SCADA INDUSTRIAL CONTROL NETWORKS HIGH-ASSURANCE ENCRYPTION

CASE STUDY

Application of High-Assurance Network Encryption	
Sector:	Energy & Utilities
Use Case:	Critical Infrastructure Control Networks
Solution:	High-assurance protection of SCADA control network traffic

SENETAS
Security without compromise

Major European energy supplier protects SCADA control network with Senetas high-assurance encryptors

Our client protects critical infrastructure control networks using Senetas encryptors, distributed by Gemalto under its SafeNet encryption brand. The energy distribution system operator required an encryption solution that enabled high-assurance protection of its communications between the SCADA system and the control centre; without impacting network performance.

They implemented several SafeNet Ethernet encryptors (CN6010 and CN4010) to ensure prevention of rogue data, control hijacking and service disruption.

THE COMPANY

Our client is an energy distributor (carrier), supplying electricity and gas to a combined systems operator in central Europe.

Since the company's facilities are considered "critical infrastructure", safety, traceability and transparency of business operations are vital. Also, the company has an important role to play in providing a major city and its surroundings with a reliable supply of gas and electricity.

BUSINESS NEED

Our client operates throughout the city and surrounding area, interconnecting several locations where natural gas and electricity are fed into the grids.

The SCADA system generates large volumes of critical data and communicates with the control centre via a dedicated Layer 2 network.

For data security and safety reasons there is no connection to the Internet. However, there is still a risk is that the corresponding network links could be physically tapped and the communication data manipulated or disrupted; resulting in very serious damage.

Consequently, there is a need to ensure that a successful cyber-attack will not harm the data and network integrity; and that control could not be hijacked.

Protecting infrastructure for our client has always been a business and technical priority. The company is a pioneer in this field and already meets the stringent requirements of the relevant safety standards that are planned to become law.

The Cyber-Security Act (expected to come into force in 2016) is an initiative by the European Union that will bring more security to the networking of industrial systems.

"The protection of industrial plants has seen recent increasing emphasis in the IT world," Head of Systems Support.

Commenting on the Stuxnet attack, where a control system was breached, our client suspects there will be a rethink in the industry: "Stuxnet has shown how easily malicious software can be introduced into control systems. This has led the Industrial IT world to look at what else, other than just gateways, must be protected".

HIGH-ASSURANCE ENCRYPTION SOLUTION

Our client chose multiple high-assurance network encryptors from Senetas (products globally distributed by Gemalto); from carrier-grade to small form-factor, field locatable encryptors.

In order to effectively secure the current assets within the SCADA system, the company needed to implement dedicated Layer 2 links and encryptors.

Standard techniques, such as VPN and IPSec were not suitable. Similarly, MACSEC based hybrid network devices with so-called "built-in encryption" were not sufficiently secure. (See inset)

Senetas high-assurance encryptors were recommended by our clients' systems operators from the outset and impressed them during a proof of concept pilot.

"We were convinced from the start by the products and manufacturer. The price-performance ratio matched; the test implementation went smoothly and the support was very professional."

Two types of Ethernet encryptor from the Senetas CN series were chosen; the field-locatable CN4010 for smaller branches and the carrier-grade CN6010 for larger installations.

Senetas' global distributor, Gemalto, supports the newly installed encryptors; as it does all Senetas encryptors around the world.

The encryptors' management software (Senetas CM7) provides both centralised and remote encryption management, as well as easy audit reporting over multiple circuits and network protocols, at any time.

The CN6010 provides near-zero latency and data overhead encryption for Carrier Ethernet and Fibre Channel networks and is FIPS, Common Criteria, NATO and CAPS certified.

These are crucial features for SCADA security applications, as they provide maximum security without compromising network performance.

Senetas CN series encryptors support all Layer 2 protocols and topologies.

The company was impressed by the underlying Senetas CN platform's characteristics, including: scalability, 100% tamper-proof hardware security, interoperability among all models, zero impact on other network assets and the flexibility of FPGA design.

"We also opted for this device because we know we will be well-prepared when we need to expand our infrastructure and support higher traffic rates."

WHY HIGH-ASSURANCE NETWORK ENCRYPTION

High-assurance network encryptors provide maximum device and encryption security performance:

> 100% secure and tamper-proof hardware (dedicated solely to encryption)

> Certification by independent testing authority

> True end-to-end network encryption

> State-of-the-art 'client side' Encryption Key Management

> Standards based and authenticated encryption

CUSTOMER BENEFITS

Using Senetas high-assurance encryptors to protect the SCADA network provides optimal security.

Any hacker attempting to tap the traffic would only get useless, jumbled data. Encryption ensures there is no chance of being able to manipulate the SCADA communications.

Manipulated data packets would be detected immediately and the devices would automatically switch off the transmission.

The system's design ensures that at the same time traffic is switched to a second secure network connection, the traffic is delivered via a different route to the destination.

"With the flexible licensing model, we don't need to buy new hardware. Instead, we can increase the capacity for more bandwidth as needed. This shows, once again, that the overall solution is ideal for our SCADA network needs."

"With the help of Senetas high-assurance encryptors from Gemalto (SafeNet brand) we could protect our SCADA network optimally against data tampering. The solution is reliable and was easy to implement with little effort.

The Gemalto support team has given us the best possible assistance during a Pilot test. Their flexible licensing model means that we are optimally prepared for future extensions if needed."

Head of Systems Support.

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN series encryptors are supported and distributed globally by Gemalto under its SafeNet encryption brand. Gemalto also provides pre-sales technical support to hundreds of accredited partners globally: systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.

www.gemalto.com/enterprise-security/enterprise-data-encryption

SENETAS
Security without compromise

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com