Case Study: Top 5 Industrial Automation Manufacturer Hardens Devices and Enables Secure Communications for its Family of Intelligent Edge Devices (IEDs)

**Challenge**

This industrial automation manufacturer needed to upgrade the security on its family of Intelligent Edge Devices (IEDs) that are used by electric utilities for feeder protection and relays in High Voltage (35kV+) and Extra High Voltage (230kV+) transmission substations. IEDs act as electronic circuit breakers that can be programmed or controlled to relay power or cut power. This manufacturer was concerned because the IEDs could be accessed remotely and used only device-based passwords as the access control. The manufacturer’s customers felt that this presented a surface for attack that hackers could use to take control of an IED and shut down power in parts of the power grid. Communication with the device was unencrypted. The manufacturer was also concerned about meeting NERC-CIP 003-7 cybersecurity standards for power utilities. Finally, the manufacturer required a stronger cybersecurity solution that worked across multiple chipsets and operating systems used across the product line.

**Mocana Solution**

This top 5 industrial automation manufacturer selected Mocana to provide its IoT Security Platform, an embedded security software solution optimized for use in industrial control and IoT devices, that could be implemented on the Intelligent Edge Devices (IEDs). The software is designed to compile into the IED application sitting on RAM and flash memory of the device. The customer benefited by upgrading the device to support:

- FIPS 140-2 L1 validated cryptographic engine
- Encrypted transport using SSL/TLS for secure communications with the SCADA network
- Multi-factor authentication, including extended authentication via a RADIUS
- Integration with Wind River VxWorks, Nucleus OS, Texas Instruments, and PowerPC.

**Impact**

The manufacturer was able to harden the Intelligent edge devices (IEDs) with stronger cryptographic controls and authentication. Because communication with the device was now encrypted, the manufacturer’s customers, electric utilities, could ensure that hackers sniffing the line could not interpret the monitoring or control messages. The manufacturer was able to productize RADIUS authentication as a new security feature and more easily meet compliance requirements for FIPS 140-2 and NERC CIP 003-7.

**About the Top 5 Industrial Automation Manufacturer**

This top 5 industrial automation manufacturer has more than $100 billion in revenues and serves critical infrastructure sectors: aviation, energy, healthcare, lighting, oil & gas, power generation, transportation, and water. This business unit manufactures energy products to improve the transmission, distribution and conversion of electricity, and to help provide safe, efficient and reliable electrical power.