Low Latency Encryption Will Secure the U.S. Electrical Grid

By John Downing, President, Encrypted Grid, LLC

The electric power grid is the backbone of America, generating and transmitting the energy to empower all sectors of our economy. Reliance on the electric grid is our fundamental need. Because of this, it has long been considered a logical target for a catastrophic cyberattack.

Power grid outages are inevitable, and the economic impacts can be significant. One of the most notable in the United States was the 2003 Northeast Blackout which left 50 million people without power for four days and caused economic losses between $4 billion and $10 billion. In 2015, a cyber attack took down parts of a power grid in Ukraine. In March 2019, a solar generation utility in the United States experienced communications outages when an attacker exploited known firewall vulnerabilities to cause unexpected device reboots. Most recent was the June 2020 cyberattack that disrupted Honda's internal computer networks, forcing it to shut factories across the globe and leaving employees cut off from email or internal servers. The attack appears to have been carried out by software designed to attack the control systems for a wide variety of industrial facilities, including power plants.

America has been heeding warnings of a widespread cyberattack on the power grid. In the last two years, reports from DHS, the Federal Bureau of Investigation and the U.S. Intelligence Community have revealed that Russian cyber attackers have covertly gained access to U.S. and European critical infrastructure. In June 2019, U.S. officials revealed ongoing efforts to deploy hacking tools against Russian grid systems as a deterrent and a warning to Russia. Around the same time, U.S. grid regulator, the North American Electric Reliability Corporation (NERC), warned of a major hacking group with suspected Russian ties was conducting reconnaissance into the networks of electrical utilities. If successful, these foreign adversaries -- most notably from Russia, China, North Korea and even Al Qaeda – can shut off power to millions.

These threats from cybercriminal groups, including Dragonfly, a.k.a. TEMP.Isotope or Energetic Bear, and Industroyer, are escalating and have prompted an executive order signed by President Trump in May 2020 declaring these types of threats to be a national emergency.

In adhering to NERC's mandated Critical Infrastructure Protection (CIP) protocols, power companies have continued to fortify their defenses for protecting electricity generation and transmission systems against cyberattacks. But because of a technical issue, the power grid remains vulnerable.

The Power Grid's Command and Control Operations Require Lightning-Fast Communication.

The U.S. power grid today comprises roughly 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines; 55,000 substations; and 5.5 million miles of distribution lines that bring power to hundreds of millions of homes and businesses.

The ability to protect the grid is not possible with the existing encryption systems of today. The grid's command and control systems in a lot of cases must communicate as close to real time as possible. Unfortunately, encryption systems currently on the market take over 50 milliseconds to encrypt and transmit this data. The current use of overlaying firewalls, routers, and network switches can be defeated by hackers. Even physical separation of systems falls prey to human error.

The grid's command and control systems include:

- Supervisory control and data acquisition (SCADA), for monitoring, gathering, and processing real-time data through human-machine interface (HMI) software often at remote locations;
- Distributed control systems (DCS) that improve reliability of control, process quality and power plant efficiency;
- Turbine generator control systems;
- Substation and generator protection systems.

The ability to protect and guard these systems requires never before seen speeds of data encryption and networking.

Vulnerabilities Leave the Power Grid Wide Open to Cyberattacks.

If the COVID-19 pandemic has taught us anything, the unthinkable can happen. In the United States, there currently are around 10,000 power plants producing greater than 1 megawatt. In addition, there are thousands of extra power plants. If a hacker gets into the operational technology (OT) system and effectively controls system voltage or

frequency, this could damage not only one plant, but dozens -- upwards of 20 to 40 power plants in a region – thus possibly resulting in extended periods of loss of electricity.

In such a situation, the needed components that make up the power grid, such as transformers and substation equipment, are not readily available. The largest transformers that make up the biggest substations in every state are built on demand; these take 12 months or more to build. Power companies can redirect electricity around a single substation, but if hackers gain access into command and control stations, they can adjust voltage and frequency of the power grid causing multiple failures in a region.

For years, industry leaders have known about the power grid's vulnerabilities, especially an aging infrastructure that's extremely expensive to replace. Most leaders are praying that the unthinkable will never happen, or that these hackers will just magically "go away."

