STORMSHIELD

CUSTOMER CASE STUDY

How can electricity production plant control systems be renovated for greater cybersecurity?

INDUSTRY

Stormshield and Clemessy, the Eiffage Énergie Systèmes brand dedicated to industry, have been working in partnership for several years. In the energy sector, the software publisher and the integrator thus supported a joint customer in a project to renovate the instrumentation and control systems of several electricity production plants.

SEVERAL PLANTS
worldwide

40
workstations per plant

25
servers per plant

01

Renovating control tools without disrupting production

This customer wanted to modernise its installations in order to deal with the obsolescence of its instrumentation and control system, which is used to manage electricity production in several plants, and at the same time to improve its cybersecurity.

Stormshield and Clemessy were selected to support it in this complex project. The production of electricity is a critical activity that cannot be easily stopped, so it was essential to be able to carry out the renovation with as little disruption to operational processes as possible. In addition, some energy structures are classified as OIVs (Operators of Vital Importance) according to the French Military Programming Law (LPM) and/or OSEs (Operators of Essential Services) according to the European Network and Information Security (NIS) directive, and as such must fulfil strict legal obligations. For example, for OIVs, the equipment installed must be certified by the ANSSI (French National Agency for the Security of Information Systems).

"***Our mission consists in finding the right balance in order to offer a secure instrumentation and control service to maintenance staff and operators, without holding up production***", explains Emmanuel Lambert, Project Manager at EES - Clemessy.

It all starts with EBIOS

This project began with a risk analysis based on the EBIOS Risk Manager method published by the ANSSI. A French reference method, it enables "the determination of security measures adapted to the threat and the implementation of a monitoring and continuous improvement framework following a risk analysis shared at the highest level". To find out more, click here for the method guide: ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

02

Securing interconnection and protecting workstations

The main risks identified were related to the interconnection of the operational system (OT) and the office network, which did not have the same level of security.

Clemessy teams were able to remedy this by interconnecting them via a Stormshield SN510 firewall. Several security modules were quickly deployed. A DMZ area hosting web and file transfer services was created. Stormshield's Client SSL VPN solution now ensures the security of remote maintenance access. The industrial system is protected by strict flow filtering and the activation of the intrusion prevention system native to Stormshield SNS solutions operating in DPI (Deep Packet Inspection) mode. The internal and critical networks were segmented and secure centralised authentication was introduced via two redundant domain controllers (Active Directory).

To further supplement the security of the IT infrastructure of the instrumentation and control system, another Stormshield SN310 firewall was installed to secure the interconnection with sub-systems with different security levels. Advanced filtering of industrial protocol commands such as Modbus was implemented using the Stormshield firewall's DPI function, enabling only read commands to be authorised.

"Stormshield is very involved in OT and is a particularly interesting supplier when we are designing operational systems for our customers. Its French equipment, certified and qualified by the ANSSI, has functions adapted to the industrial world, and its easy-to-use solutions are greatly appreciated in the field"

JEAN SCHNOEBELEN
EES - Clemessy activity manager

The IT equipment (servers, monitoring stations, workstations) was also equipped with HIPS (host-based intrusion prevention system) protection using the Stormshield Endpoint Security solution. This solution has the advantage of not requiring frequent upgrades and enables the use of peripheral devices to be controlled, particularly USB ports.

The renovation operation also included securing Windows operating systems and renewing network switches and numerous PLCs.

THE SOLUTIONS USED

- → SN510 AND SN310 FIREWALLS
- → STORMSHIELD SSL VPN SOLUTION
- → STORMSHIELD ENDPOINT SECURITY SOLUTION

Formalising and training to improve resilience

Clemessy, the Eiffage Energie Systèmes brand, also drew up documentation relating to the equipment, flow matrix, inventory, security plan, maintenance and operation of the solutions implemented with a view to ANSSI approval in accordance with the Military Programming Law (LPM).

In addition, training to raise awareness of cyber risks was provided. Operators and maintenance staff also took part in attack simulations. Their reactions were studied in order to create "reflex" sheets to improve the response in the event of an incident.

This stage remains essential, as Théo Gissinger-Schumann, Technical Manager at EES - Clemessy, explains: "***Security is never 100% guaranteed: for compatibility and operational reasons, we may be obliged to degrade certain security measures. Our role is then to list these residual risks after securing operations so that they are known and taken into account. Staff awareness and responsiveness are among the measures to mitigate these residual risks***."

All of these measures have a single goal: to make the OT system more resilient.