ETIP SNET

EUROPEAN TECHNOLOGY AND INNOVATION PLATFORM

SMART NETWORKS FOR ENERGY TRANSITION

DIGITALIZATION OF THE ENERGY SYSTEM AND CUSTOMER PARTICIPATION: Description and recommendations of Technologies, Use Cases and Cybersecurity

ETIP SNET Position Paper Summary

About ETIP-SNET

Find out more at: https://www.etip-snet.eu. European Technology & Innovation Platforms (ETIPs) have been created by the European Commission in the framework of the new Integrated Roadmap Strategic Energy Technology Plan (SET Plan) by bringing together all the interested and involved stakeholders and experts from the energy sector. The ETIP Smart Networks for Energy Transition (SNET) role is to provide advice on foreseeably important Research, Development & Innovation (RD&I) to support Europe's energy transition, more specifically, its mission is to:

- Set-out a vision for RD&I for Smart Networks for Energy Transition and engage stakeholders in this vision.
- Prepare and update the Strategic Research and Innovation Roadmap.
- Report on the implementation of RD&I activities at European, national/regional and industrial levels.
- Provide input to the SET Plan action 4 which addresses the technical challenges raised by the transformation of the energy system.
- Identify innovation barriers, notably related to regulation and financing.
- Develop enhanced knowledge-sharing mechanisms that help bring RD&I results to deployment.
- Prepare consolidated stakeholder views on Research and Innovation to European Energy Policy initiatives.

Contact

For further information about this paper and ETIP SNET activities please contact:
ETIP SNET secretariat at info@etipsnet.eu
Maher Chebbo, ETIP SNET WG4 Chair at Maher.CHEBBO@ge.com

Legal notice

Copyright Notice

INTRODUCTION

In our future energy system, the next generation of integrated technologies will monitor, observe, control, enable services and protect the smart supply and use of energy. Internet of things, artificial intelligence, machine-based learning, digital twin and other developments will find their use in the energy system. Advanced meters and modern appliances trigger the potential of active demand-response and enable new services for the energy user. We will find new relations between the end-user and the energy system. Customer participation in all stages of the development and expansion of the energy system is supported by digital tools ranging from participative geographical systems to web portals and social media. Internet of Things (IoT) Industrial Internet of things (IIoT), big data, blockchain, digital twins, all present in the system, change its planning and operation and transforms the energy markets. In summary, the digital transformation of the energy system. However, the widespread use of these digital innovations needs to be accompanied by suitable measures for data and information protection from malicious intrusions and attacks (cybersecurity) and uncontrolled use of customer data.
ETIP-SNET's WG4 on "Digitalization of the Energy System and Customer Participation" has addressed and described the digital development and its impact on the energy system within three taskforces. These teams produced three chapters bundled in a solid technical position paper. This paper is a brief summary of this technical position paper.

The first section, prepared by Taskforce 1, is about Digitalization in the energy system. A definition of digitalization is articulated: "the process of moving to a digital business, that is using digital technologies to change business models and provide new revenue streams and value producing opportunities". In the report three layers are distinguished: physical, infrastructure and business layer. The enabling **relevant technologies** are described in these layers with detailed reference to existing standards or ones in process. Notable telecommunication technologies are included, especially promising 5G.

The second section, prepared by Taskforce 2 shows digital energy disruptive **use cases** and new market and business models with customer engagement. As stated in its summary, use cases "will support a service-oriented energy system as customers expect a high-quality, personalised service available 24/7". In the technical document the use cases are structured in the same three layers as the digital technologies in the first section. An overview of some relevant existing pilots and concepts across Europe are presented and reflect trends as IoT, advanced sensors, secured internet, peer-to-peer communication, distributed storage, agent-based services, advanced customer models, or energy communities. Emerging trends and recommendations are given in the end.

The third section, prepared by Taskforce 3, solidly describes **cybersecurity** and resilience. There are two high-level concerns regarding the cybersecurity in the energy sector: to secure the evermore digital infrastructure of energy systems providing essential services and to protect the necessary data, hence, privacy of citizens. An important distinction between operational (more specific for energy) and information (more general for ICT) technologies is presented after the first chapter's consideration of recommendations by global and European institutions, examples of relevant cybersecurity projects and known cybersecurity attacks. The major part of this section is then addressing the main foreseeable cybersecurity challenges, grouping them in three clusters: Technology, Policy and Future. For each challenge there is a description and a summary of the main issues. Research topic recommendations conclude the section.

INDEX

LIST OF FIGURES

ACKNOWLEDGEMENTS

We give thanks to Antonello Monti supported by George Huitema (TF1), Elena Boskov-Kovacs (TF2) and Marcus Meisel (TF3) for their time and organization of the Taskforces, Ilaria Losa and Gustavo Jacomelli for their assistance.

ETIP SNET WG4 Digital Energy:

Maher Chebbo (Chair)
Esther Hardi (Co-Chair)
Miguel A. Sánchez Fornié (Co-Chair)

1. DIGITALIZATION OF THE ENERGY SYSTEM – TECHNOLOGY

Photo Alliander (Hans Peter van Velthoven)

1.1 OVERVIEW

Digitalization is the process of moving to a digital business, that is using digital technologies to change business models and provide new revenue streams and value producing opportunities. The digitalization of the energy system is not a recent occurrence, but it is a process that has been ongoing since at least a decade. The main focus so far has been on infrastructure operation and, coherently, the concept of *Smart Grid* has been the focus of research and applications.

