SECURING OPERATIONAL TECHNOLOGY **IN THE ENERGY INDUSTRY**

FOUR KEY CONSIDERATIONS

BAYSHORE

Executive Summary

A fourth industrial revolution is underway, driven by the interconnection of physical infrastructure and the systems that control it. The Industrial Internet of Things (IIoT), or just the Industrial Internet, is changing how products and services are designed, manufactured, sold, delivered, and operated.

This interconnection of critical industrial infrastructure is unlocking vast potential in business efficiency, transformation, and innovation, none more so than in the energy industry. But this interconnection comes with a cost, and that cost is the need for protection against cyber threats. Our energy grid is exposed. From everyday hackers to state-sponsored warfare, the electricity infrastructure has little defense against a sustained cyber-attack.

In this whitepaper, you'll learn about the current energy grid situation and its vulnerability to digital attacks, the challenges of reducing weaknesses, and how new technologies can protect the grid from catastrophic failure caused by deliberate attack. This whitepaper will also examine general trends in the convergence of IT and OT, while introducing you to four key considerations when protecting industrial assets against cyber threats. Lastly, it introduces Bayshore's Industrial Cyber Protection Platform, which stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet.

Anatomy of an Attack

2:14 PM

It started out like any other day at Consolidated Power. Just a run-of-the-mill Tuesday. Nothing out of the ordinary. Everything running as it should. Joe dropped the clipboard on the desk and sat down at his terminal. He logged in to check out the status of the grid and noticed an anomaly—a spike in power output from several of the generators. He furrowed his brow and tried to track it down but it didn't seem to originate from anywhere. It just...happened. He wrote himself a note, grabbed his lunch, and headed to the breakroom.

4:26 PM

Joe was at his desk again. He squeezed the bridge of his nose and dug into the grid anomaly. The power spike he had found was still bothering him. And right before his eyes, it spiked again. This time for a little longer. Something didn't feel right. He took a screenshot and sent it to the printer.

KEEP IN MIND

The electrical grid is getting smarter and more connected. But along with this growing sophistication and other upgrades comes inherent cyber vulnerabilities. In fact, threats from malicious cyber-attacks to the North American electric grid continue to grow in frequency and intelligence. In 2015, U.S. electrical providers faced one attack every four days .

4:38 PM

He was staring at the printout when he received an email with an ominous message: *Unusual power spikes. You know what's up?* It was from Bill in Operations. If Bill doesn't know what's going on, does anyone? Joe wondered.

4:39 PM

Spike number three. Longer. Sustained.

An idea started to make its way from the back of Joe's mind. Something unthinkable. Something preposterous.

Joe looked once more at the printout and then back at the screen where the spike subsided and the readings returned to normal. He clicked on the respond button to Bill's email and put his fingers on the keyboard. He didn't know what, exactly, to type. It was just a word. A crazy word. A word that everyone had dismissed over the years. But it haunted him now.

He typed one word:

Cyberattack?

4:45 PM

Bill hadn't responded. Joe's anxiety was growing minute by minute. He couldn't take his eyes off his screen, waiting for the next spike. Will the next one bring us down? Shut us down? He wondered.

And then the alarms started.

The Ripple Effect

The scary part about the attack on Consolidated Power isn't that cyber-attacks could potentially bring down part of the system, it's the interconnectedness. Grids, generators, brokers—they are all intertwined. An attack on a single company like Consolidated Power could open doorways to other power companies and resources, ultimately bringing down massive portions of the energy infrastructure. According to the Idaho National Laboratory, in their 2016 report:

