ETIP SNET

EUROPEAN TECHNOLOGY AND INNOVATION PLATFORM SMART NETWORKS FOR ENERGY TRANSITION

DIGITALIZATION OF THE ELECTRICITY SYSTEM AND CUSTOMER PARTICIPATION

Technical Position Paper WG4

Photo Alliander (Hans Peter van Velthoven)

POSITION PAPER “Digitalization of the Electricity System and Customer Participation” description and recommendations of Technologies, Use Cases and Cybersecurity” ETIP SNET - WG4

September 2018

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

Taskforce 1: Antonello Monti, George Huitema, 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, 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, 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: September 2018

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 queries and media enquiries about this paper, please contact: Maher.CHEBBO@ge.com

Legal notice

Notice must be taken that this publication represents the views and interpretations of ETIP-SNET, unless stated otherwise. This publication should not be construed to be a legal action of ETIP-SNET or its bodies unless adopted pursuant to the SET Plan. This publication does not necessarily represent state-of the-art and ETIP-SNET may update it from time to time.

Third-party sources are quoted as appropriate. ETIP-SNET is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ETIP-SNET nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

SUMMARY

"Digitalization of the Energy System and Customer Participation"

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.

Within this frame, the objective of WG4 "Digitalization of the Energy System and Customer Participation" is to address the use and impact of the Information and Communication technologies as a pervasive tool along the entire value chain of the power generation, transportation and use, and mainly on enabling customer participation.

In the future smart energy system, we will observe, monitor, control, enable and protect the energy supply and use. The communication layer is a pillar of the energy system and radically changes the relation between the final user and the energy system. Advanced meters and modern appliances trigger the potential of active demand-response and enable new services for the energy user. Customer participation in all stages of the development and expansion of the energy system is favoured by digital tools ranging from participative geographical systems to web portals and social media. Internet of Things (IoT) Industrial Internet of things (IoT), big data, blockchain, digital twin technology, all applied to the system, changes its planning and operation and transforms the energy market. In summary, it will mean the digital transformation of the energy system.

The widespread use of these digital technologies however needs to be accompanied by suitable measures for data and information protection from malicious intrusions and attacks, (cybersecurity) and uncontrolled use of customer data.

WG4 has addressed and described the digital development and its impact on the energy system within three Taskforces, having produced each of them a single document. In the present document the discussions and results of these Taskforces are bundled and presented, keeping the content of the ones as originated by them and consolidating within the overall WG4.

As a result, the first section of this paper, 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 Layer, Infrastructure Layer and Business Layer. The enabling **relevant technologies** are described by these layers with detailed mention to the standards, either existing ones or in process. Special attention is being given to the telecommunications technologies with a notable mention to the promising 5G technology.

The second section prepared by Taskforce 2 handles the 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". The use cases are structured in the same three layers as the digital technologies in the first section. An overview of these layers and its use cases is introduced in the fourth paragraph of this section. An overview of some relevant existing pilots and concepts across Europe are presented and reflect trends as IoT, advanced sensoring, secured internet, 5G and peer to peer communication, distributed storage, agent-based services, digital twin, advanced customer modelling, advanced energy communities and blockchain. Emerging Trends and recommendations are given in the end.

The third section of this paper, prepared by Taskforce, 3 solidly describes **cybersecurity** and resilience. There are two high-level concerns regarding the cyber security in the energy sector: to secure of energy systems that are providing essential services and to protect the data in the energy systems and the privacy of the EU citizens. Background taking into account what has been recommended in the different European institutions and forums about the subject, examples of relevant cybersecurity projects, and registered cybersecurity attacks are included in the first chapters. An important distinction between operational (more specific for energy) and information (more general for ICT) technologies is presented from the point of view of the main cyber protection characteristics: confidentiality, integrity and availability. The major part of this section is then addressing the main challenges of the cybersecurity in the future, grouping them in three clusters: Technology, Policy and Future. For each challenge or topic there is a description and a summary of the main issues to retain. The section concludes with a Conclusion and Research topic recommendations.

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)

INDEX

INDEX OF IMAGES, TABLES AND FIGURES

1. DIGITALIZATION OF THE ENERGY SYSTEM – TECHNOLOGY (TF1)

1.1 EXECUTIVE SUMMARY

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 10 years. In reality, digitalization is even older if you consider the installation of components such as RTU. 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 the European Commission 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 other 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 SGAM: Physical Layer; Infrastructure Layer and Business Layer.

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, 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 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 a 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 Cybersecurity concerns which are covered in another position paper of Working Group 4.

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 report of the Working Group 4 with more details.

This report describes in details 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 programs (varying from applied to academic levels) to leading to adequate work forces.

1.2 PREMISES

Digitalization is a process that is affecting all the business sectors. Depending on the sector, different technologies may play a critical role in this transformation. At the European level a key driver is the action of the European Commission's Digital Single Market (European Commission, s.d.), which is setting an agenda for the process.

First of all, it is critical to start with a definition:
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 main purpose of this document is to analyse how digitalization is affecting or will affect the energy sector. In particular, we focus on the enablers in the Energy Transition. The document is structured in five main parts. In the first section a vision is presented that illustrates the peculiar aspects of the digitalization of the energy sector. The second section details some of the key technologies that are driving the transformation in the energy sector. With reference to technologies, the third section covers some key present or emerging standards that are driving the digitalization process. The fourth section describes an outlook for the future and reviews current trends. Finally, the paper closes with a set of recommendations for developing enablers satisfying needs raised by the digitalization in the energy transition.

1.3 DIGITALIZATION OF THE ENERGY SYSTEM

The digitalization of the energy system is not a recent occurrence, but it is a process that has been ongoing since at least 10 years. The main focus so far has been on the infrastructure operation and, coherently, the concept of Smart Grid has been the focus of research and applications. A good overview in this sense is offered by the position paper of the Smart Grid Technology Platform (ETIP SNET , s.d.). The current concept of digitalization is a broader concept encompassing also social aspects. A key reference in this sense is given by the Winter Package of the European Commission (European Commission, s.d.) that clearly stated the central role of the customers in the future energy systems. In this sense, with respect to the traditional idea of a Smart Grid, the digitalization process involves other 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 a convergence of Smart Energy and Smart City,
- New concepts that are emerging also at the physical layers thanks to a greater role played by electronics in the new system.

In this sense, 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 market of energy with equal possibility of participation of every player as envisioned by the Winter Package.
As result, Digitalization is affecting the energy system at three different levels. For each of these levels there are peculiarities that bring different technologies to play a key role.
The National Institute of Standards and Technology (NIST) has introduced the Smart Grid Conceptual Model which provides a high-level framework for the Smart Grid that defines seven high-level domains (Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Providers) and shows all the communications and energy/electricity flows connecting each domain and how they are interrelated. Each individual domain is itself comprised of important smart grid elements (actors and applications) that are connected to each other through two-way communications and energy/electricity paths. European

extension of the NIST model also defines the scope of a pan-European Energy Exchange System and application area of a microgrid architecture.

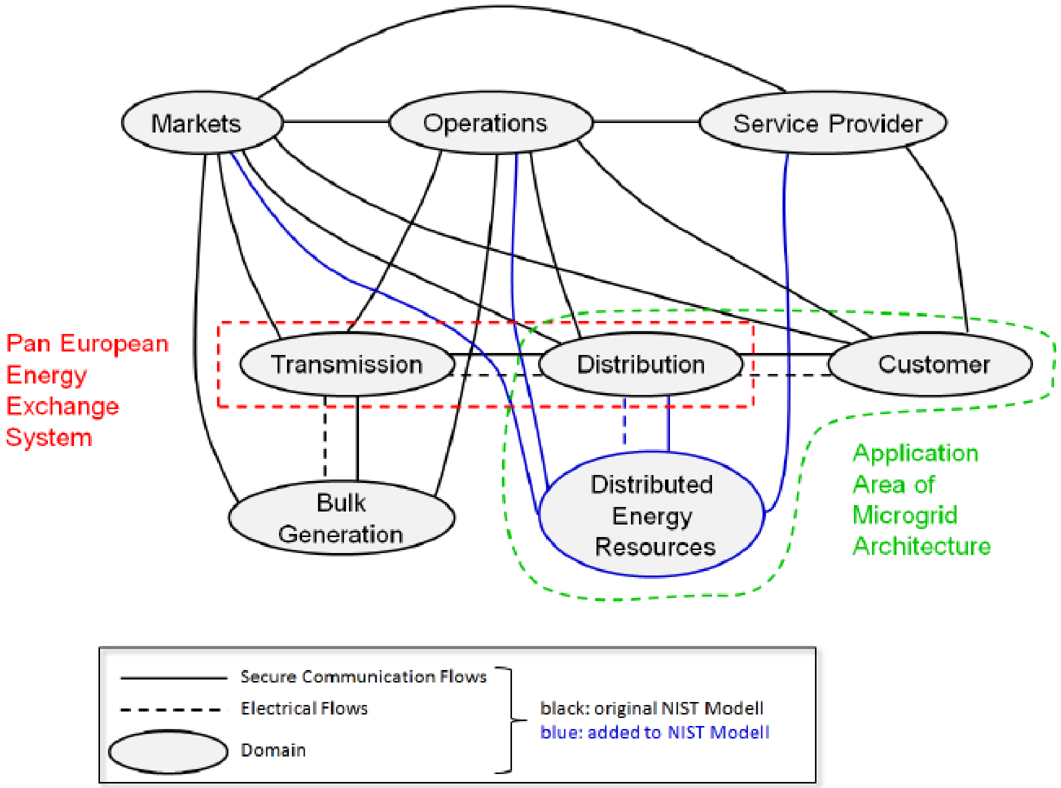


Figure 1: The modified NIST model

Another interesting view of the actors' interaction is given by Error! Reference source not found. which collects a view of all the possible relationships and market roles as identified by the Smart Grid Task Force (Smart Grids Task Force - Expert Group 3, 2015).

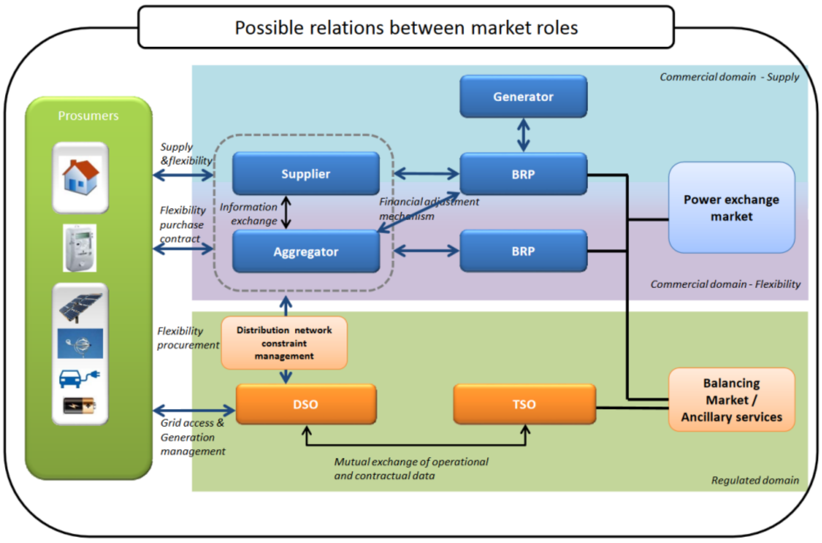

Possible relations between market roles
Commercial domain - Supply
Generator
Prosumers
Supply &flexibility
Supplier
BRP
Flexibility purchase contract
Information exchange
Financial adjustment mechanism
Power exchange market
Aggregator
BRP
Commercial domain - Flexibility
Flexibility procurement
Distribution network constraint management
Balancing Market / Ancillary services
DSO
TSO
Grid access & Generation management
Mutual exchange of operational and contractual data
Regulated domain

Figure 2: The structure of the market and actor interactions

Work done under the mandate M/490 of the EC (European Commission), resulted in the definition of a Smart Grid Architecture Model (SGAM) based on a Reference model initially defined by the NIST and evolved by CEN-CENELEC.ETSI.

Consisting of the five interoperability layers the SGAM framework allows the representation of entities and their relationships in the context of smart grid domains, information management hierarchies and in consideration of interoperability aspects.

This paper will work on a three-layer approach, which are mapped to the SGAM as in Figure 3. We can define these three layers as:

- Physical Layer
- Infrastructure Layer
- Business Layer

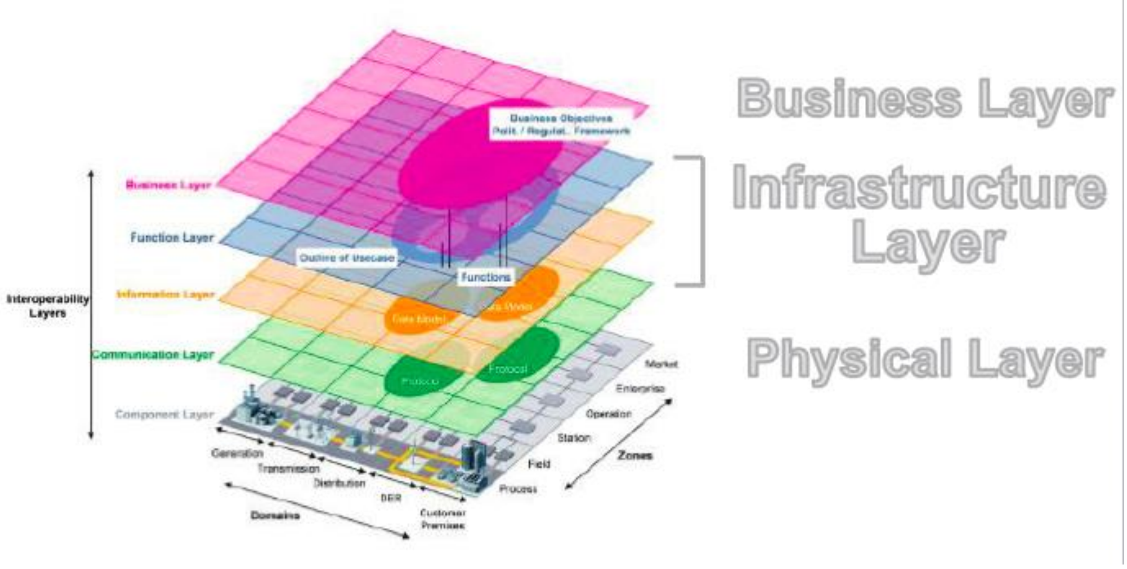


Figure 3: Layers in the Energy System

With *Physical Layer* we refer to the technologies affecting in a direct way the flow of energy in energy grids. The *Infrastructure Layer* deals with the system level intelligence that, exploiting the Physical Layer creates a new process of operation for the overall infrastructure. On top of the operation, the *Business Layer* deals on one hand with the digitalization of the business process within the companies and on the other hand with the transformation of the interaction among the players.

In the following we detail more the characteristics of each of these three layers.

Physical Layer

One of the main effects of the growing presence of renewable energy sources in the electrical grid is the growing presence of power electronics. The same process is happening also at the load side determining new characteristics for the electrical grids and opening completely new options for the grid operations. At the load level new components are also creating new opportunities such as electric vehicles and electrically driven heating systems.

As a first consequence, in a future context each device connected to the grid will have an intelligent control and will have the possibility to interact with the infrastructure in a smart way. This process corresponds to transforming the electrical grid in a network of smart components that may interact according to modern principle of the Internet of Things. Furthermore, thanks to sector coupling, the electrical grid interacts more and more with other infrastructures such as heating grids.

More from the electrical side, this change opens new challenges and opportunities.

The progressive substitution of standard generation with power electronics driven Distributed Energy Resources (DER) is progressively reducing the mechanical inertia of the grid. Inertia has been playing a key role in the grid operation allowing smooth and slow transients in dealing with the power imbalance between generation and load. As result the grid dynamics is significantly affected requiring a reconsideration of the automation principle that affects also the Infrastructure Layer of the digitalization.

On the other hand, on the load side, options of storage are offering new opportunities of flexibility and load balancing to counterbalance the volatility on the source side.

Some key questions emerge as a result:

1) What is the role of DER in the future infrastructure and how their control should be designed to better support grid operation?
2) Should constraints in operation such as maximum deviation of frequency be reconsidered?
3) Is Alternating Current (AC) still the most suitable solution for the grid or should we consider a progressive implementation of Direct Current (DC) technology? While a complete transformation is only reasonable in a very long-time horizon, local insertion of DC technology may increase flexibility and improve efficiency.
4) In an IoT-based infrastructure does it still make sense to operate the grid as a single synchronized entity or should we move towards new solutions that support an asynchronous operation of the grid?

For each of these questions, some key technologies are emerging providing possible answers. These technologies will be introduced in the following section of the paper.

Infrastructure Layer

The infrastructure layer has been the main focus of the Smart Grid process which has been active now for more than 10 years. Smart Grids should allow the enhanced monitoring, automation and control of the existing networks while ensuring that all involved stakeholders (regulated and market players) can interact: this will be made possible by a full Digitalization of the power system, and of the energy system as a whole. As of today, Digitalization is under implementation in transmission networks and distribution networks (mainly MV) but also for market applications. Still, a lot of work remains to be done to achieve a full Digitalization of the energy system.

A key role in this process will also be played by the customers and by their involvement. While Smart Metering has been already discussed for long time, new opportunities are emerging by the changes in home energy systems starting from the installation of PV to the electrification of the heating and transport sectors. All these changes, thanks to digitalization, can be exploited to redefine the role of the customer making the consumer, or better the prosumer, an active player in the energy system.

Some of the key ongoing evolutions are here summarized:

- Development of tools for monitoring, automation and control, cybersecurity; use of big data, IoT and tools for network management.
- Use of IoT and data mining to develop smart asset management strategies, manage the network, closer to physical limits.
- Coordinate and participate in standardization activities for communication and data exchanges between stakeholders.
- Develop scalable solutions to address large-scale data management issues in power systems.
- Ensure physical and cyber-security of digital substations.
- Increment of the opportunities offered by sector couplings. This goes in the direction of linking to heating systems but also more and more linking to transportation infrastructure and in particular e-vehicles.

For these evolutions, we will find in the following section some key technologies.

Business Layer:

For what concerns the business layer, it is important to distinguish between the enterprise operation and the digital business. The first refers to the internal process of transformation of the companies to incorporate digital operations. In this sense the energy sector is not different from many other business operations.

More interesting vice versa is to consider how digital technologies may affect the interaction of the different market players enabling new business models and possibly disruptive concepts. In this field, digital technologies mostly supposed to facilitate transactions with a special focus on peer to peer transactions in support of a more active role for the customer. In this respect, concepts such as Blockchain can be seen as interesting opportunities to create an unbiased and open market structure for the all the possible players.

1.4 ENABLING DIGITALIZATION – RELEVANT TECHNOLOGIES AND STANDARDS

Below we summarize enabling technologies along the three different levels of energy systems.

- Technologies at the Physical Layer
- Advanced control for Distributed Energy Resources (DER)

For what concerns the DER operations, while we move to a more power electronics driven operation, it becomes evident that the control of the converters will have to be adapted to better support the grid automation. Currently, converters operate according to a grid supporting principle (J. Rocabert, Luna, Blaabjerg , & Rodriguez, 2012), i.e. they provide support injecting active or reactive power, but they mostly operate as follower for (what 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 frequency control. Combining DER with local storage, also Renewable Driven DER will be able to provide full support to ancillary service provision.

On the other hand, the increased dynamics in the power grid are requesting to place more attention to parameters that were not part of the focus of the automation so far such as Rate of Change of Frequency (ROCOF) and measurement process of frequency as well (Zhao, Mili, & Milano).

For what concerns voltage control, it should be noted that moving towards a power electronics driven power grid is expanding the voltage stability issue from a simple reactive provision to a wide-frequency stability concern.

All in all, power electronics should be considered as an opportunity offering a variety of options for controllability not available with standard synchronous machines (D'Arco , Suul, , & Guidi, 2016). In this sense, digitalization at the physical layer may bring a way more robust grid even if more volatility in the generation will be present.

1.4.1 DC GRIDS

While AC has been the adopted solution for more than 100 years, power electronics is reopening the question of the best solution for the use of the infrastructure. The development of completely new infrastructures such as Off-shore wind farms and also new infrastructures for fast charging of electric vehicles offer considerable opportunities for technology insertion.

Smart control applied to local DC Grids embedded in larger AC infrastructures may allow a more flexible use of available infrastructures bringing significant saving in terms of infrastructure deployment facilitating the process of energy transformation.

In terms of component maturity, the availability of a DC breaker for all the possible voltage application is the major weakness at the moment but different research activities and preliminary products show that a solution to this issue could come very soon. On the other hand, in a power electronic driven system, converters may also play an active role in the protection schemas. In this sense, modern communication technologies may allow fast coordination among converters for a better selectivity and continuity of service.

1.4.2 SMART TRANSFORMERS

Power electronics is also changing the way energy transformation can be performed in a substation. Different solutions for the so-called smart transformer (Gao, Sossan, Christakou, Paolone , & Liserre, , 2018) have been proposed in literature. Main consequences of the application of this technology could be summarized by the following list of points:

- Intrinsic digitalization of the substation and full control of the power flow at every level of the grid,
- Possibility of physical decouple frequency control at different voltage levels of and easy implementation of distributed control schemas.

1.4.3 SECTOR COUPLING

To achieve the goals of the EU Climate and Energy package, the European Commission has recently adopted the Energy Union strategy (European Commission, 2016) which articulates ambitions to transform Europe's energy system in a cost-effective manner by making it more flexible, decentralised, integrated, sustainable, secure and competitive, and putting consumers at its centre. This is backed up by the new integrated Strategic Energy Technology Plan (European Commission, s.d.) which identifies strategic priorities and actions needed to accelerate this EU energy system transformation.

Besides, policy makers now need to consider issues such as the effects of intermittent or variable Renewable Energy Sources (vRES) on the reliability and adequacy of the energy system, the impacts of rules governing the curtailment or storage of energy, or how much backup dispatchable capacity may be required to guarantee that energy demand is safely met (European Commission, s.d.). It has been acknowledged that addressing the power system alone, will not ensure the achievement of the development goals: it is important to integrate all available means also from the heating, cooling and gas sectors and foster the integration with the power system. The recently published “Clean Energy for All Europeans”, indicates the main way forward (European Commission, 2016):

- To accommodate the power generation from most variable renewable energy sources (vRES), energy markets have to evolve, providing adequate rules allowing shorter term trading. The goal is to enable to better reward flexibility from generation, demand or storage.
- The potential of heating and cooling to contribute to the achievement of the overall renewables target is underused: the general approach has been set in the “Heating and Cooling Strategy” (European Commission, 2016). Heating markets have to be open up to competition and foster the integration of power-to-heat technologies.
- The shift from conventional generation to decentralized, smart and interconnected market have to be enforced. The goal is to enable consumers to participate in markets, offer Demand Response (DR) directly or through aggregators. Consumers should be able to generate, store, share, consume or resell energy to the markets.

This is yet facing many challenges and a large effort in research is needed at technological, organizational, regulation and market mechanisms levels to provide an efficient and secure energy system. The following challenges related to flexibility, storage and district heating are key for the introduction of coupled multicarrier energy systems and markets and vital to feed the policy dialogue with technological and operational innovations that can shape the policy discussions on the future of the energy system.

1. Major questions arise from the integration of the electricity and heating grids, through the operation of “power-to-heat” technologies and large thermal storage (specifically in storage tanks and pits, but also as thermal storage using the thermal inertia of networks and buildings) to shift demand and integrate renewable energy. The correct integration and operation of these technologies in district heating and cooling grids, still needs more investigation.

2. Gas storage will also play a major role to ensure supply security and grid stability: with the faster cycling of gas-based generation facilities (as CHPs or CCGTs), storage facilities will have to withstand fast withdrawal and injection cycles. Appropriate gas back-up power will be an increasing need (Eurelectric, 2011). In large scale, gas storage may represent the only solution for seasonal generation variation.
3. Despite the great potential, much still needs to be done to ensure that all heat production systems, distribution networks, storage and demand are duly interconnected in order to exchange real-time data, quantify the availability of each equipment and the demand at any time and part of the network, in order to exploit the flexibility potential that such infrastructure offers.
4. Besides, mobilizing flexibility is not only a technological challenge, but also a main concern for the overall energy market. At the same time, rules and technical requirements at national balancing, wholesale and capacity markets often prevent flexibility products provided by decentralized resources from entering those markets (European Commission, 2005). Within such market context, bringing flexibility products to market still needs the development and adaptation of the current regulation and a consequent adapted market design (European Commission, 2016).

Among the concepts of sector coupling, mobility plays also a critical role. A massive deployment of electric vehicles represents on one side a challenge for the increase in the total energy and power demand but also an opportunity offering new options of flexibility through battery storage.

Policy-makers have grasped the need of fostering integrated energy solutions, but decision making has yet to rely mainly on decision support systems as tool and studies, since existing demonstrators only partially address the above topics. Tools are the main mean to foster the circulation and acceptance of the need to further increase the synergies among electricity, heating and gas sectors and ensure more awareness, acceptance and dialogue among decision makers from these yet too distinct sectors.

However, as the energy systems are complex, so are the tools necessary to assess the consequences of actions and changes in the systems: i) physical/technical (e.g. storage or distribution), ii) operational (e.g. energy management systems) and iii) institutional (e.g. market design). As stated by the “Thematic Research Summary on Decision Support”, R&D efforts should be concentrated in making tools more transparent and increase their acceptance and reliability: model assumptions, limitations and used databases should be made more transparent and accessible to stakeholders.

One central challenge remains to provide more effective and acknowledge guidance to decision makers: “technical solutions and market design need to be brought together for the optimal design of the transformation pathway” (European Commission Energy Research Knowledge Centre, 2014). To be able to translate technical solutions into the right policy guidance, the whole process has thus to be addressed through adapted tools and decision support systems for technological, operational to institutional challenges

While sector coupling is not a digital technology per se, it is however important to mention that it can be achieved only through digital solutions. As better described in a following chapter, sector coupling is one of the key drivers in the development of digital platforms able to support data interchange among verticals. Sector coupling is in effect transforming the energy system from a set of vertical infrastructures to a set of horizontally interconnected local energy systems. This process is enabled by new software solutions that create the link among operational activities traditionally disconnected. This is particularly true in the context of Smart Cities as also underlined by the White Paper on Smart City released by the German Association of Electrical Engineers (VDE).

1.5 TECHNOLOGIES AT THE INFRASTRUCTURE LAYER

1.5.1 MODERN COMMUNICATION NETWORKS

Integration of the communication infrastructure is a key part of the digitalization of the energy system. Moreover, several options are available as illustrated in Figure 4. In the following, a comprehensive overview of communication technologies is proposed to appreciate the different options that are available to perform such integration.

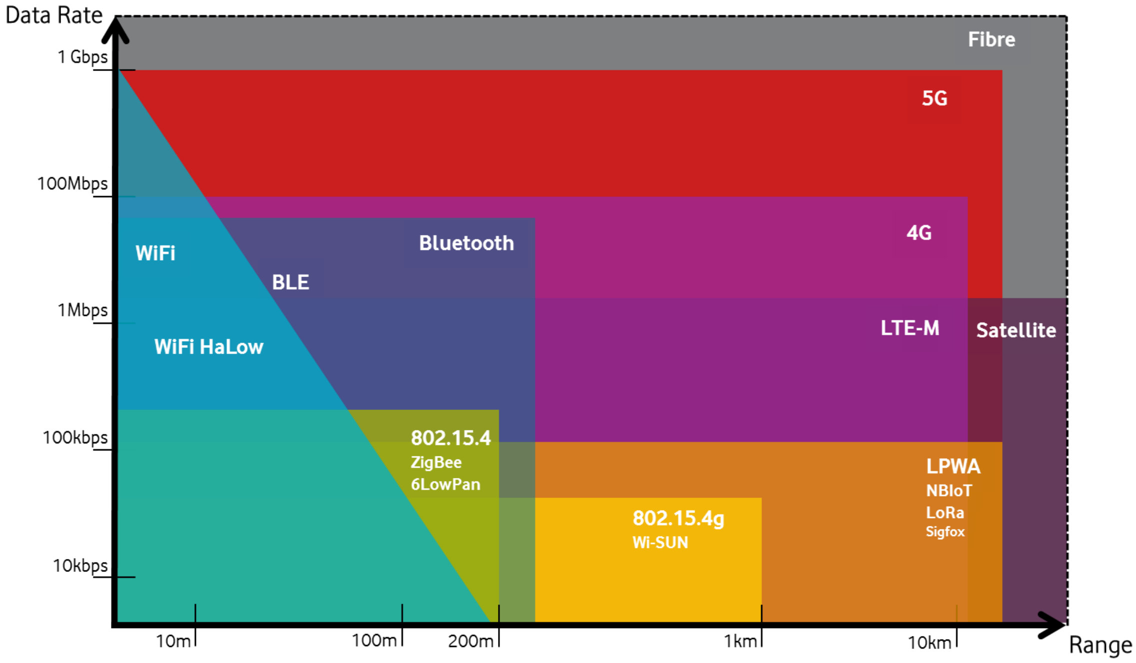


Figure 4: Communication Technologies by Range and Data Rate potential 5G

The mobile industry is developing and preparing to deploy 5G. Thanks to technology advances in many different fields, 5G networks will be at the centre of an ecosystem that powers society’s continued digital transformation. The deployment of 5G networks as enhancements to the established 4G deployments already widespread in Europe will, subject to the availability of appropriate spectrum bands at the right time, allow massive connectivity resources to ensure that user data requirements can continue to be met by licensed mobile network providers. Beyond this, 5G will support vertical industries across Europe in adapting to a changing economic and social environment, helping with their respective challenges and needs.

Various global standards bodies and organisations are working to ensure alignment in 5G, in particular the International Telecommunications Union (ITU) which has christened the next global next generation cellular system ‘IMT-2020’ and the 3rd Generation Partnership Project (3GPP) which unites seven telecommunications standard development organisations. All stakeholders are working to define what 5G should be. Technically, the aspiration for 5G is to deliver 1 Gbps speeds and <10 ms latency. However, more fundamentally, the 5G era will be characterised as the age of boundless connectivity for all and intelligent automation, enriching people's lives and transforming industrial processes. 5G networks will integrate with 4G and alternative network technologies to provide pervasive connectivity in the 5G era. This will happen as advances in computation, artificial intelligence and device capabilities come to maturity:

- 5G is the first mobile technology extensively designed from the outset both with and by the end user vertical industries, as well as by the telecoms operator, vendor and standards body communities.
- 5G is designed to ensure a smooth evolution from 4G that improves customer experience with higher data rates and lower delay.
- 5G offers wide-ranging capabilities and is able to support many applications of use and consumer innovations.
- 5G offers the resilience and security that is required to be considered for ‘mission critical’, ‘enterprise control’ or ‘life supporting’ services.
- 5G brings the performance and reliability to ‘untether’ previous fixed assets/equipment and enable new methods of production, with both existing (legacy) and new (for example robotic) tools.

