SOLUTION BRIEF

Gathering Network Intelligence from the Digital Power Grid

The US electricity grid and power generation units are the hub of a prosperous and vibrant economy. Every activity — including transportation, manufacturing, hospitals, and housing and emergency services — depends on a reliable and consistent electricity source. The US electric generation and transmission infrastructure is one of the most complex systems in the world. It comprises more than 9,000 power plants with a combined generating capacity of 1 million megawatts and more than 300,000 miles of high-voltage transmission lines. The electric utilities that operate this infrastructure face unprecedented challenges.

Three Trends Challenging Utilities

Utilities must confront three simultaneous drivers of strategic change: cyberthreats, the emerging smart grid, and a changing power mix.

Cyberthreats

Countries worldwide have acknowledged that they are investigating weaknesses in the US electricity grid's infrastructure and cyber defenses. The attacks against Ukraine's power grid in 2015, shut down entire portions of the grid, affecting 225,000 people and showing that such incidents are not purely theoretical.

New Opportunities:

Large-scale adoption of Ethernet lets utilities gather digital intelligence from their networked equipment.

Solutions:

- Network taps copy network packets for monitoring and analysis.
- Bypass switches protect the live network from inline tool outages.
- Network packet brokers deduplicate and filter network packets.

KEYSIGHT TECHNOLOGIES

The US government, backed by individual states, has mandated a strong defense for the operators of the grid infrastructure. The most prominent of these requirements are the critical infrastructure protection standards, which the North American Electric Reliability Corporation (NERC) mandates for US utilities. Further actions are likely, prompted by legislation such as the Enhancing Grid Security Through Public-Private Partnerships Act and the Cyber Sense Act, which are before the US Congress.

Increasing numbers of threats, coupled with pending legal mandates, are leading to unprecedented challenges for the utilities' IT departments. They aim to rapidly deploy new technologies to strengthen their cyber defenses.

Emergence of the smart grid

The smart grid represents a new generation of digital controls, computers, data, and internet access. The smart grid provides more efficient power transmission. Its benefits include faster restoration of service after power outages, reduced operating costs, lower peak time load, more seamless integration of renewable power sources, and customer-located energy resources.

Changing power mix

Historically, most electricity generated in the US came from large, coal-fired power plants supported by a baseload from nuclear power plants. Ethernet-enabling the infrastructure using adapters and converters has extended the life of the equipment. But now a major shift is under way: coal declined to less than 30% of generation as gas-powered plants gained dominance (34%) and renewable sources (solar, hydro, biomass, wind) climbed to 15% of power generation.

Key Management Practices

Success in managing the above areas will depend on larger-scale adoption and integration of telecommunications equipment and systems based on Ethernet technology. Traditionally, the command and control infrastructure of the electric utility grid relied on old proprietary and industry specific technologies.

The large-scale adoption of Ethernet, plus an increased dependence on the telecommunications networks as a response to the three key strategic change drivers, has led to a greater need for visibility into the traffic on Ethernet-based networks. It is critical to inspect and monitor traffic on such networks using various tools that address the areas of audit and compliance, network and application performance management, and cyber intrusion detection.

Audit and compliance

Because energy companies are in a regulated industry, audits and compliance regulations are essential. The cost of fines and penalties can significantly impact business results and run into the tens or hundreds of millions of dollars. Many regulatory and legal bodies now hold companies responsible for power outages resulting from equipment failures or spikes in demand. In addition to governmental requirements, NERC has developed stricter standards and regulations for how companies secure critical assets to protect against hacking and espionage.

To cope with these requirements, companies need to access information in their networks to better predict gaps between supply and demand and detect anomalies in traffic entering or leaving the network. They need the ability to store that traffic on a short-term (days) or long-term (weeks or months) basis. Data capture tools need to gather raw data to investigate a security breach detected many days or weeks after the incident.

Network performance management

Network operations managers require tools that can monitor the health and performance of Ethernet networks and answer questions such as “Is there congestion?” and “Are packets being dropped?” If your network packet broker (NPB) drops packets, you are creating blind spots that can interfere with network analytics or affect security.