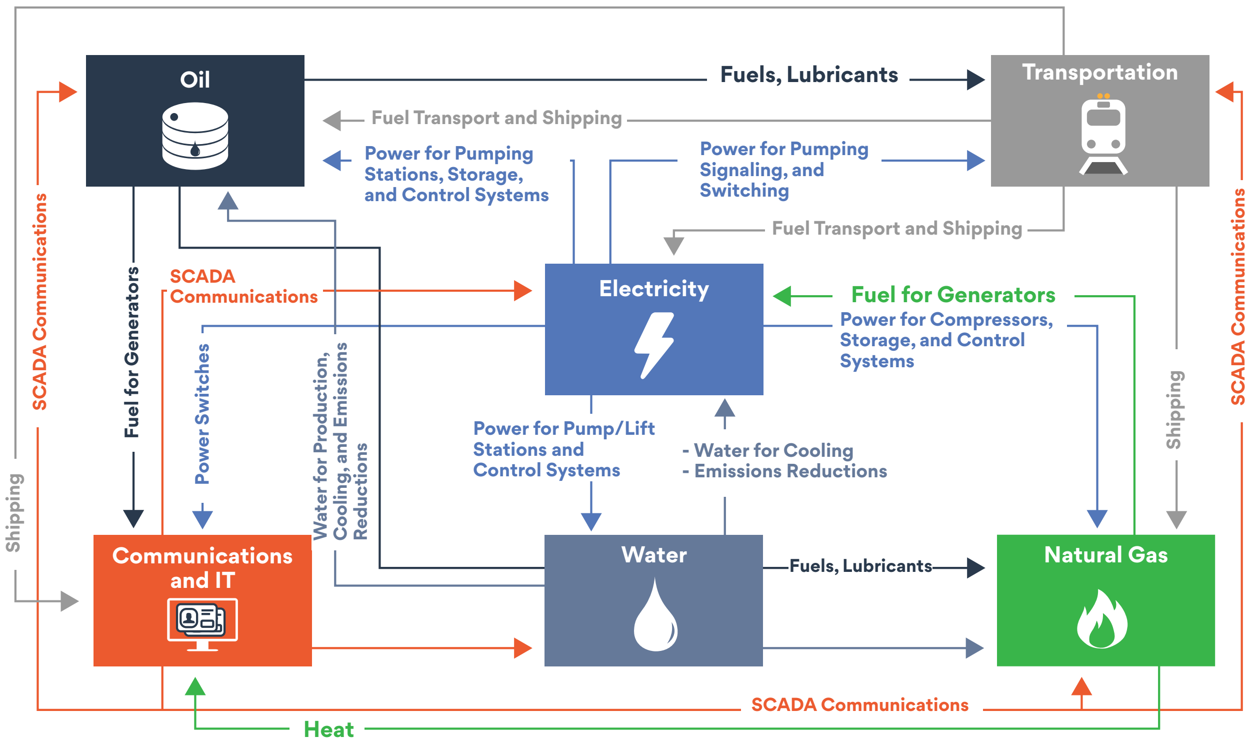
> *Components on which utilities rely to manage daily operations were originally designed for grid efficiency, with vertically integrated utilities utilizing local generation to serve local load, and for peer utility support when needed. The electric system of today relies on an advanced transmission system, market operations, independent power producers, system operators, as well as the traditional vertically integrated utilities to ensure overall system reliability. The engineering of the power system and how the system is operated has been a very dynamic environment and in many of the new automation and control elements the potential of cyber threats was unrecognized at the time the systems were adopted. As utilities have upgraded ICS and electric grid technology to meet present-day needs, the practicality of digital automation and data transfer has become necessary. A variety of vulnerabilities have emerged, particularly related to greater accessibility because of advanced communication means and Internet connectivity.*

CATASTROPHIC FINANCIAL IMPACT

It is estimated, in a joint report by Lloyd's and the University of Cambridge's Centre for Risk Studies, that economic impacts resulting from a power grid cyber-attack could include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business, and disruption to the supply chain. The total impact to the US economy is estimated at $243bn, rising to more than $1trn in the most extreme version of the scenario.

Even more frightening than just the interconnectedness of the constituents within the electricity infrastructure is that an attack on the grid does not just affect the Power industry. It has far ranging impacts into every facet of society. In our scenario, Consolidated Power would, of course, lose millions of dollars in revenue and be forced to replace expensive equipment. But what about everyone without power? People would not be able to get to work, resulting in loss of productivity. Trade and shipping ports would be at a standstill without power. Commerce would come to a halt. As predicted, the loss to the economy could easily run into the billions of dollars from a single, successful cyber-attack on a power grid resource like Consolidated Power. The impact on healthcare, communications, fire and safety are almost unimaginable. Just look at the interconnectedness of critical infrastructure below. Taking down any one component, like the electric grid, would result in a catastrophic outage.