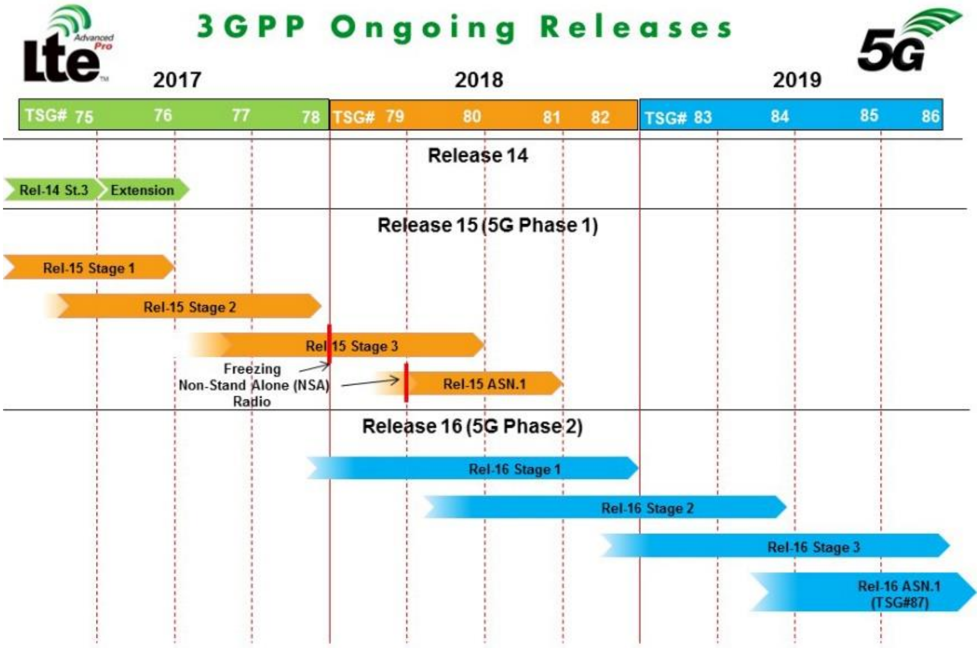


Figure 5: 5G roadmap

The introduction of 5G will be the result of improvements in LTE, LTE-Advanced and LTE Pro, but this will soon be followed by a major technology step, with the prospect of an entirely new air interface. The first drop of NR 'New Radio' features, in Release 15, will form the first phase of 5G deployments.

Full compliance with the ITU’s IMT-2020 requirements is anticipated with the completion of 3GPP Release 16 at the end of 2019 - In Phase 2 of the 3GPP 5G effort (see Table 1**).**

Release	Status	Start date	End date	Closure date
Release 16	Open	2017-03-22		
Release 15	Open	2016-06-01	2018-09-14 (SA#81)	
Release 14	Frozen	2014-09-17	2017-06-09 (SA#76)	
Release 13	Frozen	2012-09-30	2016-03-11 (SP-71)	
Release 12	Frozen	2011-06-26	2015 -03-13 (SP-67)	
Release 11	Frozen	2010-01-22	2013-03-06 (SP-59)	
Release 10	Frozen	2009-01-20	2011-06-08 (SP-52)	
Release 9	Frozen	2008-03-06	2010-03-25 (SP-47)	
Release 8	Frozen	2006-01-23	2009-03-12 (SP-43)	
Release 7	Closed	2003-10-06	2008-03-13 (SP-39)	2014-09-17 (SP-65)

Table 1: Releases of the 3GPP

Applications

- RTU/Telemetry & Control
- Smart Metering
- EV, V2G
- Self-healing networks and ultra-fast fault location
- Distributed generation control
- Grid topology restructuring
- Integration of Distributed Energy Resources (DERs)
- Micro-grids
- Forecasting generation and consumption
- (BPL, RF) Concentrator backhaul
- Security – Video, analytics, access

Sources:

1. The 5G era: Age of boundless connectivity and intelligent automation – GSM Association 2017
2. Creating a Gigabit Society – The role of 5G. A report by Arthur D. Little for Vodafone Group Plc - 2017
3. 3GPP - www.3gpp.org/about-3gpp/about-3gpp
4. 3GPP - www.3gpp.org/specifications/67-releases /www.3gpp.org/specifications/67-releases

LPWA (Low Power Wide Area)

The defining characteristic of a LPWA network is that it supports devices that are low power, in terms of both processing power consumption and transmission power; this is linked to a potential battery performance of greater than 10 years. The other two key characteristics are enhanced coverage capability, either longer range (from base stations) or high penetration (within buildings or underground), and low cost (of modules and data transportation). LPWA network technologies are available using licensed and unlicensed spectrum. In most jurisdictions, use of unlicensed spectrum is regulated such that devices must meet requirements on maximum transmission power and duty cycle to minimise undue interference with other users; this may result in region-specific limitations on the data throughput and range of LPWA technologies using particular frequency bands.

NB-IoT

“NB-IoT” stands for “Narrow Band-Internet of Things”. It is a low power wide area radio technology standard published by 3GPP in Release 13 that addresses the requirements of the Internet of Things (IoT). The technology provides improved indoor and outdoor coverage, supports very large numbers of low throughput IoT devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimised network architecture. The term NB-IoT encompasses the use of this technology within the LTE bands and also includes use of the same protocols in other, licenced radio spectrum outside the normal LTE bands. NB-IoT uses dedicated licensed spectrum so does not compete against other cellular spectrum users.

LTE-M

LTE (“Long Term Evolution”) is a 4G (fourth generation) cellular mobile technology standardised by 3GPP. The LTE standards accommodate multiple categories of device (UE, “User Equipment”) with varying uplink and downlink capabilities. In 3GPP Release 13, LTE UE category M1 is defined to suit devices with simpler, cheaper wireless modules (with the modem costs reduced to 20-25% of the current EGPRS modems) and very long battery life; use of LTE with this UE category is referred to as LTE-M for short. LTE-M also offers enhanced coverage compared to machine-to-machine UE categories in 3GPP Release 12. LTE-M is operated in licensed spectrum.

LoRaWAN

LoRaWAN is a public specification for LPWA technology developed by members of the non-profit LoRa Alliance. With a low-cost base station available, it is being used for self-managed private network installations as well as by providers of public networks. "LoRa" alone describes the underlying, proprietary, physical radio layer which can also be used for peer-to-peer communications, whereas "LoRaWAN" describes the link layer protocol. LoRa is operated in unlicensed spectrum.

Sigfox

Sigfox is a licensable LPWA technology developed by the French-based company of the same name. A particular characteristic of Sigfox is its use of "Ultra Narrow Band" radio transmission, which is designed to enable good coverage with a very low transmission power, but it is limited to a very low data rate even compared to some of the other LPWA technologies covered here and has very limited downlink capability. Wireless modules are very low cost (and royalty free); network providers pay license fees to Sigfox, and Sigfox also run their own commercial networks in some territories. Sigfox is a proprietary technology and is operated in unlicensed ISM bands.

Technology	**LTE-M**	**NB-IoT**	**LoRaWAN**	**Sigfox**
Bandwidth	1.08MHz	180kHz	125kHz (500kHz d/l)	100Hz (1.5kHz d/l)
Approx. max. coupling loss	160dB	164dB	157dB	153dB
Max. downlink peak data rate	1Mbps	250kbps	50kbps	600bps
Max. uplink peak data rate	1Mbps	250kbps	50kbps	100bps
Typical module cost	Medium	Low	Low	Very Low

Table 2: Characteristics of communication technologies

Status

Active	NB-IoT	open global standard 3GPP Release 13 and onwards
Active	LTE-M	open global standard 3GPP Release 13 and onwards
Active	LoRaWAN	open global standard 1.1, LoRaWAN 1.1 Regional Parameters rev A, and LoRaWAN Backend Interfaces 1.0 Specifications
Active	Sigfox	Proprietary

Table 3: Status of communication technologies

Applications

- Simple Metering
- Asset sensors (cable pits, cable terminations points, OHL monitoring)
- Infrastructure integrity
- Waste collection
- Environment monitoring
- Low data/speed smart grid applications – MDI, FPI

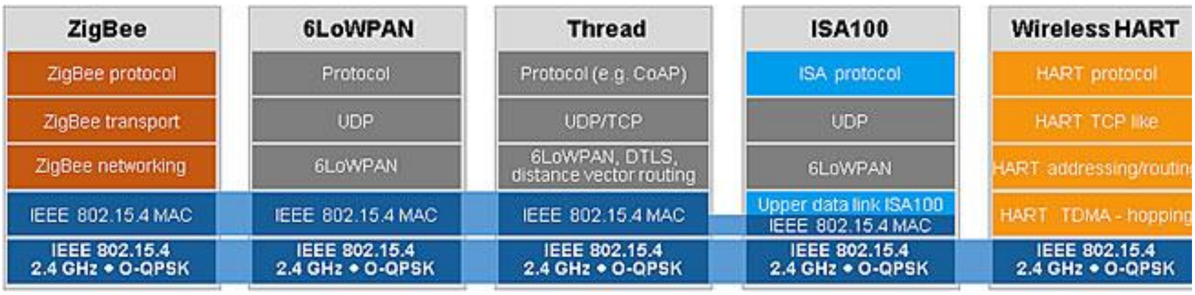
Sources:

- LPWA Technology Security Comparison - A White Paper from Franklin Heath Ltd 2017
- www.gsma.com/iot/
- www.lora-alliance.org/technology
- www.sigfox.com/en/sigfox-iot-technology-overview
- www.3gpp.org

IEEE 802.15.4 (WPAN)

IEEE 802.15.4, is a wireless (physical layer and media
access control) specification defined by IEEE, for wireless personal area networks (WPANs). IEEE 802.15.4 has characteristics such as low power, low cost and peer to peer network support. IEEE 802.15.4 provides a framework for low data rate communications systems, typically sensor networks. The standard specifies 5 MHz channels ranging from 2.405 GHz to 2.480 GHz. The specified maximum over-the-air data rate is 250 kbps. The transmission distance ranges from a few metres to around a hundred metres, depending on RF power and environmental conditions.

IEEE 802.15.4 usually operates in the unlicensed 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS), it uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)-based MAC and is capable of associating with 65,000 devices.



ZigBee	6LoWPAN	Thread	ISA100	Wireless HART
ZigBee protocol	Protocol	Protocol (e.g. CoAP)	ISA protocol	HART protocol
ZigBee transport	UDP	UDP/TCP	UDP	HART TCP like
ZigBee networking	6LoWPAN	6LoWPAN, DTLS, distance vector routing	6LoWPAN	HART addressing/routin
IEEE 802.15.4 MAC	IEEE 802.15.4 MAC	IEEE 802.15.4 MAC	Upper data link ISA100 IEEE 802.15.4 MAC	HART TDMA - hopping
IEEE 802.15.4 2.4 GHz • O-QPSK	IEEE 802.15.4 2.4 GHz • O-QPSK	IEEE 802.15.4 2.4 GHz • O-QPSK	IEEE 802.15.4 2.4 GHz • O-QPSK	IEEE 802.15.4 2.4 GHz • O-QPSK

Figure 6: Example of 802.15.4 based WPAN Technologies

IEEE 802.15.4g Smart Utility Networks (SUN)

IEEE 802.15.4g, also known as the Smart Utility Networks (SUN) standard defines a PHY amendment to IEEE 802.15.4 that facilitates very large scale process control applications such as the utility Smart Grid Networks. It addresses outdoor low data rate wireless Smart Metering Utility Network requirements. Smart Utility Networks (SUN) PHY are provided with a wide range of frequencies ranging from 450 MHz to 2.4 GHz in different operating modes.

DSSS (Direct Sequence Spread Spectrum)	6.25kbps
GMSK (Gaussian Minimum Shift Keying)	50, 100, 150, 200kbps
OFDM (Orthogonal Frequency-Division Multiplexing)	50, 100, 150, 200, 300kbps

Status

Active	IEEE 802.15.4 latest release 2015
Active	IEEE 802.15.4g latest release 2012

Table 4: Physical layer modulation techniques (within 200kHz channel)

Applications

IEEE 802.15.4
- Home Area Networks
- Smart Homes / Home automation
- Home Energy Management Systems

IEEE 802.15.4g
- Field Area Networks
- Low data/speed smart grid applications
- Smart Metering
- Smart City (specific applications e.g. smart lighting)

Sources:
1. www.ieeexplore.ieee.org

2. A comparison of 802.11ah and 802.15.4 for IoT – ScienceDirect - N. Ahmed, H. Rahman, Md.I. Hussain 2016
3. www.wi-sun.org/index.php/resources/general
4. www.silverspringnet.com

Wi-Fi

Wi-Fi refers to a set of technologies covered by the IEEE 802.11 standards for WLANs. IEEE 802.11 addresses wireless connectivity for fixed, portable and moving stations within a local area. As of 2017, 802.11ac is the de-facto wireless connection method for new WLANs. 802.11ac has a theoretical aggregate capacity ranging from 433Mbps and 6.7Gbps depending on channel bandwidth, number of stations and number of antennae. However there are some new and emerging wireless standards to be considered, four of which are described below:

IEEE 802.11ax

The 802.11ax standard is at the top of the list. Like 802.11ac and 802.11n before it, the 802.11ax protocol operates in both the 2.4 and 5 GHz frequency spectrum and utilises hardware chips that are fully backwards compatible with previous Wi-Fi standards. 802.11ax theoretical speeds are said to approach 10 Gbps in early tests.

IEEE 802.11ay

Technically an update to the already-certified 802.11ad (WiGig) standard, 802.11ay is a high-performance wireless technology that operates in the unlicensed 60 GHz frequency range. The advancements of 802.11ay improve on the original specification in both throughput and range; with data transfer rates between 20 and 40 Gbps and wireless ranges that reportedly reach upwards of 300 meters.

IEEE 802.11ah

Wi-Fi 802.11 ah (HaLow) extends Wi-Fi into the unlicensed 900 MHz band, enabling the low power connectivity necessary for IoT applications including sensor and wearables. Wi-Fi HaLow's range is intended to reach distances of up to 1000m, and will not only be capable of transmitting signals further, but also providing a more robust connection in challenging environments where the ability to more easily penetrate walls or other barriers is an important consideration. In addition to the range boost, the standard can support highly dense deployments of IoT sensors. This can translate into significant IoT deployment cost savings.

Potential maximum throughput for 802.11ah is just shy of 350 Mbps. This is lower than 802.11ac, but sufficient for most IoT deployment needs.

IEEE 802.11af47

The fourth emergent Wi-Fi standard is 802.11af, also known as Super Wi-Fi or White-Fi. This standard takes advantage of unused "white space" frequencies that reside between television channels in the designated UHF-VHF spectrum between 54 and 790 MHz. While this white space can be used for a multitude of use cases, the primary purpose for 802.11af at least in the United States is for long-range wireless connectivity to rural areas.

Unlike the aforementioned IEEE standards, 802.11af requires an FCC or equivalent license change to operate.

Active	2016	802.11ah
Active	2016	802.11af
Expected	2019	802.11ax
Expected	2019	802.11ay

Table 5: Latest Wi-Fi standards

Applications

- 802.11ah – Sensors and Meters: Smart Grid – Meter to concentrator, Environmental monitoring, Building automation, smart city. Backhaul sensor and meter data. Extended range Wi-Fi.
- 802.11af – Long range broadband (Remote Smart Homes/Digitally enabled sites and assets)
- 802.11ax – AR, AI
- 802.11ay – VR, static point-to-point or point-to-multipoint outdoor backhaul

Sources:

1. IEEE Multimedia Version 5 Issue 2 1998. www.networkcomputing.com/cloud-infrastructure/4-emerging-wireless-standards-watch - Andrew Froehlich 2017

Bluetooth

Bluetooth® is a low-power wireless connectivity technology used to stream audio, transfer data and broadcast information between devices. There are two flavours of Bluetooth technology, Basic Rate/Enhanced Data Rate (BR/EDR) and Low Energy (LE), which offer different communications capability. Bluetooth communicates using Frequency Hopping Spread Spectrum (FHSS) technology over 79 channels in unlicensed spectrum (2.4GHz to 2.485GHz band) and is standardised through IEEE 802.15.1.

Basic Rate/Enhanced Data Rate (BR/EDR)

- Point-to-Point

Low Energy (LE)

- Point-to-Point
- Broadcast
- Mesh

Status

Active	Bluetooth v4.2	2014
Active	Bluetooth 5	2016

Table 6: Latest Bluetooth standards

Applications

- Bluetooth v4.2 – industrial sensors, metrology, home automation (connection to a hub or access point)
- Bluetooth 5 – industrial sensors, home automation, metrology

Sources:

1. Bluetooth SIG blog.bluetooth.com/introducing-Bluetooth-mesh-networking
2. Bluetooth SIG www.bluetooth.com/bluetooth-technology

Power Line Carrier (PLC)

PLC works on a similar principle to Digital Subscriber Line (DSL). Network data is transmitted over power cables using imposed higher frequency signalling than that used for the incumbent purpose, for example above 50-60 Hz in the case of AC power cables, taking advantage of otherwise unused transmission capability of the wires. In this way data can be sent back and forth across a PLC network with no disruption to power delivery. In practice, the high level of attenuation (or data signal loss) from access PLC power cables results in significant bandwidth and related distance limitations. However, there are many benefits to PLC deployments too, and enough capacity can be made available to support a range of targeted applications, such as Smart Metering or grid control signalling.

There are two principal variants of PLC relevant to this paper, Broadband Power Line and Narrowband Power Line Carrier, and these are described in the section below.

Broadband Power Line / Broadband PLC

The IEEE 1901 standard defines the technology for high-speed power line communications. The standard defines methods for both in-home networking and access networking. The standard consolidates two existing standards in the market – FFT OFDM modulation and Wavelet OFDM modulation. This necessitated that two physical layers had to be specified, with vendors not required to offer both in their products; which meant that devices conforming to the standard could, potentially, be incompatible with each other. The market-ready products conforming to IEEE 1901 are best known as the HomePlug Access BPL, and HD-PLC. Neither has been widely adopted in the MV BPL space. BPL uses some of the same radio frequencies used for over-the-air radio systems, therefore modern BPL employs frequency-hopping spread spectrum to avoid using those frequencies actually in use, though early pre-2010 BPL standards did not. The criticisms of BPL from this perspective are of pre-OPERA, pre-2005 standards. OPERA – Open PLC European Research Alliance technology has been demonstrated through large scale deployments in field since 2008 and is focused on both MV and LV grid environments.

The IEEE1901 standard defines a frequency range of about 2MHz to 250MHz, but in reality, 87.5MHz is the typical upper limit. Distances achievable are from hundreds of meters to a few kilometres. Practical data rates are up to 200Mbps for standard delivery and 30Mbps over MV and 3Mbps over LV for real-time delivery.

Active	IEEE 1901.2010
Active	ITU-T G.9960 (2015) / G.9961 (2015)

Table 7: Latest Broadband PLC standards

Applications

Low Voltage Grid

- Conductor mounted sensors
- Electricity Smart Metering
- Low speed internet access

Medium Voltage Grid

- Secondary substation communications backhaul

Sources:

1. Lifewire – Introduction to BPL – Broadband over Power Line, Bradley Mitchell October 2016
2. Telecommunications Networks for the Smart Grid, A Sendin, M Sanchez-Fornie, I Berganza, J Simon, I Urrutia 2016
3. Power Line Communication: Anees Ahmed**,** Mistral Solutions Pvt. Ltd.

Narrowband (NB) PLC

NB PLC is the most mature of the PLC technologies currently in use and has been deployed for many decades. Although it can operate in both MV and LV grid environments the majority of recent interest has been in the LV area, particularly in relationship to Smart Metering, where with the right combination of market conditions, infrastructure topology, AMI density and functional objectives it can deliver the optimal access solution.

The NB PLC standards define frequency ranges of between 3kHz to 500kHz. Distances achievable are from hundreds of metres to a few kilometres. Data rates are influenced by the number of carriers used. Low data rate (single carrier) are up to a few kbps. High data rate (multiple carriers) are up to a few hundred kbps.

All of the standardised NB PLC technologies employ OFDM at the physical layer and then a range of modulation techniques depending on the network device operating requirements.

There are four primary standardised NB PLC technologies relevant to this paper:

PRIME (PoweRline Intelligent Metering Evolution)

PRIME has been developed by the PRIME Alliance, a collaboration of utilities, chipset manufacturers and meter vendors. It offers a public, open and non-proprietary telecommunications architecture defined in 3 layers (PHY, MAC and convergence) and operating between 42kHz and 472kHz with 96 usable subcarriers available in the Cenelec A band.

In the PHY layer PRIME offers modulation schemes based on DBPSK, DQPSK and DBPSK with Convolutional Code and Robust (repetition) options which are selected depending on the data service characteristics required. A raw data rate of between 5.4kbps and 1,028.8kbps can be achieved depending upon channel allocation and modulation type selected. The MAC layer is used to support subnetwork management and inter-nodal switching, using CSMA/CA. In the convergence layer PRIME specifies 3 further layers for IPv4, IPv6 and IEC 61334-4-32.

G3-PLC

G3 PLC has been developed by the G3 PLC Alliance, another collaboration of utilities, chipset manufacturers and meter vendors.

Its architecture is defined in 3 layers (PHY, MAC and adaption) and operates between 10kHz and 490kHz with (typically) 36 subcarriers available in the Cenelec A band.

In the PHY layer G3-PLC offers modulation schemes based on DBPSK, DQPSK and DBPSK with Convolutional Code and Robust (repetition) options which are selected depending on the data service characteristics required. A raw data rate of between 4.5kbps and 298.2kbps can be achieved depending upon channel allocation and modulation type selected. The MAC layer is based upon IEEE 802.15.4, using CSMA/CA. The adaption layer is based on 6LoWPAN and supports IPv6 packets.

IEEE 1901.2

IEEE 1901.2 has been developed by the IEEE following the developments initiated by the PRIME Alliance and G3-PLC Alliance. IEEE 1901.2 refers to the PRIME and G3-PLC standards as being compliant.

It operates between 10kHz and 490kHz with 36 subcarriers available in the Cenelec A band.

In the PHY layer IEEE 1901.2 offers modulation schemes based on DBPSK, DQPSK, DBPSK and 16QAM with Convolutional Code and Robust (repetition) options which are selected depending on the data service characteristics required. A raw data rate of between 4.5kbps and 298.2kbps can typically be achieved depending upon channel allocation and modulation type selected. The standard has theoretical targets of >300kbps and ≤500kbps The MAC layer is based upon IEEE 802.15.4 using CSMA/CA, with the architecture supporting L2 mesh or L3 routing.

G.hnem

G.hnem has been developed by the ITU-T in cooperation with members of the G3-PLC and PRIME Alliances, as an evolution of G.hn with ‘em’ standing for energy management.

It forms part of a set of ITU-T standards covering the respective MAC layers for G.hnem, G3-PLC and PRIME, with ITU-T G.9901 capturing Power Spectral Density and PHY requirements. It operates between 10kHz and 490kHz with 128 or 256 subcarriers available. In the PHY layer G.hnem offers modulation based on 16QAM. A raw data rate of up to 1Mbps is stated depending upon channel allocation and modulation type selected. The MAC layer uses CSMA/CA with support for L2 or L3 switching/routing mechanisms.

Status

Active	IEEE 1901.2a-2015 (Amendment to IEEE Std 1901.2-2013)
Active	ITU-T G.9904 (2012) – PRIME v1.4 - Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME v1.4 networks
Active	ITU-T G.9903 (2017) – G3-PLC - Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks
Active	ITU-T G.9902 (2012) – G.hnem - Narrowband orthogonal frequency division multiplexing power line communication transceivers for ITU-T G.hnem networks
Active	ITU-T G.9901 (2017)- Narrowband orthogonal frequency division multiplexing power line communication transceivers - Power spectral density specification

Table 8: Latest Narrowband (NB) PLC standards

Applications

- Electricity Smart Metering
- LV Grid Control & Automation

Sources:

1. Telecommunications Networks for the Smart Grid, A Sendin, M Sanchez-Fornie, I Berganza, J Simon, I Urrutia 2016
2. https://www.trialog.com/en/technical-overview-of-g3-plc/
3. http://www.prime-alliance.org/wp-content/uploads/2014/10/whitePaperPrimeV1p4_final.pdf
4. http://www.g3-plc.com
5. https://www.itu.int/rec/T-REC-G/en
6. https://www.comsoc.org/blog/ieee-19012%E2%84%A2-%E2%80%9Cstandard-approved-driven-and-sponsored-ieee-comsoc-power-line-communications-stand
7. http://www.electronicdesign.com/energy/power-line-communications-emerge-core-networking-technology

Optical Fibre Technology

Fibre-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fibre. The light forms an electromagnetic carrier wave that is modulated to carry information. Fibre has advantages over copper and radio-based technologies when high bandwidth, long distance, or immunity to electromagnetic interference are required. It is also inherently a more secure media than radio although not impervious to determined attack.

Optical fibre, along with 5G capable radio, will form the backbone of future digital environments. Transmission speeds and range are continually being improved upon and methods to improve the efficiency of the raw material (the fibre), such as with DWDM, and active components (nodes), via OTN technology for example drive the development of standards.

This section is divided in to optical fibre cable, the media, and fibre transmission, the nodes.

Fibre cable

ITU-T G.651.1	2007	Characteristics of a 50/125 µm multimode graded index optical fibre cable for the optical access network.
ITU-T G.652	2016	Covers single-mode NDSF (non-dispersion-shifted fibre). This fibre is in most of the cable that was installed in the 1980s. Optimized in the 1,310-nm range. Low water peak fibre has been

		specifically processed to reduce the water peak at 1400 nm to allow use in that range.
ITU-T G.653	2010	Covers single-mode dispersion-shifted optical fibre. Dispersion is minimized in the 1,550-nm wavelength range. At this range attenuation is also minimized, so longer distance cables are possible.
ITU-T G.654	2016	Covers single-mode fibre which has the zero-dispersion wavelength around 1300 m wavelength which is cut-off shifted and loss minimized at a wavelength around 1550 nm and which is optimized for use in the 1500-1600 nm region. designed mainly for submarine applications
ITU-T G.655	2009	Covers single-mode NZ-DSF (nonzero dispersion-shifted fiber), which takes advantage of dispersion characteristics that suppress the growth of four-wave mixing, a problem with WDM (wavelength division multiplexing) systems. NZ-DSF supports high-power signals and longer distances, as well as closely spaced DWDM (dense WDM) channels at rates of 10 Gbits/sec or higher. Optimized for WDM and long-distance cable runs such as transoceanic cables.
ITU-T G.656	2010	Medium Dispersion Fiber (MDF), designed for local access and long-haul fibre
ITU-T G.657	2016	Covers bend-insensitive single- mode fiber. FTTH application. Designed to bend at small radius.

Table 9: ITU-T active standards

SDH and SONET

SDH (Synchronous Digital Hierarchy) and SONET (Synchronous Optical NETwork) are transport protocols that utilise time division multiplexing (TDM) technology controlled by highly accurate clocks, they were developed to improve multiplexing efficiency and to enable higher transmission speeds. They also provide for greater flexibility in tributary and line interfaces. Later developments also support data planes/switches for Ethernet interfaces.

SDH is standardised by a series of ITU-T recommendations: G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH), G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks, G.707 Network node interface for the synchronous digital hierarchy (SDH) and G.957 Optical interfaces for equipment and systems relating to the synchronous digital hierarchy amongst others. SONET is formalised in several standards, such as ATIS 0900105 “Synchronous Optical Network (SONET) – Basic Description Including Multiplex Structures, Rates, and Formats (formerly ANSI T1.105) and ATIS 0600416 “Network to Customer Installation Interfaces – Synchronous Optical NETwork (SONET) Physical Layer Specification: Common Criteria” (formerly ANSI T1.416).

SONET Optical Carrier level	**SONET frame format**	**SDH level and frame format**	**Payload bandwidth (kbit/s)**	**Line rate (kbit/s)**
OC-1	STS-1	STM-0	50,112	51,840
OC-3	STS-3	STM-1	150,336	155,520
OC-12	STS-12	STM-4	601,344	622,080
OC-24	STS-24	–	1,202,688	1,244,160
OC-48	STS-48	STM-16	2,405,376	2,488,320
OC-192	STS-192	STM-64	9,621,504	9,953,280
OC-768	STS-768	STM-256	38,486,016	39,813,120

Table 10: SONET/SDH Designations and bandwidths

Active	2007	G.707/Y.1322 Network node interface for the synchronous digital hierarchy (SDH)
Active	2006	G.957 Optical interfaces for equipment and systems relating to the synchronous digital hierarchy
Active	2016	G.709(Y.1331) Interfaces for the optical transport network
Active	2016	G.959.1 Optical transport network physical layer interfaces
Active	2015	ATIS 0900105 Synchronous Optical Network (SONET)—Basic Description including Multiplex Structure, Rates, and Formats.
Active	1999	ANSI T1.416.01 Telecommunications - Network to Customer Installation Interfaces - Synchronous Optical NETwork (SONET) Physical Media Dependent Specification: Multi-Mode Fiber
Active	1999	ANSI T1.416.02 Telecommunications - Network to Customer Installation Interfaces - Synchronous Optical NETwork (SONET) Physical Media Dependent Specification: Single-Mode Fibre

Table 11: Example of SDH/SONET standards status

WDM

As the demand for transmission capacity and optical efficiency pushed the boundaries of SDH/SONET advances in optoelectronic components allowed the design of systems that simultaneously transmitted multiple wavelengths of light over a single fibre. Multiple high-bit rate data streams of 2.5 Gbps, 10 Gbps and, more recently, 40 Gbps, 100 Gbps, and 200 Gbps could be multiplexed through divisions of several wavelengths, hence Wave Division Multiplexing (WDM)

There are two types of WDM today:

- **Coarse WDM (CWDM):** WDM systems with fewer than eight active wavelengths per fibre. CWDM is defined by wavelengths. CWDM is for short-range communications, so it employs wide-range frequencies with wavelengths spread far apart. Standardized channel spacing permits room for wavelength drift as lasers heat up and cool down during operation. CWDM is a compact and cost-effective option when spectral efficiency is not an important requirement.
- **Dense WDM (DWDM):** DWDM is for systems with more than eight active wavelengths per fibre and is designed for long-range communications. DWDM is defined in terms of frequencies. DWDM's tighter wavelength spacing fits more channels onto a single fibre, but costs more to implement and operate. DWDM dices spectrum finely, fitting in excess of 40 channels into the same frequency range used for two CWDM channels. Wavelength densities of 40, 88, 96, or 120 are being offered by vendors and when boosted by Erbium Doped-Fibre Amplifiers (EDFAs)—a performance enhancer for high-speed communications—these systems can work over thousands of kilometres.