Application performance management

Application teams need tools to monitor the applications running across networks and answer questions such as “How long does it take to access data from a large database?” and “What is the quality of a voice call?”

Cyber intrusion detection

Security teams need the right tools to detect breaches of their cybersecurity systems.

Tools That Deliver Network Intelligence

Keysight supplies a range of visibility appliances and software that gives network tools access to direct copies of traffic flowing on Ethernet networks. Key among them are network taps and NPBs.

Network taps

Fiber optic and copper-based taps give network or cybersecurity tools copies of the exact traffic flowing over physical communication networks. This traffic then goes to the tools.

Network packet brokers

Keysight's Vision Series NPBs take traffic from multiple taps and deliver a single stream of traffic to each monitoring tool. One advantage of this approach is that the Vision NPBs collect traffic from switches operating at different speeds and can combine and deliver them to tools at whatever speed they operate. This allows IT to upgrade network links without necessarily upgrading monitoring tools, which can substantially reduce expenses. A single tool can also receive traffic from multiple taps. NPBs allow utilities to make maximum use of expensive management and cybersecurity tools. The inclusion of high-performance decryption capabilities also allows tools to see encrypted network traffic and allows IT teams to discover intrusion attempts hidden in HTTPS traffic.

In addition to the products described, Keysight provides solutions designed to protect critical IT infrastructure in the electrical grid system, including bypass switches, passive monitoring, and Keysight ThreatARMOR.

In addition to world-class hardware solutions, application stacks such as NetStack, AppStack, SecureStack, and PacketStack add more value and functionality to Keysight NPBs. A purpose-built design in each stack of software features ensures you get the best performance while fully leveraging the intelligence they bring to your visibility architecture.

Utilities can manage change in their industry more effectively by tapping the intelligence embedded in their digital networks.

Bypass switches

Keysight's iBypass range of bypass switches allows IT teams to rapidly deploy new security devices in their networks with no resulting downtime. These switches can detect faults in security tools and immediately switch over to secondary systems; they allow operators to "harden" their "ruggedized" IT infrastructure. You can deploy them on a standalone basis or in conjunction with Vision Series NPBs to harden multiple cybersecurity tools.

Passive monitoring

Hackers are increasingly turning their attention to the critical infrastructure that keeps society functioning. Unfortunately, many water and electrical systems are not secure from malware and other attacks. Real-time monitoring, also called passive monitoring, is critical to ensure access to critical infrastructure.

ThreatARMOR

ThreatARMOR sits in front of firewalls or intrusion protection systems as part of a multilayer cybersecurity defense. The tool has an extensive allowlist of global IP addresses and blocks known bad actors or corrupt nation-states from getting internet access.

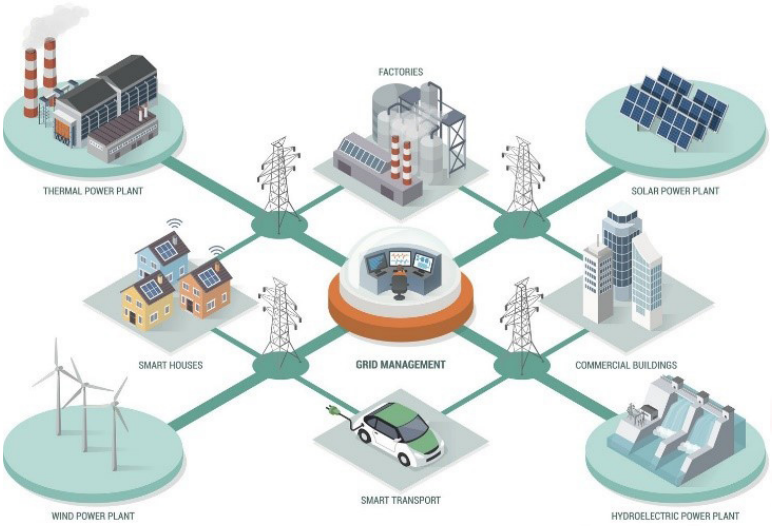

Figure 1. The surrounding ecosystem relies on secure and efficient grid management