CRITICAL INFRASTRUCTURE INTERDEPENDENCIES


Oil
Fuels, Lubricants
Transportation
Fuel Transport and Shipping
Power for Pumping Stations, Storage, and Control Systems
Power for Pumping Signaling, and Switching
Fuel Transport and Shipping
SCADA Communications
SCADA Communications
Fuel for Generators
SCADA Communications
Electricity
Fuel for Generators
Power for Compressors, Storage, and Control Systems
Power Switches
Water for Production, Cooling, and Emissions Reductions
Shipping
Shipping
Power for Pump/Lift Stations and Control Systems
- Water for Cooling
- Emissions Reductions
Communications and IT
Water
Fuels, Lubricants
Natural Gas
SCADA Communications
Heat

In their report, Lloyd's and the University of Cambridge imagine three scenarios (S1, S2, and X1) like our Consolidated Power story, of varying severity related to how long the power would be out. The table below summarizes the loss of revenue (in $BN) to different economic sectors in the United States:

Cost of Electricity Interruption ($bn)	S1	S2	x1
Wholesale and Retail Trade	$14.35	$30.68	$52.51
Public Sector	$8.53	$18.24	$31.22
Households	$7.54	$16.12	$27.60
Manufacturing	$6.41	$13.71	$23.46
Accommodation and Food Services	$5.64	$12.05	$20.62
Administrative Support Services	$4.65	$9.95	$17.02
Professional, Scientific and Technical Services	$4.19	$8.96	$15.34
Real Estate	$3.62	$7.74	$13.24
Inforamtion and Communication	$1.86	$3.97	$6.80
Finance and Insurance	$1.77	$3.78	$6.47
Transport	$0.63	$1.34	$2.29
Agriculture	$0.62	$1.32	$2.26
Electricity and Gas Supply	$0.45	$0.96	$1.65
Construction	$0.37	$0.78	$1.34
Mining	$0.20	$0.44	$0.75
Water Supply, Waste Management	$0.07	$0.15	$0.26
TOTAL	$60.90	$130.19	$222.83

Post-Mortem

So, what happened with Consolidated Power? How did the hackers get into the subsystems that control power distribution and storage? How did they force the release of power and spike the system, ultimately destroying critical components and infrastructure?

It was most likely a combination of factors—reverse engineering safety systems and grid operation, the installation of malware through social hacking and brute-force intrusion. Regardless of how it happened, it was clear that Consolidated Power wasn't ready for the attack. In fact, it's quite possible that the attack lay dormant for months or even years as the hackers prepared for the day of deliverance.

Accepting that the Improbable Could Happen

You might be thinking, "Yeah, this is a lot of speculation. Nothing like this could really happen." On the contrary, it already has in some ways. Consider the Havex campaign. "This cyber-attack employed spam email to distribute a Remote Access Trojan (RAT) tool to targets, using watering hole attacks deployed from compromised ICS/supervisory control and data acquisition (SCADA) vendor websites.

Since around 2013 a group known as 'Dragonfly' and 'Energetic Bear', thought to be a state-sponsored organization, is responsible for Havex and targets energy sector companies (and other sectors) in the U.S. among other countries. By targeting electric grid operators, equipment vendors, and relevant software providers, the attackers can spread malware that "instructs infected machines to download and execute additional components." Though no reports have yet emerged confirming exploit or damage of Havex-infected systems, the malware's complexity and range of access thus far could produce future effects if not properly mitigated."

FROM IMAGINATION TO REALITY

In a similar scenario described by a major insurance company, it's possible that a scenario involving malware could "covertly and systematically disable safety systems which would usually protect the generators from desynchronization events. The malware sends out control signals which opens and closes the generator's rotating circuit breakers in quick succession, using the inertia of the generator itself to force the phase angle between supply and load out of sync. The impacted generators would begin to catch fire and pour smoke; some even being partially destroyed as the engine blows apart."