Active	2012	G.694.1 (02/12) Spectral grids for WDM applications: DWDM frequency grid
Active	2003	G.694.2 (12/03) Spectral grids for WDM applications: CWDM wavelength grid
Active	2015	G.695 (01/15) Optical interfaces for coarse wavelength division multiplexing applications
Active	2009	G.698. 1 (11/09) Multichannel DWDM applications with single-channel optical interfaces
Active	2009	G.698.2 (11/09) Amplified multichannel dense wavelength division multiplexing applications with single channel optical interfaces
Active	2012	G.698.3 (02/12) Multichannel seeded DWDM applications with single-channel optical interfaces

Table 12: WDM Standards status

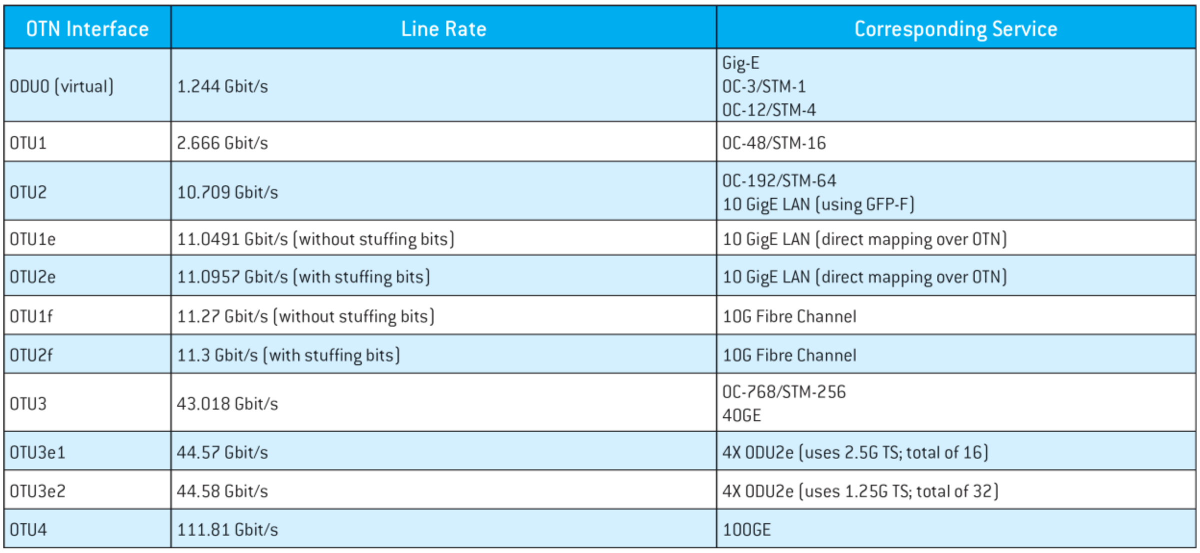
OTN

Optical Transport Networking (OTN), also commonly referred to as ‘digital wrapper’, is a next-generation, industry-standard protocol that enables various service types to be efficiently multiplexed on to optical infrastructure.

Legacy networking technologies (for example SDH/SONET) had a design reference that was linked to the requirements for transporting voice services in a circuit orientated deterministic model, however most modern traffic is packet based (even end-to-end voice eventually) and needs to support a wide range of service parameters and characteristics.

OTN wraps each client payload transparently into a container for transport across optical networks, preserving the client’s native structure, timing information, and management information. The enhanced multiplexing capability of OTN allows different traffic types—including Ethernet, storage, and digital video, as well as SONET/SDH—to be carried over a single Optical Transport Unit frame

OTNs are able to provide functionality of transport, multiplexing, switching, management, supervision and resilience of optical channels carrying client services.



OTN Interface	Line Rate	Corresponding Service
ODU0 (virtual)	1.244 Gbit/s	Gig-E OC-3/STM-1 OC-12/STM-4
OTU1	2.666 Gbit/s	OC-48/STM-16
OTU2	10.709 Gbit/s	OC-192/STM-64 10 GigE LAN (using GFP-F)
OTU1e	11.0491 Gbit/s (without stuffing bits)	10 GigE LAN (direct mapping over OTN)
OTU2e	11.0957 Gbit/s (with stuffing bits)	10 GigE LAN (direct mapping over OTN)
OTU1f	11.27 Gbit/s (without stuffing bits)	10G Fibre Channel
OTU2f	11.3 Gbit/s (with stuffing bits)	10G Fibre Channel
OTU3	43.018 Gbit/s	OC-768/STM-256 40GE
OTU3e1	44.57 Gbit/s	4X ODU2e (uses 2.5G TS; total of 16)
OTU3e2	44.58 Gbit/s	4X ODU2e (uses 1.25G TS; total of 32)
OTU4	111.81 Gbit/s	100GE

Figure 7: OTN interface data transfer rate comparison

Active	2016	G.709 /Y.1331 (06/16) - Interfaces for the optical transport network
Active	2017	G.798 (012/17) Characteristics of optical transport network hierarchy equipment functional blocks
Active	2013	G.798.1 (01/13) Types and characteristics of optical transport network equipment

Table 13: OTN Standards status

Optical Ethernet interfaces

Optical Ethernet is the physical layer of the Local Area Network (LAN) communications protocol for sending data over fibre-optic cable. Highly defined in multiple standards it is typically used for short range (in building), campus or metropolitan area network sections with direct compatibility with other Ethernet based elements.

802.3z-1998	1000BASE-SX, 1000BASE-LX	1000Mbps, Single Mode 5km, Multimode 550m
802.3ah-2004	1000BASE-BX10, 1000BASE-LX10, 1000BASE-PX10-D,	1000Mbps, Single Mode up to 10 km/20 km/40 km

	1000BASE-PX10-U, 1000BASE-PX20-D, 1000BASE-PX20-U	
multi-vendor	1000BASE-LH 1000BASE-ZX	1000Mbps, up to 40 or 100 km over single-mode fibre
802.3ae-2002	10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW	10Gbps, ranges 26m to 400m, 10km, 40km, over Single Mode and Multimode fibre
802.3aq-2006	10GBASE-LRM	Extend to 220 m over deployed 500 MHz·km Multimode fibre
	10GBASE-BX", "BiDi	offered by various vendors; bidirectional over single strand of single-mode fibre for up to 10 to 80 km using two wavelengths
802.3av-2009		10Gbps, EPON
802.3bk-2013		Extended EPON
SR 802.3by-2016	25GBASE-SR	over Multimode cabling with 100 m (OM4) or 70 m (OM3) reach
802.3ba-2010	40GBASE-SR4 100GBASE-SR10, 40GBASE-LR4, 100GBASE-LR4, 100GBASE-ER4, 40GBASE-FR	40Gbps and 100Gbps, up to 100m,150m, 2km, 10km, 40km over Single Mode and Multimode fibre
802.3bg-2011	40GBASE-FR	40Gbps, up to 2km over Single Mode fibre
802.3bm-2015	40GBASE-ER4 100GBASE-SR4	40 Gbps/ 100Gbps over Single Mode and Multimode fibre
802.3bs-2017	200GBASE-DR4, 200GBASE-FR4, 200GBASE-LR4, 400GBASE-SR16, 400GBASE-DR4, 400GBASE-FR8, 400GBASE-LR8	200Gbps, 400Gbps, up to 500m, 2km, 10km over Single Mode fibre and CWDM
802.3cc-2017	25GBASE-LR 25GBASE-ER	25Gbps, up to 10km/40km over Single Mode fibre.

Table 14: Optical Ethernet standards (Active)

P802.3ca		25 Gb/s, 50 Gb/s, and 100 Gb/s Ethernet Passive Optical Networks Task Force.
P802.3cd	50GBASE-SR, 100GBASE-SR2, 200GBASE-SR4	over multi-mode fibre with 100 m reach
	50GBASE-LR/-LR10	over single-mode fibre with 2 and 10 km reach

Table 15: Optical Ethernet standards (Development)

Optical fibre applications

- Digital substation (IEC 61850)
- Primary Substation communications
- Shared services in metropolitan/municipal areas
- Third party DER control in urban/industrial areas
- FTTH/FTTC applications

Sources:

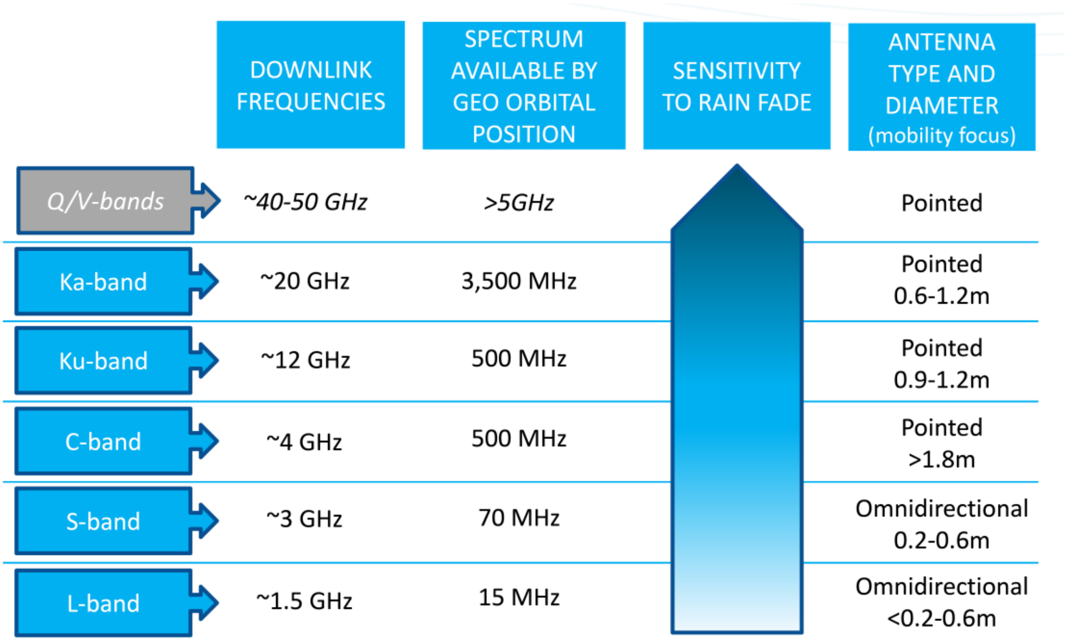
1. The Fibre Optic Association

2. Telecommunications Networks for the Smart Grid, A Sendin, M Sanchez-Fornie, I Berganza, J Simon, I Urrutia 2016
3. ITU
4. IEEE
5. EXFO
6. www.ciena.com/insights/what-is/What-Is-WDM.html

Satellite

Satellite communications is based upon the use of space stationed satellite platforms to receive and relay radio wave carried communications signals. The topology of a satellite network can be both ground station (hub/gateway) to outstation (via satellite) or a combination of outstation to outstation and outstation to ground station.

Satellite communications service terms have been defined by the ITU, with the three most relevant to this paper being FSS (Fixed-service satellite), MSS (Mobile-satellite service) and the more recent HTS (High-Throughput satellite). Their designation is linked to spectrum allocation across 3 regions, by which the world has been divided. The spectrum allocation influences the potential bearer capacity, antenna size and ability to withstand rain fade (absorption of microwave RF due to rain, snow etc. which is particularly prevalent above 11GHz).



	DOWNLINK FREQUENCIES	SPECTRUM AVAILABLE BY GEO ORBITAL POSITION	SENSITIVITY TO RAIN FADE	ANTENNA TYPE AND DIAMETER (mobility focus)
Q/V-bands	*~40-50 GHz*	*>5GHz*		Pointed
Ka-band	~20 GHz	3,500 MHz		Pointed 0.6-1.2m
Ku-band	~12 GHz	500 MHz		Pointed 0.9-1.2m
C-band	~4 GHz	500 MHz		Pointed >1.8m
S-band	~3 GHz	70 MHz		Omnidirectional 0.2-0.6m
L-band	~1.5 GHz	15 MHz		Omnidirectional <0.2-0.6m

Figure 8: Primary frequencies used for satellite communications

The Q/V bands lie between 33-75 GHz, within the Extremely High Frequency (EHF) area of the radio spectrum. EHFs have the potential enhance the performance of the next generation of High Throughput Satellite (HTS) programs by enabling the offload of satellite links between a satellite and its hubs from the Ka band to the Q/V bands. This would make more bandwidth available for users in Ka-band and would also reduce the number of hubs required.

Another key attribute is the orbit in which satellites operate. This effects latency of the service and in some models the availability of an accessible satellite at any particular time.

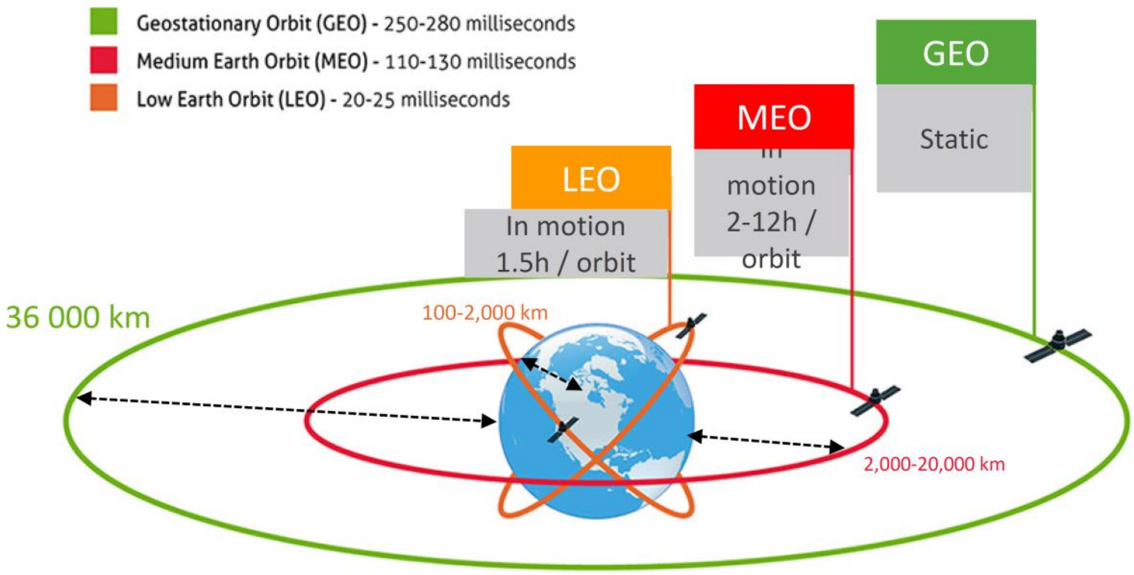

🟩 Geostationary Orbit (GEO) - 250-280 milliseconds
🟥 Medium Earth Orbit (MEO) - 110-130 milliseconds
🟧 Low Earth Orbit (LEO) - 20-25 milliseconds
GEO
Static
MEO
In motion
2-12h / orbit
LEO
In motion
1.5h / orbit
36 000 km
100-2,000 km
2,000-20,000 km

Figure 9: High throughput Satellite (HTS) programmes

MSS terminal (L-Band)	Data rate
M2M s&F	<10kbps
Handheld	2-60 kbps
Broadband	128-800 kpbs

VSATs(C, Ku & Ka-band)	Data rate
Low data rate	0.056-1Mbps
High data rate	1-5 Mbps
Very high data rate	>5Mbps (typical max 16Mbps)

Table 16: Effective terminal access capacity at present

Satellite applications

- Environmental monitoring
- Secondary substation connection
- Primary distribution substation connectivity
- Distribution network reclosers
- Asset condition monitoring
- Rapid deployment for disaster recovery
- Pipeline monitoring
- Compressor monitoring
- Well site automation
- Video Surveillance
- Out-of-band management to primary site communications

Active	2015	ETSI TS 102 292 V1.2.1 (2015-07) - Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks
Active	2011	ETSI TS 102 855 V1.1.1 (2011-03) - Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM);

		Interworking and Integration of BSM in Next Generation Networks (NGNs)
Active	2017	ETSI EN 301 428 V2.1.2 (2017-05) - Satellite Earth Stations and Systems (SES); Harmonised Standard for Very Small Aperture Terminal (VSAT); Transmit-only, transmit/receive or receive-only satellite earth stations operating in the 11/12/14 GHz frequency bands covering the essential requirements of article 3.2 of Directive 2014/53/EU

Table 17: Examples satellite standards

Sources:

1. Euroconsult for Inmarsat - EC-Inmarsat-Capital-Markets-Day-2016
2. ETSI

Trends and future direction for communications networks

- As the topology, or hierarchy, of power grids is changing, with the introduction of large scale dispersed renewable generation, distributed energy resources and new consumption actors with new profiles (e.g. EV), so too must change the logical and physical models for the components that support grid management, safety and balancing. Communications is no exception and the requirement for greater penetration of monitoring and control, and of the application of analytics and automation, along with consumer integration, all leads towards the need for a revised approach.
- The energy industry is in a state of flux with development and implementation of technological advancement proceeding at different rates across Europe due to a range of influencing factors, including but not limited to: regulatory mandates, government influence and stimulus, market opportunities, and local operational / business priorities to name a few. What is clear though is a requirement to ensure that, given the known dynamic state, development and investment is flexible or forward thinking enough to avoid constrained capability a short while on from delivery.
- Equally as important and increasingly evident for success is growth in collaboration based (end to end) services. These can be formal or informal, but the key is in the working together, rather than delivery of systems through a hierarchical series based contractual programme. The complexity of modern and future solutions requires a whole system approach to manage the many integrated components and to ensure process integrity and outcomes.
- Not only is there a need to successfully convene collaborative solutions from different providers, but there is also a recognition that present and future requirements will be optimally served by a hybrid approach to communications technology selection, whether in the last-mile, in the access or backhaul sections. And this in turn requires a common or universally compatible integration capability. An example of this is the position taken by the GSMA that predicts and accepts that services in a 5G future will be interdependent upon enduring 4G, optical fibre, satellite and other technologies.
- The prevailing trends in technical capability, relevant to the energy industry are in part being driven by the grid topology shift mentioned above, and in addition are being influenced by core and field network developments such as deployment of OTN (Optical Transport Network), SDN, (Software Defined Networks) and NFV (Network Function Virtualisation) capability. Further out in to field Edge/Fog computing and developments in 4G, 5G, broadband satellite and LPWA technologies are having the greatest impact. All of this has the aim of increasing flexibility, data efficiency, commercial advantage, service specific functionality/performance, and reactive and pre-emptive resilience.

1.5.2 POWER GRID OPERATION

The main challenges

Obviously, the key challenge to modern or future power grids is to accommodate more clean, renewable resources, such as solar power, wind power, small hydro, biogas, biomass, geothermal, tidal power etc. The common characteristic for many of these clean renewable resources is that the power output is intermittent and less predictable, resulting in the difficulties on power balancing and frequency synchronization of all generators.

Another key challenge is given by the need to significantly increase the efficiency of the whole system while optimizing the use of the available assets. While the aforementioned challenges impact also the transmission network, it should be noted that Transmission System Operators (TSO) have been involved in a process of digitalization of the infrastructure already for quite some time.

The impact on the distribution system is vice versa more critical because this portion of the network used to be a passive system characterized by a unidirectional power flow. However, in the future's distribution network the bi-directional power flow will take over, therefore not only all the protections and controls need to be refurbished, but also the stability of the optimal power flow needs to be considered in distribution networks.

Digitalization and the automation system

Digitalization has a large impact on the architecture of the automation systems in the power grid. The process of digitalization in the substation has been tremendously enhanced by the development of the IEC6150 family of standard that brought IP technology in the substation. The progressive need of automation at distribution level though created interest in exploring new automation architectures that can better fit the large scale of the distribution grid and the intrinsic locality of the operation.

Distributed intelligence- Multi-agent systems

As mentioned above, the locality of the action together with the large scale of the infrastructure has led to consider the use of Distributed Intelligence is a possible solution for Distribution System Automation.

Recent research projects such as FP7 IDE4L (Ideal Grid for All) proposed a complete architecture for Distribution Automation based on mix of hierarchical and distributed solutions. The key element of novelty for an Active Distribution Grid Management is the need of smart devices in each of the substations. While this process is already going on for primary substations, it is expected to be extended in the short future also to secondary substations. A complete description of an architecture implementing full observability up to the Low Voltage feeders can be found in deliverables from the IDEAL project (IDE4L project). More advanced architectures envision a flatter architecture in which the intelligent units (usually called agents) coordinate using a peer to peer approach. While a complete overview of applications in power systems has been presented already a few years ago (McArthur , 2002), this area is still the focus of significant research. Concepts such as Web of Cells proposed by the project ELECTRA could be seen as a recent application of such (peer to peer) approach.

Independently from the automation architecture, some key functions are emerging as key for an Active Distribution Grid Management. These can be summarized as:

- Monitoring: execution of a state estimation algorithm for Medium Voltage and possibly Low Voltage Grids;
- Fault Location Identification and System Restoration (FLISR): this function deals with the exact location of a fault and with the determination of the appropriate action to limit the impact of the fault;
- Load and Generation Forecast: forecasting functions are critical to identify possible critical situations of operation;
- Generation Control: this function deals with the possibility to act on the power insertion from Distributed Energy Resources. It mostly identifies with Generation Curtailment.

Such functionalities can be implemented using traditional algorithms extended for distribution grids by using more modern approaches based on Data Driven solutions and Artificial Intelligence.

It should be also highlighted that the expected deployment of 5G wireless networks will also enable the implementation of the aforementioned functions by means of virtual machines running in the edge cloud. In such a scenario the substation automation is significantly simplified, and the complexity is moved to the cloud.

Cloud based solution, data platforms and Internet of Things

As already introduced in the previous paragraph grid automation is moving more and more away from the traditional architectures based on centralized logics. This trend, mostly driven by the geographical distribution of the actors (including the customers) is calling for scalable, flexible and reconfigurable computational platforms. Cloud technology offers the perfect solution to these types of challenges. It should be clarified that using cloud technology does not mean necessarily using public cloud implementation but simply the adoption of a flexible scheduling of the computational capabilities.

While many manufacturers are offering a variety of cloud platforms, some generic architectural concepts can be still identified.

A common 5-layer platform architecture for cloud solutions comprise an Adapters Layer, a Data Storage Logic Layer, a Data Access Logic Layer, a Service Logic Layer and a Presentation Layer. The 5 layers comprise an Adapters Layer, a Data Storage Logic Layer, a Data Access Logic Layer, a Service Logic Layer and a Presentation Layer. Cloud platforms normally use a service-oriented architecture (SOA) where each layer offers simple, extensible APIs to its users, which can be other layers or, for the Presentation Layer, Platform-external applications. SOA hides underlying complexity which is suitable for implementation in a distributed cloud computing environment.

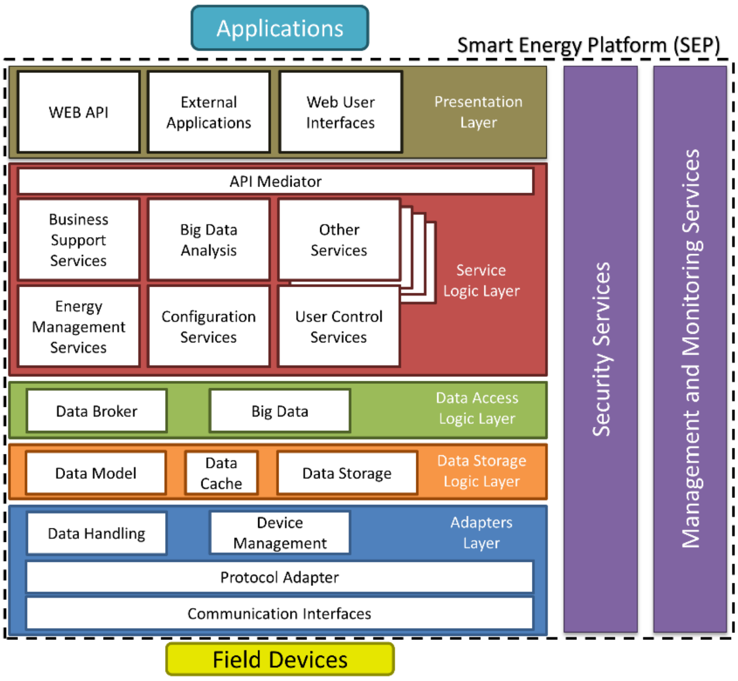


Figure 10: A reference architecture for cloud solutions

The Adapters Layer (AL) supports miscellaneous communication interfaces, for data exchange and acquisition, towards the various Smart Energy devices (in electricity grids, buildings etc.). This layer provides the connection between the field devices and the Platform and interprets the different protocols used by these devices, whether they are standardised protocols (e.g. Automation architecture IEC 61850, IEC61599, Open-ADR etc.) or custom protocols, used by particular devices. This means that SEP, through its south-bound interface, is able to deal with a number of different data syntaxes and semantics. Therefore, the Protocol Adapter is flexible and extensible, in order to be compatible with present and future protocols used by field devices. Internally, SEP maps these protocols onto its own unified data model, upon which its north-bound services are based. The core asset of the SEP is; therefore, this unified data model, that resides in the Data Storage Logic Layer (DSLL).

Data coming from the Adapters Layer is mapped by the DSLL onto the unified data model and then stored. The Platform incorporates two data storage systems, one short-term data cache, meant to contain those data that are requested more frequently or to access live data coming from the field devices, thus speeding up their retrieval, and a long-term data database, that retains all data passing through the Platform. The unified data model unifies the underlying device data models based on a common semantic model.

The Data Access Logic Layer (DALL) receives requests from the services on the upper layer and provides them the data they need. It can also push data to the devices, like configuration data or commands coming from the services running on the Platform. The DALL also includes a Big Data access block to manage Big Data storage.

The Service Logic Layer offers a set of services to Smart Energy actors, supporting them in their roles and hiding the underlying complexity involved in implementing the services.

The last level is the Presentation Layer, which represents the entrance door to the Platform. External applications connect to this layer in order to communicate with the Platform. Alternatively, applications may be located directly here in the Presentation Layer and use the lower-level Platform layers from here. This means that every application makes use of the Presentation Layer in different ways, ac-cording to their architectures (e.g. thin or thick client).

The two right-hand side vertical layers identify the services needed at every level of the Platform, and hence go through all the other layers. These services provide security for the Platform and for its own management and monitoring. The security services cover a number of aspects involving Users' access to networks, services and applications, including identity management, used for authorising external services to access personal data stored in a secure environment.

While no real standard architecture is so far emerged in this field, a notable example is given by the FIWARE approach developed within the Future Internet PPP of the European Commission. Such a platform is, in particular, emerging as a solution for Smart City platform implementations but extensions for energy systems have been also proposed[1].

Connected to the concept of platform is also the concept of Internet of Things (IoT). The idea behind IoT is the possibility for every object to be connected and to be able to communicate. Each object has a corresponding address and a form of identifier through which it can exchange data with peers or with a suitable cloud platform. This paradigm is evolving particularly in the context of Smart Cities as a way to incorporate a massive number of sensors of different nature in a cloud context to provide knowledge as result of the processing of non-homogeneous information. Similar concepts apply also to the energy systems and fits in the general definition of cloud application as reported above. Example of “things” in the energy sector can be given by sensors displaced in the network as well as controllable devices as, for example, appliances at home. Also, for this sector the process of standardization is critical for wide-spread application. Different initiatives in this direction are currently under development (e.g. IoT Alliance for Innovation).

1.5.3 DIGITAL TWINS

1. Introduction

With the development of IoT, the new concept of Digital twin, which refers to a digital replica of physical assets, processes and systems that can be used for various purposes, has been proposed in recent years (from Wikipedia). Digital twin is a software representation of a

[1] See for reference www.finesce.eu

physical asset. Digital twin technology enables companies to better understand, predict and optimize the performance of each unique asset. A digital twin can represent an individual asset, an integrated system or a fleet of assets (https://www.ge.com/digital/predix/digital-twin). Actually, in the area of electric power system, the physical model or digital modelling for power grid has been employed for analysing the performance of the system behaviour or control for very long time, such as dynamic physical modelling system, real time dynamic simulation system (RTDS), etc. However, all these modellings only can be available for off-line analysis while it is hard to model the whole system on-line and in real time giving the operators more comprehensive, predictive and fast instructions or decisions in time. Obviously, the development of IoT and the parallel computation techniques provide an opportunity to fulfil this task.

2. The benefit of the digital twin in IoT

The value of the digital twin in the digital grid is listed below:

- Visibility, all the physical assets including the topology of the system can be connected in the cloud; the digital twin can supply the visibility of the operating status of the physical assets (including switchgears and controlling devices and system) and power grid system to the operators and their customers. It can even supply the 3-D virtual twins of devices for visibility and supervisory.
- Predictive and security analysis on-line, the operating status of the physical assets or the whole grid is linking with the digital twin models, therefore the on-line predictive analysis or security analysis can be provided by the digital twin. For example, the on-line N-1 analysis for static or dynamic security analysis (both N-1 and security analysis are actually what-if analysis) for the power grid. Or another example is the asset predictive life analysis to help the operators to make the optimal maintenance and service plan for power assets.
- Comprehensive optimization to seek the maximum profits, the operating status of all power assets are uploaded into the digital twins, therefore the digital twins can provide the comprehensive optimal solutions for power grid operation, including power dispatching and marketing optimization, power flow optimization, power asset life and maintenance and service optimization, etc.
- Improving the design of assets and control devices and control systems. Digital twins are the real-time virtue projection of the real physical assets, therefore can be employed to test the performance and behaviour of the assets or the corresponding control system, and subsequently improve the design of the assets and/or control system.

3. The structure of a digital twin

The digital twin is actually the digital model focusing on various special aspects for the corresponding physical asset. For example, for the power grid, the digital twin could have power grid anomaly models, power flow operating models, transient/dynamic stability models, fault models, transient behaviour models, etc. For a power generator, it could have life models, anomaly models, thermal models, transient models, etc.

By acquisition of field data, the digital twin can mimic the operation of the real system, based on the models, combining the customer KPI, which is actually the objective for the optimization, the optimal solutions for business, operation, assets management as well as the advanced control (including the aided strategy and information for fast control, or even for adaptive protections) can be available. Based on these acquired data, the predictive diagnostic of the asset or system can be made, where the severe fault can be likely avoided.

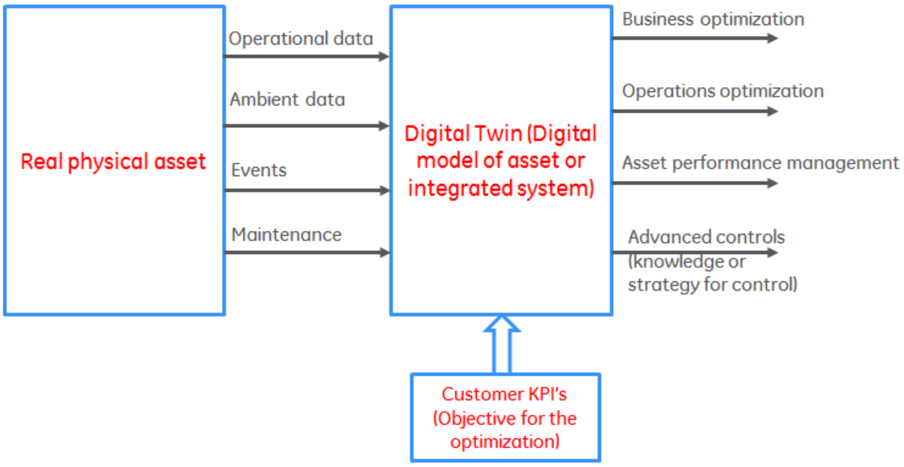

Real physical asset
Operational data
Ambient data
Events
Maintenance
Digital Twin (Digital model of asset or integrated system)
Business optimization
Operations optimization
Asset performance management
Advanced controls (knowledge or strategy for control)
Customer KPI's (Objective for the optimization)

Figure 11: The structure of the digital twin

4. Application of Digital twins in digital power grid

The digital twins of the power grid comprise Asset Model, Fault/Thermal model, Operational Model, and Business Model. See Figure 12.