This position paper takes a broader approach and considers all the implications, and then all the energy system levels at which digitalization has an impact. A key reference in this sense is given by the "Winter Package" of measures of the European Commission (2016) that clearly states the central role of the customers in future energy systems. Thus, with respect to the traditional concept of a smart grid, the digitalization process involves new factors such as:

- Customer involvements and possible disruptive new business models that could emerge from this involvement;
- Greater attention to sector coupling and then correspondingly to the convergence of Smart Energy and Smart Cities and Communities;
- New concepts and technologies that are emerging also at the physical layers thanks to a greater role played by electronics in the new digital energy system.

Hence the digital energy network paradigm is a broader concept than Smart Grid with significant social components and focused on service. The final goal is to enable a flexible open, transparent trade market of energy with equal possibility of participation of every player as envisioned by the Winter Package. For this reason, this report uses a three-layer approach of the energy system, which can be uniquely mapped to the broadly used Smart Grid Architecture Model (SGAM) for designing smart energy systems.

The Physical Layer deals with the grid itself and with the equipment that is part of the infrastructure. Because of the growing presence of Distributed Energy Resources (DER), we move to a more power electronics driven operation, making evident that the control of the converters will have to be adapted to better support grid automation. Currently, converters operate according to a grid supporting principle, i.e. they provide support injecting active or reactive power, but they mostly operate as follower for what it concerns frequency support. It is envisioned that, in the future, there will be more and more need for the power converters to operate in a grid forming mode, i.e. playing a key role in the frequency control. Combining DER with local storage, also Renewable Driven DER will be able to provide full support to ancillary service provision.
Another important transformation at the physical layer is potentially represented by the application of Smart Transformers. These new devices could define new types of service-provision and when integrated with storage, could also play a key role in the management of the energy balance supporting a smarter transfer of energy among the levels.
New types of load are also appearing, and they are typically characterized by new elements of flexibility. One very important example is given by electric vehicles, but another important case is offered by electricity driven heating systems. Both these examples offer new options of storage (directly electrical or through heating) that can be used as resource to achieve load shaping and energy profile control.
In a vision of a fully power electronic driven energy system, Direct Current (DC) technology could play also a key role. During the transition DC could support the distribution providing option of meshing at medium voltage which today is not possible in Alternate Current (AC).

At the Infrastructure Layer a key role is played by ICT. A lot of different technologies are available, and it is expected that not one single solution will prevail across the energy system. Nevertheless, high potential is envisioned with 5G thanks to low latency, network slicing and the option of edge cloud. Edge cloud could represent a key technology to bridge between the field and the concept of central data platform. Central data platforms are emerging in different forms as a way to provide various types of services at different level. In this area, it is critical to reach a high level of convergence to avoid the risk of data silos. The increasing role of ICT raises also important Cybersecurity concerns which are covered further on in this position paper.

Finally, at the Business Layer, key is the creation of digital mechanisms and adequate service management and operations that facilitate the participation of any energy party, residential or business, to open, transparent energy markets. Two options seem to be emerging: one solution given by aggregators acting by means of data platforms, but a more compelling case is emerging, thanks to the trust raising Blockchain technology, the possibility of peer-to-peer trading. More details about the business layer and corresponding new use cases and business models are discussed in another part of this positioning paper.

The technical report describes in detail the options and technologies enabling the digitalization in the energy transition. Last but not least, it should be mentioned that digitalization will not only affect the energy business but will also require other new skills and knowledge for energy engineers. Hence a strong recommendation of this report is to consider adequate educational programmes (varying from applied to academic levels) to leading to adequate work forces.

1.2 ENABLING DIGITALIZATION – RECOMMENDATIONS

Digitalization is affecting the energy system at every level. In particular, the transformation from an electromechanical system to an electronic system is a fundamental change that will

transform the fundamental principles around which the energy system is operating. On the different layers of the energy system we find the following recommendations:

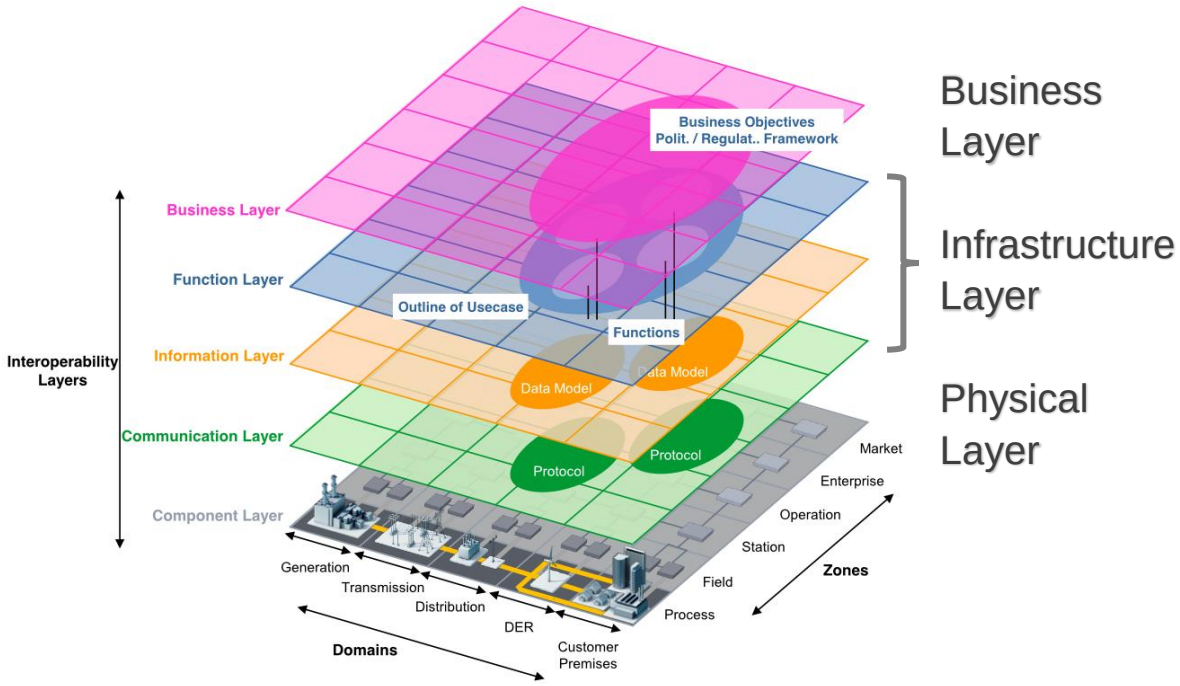


Figure 1: SGAM (Smart Grid Architecture Model) reuse of Smart Grid Reference Architecture by CEN-CENELEC-ETSI Smart Grid Coordination Group

PHYSICAL LAYER

Need for new principles of operation. Future energy systems will be fundamentally different and new principles of operation are needed for a future grid mostly based on digital systems. Moreover, the transformation from a load driven to a generation driven system will also call for new principle of operations. Classical networks are based on a global balancing concept. This idea is now extended with the exploitation of flexibility. In a longer future, though, it may be easily understood that the flexibility exploitation has a limit and it will call for new ways of operations beyond synchronous balancing. Finding technical solutions able to support grid operation in which the mechanism of synchronism between generation and consumption is removed, is a critical task in a vision of the expected penetration of renewables in the long term.

Using AC versus DC. In a fully electronic system, the choice of using flows of electrical charge type AC (Alternating Current) versus DC (Direct Current) should be discussed again the more we proceed in the process of digitalization.

INFRASTRUCTURE LAYER

Moving to the infrastructure level, digitalization means a progressive smartness of the grid. This process is mostly affecting the distribution grid. While the process is still moving quite slowly, this process is supposed to pick up at a completely different speed very soon.

Sharing infrastructure investments. Introduction of new emerging technologies such as 5G, allowing a sharing of infrastructure investment can be seen as a possible trigger for a speeding up of the Digitalization process.

Need for overall covering architectures. A major threat for successful digitalization is given by data management issues. While reference architectures have been proposed in the past, a complete architecture able to cover the complexity of the futuristic scenario including sector coupling is missing. This is critical for interoperability and to avoid data silos.

BUSINESS LAYER

At the higher Business Layer, digitalization brings new options for small players entering open markets.

Need for open API's that will support interaction with other business sectors. As made clear by the concept of sector coupling, the electricity and the energy sector more in general need interactions with other business sectors such as Health and Mobility to mention the most typical. This interaction will be made possible creating open cloud solutions that support open APIs (Application Programming Interfaces): These open APIs will also enhance the role of SMEs and start-ups in providing innovative services. A reference in this sense is given by the work developed within the Future Internet Public Private Partnership (FI-PPP) of the European Commission and the development of the open source cloud FIWARE platform.

Need for a data economy based on open platforms. Open platforms offer rapid development solutions in a cloud environment. A proper combination of open source and proprietary solutions creates a dynamic eco-system in which concepts such as open API reported above can support rapid development and innovation in service provision.

Need for trust raising technologies. To support a fairer access to market, digital technologies can offer important solutions enabling secure, trustful data transfer and hence automatic, transparent trade agreements and contracts. An example of such technology is given by Blockchain, but it should be reminded that it is not the unique solution. Research in this area should clarify which is the best approach to create open, flexible and trustworthy markets.

Need for adequate Service Management & Operations. The digitalization of the energy system and processes leads to new business models, new revenue streams and value producing opportunities. That is, businesses in the digital energy eco-system face the challenge to set-up appropriate service management processes, systems and organizations that meet demand for superior customer service and deals with strong competition. Research & Development has to cover the design of adequate service management.

<u>Other important needs independently from the layer structure are:</u>

Need for adequate education. The digital change of energy systems is not only technical but also educational. The new grid will need new competences: the transformation of the grid not only poses technical problems but also entails the need for new skills, and hence asks for adequate education. Not only we will need power engineers to understand digital topics, but also the basic principle operation will be different and hence courses and text books need to be updated.

Need for adaptation of legislation. Currently regulatory problems are envisioned as the main factor limiting a massive application of smart technologies. Adaptation of legislation could positively affect the process of digitalization.

2. DIGITAL ENERGY DISRUPTIVE USE CASES AND NEW MARKETS, BUSINESS MODELS AND CUSTOMER PARTICIPATION

Photo Alliander (Bram Vreugdenhil)

2.1 OVERVIEW

Digital technologies will bring key contributions to the achievement of the Energy Union objectives for the transition to a 21st century secure, affordable and climate-friendly energy system. They will support a service-oriented energy system as customers expect a high-quality, personalised service available 24/7.

New digitalization business models are emerging upstream and downstream on the energy value chain. Upstream, new business models are emerging to monetize distributed generation, storage, and demand response. Downstream, utilities and network operators are moving toward the energy service company model, actively trying to engage the customer. In both, new business models are strongly enabled by digitalization and use cases are critical for further acceptance and success of energy transition.