So why is the U.S. Energy Grid infrastructure under attack? There are lots of proposed reasons why an attack like that depicted on Consolidated Power would happen in the first place. Here are just a few:

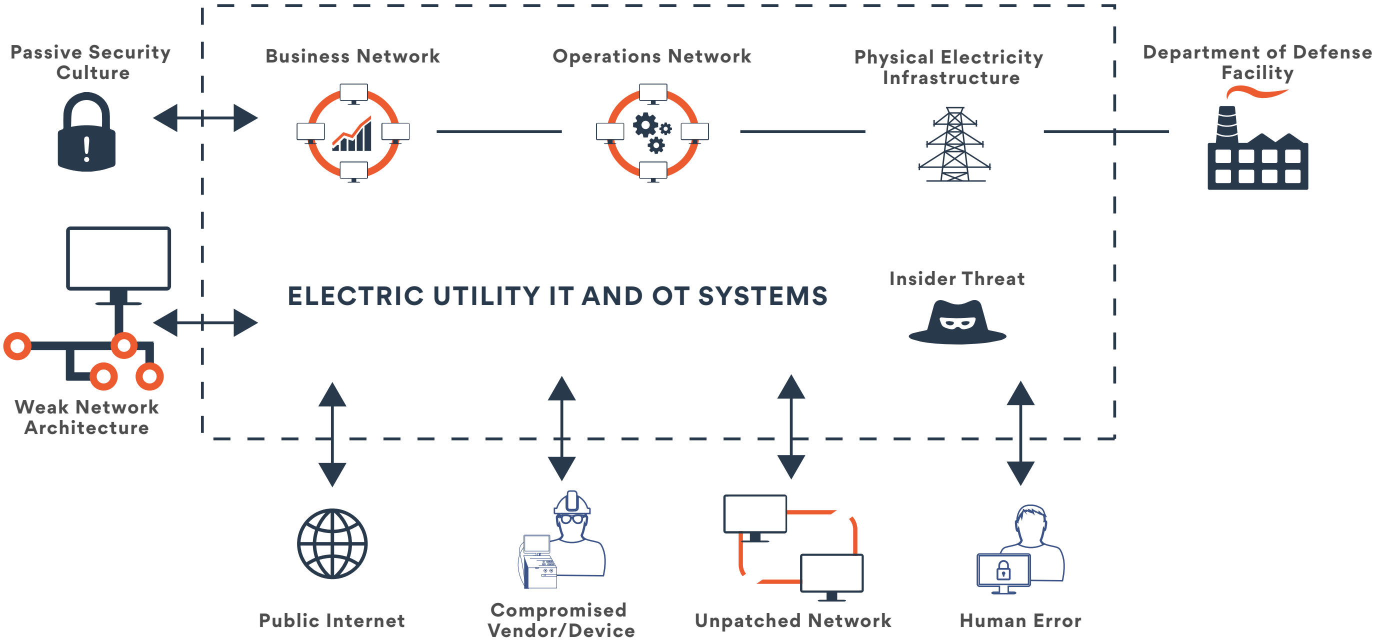
- **State-sponsored terrorism**—countries that are enemies of the United States could attack the power grid to enforce their will and cripple our economy
- **Hacktivism**—hacker groups could bring down the power grid as a way of making a political statement

- **Ransom**—hacker groups could lock personnel out of critical systems until their monetary demands are met

Regardless of the why or the how, attacks against the energy grid are happening. To thwart would be hackers, it's critical to understand just how intrusion can happen and how you can prevent it.

Breaking Down the Attack

There are two main areas where an attack can take place on the electrical power grid—the power plant and the substation. Although substations might present physical vulnerabilities (i.e., a hard integration with the SCADA communication system), it is the power plants, like in our Consolidated Power scenario, where it's most likely for an attack to occur given the large number of potential vectors (as illustrated below):


Passive Security Culture
Business Network
Operations Network
Physical Electricity Infrastructure
Department of Defense Facility
ELECTRIC UTILITY IT AND OT SYSTEMS
Insider Threat
Weak Network Architecture
Public Internet
Compromised Vendor/Device
Unpatched Network
Human Error

- **Passive Security Culture**—when the energy provider isn't actively improving security across all aspects of power generation and distribution (i.e., patching systems, requiring strong authentication, etc.), it leaves the entire system vulnerable. Energy providers like Consolidated Power cannot adopt a "it won't happen to us" attitude.

