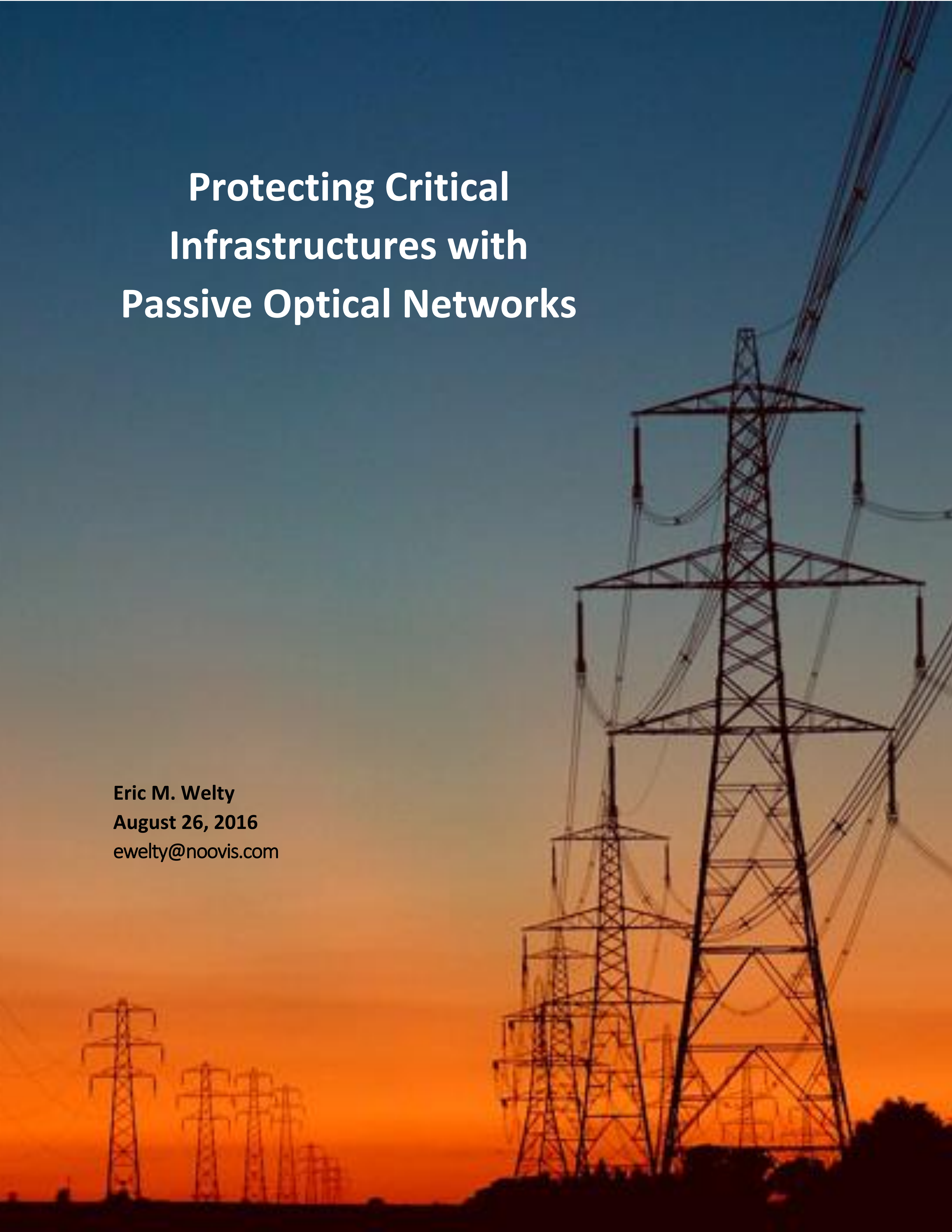


Protecting Critical Infrastructures with Passive Optical Networks

Eric M. Welty
August 26, 2016
ewelty@noovis.com

Acknowledgements

This paper would not have been possible without the support of many parties. In particular, I would like to acknowledge the following:

Network engineering team consulted on multiple occasions for cyber security issues.

Steve Heuber – Director of Engineering, Noovis
OMNI Technology Group

Fiber optic resources providing expert guidance on the design and implementation of PON infrastructures.