While the previous chapter focuses on technology, this one focuses on Digital Energy Disruptive Use Cases and New Market and Business Models (services) with customer engagement and presents an overview of existing pilots and concepts across Europe, highlighting some of the important trends:

- IoT, virtual interfaces to all devices, which may become Cyber Physical Systems (“CPS”)
- Advanced sensors
- Secure Internet
- 5G Communications, peer to peer communications at the edge of the grid
- Electric vehicles as a resource

- Distributed storage, in combination with PV installations and DSM are supporting Local Energy Community development
- Big data, data analytics, data mining support new innovation and investments
- Agent based services, simulation and forecast applications
- Digital twin concept applied to assets and smart devices
- Advanced customer modelling including behaviour, local controls, resources, etc.
- Advanced energy communities, microgrids for resiliency, energy management and grid participation
- Blockchain technology and transactive-based energy trading is already piloted and tested

Note that it is not the intention of this report to provide an exhaustive overview of all possible use cases that use digitalization. We list and describe some promising use cases through projects in Europe, based on which we can build a vision on the future power system. Most of the use cases described are still in the innovation stage, which is in line with the ETIP SNET ambition to discuss the future technologies and applications. The following have been selected to present in PoV publication:

Monitoring, visualisation, and analytics for every stakeholder group. The capability to leverage existing digitalization efforts, with advanced data analytics modules that seek to improve the services provided to consumers and strengthen its relationship is of utmost importance for energy transition and are being developed per stakeholder group.

Use cases between DSO and TSO. The introduction of flexibility services, providing ancillary services at any level, requires the identification and definition of effective coordinated schemes between TSOs and DSOs. This challenge has been faced by the SmartNet Project (2016-18), that aimed to compare different architectures for optimized interaction between TSOs and DSOs focused on managing the purchase of ancillary services located in the distribution segment, such as reserve and balancing, voltage regulation or congestion management.

ebay for energy - ENSquare: A transparent market for labelled energy. ENSquare offers an accessible market where energy in the form of gas, electricity and heat with possibilities for storage and conversion are traded and combined to provide a total energy package to the consumer, on an hourly basis. It offers energy choices and makes ample product information available which ensures that existing customers as well as newcomers are able to provide for the needs of their clients.

Local energy community (LEC). The concept of LEC is intended to acknowledge and empower co-operatives and other community energy business models to participate across the energy sector. They include the activities including local electricity generation, storage, electricity supply, energy sharing, aggregation of flexible energy, provision of services including energy efficiency, and distribution grid/micro-grid operation and management with implementations across Europe.

Deliver flexibility to the market. Projects such as GOFLEX focuses on active use of distributed sources of flexibility to provide services for grid operators, balance electricity demand and supply, and optimize energy consumption and production at the local level. Sources of load flexibility include thermal (heating/cooling) and electric storage (electric vehicles charging/discharging).

Transparent Flexibility Market with LV monitoring. Agder Energi´s demonstrated development of a transparent flexibility marketplace in a distribution grid which can be integrated with the existing power markets. The underlying goal is to make the distribution

flexibility available to an integrated market, thereby exposing the real value and utilization of all flexibility throughout the various levels of the power system.

Figure 2: Example of the architecture and functionalities of the flexibility marketplace (source: Agder Energi)

Preventive Maintenance – smart metering use case. The use of smart meter events with predictive maintenance purposes has been undertaken in the UPGRID project, focused on real proven solutions to enable active demand and distributed generation flexible integration, through a fully controllable low voltage and medium voltage distribution grid.

EV / mobility use case. CECOVEL (Control Centre for Electric Vehicle) is a control centre specific for electric mobility that is helping to integrate into the electric system this new energy demand. It includes software systems that provide the Spanish TSO with visibility and manageability in real time of the electricity consumed by vehicles in Spain as well as a simulation of the impact of future scenarios with high penetration of electric vehicles.

Increasing Photovoltaic self consumption with digitalization using Blockchain. The collective PV self-consumption case involves of a group of prosumers capable of both producing PV electricity and consuming electricity at the same time in the mode of exchange (with or without trading), leveraging blockchain technology and smart contracts for trading. This model is now starting to be usable at the level of experimentation in France with the important condition to have all the actors in this virtual network below a HV/LV transformer.

Jouliette - blockchain-based energy token. The Jouliette is a blockchain-based energy token which empowers individuals and communities to easily manage and share their locally produced renewable energy. It was launched at De Ceuvel, a community in Amsterdam which has become a globally visible showcase for sustainable urban development.

Consumer empowerment, customer relationship and behavioural change. It is important to bear in mind that, despite the widespread idea that price is the most important criterion for a consumer to choose an offer for electricity, it appears that price is key for detractors, but promoters focus more on brand, image and service – a number of new services and awareness initiatives are in deployment across Europe contributing to energy transition.

Democracy by Design. The project Democracy by Design we aim to develop a framework that will support policy makers, technologists, project managers, civil servants, and other relevant parties in safeguarding democratic values “by design”.

Digital Twin. Digital twins are dynamic digital or virtual software replications of physical assets, products and constructions. They aim to remove the silos, inefficiencies, uncertainties, errors and huge resources in working with models in energy value chain.

2.2 USE CASE RECOMMENDATIONS

The customer, in this case the Power producer, needs to allow the connection to its assets. Furthermore, it is important to understand one’s own requirements and benefits.

Data Exchange Platforms (DEPs), also called data hubs, seek to improve data exchange processes between the different parties connected to the electricity system and market. The upcoming use of DEPs are subject to different regimes and practices throughout Europe.

Projects involving cross sector coupling offer an accessible market where energy in the form of gas, electricity and heat with possibilities for storage and conversion are traded and combined to provide a total energy package to the consumer. However, a regulatory framework would need to follow and facilitate these services.

LEC offer many benefits with particular customer visibility and engagement potential. However, the ownership structure of LECs should be defined more clearly given LECs may have significant impacts on incumbent distribution system operators in some Member States. A backbone data-services platform that offers localised estimations and short-term predictions to support data-driven decisions for stakeholders is needed to ensure true flexibility of the market place.