- **Weak Network Architecture**—a poorly designed network architecture can present numerous "holes" for attackers to compromise.

- **Public Internet**—connecting the energy provider to the public internet, which is required for daily business like sending emails, provides a conduit by which hackers can enter the provider's network (if the network is weakly architected and doesn't do a good enough job of keeping the internal and external networks separated).

- **Compromised Vendor/Device**—when the public internet can't provide a way into the electric provider, the next best vector is to compromise a device (such as a laptop infected with malware that will connect to the provider's internal network). This provides a less direct, but ultimately more intrusive, method to gain access to the network.

- **Insider Threat**—although not one wants to admit it, there's always the chance a disgruntled employee, with deep understanding of the information systems within the electricity grid, could effectively hack the system as retribution for perceived wrongs.

- **Human Error**—not all hacking happens remotely. It's possible, through social engineering, that a human being could make a mistake and provide hackers with critical information they need to force an intrusion.

WHAT HAPPENED WITH CONSOLIDATED POWER?

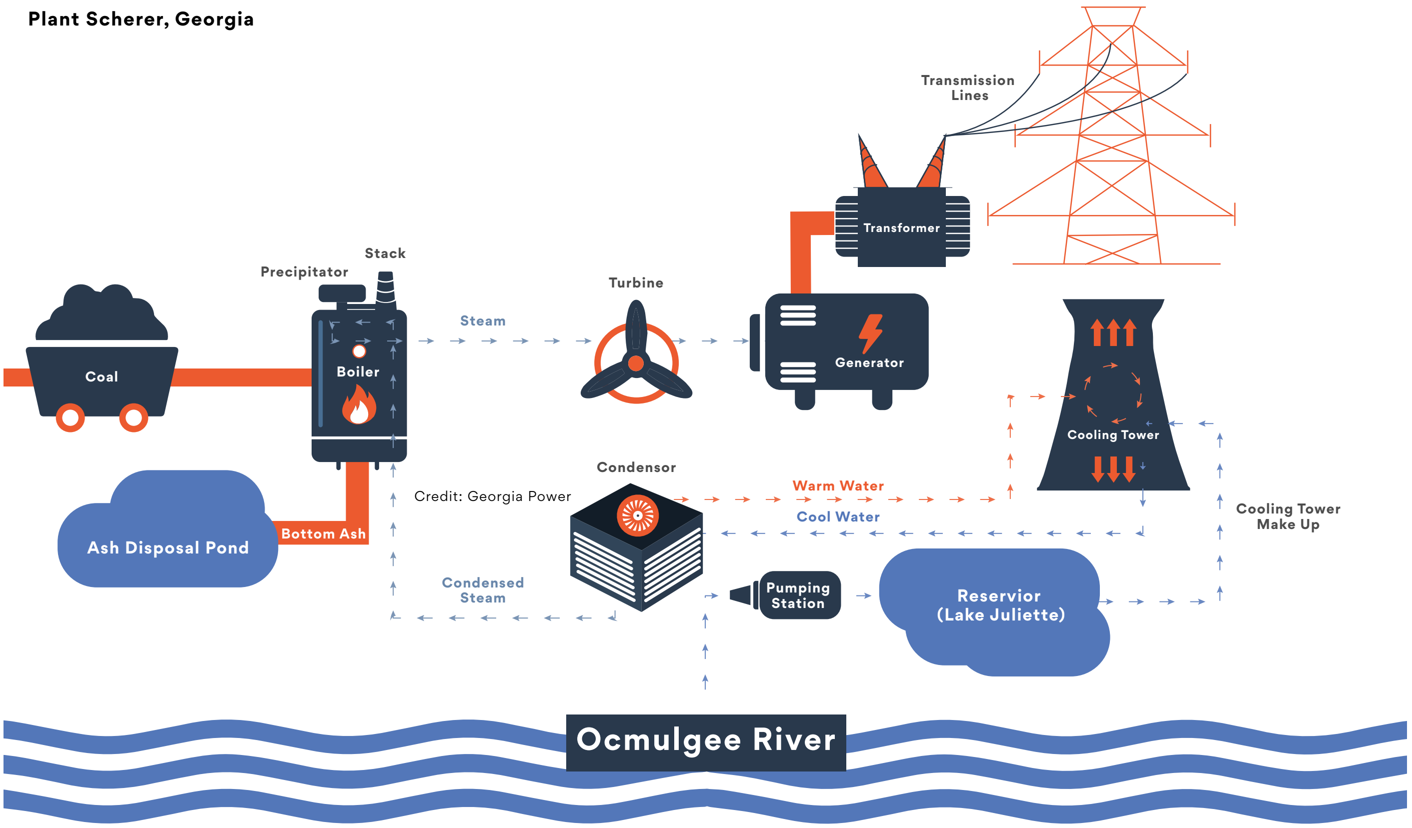
In the case of our scenario, there are a lot of possibilities but it's most likely that the system was compromised months, if not years, before. Using various methods of intrusion—coming in through the Internet, compromising a weak network architecture, even social engineering—malware was installed in unpatched and vulnerable systems waiting for the appropriate time to be enabled by the hackers to carry out their nefarious plans.