Mike Watts – V.P. Operations, Noovis
Mike Stedman – Director of Operations, Noovis

Electromagnetic Pulse and High Powered Microwave guidance.

Mikell Vibbert – Electronics Service
Travis Vibbert – Electronics Service

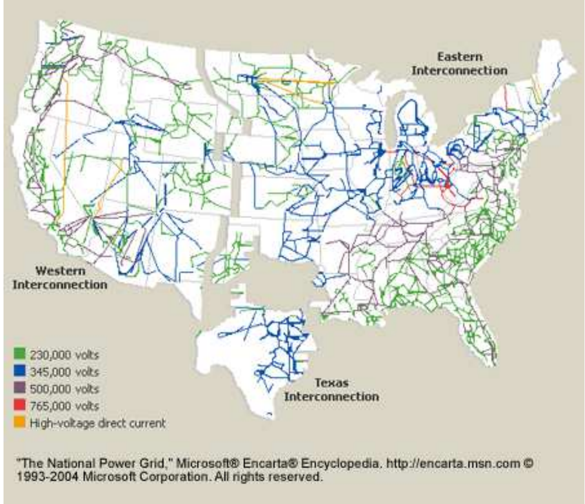
Table of contents

List of Figures

Abstract

Protection of the nation's power grid is a topic that has been discussed throughout all levels of America's government and industry. While there is no shortage of opinions on the subject matter, there is often a lack of consensus on the important "next steps" that we should take as a nation. Many believe this leaves us vulnerable to attack and ill-prepared to cope with the aftermath resulting from a prolonged and far reaching power outage.

Our nationwide infrastructure quite literally touches every electrical device across our country and as one would expect, possesses a vast number of vulnerabilities. The complexity of such a system is further encumbered by a bureaucratic quagmire that is slow to develop security standards and a largely self-policed industry that is even more reluctant to adopt them given the cost to do so. As "bottom-line" driven entities, one cannot expect a utility to simply take on the burden of the investment without being held accountable by shareholders.



"The National Power Grid," Microsoft® Encarta® Encyclopedia. http://encarta.msn.com © 1993-2004 Microsoft Corporation. All rights reserved.

Figure 1: National Power Grid

Aside from funding concerns, too often plans to protect the grid are bogged down in the legislative process due to both real and perceived privacy concerns for the utility companies. Even when reasonable recommendations are brought forth and approved within the industry it is up to the regional authorities and individual utilities to implement the changes.

A solution that removes complexity from our systems, increases protection of communications networks, avoids privacy matters altogether, and provides all these benefits at a reduced cost compared to current technologies may seem unrealistic but it is not, the solution is Passive Optical Networking (PON).

PON based systems reduce the number of managed devices, namely access switches, within a Local Area Network (LAN) and provide an entirely passive and encrypted optical pathway for data to support typical end user devices as well as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks thus providing an inherently more secure management of the nation's grid. Moreover, the removal of the extraneous electronics and their copper-based infrastructures allows PON systems to be both deployed and maintained at a ***lower*** cost than traditional switched Ethernet networks.

Grid(lock)

The nation’s power grid is divided into three major sectors: Eastern, Western and Texas. According to the Energy Information Administration (EIA), these interconnected systems require more than 7,200 power plants to support 2,000 utilities and over 300,000 miles of transmission and distribution lines[i].

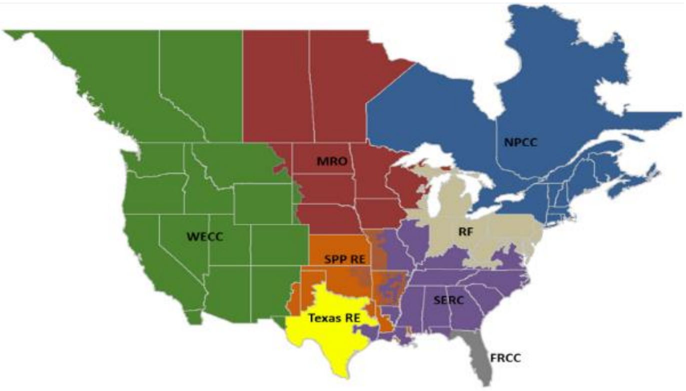


Figure 2: NERC Regions

Federal regulation for the reliability of the Bulk Electric System (BES) is administered by the Federal Energy Regulatory Commission (FERC) which uses the North American Electric Reliability Corporation (NERC) to create and enforce standards that ensure the system’s reliability[ii]. The NERC delegates the enforcement of these standards across eight regions that cover the U.S. as well as Canada.