Business Model, Optimal power dispatching, on-line power marketing and trading

Operational Model, optimal power flow distribution, increasing the efficiency of the power transmission and distribution, reduce the cost to the minimum.

Fault/Transient model, prediction of an potential fault, for example, the overload prediction, out-of-step prediction to avoid such fault happening. Optimizing the advanced control strategy lists.

Asset model, Asset Performance Management, Health prediction, early fault detection, performance and efficiency optimization

Figure 12: The application of digital twins in power grid

- Advanced Assets Management and optimal performance and efficiency of Power assets.
  The Asset model of digital twins are typically used in applications for maintenance and equipment healthy, predictive maintenance and healthy diagnose. For example, a digital twin of a beaker can provide the whole vision of the breaker with all the necessary parameters, and the record of real-time operating status, such as conductor status (such as conductor temperature), insulation status (discharging, insulation density, pressure, etc), ambient status, operating status (current and voltage), as well as the breaking time, etc. Based on these data, the behaviour of the breaker (prognostic early fault detection or diagnose) can be predictively analysed, therefore the optimal maintenance and service plan for the breaker can be made.
  Another example, a thermal model of digital twin of a transmission line can provide all necessary information of parameters, real-time current or power, ambient conditions, so that the dynamic rating can be provided on-line.

- Optimal emergency/ advanced control and protection
  Fault/thermal model of the digital twin of power grid can do the what-if analysis of the power grid to detect the potential risk of fault or over-heat in the grid (same as the N-1

analysis or security analysis of the grid). And for the stability control of the power grid, the fault model can offer the most effective and optimal solution lists (control strategy list) by what-if analysis in the fault model. Once the fault happens, the control strategy list can supply the fast effective and optimal solution to stabilize the system.

- Optimal power flow
  The operational model of power grid could be also included in the digital twins, which is used for calculating the optimal power profile (distribution), which objective is to reduce the transmission and distribution costs meanwhile to increase the efficiency of transmission and distribution.

- Optimal dispatching/on-line trading
  For power grid, the digital twin comprises business model, where the on-line trading is carried out. The business model is based on the power balancing equations, with the objective of maximum profit or lowest costs combing with the lowest emissions (green). The predictive analytics of the operation data can supply the pricing solutions for marketing. The intelligent optimization techniques can be used for avoiding the convergence of the solution to partial optimum. Parallel computation and distributed intelligence techniques may be used for solving the large-scale non-linear optimization problems.

5. Associated technology
   - Power devices and power system modelling;
   - Predictive analytics;
   - Big data;
   - Artificial intelligence, distributed intelligence;
   - Parallel computation;
   - Intelligent system optimization;
   - Knowledge/expert system;
   - Fibre security;

Unmanned Aerial Vehicle (UAV)
Commonly known as “drones”, UAVs are currently in use and experimentation in several utilities. Regulation is currently limiting their scope of use, for example the obligation for the pilot to stay in the line of sight.
Small UAVs can accomplish **surveillance and data collection** missions, with a variety of captors, from digital high-resolution or infrared cameras to LIDAR (Laser Detection and Ranging). A variety of asset-management tasks are simplified by UAVs, such as tower painting commissioning, substation, towers and lines inspection, hot spots locating, vegetation proximity checks. In the future, those missions may be extended. For example, one can imagine UAVs automatically taking off to a substation after a problem was signalled either the SCADA system or the intruder alarm and provide quick damage assessment. A 3D cartography of the utility aerial assets could also be performed and actualized by autonomous drones.
Bigger UAVs can carry substantial payloads and be a cheaper or safer counterpart to helicopters. For example, a pulling rope can be passed between two high voltage towers by the drone and used to pull a power cable. As the technology grows mature, more complex work will be possible, such as live works operated from the ground. Dirigibles can also pave the way to more important payloads.

UAVs will enable quicker and cheaper maintenance operations leading, amongst others, to a better availability of the assets.

Figure 13: A drone in operation for RTE

1.6 TECHNOLOGIES AT THE BUSINESS LAYER

1.6.1 VISUALIZATION TOOLS

With digitalization the available data grows fast and becomes increasingly complex. Therefor the presentation of data has been evolved from simple graphs and pie-charts to very elaborated interactive visualizations based on real-time data sets. Data projects bring in large number of structured as well as unstructured data sources. New available techniques like Virtual Reality (VR) and Augmented Reality (AR) now offer related stakeholders like researchers, consultants, users and decision-makers to step 360-degree around inside data, reactive intuitively and touch and manipulate what is shown. Based on machine learning AR/VR-reporting will help to unlock the data potential of businesses and organizations. With the uptake of these new visualization and reporting tools the presentation of complex information is thus no case for individuals but can be fulfilled for more than one person at the same time by touching and manipulated it.

Definition of the technology

The choice of a visualisation tool depends primarily on the type of data generated, ease of adaptability and performance. Choices for visualisation vary from pre-compiled tools to libraries. Either way, data-driven visualisations are always backed by an appropriate database management system. Pre-compiled tools provide a limited number of possibilities to visualise the data, whereas using libraries to code a custom dashboard gives access to a wide collection of visualisation techniques.

The popularity and ease of use of web-based visualisation tools have made obsolete graphic user-interface services such as Java Abstract Window Toolkit, Matlab plot functions and Python's matplotlib library. However, these are preferred in case of quick prototyping over eventual deployment.

Possible applications

Described here are three options to explore web-based visualisation techniques classified by the type of data generated by the system.

- *Visualization of Time Series Data.* In most cases where there is data showing progression of the state of a system over time, a Time Series Database (TSDB)2 is used and attached to it, a visualisation tool optimised for time series data. This is handy for real-time monitoring of the system and also allows the viewers to traverse back to a time of interest and investigate a particular event or state of the system. Examples of such databases are

[2] A Time Series Database is one in which data is indexed by time

InfluxDB3, Graphite4, etc. and an example of a visualisation tool optimised for such data is Grafana5. Graphite also has its own native visualisation tool in the same package as the database.

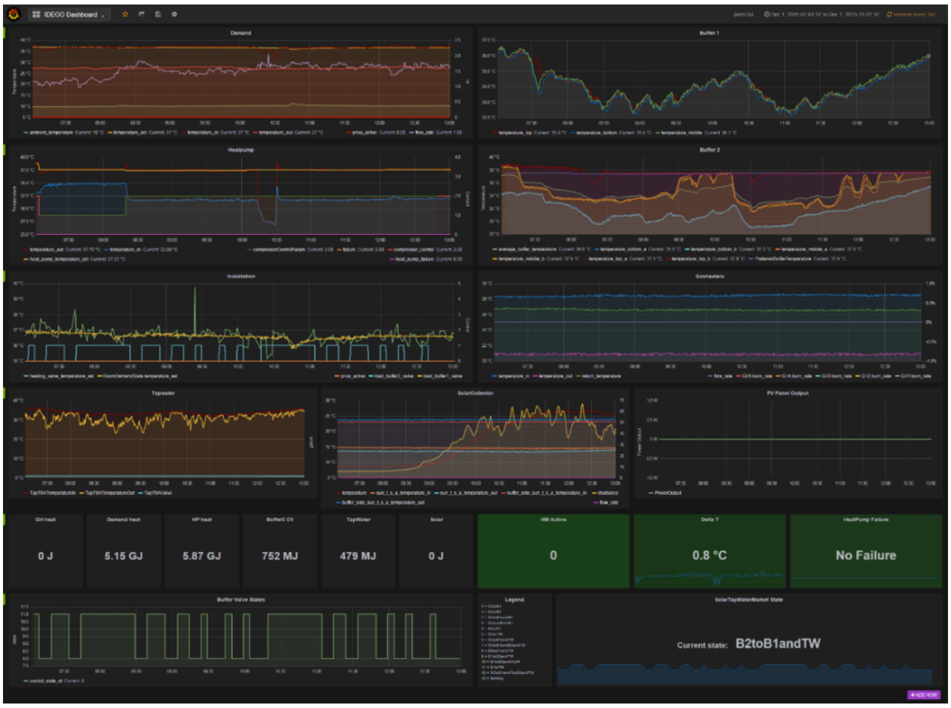


Figure 14: Example of a Grafana dashboard monitoring a heating installation in real-time. The dashboard consists of measured as well as aggregated data, visualised using different methods such as graph panels, static number panels, spark lines, etc.

- *Visualization of Search-Optimised Data.* Sometimes the progression of system state is redundant and the data to be visualised are analysis results or pre-defined KPIs. In such cases, a database and visualisation system optimised for searching of data content may be more adequate. Examples of such tools are Elasticsearch6 and Kibana7. The key difference here is in tagging the generated data with metadata to enable classification and eventually help search for it.
- *Visualization of Custom Visualisations.* The advantage of using a pre-compiled visualisation tool such as Grafana or Kibana is that it takes care of all the backend services necessary to enable the visualisation and some more. For example, the server hosting the dashboard itself, authentication mechanisms, UI for querying data, etc. The disadvantage however, is that it may not have the right type of visualisation that is needed for a project. For example, a tree-like depiction of the topology of an electrical network. Tools like Grafana have a library of plugins allowing users to develop and deploy open-source custom visualisations to cater to this need. In such projects, it makes sense to take a step back and visualise using JavaScript libraries such as D3. D3 is a JavaScript library for manipulating HTML documents based on data using SVG and CSS. There is an entire collection of visualisation options with such a library containing static visualisations, interactive ones and even animations. And the list expands regularly with more users actively developing each day.
- The downside to using such custom visualisations is, as explained before, the extra effort in enabling the visualisation, such as hosting the page, querying the database, etc.

[3] InfluxDB - https://www.influxdata.com/
[4] Graphite - http://graphiteapp.org/#overview
[5] Grafana - https://grafana.com/
[6] Elasticsearch - https://www.elastic.co/
[7] Kibana - https://www.elastic.co/products/kibana

1.6.2 FLEXIBILITY AGGREGATION PLATFORMS

- **Definition of the technology**
  Flexibility aggregation platform is an advanced ICT system for aggregation of flexibility resources (loads, distributed generators and storage) into a clean energy asset which acts like a conventional peaking power plant. Its deployment is possible in different variations known as Energy Management Systems, Demand Response System, Virtual Power Plant and Virtual Battery, allowing flexibility to be utilized on all five power system levels (local, community, DSO, TSO, cross-border) and monetized on different electricity markets (day-ahead, intraday market, balancing, TSO/DSO ancillary services, etc.).

A flexibility aggregation platform participating at any electricity market, needs to comply with the rules and requirements defined either by market operator, power exchange, TSO or DSO. General requirements for flexibility aggregation platforms covering most of the markets are:

- Reliable operation and service delivery. It should be reliable, providing reliable services with redundant state-of-the-art features.
- Secure data management. It should meet security requirements, ensuring data security aspects on all levels.
- Integration with market platform. It should be able to connect to market platform to exchange data (bids, aggregated baselines, activation triggers, set-points, aggregated measurements, etc.) in both directions.
- Integration with flexibility units. It should be able to connect with Direct Load Control (DLC) systems, distributed generation and storage units via standardized communication protocols to exchange data (baselines, activation triggers, set-points, measurements, etc.) in both directions.
- Optimally aggregate flexibility units. It should perform aggregation based on different sets of criteria and objectives in order to meet, one side owner's business model requirements, and on the other market/TSO/DSO requirements (including N-1 and similar). Furthermore, it should have a mechanism to create a priority list and place flexibility units in the ascending order by their costs/reliability/activation frequency and pick the most appropriate one when called for activation.
- Calculate consumption, generation and flexibility forecasts of units. It should be able to calculate these forecasts on the unit and pool level with sufficient data granularity and accuracy.
- Measurement and verification methodology (baseline). It should be able to calculate the amount of capacity and energy delivered as flexibility service to different markets according to its baseline rules.
- User interface for administration and operation. It should be able to visualize processes and enable user to operate flexibility platform with a user-friendly interface.

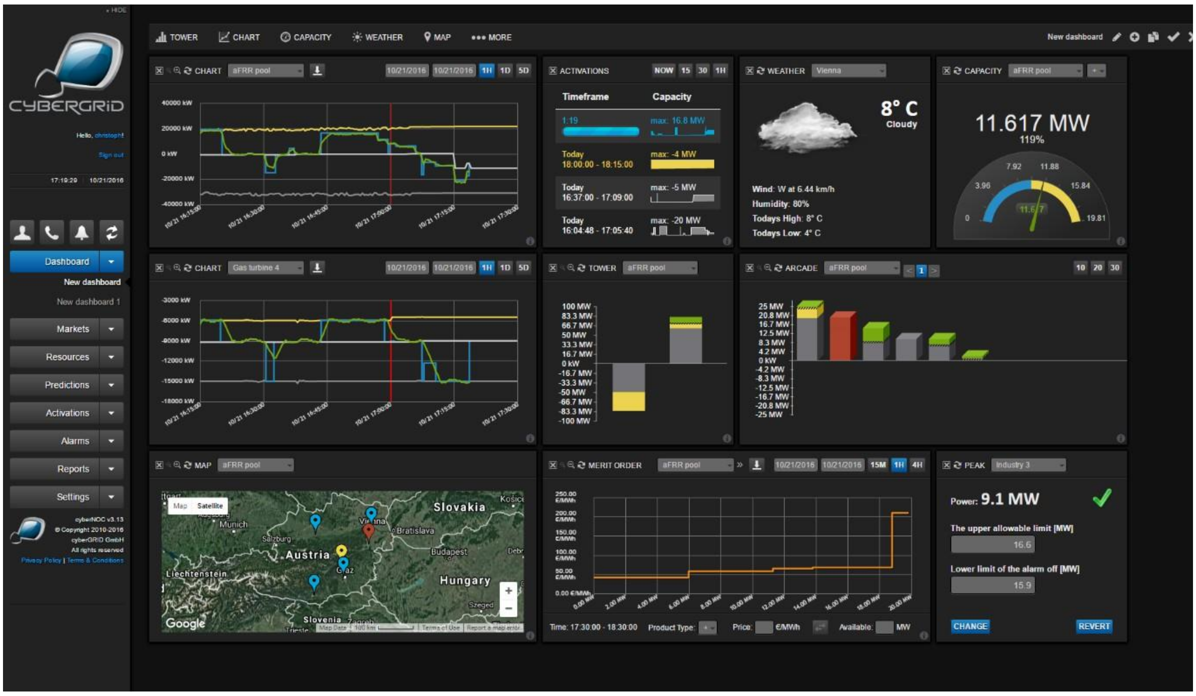


Figure 15: Example of deployed flexibility platform (aFRR and mFRR Virtual Power Plant)

Possible applications

Flexibility aggregation platforms can be deployed as Energy Management Systems (EMS); Demand Response System, Virtual Power Plant and Virtual Battery:

- EMS and Demand response system aggregates mostly flexibility of consumers. This means mostly loads, but also distributed generation and storage, located behind the meter and not exceeding the consumption levels.
- Virtual Power Plant aggregates mostly flexibility of distributed generation. This means primarily RES and CHP, sometimes also diesel back-up systems. In some cases, loads and storage can be added as well.
- Virtual Battery aggregates flexibility of batteries.

In all three cases the resulting flexibility service must be of suitable quality, reliability and profile to match targeted market(s) requirements.

1.6.3 DATA ANALYTICS AS A SERVICE (SAAS)

Definition of the technology

The ongoing international smart meter deployment has led to the installation of more than 1.000 million smart meters (electricity, water and gas) in 2017, and this number is expected to reach more than 1.600 million by 2020[8]. This means that a huge dataflow of raw data is being generated with a massive potential to generate benefits for the overall energy value chain if the proper data analytics capabilities are in place.

As an example, assuming a 1 million smart meters deployment using 15-minute data would be responsible for 35 billion data entries totalling 2920TB of data per year, from smart metering data alone. Nonetheless, for several energy related data analytics applications, other sources of data are also extremely important (like weather data, buildings data, cloud coverage data, etc.) adding up to the big volume of data that needs to be processed to produce meaningful information form smart metering data.

These trends clearly justify the extreme importance that Big Data and analytics are gaining within the energy sector. This vast amount of raw data that is currently being generated from

[8] https://www.statista.com/statistics/625890/worldwide-smart-meter-deployment/

smart meters and other IoT devices, or made available through existing API's, is creating the base for the application of advanced data analytics modules that can effectively support energy utilities business layer in several business cases and applications.

Status and current on-going research

Looking at the foreseen expansion of the bidirectional energy production/demand value-chain, for an effective management of the grid it is necessary that the system may be capable of detecting faults in the grid and ensure the health of the grid (harmonics, voltage, current).

An important way of guaranteeing the health of the grid is to have a robust demand predictive model. Coupling to that, the increase of DER requires that the individual production of each system is also predicted. With the increase of the processing power of computers, the deployment of advanced data analytics methodologies to implement added-value services to the grid becomes increasingly feasible.

The development of these big data analytics services that seek to add value to the whole energy value-chain are relying more and more on the so-called 'artificial intelligence' (AI). The AI concept has various definitions, all agreeing that an AI algorithm should be able to learn and adapt along the evolvement of the conditions of the setup.

Some of the most relevant AI models are the following:

- Neural Networks. Neural networks (NN) are non-linear models with an architecture that was inspired by the way the human brain reasons as a dynamically time-continuous system. NN compute the weight given to each input, learning those that generate the outputs to which the model performance is the highest. This weight-learning process is achieved through the interactions between the neurons of the NN ('synapses').

  NN are adequate when the mathematical inter-dependencies between the variables of the system are unknown, when addressing a multi-dimensional problem and when there is no requirement of interpretability of the model. In this way, NN process in a closed way, generating the optimal result under a structure that is not interpretable by the user.
- Reinforcement Learning (RL) is a computational method that is recognized by its simplicity and easiness to implement. This methodology operates through a reward-system that penalizes solutions that diverge from optimal solutions and rewards those that converge to the optimal solution. RL is an adequate method for adaptive control due to its capacity to converge to the optimal solution and can adapt to the dynamics of the system, changing the weight vector accordingly to re-converge to the optimal solution (e.g. minimizing discomfort or cost).

Regarding the optimization methods for control strategies to enable Demand Response (DR) programs, the standard models (e.g. linear/non-linear programming, convex programming, stochastic rule-based models) suffer from the drawbacks of lack of adaptiveness to different contexts, and lack of scalability. Heuristic and metaheuristic models are emerging to tackle multivariable optimisation problems dealing with complex problems and being able to converge to optimal values with low supervision. Coupling with self-learning algorithms, these promise to tackle effectively DR.

Heuristic models have been developed to take 'non-rational' decisions combining the input variables in different ways and select those combinations with which the model converges to the minimization of a cost function. The cost function is the mathematical definition of what we want to minimize (e.g. cost, discomfort). The most common heuristic models are the evolutionary algorithms such as genetic algorithms:

- Genetic Algorithms (GA). GA have been designed to mimic the Darwinian principle of evolution, where the fittest species to the adversities of their surroundings are the ones that survive. In this way, GA models search for the optimal solution (the one where the outputs of the model converge to the minimization of a cost function) within a limited number of possible solutions (population). The population members is characterized by a vector ('chromosome') that has its own objective value (fitness) that changes at each iteration, selecting the chromosomes with the highest fit through mutations and crossovers.

Recognizing the extreme diversity of existing energy consumers along with the need to be able to address them as unique consumers, acknowledging their individual needs and consumption profiles, other data analytics methods like clustering approaches can also be coupled to models, which identify the degree of similarity between variables (e.g. consumption profiles of end users or geographical demand/production in the grid) and their importance in the performance of the models.

Clustering techniques reveal their importance when the performance of self-learning algorithms does not suffice due to the high complexity of the system. These techniques help identify which are the most important variables that affect the final result of other models (e.g. predictive or control optimization models).

Possible applications

One concrete example of the application of data analytics to provide innovative services to the energy consumer and extract value to the whole value-chain is a method entitled Non-Intrusive Load Monitoring (NILM) which from the aggregate energy consumption data obtained from smart meters, can identify the existence and the energy consumption allocated to the main residential appliances or energy services. This approach may incorporate various hybrid methodologies including pattern recognition, clustering, time series, multivariate modelling, machine learning among others, relying only on data from the most common smart meters, coupling it, when necessary, with other exogenous streams of data.

From the new layer of information generated through smart metering data and NILM, utilities are able to better engage with their energy consumers providing targeted advices that and will for instance also be able to better understand their consumption dynamics identifying which ones are more suited for DR programs.

The application of several data analytics methods mentioned above will allow the energy value chain actors to achieve:

- Better consumer segmentation;
- Improved load forecasting for optimized intra-daily energy market usage;
- the delivery of new services (made available through cloud-based platforms) focused on improving consumer engagement by providing the energy consumer with targeted energy efficiency measures, taking advantage of NILM;
- Better Demand Response program planning for utilities through added knowledge regarding the consumption dynamics of energy consumers;
- Achieve a better understanding of the real-time penetration of DER on the grid;
- Diversifying revenue streams through automated dimensioning and proposal of renewable DER and storage solutions;
- Real-time identification of anomalous consumptions based on historical data.

Forecasting technologies in the service of digitalization.

Forecasting functionality is an important component in the intelligence layer of modern energy systems. Several types of short-term (few minutes to days ahead) forecasts for load, renewable generation, head demand, dynamic line rating, market quantities etc, are needed by different actors and applications.

For decades efficient models have been developed to forecast electricity demand at regional/national level with a good performance in the order of 1%-3%. Research continues since demand profiles at this scale change as new usages, active demand programmes etc require introducing new features to classical models to explain these evolutions. Moreover, due to the scale, even small improvements in the accuracy of the forecasts have a high economic impact.

The emergence of smart grid applications in distribution grids, like management of smart-homes and microgrids or flexibility provision by aggregators, have made it necessary to develop forecasting approaches for electricity demand at local level, from customer/building to feeder. This has been feasible thanks to the availability of smart meter data in the last years. Research focuses on load profiling, segmentation and forecasting. First operational models have been implemented in several smart grid demonstration projects (i.e. H2020 Sensible), where performances are in the order of 29% error for houses with an acceptable quality of data (Gerossier, 2017). A crucial aspect for this application is the possibility to have frequently updated data from smart meters so that they can be used for intra-day prediction. This is not always the case. In addition to load forecasts, in several applications it is necessary to have forecasts for heat demand at local level, or for the load of EV charging stations. In general, statistical and artificial intelligence/data mining techniques are applied. Regarding load demand at customer level there is discussion about the exploitation of information that can be made available from specific usages (i.e. through connected IoT devices), big data that could be informative on the presence of the customers etc. Although the research problem is interesting, there is always a compromise to find between cost of a forecasting method (in terms of data, modelling chain, privacy constraints etc) and the value it brings. A recommendation would be to assess systematically the value if predictability for each specific application through a comparison of using a “perfect” forecast versus naïve forecasts methods like persistence (i.e. load curve of the previous day). The margin between the two defines the value of an advanced method and the investment in terms of research and data that is worth to make.

Due to the increasing introduction of renewables, mainly wind and photovoltaics, it is necessary to use forecasts for their production for different power system management functions (i.e. reserves estimation, congestion management, scheduling, energy trading, ancillary services provision etc). Research in wind power forecasting was initiated in the mid 80’s. Exhaustive reviews (i.e. more than 200 references) of the state of the art in wind power forecasting are available (Kariniotakis, June 2017). Today there are several operational tools based on different physical or statistical/AI methods. Research focuses on probabilistic forecasting (in different forms i.e. quantiles, pdfs, scenarios, ensembles), on prediction of extremes (i.e. ramps, cut offs), alarming methods for large forecast errors, risk indices etc. These later tools consist of additional products that provide complementary forecasting information. In the last years there are promising developments through the spatio-temporal approach, where the aim is to use off-site information to improve predictability (i.e. up to 20%) at the level of a wind farm for the next hours (i.e. up to 6 hours). Other directions concern methods to integrate information using new measuring technologies like Lidars (LIght Detection And Ranging of Laser Imaging Detection And Ranging). These Lidars imply models able to treat large amounts of data (though not “big data”).

Forecasting the power output of solar installations is another very active area of research in the last 15 years (Pedro, , Inman, & Coimbra, , Woodhead Publishing/Elsevier). The proposed methods, either physical or statistical, try to exploit information in various sources of data coming from the solar plants, spatially distributed measurements, satellite images or sky images. Focus is given on probabilistic approaches. The consideration of multiple data as input also requires models able to treat large amounts of data without overfitting issues. A recommendation for the future would be to work towards that direction. Still the largest error, both for wind and solar forecasting, comes from the Numerical Weather Predictions. Improving the performance of the weather models is a great research challenge. In general, improving predictability of renewable generation is far from trivial. Experience has shown through previous EU projects like Anemos, Anemos.plus or SafeWind that multidisciplinary research is needed and especially synergies between research in meteorology and research in classical energy forecasting.

With the emergence of virtual power plants and aggregators that participate in electricity markets there is increasing interest for combined forecasts of wind, solar and eventually hydro (run-of-the-river) production. This is because for applications like trading or ancillary services provision it is necessary to use probabilistic forecasts and it is a complex issue to combine individual probabilistic forecasts for each type of generation. As mentioned above, this application raises the interest in methods able to deal with large amounts of input data.

A forecasting application with increasing interest especially in transmission networks is dynamic line rating forecasting (Michiorri , 2015). This permits the adjustment of the ampacity rating of a line in a dynamic way as a function of weather conditions. The DLR technology enables a better use of the transmission lines and a better integration of renewable generation through avoidance of congestions. The state of the art is not as rich as for RES forecasting. The main focus is on probabilistic approaches with focus on low quantiles (i.e. <10%) that are applied in practice to avoid risky situations. DLR forecasts used should be extremely reliable. A research challenge is thus to provide good probabilistic forecasts for the lower tail of the distribution. A similar challenge is valid for the case of RES forecasts when they are used for ancillary services provision.

Finally, forecasts of market quantities are needed for several applications like trading of renewable generation in markets, provision of ancillary services etc. More precisely, these applications may use forecasts for day-ahead prices, imbalance costs, prices of aFRR energy or aFRR activation probabilities etc. Several of these quantities are highly volatile and challenging to predict.

Several publications have shown the implications of predictability in different applications. For example, the level of predictability is determinant for sizing storage devices when coupled with renewables. Improving predictability of demand and generation may result in requesting lower levels of expensive flexibilities to hedge for the uncertainties. The increasing availability of data is an opportunity for increasing predictability given that appropriate methods are applied to avoid overfitting and the curse of dimensionality. Quality of data is an important factor for the quality of the forecasts. Finally, making available to public data may help to engage a broader research community to deal with the challenging research problems.

Open Questions

As referred above, AI is emerging as a remedy to deal with the increasingly high complexity of the energy systems. The increase of computational processing power, especially the development of cloud computing infrastructure, the frontiers are opening for the deployment of advanced data analytics models. However, the practical implementation of these models still requires a massive development to consider the various real-life scenarios that are expected (and unexpected) to occur. In fact, when the grid balance begins to be more dependent on autonomous self-learning algorithms, if an event stresses the grid (e.g. a peak consumption due to an event that was not included in the training of the model), human response may not be quick enough to minimize the negative impacts.

With increased volume of data, concerns regarding data privacy and data protection arise. Modern society is increasingly more dependent on energy to run this digitalized world. Therefore, a hacker attack to the grid is a hugely important liability and so the energy value-chain needs to be secured, which requires a substantial investment in the infrastructure.

The readiness of end users in accepting a smart energy management system that suggests/controls her/his consumptions is still an open question. Although several pilots have been developed that suggest a relatively good acceptance of end users, a successful wide implementation of demand response programs is still to be demonstrated.

1.7 STANDARDS IN SUPPORT OF DIGITALIZATION

Standard related to grid digitalization covers a variety of fields. The previous chapter reported comprehensively on the Communication aspects. In relationship to Smart Grid, IEC provided a complete and interactive overview through a web interface[9]. Nevertheless, this review covers only the activities within IEC. Some of the most relevant IEC standards for Smart Grid are here mentioned:

- CIM standards: 61970 for energy management systems, 61968 for distribution management systems and an interface reference model, 62325 for deregulated energy market communications…,
- 61850 for automating electrical systems,
- 61131 for programmable logic controllers,
- 62898 for microgrids,
- 62351 for security,

[9] See for reference http://smartgridstandardsmap.com/

All these standards enable harmonization between different domains (e.g. OT[10], IT[11], Data Analytics) by means of semantic correspondences. They also contribute to interoperability and interchangeability of solutions, which is very important for utility companies.

IEC recommends other standards gathered in standard maps[12] which help draw big pictures of overall systems (either already existing or to be developed) made with logical systems (e.g. monitoring systems, metering devices…).

On the other hand, many other sources of standard will or may affect the digitalization of the energy sector.

At the European level the process has been mostly driven by the work started as consequence of the M/490.

One example is given by the management of the Smart Meter Data. In this respect an important work has been done by an ad-hoc group under the Expert Group 1 (EG1, 'Standards and Interoperability for Smart Grids Deployment') of the European Smart Grids Task Force[13].

Other elements of standardization are appearing in relation to the growing role of e-mobility as well as from all the other elements of sector coupling.

All in all, the main concern in the future is mostly given by the risk of the so-called data silos. The growing number of actors and sectors involved may create issues of data compatibility and data interoperability. Such issues are already appearing in the area of Smart City where ETSI is working at the standardization of the so called CIM Context Information Management[14]. This CIM should not be confused with the Common Information Model from IEC.

Still in the area of data interoperability, of key importance is the work performed by the European Commission Connecting European Facility Expert Group[15]. The work of this group is introducing important standards for data interoperability such as the Context Broker from FIWARE foundation.

1.8 ENABLING DIGITALIZATION – TRENDS

This section deals with a future outlook to digitalization as enabler of the energy business. In this outlook we will describe trends which already can be seen nowadays but will last for many years not to say the coming decades. Here energy businesses will evolve along a number of maturity levels, in particular from a no organized level up to commodity market and ending in a fully decentralized energy market. First, we describe two main overall trends “Adaptive & Holistic Development” and “User Cantered Experience” which in fact hold for every industry branch. Here to be specific we also will indicate the direct application to the energy domain. Secondly, we describe the trend in disruptive digital innovation by mentioning a number of disruptive digital technologies. These technologies are characterized by the fact that by applying them to the energy domain it will lead to new services, business models and markets, potentially disrupting existing business and establishing new actors. See Error! Reference source not found. below where these trends are plotted on the layered Energy System.