U.S. Senator Angus King (I-Maine), co-chair of the bipartisan Cyberspace Solarium Commission (CSC), has been advocating for the inclusion of vital cybersecurity amendments in the 2021 National Defense Authorization Act (NDAA). In a speech on the U.S. Senate floor on June 30, 2020, Sen. King stated: "Just as the pandemic was unthinkable, nobody could think of an attack that could bring down the electric system, or the transport system, or the internet, but it can happen. The technology is there… I believe, Mr. President, the next Pearl Harbor will be cyber. That's going to be the attack that attempts to bring this country to its knees, and as we've learned in the pandemic, we have vulnerability, and we have to prepare for it."

Progress has been made in detecting hacks and threats when they are occurring. However, we need encryption systems that will prevent hacks from ever occurring in the first place.

Power Providers' Out-of-Date Software Systems are Difficult to Protect.

Among its many directives, the North American Electric Reliability Corporation (NERC) issues critical infrastructure protocols (CIPs) that mandate all owners, operators and users of the U.S. bulk power system comply with Federal regulations (FERC) from the U.S. Department of Energy.

Among NERC's CIP requirements are monthly or quarterly virus updates on HMIs. Despite Windows 10 being the latest upgrade, many power control systems are still

operating on legacy technology platforms, such as Windows XP, Windows NT and Windows 2000 platforms, which were not designed with advanced security in mind. They are extremely vulnerable and expensive to upgrade. An internal employee tasked with running NERC's CIP updates on a legacy platform could inject a virus simply by using a thumb drive or USB stick.

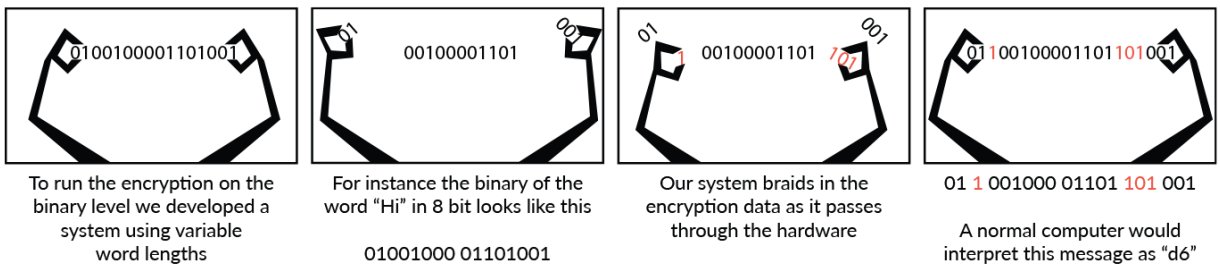
NERC requires energy providers to perform daily tests and report their levels of protection; fines for violating these regulations can be up to $1 million per day, per offense. These entities spend hundreds of thousands or millions to stay up to date on NERC guidelines. The average power plant producing greater than 10 megawatts spends typically $250,000 per year minimum to maintain NERC and FERC regulations.

Most large utilities and independent power producers (IPP's) use a remote central location to monitor and collect data from their plants. These remote connections are only being guarded by fancy firewalls and routers. Because of the high speed of the data required by command and control systems, none of them are encrypted. Many encryption companies are attempting to offer the next best solution, including services to scrub systems of malware, ransomware and viruses. But this is not enough.

The Solution: 0.06 Milliseconds.

Until now, the need for an extremely high encryption speed (less than 4 milliseconds) to protect the power grid's command and control systems has not come close to being solved.

In July 2020, Encrypted Grid, LLC, successfully tested a patented encryption solution to protect the power grid at an extremely low latency of 0.06 milliseconds. The encryption is non-algebraic and happens at the binary level. Everything is secured; the binary encryption scheme creates its own ever-changing computer language using variable word lengths. Placed in stand-alone hardware units, the technology braids the encryption data as it passes through, eliminating backdoors and user errors that can occur on user-driven software programs.