The Critical Infrastructure Protection (CIP) v5 standards that have been developed by NERC are meant to lessen our exposure to cyber related threats and provide “appropriate protection against compromises that could lead to misoperation or instability in the BES”[iii]. Where some may feel these standards fall short, recommendations have been made to have the CIP standards largely follow the existing National Institute of Standards and Technology (NIST) guidelines. This would offer some comfort were it not astutely pointed out by former NSA Chief Scientist, George Cotter, that the CIP standards go on to actually define certain areas that are “exempt from classification as cyber assets”[iv] thus rendering them immune to the standards. Absent standards to follow, each individual utility is left to build, manage, and secure their communications networks as they see fit.

Chilling as it may seem, protecting the nation’s power grid can hardly be considered a top priority in an industry constantly needing to update an aged infrastructure while working to integrate it with modern renewable energy resources. The U.S. Energy Information Administration’s website lists current challenges for the power grid; at the bottom of the list, seemingly added as an afterthought, the last bullet item is ***“Protecting the grid from physical and cybersecurity attacks”***[v]

This is not to say that the organization doesn’t take cyber threats seriously. In fact, the EIA released the “Roadmap to Achieve Energy Delivery Systems Cybersecurity” in 2011. Intended to improve cybersecurity across the energy sector, this 70+ page report outlines a framework to increase the survivability of our grid, the Vision of which is “By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.”[vi] While this Roadmap is comprehensive, indeed demonstrating the collaboration of over 80 stakeholders, it recognizes and, to its credit, documents the multitude of barriers it faces in achieving its Strategic Framework.

In perhaps a more conservative if not pragmatic approach to the subject, the Foundation for Resilient Societies produced its own report on the current state of our nation’s energy systems in January of 2016. In what most reasonable people would consider a scathing review of the vulnerabilities within our energy system, the report clearly states that it’s not a matter of ***IF*** but rather ***WHEN*** a cyber terrorist will attack “The Real Targets – Critical High Impact National Security, Industrial, Social and Urban Infrastructure”[vii].

Regardless of where one stands on the issues, it is apparent that vulnerabilities do exist. What is needed is a solution that can mitigate existing risks to cyber threats at a reduced cost over current efforts. By driving a net savings to the cost side of the equation, one would hope that we could accelerate change across the industry as utilities would actually improve their bottom lines by implementing a more secure network. Surely, such an evolution would garner support from all stakeholders and allow us to align the priorities of both the public and private sectors.

Principles

Yesterday's Network

Most large enterprises support remote offices and facilities from one or two main locations. This provides them a lean, centrally managed yet redundant architecture that supports all of their users in a uniform manner.

A typical communications network, as depicted in Figure 3, connects an Enterprise's services to its remote offices and facilities by traversing a Carrier's Wide Area Network (WAN) and connecting via a local router and firewall at the client site. These services are then passed to distribution switches where any site-specific local requirements i.e., servers, controllers, local back-ups, etc. are converged onto the Local Area Network (LAN). All services then pass further downstream to access switches before they are handed off to end points such as computers, phones, cameras or SCADA and ICS devices. From the datacenter to these access switches all connections are generally performed with singlemode or multimode fiber optic cables.

Access switches provide the "horizontal" connection to each user station with copper cabling terminated on faceplates. The final connection to the end user device (computer, phone, camera, SCADA/ICS component) is then made with a copper patch cord.

This architecture has additional inherent weaknesses that, over the course of decades, have morphed into "network requirements" and now impact not just their networks but the very buildings they occupy. Specifically, the 90-meter distance limitation of copper has driven the unfortunate standard of placing multiple communications closets throughout a facility in order to house access switches close enough to end user devices. These communication's closet requirements also force network teams to fully secure these spaces and environmentally condition them with power and cooling systems – all at a cost.