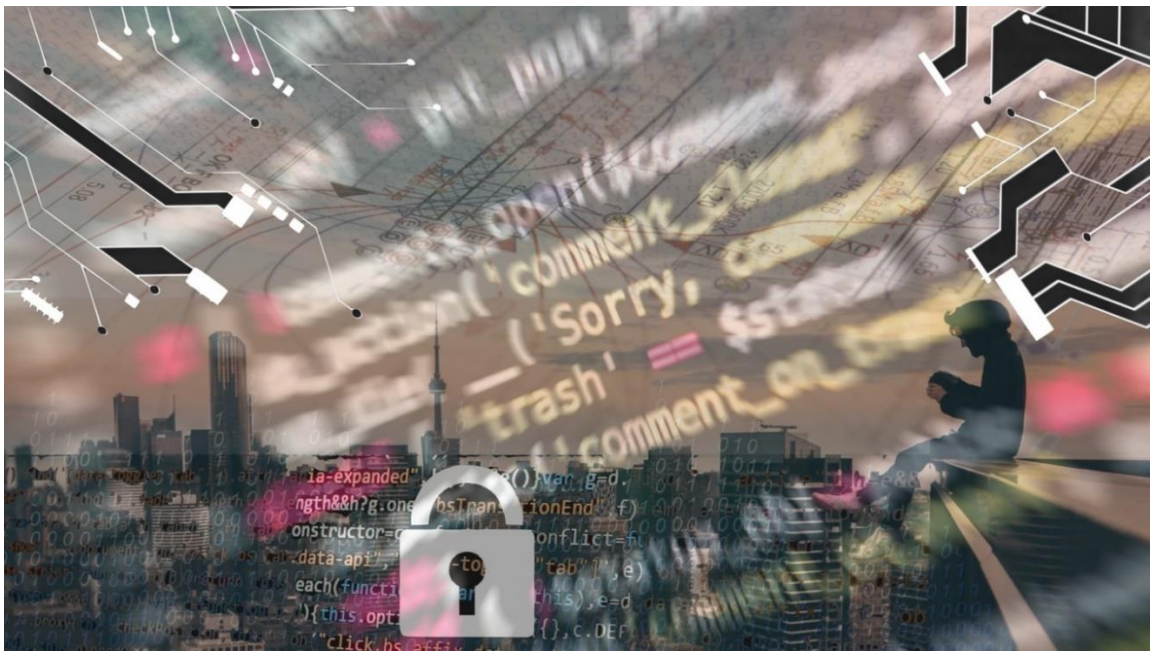
A strong collaboration between industry leaders and utilities is needed to ensure accelerated innovation and replicability of the new flexibility models. Also, a number of new associations established to foster industry collaboration between different stakeholders are being set up and prove to be bringing additional innovation and new projects in the market.

Existing infrastructure such as smart metering should be further exploited and utilized for use of smart meter events with predictive maintenance purposes.

With new consumer demands aiming to accelerate penetration of Electric Vehicles (EVs), good practice can be to establish an innovation/expert centre for EVs within a transmission or distribution network operator (TSO/DSO stakeholder).

The current extent of data digitalization among DSOs, TSOs and other energy stakeholders is uneven; however, benefits have a wide range for digital twins.
Blockchain is certainly one of the biggest trends in the 2017/18 energy industry with many pilots testing the technology. As demonstrated in Juliette token project and several French and Dutch examples mentioned, there is a high potential for faster transactions and lower transaction costs for stakeholders. However, many challenges remain to be explored in further research including: standards needed, clarifying uncertain regulatory status, large energy consumption, cost and control, security and privacy – as most of these examples are being developed not as open source, integration concerns, and cultural adoption.

3. CYBERSECURITY - CYBER-ROBUSTNESS



3.1 OVERVIEW

Cybersecurity is a crosscutting issue enabling the safe and secure use of new products, services, and technologies, in an increasingly more distributed energy system with a tighter inclusion of customers as energy producing consumers (prosumers). Some issues concerning the resilience of the energy system as critical infrastructure need good practice examples, governance, or directed focusing and cannot be left to a voluntary by-chance basis.

The goal of these digital cybersecurity recommendations (resilience) is to estimate, where the energy system digitalisation will be in 2050, and what is needed now, regarding cybersecurity, so that customers equipped with smarter solutions, can rely on a resilient network in Europe.

To achieve the global climate goals in spite of a growing economy, increasing electricity consumption, rapid digitization, and decentralization of infrastructure for a smart energy system; a renewable, digital power system needs to provide cybersecurity and enough resilience for continuous electricity supply at a reasonable cost for everyone in Europe. In the recommendations, there is a focus on Europe, but global connections are mentioned where appropriate.

Sectors such as finance, health, energy, and transport are becoming increasingly dependent on Information Technology (IT), and long-lasting, cascading effects will be pre-programmed if resilience is underestimated now. Growing amounts of Operational Technology (OT) are connected or replaced with IT, which introduces cybersecurity issues into critical infrastructure components and systems. IT enables the highly needed flexibility, automation, and interoperability possibilities, but issues arising from the complexity of systems of systems are not researched, tested, nor standardized. This work does not aim at creating standards, rather it highlights existing or missing ones. The digitalization use cases and technologies studied, resulted in 27 cybersecurity topics.