Now let's look at those attack vectors in relation to the machinery within a coal-burning power plant.

As depicted, there are innumerable systems and subsystems that hackers could potentially target especially as more of these components become connected to larger IT/OT networks:

- **The boiler**—hackers could compromise thermostats or shut off boilers entirely
- **The condenser**—hackers could shut off water flow causing warm water buildup and leading to turbine overheat or shutdown
- **The turbine**—hackers could disrupt steam flow or shut down the turbine entirely
- **The generator**—hackers could repeatedly engage circuit breakers causing the generator to start and stop, eventually resulting in physical damage
- **The transformer**—hackers could spike electricity flow through the transformer causing it to malfunction or catch fire

Plant Scherer, Georgia



Credit: Georgia Power

When combining the number of components (there may be hundreds of connected devices within the power plant diagram) with the number of attack vectors explored previously, the various opportunities for intrusion and damage grow exponentially.

Protecting Against Cyber Threats to the Energy Grid: Four Key Considerations

Identifying and protecting against cyber threats is a mandatory first step before connecting generation plants, transmission facilities, substations, and other power related industrial infrastructure to the Industrial Internet. Here are four key considerations when assessing solutions:

1) Improve End-to-End Asset Visibility: You Can't Protect What You Can't See

Ensure your solution continuously maps and monitors industrial traffic, learning as it adapts to observations. You'll want to combine advanced threat intelligence from public and private sources with out-of-the-box policies to establish and maintain a baseline of acceptable behaviors. Look for an approach that helps you optimize and protect your OT environment, including protocols, sources, destinations, equipment, and anomalies or violations of baseline policies. In addition, ensure that the solution can inspect full messages (regardless of protocol) for both content and context at the transaction level and that all reporting can be integrated into your SIEM/SOC and forensic analysis tools of choice.

2) Mitigate Cyber Threat Risks: Just Seeing a Threat Won't Stop It

Look for an approach that stops cyber threats in real time, before they can damage your industrial infrastructure or the environment. Look for active alerting and proactive blocking of unauthorized communication and commands, preventing cyber threats from reaching and affecting targeted objects and data. You'll want a solution that operates at line speed, providing protection at a fine-grained transaction level, enabling authorized traffic and normal workflows to continue unimpeded even in the face of ongoing cyberattacks.

3) Provide Managed Remote Access: Protection Means Control over Access and Actions

Allowing vendors to remotely access industrial equipment for maintenance and troubleshooting offers obvious advantages. Providing industrial data to service providers may help improve business outcomes. However, opening industrial infrastructure to 3rd parties creates significant risk. Traditional VPNs can help with controlling access, but once a connection is made, owner/operators have no way to know or control the actions that remote users undertake on their open ports. The porous lack of cyber protection provided by VPNs is simply unacceptable in the industrial world. Look for a Managed Remote Access solution that goes far beyond traditional VPNs to create an on-demand, encrypted, policy-protected, bi-directional tunnel between remote users and your industrial infrastructure.

Ensure that every element of communication between you and 3rd parties is verified, managed, and blocked if necessary. Look for Managed Remote Access that enforces authentication, authorization, white lists, and other security controls at the device command and individual transaction level.