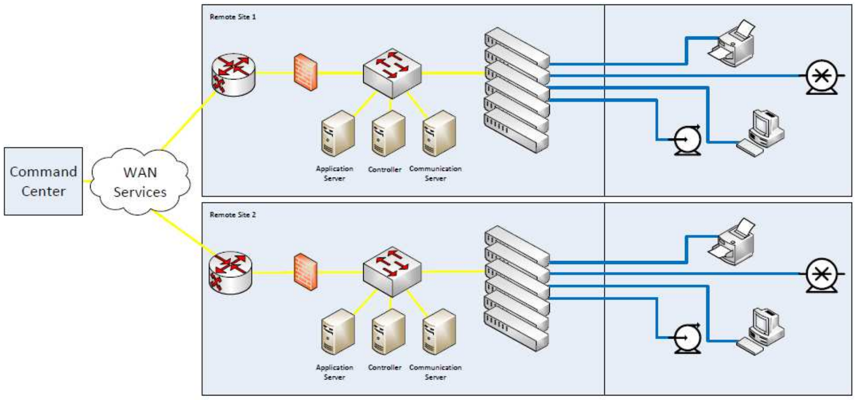


Figure 3: Traditional switched Ethernet architecture

True Network Modernization

The PON Solution provides a fully converged voice, data and video network infrastructure that is based on proven Commercial Off The Shelf (COTS) technology. This standards-based technology does not require active electronics between the data center and the end user thereby providing an entirely passive network infrastructure that is both reliable and expandable.

As detailed in Figure 4, an Optical Line Terminal (OLT) will be located in the campus/facility data center and distribute the client's services across the network. Passive fiber optic splitters are strategically placed to distribute the services to up to 32 users per PON interface **(in place of access switches)**. Encrypted connectivity is extended across the "horizontal" with singlemode fibers connecting to each workstation where an Optical Network Terminal (ONT) is placed to perform the optical to electronic conversion and provides Ethernet connectivity for devices.

This architecture essentially provides an encrypted connection to any IP based end user device (phone, computer, access point, SCADA component, etc.) from its network head-end up to 12 miles away without the need for signal regeneration or additional network switches.

There are two key parts to this paradigm shift from the legacy architecture to the modern option. First, the multiple access switches typically deployed throughout a facility are collapsed back into a single Optical Line Terminal and optical splitters perform their connectivity function in the field where "riser" and "horizontal" infrastructures meet. The OLTs can provide all the same Layer 2 switching functions of your typical switch but it is now done at the head end. Second, with optical splitters now available in the field we can extend fiber all the way to the end user devices and eliminate altogether the previous copper distance limitation. Also, removing these switches provides a meaningful benefit to Capital and Operating budgets as the secure and environmentally conditioned closets are no longer needed but rather just a few square feet of space to house an optical splitter.

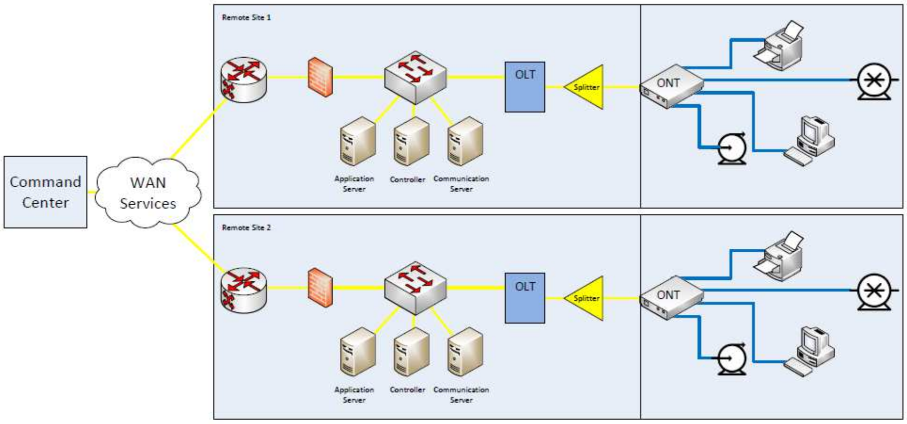


Figure 4: PON System Architecture

Key PON Benefits

Due to their efficiencies, these PON systems are seeing adoption across all industries in both the public and private sectors. The PON design allows for a single centrally managed datacenter to support all LAN services throughout the campus/building/facility on a resilient system. There are several inherent benefits of this design:

