



Cybersecurity for Solar Solutions

A growing demand

Cybersecurity is a risk management and is one of our top priorities at Schneider Electric Solar Business.

As the demand for distributed cloud computing & Internet of Things (IoT) is growing rapidly, our customers face increasing threats (hackers or virus) against critical infrastructures.

Your information could be a target of these attacks, leading to the following critical consequences:

- Plant production stop and control (stop inverters, change parameters, etc)
- Financial loss due to a non-production
- Data diffusion or loss (user personal data): contact information such as emails, name, company ...

Moving to the Cloud, in the most secured way for your data and plant

At Schneider Electric Solar Business, our previous products offered a solution with SCADA, hosted on site or centralized in data center for which you had to connect through a VPN.

This solution brought some undeniable disadvantages:

- Data loss in the case of server crashing
- Maintenance of the server needed

As we want to bring more value to our customers through our Digital Services and managing those risks, we offer our software products on the latest platform: **Cloud computing** also known as **Software as a Service**.

Several processes have been implemented to assure our customers that their investments are well-protected: developing partnerships with reputable companies, selecting the best tool, following experienced requirements, implementing most secured models of threat analysis.

“ Cloud computing is a model for enabling near to unlimited on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) ”

Cybersecurity, our top priority

We offer best-in-class, integrated cybersecurity solutions for critical infrastructures, allowing users to increase the safety, availability and reliability of Industrial Control Systems:

- Centralize security
- Provide robust change management
- Automate reporting that supports regulatory compliance
- Ensure that only trusted applications run on critical infrastructure environments
- Protect systems from zero day attacks and advanced persistent threats (APTs)

Secured Monitoring Platform

Our team of experts works hard to minimize consequences of the cyber-attacks by developing the most secured product in terms of PV Plant Monitoring platform: Conext™ Advisor 2.



Conext™ Advisor 2 is a web portal with an efficient, task-oriented interface for managing and optimizing the performance of solar power plants, and includes a complete suite of tools for professional users:

- Intuitive and User friendly interface
- Real-time Operation and Control of a PV plant.
- Performance Analysis through advanced Solar KPI.
- Production forecast.
- Identification of underperforming PV plants and equipment.
- Reporting and Data extraction.
- Custom dashboards.
- Utility Grid management.

Main benefits of Conext™ Advisor 2 as PV Monitoring System

- ✓ Leverage digital technology
- ✓ Cybersecurity of the whole system.
- ✓ Access from wherever at anytime.
- ✓ Reduce on-premise hardware expenses.
- ✓ Long term partner to ensure consistency, integrity and availability of data over 20 years with management of the strategy for data storage (minutes, hours, months and years).
- ✓ Cloud storage to ensure data scalability and security.

Global Architecture

Conext™ Advisor 2

Conext™ Advisor 2 Architecture provides better understanding on what we have done to protect your data:

On premise equipment collect all local data and stores it on a local Industrial PC located in the GridBox Monitoring Cabinet. This industrial PC is doing the link between the local infrastructure and the Cloud: We call it Conext Gateway. This IoT Gateway pushes data into the Cloud and makes them available for the Customer in a secured way using standard protocol.

Additionally, a firewall is installed to prevent communication from the Cloud to onsite devices and to leave free access to the private data. Our partner in this is Phoenix Company.

A team of Cybersecurity Experts is available to answer to any of your questions. Please contact us for further information.

1



Data is collected by the PLCs using Modbus protocol or Analog Module cards. The data are locally aggregated.

2



Data is collected by the gateway. The data are locally stored (MySQL) and aggregated.

3



Data is sent to the Cloud through secured protocols inside a message queue. Once the queue acknowledges the message, message is locally removed.

4



Data is extracted from the queue. The most recent data are sent to a temporary memory to animate the Operation pages. All the data received are sent to the long term storage database.

5



Data is available through a web platform and apps (mobile, tablet)

Secured processes and reliable partners

We collaborate with partners, leaders who develop and manage secured software to minimize threats to our customers and protect their data and services at maximum. We take advantage of their expertise to do our job properly and allow our customers to manage their business serenely.

Edifixio, Microsoft, cybersecurity experts and Schneider Electric Solar Business worked as strong partners on defining Conext™ Advisor 2 initial architecture as secure as possible. It also be the case for future major updates/upgrades.

Our Cloud provider
DATA HOSTING



- One of the leaders on the market on security, performance, reactivity of services, strong and experienced components.
- Responsible of the security.
- Experienced partner in robust security technologies and practises.
- Conext™ Advisor 2 with Microsoft Azure Cloud: resilient to attack, safeguards user access, responsible of data security (encrypted communications) and threat management & mitigation practises (regular penetration testing).

Our Cloud environment Manager
DATA AVAILABILITY
& MANAGEMENT



- Infrastructure Production Management, Supervision and 24/7 support.
- Several back-up data centers in the same region in case of failover purposes.

Our Identity Provider
DATA SECURITY & PRIVACY

- Identify and store Conext™ Advisor 2 user's data.
- Data protection (or Privacy according region): natural persons to the processing of their personal data.
- Protection data: covered by Data Privacy National Laws & regulations.
- Security Systems & related Data: covered by Cybersecurity Policies and National Laws.
- Main challenges: collect, transmit, store, modify and delete data in a secure way.

Our Cybersecurity Advisor

- Identify and audit main points/risks in Cybersecurity.

Protect your valuable investment from cyber threats.
Work with a trusted partner. Work with Schneider Electric Solar Business.

Our team and partners work hard to minimize consequences of the cyber-attacks. So decide wisely what is important for you, protect your data and secure your plant.

To receive additional information from cybersecurity experts, please contact us at info.schneiderelectricsolar@schneider-electric.com