The identified topics were clustered into three areas of research needs, nine each:

(T) Technical topics, focusing on near-future research needed	(P) Policy topics, with near to midterm future research relevance	(F) Future challenges, midterm future leading into 2050, can seem far-fetched
Related to a need for cybersecurity research, or can be used for solving cybersecurity and resilience challenges	Policy and governance related topics in need for cybersecurity research, or can be used for solving cybersecurity and resilience challenges	We understand these as interdisciplinary research necessary in today maybe unrelated fields, to try to deal with unknown cybersecurity challenges from suddenly exponentially growing sectors (biotech, AI, quantum computing)

Based on the study of background information, differentiation to parallel activities, and relevant European cybersecurity covering projects, it can be concluded, that cybersecurity is still often considered as an addon and not yet included as a process “by design,” as it is recommended to stay safe, secure, and resilient. Therefore, it is very beneficial for the stability and security of the future energy system to earmark research funding, to consider, plan, use, or develop cybersecurity technologies which are suitable for the individual needs of the specific application or the energy system in general.

The accompanying technical paper of this position paper provides a glimpse into the different needs of cybersecurity considering Information Technology (IT) and Operational Technology (OT) is provided. A more in-depth look into cyber attacks in industrial control systems and common risk assessment is further underlining the need for research of new methods, new components, new systems, and new norms.

This position paper takes the approach of offering topics and described scenarios with the aim of sparking research ideas with the hope of resulting in more transdisciplinary research teams, trying to tackle issues imaginable through the topic and scenario descriptions, instead of already matching specific stakeholder groups to formulated research recommendations.
This approach was adopted from the previously mentioned technical paper that provides a list of takeaway messages after the description of each topic.

In this summary document the recommendations are presented as recommendations for research in the three clusters (Technology, Policy, Future Challenges), and a possible prioritization discussed. Acting on those topics does close identified research gaps with results needed when creating policies, regulations, and directives to improve cybersecurity and resilience for the future. For in-depth analysis please refer to the technical paper available online at the ETIP-SNET website.

3.2 CYBERSECURITY – RECOMMENDATIONS

Cybersecurity, as it is known in Information Technology (IT) systems is very different in cyber-physical systems. It does not stop at the vulnerable information exchange but includes the issuing of commands for components, devices, machines, and systems of systems within Operational Technology (OT). These commands represent actions being taken by OT and need a new bottom-up security paradigm of different granularities of importance, protection, and privilege separation for each command ranging from comfort to safety or survival, especially taking into account the requested use of artificial intelligence as the only possible

way of managing and controlling the exponentially growing amount of data on the course of the smart grid's deployment. In parallel evolving IT security, is necessary to provide top-down innovations, protecting protocols, common criteria, defining encryption standards, and technologies, and provide interoperable good practice security configuration guides to complete cyber-physical system robustness. Already, new smart grid devices are beginning to offer monitoring or even diagnosis functions for detecting and stopping misuse of rights attacks, but modern energy systems need to be designed to be resilient and secure from the beginning, to handle (semi-)automatic recovery from unpredictable attack models not foreseeable today. Figure 3 depicts a (non-extensive) timeline of rising numbers of attacks.

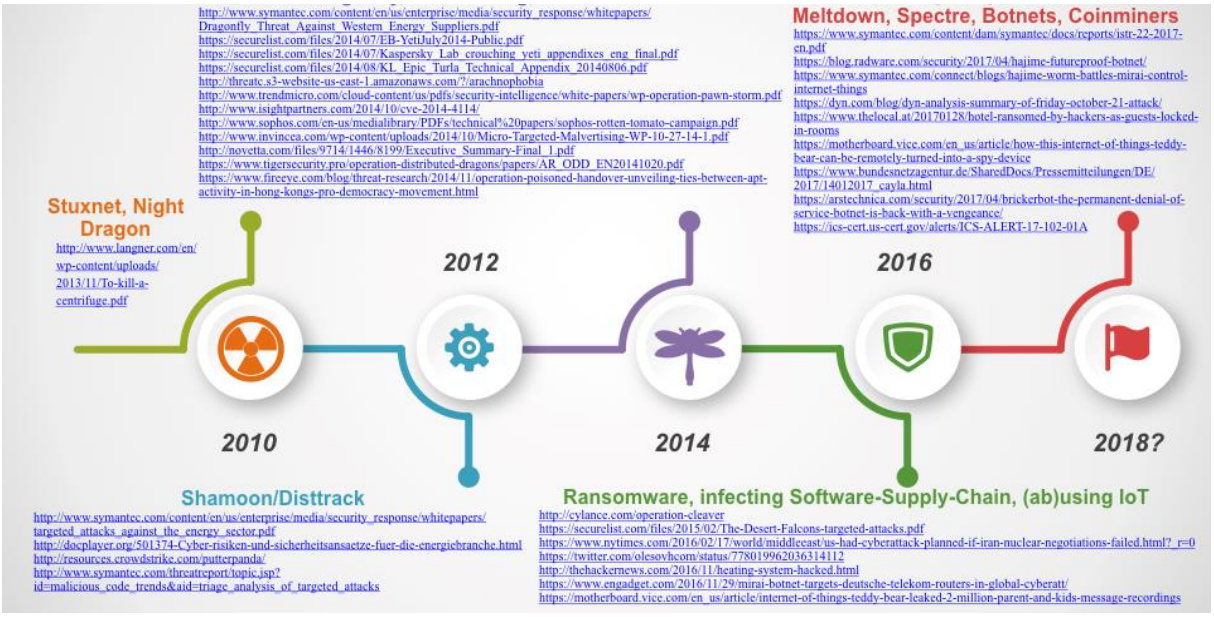


Figure 3: Power grid infrastructure related cyber-attacks snapshot

CYBERSECURITY BY DESIGN: FROM THE BEGINNING THROUGHOUT

Smart energy system components created a need to be (formally) verified to check, if they are doing the tasks they were conceived for, continue doing so, and recover to a trusted mode if they don't. Broad adoptions of information security management (e.g., ISO 27001) and evaluation criteria (e.g., ISO 15408) are important policy tools to contribute to a collective cybersecurity "herd immunity." The EU Cybersecurity Strategy (European Commission, 2013), the GDPR, and the NIS Directive are providing essential steps to increase fragmented cooperation, the EU wide sharing of knowledge, transparency for markets.