- Centrally Managed Network
  - Access switches are removed with this Layer2 responsibility collapsed into a single source that provides encrypted connectivity to end points
  - No need to replicate the head end switching and routing throughout a facility
    - Telco closets are now passive
    - Saves on power, space, CapEx and OpEx
    - No additional redundant power and network connectivity required
    - Less active switches allow for faster Disaster Recovery times
- Flat network architecture
  - IP services for all end points (voice, data, RF video, video surveillance, access controls, wireless access points, etc.) can all traverse the PON system
- Carrier grade reliability
  - Supports “five-nines” (99.999) of availability
  - “Six-nines” (99.9999) is available with redundant head ends
- Any existing singlemode fiber plant can be leveraged
  - Over 12-mile range for network without signal regeneration
- Horizontal cabling is minimized
  - A single fiber can provide up to (8) Ethernet ports and multiple VLANs of connectivity

While these benefits may be impressive, our critical infrastructures require putting a heavy emphasis on security. This was a critical part of the Sandia National Labs evaluation of this technology when it conducted its own study in 2009. Below is an excerpt from their full evaluation - It is also worth mentioning that as a result of their evaluation, Sandia fully adopted the technology across its campus in Albuquerque, NM, implementing a PON system in over 265 buildings to support 13,000 users.

> ***Comparison to Current Network Technology***
>
> *In some ways the final security topic can be summed up with the question “Is it any worse than what we have now?” Since the current technology is Ethernet over copper, and/or Ethernet over fiber, it has been determined that we have no indications that GPON is worse than the current technology. In fact, the architecture adds encryption, increased manageability, endpoint registration, and fiber optics to increase the overall security position.*
>
> *- Sandia National Labs GPON Evaluation, 2009*

Combating the Cyber Attack

According to Verizon's 2016 Data Breach Investigation Report (DBIR), this year's incidents "affect[ed] organizations in 82 countries across a myriad of industries"[viii].

Computer driven by the very definition, cyber-attacks aim the perpetrators resources at the active components of a network. In some instances, the hackers may be targeting the distribution or access layers of a network by attempting to breach existing firewalls, routers and switches. Other times their resources are focused on exploiting the actual ICS or SCADA components directly.

All of the nation's power utilities are supporting their sophisticated networks with essentially the same switched Ethernet technology that supports virtually every other industry. These Local Area Networks (LAN's) have seen changes, upgrades and improvements for decades since personal computers began their proliferation in the 1980's. While regular improvements have been made to network throughput and security parameters, what has been missed in this accepted status quo of planned obsolescence is a wholesale improvement and upgrade to the way these LANs are designed and deployed.

It is also worth noting that having remained largely unchanged for so long, hackers have developed a long list of well-known and readily exploitable vulnerabilities. Worse yet, software companies regularly go to market with products containing "known vulnerabilities" to meet development deadlines. Anyone wishing to challenge this argument need only ask why software patches and updates are now a matter of routine maintenance. This "good enough for now" approach to software development has created a window of opportunity for bad actors to exploit a published vulnerability prior to companies implementing the lagging "bug fixes".

Verizon's 2016 DBIR looked to not only review how hackers were exploiting networks but conversely how well enterprises went about applying fixes. The resulting data indicates that "Half of all exploitations happen between 10 and 100 days after the vulnerability is published, with the median around 30 days."[ix] Leaving a critical network exposed for a full month surely fails reasonable standards for most stakeholders.

Adding to the anxiety resulting from attempting to secure something that is inherently unsecure is the fact that the ICS and SCADA systems that are used far and wide to maintain and manage industrial control devices are manufactured by a very limited number of sources. Assuming that these entities do everything within their power to lockdown their software and prevent intrusion we are still left with the fact that limited products mean there is more time for bad actors to focus their attention on breaching a software bug that may provide them access to multiple networks worldwide. Worse yet, nation states and rogue hacktivists with malicious intent have ready access to these systems with minimal investment.