[10] Operational Technology
[11] Information Technology
[12] http://smartgridstandardsmap.com/
[13] See for reference https://ec.europa.eu/energy/sites/ener/files/documents/report_final_eg1_my_energy_data_15_november_2016.pdf
[14] Se for reference http://www.etsi.org/news-events/news/1152-2017-01-news-etsi-launches-new-group-on-context-information-management-for-smart-city-interoperability
[15] See for reference https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=52603811

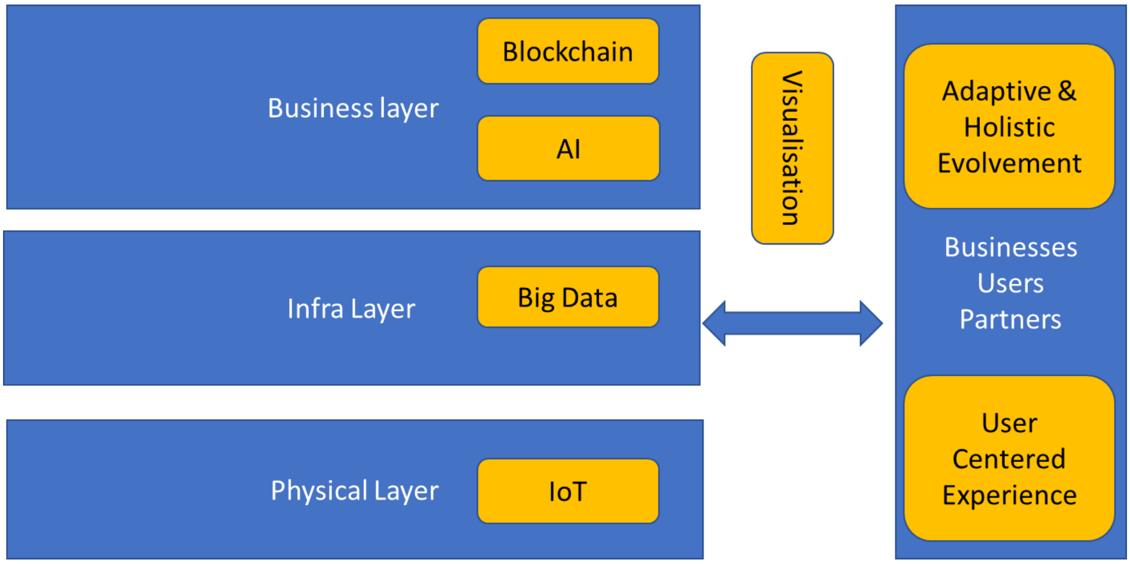


Figure 16: Main Digitalization Trends and Disruptive Technologies of the Energy System

1.8.1 ADAPTIVE & HOLISTIC EVOLVEMENT

Businesses will be constantly touched by digitalization. Some will change drastically, others may be lightly adjusted. For all, and thus specifically for the energy branch, change will be a constant. Therefore, in order to stay viable, the energy business must be able to adapt new digital technologies. Moreover, since digital innovations come rapidly, launching quick proto types to trigger interactive innovation, businesses evolve quickly and have to adapt accordingly. Hence digitalized energy businesses will go through a cycle of complexity followed by simplicity, and so on, thus coming to a higher maturity level.

Digitalization is not only addressing technology within businesses but also relates to soft factors like the culture of a company. In particular this is felt when companies work together and are part of a service chain delivering services to customers. A new digital way of giving input may affect the way another company deals with the further processing. Therefore, digitalization leads to a holistic, integrated adaption of new technology into businesses.

1.8.2 USER CENTERED EXPERIENCE

Digitalization has a great impact on the user experience. Anytime and anywhere customers, and so users, interact with businesses. The services they are subscribed to are delivered by digital business processes. Consumption of services occurs interactively by means of providing input on screens of input devices like phones, tablets. Sensors are picking up data in users living environments. The interaction is two-sided since processed information also comes to users in a digital way by the same screens. Hence digital business transformations hit the user experience most directly. This implies that digitalization can break customer loyalty when preferably could make customers involved. Therefore, a successful implementation of digitalization requires a strong user-centric focus, with a sound market model which underpins customer engagement. The emphasis on social media through mobile apps and data analytics can greatly help in pinpointing crucial factors and barriers in specific user experience (Moreno-Munoz, Bellido-Outeirino, & Siano, 2016).

1.8.3 FUTURE ROLE OF AGGREGATION PLATFORMS

Flexibility aggregation platforms started developing some 10 years ago by technology providers like cyberGRID, Siemens, ABB, Schneider Electric, GE and independent aggregators like EnerNOC (now owned by Enel), Voltalis, KiwiPower, Entelios, EnergyPool, ReStore (now owned by Centrica), etc. Today, necessary functionalities are developed and mature. However, many features and functionalities are still missing, some being already under development, others still in the research pipeline:

- Native Cloud solutions.
- Residential up-scaling.
- Interoperability on flexibility unit and market level (IoT).
- Artificial Intelligence aggregation and optimization tools.
- Artificial Intelligence consumption, generation and flexibility forecasting tools.
- Blockchain based measurement and verification.
- Blockchain based biding and service delivery.
- Security and reliability improvements.
- Cooperative ownership model.
- Etc.

The definition of suitable algorithms for baseline calculation are crucial for participation of flexibilities in electricity markets. Currently there is no common procedure in Europe for baseline calculation which could meet all the requirements related to different characteristics of various resources of flexibilities. Therefore, it is important for TSO/DSO not to insist on too strict rules but rather to allow different verification approaches as long as the fundamental requirements are fulfilled. The baseline methodologies, which are proven practice in some control zones, are:

- (corrected) power market schedule,
- baseline submitted with short lead time (min. equal to full activation time),
- continuation of the current measurements, and
- available active power (of renewable generators) based on short-term forecasts.

Further methods may also be applicable but are not approved by sufficient practical experience yet. In case that the real-time calculation of provided flexibility requires a short-term baseline correction it is preferable that the provider performs the correction, which of course requires transparent rules to support ex-port verification by the TSO/DSO. Some TSOs/DSOs accept new proposals for verification methods developed by the providers of flexibility as long as reliability and transparency fulfil the requirements for flexibility provision. This approach proved to be good practice to facilitate the participation of RES and VPPs in balancing markets. Alternatively, the provider could choose a baseline method from a catalogue of methods already verified by the TSO/DSO.

Flexibility resources (e.g. batteries, RES, smart appliances, etc.) should be able to serve with its flexibility all five power circles: local, community, DSO, TSO and cross-border. Its deployment should be seamless like installing new printer – plug into power socket, login to wireless network and start offering flexibility services to any electricity market player (regulated and non-regulated) or Energy market. True Plug and Play Internet of Things (IoT) device.

Standards allow best possible service for consumers by enabling innovation and diversity. Existing standards should be used as much as possible and extended where needed to enable a standardisation of bi-directional data exchange on flexibility resource and system level (management, aggregation, trading). Interoperability between devices and systems is crucial. Data security is vital for system stability and reliability and should have high priority all the time.

1.8.4 DISRUPTIVE ENABLING TECHNOLOGIES

Digitalization brings ICT to the business. We find some major disruptive technologies:

1.8.4.1 BIG DATA AND ANALYTICS

Data is the main driver in digitalization of businesses. Data may be gathered from the surroundings of users (context) and user usage of services. When appropriately analysed and interpreted, business can use it to plan, design and operate adequate (new) services and position these in the market. It is foreseen that the amount of data gathered will be growing and more power is available for analytics.

1.8.4.2 INTERNET OF THINGS (IOT)

The availability of myriads of “Things” on the Internet will generate gigantic sources of big data. With strong analytics it will be inevitable that IoT will not only transform businesses but will also give rise to disruptive business models by offering valuable insights to wishes and needs of businesses, customers and all involved actors.

1.8.4.3 ARTIFICIAL INTELLIGENCE (AI)

AI brings in intelligence, that is smartness to applications and systems. AI thus can be found in smart algorithms, smart devices and smart decision systems. It replaces manual decisions, brings in advanced learning machines and will work closely together with employees, users and business partners. The adaption of AI will give us smart self-learning processes and systems. In decades it is expected to have a smart energy world with an abundance of robotized entities, carrying out a complex series of actions automatically. The introduction of AI has to go together with Accountability, Reliability and Transparency (ART).

1.8.4.4 VISUALIZATION

Digitalization brings many new innovative techniques for creating images, diagrams, or animations to interact with users. In particular this holds for computer graphics. Technologies such as virtual reality (VR) and augmented reality (AR) will find its way to the development of new business models and business strategy. Also, this will lead the way to embed gaming into the workplace sustaining business decisions.

1.8.4.5 BLOCKCHAIN

In recent years Blockchain technology has gained much attention. This technology ensures that transactions between different business parties take place in an efficient, verifiable and permanent way. Since any service delivery has to be accompanied by the registration of usage records, Blockchain is an appropriate candidate for administration of business transactions. It is expected that Blockchain technology will replace at many places the current administration which is lacking a solid base for registration.

A Blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block a timestamp and transaction data. By design, a Blockchain is inherently resistant to modification of the data. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. A Blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.
While transactions are stored immutably on the internet, Blockchain protects the identity of actors and their transactions and it makes transactions transparent and auditable. This provides trust between parties that do not necessarily know or trust each other. Trust is designed to be provided by the network and the design of the technology.
Blockchain is seen as an emerging technology with many interesting applications. The following advantages of blockchain are reported:

1. **Disintermediation & trustless exchange.** Two parties are able to make an exchange without the oversight or intermediation of a third party, strongly reducing or even eliminating counterparty risk.
2. **Empowered users.** Users are in control of all their information and transactions.
3. **High quality data.** Blockchain data is complete, consistent, timely, accurate, and widely available.
4. **Durability, reliability, and longevity.** Due to the decentralized networks, Blockchain does not have a central point of failure and is better able to withstand malicious attacks.
5. **Process integrity.** Users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party.
6. **Transparency and immutability.** Changes to public Blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
7. **Ecosystem simplification.** With all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.
8. **Faster transactions.** Interbank transactions can potentially take days for clearing and final settlement, especially outside of working hours. Blockchain transactions can reduce transaction times to minutes and are processed 24/7.
9. **Lower transaction costs.** By eliminating third party intermediaries and overhead costs for exchanging assets, Blockchains have the potential to greatly reduce transaction fees.

Since Blockchain is a developing technology, not all issues are solved to date. The following challenges are reported:

1. **Nascent technology.** Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making Blockchain widely applicable.
2. **Uncertain regulatory status.** Because modern currencies have always been created and regulated by national governments, Blockchain and Bitcoin face a hurdle in widespread adoption by pre-existing financial institutions if its government regulation status remains unsettled.
3. **Large energy consumption.** The Bitcoin blockchain network’s miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, using substantial amounts of computer power.
4. **Control, security, and privacy.** While solutions exist, including private or permissioned blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a Blockchain solution.
5. **Integration concerns.** Blockchain applications offer solutions that require significant changes to, or complete replacement of, existing systems. To make the switch, companies must strategize the transition.
6. **Cultural adoption.** Blockchain represents a complete shift to a decentralized network which requires the buy-in of its users and operators.
7. **Cost.** Blockchain offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

1.8.4.6 BLOCKCHAIN: DISRUPTIVE TECHNOLOGY OR HYPE?

Different sources (McKinsey, Harvard Business review, Forrester) report that Blockchain is a disruptive technology. The essence of a disruptive technology is that it makes incumbents obsolete, has a certain growth curve and forces society in a new and unparalleled direction. Effects of this disruption can, almost by definition, not been foreseen or described.

Disruptive technology has an incubation period of a number of years before general acceptance is achieved. This includes adaptation of the educational system, production and maintenance and general acceptance. Societies that adopt such changes or adept to such changes survive in some other form, where societies that resist this become obsolete and disappear. The question with disruptive technology is what the effect of the disruption will be on which time scale.

Given the fact that large investments are made in the Blockchain technology, the subject is 'hot', in some cases even 'hyped'. As of today, the lack of a killer application is a reason to be skeptical.

Blockchain in Energy

The ongoing energy transition is reforming the landscape of the sector. Generation of power is shifting from stable, centralized, but often polluting and unsustainable power sources towards clean, sustainable, but often decentralized and less constant power sources such as wind and solar energy. Microgrids are popping up in emerging markets without grid connection to provide electricity access or to function as backup for the grid. Surpluses of green energy are traded through certificates in different trading schemes. Blockchain may not be the Holy Grail that will solve all problems of this energy transition, nor is it - at this point - a mature technology. It is, however, a promising technology that might work as a catalysator of the energy transition. Therefore, it is no surprise that Blockchain related start-ups and pilot projects are emerging rapidly, leading to an active but slightly opaque landscape of Blockchain applications in the energy sector.

SolarPlaza analysed in "Comprehensive Guide to Companies involved in Blockchain & Energy" over 65 companies and pilot projects working with Blockchain and energy. Some of the key insights:

- Most of the action (over 64%) is concentrated on the European continent.
- In terms of use cases, the most common one is P2P energy trading (see Figure 17).
- The Ethereum Blockchain enjoys a significant lead over the rest of the Blockchains. Around 50% of the projects use Ethereum.
- Close to 74% of the companies were started/founded between 2016 and 2017, which reflects the early stage the technology is still in.

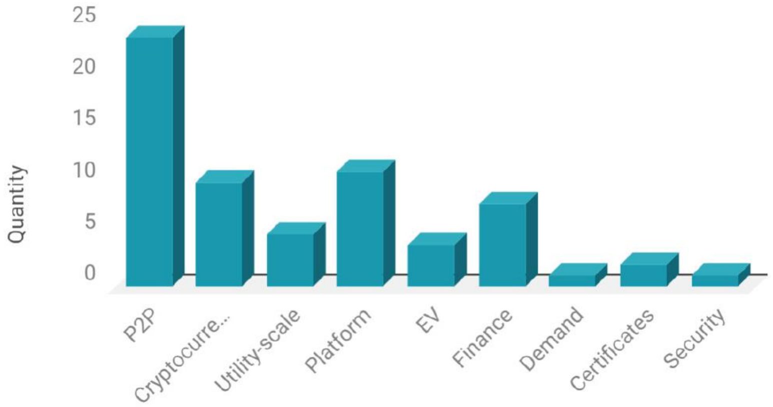


Figure 17: Total amount of use cases (source: SolarPlaza, Comprehensive Guide to Companies involved in Blockchain & Energy)

Another interesting report[16] on the crossroads of blockchain technology and energy was published and presented by the Cleantech Group (www.cleantech.com) during the second edition of EventHorizon, the largest conference on blockchain in the energy space. The study, on which the report was based upon, was carried out by analysing the data from more than 150 companies or consortia in the wider cleantech space.

The report reveals some very interesting findings regarding the investments the cleantech sector has attracted over the past year, like the tremendous increase in both investments and number of deals from 2016 to 2017. For 2018, the investments the sector attracted only in Q1 were almost equal the total amount of money raised by companies throughout 2017. But

[16] https://www.cleantech.com/blockchain-in-energy-industry-raises-1-billion-and-heads-into-challenging-times/

probably the most interesting finding is the increase in the confidence of investors in blockchain technologies, encoded by the total number of deals. While in 2017 an average of approximately $14m per deal is reported, investors increased their average deal size in Q1 2018 to $24m per deal.

Another interesting finding of the study is associated with the type of investments in blockchain companies within the cleantech sector, where a clear shift is observed from traditional funding schemes, like seed financing, series A financing, and growth equity, towards Initial Coin Offering (ICO) schemes, which represent the most modern way of financing blockchain-related companies. Also, while until 2016 the concept of ICOs was not yet emerged, ICO-related funding during 2017 represents the 41.5% of the deals. In Q1 2018 ICO-related funding is above 66.5%. However, it should be pointed out that ICO schemes may see a slow-down in the not-so-near future, mainly due to regulation-related issues.

Coming down now to the energy sector, the Cleantech Group study also reports some additional findings. Consolidating the funding amounts received within 2017 and Q1 2018, among the various energy-related use cases in the blockchain ecosystem the one leading the board is by far the peer-to-peer (P2P) and retail energy trading. Such a result comes as no surprise taking into account the current trend of the 4Ds of the “new energy revolution”: Decarbonisation, Decentralisation, Democratisation, and Digitalization.

According to the same report the EU is as of Q1 2018 the leader in the total amount of investments and number of blockchain companies, compared to the North America. This radical change is mainly favoured from the ICO schemes as the means for financing a company, raising the cross-country currency exchange barriers, as well as from the fact that EU financiers seem to be more open-minded compared to their North American colleagues when it comes down to providing financing to disruptive and fast-paced technologies, such as blockchain and distributed ledgers in general. Moreover, EU investors seem to provide financing in a more “aggressive” manner that the North American ones, with an average deal amount of $10.3m per deal compared to an average of $3.7m per deal in North America; in other words, investment is approximately 3 times more aggressive in the EU.

Another interesting finding that this study reveals has to do with the balance of funding between energy projects and projects related to food and agriculture, Internet of Things (IoT), logistics, and transportation. There is a significant shift towards energy-related blockchain projects, representing in 2018 almost the two-thirds of the money invested in total in the blockchain ecosystem.

The increasing interest of the industry (the energy industry included) is also reflected in the number of patent applications filed worldwide that have in their title the term “blockchain”. The data are as of June 2018, have been mined via the Espacenet patent search tool (https://worldwide.espacenet.com) of the European Patent Office, and are illustrated in the following chart.

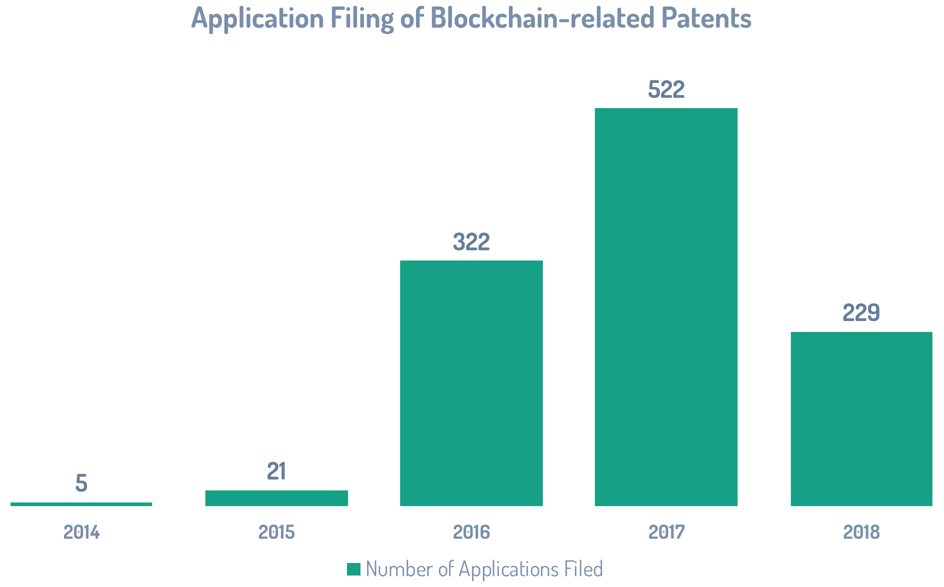


Figure 18: Number of filed patent application having the term “blockchain” in their title as of June 2018

One of the Horizon 2020 projects, FutureFlow (http://www.futureflow.eu) is addressing flexibility trading in balancing markets. In the future we can expect emergence of new electricity markets for flexibilities, especially in the DSO domain, as recent winter package suggests. This plethora of markets presents a possibility to double sell flexibility, which poses a threat to buyers and the electricity system. The use of blockchain in this case would eliminate this risk, as demonstrated in the FutureFlow pilot.

Another example of energy blockchain pilot in Horizon 2020 is CROSSBOW (http://crossbowproject.eu/) project where cooperative flexibility platform will be designed around blockchain, as underlying technology, and will enable creation of cooperative organization, management of shares, democratic governance, voting and efficient integration with flexibility systems like Demand response, Virtual Power Plant, etc.

1.9 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:

1.9.1 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 question of using AC versus DC should be discussed again the more we proceed in the process of digitalization.

1.9.2 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.

1.9.3 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, Mobility to mention the most typical. This interaction will be made possible creating open cloud solutions that support open API (Application Program Interfaces): These open API will also enhance the role of SME and start-up in providing innovative services. A reference in this sense is given by the work developed within the FI-PPP of the European Commission and the development of the 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 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.

Other important needs independently from the layer structure are:

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.

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 (TF2)

Photo Alliander (Infocaster)

2.1 EXECUTIVE SUMMARY

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. There are many benefits promised by introducing digitalization – it is expected to make key contributions to the achievement of the Energy Union objectives for the transition to a 21st century secure, affordable and climate-friendly energy.

While Task Force 1 position paper focuses on technology, Task Force 2 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
- Big data, data analytics, data mining
- 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

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.

2.2 INTRODUCTION

The energy sector is undergoing fundamental change. The utilities today are being transformed as the energy system moves towards an integrated model combining aspect of centralization with increased uptake of distributed energy resources.

The scale of uncertainty presents big challenges for energy companies, policy makers and regulators. The new energy system will be driven by falling costs, new technology, new players and climate policies and is creating a consumer-driven, digital-connected and real-time controllable energy consumption and supply.

2.3 IMPORTANT QUESTIONS TO ANSWER

Considering the main Questions of ETIP SNET

- Q1: What would be the ideal Energy System if we started everything from zero?
- Q2: What will be the day in the life of a consumer by 2050?
- Q3: What is the future of Energy infrastructure versus or in combination with Digital infrastructure?
- Q4: Where should every stakeholder innovate “Individually” and where should they innovate as a “System”?
- Q5: What’s the role of technology data science and intelligent models in the future energy system?

Some more detailed questions were raised within Taskforce 2:

- What is a customer centric model and who is the customer?
- Which technologies are available?
- Why do we need new business models?
- What is the timeframe we are looking at?
- Which is the main focus/market of those business models and how do they interact?
- Are we looking for services or products?
- In terms of electricity: congestion or energy market?
- Blockchain: Is there a business case? Who benefits? Can it deliver on the promise of disintermediation?
- Why would consumers participate in energy markets?
- Who is giving value to business models/flexibility/services/products?
- Which potential is in which customer group?
- Which stakeholder should look into what business cases?
- Level of engagement?
- Business models other than energy related? E.g.: Alarming or predictive maintenance
- How aware is which kind of customer of the energy system or the provided models?
- Who is owning the problem? Who needs to move first/ Maybe DSO/TSO
- Who has and should have the dialog with the customer and how?
- How attractive is the TSO/DSO - normally contacted only when there is a problem
- Necessary regulative changes for business models?
- Social aspects of upcoming use cases? Who should pay for what? E.g. should people who cannot afford electric cars pay for the integration of electric cars?

2.4 EXPECTED IMPACT OF ETIP SNET AND WORKING GROUP 4 TASKFORCE 2

- Enabling new Digital Use Cases and Services supporting the energy transition while maintaining the quality of services in the energy provision
- Significant economic benefits related to the digitalization of the assets, customer services and back-office processes
- Enabling a full effective SmartGrid system across the energy value chain
- A large-scale demonstrator for specific use cases should demonstrate the feasibility of disruptive real-time services
- Articulation and involvement of the customer and end user in digitalization of energy supply

2.5 ROLES AND DEFINITION

In the report published by ETP SG Digital Energy, ‘Digitalization of the energy system’ is defined as ‘The process of implementing and operating a set of assets by monitoring, transferring and analysing data which have been generated by one of the actors in the energy system’. This includes smart operation of the grid at all voltage levels to reduce losses and outage times, retailers that optimize their portfolio by balancing based on forecasting algorithms, aggregators that control flexible consumption for various business cases, and new market platforms that provide suitable interaction between all these actors to optimize the overall efficiency.

This issue deals with the concept of local flexibility markets and the stakeholders involved in such local markets. In a future system based on renewable energy generation which is mainly taking place in the distribution grid, flexibility which is locally available becomes more and more important. Flexibility can be defined as the ability of the electricity system to respond to fluctuations of supply and demand while, at the same time, maintaining system reliability. Flexibility is the modification of generation injection and/or consumption patterns in reaction to an external signal (price signal or activation) in order to provide a service within the energy system. The parameters used to characterise flexibility include the amount of power modulation, the duration, the rate of change, the response time, the location, etc. Flexibility needs to be considered as tradeable product separate from energy products. Today there are markets for flexibility for TSOs and Balance Responsible Party (BRPs) (reserve markets, capacity markets, spot markets) but not on local or regional level. Local flexibility markets are supposed to handle local constraints, which are impacting the DSO but also the TSO. Aggregators have possibly a key role in such markets. Possible users of local flexibilities could be DSOs, TSOs and BRPs, but also Microgrid Operators or Local Energy Communities. The task is very much related to Issue 5 “Market design for the use of flexibility by the Distribution System Operator (DSO)” since the DSO is regarded as the main beneficial of a local flexibility market.

Just as the concept of Smart Grid evolved and is reflected by ETIP SNET due to the increasing need to consider smart electricity networks within the wider energy system, the range of stakeholders addressed by use cases has been broadened beyond the traditional ones (distribution and transmission networks, technology vendors and ICT, research and academia) to include storage, consumers and other connected energy carriers (gas, heat, hydrogen, transport, etc.).

The digitalization of the energy system is a broader concept than Smart Grid or Smart Networks with significant social components and not only technology innovation. The final goal is to enable a flexible open market of energy with equal possibility of participation of every player as envisioned by the Winter Package. It also needs to ensure maintenance and development of the necessary infrastructure, and a system for a fair distribution of the related costs.

2.6 STATE OF THE ART

Energy trading today has been developed and regulated for a Europe-wide centralized energy system, assuming that the physical flow of energy is in line with the commercial flow of energy – see Error! Reference source not found. (left side). With a considerable increase of decentralized power generation, we now have to face the situation that the physical flow of energy sometime collides with the commercial flow of energy – see Error! Reference source not found. (right side). From a commercial point of view this leads to price risks and the risk of buying energy when prices are high. Rising technical challenges derive from the increasing demand for balancing capacity and protection mechanism to avoid grid congestions and to grant grid stability.

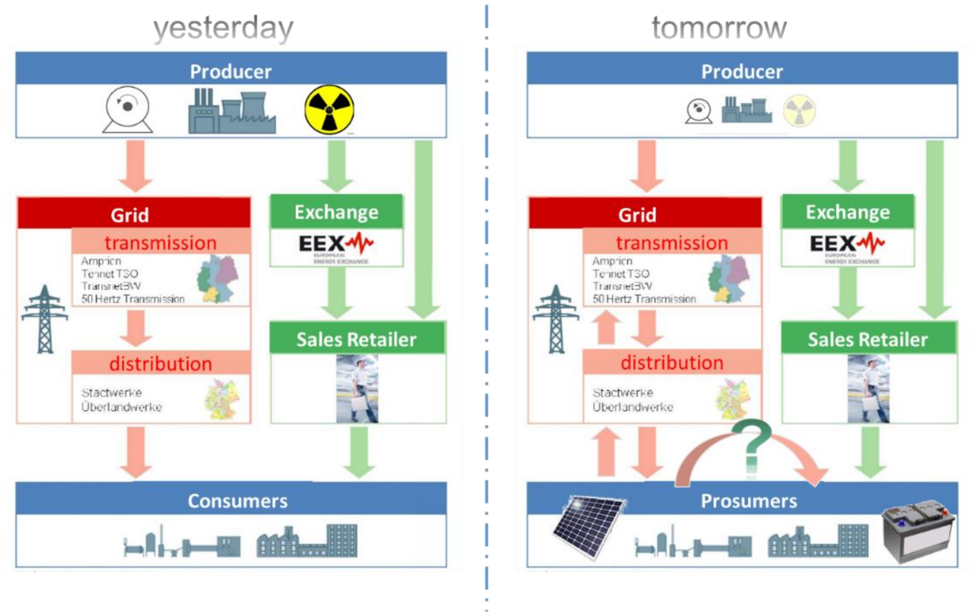


Figure 19: Physical vs. commercial flow of energy yesterday (left) and tomorrow (right) – the market has been designed for a centralized energy production, which works against physics in a decentralized world of energy production – (picture elements: Siemens)

Today the Transmission System Operator ("TSO") is responsible for grid stability and is remunerated by transmission network charges, which have increased drastically to justify high investment for grid expansions, phase shifter technology or costs for balancing capacity. In case of emergency the TSO is allowed to request load shedding from the Distribution System Operator ("DSO"), for which the later would not be remunerated.

The tariff system for end users is very rigid and does not provide any benefit for flexibility in energy consumption or production, though this flexibility could help to improve balancing capacity to stabilize the grid and to avoid grid congestions. In contrary customers may suffer from penalties for failing to balance supply and demand.

Increasing self-consumption of energy, which will become most interesting to those who can afford the invention of Renewable Energy ("RE") production and storage technology, makes current business models void, allocates fixed energy charges to fewer people and increases the risks from fluctuating loads.

The deployment of Smart Grid infrastructures motivated a discussion about the current and future roles of the energy stakeholders, with particular attention on customer engagement. Most of these discuss the advantages and disadvantages of the different data models rather than proposing a conceptual and functional architecture for one model. The main innovation and contribution from the recent Horizon 2020 projects is to propose a conceptual and functional architecture that adopts the recommendations and models from the state of the art. New solutions go beyond a neutral access market platform (such as the one designed in

H2020 Flexiciency project), and encompass the exchange of information, including consumption profiles from the DSO and flexibility profiles from the Home Energy Management System (HEMS). This design situates the new digital platforms as a more flexible mediator but raises natural performance and security concerns: it should be capable of handling requests from the multiple stakeholders but facilitate private client information only to rightful stakeholders.

2.7 USE CASES – MAIN OUTCOME

As mentioned in Task Force 1 position paper, digitalization is affecting the energy system at three different levels. For each of these levels there are peculiarities that bring different technologies to play a key role. These three layers were defined this way:

- Infrastructure Layer
- Physical Layer
- Business Layer

In this report, we present several of these use cases illustrated by practical examples in the field. In every use case, a digital aspect is present that facilitates transition to a new way of energy system operation, either at the physical, infrastructure or business layer. In particular, for each use case it was emphasized what digitization contributed and what the benefits or business case was for the technologies introduced.

As mentioned beforehand, 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 at the innovation stage, which is in line with the ETIP SNET ambition to discuss the future technologies and applications.

Table 18 presents an overview of use cases presented in this position paper:

Title	Layer	Stakeholders	Markets and Regulatory Framework
Increasing self-consumption with digitalization.	Business layer mainly, layer for the data monitoring	DSO, TSO, PV prosumers, public authorities, PV manufacturers, Blockchain engineering specialists	PV self consumption market, Distributed / collective self consumption in France (with ENEDIS)
Deliver Flexibility to the Market. Avoiding expensive grid upgrades Limiting penalties for failing Infrastructure and reduce downtime	Infrastructure	TSO, DSO, utility	Germany: EnWG, EEG, StromNEV, BSI
Cross sector optimisation - Demand response service level Sector coupling: Ebay for Energy: ENsquare	Infrastructure	DSO, gas SO, PV prosumers, public authorities, PV manufacturers, Blockchain engineering specialists	Netherlands – market framework
Energy Community - customer engagement	Infrastructure and business layer	DSO, DER generators and	Ancillary services market.

