SOLUTION BRIEF

Ensuring Cybersecurity Compliance in the Electrical Power Industry

Vulnerability of Critical Power Infrastructure

Maintaining the resiliency of the power sector is critical to national security. Accounting for 5% of US GDP, the electrical system serves as the hub for transportation, manufacturing, and society in general. The US grid has over 3,300 utilities, 55,000 substations and 450,000 miles of transmission lines.

The North American Reliability Corporation (NERC) mandates critical infrastructure protection (CIP) standards for high-voltage electric transmission and power generation. States and local Public Utility Commissions (PUC's) regulate the distribution sector. Many, including in California, Connecticut, and New Jersey are adopting approaches similar to NERC CIP.

The Security Imperative

- Several operators have been fined millions of dollars in recent years for failing to comply with NERC CIP.
- Plus, a targeted attack on the Western power grid took place in 2019.

The Challenge for Utilities Security Personnel

Grid modernization exposes operators to new potential threats from nation states, criminals and disgruntled employees. Operational technology (OT) networks and Industrial Control Systems (ICS) that were physically separated from traditional IT infrastructure are increasingly interconnected, creating unique security issues:

- Proprietary appliances and sensors with outdated software, vulnerable passwords and lack of encryption
- Malware insertion via dedicated attacks to take control of critical infrastructure by criminal and nation-state actors
- Third-party remote access for contractors that may have lax security processes

The attacks against Ukraine's power grid in 2015 showed that the threat is real. CSO's and IT teams need new strategies, tools, and expertise.

KEYSIGHT TECHNOLOGIES

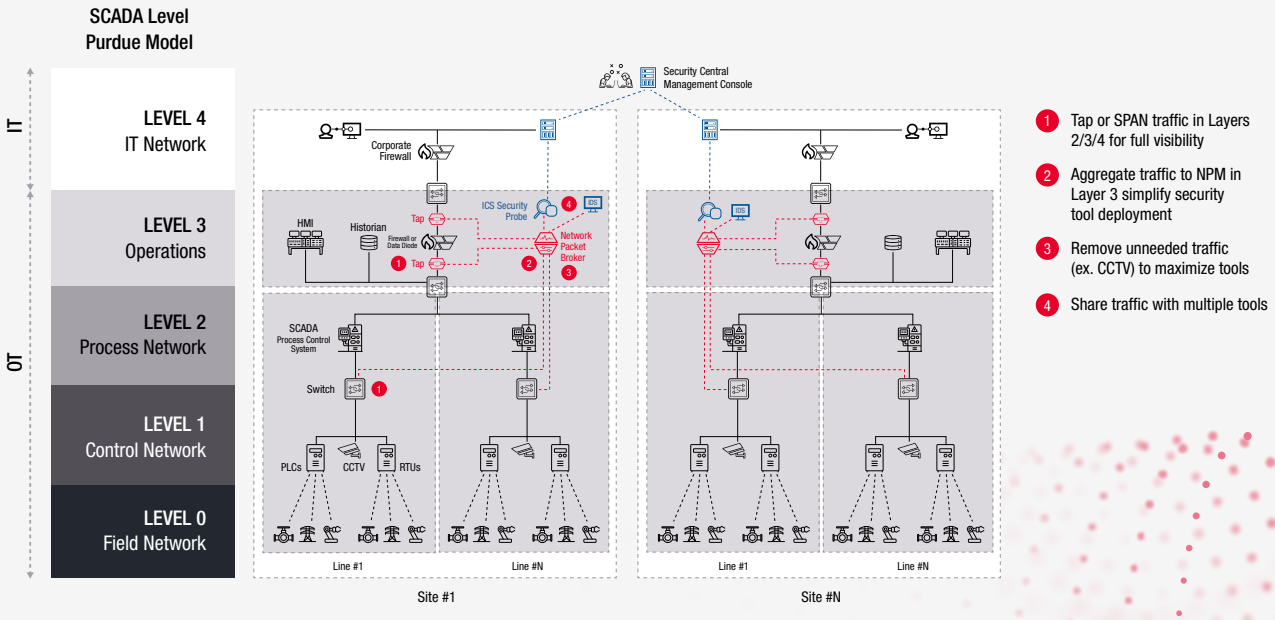
Keysight Solution for Security and Compliance

NERC CIP Standards 5, 7, and 10 require utilities to collect and archive network traffic data at the plant and substation level. Utilities must also regularly conduct audits and vulnerability assessments. Keysight's Visibility Architecture can help:

First, operators should place Ethernet-based taps in power plants and substations at multiple levels of the SCADA network. Taps give OT personnel and network managers easy access to data from critical infrastructure systems.

After tap installation, a network packet broker (NPB) aggregates data from the various taps, remove unnecessary pieces of monitoring data, and then pass that data on to application monitoring tools. Keysight partners with OT security companies such as Nozomi Networks and Claroty to provide a tightly integrated solution for utilities. Because Keysight's NPB's do not drop any packets, they create a complete historical archive of required data to meet strict NERC audit requirements.

ICS/OT Security Visibility Reference Architecture



KEYSIGHT TECHNOLOGIES