Today's Information Technology organizations are expected to maintain networks supporting a wide array of requirements. Today's "typical" network engineer is expected to understand routing and switching, troubleshoot voice gateway's, maintain audio/visual equipment, stay current with rapid wireless advancements and integrate everything across aging systems. At the same time, these IT teams are overwhelmed with shrinking budgets, untrained personnel and changing priorities all while being tasked to manage more and more complex systems.

These conditions directly contribute to common network access upgrades/patches being overlooked. Access infrastructure not patched correctly can provide numerous attack vectors. Too often cyber defenses leave us adding software and hardware to our systems with the intention of making things more secure. While these are well meaning efforts, what gets lost in the fray is the notion that ***the less complex a network is, the more secure it is likely to be.***

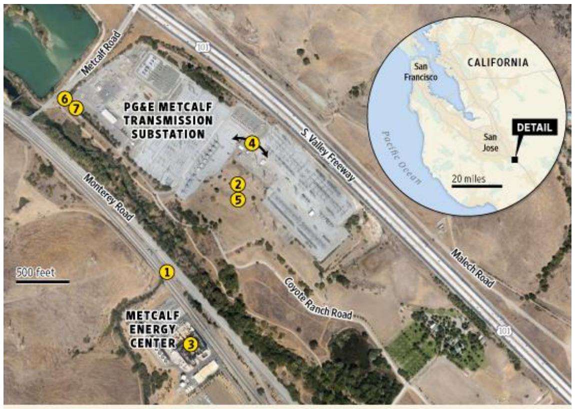
The implementation of PON technology allows organizations to utilize advancements that elevate the security posture in an IT Enterprise while radically simplifying their access layer as a whole. PON technology reduces the quantity of access switches that require management, regular patching and security scans throughout their network. PON systems, based on widely accepted ITU standards, centralize the access layer at the existing datacenter. From here all communications traffic being passed across the access layer down to end devices is protected by AES128-bit encryption. This encrypted transport creates an enclave that significantly increases the complexity requirement for exploits and mitigates the threat of (outsider and insider) man-in-the-middle (MitM) attacks. Furthermore, by removing the need for copper-based architectures the many advantages of fiber optics, previously only realized in wide area networks are now available in the campus and local area systems as well. In the end, we are left with a network enterprise that is simpler and as a result, more secure.

Physical Intrusion Detection

Traditionally Inside and Outside Plant Infrastructures were secured via Protected Distribution Systems (PDS). These systems often called for entire outside plant (OSP) pathways to be encased in concrete and in-building networks to be secured in conduit end to end from a datacenter to the end user - both expensive and extremely inefficient options. Moreover, as these networks may only be considered “tamper resistant” regular inspections, sometimes multiple times a day, are required to determine if these conduits and raceways have been tampered with. Should something be found we’d only know *after the fact*. Unfortunately, not knowing a physical attack has happened until it’s too late isn’t a mere theoretical discussion point. In fact, it became all too real when the Metcalf substation was attacked in San Jose in 2013.

The Pacific Gas and Electric (PG&E) facility was the victim of a two stage attack. First a manhole was accessed outside of the Metcalf Energy Center where its communications cables were cut. A full twenty-four minutes later snipers opened fire on the facility, strategically attacking the cooling systems. Within fifteen minutes’ transformers began crashing.

Facing a potential power blackout, PG&E rerouted existing resources and ramped up others to mitigate the loss. It took 27 days to repair the damage and three years later still no arrests have been made.



Shots in the Dark

A look at the April 16 attack on PG&E’s Metcalf Transmission Substation

1	2	3	4	5	6	7
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can’t enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff’s Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

Figure 5: PG&E Attack Timeline

Advancements in physical intrusion detection have provided a much more cost effective and inherently more secure methodology. Today manholes and their fiber optic cables can be monitored in real-time to determine if an intrusion is being attempted. In fact, so sensitive are these monitoring capabilities that “false positives” are common place when new systems are deployed until they are given ample time to baseline normal conditions for a site. Designed properly, Alarmed Zones are designated which allow network security teams to pinpoint where alarms are occurring and address whether they may be due to routine maintenance or are the result of a malicious attack. Upon determining the latter, protected circuits could be shut off if it was believed that an intruder was actually attempting to compromise the data rather than just cut the cables carrying the circuit.