Title	Layer	Stakeholders	Markets and Regulatory Framework
		storage, aggregators	Regulatory framework is being prepared
Democracy by design			Framework for design
Monitoring, visualisation, and analytics for every stakeholder group	Infrastructure and business layer	Manufacturers, Power producers, TSO, DSO, Retailers & Aggregators, energy consumers & prosumers	Complete value chain
Delivering flexibility to the market Transparent flexibility market with LV monitoring	physical and business layer	DSO, aggregators, regulators	Ancillary services market. Regulatory framework is not defined yet. Winter Package (November 2016) assigns the frequency control to TSO, while the DSO is allowed to open local markets to congestion management.
Use Cases between DSO and TSO	Infrastructure and business layer	DSO, TSO, DER generators and loads, aggregators, regulators	Ancillary services market
Preventive Maintenance	Physical and infrastructure layer	DSO	Not oriented to a defined market. Regulatory framework applicable to DSO quality service
Digital Twin	Business layer	TSO, DSO, regulators, end users	Regulatory framework applicable to DSO, i.e.. KPIs on OPEX reduction
Enable electric vehicles smart charging and roaming	Physical and infrastructure layer	Charge manager, TSO, DSO, regulators, end users	Electric Vehicle demand supply and operation
Consumer empowerment, customer relationship and behavioural change			Framework for design

Table 18: Overview of use cases presented in this position paper

2.8 INFRASTRUCTURE LAYER

2.8.1 MONITORING, VISUALISATION, AND ANALYTICS FOR EVERY STAKEHOLDER GROUP

Throughout the whole overall energy value chain, from equipment’s manufacturer to the final energy client, advanced data analytics, monitoring and visualization tools are a key component to address the complex challenges like increased penetration of Distributed Energy Resources (DER) and a two-way flow of energy from Prosumers that create an increasing demand for balancing capacity and the capacity to guarantee grid stability.

Figure 20 presents a non-exhaustive list that seeks to identify areas, throughout the energy value chain, in which advanced data analytics, monitoring and visualization tools can effectively bring added value to the market agents.

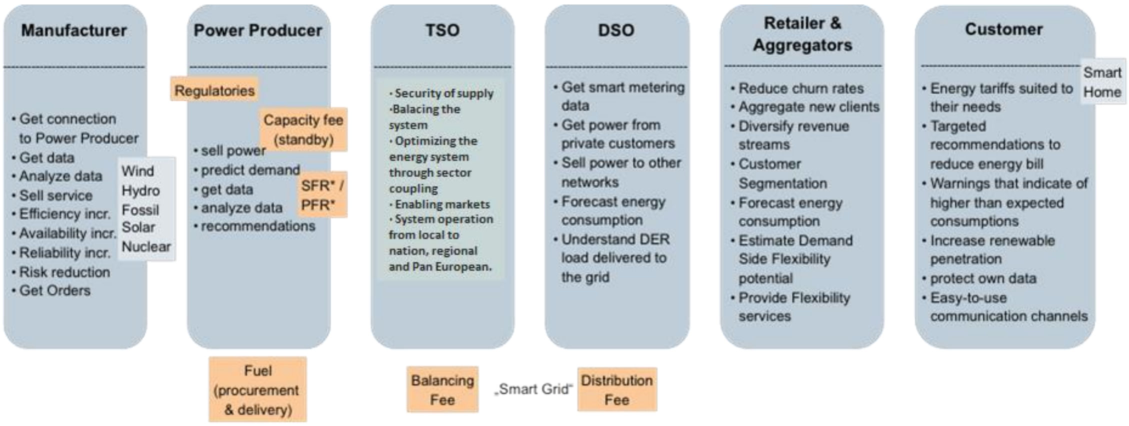

Manufacturer
• Get connection to Power Producer
• Get data
• Analyze data
• Sell service
• Efficiency incr.
• Availability incr.
• Reliability incr.
• Risk reduction
• Get Orders
Wind
Hydro
Fossil
Solar
Nuclear
Power Producer
Regulatories
Capacity fee (standby)
• sell power
• predict demand
• get data
• analyze data
• recommendations
SFR* / PFR*
Fuel (procurement & delivery)
TSO
• Security of supply
•Balacing the system
• Optimizing the energy system through sector coupling
• Enabling markets
• System operation from local to nation, regional and Pan European.
Balancing Fee
„Smart Grid“
DSO
• Get smart metering data
• Get power from private customers
• Sell power to other networks
• Forecast energy consumption
• Understand DER load delivered to the grid
Distribution Fee
Retailer & Aggregators
• Reduce churn rates
• Aggregate new clients
• Diversify revenue streams
• Customer Segmentation
• Forecast energy consumption
• Estimate Demand Side Flexibility potential
• Provide Flexibility services
Customer
• Energy tariffs suited to their needs
• Targeted recommendations to reduce energy bill
• Warnings that indicate of higher than expected consumptions
• Increase renewable penetration
• protect own data
• Easy-to-use communication channels
Smart Home

Figure 20: Potential areas profiting of monitoring, visualisation, and analytics in the energy value chain

Requirements for Monitoring, Visualisation and Analytics (Manufacturer – Power Producer)

Figure 21 summarizes the requirements for monitoring, visualization and analytics for the connection between Manufacturer and Power Producer. In this case the Manufacturer can be seen as the "Supplier" and the Power Producer as the "Customer".

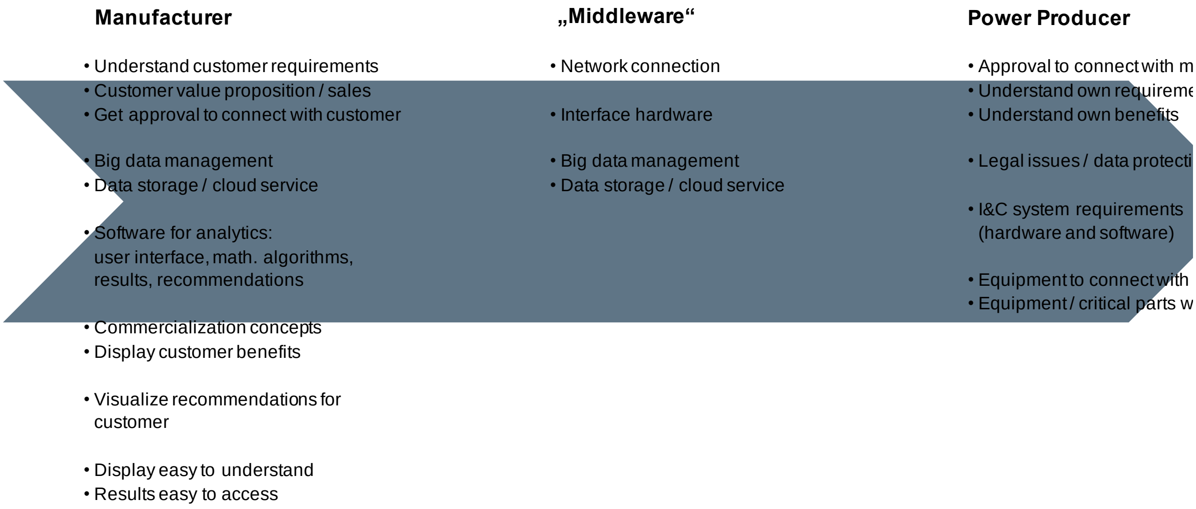

Manufacturer
• Understand customer requirements
• Customer value proposition / sales
• Get approval to connect with customer
• Big data management
• Data storage / cloud service
• Software for analytics: user interface, math. algorithms, results, recommendations
• Commercialization concepts
• Display customer benefits
• Visualize recommendations for customer
• Display easy to understand
• Results easy to access
„Middleware“
• Network connection
• Interface hardware
• Big data management
• Data storage / cloud service
Power Producer
• Approval to connect with m
• Understand own requireme
• Understand own benefits
• Legal issues / data protecti
• I&C system requirements (hardware and software)
• Equipment to connect with
• Equipment / critical parts w

Figure 21: Requirements for Monitoring, Visualisation and Analytics

For the Manufacturer It is important to understand customer requirements and present benefits to the customer by conducting a customer value proposition. It is essential to get connected to customer's assets and to be able to handle the amount of data that is required for respective data analytics. Software for analytics, user interface, mathematical algorithms, display of results and recommendations should to be developed. Commercialization concepts to be developed from supplier and customer view. User interface and display of analytics and recommendations should be accessible through multiple devices and easy to understand. The following value-added can thus be created through the application of Monitoring, Visualisation and Analytics tools:

- Understand customer requirements
- Customer value proposition
- Get approval to connect with customer
- Big data management
- Data storage / cloud service
- Software for analytics: user interface, math. algorithms, results, recommendations
- Commercialization concepts
- Display customer benefits
- Visualize recommendations for customer
- Display easy to understand
- Results easy to access

A layer between supplier and customer might be required (the Middlelayer), that includes e.g. network connection, interface hardware, big data handling, data storage and cloud service activities. Within this layer the following requirements apply:

- Network connection
- Interface hardware
- Big data management
- Data storage / cloud service

The customer, in this case the Power producer, needs to allow connection to its assets. Furthermore, it is important to understand customers' own requirements and benefits. Close cooperation between supplier and customer helps to specify these. Legal issues, e.g. data protection requirements need to be considered as well. Technically, customer's hardware and software needs to meet certain requirements to get connected and the equipment that needs to be monitored and evaluated requires possibly additional hardware such as sensors. For the Power producer business model, the following requirements apply in which the application of Monitoring, Visualisation and Analytics tools may add value:

- Approval to connect with manufacturer
- Understand own requirements
- Understand own benefits
- Legal issues / data protection
- I&C system requirements (hardware and software)
- Equipment to connect with
- Equipment / critical parts with sensors

How Does Digitalization Help?

Achieves a better understanding of the household client energy consumption dynamics through data analytics

As it is already being witnessed by several ongoing projects, digitalization creates a big opportunity to further engage with the energy client, with utilities seeking to provide digitally a set of services that streamline and make more transparent their relationship with energy consumers. Looking at the value that may be generated through digitalization, it is also recognized[17] that digitally engaged consumers typically have higher trust and satisfaction

[17] Accenture, The New Energy Consumer: Unleashing Business Value in a Digital World, 2015

levels with their energy provider when compared to consumers that do not use digital channels and they are also more inclined to acquire new services or adopt recommendations targeted to energy efficiency, thus leading the way to revenue diversification for utilities.

Consumer Engagement example

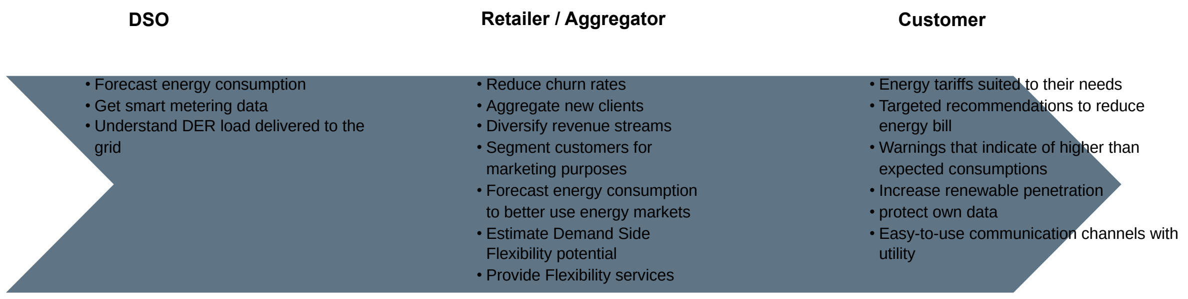
In parallel, common use cases related with the provision of information from smart meters to final energy clients are focused on merely making available load profile data to energy clients or price signals to be incorporated into Consumer Energy Management (CEM) devices. Nonetheless, from the experience that has been gained with several smart metering pilot projects, it is safe to argue that the average consumer does not have the needed energy knowledge to properly understand what measures he needs to take in order to correct inefficiencies and reduce his energy bill just from looking at a simple load profile.

A new layer of information is therefore needed that, feeding on common smart metering data (without the need of replicating investments on higher resolution meters or smart plugs) may provide meaningful information regarding the energy consumption dynamics of final energy clients and may generate value to both energy clients and the remaining actors in the energy value chain.

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 thus of utmost importance. One example of the application of such data analytics tools is a method entitled Non-Intrusive Load Monitoring (NILM) which from the aggregate energy consumption data obtained from smart meters, can identify the existence and the energy consumption allocated to the main residential appliances or energy services. This approach may incorporate various hybrid methodologies including pattern recognition, clustering, time series, multivariate modelling, machine learning among others, relying only on data from the most common smart meters, coupling it, when necessary, with other exogenous streams of data.

From this new layer of information and coupling it with additional data analytics modules such as automated PV dimensioning, tariff optimization capabilities, appliance substitution evaluation or demand response potential estimation, it is possible to automatically provide the final energy consumer with a new set of services that seek to help him have a more energy efficient behaviour and that may be embedded in already existing consumer engagement platforms, leveraging on the data being provided by existing smart meters. Given the new level of services made possible from this data analytics capabilities, the energy consumer will also become more engaged with the energy supplier which in turn generates a value added for the energy supplier itself, due to the reduction of churn rates.

Apart from the benefits generated for the energy consumer, digitalization provides an overall overview of how the application of specific data analytic modules such as Load disaggregation, Load Forecasting or the identification of DR potential, leveraging on smart metering data can add value throughout several stakeholders of the energy value chain.



DSO

- Forecast energy consumption
- Get smart metering data
- Understand DER load delivered to the grid

Retailer / Aggregator

- Reduce churn rates
- Aggregate new clients
- Diversify revenue streams
- Segment customers for marketing purposes
- Forecast energy consumption to better use energy markets
- Estimate Demand Side Flexibility potential
- Provide Flexibility services

Customer

- Energy tariffs suited to their needs
- Targeted recommendations to reduce energy bill
- Warnings that indicate of higher than expected consumptions
- Increase renewable penetration
- protect own data
- Easy-to-use communication channels with utility

Figure 22: Value added by the application data analytic throughout the energy value chain

Benefits of Digitalization

In the 2 use cases presented it becomes clear that the application of Monitoring, visualisation, and advanced data analytics to both sides of the spectrum of the energy value chain bring added-value to the market players that adopt them.

In what regards the data analytics and consumer engagement example, the new layer of information provided by data analytics modules such as Load disaggregation, tariff optimization and targeted energy efficiency measures, enables a better understanding of the energy consumer consumption dynamics and brings value for several stakeholders in the energy value-chain as it allows:

i. energy retailers to achieve a better client segmentation and the development of new services like targeted recommendations;
ii. the estimation of demand side flexibility potential of individual clients or sets of clients, targeted to flexibility aggregators, due the identification of specific loads with load shifting potential;
iii. for DSO’s to have a more accurate estimation of existing DER load in the grid;
iv. improved demand forecasting services for retailers, aggregators, DSO’s and TSO’s due to the added knowledge of the consumption dynamics of each individual client;
v. the delivery of new services (made available through cloud-based platforms) focused on improving consumer engagement by providing the energy consumer with targeted energy efficiency measures aimed at helping him to become more energy efficient and reduce his energy bill.

2.8.2 USE CASES BETWEEN DSO AND TSO

Overview

The widespread penetration of Distributed Energy Resources (DER) is causing important changes in the energy market. The main challenge of introducing DER in a system designed for one-way flow of power, from generation to distribution, through transmission, is bringing also new opportunities. Distributed generation could be seen as an actor able to provide services to the whole power system, being managed together with demand response and storage. However, the introduction of this kind 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 (SmartNet project, 2016-2018). It is 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. Three physical pilots enable the test of exchanging monitoring and control signals between transmission and distribution networks, as well as flexibility services which can be offered by agents connected to distribution.

SmartNet (Gerard , 2016) proposes and makes a conceptual analysis from five TSO-DSO coordination schemes. These schemes present different possibilities to enable the interaction between system operators, where a specific set of roles are defined in each one, as well as a detailed market design. The procurement of the Ancillary Services (AS) or local system services is different in each one of the coordination schemes:

1. Centralized AS market model: the TSO operates a market for resources connected both at TSO and DSO level, without extensive involvement of the DSO.
2. Local AS market model: the DSO organizes a local market for resources connected at the DSO grid and, after solving local grid constraints, aggregates and offers the remaining bids to the TSO.
3. Shared balancing responsibility AS market model: balancing responsibilities are divided between TSO and DSO according to a predefined interaction schedule. The DSO organizes a local market to respect the schedule agreed with the TSO while the TSO has no access to resources connected at the distribution grid.
4. Common TSO-DSO AS market model: the TSO and the DSO share the common objective of decreasing costs for system services. There is a centralized variant, where objective is realized by the joint operation of a common market. Besides, there is a decentralized variant where the DSO operates a dynamic integration of a local market, and the TSO operates a central market.
5. Integrated flexibility market model: the market is open for the regulated market entities (TSOs, DSOs) and for non-regulated ones, such as Balance Responsible Parties (BRPs) or CMPs). This scheme requires an independent market operator to guarantee neutrality.

The specific benefits and attention points with regard to the TSO/DSO grid operation and to other involved market participants are listed in Table 19**.**

Scheme	Benefits	Attention points
Centralized AS market model	• Efficient scheme in case only the TSO is a buyer for the service • A single market is low in operational costs and supports standardized processes • Most in line with current regulatory framework	• No real involvement of DSO • DSO grid constraints not always respected
Local AS market model	• DSO has priority to use local flexibility • DSO supports actively AS procurement • Local markets might create lower entry barriers for small scaled DER	• TSO and DSO market are cleared sequentially • Local markets might be rather illiquid • Need for extensive communication between the TSO market and the local DSO markets
Shared balancing responsibility AS market model	• The TSO will need to procure a lower amount of AS • Local markets might create lower entry barriers for small scaled DER	• Total amount of AS to be procured by TSO and DSO will be higher in this scheme • Balance Responsible Parties might face higher costs for balancing

	- Clear boundaries between system operation TSO and DSO	- Small local markets might be not liquid enough to provide sufficient resources for the DSO - Defining a pre-defined schedule methodology agreed by both TSO/DSO might be challenging
Common TSO-DSO AS market model	- Total system costs of AS for the TSO and local services for the DSO are minimized - TSO and DSO collaborate closely, making optimal use of the available flexible resources	- Individual cost of TSO and DSO might be higher compared to other schemes - Allocation of costs between TSO and DSO could be difficult
Integrated flexibility market model	- Increased possibilities for BRPs to solve imbalances in their portfolio - High liquidity and competitive prices due to large number of buyers and sellers	- Independent market operator needed to operate the market platform - Negative impact on the development and liquidity of intraday markets - TSO and DSO need to share data with Independent Market Operator

Table 19: Benefits and attention points of SmartNet TSO-DSO coordination (source: [24])

Independently of the coordination scheme, the procurement of AS from the distribution grid should be clear, easy to understand, non-discriminatory, reliable, cost-efficient and fast. Although closer cooperation between TSOs and DSOs is needed, TSOs should remain responsible for the transmission grid while DSOs remain responsible for the distribution grid. This involves that DSOs will be responsible for local constraints management, and that the feasibility of coordination schemes depends on the evolution DSO roles and vice versa.

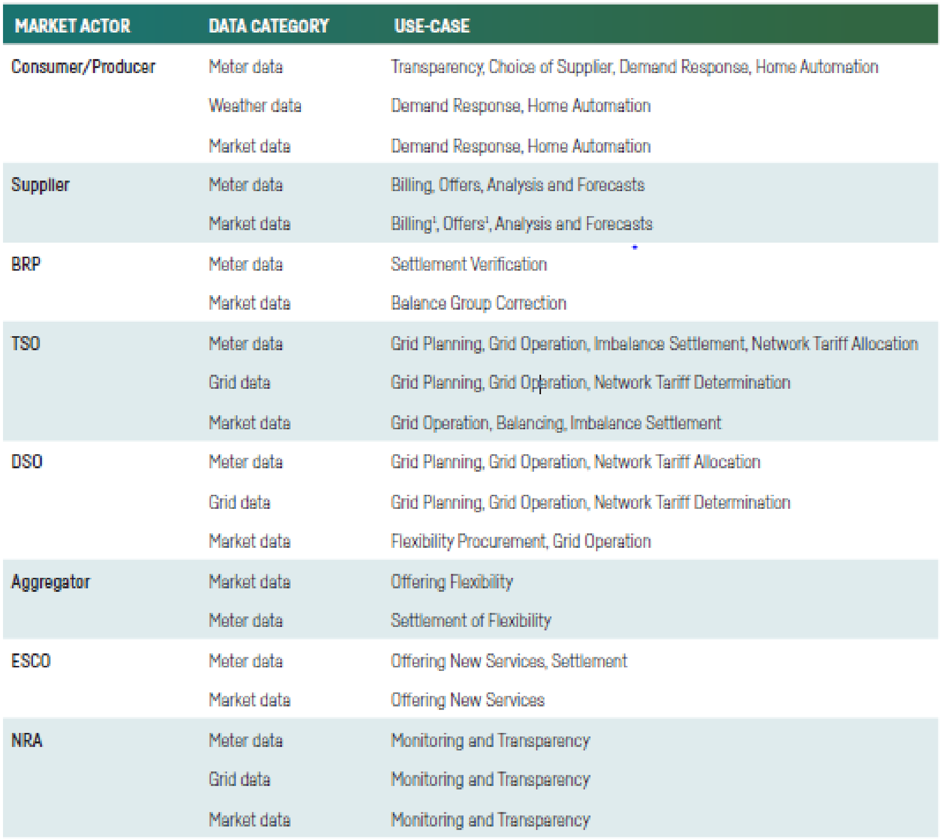
How did Digitalization Help?

Data exchange platforms are a tool for improving coordination and market functionality

In the building of an efficient integrated European electricity market, information exchange and data management are becoming more connected. Increased information access and exchange not only leads to substantial efficiency gains in grid operation and planning, but also lowers market access barriers, ensures transparency in consumers' usage and creates new market opportunities (e. g., energy services companies). Efficient data exchange is also necessary for achieving a seamless integration between wholesale and retail markets.

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 and their functionalities are subject to different regimes and practices throughout Europe. Furthermore, several recent studies and reports have covered the development of DEPs primarily from a retail market perspective. This has also been the focus of several of the DEP projects that have been implemented or planned to date, however, there are certain examples serving both retail and wholesale markets, such as in Denmark and Estonia.

The range of possible benefits from DEPs clearly goes beyond the retail market and the DSO level. DEPs that take a wider system perspective and facilitate innovation through stimulating the development of third-party applications (for example, in the Estonian DEP) can be said to constitute the state-of-the-art with regards to data exchange in the European context.



MARKET ACTOR	DATA CATEGORY	USE-CASE
Consumer/Producer	Meter data	Transparency, Choice of Supplier, Demand Response, Home Automation
	Weather data	Demand Response, Home Automation
	Market data	Demand Response, Home Automation
Supplier	Meter data	Billing, Offers, Analysis and Forecasts
	Market data	Billing[1], Offers[1], Analysis and Forecasts
BRP	Meter data	Settlement Verification
	Market data	Balance Group Correction
TSO	Meter data	Grid Planning, Grid Operation, Imbalance Settlement, Network Tariff Allocation
	Grid data	Grid Planning, Grid Operation, Network Tariff Determination
	Market data	Grid Operation, Balancing, Imbalance Settlement
DSO	Meter data	Grid Planning, Grid Operation, Network Tariff Allocation
	Grid data	Grid Planning, Grid Operation, Network Tariff Determination
	Market data	Flexibility Procurement, Grid Operation
Aggregator	Market data	Offering Flexibility
	Meter data	Settlement of Flexibility
ESCO	Meter data	Offering New Services, Settlement
	Market data	Offering New Services
NRA	Meter data	Monitoring and Transparency
	Grid data	Monitoring and Transparency
	Market data	Monitoring and Transparency

Figure 23: Data requirements per actor (source:)

Benefits of Digitalization

Current state of data exchange models

We distinguish between two different data exchange models, namely DEPs and decentralised data exchange. With DEPs, we refer to a single platform that supports information exchange between electricity market actors. This central model implies that market actors have one point of access to the information needed to carry out different tasks as outlined in the previous chapter. With a decentralised data exchange model, data are collected and distributed either directly from each individual customer to the various legitimate parties or via the DSO (or TSO in the case of customers connected directly to the transmission grid). This decentralized data exchange can be strictly standardised, bestowing an element of centralization upon the exchange protocol definition. However, the decentralised model implies in any case that all market actors communicate with each other, creating a large amount of interactions.

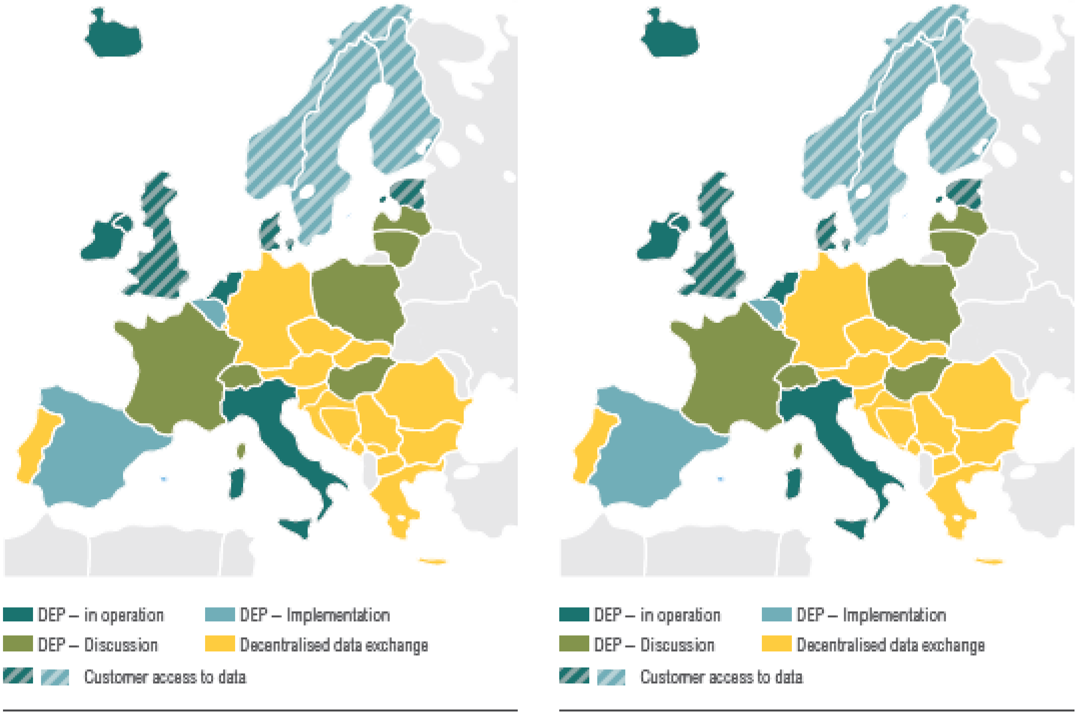
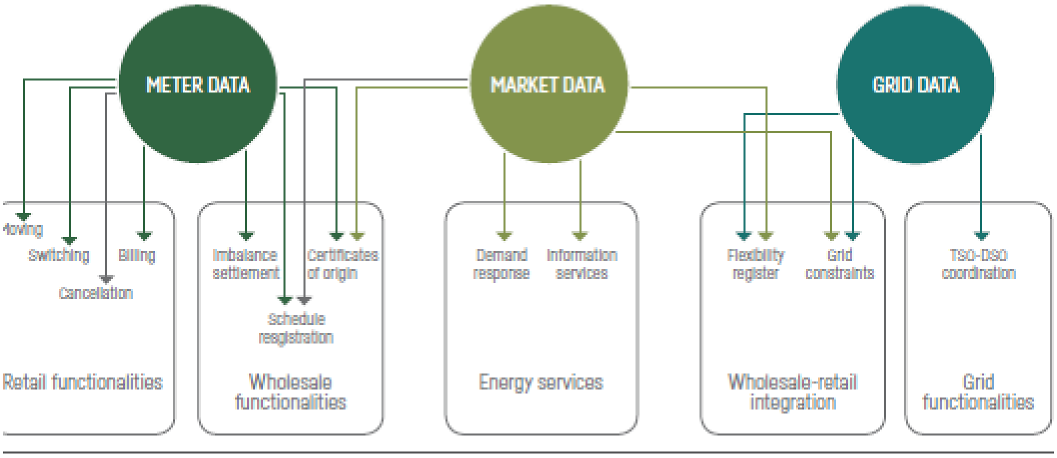


Figure 24: Current state of data exchange models

Future developments are around four dimensions in which DEPs might develop: wholesale functionalities, energy services, wholesale-retail integration and grid functionalities. These dimensions are largely independent of one another and can be added in any order (see Figure 25).



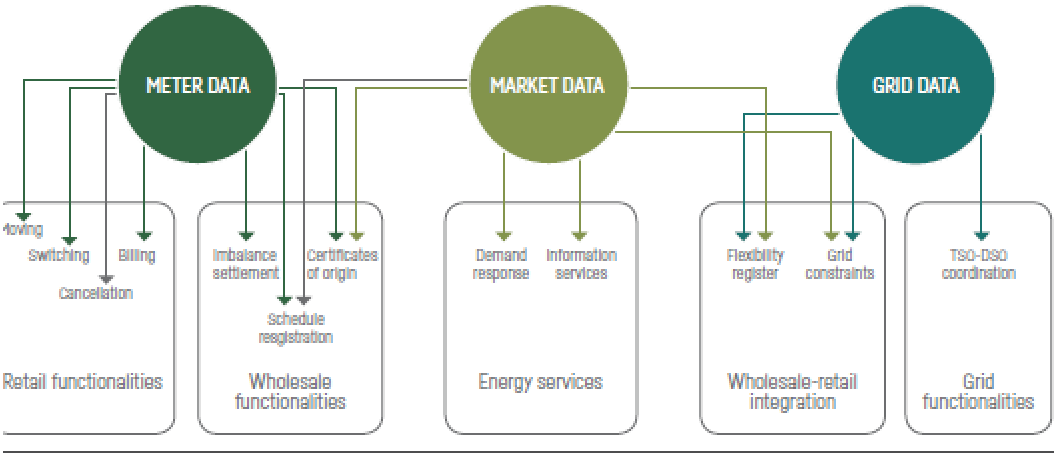
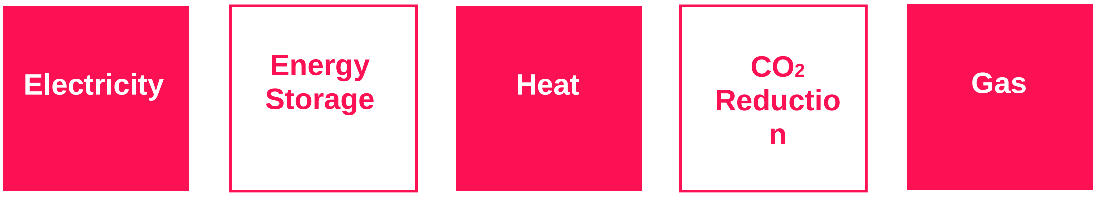


Figure 25: Four dimensions in which DEPs might develop: wholesale functionalities, energy services, wholesale-retail integration and grid fuand grid functionalities

2.8.3 EBAY FOR ENERGY - ENSQUARE: A TRANSPARENT, ACCESSIBLE MARKET FOR LABELED ENERGY

Overview

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. ENSquare can show that the agreed-upon type of energy is actually delivered, every hour of the day. ENSquare 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. This information can give support to innovative organizations in developing new products and services.