4) Secure Your Industrial Internet: Protect Your Assets Before You Connect

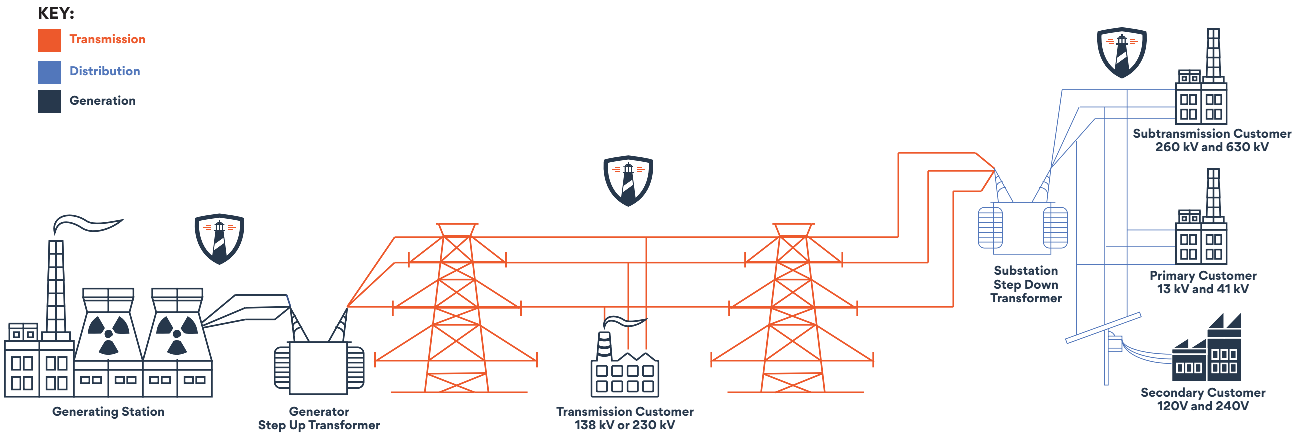
When you are ready to interconnect your infrastructure and data to take advantage of all the Industrial Internet must offer, look for a solution that offers bi-directional, access-controlled, and policy-protected tunnels between your organization and your chosen IIoT partners. This means that not only is access limited to specific sources and destinations, but also that content and context is controlled by policy so that every element of communication between the organization and its external IIoT ecosystem can be verified, alerted, and blocked if necessary.

You need a proven leader with a solution that can provide the deep system level protection while enabling your IT resources to effectively manage it. That leader is Bayshore Networks and the solution is the Bayshore Industrial Cyber Protection (ICP) Platform.

How Bayshore Networks Can Help

The Bayshore Industrial Cyber Protection (ICP) platform stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet of things (IIoT).

The Bayshore ICP platform delivers a comprehensive set of capabilities required to protect and defend against sophisticated, complex attack systems. Bayshore empowers industrial enterprises with safe and efficient production, operational insights, and improved business outcomes, while blocking cyber threats to industrial plants, machinery, and people. It is designed to support customers throughout the entire industrial cyber protection life cycle, leading to improved business outcomes.



The journey begins with mapping networks assets and progresses to identifying anomalies, preventing attacks and incidents, optimizing business efficiencies, and finally, to enabling innovation and digital transformation, such as creating new revenue sources and product markets.

What if Consolidated Power Had a ICP Platform?

Consolidated Power did not have the right tools in place to provide them the visibility across their IT/OT systems and stop the attack from happening in the first place. But with a Bayshore ICP platform, Consolidated Power would have been able to see and prevent what resulted in a catastrophic event.

Step One: Deep Insight

At the heart of the Bayshore ICP platform is the ability to see across the network. The platform provides Discovery, Monitoring, and Reporting capabilities that are key to detecting attacks before they happen. Bayshore's automated discovery engine maps and monitors all industrial network elements. Fast. Non-disruptively. In minutes, users receive action-ready insights to optimize and protect the OT environment, including protocols, sources, destinations, equipment, and anomalies or violations of baseline policies.

