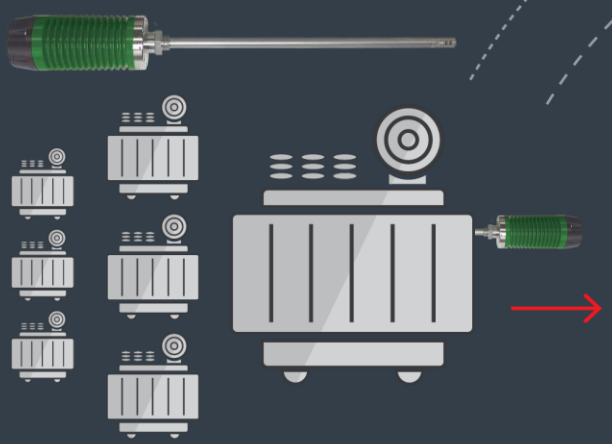
EcoStruxure Transformer Expert

Digital transformation of transformers with IoT sensors and expert analysis

Security Overview

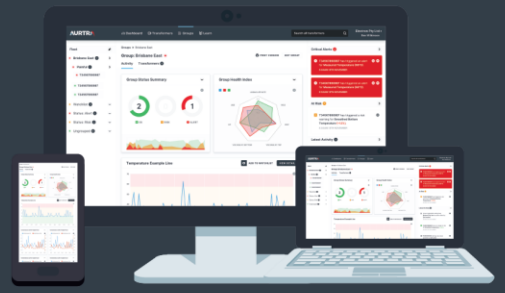
EcoStruxure Transformer Expert Solution Architecture



Fleetwide intelligent
IOT sensors

Life Is On Schneider Electric

Expert analysis



Fleetwide dashboard

Embedded expert system
in 3rd party solutions

Life Is On Schneider Electric

IT Security Overview

Schneider Electric has designed the IOT data transfer process, storage, access and management operations to be compliant with the EU power utility data security requirements.

- **EcoStruxure Transformer Expert Architecture**: Novel file format ensures data cannot be interpreted. In the unlikely case it is intercepted, data is verified and encrypted multiple times as it moves through our cloud and pipeline.

- **IoT Architecture**: Ensures customers can be automatically upgraded with security system updates as part of their Subscription Agreement. No customer involvement needed to be up to date with security enhancements.

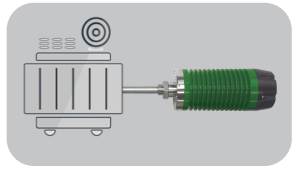
- **Use of AWS:** The AWS hosted architecture ensures system reliability and security are in line with industry standards.

- **No Transformer Control:** There is no access to SCADA or transformer control through the communications or software actions of the solution. The solution monitors and analyses the transformer only.

IT Security Overview

- EcoStruxure Transformer Expert security architecture protects customer data using four key features.

Remote Sensor Security | **Network Connection Security** | **Data Transfer & Backend Security** | **User Data & Dashboard Security**



Remote Sensor Security

- Data contains no local information or direct load information
- No direct sensor-to-customer network interface
- No backdoor access to the customer’s network
- All data is transferred over the 3G/4G network
- Files are stored in a Linux operating system
- Linux protection processes safeguards the files against any data damage

Network Connection Security

- Sensor data upload is conducted at a different, random time with a new IP address each day
- The 3G/4G interface is on-line for less than 2 minutes per day for uploading data
- The 3G/4G interface is powered down when not uploading
- Before transmission data is encrypted with AES-256 using Key Derivation Function algorithm
- Data can only be decrypted if it is undamaged
- Encryption checksum process restricts even a part file from being decrypted correctly
- Damage of even 1 byte would result in a complete scramming of the output

Data Transfer and Back-End Security

- EcoStruxure Transformer Expert uses a novel data upload format
- The sensor connects to a dedicated clearing site
- No direct access from the sensor to the back-end processing server
- Data integrity of upload is checked prior to ingestion and stored in a AES-256 encrypted database
- Raw data from the sensors is stored in a separate data base which contains no identifiable information
- There is no link from the data to a transformer/customer without access to the other databases

User Data & Dashboard Website Security

- Use of encrypted upload from the back-end processing service to the user-accessible website
- Secure password and HTTPS encrypted access for users
- Benchmark password security including password hardness management
- User interface only holds and displays processed plot-based data and outputs i.e. no raw data
- User interface has no system-stored linkage between data and a user site (unless entered at the user’s discretion)

API Security

- EcoStruxure Transformer Expert provides a REST-based API that returns structured JSON data. API keys, generated by an organisation's user admin on demand, protect data from unauthorized access.

Secure ETE databases

Secure API Interface

Customer Asset Management or
3rd party solutions