The proposed Cybersecurity Package (European Commission, 2017) wants to go a significant step further, to take lessons from other domains and provide assurance for customers by introducing new ICT cybersecurity certification for ICT technologies/products with high cybersecurity requirements. The package introduces a liability for ignoring cybersecurity, as it is a known driver already for automotive, aeronautics, passenger safety, banking, or industrial control systems. All these measures aim at increasing the EU's cybersecurity resilience in the face of exponentially growing numbers of networked, exploitable, commendable, Internet of Operational Things in a single digital market. With a horizon set on 2050, important innovation and research topics in need of results were identified in different clusters and described.

CYBERSECURITY RESEARCH TOPICS RECOMMENDATIONS

Digitization and customer participation is an interdisciplinary issue which affects many different verticals and also entails potentially new directions of necessary research in basically all topic areas previously listed in clusters. Despite the (r-)evolution of new cybersecurity topics, it is evident that know-how and expertise from of related domains information security, telecommunications, automotive, healthcare, is essential for the development of cybersecurity and resilience in the future. The summarized takeaway messages are recommendations for research in the three clusters:

(T) Technology; Research in the following topic areas is recommended because:

1. **AI** helps the cybersecurity industry to monitor sophisticated threats efficiently.
2. The blockchain is considered as a promising technology to address **authentication**, **authorization**, **consensus**, and **immutability**.
3. **Decentralized distributed systems** efficiency needs to be measured and its scaling understood.
4. Digitalization enables and relies on data of massive deployment of **IoT** enabled devices and sensors that make the energy system more transparent and efficient with analytics.
5. OT/IT cybersecurity architecture raises the question of on-**premise vs. cloud**-based calculation.
6. For highly networked components, **safety** is **not reachable without cybersecurity**.
7. **Blockchain** deploys a mathematically secure decentralized way to guarantee the veracity of transactions, but connecting the real world safely too, is open research.
8. Machine learning enables **predictive analytics** which helps in detecting cyber-attacks.
9. To ensure security and integrity of the system, addressing these issues at a device level and along the whole supply chain of these devices should be investigated as research scope.

(P) Policy; Research in the following topic areas are recommended because:

1. **Metrics** and frameworks should be developed for decision making tools on cyber-risks.
2. Stakeholders operating in isolated silos need a **communication platform** (IT, TSOs, DSOs, ESCOs, Policy) to stimulate cybersecurity research at a meta-level among member states.
3. Transparency of data flows, and standardized data models are required for **GDPR**.
4. To lower burden on society, **cost-benefit analyses** shall be considered (e.g., blackout simulators, mandatory patch & updates, hacked IoT device vendor liability).
5. Opposing demands of **anonymisation** and **aggregation** need research to allow both.
6. Research should investigate **privacy layer** design principles and techniques beyond cryptography, to guarantee data privacy protection, without halting innovation, research, and progress, meeting a delicate balance.
7. The **NIS directive** boosts cooperation between the Member States for cybersecurity, but the EU should go further following USA NERC example, organizing research of large-scale interdisciplinary attack scenarios.
8. **Knowledge databases** are used to share, and access known vulnerabilities.
9. Regular **trainings** are vital to make our critical infrastructure resilient against cyber-attacks.

(F) Future challenges; Research in the following topic areas are recommended because:

1. Technological **progress** is ongoing and predicting research needs to include variations.
2. **Society** and energy users need awareness about cybersecurity in the energy system. Involvement of energy users is necessary to achieve the desired level of risk protection.
3. **Quantum cryptography** is a promising disruptive computing technology.

4. Simulation is promising to **quantify** cyber-attack **impacts** on energy systems.
5. Research on **new crypto-environments** should include field demonstrations with cryptographic open protocol solutions.
6. New communication technologies, e.g., 5G need new methods to guarantee SLAs for critical infrastructures **data streams** and the infrastructure needs to expect this failure.
7. **Bio- and nano-technologies** raise the number of cyber threats which require research; Programming tools need to offer new testing and simulation frameworks, and security protocols for life forms need to guide customers, e.g., at home with DIY CRISPR Kits.
8. **Robotics** introduces new threats together with opportunities, which requires research in, e.g., Physical Unclonable Functions (PUF) for robot-identification.
9. Investigate **autonomous vehicles**, such as drones and cars, introducing new threats to energy systems.

Being able to map topics to existing security services does not mean current research and innovations in cybersecurity are obsolete. On the contrary, the vision of the full technical document was to think forward to 2050 and from current trends and open issues, try to identify relevant topics that need to be tackled. The currently growing application of artificial intelligence solutions in thousands of niches of every sector, the progress in quantum bits being cheaply created via superconducting circuits, and currently changing laws and policies introducing general data protection regulation is just a selection of current topics which were a foundation for this position paper.