These modernized alarmed PDS's are approved for use and widely accepted by the nation's DoD space. Considering the DoD's mission, it could easily be argued it is charged with maintaining some of the most critical networks in any operational environment and does not have the luxury of choosing security systems that are less than 100% dependable.

EMP and HPM Protection

Electromagnetic Pulse (EMP) and High Powered Microwave (HPM) attacks are very real threats to our nation's infrastructure and other critical communications networks. During the cold war era the threat was contained to a High-Altitude EMP (HEMP) attack that resulted from the detonation of a nuclear warhead miles up in our atmosphere. Ignoring the fallout from this scenario (if that's possible) the resulting energy wave alone would extend to the horizon in all directions overloading and essentially rendering useless any sensitive electronics in its path. Modern advances have now provided countries the ability to produce the same EMP effects without using nuclear weapons. This technology is known as High Powered Microwave (HPM) and by its very nature it can be used in a much more targeted fashion against specific locations.

In either case, regardless of which type of attack might occur, protecting a system as vast as our nation's power grid from a weapon that travels at the speed of light and can use the miles of transmission lines as direct links into every substation and home is a costly endeavor. Many consider deterrence to be the best defense.

Many see this as the new cold war in that a nation capable of launching an EMP/HPM attack would not do so for the same deterrence factors that kept nations in check when considering the nuclear option. Basically, if a country uses this technology then it can expect a reciprocal attack leaving them equally damaged. The risk many believe is from the rogue nation states like North Korea that may see the launching of this type of attack against the United States as an advantage for them as we would clearly see more devastation to our Grid than they would.

Hardening Existing Networks

Hardening a traditional network to protect against such attacks must be done in several stages.

- First, the datacenter must be protected by isolating all connections that penetrate its walls and then shielding the walls themselves
- Second, telco closets on each floor house sensitive electronics just as the datacenter. As such they must be protected in the same costly manner.
- Third, short of shielding the entire building, all horizontal cabling and user stations are vulnerable to EMP/HPM attacks. This must be accepted and addressed in the Disaster Recovery (DR) plan.
- Should an EMP attack occur, a Disaster Recovery plan must be executed where any damaged electronic components must be replaced and provisioned. This may require a full network swap of all layer 2 devices to include switches if they cannot be recovered following an attack.

Operating in this manner, even if the expense was incurred to protect the datacenter and telco closets throughout a building/complex the network will be lost if exposed to EMP/HPM due to the inherent vulnerability of a traditional network's "horizontal" copper infrastructure. Disaster recovery times could be measured in days or even weeks depending on the extent of the damage and lead times to replace critical components.

Defending Against the EMP/HPM Threat

Due to their low cost, high bandwidth and overall flexible nature, PON systems have been used by our nation's military and the Intelligence Community to support every possible network classification for years. Leveraging this technology's "fiber rich" attributes is the logical next step towards protecting our nation's most critical networks from known threats such as EMP/HPM attacks.

Building on the network characteristics outlined previously we can see where the PON system provides its advantage.

- The datacenter must be protected by isolating all connections that penetrate its walls and then shielding the walls themselves
    - This must remain a basic tenet for building an EMP/HPM resistant system. Done correctly, centralizing network management and applying appropriate levels of redundancy, the cost can be minimized.
- Telco closets no longer require protection as access switches and their related power supplies and HVAC systems are no longer required
- Singlemode fiber replaces the copper cabling in the "horizontal" thus removing the coupling effect that stems from pulling RF signals onto electronics at either end
- Disaster recovery plans only need to focus on the critical user stations (phones, computers, etc.) as an ONT can be replaced in minutes and will automatically provision itself based on the last known configuration for each user station – total lapse time to have a user station back on line is estimated to be less than 5 minutes.
- Additional protection can be supported by hardening the ONT itself. If done correctly there would essentially be **NO** network downtime

It is reasonable to assume that a PON system provides an inherently more resilient platform for supporting critical networks. This fiber-based system can reduce network downtime to a fraction of what would typically be expected and can be implemented at a dramatically lower cost than traditional networks.

Common Misconceptions

"We use shielded copper cables so we are not susceptible to EMP."

