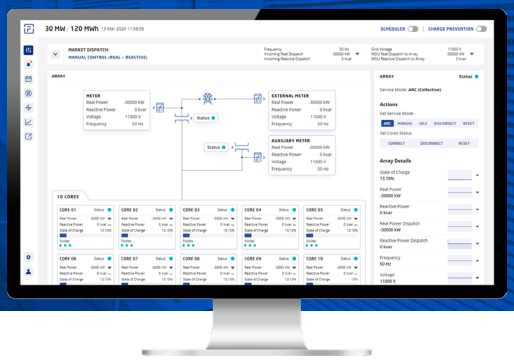
FLUENCE
A Siemens and AES Company

FLUENCE OS

Cybersecurity

Enterprise-class network security and firewall capabilities keep critical grid infrastructure secure and support international cybersecurity standards



The electric grid is a fundamental asset of modern-day societies, ensuring that homes and businesses around the globe have a consistent and reliable supply of electricity. As battery-based energy storage system installations grow and become a critical component of our power infrastructure, it is imperative these assets are secure and protected from cyberattacks.

Fluence's approach to cybersecurity is based on the harmonization of two key cybersecurity models – Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), and the Critical Security Controls (CSCs) for effective Cyber Defense. Our goal is to protect against or minimize the impacts of known threats and improve our customer's ability to respond to and recover from incidents that may occur.

Our cybersecurity practices are based on three core functions:

Identify

- Each site implements a secure, logically isolated network security architecture
- Sites create and maintain an inventory of authorized and unauthorized devices connected to the network (both IT and OT)
- Annual penetration tests proactively evaluates the effectiveness of security defenses, mimicking the action of real-life hackers

Protect

- Periodic vulnerability assessments and regular patch management proactively identify, risk-rate, and remediate vulnerabilities
- High grade encryption protects all data in transit, providing a secure method to allow data flow to and from the ICS network
- VPN remote site access with 256-bit encryption, multi-factor authentication, and enterprise-class network security software

Respond & Recover

- Regular monitoring activities of logged data shall be performed to detect and respond to potential incidents
- Fluence works with customers to document incident response plans, including all phases of the incident lifecycle
- Incident response includes a communication plan for internal and external stakeholders with roles and responsibilities defined

Fluence regularly performs cybersecurity patches and updates on our hardware and software, included in every project scope. Fluence supports customers in meeting their responsibilities for NERC Critical Infrastructure Protection (CIP) compliance, which addresses the security of cyber assets that are critical to the operation of the North American electricity grid.