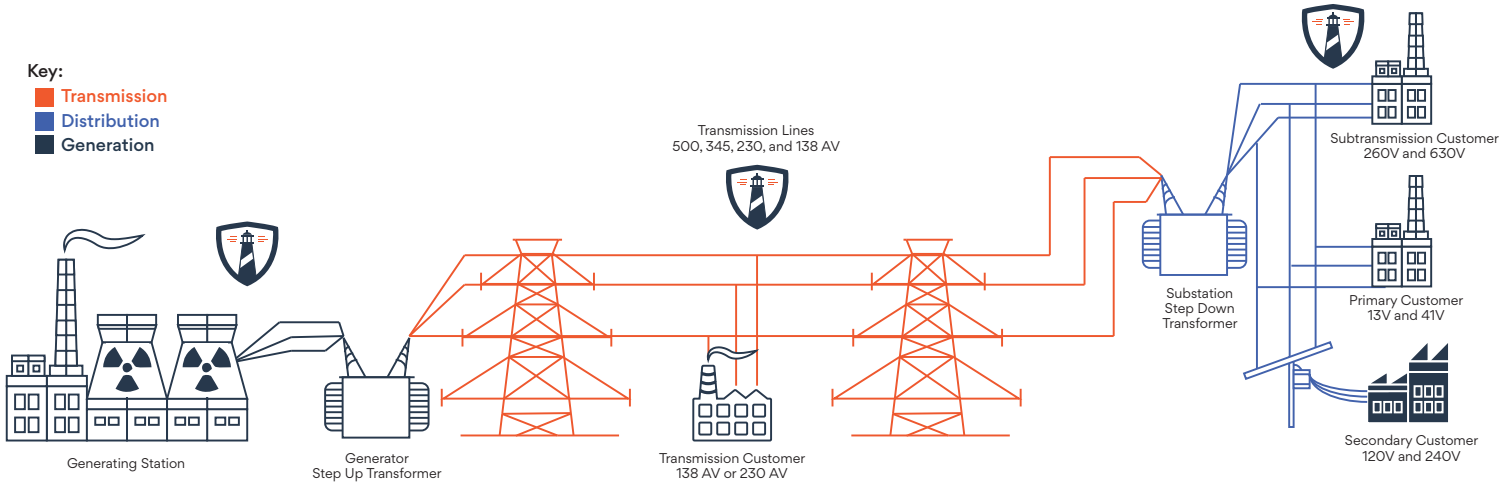
BAYSHORE

USE CASE
Energy

Electric power generation and distribution utilities in the US, UK and other markets are migrating to Industrial Internet (or smart grid) architectures at an increasing pace. This shift is accelerating, presenting utilities with new security, operational policy, and safety based concerns. Indeed, many studies indicate that power facilities are considered the most likely target for near-term politically motivated cyber attacks. Energy utilities need to immediately determine:

- How to identify and protect cyber assets to address the increased attack surface inside the sub-station and across transmission architectures.
- How to control access to sensor/customer data according to class of users (maintenance, field worker, third party, etc.)
- How to defend OT environments through detection and remediation of remote access and insider attacks on OT-protocol based networks.
- How to provide security for demand response sensor networks by ensuring highly flexible response and interconnection; avoiding outages and operational errors; and ensuring operational compliance and safety at critical substation locations.