Even when shielded cables are used more often than not they are either **NOT** terminated properly or the grounding system is faulty. It only takes a single faulty copper connection to render the network vulnerable to attack. Moreover, the singlemode fiber optic cable used in PON systems can be procured and installed at a *fraction* of the cost of shielded copper cable.

"We use multimode fiber in our 'horizontal' so we have the same benefits as a PON system"

Multimode fiber still requires electronics at each end, a switch in the IDF and a media converter at the user station, that must be protected.

Microgrid Adoption

Advancements in renewable energy have spurred investment in the research, development and deployment of Microgrids. Largely driven by the need to provide improved resiliency in supplying energy for its users, these independent energy systems require a protected infrastructure by default. While a full discussion of the topic goes beyond the scope of this paper, these same benefits apply to micro grid initiatives.

In practice, it should be expected that implementing PON systems into the standards for microgrids should be a relatively simple endeavor compared to the national grid, given that the largest hurdle, getting complete buy-in from every stakeholder involved, can now happen on a much smaller scale. Moreover, advocates for microgrid adoption are already comfortable with finding novel approaches to solve problems. A modernized network deployed at a reduced cost that requires less energy to run fits the mission for microgrids without equivocation.

A Way Forward

This paper highlights the clear benefits of using Passive Optical Network's to support Campus and Local Area Network requirements for critical infrastructures. The main goal being to find common ground between the public/private sectors that may streamline and if possible fast-track improved security standards for our nation's energy grid.

With budget constraints being an omnipresent hurdle across all industries public and private, it stands that adopting a technology that reduces Capital and Operational costs while at the same time increasing the security of critical communications networks cannot be ignored.

Specifically, a PON, designed and implemented correctly can be done at a lower cost than a conventional switched Ethernet system that relies on extraneous switches, environmentally conditioned spaces and copper cabling. Multiple cost studies have been done to compare the two architectures that typically tout a 50% savings in both capital and operating expenses when PON is chosen for the implementation.

Seeking to better understand the potential savings, IBM performed its own Total Cost of Ownership (TCO) study to compare a legacy copper network to a PON implementation. The scope of the network being used in the exercise resembled the typical small office space of about 100 cubicles and eight separate offices. In all, the network supported 1,920 Ethernet ports inclusive of the Wireless Access Points (WAPs). The results were "On average, the approximate Total Cost of Ownership for using Passive Optical LAN technology over five years may be up to 47 percent less than traditional copper LAN networks"[x].

Moreover, after conducting its own evaluation and deciding to move ahead with PON technology across its Albuquerque, NM campus, Sandia National Labs estimates that its energy savings will be about 65% of what is currently being consumed and that they will achieve a $20M cost savings over five years[xi]. These are dramatic numbers indeed and surely warrant the very serious consideration for this technology to be adopted to support our critical national power grid infrastructure.

References

[i] Energy In Brief, U.S. Energy Information Administration, http://www.eia.gov/energy_in_brief/article/power_grid.cfm

[ii] About NERC, North American Electric Reliability Corporation, http://www.nerc.com/AboutNERC/Pages/default.aspx

[iii] Cyber Security — BES Cyber System Categorization http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&jurisdiction=null

[iv]George R. Cotter, *Security in the North American Grid – A Nation at Risk* (2015), 9

[v] Energy In Brief, U.S. Energy Information Administration, http://www.eia.gov/energy_in_brief/article/power_grid.cfm

[vi] Energy Sector Control Systems Working Group*, Roadmap to Achieve Energy Delivery Systems Cybersecurity*, 2011, 2

[vii] Thomas S. Popik, Joseph M. Weiss and George R. Cotter, *Exercise of FERC Authority for Cybersecurity of the North American Electric Grid*, 2016, 14

[viii] Verizon, *2016 Data Breach Investigations Report*, 2016, 3

[ix] Verizon, *2016 Data Breach Investigations Report*, 2016, 14

[x] Nikos Anerousis, R. Todd Christner, Luis Farrolas, Yaoping Ruan, John Short, Mudhakar Srivatsa, Jin Xiao, *IBM: Smarter Networks with Passive Optical LANs*, 2014, 10

[xi] John Holden, The Green Room report on Tellabs Passive Optical LAN using GPON technology at the Department of Energy Sandia, NM national laboratory, https://www.youtube.com/watch?v=G1UyylAlfSM, 2013