Broad, accessible energy market

- Available to all markets, large and small
- Offers business across all forms of energy, via storage and conversion services

Measuring of energy characteristics

- Measures the particular characteristics of the energy, such as origin, type, and CO2 emissions at each hour of the day
- Offers chances for new services

Transparent and continuously traceable

- The specifics of the energy are transparent and continuously traceable
- The link between the source and the customer can be checked at any moment

Figure 26: Products of Ensquare

How did Digitalization Help?

Once the transactions have been settled on the ENSquare marketplace, an (remaining) open position is expected to arise. ENSquare automatically places orders on relevant exchanges which close the open position (future, day ahead, intraday, gas and electricity). ENSquare works as a market coupling and is therefore portfolio free. A saving of 10-30% is expected to be achieved as project outcome.

Project Planning

- PoC (Proof of Concept): until mid-2018
  - A website where clients of ENSquare can log in and transact business
  - Find customers and explore what is necessary to begin trading
  - Manual processing of bid orders, using Excel

- MVP (Minimum Viable Product): mid-2018 to end of 2019
  - Approval required for budget, possibly request a subsidy (TKI or otherwise)
  - Design architecture, develop functionalities, realise minimal product
  - Basis is marketplace, also design and realisation of services for market entrepreneurs, creating market demand and creating ESPs

- PoH (Point on the Horizon): from 2020
  - Upscaling and extending services and increasing clientele (number of customers)

Benefits of Digitalization

During ENSquare phase 1 the following will be realised (among others):

- Basic version of a business model and business plan
- Basic version of the marketplace (IT application of the marketplace which enables the marketing of labelled energy and energy services)
- Demo (interactive PowerPoint with a link to the above-mentioned marketplace, so a case can be reproduced)
- Supply of energy (electricity, gas) with specific characteristics
- Demand of various types of energy with specific characteristics and services and deals
- The settlement, the payment of the energy is possible with blockchain.

For example: sun from own energy corporation, or if there is a deficit then from battery X and otherwise green from NL. Obtain green gas from a source as close as possible, if not available from TTF Realisation of energy use according to a specific profile and the quality and volume, as well as the source and which label (100% CO_2-free, local energy, energy from bio-farm).
A set of data that can be used in the demo

Connection with other Initiatives and projects
Alliander / EXE (Energy Exchange Enablers) has a number of new products, that possibly would fit into the ENSquare concept.
Entrnce: processes energy transitions entirely automatically on a quarterly basis and from EAN to EAN for companies that have independently purchased and sold electricity. The platform offers direct access to the energy trade markets (eg APX and Endex). Financial settlement is fully (administratively) arranged.
Rex: offers an operating system to control flexible appliances, thereby maximizing the flexibility in consumption of end users against the market price on the wholesale market.
Project Partners
Gasunie and Alliander, Pre-phase supported by knowledge institutes TNO and DNVGL
For whom:

- Suppliers, large customers
- Medium enterprises

2.8.4 LOCAL ENERGY COMMUNITY

Overview

The role of the DSO as the enabler of local energy community initiatives

In the Clean Energy Package of the EU, the Chapter III of the Electricity Directive defines a framework for Local Energy Communities (LEC) and Regional/Renewable Energy Communities (RECs). They define LEC as an entity which is distinct from traditional electricity undertakings operating in the market, based on their characteristics as value rather than profit driven, and which is effectively controlled by local citizens, local authorities or small and micro-enterprises. The concept of LEC/REC 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.
LEC/RECs as a market actor, while not a new concept, is still perceived as novel in the energy arena. It can be implemented differently in each country according to the regulatory framework as long as they comport with the eligibility requirements established at EU level. Some countries like Greece and Portugal have already paved the way, submitting proposals to change regulation allowing this concept to be implemented. The concept investigates how a new generation of LEC can be implemented in a specific country, hereby Austria using one of the existing smart grid demo sites.

How did Digitalization Help?

DSO has the command, retains the decision-making power, but enables the flexibility providers (e.g. flexible prosumers, DR aggregators, or LECs/RECs) to operate.

For this purpose, the DSO needs a comprehensive package, consisting of:

- Regulatory framework: Clear overview of the current and the proposed evolution direction. The ownership structure of LECs/RECs should be defined more clearly given LECs/RECs may have significant impacts on incumbent distribution system operators in some Member States. This has already been undertaken somewhat through improvements to the definition in the negotiations over the Clean Energy Package. However, a better understanding of existing ownership and control constructs of LECs/RECs is needed moving forward.

- Know how: case studies, demonstrations of the application of the advanced aggregation concepts
- DSO tools to manage flexibility in the distribution grid: Traffic Light Systems (TLS),
- Tools to perform the forecasts relevant for the aggregation of flexible resources, and to provide them to the actors on the market for a fee.
- Tools to enable the aggregators and LECs/RECs to operate in accordance with the needs of the grid and the requirements of the DSO. Such tools would be fully compatible with the TLS of the DSO.

The aim of the project is to take stock of existing demo and real-life examples that would fall under the concept of LECs/RECs. The actors involved, the organisational forms and investigated business models are mapped, its value analysed, and a report generated.

REScoop.eu, a European-wide federation of renewable energy cooperatives, provides a good basis for better understanding the concept of LEC/RECs. With around 1,500 members engaging in distributed renewables production, retail supply, energy efficiency, storage, aggregation, distribution and electric vehicle sharing, they have members who are already in a professionalised state to be able to engage with DSOs to develop and test out new flexibility services at the local level.

More information about other existing and pilot REC/LECs, including citizen- and business-based from the business sector can be found in the following links: http://www.flexcoop.eu/ and http://www.steeep.eu/lecs/.

Benefits of Digitalization

In the project, a comprehensive package of tools and information is specified for the DSO. The package would enable LEC to operate in the DSO’s grid in a way to support the DSO’s operation, and would receive benefits in return, and the DSO would provide this package to the prospective Aggregators or LECs.

In addition to providing potential system benefits for the DSO, some benefits of LEC can be (and sometimes have been) quantified as follows:

- Reinvestment in local economy. A much larger part of the initial investment and profits derived from energy communities flows back to the local economy as compared to external projects (up to eight times larger). These can go into local social initiatives (e.g. addressing energy poverty), into renovations of private and public buildings, or towards investment in local infrastructure (e.g. schools, community centres, etc).
- Lower electricity prices are to be expected as energy communities expect lower return-rates than external projects. This is crucial to help fight energy poverty.
- Stable real-estate value and reinvigorating rural areas. Due to the positive image of energy communities compared to villages where a renewable power-plant was installed by external actors, the value of the real-estate is largely sustained or improved.
- Public acceptance. RECs/LECs have shown to shape local perceptions of renewable energy and other clean energy technologies. When citizens have the opportunity to invest and participate, particularly in the planning and development of renewable energy generation projects, they are more likely to support the projects.
- Empowerment of consumers. Because they are members, the consumer, as the final user of the service provided by the LEC/REC, has an active say about the management of the LEC/REC, and how benefits are distributed and used at the local level.

2.9 PHYSICAL LAYER

2.9.1 DELIVER FLEXIBILITY TO THE MARKET

Overview

"Deliver Flexibility to the market" is a use case that existed for a long time. It means shifting electrical loads or generation in time to reduce grid congestions, avoid high electricity prices, avoid major voltage drops or stabilise frequency. There is a huge variety of reasons why the market needs flexibility. Especially in the last years the electrical system is changing, mostly due to the integration of fluctuating renewable energy sources and increase of electrical demand like heat pumps or e-mobility. The energy system of the future will most likely be decentralised with consumption and generation on every voltage level of the grid.

Enabling the flexibility from large power plants, mostly owned by power utilities, even though the flexibility of some power plants is limited, it is already done within a portfolio optimisation. Shifting loads from large industrial energy consumers is already done within virtual power plants or automated demand response aggregators.

Future use cases will most likely target smaller devices in terms of electric consumption or generation like household photovoltaic with electric storage, heat pumps or electric cars.

When speaking of households, the use case "deliver Flexibility to the market" is quite new.

The idea is, to enable the customer to shift his load or generation with the help of storage technology and participate on a market.

How did Digitalization Help?

Most concepts are based on a control box to control devices and communicate with a highly performant platform that aggregates and disaggregates flexibility and manages the devices.

Data analytics and forecast are a major functionality as well.

At the time there are only the following markets involved with different requirements in terms of performance (reaction time)

- Energy Markets (15 minutes to several hours)
- Balancing Energy (seconds to 15 minutes)

In order to succeed and find a business model the markets and regulations might need to change.

One example project for the use case "deliver Flexibility to the market" is the "GOFLEX project" http://www.goflex-community.eu/

Benefits of Digitalization

Summary of the GOFLEX project:

The GOFLEX project innovates, integrates, and demonstrates a group of electricity smart-grid technologies for managing flexibility in energy production and consumption. 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). A backbone data-services platform offers localised estimation and short-term predictions to support data-driven decisions for stakeholders. Demonstration sites for GOFLEX are in Cyprus, Switzerland and Germany and cover a diverse range of structural and operational distribution grid conditions. The project kicked-off in November and is in the process of specifying in detail how the various smart-grid technologies work together and how they will be deployed at the demonstration sites.

2.9.2 TRANSPARENT FLEXIBILITY MARKET WITH LV MONITORING - AGDER ENERGI

Overview

This use case describes the pilot related to Agder Energi´s 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.

It highlights the experiences from the Pilot on Agder Energi´s Engene substation and an early prototype of a flexibility marketplace in the distribution grid (hereafter: flexibility marketplace) which has been in operation since March 2017. Behind the success of the Pilot project is the collaboration between Agder Energi, Enfo, Powel and Microsoft in finding technological solutions to make the grid smarter. While energy technologies have made tremendous advances in the past decade, the electrical grid around the world has not. Power grids already require massive investments to keep pace with growing energy consumption; they are now challenged to leverage new resources — distributed energy systems like rooftop solar panels, batteries, EV cars, smart homes and facilities — that can help provide support back to the grid in times of high demand. The theoretical potential for demand side flexibility in the Nordics is estimated to be up to 12.000 MW (5.000 MW in Norway). In addition to the socio-economic benefit with increased use of renewable energy and demand response, the players in the power market will individually gain from utilization of flexibility from distributed energy resources, including demand response. DSOs need to have adequate means in place to make use of flexibility resources, supervise flexibility operations and make it easier and cost-effective for customers to benefit the most, while assuring quality of service and security to supply in a challenging environment.

How did Digitalization Help? **Description of Pilot**

The first step in the project was technically to demonstrate that an optimized decentral grid with demand response can be used to handle overload in an automated process. The next step was to use the proven technological solutions to operate a flexibility marketplace in the local grid area of Agder Energi. Thus, the focus has been to prove the technical functionalities of a flexibility marketplace rather than scale.

Figure 27 provides a conceptual view of the flexibility marketplace. The Proof of Concept is integrating the grid optimization (buyer) with the provider of flexibility (seller) through a distributed flexibility marketplace.

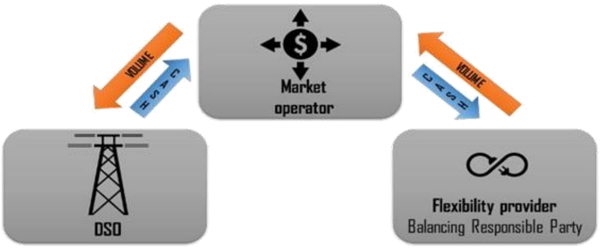


Figure 27: The distributed flexibility marketplace

The Pilot on Agder Energi´s Engene substation (25 MW) has demonstrated that an optimized decentral grid, with demand response, can be used to handle overload in a 100% automated process that analyses and predicts loads and flexibility in the grid using cloud-based technology. Several flexible loads have been tested and/or evaluated, including smart homes with solar panels and batteries, electric vehicles and commercial and residential demand response customers.

Today, the fully automatic demand response functionality is successfully up and running in the cloud as a non-wire-alternative to reinvestments. Since Agder Energi launched an early prototype of flexibility marketplace (March 2017) the entire technical set-up has also been demonstrated in a single DSO marketplace framework. In the marketplace, the consumer can offer his flexibility at a desired price, while DSO's optimization solution provides the basis for DSO's willingness to pay. This is automated in a closed loop. The Pilot of Agder Energi utilizes new innovative technology and digitalization to operate the grid in a more flexible way. Innovative digital solutions enabling flexible consumption, production and storage are to be registered and traded by all participants. The Pilot uses a cloud computing platform from Microsoft Azure. The solution is connecting components in the grid to open architecture for real-time information and control, allowing every part of the grid to participate. The solution will always use the most economically advantageous alternative first, which means the least expensive of DR assets, battery assets or a combination hereof. The economic optimization also takes place in normal operation situations without capacity constraints. Every hour a new optimization process is started. In short: The cloud-based technological innovations will improve the communication/interaction between the one responsible for the operation of the grid and the one who uses the services of the power system.

Benefits of Digitalization - Prototype of a flexible marketplace

The key goal of the Pilot is to create a well-functioning flexibility marketplace to ensure social economic benefit of flexible resources in a distribution grid. The demonstration shows that a flexibility marketplace can provide scalable and optimal use of flexibility and provide a transparent view using the demonstrated technological solutions. In this early prototype, the marketplace will be open for flexibility trade with the DSO. In a later phase, it will also include the TSO level/other capacity markets. So far, the marketplace concept has proved to work in Agder Energi´s local grid area.

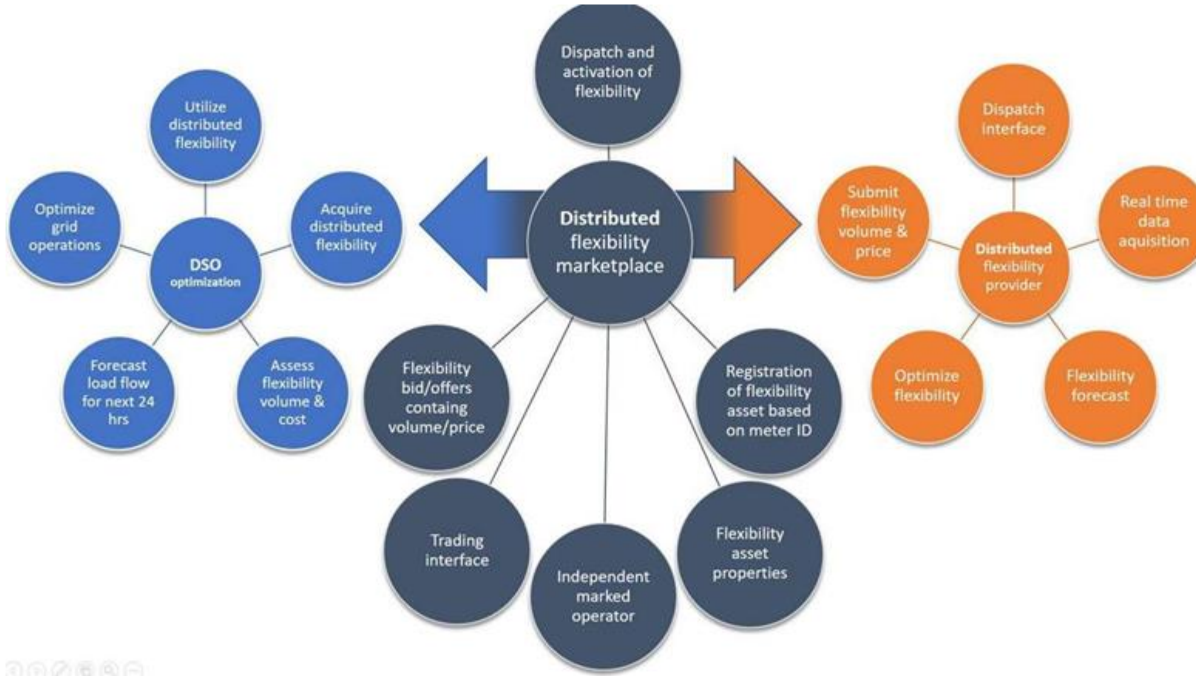

Dispatch and activation of flexibility
Utilize distributed flexibility
Optimize grid operations
DSO optimization
Acquire distributed flexibility
Forecast load flow for next 24 hrs
Assess flexibility volume & cost
Distributed flexibility marketplace
Flexibility bid/offers containg volume/price
Registration of flexibility asset based on meter ID
Trading interface
Independent marked operator
Flexibility asset properties
Dispatch interface
Submit flexibility volume & price
Real time data aquisition
Distributed flexibility provider
Optimize flexibility
Flexibility forecast

Figure 28: The architecture and functionalities of the flexibility marketplace

This early prototype of a flexibility marketplace is based on a “pay-as-bid” approach. In a pay-as-bid auction, prices paid to winning suppliers are based on their actual bids, rather than the bid of the highest priced supplier. The market operator of the flexibility marketplace is responsible for management, facilitation and operation of the marketplace where DSOs (in the pilot case) or TSO/BRP (in a future scenario) can buy needed flexibility from those participants who have flexibility to offer. The Flexibility Provider is a participant in the flexibility marketplace and controls one or more flexible assets. Each asset has a forecasted or nominated plan of consumption/production which can be deviated if required. This controlled deviation represents the flexibility of the asset. The DSO is responsible for providing grid related topological/geographical information to the marketplace. The DSOs can filter and choose the appropriate grid level in the marketplace, where the flexibility is needed, and bids below that grid level will be aggregated (in the marketplace). The Balance Responsible Parties participating in the flexibility marketplace can be both a Flexibility Provider and a buyer of flexibility, depending on its needs. Today, the regulatory framework in Norway only gives DSOs access to hourly based load information from the customer meters. In the future flexibility marketplace, the DSOs are given access to information about what happens behind the meter in the local grid area of which they are responsible. In the future, the customers are given access to a flexibility marketplace where they can sell and buy power at the desired price and volume to the grid company/flexibility service providers as well as to other customers or to the wholesale market.

Future Perspective

The ambition of Agder Energi is to expand the Pilot into other DSO areas in Norway and Europe, to prove that the Pilot works in other geographical locations and to identify added functionality. The ambition is that the experiences and innovations will contribute towards developing a fully integrated European marketplace for distributed flexibility.

Further development of the project aims to develop a digital architecture that can be used to optimize the grid by creating an independent and transparent digital marketplace where flexibility is displayed and traded in the power system. This phase will require new coordinating rules between the TSO and DSO. The main blockers for realizing this project are the current market model and regulations. Gradually moving away from the existing market model and designing a new integrated market from a bottom-up approach will be a better way of solving the future challenges.

2.9.3 PREVENTIVE MAINTENANCE – SMART METERING USE CASE

Overview

Advanced Metering Infrastructure (AMI) deployments are improving the lack of monitoring of the LV (Low Voltage) distribution grids, increasing the visibility and even enabling the controllability, operation and management of the LV network. Smart meter roll-out brings new opportunities to deal with challenges such as DER penetration increase, power supply restoration time improvement, more accurate and immediate information and/or ease consumer participation in the market. Once the wide range of measurements offered by smart meters is available, the challenge is to understand and correlate this set of data to anticipate the LV grid status. The smart meter events are one example of not fully exploited new information at network operation. Events indicate anomalous network situations or notifications, and they are reported by smart meters, enabling the DSO to automatically receive data from the LV network. Smart meter events cover circumstances related to Quality of Supply (QoS), demand response, security failures, fraud, communications or specific issues of network devices. Besides their type, smart meter events can also be classified as spontaneous or non-spontaneous. The first ones are reported when events take place, while the second ones are stored in the smart meters until there is a request to retrieve them to DSO (e.g. once per week).

From the wide range of events, those which could be useful for network operation are:

- Undervoltage and overvoltage: these set of events indicate that one or several phases of the customer meter are over or under the regulatory voltage limits. The duration of the anomalous situation is included in the event data;
- Loss of neutral: This event points that the neutral of the customer meter is broken or not connected;
- High impedance: this event only is reported by Medium Voltage (MV) meters, and it happens when one of the phases is broken;
- Reverse energy flow: the event occurs when the meter detects that energy is being injected in the grid, instead of being consumed;
- Power outage at the meter: the event is reported when the meter goes under an outage.

How did Digitalization Help?

The use of smart meter events with predictive maintenance purposes has been undertaken in the UPGRID [18]project. This project, funding by Horizon 2020 research and innovation program is 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. It includes 4 demonstrators, and the Spanish and the Swedish ones includes exploratory analysis of smart meter events potential. Within the Spanish pilot[19], the analysis of undervoltage and overvoltage events from customer meters has caused the modification of some tap changer position at distribution transformers, with the aim of avoiding potential problems at the distribution grid. Another consequence derived from the smart meter event analysis has been the development of a software tool, called Virtual Register. This tool monitors consumer voltage when necessary, allowing setting priorities to some of the maintenance crew commutes to the household facilities.

Benefits of Digitalization

In the case of the Swedish pilot[20], the use of events is more developed, and it is estimated that their use could decrease System Average Interruption Duration Index (SAIDI) by 4-10 %. Moreover, it is possible to distinguish power outages at secondary substations from an outage at customer meter by monitoring system events. Furthermore, individual meters can be requested for an acknowledgement confirmation which confirms that they are online, improving the outage detection. This kind of preventive maintenance, which is enabled through the grid digitalization, needs some steps to take full advantage of smart meter events, such as:

- Standardisation of event generation and delivery at customer meters;
- Deep review of events priority to classify them as spontaneous, non-spontaneous or even as non-recording in the DSO system;
- Analysis with broader time horizon aimed to avoid temporalities or misunderstanding consumption patterns;
- Enhance the ping request feature of customer meter.

2.9.4 EV / MOBILITY USE CASE

Overview

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. CECOVEL 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.

[18] UPGRID project, 2015-2017, European Union’s Horizon 2020 research and innovation programme grant agreement No 646.531, www.upgrid.eu

[19] J. García Prado, A. González, S. Riaño, „Adopting smart meter events as key datafor low-voltage network operation“ 2017, 24th International Conference & Exhibition on Electricity Distribution (CIRED)

[20] N. Eherden et al „ENHANCED LV SUPERVISION BY COMBINING DATA FROM METERS, SECONDARY SUBSTATION MEASUREMENTS AND MV SCADA“. 2017, 24th International Conference & Exhibition on Electricity Distribution (CIRED)

Currently it gathers real time information from approximately 1.000 charging points (in Spanish mainland and islands) provided by the main electric vehicle charge manager companies in Spain.

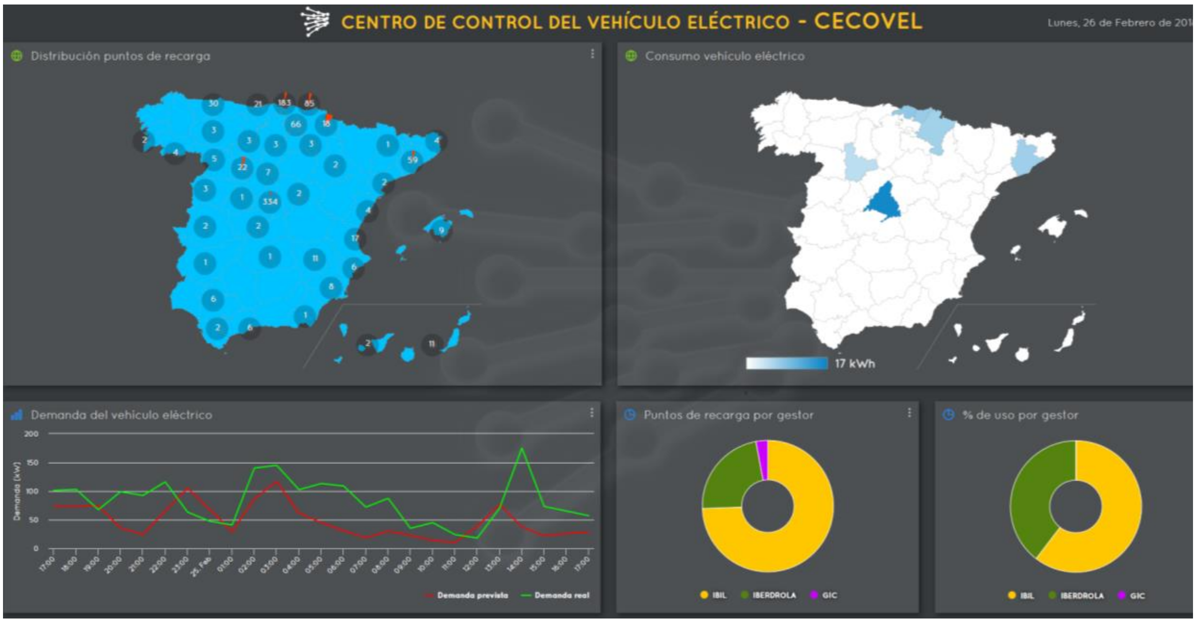


Figure 29: CECOVEL Software

Figure 30: CECOVEL Software within the Balearic Islands Control room

How did Digitalization Help?

Thanks to the digitalization of the information gathered in this project it is possible to analyse, using big data analysis technologies, and display the information associated to each charging point in Spain, its geographical position, demand forecasts and historic consumption data. CECOVEL offers to the control room operator a complete indicators panel that enables and facilitates the decision-making process. The most important aspects in which digitalization is helping are the following:

Better decisions

Access to this information allows a global vision of the situation of this new demand. More precisely it is possible to analyse consumer behaviour, profiling and load and production forecasting. This can be useful in order to define policies and initiatives adapted to these new consumers.

Costs savings

Visibility and manageability of consumption can lead to a better optimization of costs associated to electric vehicle demand supply.

Benefits from Digitalization

The main benefits of the CECOVEL control room are the following:

- Integrates electric mobility in the electric system in a safe and reliable manner;
- Helps to integrate renewal energies in the electric system;
- Enables new schemes of demand side management for these consumers;
- Allows a national vision on electric mobility and therefore it is a tool that all the stakeholders involved (vehicle manufacturer, utilities, charging infrastructure providers, charging managers companies and end-users) can use as a driver to impulse electric mobility.

2.10 BUSINESS LAYER

2.10.1 INCREASING PHOTOVOLTAIC SELF CONSUMPTION WITH DIGITALIZATION USING BLOCKCHAIN

OVERVIEW

“Increasing self-consumption with digitalization” is a use case which can be applied specifically to the recent boom of the solar photovoltaic (PV) systems in Europe and particularly with the new generation of systems which can no longer just profit from “feed-in tariffs” in their business models. In this case, PV self-consumption is becoming a must, especially in the building sector in countries such as Germany, Italy and France. The initial simple PV self-consumption concept is based on PV systems producing electricity which is directly used in the same place, at the same time and by the same entity. However, this simple case is leading to quite limited solar penetration into the building electric load (coverage rate) and self-consumption ratio (share of PV locally consumed).

How did Digitalization Help?

This use case is presenting the huge added value brought by digitalization to allow the extension of a limited market and limited impact of simple self-consumption to a new much more promising model of self-consumption: the collective one. This model is based on the creation of a virtual closed electric network inside a real public electric network thanks to very powerful digital instruments such as blockchain.

The collective self-consumption leads to the realization 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).

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.

The added value brought by a digital instrument such as blockchain is that this technology permits to manage a very large quantity of data in a local safe and secure mode (in terms of authenticity) which is fully disruptive compared to the actual situation in the electric conventional distribution model. Blockchain technology is of course in this use case developed in a special way to minimize the quantity of energy to function. In this French case, ENEDIS, one of the major French DSO is specially paying attention and is following this important and promising topic which can present a big development potential for renewables in the French electric grid. At the same time this concept has to be firstly experimented in good conditions to be further generalized.

One first experiment is being developed in South of France in Perpignan by several companies including Tecsol, a PV engineering company, and Sunchain that implements a Blockchain for a local authority and for a group of buildings in the city.

Other experiments are under development including one with several customers in a multi-family building sharing electricity produced by a unique PV plant on the roof. Then, electricity will be shared according to a dynamic repartition key with criteria fixed to optimize the self-consumption level. The dynamic behaviour of this process completed through a solution based on Blockchain technology.

Benefits of Digitalization

The main benefit using Blockchain and digitalization for this case is to make possible in a realistic way a potentially huge number of energy exchanges between prosumers and at an acceptable cost.

Digitalization opens a wide potential to ease the electric grid management from the DSO side however the number of prosumers increase in this concerned network.

Finally, using Blockchain for photovoltaic self-consumption makes finally feasible a very promising business concept for the deployment of solar energy in the European grids: peer to peer exchanges between prosumers.

End user benefit and commitment

PV Distributed/collective self-consumption is offering a real leverage for municipalities to benefit long term from cheaper electricity and ways to organize its management. A municipality in the South of France has recently checked and has started such a project with the installation of nearly 30 kWp PV on the roof of its Culture and Art Center and offering cheap electricity to other public buildings in the village such as the School, the Post Office and the Baker shop and several other electricity users in the village having a contractual link with the municipality (for instance, renting an office building). Digitalization and blockchain in this village is making the concept a reality including energy flux management.

Further information: this use case is being developed in the framework of a collaborative innovation project called DIGISOL thanks to the French funding system called Investment of the Future managed by the French Energy and Environment Agency ADEME (http://autoconsommation.cre.fr/documents/2017_09_26_autoconsommationCollective_Tecsol.pdf)

2.10.2 JOULIETTE - BLOCKCHAIN-BASED ENERGY TOKEN

Overview

The Jouliette is a blockchain-based energy token which empowers individuals and communities to easily manage and share their locally produced renewable energy.

On 15 September 2017, the Jouliette token was launched at De Ceuvel, a community in Amsterdam which has become a globally visible showcase for sustainable urban development.

The goal of the pilot is to investigate whether blockchain technology can be harnessed to create greater social value and to support a bottom-up movement in our transition towards 100% renewable energy supply.

The Jouliette project was a collaboration between De Ceuvel, Alliander and Spectral.

How did Digitalization Help? - How does it work at De Ceuvel (village in the Netherlands)

The trading interface for the Jouliette is not publicly accessible, however, below is a screenshot of one of the blockchain user interface pages. Via the interface, users can select which wallet they want to send Jouliettes to, and the transactions are automatically validated and displayed on the embedded blockchain explorer. Beyond manual transactions, the Jouliette platform also supports user configurable automated trading functions. Over the course of Q4 2017, the De Ceuvel community and Jouliette system developers will be working on integrating new features and applications, such as local time banking and car sharing.

