BELDEN
SENDING ALL THE RIGHT SIGNALS

Solution Guide

Market Dynamics Facing Energy and Utility Modernization

An aging power grid infrastructure along with new demands for digital technology that depend upon it, are driving forces for the next generation grid infrastructure that will be needed to automate and manage electricity needs now and the future.

Digitization and compliance

Smart grids are the next generation grid infrastructure that efficiently transmit electricity, adjust to changes in demand, quickly restore electricity after power disturbance and reduce operation cost. This requires an increasing number of devices being connected to a network and transforming data into information. Concern comes from connecting devices or environments that have never been connected in the past. This exposes these once air-gapped or physically-isolated electrical substation networks to the world of cybersecurity.

Step One: **Visibility**

Having visibility of your smart grid is the first step to a cyber-secure network. **Tripwire Industrial Visibility** and **Tripwire Log Center** provides this visibility:

- Understand all the devices on your smart grids inclusive of devices in substations as well as control center, what they are communicating with, and when their configurations change.
- Correlate log events from multiple sources and writing rules to flag events of interest. For example, if a failed login is attempted 5 times on a critical device in a substation, **Tripwire Log Center** emails an automatic notification to the network manager.

Step Two: **Protective Controls**

Once complete visibility has been achieved, the right protective controls to mitigate the risk or impact of cyber events can be put into place. Whether adopting a framework, such as IEC 62443 or NERC CIP for North American Utilities, all industrial cybersecurity frameworks call for two basic, fundamental measures:

- **Network Segmentation:** Substation compliant Hirschmann EAGLE and Tofino Security appliances enable robust network segmentation (organizing networks into smaller segments and explicitly permitting communication required for smart grid applications.)
- **Device Hardening:** Ensure all devices – HMI, SCADA, engineering workstations, switches, routers, etc. – are configured to industry cybersecurity best practices and frameworks, such as IEC 62443 or NERC-CIP

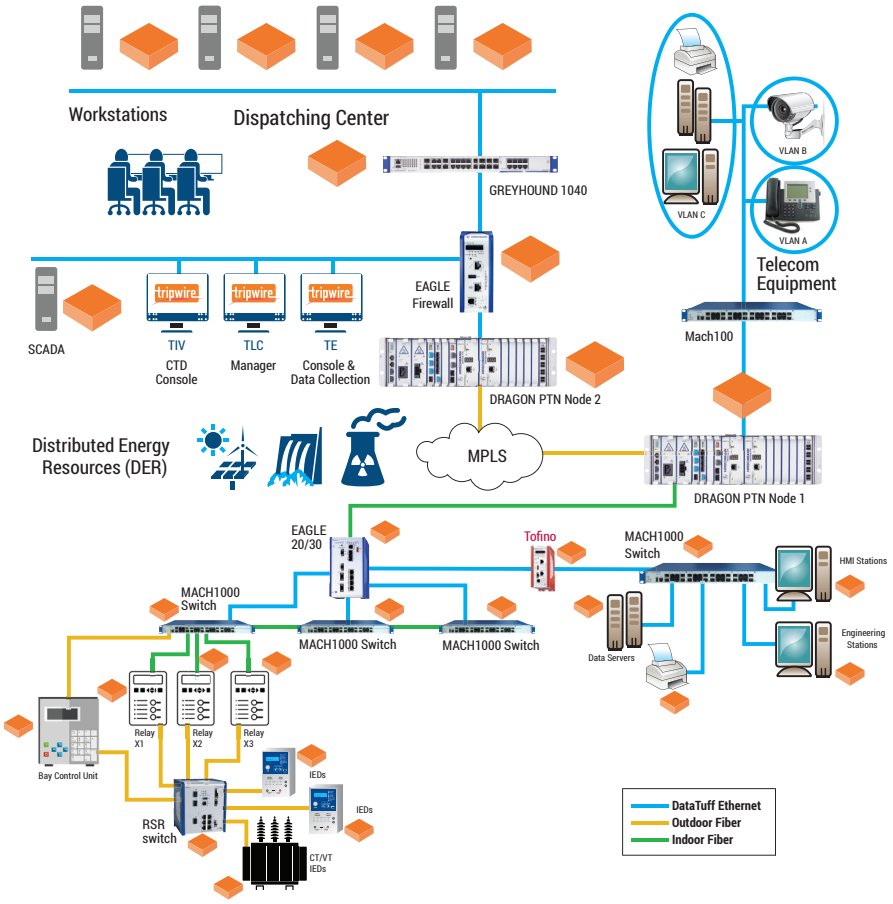
Step Three: **Continuous Monitoring**

Once a foundation of visibility and protective controls has been established, you can begin continuously monitoring the smart grids for ongoing situational awareness to manage abnormal or unexpected behavior. This awareness allows you to keep your grid operational and avoid unnecessary or unplanned downtime. Tripwire solutions can enhance awareness via a continuous monitoring solution:

- **Understand** when controller modes or configurations have been changed that do not map to authorized work orders
- **Know** if a rouge asset has been connected to the network and is propagating malware or making connections to external networks
- **Monitor** engineering workstations and SCADA servers to ensure correct configuration against internal build specifications or selected cybersecurity framework

BELDEN
SENDING ALL THE RIGHT SIGNALS

Energy & Utility Network Reference Architecture Example



Customer Successes

- Substation Environment for Utility: Leveraged Tripwire Industrial Visibility to automate creating and sustaining an asset inventory of all of the devices in their substations as well as provide vulnerability and change configuration information related to those assets
- Nuclear Power Generation: Excited to leverage the use of the Tofino Security Appliance to secure controllers within their nuclear power generation facility with deep packet inspection on their industrial protocol Modbus TCP
- North American Electrical Utility: Saved hundreds of man-hours preparing for NERC CIP audits as Tripwire helped us automate the collection of evidence for many of the NERC CIP requirements

TLC = Tripwire Log Center | TE = Tripwire Enterprise | TIV = Tripwire Industrial Visibility
Industrial visibility, protective controls and monitoring enabled through active and passive solutions: Tripwire Enterprise, Tripwire Log Center and Tripwire Industrial Visibility

Energy Automation

Belden's solutions can:

- Provide complete asset inventory and industrial protocol communication
- Identify vulnerabilities to all assets
- Identify changes to controllers – configuration, mode and firmware
- Data from many disparate substations can be aggregated into a centralized console or enterprise management hub
- Measure the configuration for HMI, SCADA, engineering workstations and network infrastructure to IEC 62443, NERC-CIP, NEI 08-09 (Nuclear Energy Institute), and many others
- Provide visibility to all log information from controllers, SCADA, HMI, engineering workstations and network infrastructure
- Provide network segmentation between the grid and corporate IT, inter-substation communication and enforce all industrial protocol communication to remote terminal units (RTUs)

Call your Belden or Tripwire sales representative to schedule a demonstration or visit our websites at www.belden.com and www.tripwire.com.

Belden US 1-855-400-9071 ■ Tripwire US 1-503-276-7500
Belden EMEA +49 (0)7127 14 1809 ■ Tripwire EMEA +44 (0) 16 2877 5850
Belden APAC +65 6879 9800 ■ Tripwire APAC +65 6879 9839