STORMSHIELD

BUSINESS CASE

How to ensure communications security in charging stations for electric vehicles?

URBAN MOBILITY

Rapidly expanding networks of electric car charging points have become a target for hackers looking to disrupt charging sessions or even destabilise an electricity network. These new connected systems have a weak spot: their easily accessible external installations.

As part of the new roll-out of charging stations in the Paris urban network and motorway service areas, the service operator behind these projects wanted to ensure flawless cybersecurity. Hence their choice of Stormshield Network Security solutions, which are perfectly suited to the constraints they identified.

Faced with the exponential growth in the number of electric vehicles on the road, a leading operator of charging stations in the French market launched a new project to roll out ten new charging stations on motorways and several new ones in major cities.

This large-scale project needed to be exemplary in terms of cybersecurity, to prevent any kind of intrusion by “man in the middle” interception between the terminals and all the remote maintenance and business applications within the information system.

The operator wanted both a reliable virtual solution for secure access to application servers hosted in the cloud, and a robust industrial security solution to secure the charging areas. Both of these solutions are available in the Stormshield Network Security (SNS) range.

“Protecting charging areas requires the installation of specific, robust equipment capable of operating without interruption in constrained outdoor operating environments.”

Vincent Nicaise
Team Leader Industry at Stormshield

Industrial cybersecurity tailored to constraints

Protecting charging areas requires the installation of specific, robust equipment capable of operating without interruption in constrained outdoor operating environments. Hence the choice of SNi20 industrial firewalls, designed to withstand variations in humidity and temperature, with DIN-rail format enclosures for installation in cabinets located close to the charging points in each of the charging areas.

SOLUTIONS USED

→ SNi20

→ SNS ELASTIC VIRTUAL APPLIANCE

Combining advanced security features, they can be used to set up IPSec VPN tunnels for bi-directional data transmission and to carry out all remote control operations for charging stations or remote maintenance. Multi-factor authentication (MFA) in TOTP (Time-based One-Time Password) also adds an extra layer of protection to the connection process.

At the other end, an SNS virtual appliance adds a further barrier of protection to access to the mobile application and remote payment management servers, hosted in a Cloud environment.

Each charging area also has its own local VLAN network to avoid any risk of massive compromise, either when an attack on one of the areas spreads to all the areas in the network, or when information is passed on to IT applications and vice versa.

The data that travels between the charging stations provided in the city and the application servers passes over a private 4G line and is also secured by the SNS virtual appliance.

The supplied cybersecurity architecture is based on enhanced security measures that comply with standards for the protection of critical systems and are fully able to handle the constraints of the local environment. This greatly reduces the vulnerabilities that could be exploited by cybercriminals, protecting the operator's information system and all its applications.

Version 1.0 - Copyright Stormshield 2025