Energy Operator Protects Critical Infrastructure Using SafeNet High Speed Encryptors from Gemalto

CASE STUDY

The Organization
In one of Europe’s largest cities, this energy distribution company supplies electricity and gas through a combined system operator in the city proper and the surrounding region. Since the company’s facilities are considered “critical infrastructure,” factors such as safety, traceability, and transparency to business operations play an important role in its operations. It is essential that the company is able to supply the city and its suburbs with reliable electricity and gas every day, around the clock.

Challenge
The company needed to protect its critical infrastructure communications at Layer 2, ensuring hackers were unable to physically tap into lines and steal or manipulate utility information.

Solution
By encrypting communications regarding electricity and gas using the SafeNet High Speed Encryptors, data within the SCADA network cannot be stolen or manipulated.

Benefit
The company ensures that the city’s gas and electric supply has maximum protection from hacker attacks with Gemalto’s SafeNet High Speed Encryptors.
With the help of SafeNet High Speed Encryptors from Gemalto, we can ensure our SCADA network has premium protection against data tampering. The solution is reliable and was easy to implement with little effort. The Gemalto team gave us the best possible assistance during the pilot phase. Their flexible licensing model means that we are optimally prepared for future extensions when needed.

-Head of Systems Support, Energy Distribution Company

**The Business Need**

The supplier operates throughout the city and surrounding area to connecting several outdoor locations where natural gas is fed into the supply grid. To track and manage the operation, the company’s SCADA system generates a lot of data and communicates with the control center via its own network, which, for safety reasons, is not connected to the Internet. However, the danger exists that the proprietary lines could be physically tapped and the data stolen or manipulated.

Protecting their infrastructure has always been a major concern, and the company wanted to ensure such an attack could not occur. The company is one of the pioneers for data security, and already meets the stringent requirements of current and upcoming safety standards and recommendations, such as the Cyber Security Act.

The Cyber Security Act is an initiative of the European Union to enhance industrial systems network security. “The protection of industrial plants has seen an increasing emphasis in recent years in the IT world,” said the Head of Systems Support at the company. He suspects that the Stuxnet case has led the industry to rethink their security measures. “Stuxnet has shown how easily malicious software can be introduced. This has also led the Industrial IT world to look beyond perimeter security to the core of what must be protected.”

**The Solution**

The energy supplier decided to use multiple network encryption appliances from the Gemalto portfolio. To address the devices within the SCADA system, they needed a solution to secure data on Layer 2. Layer 3 solutions such as VPN or IPsec were therefore not suitable, and did not meet their performance requirements. The company’s solution partner recommended Gemalto solutions, and the company began testing Gemalto Ethernet solutions.

“From the start, we were convinced of the products and Gemalto as a vendor,” reports the Head of Systems Support. “The price to performance ratio matched, the test implementation went smoothly, and the support was very professional.”

The team chose two Ethernet encryptors from the SafeNet family: the SafeNet Ethernet Encryptor CN6010 for larger installations, and the SafeNet Ethernet Encryptor CN4010 for smaller branches of the network. Gemalto offers centralized management and simple administration and easy audit reporting over multiple circuits and network protocols at any time. The SafeNet Ethernet Encryptor CN6010 provides near zero-latency encryption for Ethernet or Fibre Channel and ensures FIPS, Common Criteria and CAPs-certified safety. “We opted for Gemalto solutions because we know we will be well prepared when we need to expand our infrastructure to support higher bandwidths,” the Head of Systems Support explained.

**The Benefits**

Using the encryption appliances for communications throughout the network provides optimal security, and also the flexibility for the future.

**Security.** Because the data is encrypted, any hacker attempting to tap the traffic would get only useless material, and would therefore have no chance of being able to manipulate the data for their own purposes. Furthermore, Gemalto Ethernet Encryptors can immediately detect manipulated data packets and the devices would then shut down the compromised transmission. At the same time, the devices would switch traffic to a second secure network connection so the traffic can be delivered to the destination via a different route.

**Room for Growth.** The company is also well equipped for future expansion. “With the flexible licensing model, we don’t need to buy new hardware as we expand. Instead we can increase the capacity for more bandwidth as needed. This proves once again that Gemalto’s Ethernet Encryption is the ideal solution to maintain the network security required for a municipal utility infrastructure.”

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

GEMALTO.COM

Energy Operator Protects Critical Infrastructure Using SafeNet High Speed Encryptors from Gemalto- Case Study