Cybersecurity in a decentralising electricity system

Smart Energy Europe
Rue d'Arlon 69-71,
BE-1040 Brussels

+32 (0) 2 58 88 992
info@smarten.eu
www.smarten.eu

September 2018

About smartEn - Smart Energy Europe

smartEn is the European business association for digital and decentralised energy solutions. Our members include innovators in services and technology for energy and data management, finance and research. By taking an integrated perspective on the interaction of demand and supply, our mission is to promote system efficiency, encourage innovation and diversity, empower energy consumers and drive the decarbonisation of the energy sector.

For further information please visit www.smarten.eu

ade
APPLiA Home Appliance Europe
BayWa r.e. renewable energy
bne
EDF
enel x
entelios
geo smarter energy
JOULE ASSETS
REstore
Schneider Electric
SIEMENS
vaasaETT
VOLTALIS
AutoGrid
CYBERGRID
DNV·GL
EDGE ELECTRONS
energy·21
FLEXIBLEPOWER ALLIANCE NETWORK
GNE FINANCE
Honeywell
Microsoft
natGAS
NUVVE
PÖYRY
TESLA
tiko
United Technologies Research Center
WIREPAS
Brattle
CUCULUS
DELTA
ENERCOUTIM
e·on
EVN
GE
gemalto
KISTERS
Landis+Gyr
Climate
meteo
olivoENERGY
Ørsted
REGALGRID
smappee
VATTENFALL
Vestas

The positions expressed in this document represent the views of smartEn as an association, but not necessarily the opinion of each specific smartEn member

Cybersecurity in a decentralizing electricity system

BACKGROUND PAPER

It is no secret that the energy system is one of the most important and complex pieces of infrastructure in our society today. On top of this, the rapid digitalization of energy infrastructure and the increasing number of interconnected market players have brought significant benefits to the energy system, making it more efficient, reliable, and sustainable. As a consequence, cybersecurity has become a key priority for the energy sector, and thus for the European decision makers. At a European level, this topic is currently being approached by European legislation from various angles (outlined in the box below).

The Network and Information Security (NIS) directive

The first EU-wide piece of legislation on cybersecurity was the Network and Information Security (NIS) directive, adopted in July 2016, which Member States were required to transpose into national laws by May 2018. This directive is focused on boosting the overall preparedness of Member States (e.g. through setting up competent authorities, incident reporting, cooperation between Member States, etc.). An important component of this is the requirement for Member States to identify Operators of Essential Services, including within the energy sector. These operators of essential services are required to comply with certain security measures and report on security incidents. The deadline for Member States to identify these Operators of Essential Services is on 9 November 2018.

Cybersecurity Act

As part of the Digital Single Market strategy, the NIS directive was followed up by another proposed regulation, referred to as the Cybersecurity Act. This is another piece of horizontal legislation, which aims to outline an EU-wide cybersecurity certification framework for ICT products and services. Currently, there are various national certification schemes, which are not aligned and not necessarily recognized by other Member States. The creation of EU-wide certification schemes aims at addressing this market fragmentation within the EU, as mutual recognition, eliminates the cost of participating in multiple certification schemes, and removes market-entry barriers for cross-border trading.

Smart Grids Task Force / Network Code

In addition to the horizontal legislations outlined above, there are also several energy specific work streams on cybersecurity. For example, the Clean Energy Package acknowledges the importance of cybersecurity for the energy sector and calls for a dedicated network code on cybersecurity, while the Experts Group 2 of the Smart Grids Taskforce is currently laying the groundwork for such a potential cybersecurity network code. This network code would cover TSOs and DSOs, but could indirectly affect connected infrastructure and service providers when the code is implemented.

Changing market environment

In summary, a considerable amount of work is being done on cybersecurity within the EU context. However, the rapidly changing market environment in the energy sector poses specific challenges. The increasing decentralization is leading to an increased number of market players (active prosumers as well as aggregators, third party service providers, etc.) with more financial interactions between them. The convergence of operational technology (OT) and information technology (IT) is optimizing operations and enabling full information accessibility and control, yet it is also increasing the number of connected devices, which are only expected to continue to grow further (50 billion connected devices are expected by 2020).

smartEn recommendations

1. **A specific approach to the energy sector:** industry sectors have extremely diverse framework settings in terms of technology, applications, interconnectivity, and constraints. When it comes to cybersecurity, the energy sector has its own specificities such as dealing with legacy installed base systems, with new technologies, or real-time application requirements. It is essential to have a sector-specific approach for the energy sector, that would not only be very efficient but also suitable to enhance the cybersecurity resilience of the sector, and includes the consideration of existing industry specific standards (see below).

2. **Apply existing Cyber Security Industry Standards in the Energy Sector:** many existing international standards provide a strong foundation for the deployment of cybersecurity in the energy sector. These standards can address both the security of Operators of Essential Services, such as utilities, as well as that of actors in the new energy landscape. These standards provide recognised and market adopted solutions for the security of the "System of System" and relevant solutions to the security of field infrastructure that are quite often underestimated. This approach is used globally and based on the methodology developed by the ISO / IEC 27000 series which is complemented by the IEC 62443 series of the OT part.

3. **Clarity on who is considered an Operator of Essential Services:** The NIS directive calls on Member States to identify Operators of Essential Services, who will be required to comply with certain security measures. Although it's clear that grid operators are to be classified as an Operator of Essential Services, the directive does not explicitly include energy generators, leaving this to be interpreted at the discretion of the Member State. What is even less clear however is how Member States are to consider new market players, such as aggregators, virtual power plant operators, third party cloud-computing services etc. As the electricity system decarbonizes, it will become increasingly reliant on such players for grid stability and security of supply. For cases where these new market players are therefore considered Operators of Essential Services by Members States, guidelines should be established so that there is a consistent, harmonized and transparent approach.

4. **Cybersecurity certification:** Under the Cybersecurity Act, this process is streamlined within an EU-wide cybersecurity certification framework, whereby these certificates will be mutually recognized by Member States. Currently, cybersecurity certification for market players is not mandatory, but depends on the wishes of the client. This voluntary approach is also reflected in the original proposal by the Commission and has been supported by the Council. smartEn generally supports this approach, but believes there could be a compulsory “high-level” certification which is decided on a case by case basis, and for a limited number of defined products used in critical infrastructure or where personal data is at risk. This should be based on a risk analysis.

   Regarding the conformity assessment method, declaration of conformity should be allowed for the assurance levels “low” and “substantial”, while for the assurance level “high” independent certification should be a requirement.

5. **The risk of fraud in new digital energy applications should not be overlooked:** Minimizing the risk of black-outs in the energy sector is clearly of the utmost importance to our society and economy, and as such should be given the highest priority. However, the risk of fraud should also be given its due consideration within the context of the energy system. As new applications are developed for the energy sector, data integrity standards need to be defined for data coming out of decentralized devices that would like to provide services to the grid. This will contribute towards more trust between actors in the energy system, leading to opportunities for market players to develop new services and create new business models based off the data provided by the devices. However, these data integrity standards should not induce dependency on a specific communication technology.

6. **Industry standards for device identification and authentification:** If devices are communicating with each other on a virtual level to provide new services (as mentioned above), it is also important for there to be a reliable way to identify devices. In this way, the different actors will be able to trust the source of the information coming from the device, and this enable for services to be monetized. A standard for authentification would allow for an additional level of security, in which a compromised device could be detected and put offline in the case of erratic behaviour compromising grid stability. If a device is running multiple applications from different service providers, identification and authentification should take place at the application level instead of only on the device level.