To run the encryption on the binary level we developed a system using variable word lengths

For instance the binary of the word "Hi" in 8 bit looks like this

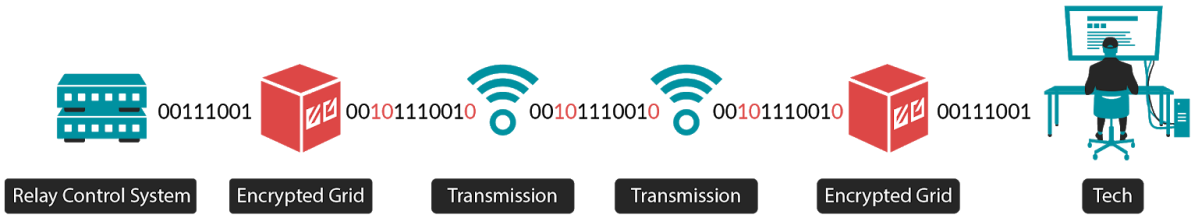
01001000 01101001

Our system braids in the encryption data as it passes through the hardware

01 1 001000 01101 101 001

A normal computer would interpret this message as "d6"

Because the system has zero software controls or operating systems, it's called an Actual Private Network (APN, versus the software-reliant VPN). The encryption can effectively protect and overlay even the oldest legacy systems, at a fraction of the cost of upgrading or replacing existing networks. It is proven to keep non-corporate traffic outside of its walls. Here's how this will work:



- The APN forms a solid cyber wall around the entire corporation, protecting everything from the IT to the OT. This impenetrable wall allows both sides to continue full communications within their organization without disruptions and without fear of someone in an admin role giving access via their computer being hooked up to a combination network.
- Substations, switchyards and generator protection relays can remotely communicate with one another through the Generic Object Oriented Substation Event (GOOSE) network enabling super high-speed data collection, command and control. The IEC 16850 protocol mandates that all OEMs use GOOSE. Because the protocol requires a high encryption speed of less than 4 milliseconds for protective relaying, GOOSE is vulnerable to cyberattacks.
- Encrypted Grid's technology is able to seamlessly convert and encrypt hundreds of access points in every power plant, including multiple protocols from GOOSE, turbine generator control systems, SCADA and DCS all on the same network.

In November 2019, Encrypted Grid began testing its encryption in lab environments. In July 2020, this testing was extended throughout the United States. The algorithms have been tested by highly advanced mathematicians at the Ph.D. and doctoral levels, who have validated them for strength and legitimacy. In multiple tests performed, Encrypted Grid successfully demonstrated the ability to encrypt data fast enough to not interfere

with command and control systems. This is using our prototype system that currently has a latency of less than 0.06 milliseconds.

In June 2020, Encrypted Grid demonstrated its hardware to Casco Systems in Cumberland, Maine.

“I was skeptical when first introduced to the Encrypted Grid hardware,” said Casco Systems president, Kevin Mahoney, PE. “I didn’t believe that you could encrypt high speed communications in under 2 milliseconds from end to end, without adversely impacting system performance. This speed is necessary for protective relays and control systems used in power generation and transmission. When Encrypted Grid demonstrated reliable encryption and transmission of IEC 61850 GOOSE messages in under 1 millisecond, I became convinced that a solution is here.”

“I’ve been in controls and protection for over 30 years and am amazed how efficiently this encryption technology works,” added Mahoney. “I finally have hope that we can secure the grid from cyberattacks.”

Securing America’s power grid from foreign adversaries and cybercriminal groups cannot depend on vulnerable software programs and operating systems. The solution lies in a hardware-based device with extremely high encryption speeds, which until now has not been commercially available. The solution is encryption in 0.06 milliseconds, and I believe it’s here.

About the Author

John Downing is president of Encrypted Grid, LLC, a patented data encryption technology that will revolutionize cyber security of the Bulk Electric System. He is a power generation thought leader with over 30 years of experience in the design, manufacture, operation, troubleshooting and repair of complex power generation control systems. He is the CEO and Principal of multiple power generation companies.

John Downing can be reached online at john.downing@encryptedgrid.com. For more information, visit https://encryptedgrid.com/.