Throughout the increasing speed of technological developments, the topics need to be adapted and revaluated. Also, the importance of each topic varies from stakeholder to stakeholder. The suggested prioritization of the topics provided can only be seen as a starting point and is as follows – but, due to the nature of a cross-cutting issue such as cybersecurity, this list will be different for each field, domain, or team of experts and time undertaken. To ease and allow referencing, the labelling of the topics is provided according to the full technical document (e.g., T3 signifies Technology cluster topic three):

1. T3 Vision Cybersecurity Centralized vs. Distributed.
2. T1 Artificial Intelligence, P4 Naming Risk Cost Benefit.
3. F1 Progress Considerations, P2 Existing Related/Background Efforts, T9 System Integrity.
4. F6 Data Stream Challenges, T6 Safety Intersecting Security, T5 Cloud Computing, F2 Societal Impact.
5. P3 GDPR, P1 Metrics, T4 Huge Sensor Databases, T7 Blockchain, F3 Quantum Processing.
6. T8 Predictive Analytics, T2 Authentication, P6 Privacy Layer, P9 Training and Policy Amendments, F4 Quantifying Impacts, F5 New Crypto Environments.
7. P5 Anonymisation Aggregation, P7 NIS Directive, P8 Sharing of Vulnerabilities, F7 Bio-Nano Challenges, F8 Robotics Safety Impact, F9 Autonomous Vehicles Regulation.

The ideal would be, to fund research in all topics at the same time, and adjust funding as a society, technology, and trends develop. It is certain that there is not going to be a one-size-fits-all solution and hence, the need for increasing cybersecurity research funding along every development of technology and society, now and in any foreseeable future.

CONCLUSION

Digitalization is impacting all economic and social sectors in such a way that all of them are being transformed. The energy sector, in particular, strongly needs to go through a specific transformation with two major targets: on one hand, establishing a clean and sustainable energy system; on the other hand, allowing energy users to participate in the entire value chain of the energy system which will enable the achieving our target to fully decarbonising Europe by 2050.

Innovative research work on identified issues has already begun, for example, on Blockchain in the Juliette token project, to gain experiences with Blockchain as Technology, to implement a first Use Case and to include Cybersecurity by design. The map of De Ceuvel in Figure 4 depicts the advanced local energy community and allows them to receive a real-time flow view of electricity within the microgrid. However, many challenges remain to be explored in further research within the vision 2050 timeframe.

Figure 4: Blockchain technology cybersecurity use case example, Jouliette at De Ceuvel Community Map

Within this strategic frame, digitalization must be seen as a very powerful tool, rather than as an objective itself, to accelerate the achievement of our targets, especially in Europe where the clean energy is a fundamental and generally accepted one.

WG4 of ETIP SNET, which includes over 60 experts representing all stakeholders of the energy system, has written a detailed document, which is summarized in this short one, analysing the needs for digitalization to arrive to the future 2050 European energy system and sector coupling, with the technology perspective, from the experience described in relevant use cases and with the need of ensuring security of the system and its data through the implementation of the cybersecurity.

As a major contribution, the recommendations presented in this document are dedicated to the different stakeholders involved in the establishment of the future 2050 energy system. We look forward to having these recommendations being considered and implemented.

REFERENCES

Bacher, R, Eric Peirano, Michele de Nigris - Eds (2018). “ETIP SNET Vision 2050 – Integrating Networks for the Energy Transition: Serving Society and Protecting the Environment” (2018) Available online at: https://www.etip-snet.eu/publications/etip-publications/

Chebbo, M, Esther Hardi, Miguel Sanchez Fornie *et al.* (2018) “Digitalization Of The Electricity System And Customer Participation - Technical Report”. Available online at: https://www.etip-snet.eu/wp-content/uploads/2018/10/ETIP-SNET-Position-Paper-on-Digitalisation-FINAL-1.pdf

Chebbo, M, Nikos Hatziargyriou, Pieter Vingerhoets *et al.* (2016) “ETP Smart Grids : The Digital Energy System 4.0.“ Available online at: https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf

European Commission, (2013) “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,”. Available Online at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [Accessed 03 2018].

European Commission, “Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector”.

European Commission (2016). “Winter Package of the European Commission”. Available online at: https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/cleanenergy-all-europeans

ISO27001/2 Information security management / Information technology -- Security techniques -- Code of practice for information security controls.

ISO/IEC 15408 & ISO/IEC 18045 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model & Methodology for IT security evaluation.

AUTHORS

Authors: Working group 4 members from businesses, knowledge institutes, universities, governmental and public organisations. Authors are listed per chapter.

Taskforce 1: Antonello Monti (Taskforce leader), George Huitema (co-leader), Moamar Sayed-Mouchawe, Aitor Amezua, Liam Beard, Theo Borst, Miguel Carvalho, Angel Conde, Aris Dimeas, Guilaume Giraud, Hengxu Ha, Ludwig Karg, Georges Kariniotakis, Antonio Moreno-Munoz, Peter Nemcek, Eric Suignard, Arjan Wargers

Taskforce 2: Elena Boskov-Kovacs (Taskforce leader), Esther Hardi, Norela Constantinescu, Daniel Mugnier, Asier Moltó, Miguel Carvalho, Sandra Riaño, Henric Larsson, Pierre Serkine, Gerhard Kleineidam, Marco-Robert Schulz, Jan Pedersen, Christian Lechner

Taskforce 3: Marcus Meisel (Taskforce leader), Rolf Apel, Jeff Montagne, Miguel Angel Sanchez Fornie, Bruno Miguel Soares, Manolis Vavalis, Liliana Ribeiro, Arjan Wargers, Moamar-Sayed Mouchaweh, Antonello Monti, and Maher Chebbo

Quality check: ETIP SNET EXCo

Delivery date: November 2018

ETIP SNET

EUROPEAN TECHNOLOGY AND INNOVATION PLATFORM

SMART NETWORKS FOR ENERGY TRANSITION

This publication has been developed in the frame of the INTENSYS4EU project, funded by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement N° 731220.

www.etip-snet.eu

PLAN. INNOVATE. ENGAGE.