Bayshore's automated learning engine continuously monitors industrial traffic, and adapts policy recommendations to observations. Combining advanced threat intelligence from both public and exclusive private sources, with Bayshore's own deep industrial cyber protection expertise, a rich set of out-of-the-box policies help establish and maintain a baseline of acceptable traffic.

Step Two: Protection

As we saw in our electrical grid scenario, by the time cyber alerts reach humans, catastrophic damage may have already occurred. Action must be taken instantly when cyber threats arise, before they reach their targets.

Only Bayshore offers active alerting and proactive blocking of unauthorized communication and commands, preventing cyber threats from reaching and affecting targeted objects and data. Bayshore operates at line speed, and protection is provided at a fine-grained transaction level, enabling authorized traffic and normal workflows to continue unimpeded even in the face of ongoing cyberattacks.

Bayshore leverages known threat intelligence to proactively block or filter malicious machine instructions at the most granular levels of data transmission. The flexibility and breadth of the Bayshore ICP platform's content inspection also make it suitable to protect against unknown (i.e., zero day) threats, including attacks that may be years in the future. Going far deeper than packet, signature, or payload, Bayshore inspects full messages regardless of protocol for both content and context at the transaction level.

From environmental changes, baseline anomalies, to policy violations nothing gets by Bayshore undetected. Even low-risk, or normal changes can be flagged for validation and follow up. And, of course, all reporting can be integrated into SIEM/SOC and forensic analysis tools of choice.

Managed Remote Access

No longer does interconnection mean opening a port with no visibility or control over what occurs on the ensuing link. Bayshore's Managed Remote Access solution goes far beyond traditional VPNs to create an on-demand, encrypted, policy-protected, bi-directional tunnel between remote users and local industrial infrastructure.

With Bayshore, not only is access limited to authorized users and assets, but administrators have complete control over actions taken via the link. Bayshore Managed Remote Access enforces authentication, authorization, white lists, threat intelligence, and other security controls at the device command and individual transaction level.

For example, administrators can allow a 3rd party vendor to remotely monitor, manage, or troubleshoot only specific pre-authorized assets, using only selected pre-approved commands. Access, visibility, and control is blocked for that same vendor elsewhere in the infrastructure. Another common use case is enabling a central SOC to establish secure tunnels to many remote locations such as substations to gather telemetry, check status, or gather other industrial data for monitoring and analysis.

Next Steps

The Bayshore Industrial Cyber Protection (ICP) platform stops cyber threats before they can damage critical industrial assets and systems, and allows secure connection to the industrial internet of things (IIoT).

The Bayshore ICP platform delivers a comprehensive set of capabilities required to protect and defend against sophisticated, complex attack systems. Bayshore empowers industrial enterprises with safe and efficient production, operational insights, and improved business outcomes, while blocking cyber threats to industrial plants, machinery, and people. It is designed to support customers throughout the entire industrial cyber protection life cycle, leading to improved business outcomes.

About Bayshore Networks, Inc.

Bayshore Networks® is the leading provider of industrial cyber protection. The Company's award-winning technology unlocks the power of the Industrial Internet of Things (IIoT), providing enterprises with unprecedented visibility into their Operational Technology infrastructure while safely and securely protecting ICS systems, industrial applications, networks, machines, and workers from cyber threats. Bayshore's strategic partners include among others Arista, AT&T, BAE, Cisco, Dell, SAP, VMware, and Yokogawa. Bayshore is a privately held company headquartered in Washington, DC and backed by Trident Capital Cybersecurity, Yokogawa, Samsung Next, and BGV Capital. For more information, visit **www.bayshorenetworks.com.**

BAYSHORE

[i] Department of Energy, "Transforming the Nation's Electricity Grid." January 2017.
[ii] Kovacs, Eduard, "Attackers Using Havex RAT Against Industrial Control Systems," Securityweek, June 24, 2014, accessed November 10, 2015, www.securityweek.com
[iii] Dragonfly: Western Energy Companies Under Sabotage Threat" Symantec Security Response, June 20, 2014, accessed November 9, 2015, www.symantec.com/connect/blogs
[iv] Idaho National Laboratory, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," 2016
[v] Department of Energy, "Transforming the Nation's Electricity Grid." January 2017

BAYSHORE

www.bayshorenetworks.com