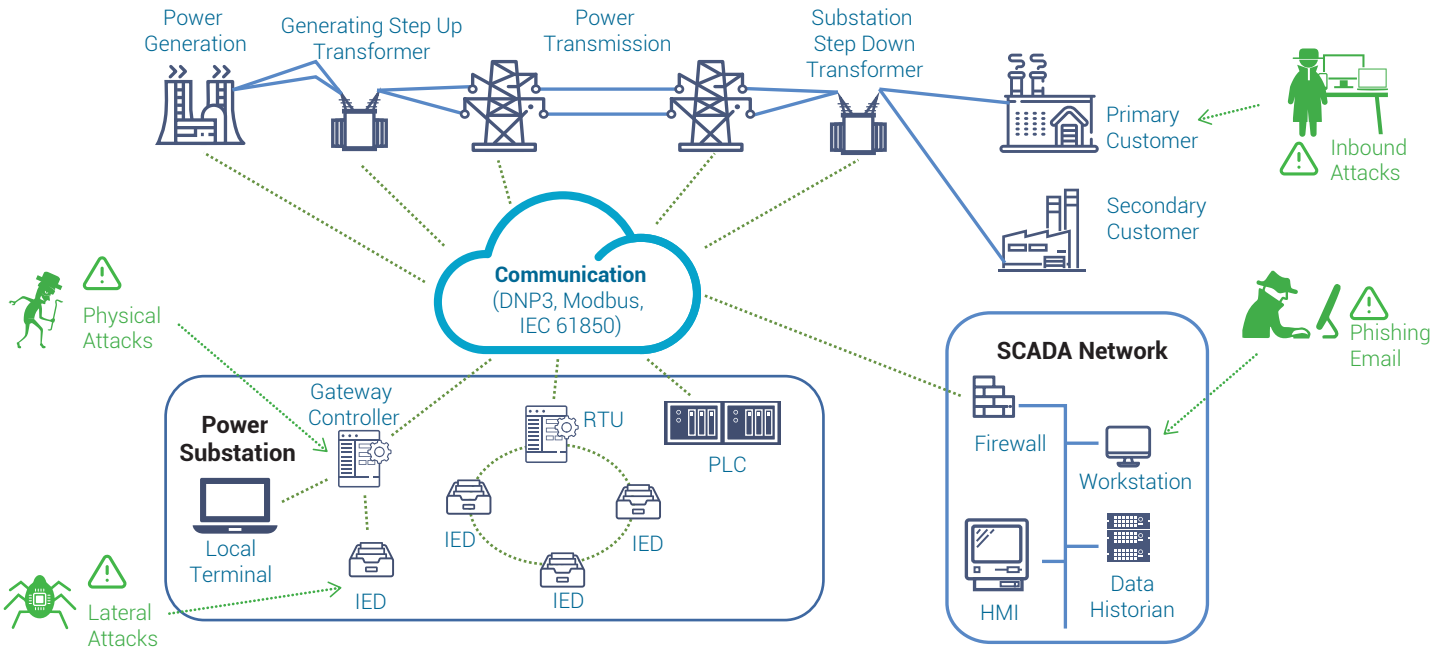
Industry Brief: Electric Utilities

MOCANA



Electric Power Grids Present Many Surfaces for Attack

Ensuring Safety, Reliability and Compliance

Perimeter-based defenses and threat detection technologies are not enough to defend against modern cyber attacks. Many programmable logic controllers (PLCs), intelligent edge devices (IEDs), remote terminal units (RTUs), controllers, gateways, smart meters, and Internet of Things (IoT) edge devices are vulnerable due to a lack of strong cryptographic controls, including: multi-factor authentication, secure boot, secure update, and secure, encrypted communications.

Industrial automation manufacturers and critical electric utilities must ensure compliance with cybersecurity standards such as NIST 800-53, Revision 4, IEC 62443-3-3, and FIPS 140-2. Furthermore, electric utilities must comply with additional standards such as NERC CIP 003. Keeping up with these standards as well as emerging standards from the Industrial Internet Consortium (IIC) and Industrie 4.0 is challenging. New regulations such as GDPR in Europe raise the stakes for non-compliance to more than €20 million per incident. Older protocols such as Modbus, DNP3 and BacNet can be difficult to secure.

In operating technology (OT) environments, risk is measured in terms of safety and reliability of the systems. While data privacy is important, oftentimes physical human safety and uptime drive the security needs of plants and large SCADA systems.

Mocana's Proven Cybersecurity Solution

Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications by giving industrial automation manufacturers, OEMs and critical infrastructure operators an easy way to:

- Harden IEDs, RTUs, gateway controllers, PLCs, and smart meters with multi-factor authentication using X.509 certificates and trust chaining
- Secure the boot process to validate the firmware, OS and applications
- Enable secure, cryptographically-signed over-the-air (OTA) and over-the-web (OTW) firmware updates
- Integrate hardware or software-based roots of trust such as
- TPM, SGX, TrustZone, HSMs, SIMs, and MIMs
- Replace open source crypto software such as OpenSSL.

For more information on Mocana's comprehensive IoT Security Platform and how it can help you secure your critical infrastructure, visit our website at mocana.com or send us an email via sales@mocana.com.

A: 111 West Evelyn Avenue, Suite 210, Sunnyvale, CA 94086 **W:** www.mocana.com **T:** 415-617-0055