BASIC STRUCTURE OF THE ELECTRIC SYSTEM

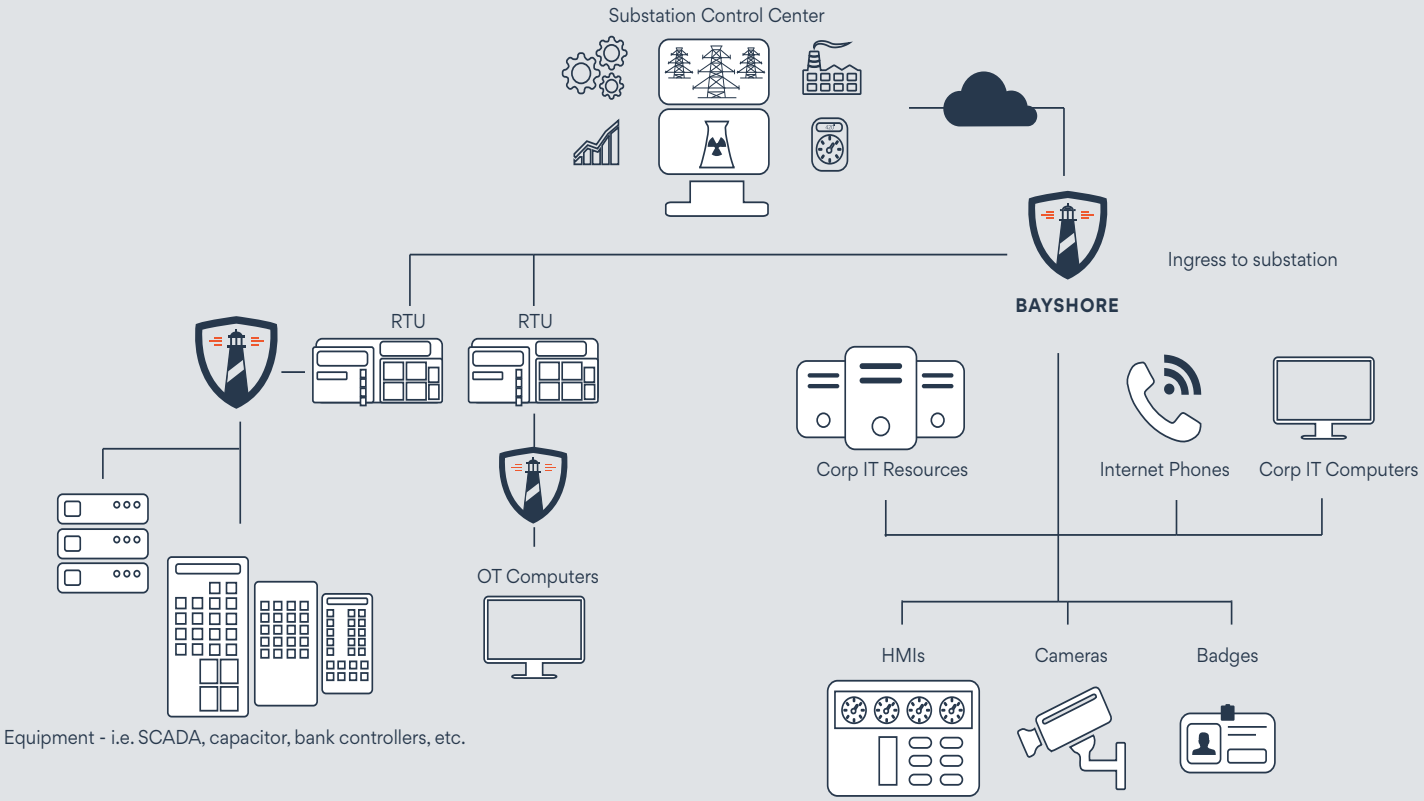


Where Legacy Solutions Fall Short

Energy utilities requirements impact the full spectrum of the Base Electrical System (BES) and create security and policy enforcement challenges where legacy solutions fall short, such as:

- Cyber-asset protection (large attack surface)
- Substation OT system access control and cyber defense (key Internet entry point)
- Policy-based enforcement by role and asset
- Regulatory compliance and adherence – expanded focus on safety, policy compliance and security.

BAYSHORE IN ELECTRIC UTILITIES



- Allows traffic between V-LANs only according to policy
- Provides OT device inventory capabilities
- Bayshore filter on each V-LAN, separated physically
- Parses protocols including DNP3 and others

System availability and downtime avoidance

End-to-end solution / integrated security

Support for new industrial internet use-cases (with near term ROI)

Scalability to support global OT infrastructure

Multiple deployment options

More efficient operations via improved response time/ reduced service disruption risk

BAYSHORE
INDUSTRIAL CYBER PROTECTION

www.bayshorenetworks.com