History

The graphs in Figure 31 and Figure 32 show high resolution data regarding the total energy production and consumption within the microgrid. Hover over the graph to see the exact timestamp and values. A custom date range can be selected using the dropdown menu.

Power Consumption

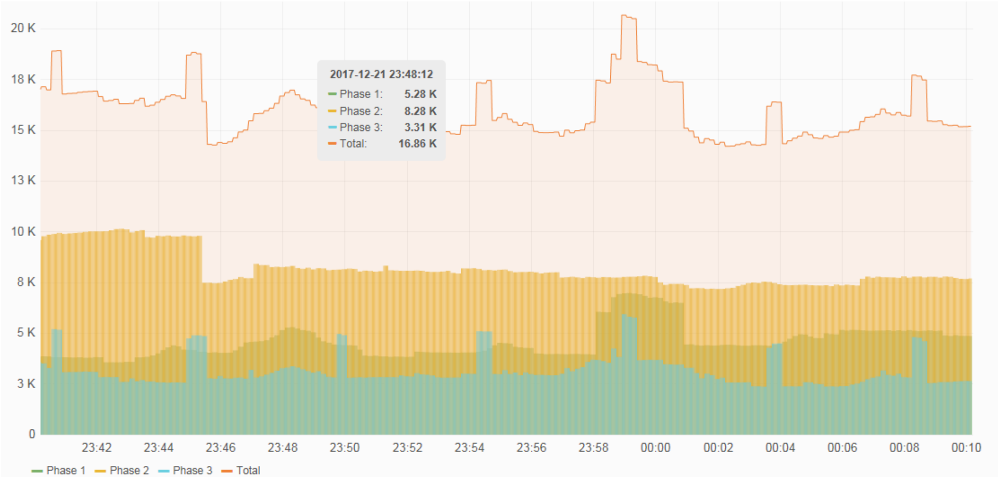


Figure 31: Example power consumption display of the History freature in Jouliettes system

PV Production

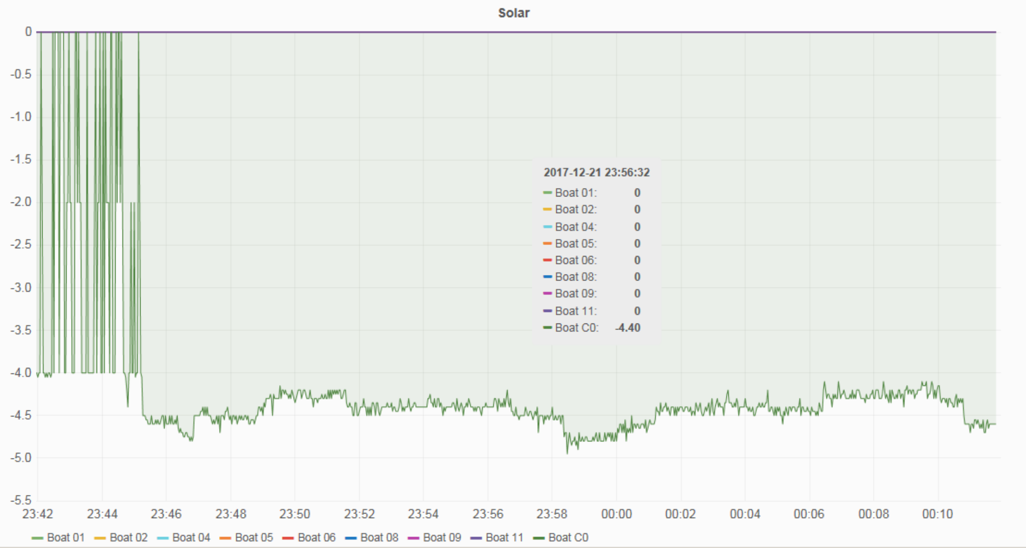


Figure 32: High resolution data regarding the total energy production and consumption within the microgrid (Snapshot of actual data on website)

Community Map

This map of De Ceuvel (Figure 33) shows the real-time flow of electricity within the community's microgrid. Green lines represent active feed-in of renewable energy, while red lines signify that the building is consuming energy. To see a snapshot of the real-time electricity production / consumption of each building, use your mouse to hover over. Clicking on the building will reveal a more detailed overview of its current energy usage, including a visualization of the energy consumed by the heat pump (where applicable).

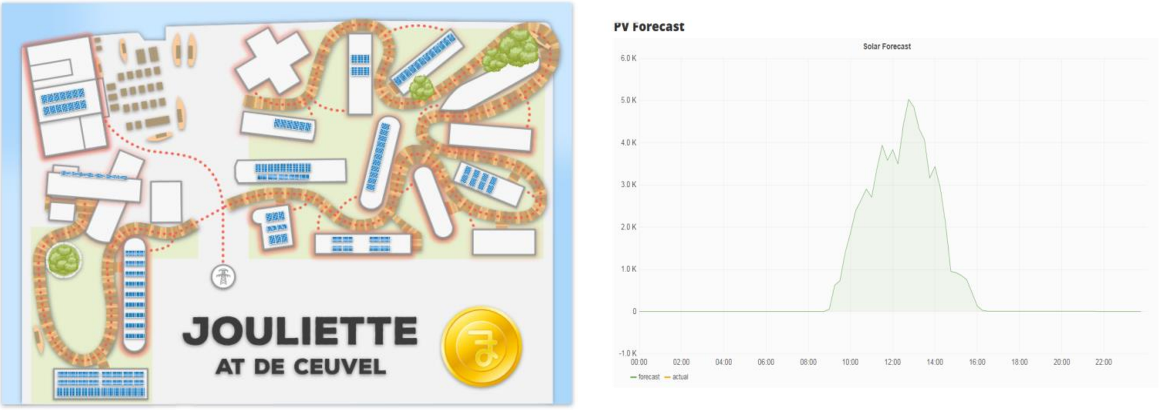


Figure 33: Community Map

2.10.3 CONSUMER EMPOWERMENT, CUSTOMER RELATIONSHIP AND BEHAVIOURAL CHANGE

Overview

The liberalisation of electricity markets led to the emergence of numerous offers on the market, with various options (such as "green" electricity option or Time of Use schemes), which contributes to the decision-making process for consumers (see graph below). In the meantime, consumer empowerment in the energy system became a clear goal of the European Commission, as stated in the Energy Union Communication published in February 2015 (Beyond choosing the supplier, these services can also contribute to identify sub-optimal settings of some domestic appliances, such as the hot water tank).

This empowerment is usually seen as the ability for consumers to easily (i.e. in less than 3 weeks with no additional cost) switch supplier, to be exposed to an understandable electricity bill (making sure that there are not too many elements on the bill, which confuses the reading), and to get access to a certified and reliable comparison tool allowing them to take well-informed decisions.

In the same Communication, the European Commission states that "smart technologies will help consumers and energy service companies working for them to reap the opportunities available on the energy market by taking control of their energy consumption (and possible self-production). This will deliver more flexibility in the market and potentially reduce consumer bills".

In this regard, the smart meter is an essential building block to fill the informational gap and to enable this control taken by the consumer.

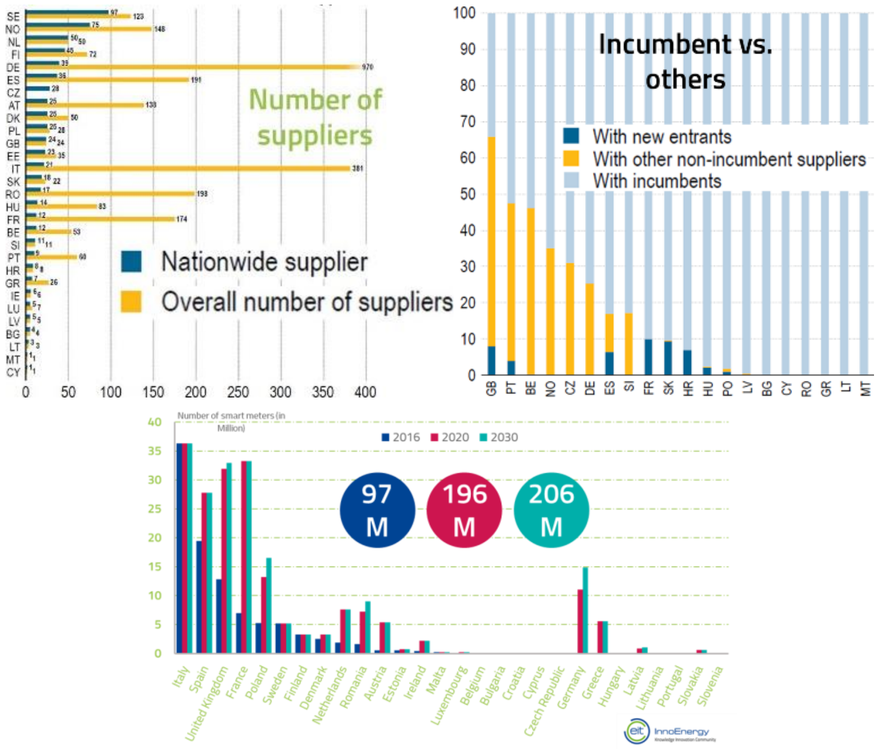


Figure 34: ACER/CEER, Annual Report on the Results of Monitoring the Internal Electricity and Natural Gas Markets in 2014, November 2015

How did Digitalization help?

In this context, new services for consumers are emerging, combining the data coming from the smart meters and a database of all the existing offers for households, to help them navigate it and choose the offer which suits their preferences, taking into consideration their actual consumption and not an estimate. For instance, thanks to the Linky smart meter currently deployed by the French DSO Enedis, new players like Wivaldy propose services to households, like a free 7-day diagnosis based on real consumption. Similarly in other countries, new players are appearing in the wake of the smart metering deployment, aiming at empowering the consumers, such as Greenely in Sweden, which develops a personal coach to guide users and provide them with tips and tricks to optimise their consumption.

Consumer empowerment is not only a matter of being able to choose the best [21] offer from various suppliers or to get a clearer bill, but also to become more active in the energy system. Being a more active consumer usually refers to being able to generate, self-consume, store or sell electricity. However, a consumer becomes active as soon as he starts using electricity in a conscious manner, and he starts to alter his own consumption towards efficiency or flexibility, contributing thus to the transition of the energy system. In this regard, EIT InnoEnergy develops and invests in Societal Appropriation, aiming at raising people's awareness about energy to progressively lead them towards playing a steering role within the energy transition.

[21] Here, « best » does not necessarily mean the cheapest, but the offer which suits the consumer's preferences best.

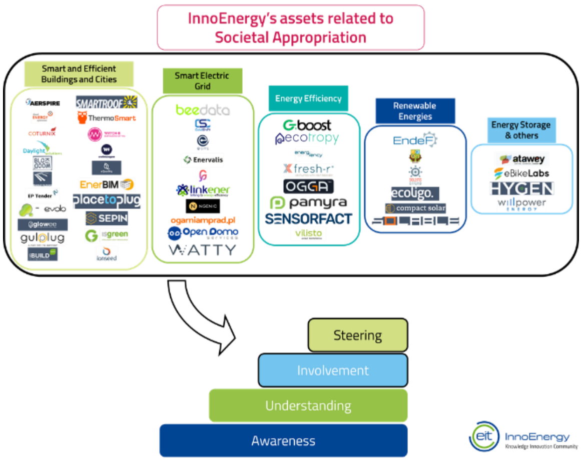


Figure 35: InnoEnergy's assets related to societal appropriation

This also opens the door to the contribution of behavioural change to the energy transition. In this regard, there is expanding research activity in Europe. We can mention initiated Horizon 2020 projects like UtilitEE [22], inBETWEEN [23], Eco-Bot [24], eTEACHER [25], or FEEdBACk [26] or ECO2[27]. At the core of these projects, the use of ICT is clearly established, and the key challenge of increasing or facilitating the adoption of those ICTs by the end-users is targeted. In this regard, behavioural interventions, involving strategies such as goal-settings, commitment, feedback (direct and indirect), comparison to others, or information prompts, are dramatically eased by the use of smart metering, notably to create personalised and contextualised interventions. Companies, mainly innovative SMEs and start-ups are developing solutions in this direction, to motivate users to change their energy behavior [28].

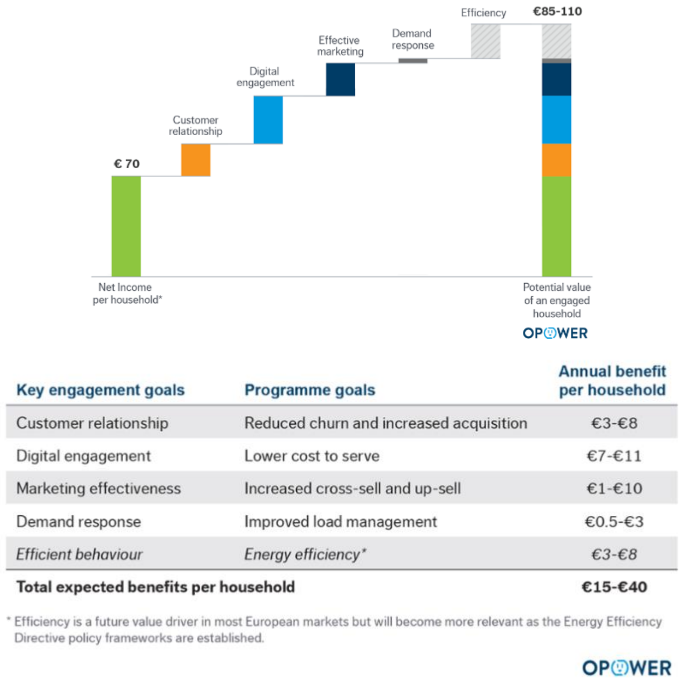
Beyond that, as argued in the literature [29], the combination of behavioural intervention strategies (Behavioural intervention strategies are small pieces of behavioural intervention programmes) is more effective than individual strategies, and specificity and customization concepts are essential for effectiveness of programmes. Besides, community-based programmes targeting specific audiences can lead to up to 31% of energy savings [30.] In this direction, gamification of energy use and of energy savings, as well as proper gaming as such, are growing fields in Energy, enabled by ICTs and by the broad deployment of smart metering, which combine in a personalised and highly engaging way, several behavioural intervention strategies, in order to motivate and nudge a behavioural change in a persistent manner. To illustrate that, the research projects DOMINO [31], or Social Power [32] (from Swiss organisations such as ZHAW- the Zurich University of Applied Sciences) are relevant initiatives that could serve as a source of inspiration.

Benefits of Digitalization

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.[33] According to Opower,

[22] Utility Business Model Transformation through human-centric behavioural interventions and ICT-tools for Energy Efficiency
[23] ICT enabled BEhavioral change ToWards Energy EfficieNt lifestyles
[24] Personalised ICT-tools for the Active Engagement of Consumers Towards Sustainable Energy
[25]end-users Tools to Empower and raise Awareness of Behavioural CHange towards EneRgy efficiency
[26] Fostering Energy Efficiency and BehAvioural Change through ICT
[27] Energy Conscious Consumers
[28] The two start-ups mentioned earlier on, namely Wivaldy in France and Greenely in Sweden, can be referred to here, but some other companies like Opower (acquired by Oracle in May 2016), Bidgely, Tendril, or Intelen are noteworthy.
[29] Sussman, R,.Chikumbo., 2016. Behaviour change programs: Status and Impact, Report. American Council for an Energy-Efficient Economy, Washington, D.C,
[30] Sussman, R,.Chikumbo., 2016. Behaviour change programs: Status and Impact, Report. American Council for an Energy-Efficient Economy, Washington, D.C, p.36.
[31]DOMINO - Connecting Europe, Saving Energy
[32] The reader can find the website of this project here and a publication about the results can be found here.

the question of customer engagement is of great business interest for energy companies, as they value this engagement between 15€ and 40€ annually (see Figure 36).



Key engagement goals	Programme goals	Annual benefit per household
Customer relationship	Reduced churn and increased acquisition	€3-€8
Digital engagement	Lower cost to serve	€7-€11
Marketing effectiveness	Increased cross-sell and up-sell	€1-€10
Demand response	Improved load management	€0.5-€3
Efficient behaviour	*Energy efficiency**	*€3-€8*
Total expected benefits per household		**€15-€40**

* Efficiency is a future value driver in most European markets but will become more relevant as the Energy Efficiency Directive policy frameworks are established.

OPOWER

Figure 36: Drivers and barriers for customers participation in Opower

In the same vein, in a recent study based on interviews with 200 senior business and technology executives from major European utilities [34], the 2 main challenges faced by their companies are respectively the acquisition of new customers (73%) and the customer retention/reducing the churn (60%). When these executives are asked in which areas they plan to invest to improve customer engagement, the top 3 answers are respectively Customer experience management (84%), Customer segmentation (68%) and Social media as a customer service channel (68%), all leveraging digitalization technologies.

2.10.4 DEMOCRACY BY DESIGN

Overview

Our world is digitizing, and new systems are emerging. Across the globe, public and private parties are building the smart cities and smart infrastructures of tomorrow. They strive to improve the efficiency of systems, reduce costs, improve reliability and offer better services by implementing information technology in our public spaces and infrastructures. These developments will play an important role in the way we will shape our future lives and society. Information technologies will be delegated decisions that affect our economic, social, personal and physical environment. Amidst new possibilities, we need continue to ask ourselves ethical questions on the functioning of our infrastructures and cities. For example, when an energy system's malfunction leads to temporary scarcity, who will enjoy uninterrupted energy supply? And who will have priority on the congested roads when a road accident has happened? Increasingly, information technology systems will decide how we are treated and who gets prioritized. Yet, whose technology makes decisions and based on which principles? And do these choices take into account the interests of all concerned? We urgently need to start the discussion on how our decision makers and citizens can make the right choices, as the pace of the developments is rapidly increasing.

[34] Mayes,N.,2017, Digital Utilities: From Behind the Curve to Innovation: How Europe's energy and water retailers plan to ride out the revolution in customer engagement, Trendy Study, CPX Group..

How to include democratic values in smart decision-making processes?

The growing pervasiveness of digital technologies in our cities raises the question of how they relate or should relate to democracy. To what extent do they enhance or subvert democratic values and how do they shape democratic decision-making processes? The complexity of algorithms, for example, can make it difficult to hold decision-makers accountable and the automation of decision-making processes can disadvantage less tech-savvy citizens and reduce their ability to participate in society. Municipalities, public infrastructure providers, civil society organizations and others that are concerned with issues of common concern, such as improving the air quality, the sustainability of a city transport system or the facilitation of the energy transition, look to digital technologies for solutions. As such they are faced with the question of how to develop, implement and maintain technologies to solve particular problems, while safeguarding democratic values and the democratic process.

Project goals

In 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”. The framework will allow them to ask the right questions and identify possible challenges and solutions. We do this by organizing a series of round-tables and workshops to explore what designing for democracy means and to develop concepts, tools and methods for practitioners to work with. Another important project delivery is the development of a platform for knowledge sharing with stakeholders and the industry to further set the agenda for this topic, create awareness and provide concrete recommendations. We will be using case studies to investigate real-life smart city cases in detail. We focus on innovative smart projects which aim to develop new smart city solutions. These case studies will be in the field of energy, electric mobility, public lighting and traffic management.

How did Digitalization Help?

Use case: transparent charging station

Based on which principles does the new technology make decisions? If you can’t see what choices are being made or why, you might feel you’re at the mercy of technology and algorithms. Consumers who use smart technologies want to see and understand the applied transparency principles. A transparent charging station – a project of Elaad & Alliander, designed by The Incredible Machine – is a response to the growing importance of algorithms in our daily lives, making visible the invisible logic when charging an electric vehicle. The display shows how the electricity is allocated between the cars being charged. In the program Democracy by Design we use the transparent charging station as a use case to research the way democratic values are applied in smart decision-making processes.

Benefits of Digitalization

The main benefits are to be achieved in improved decision making by policy makers, technologists, project managers, civil servants, and other relevant parties in safeguarding democratic values “by design”. For example, the city of Amsterdam, infracompanies, IT architects and IT design engineers. Read more about this use case in the white paper Designing a Transparent Charging Point and the press release by Elaad & Alliander (28-09-2017)

2.10.5 DIGITAL TWIN

Overview

Digital twins are dynamic digital or virtual software replications of physical assets, products and constructions. Which asset, product or construct, from cars and motor cycles to engines, wind turbines and even buildings, spacecrafts, airplanes or factories needed to be virtually replicated or represent depends on several factors as of course there needs to be a goal and a value within a context of specific stakeholder in the energy business. Digital twins remove the silos, inefficiencies, uncertainties, errors and huge resources in working with models.

How did Digitalization Help?

Digital twins have moved from concept to reality much faster in recent years, thanks to modern information and data management and analytics possibilities, technologies enabling digitization and much more. The current acceleration, however is mainly made possible thanks to the IoT and the lowering costs of technologies that boosted both IoT and the digital twin. IoT and sensors power digital twins. By having a smart connected product with its virtual representation, ample business goals can be served which is also a driver of digital twin adoption, along with the convergence of several factors. According to the Gartner report, as of October 2017, digital twins in the context of IoT projects are particularly promising over the next three to five years and are leading the interest in digital twins today. Digital twin technology is to expand its reach beyond the currently predominant context of somewhat more mission-critical and/or expensive assets – called collectively Digital Assets in DSO and TSO agendas, into more 'simple' physical products as technology costs keep dropping and both the business rationale and – affordable – technologies to do so come closer for other stakeholders such as VPPs, aggregators, and prosumers in general.

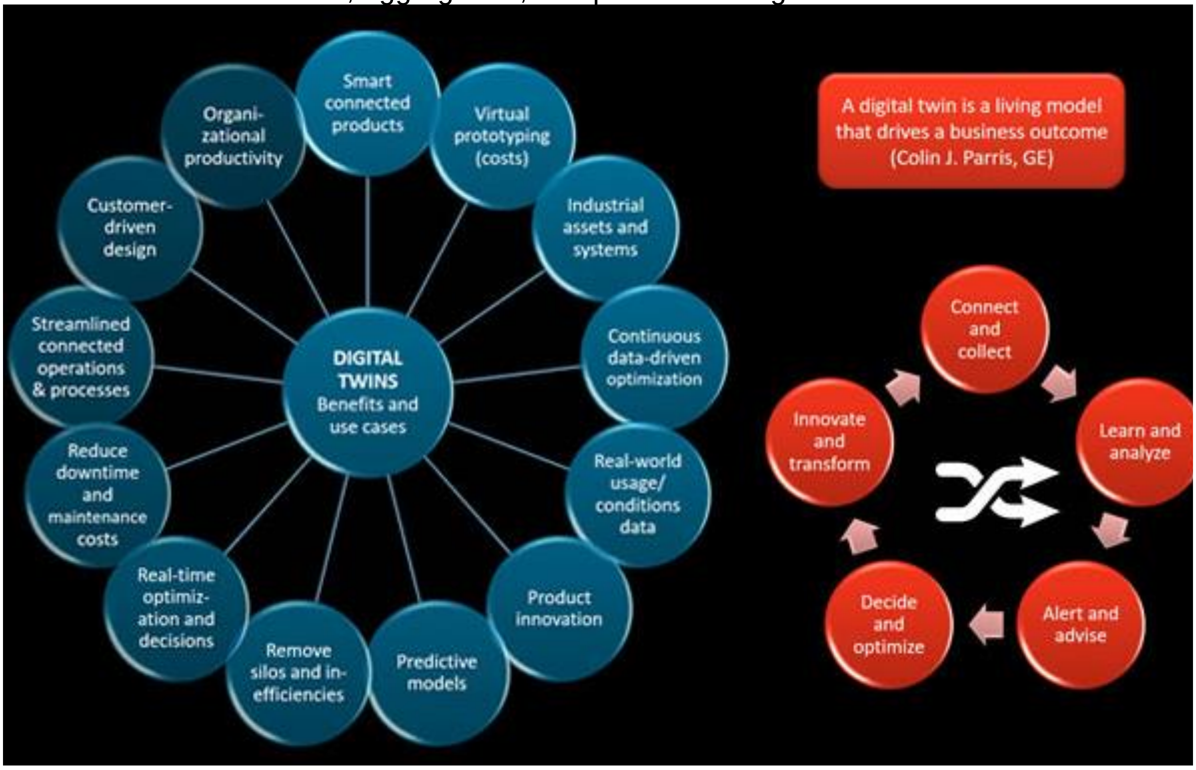

DIGITAL TWINS Benefits and use cases
Smart connected products
Virtual prototyping (costs)
Industrial assets and systems
Continuous data-driven optimization
Real-world usage/ conditions data
Product innovation
Predictive models
Remove silos and in-efficiencies
Real-time optimiz-ation and decisions
Reduce downtime and maintenance costs
Streamlined connected operations & processes
Customer-driven design
Organi-zational productivity
A digital twin is a living model that drives a business outcome (Colin J. Parris, GE)
Connect and collect
Learn and analyze
Alert and advise
Decide and optimize
Innovate and transform

Figure 37: Picture used from GE Digital Twin overview

Benefits of Digitalization

Use cases for digital twin technology vary as mentioned and digital twins combine sensors, cognitive analytics and data to make digital simulations and virtualized products and assets (the twins) whereby of course there is an overlay of digital information onto the physical world which needs to be leveraged for, among others, product design and service purposes. The real advantage of the digital twin, however, materializes when all aspects, from design to real-time data feed, are brought together to optimize over the lifetime of the asset. An accurate digital description of a physical asset, for example, does not just cut prototyping or construction costs, it also enables to predict failure more easily once real-time data is fed into the model, thus reducing both maintenance costs and downtime. Another example is currently piloting a “digital wind farm” concept, which informs the configuration of each wind turbine prior to procurement and construction. Once the farm is built, each virtual turbine is fed data from its physical equivalent, and software enables to optimize power production at the plant level by adjusting turbine-specific parameters, such as torque of the generator or speed of the blades. The hope is to generate 20% gains in efficiency.

Example – Cost Impact Simulation of Blackouts within the Electrical Grid

A successful attack to the critical infrastructure of utilities or distribution system operators (DSO) critical infrastructure may cause tremendous costs and severe damage to individuals, society, industry, or public or legal entities. However, mitigating the risk by implementing security technology requires a costly up-front investment and ongoing maintenance. Within the EU FP7 project Smart Grid Protection Against Cyber Attacks (SPARKS) a simulation tool has been developed to explore costs from power outages in order to justify investment into reasonable security measures. The Blackout Simulator can be used by utilities or DSOs to plan and upgrade their grid infrastructure to grant reliability of supply. Municipalities, investors, and insurance companies would receive a risk assessment by evaluating attack or blackout scenarios, which provide damage cost figures and potential losses in terms of revenue or taxes.

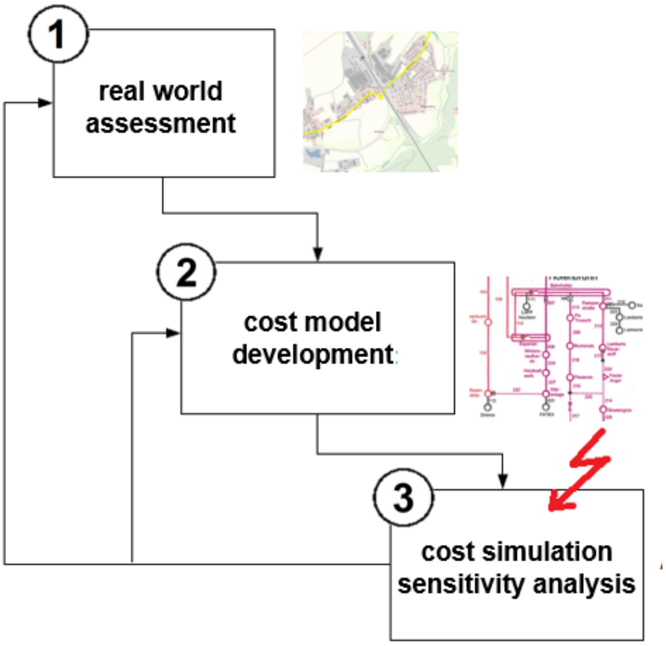


Figure 38: The digital twin of the grid infrastructure can be used to simulate blackout scenarios and to justify investment into security measures.

The SPARKS project has been supported by the EU FP7 Programme under Contract No. 608224. Start Date: 1st April, 2014; Duration: 3 years[35].

2.11 EMERGING 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
- Big data, data analytics, data mining
- 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
- Model-based management
- Augmented reality
- Advanced geographic-based models and UAVs
- Power electronics everywhere based on broad application of wide band-gap devices
- Smart inverters for PV, storage and other technologies
- Electrification technologies
- Integrated security operation centres (ISOCs)
- Advanced visualization approaches
- New market structures, transparency of prices, approaches for flexibility

2.12 RECOMMENDATIONS

Enabling monitoring, visualization, and analytics for every stakeholder group
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. Close cooperation between supplier and customer helps to specify these. Legal issues, e.g. data protection requirements need to be considered as well. Technically, the customer's hardware and software need to meet certain requirements to get connected and the equipment that needs to be monitored and evaluated requires possibly additional hardware such as sensors.

Building data hubs
Data Exchange Platforms (DEPs), as mentioned with Smartnet project (in collaboration between TSOs and DSOs segment), 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 and their functionalities are subject to different regimes and practices throughout Europe. DEPs that take a wider system perspective and facilitate innovation through stimulating the development of third-party applications (for example, in the Estonian DEP) can be said to constitute the state-of-the-art with regards to data exchange in the European context.

Cross-sector coupling
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

[35] Reference publications: Kleineidam G., Jung G., Wöltche A.: „Cost Impact Simulation of Blackouts within the Electrical Grid“, proceedings International ETG Congress 2017, November 28-29, 2017, Bonn, Germany (pages125-130). ISBN 978-3-8007-4505-0

package to the consumer. However, a regulatory framework would need to follow and facilitate these services.

Local energy communities – regulation and ownership structure
LEC offer many benefits with particular customer visibility and engagement potential as indicated by the Flexcoop project. However, the ownership structure of LECs/RECs should be defined more clearly given LECs/RECs may have significant impacts on incumbent distribution system operators in some Member States. This has already been undertaken somewhat through improvements to the definition in the negotiations over the Clean Energy Package. However, a further understanding of existing ownership and control constructs of LECs/RECs is needed moving forward. Furthermore, tools to perform the forecasts relevant for the aggregation of flexible resources that enable the aggregators and LECs/RECs to operate in accordance with the needs of the grid and the requirements of the DSO need to be further developed. 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, as observed from the demonstration sites for GOFLEX project in in Cyprus, Switzerland and Germany.

Industry collaborations
A strong collaboration between industry leaders and utilities is needed to ensure accelerated innovation and replicability of the new flexibility models. The experiences from the Pilot on Agder Energi´s Engene substation and an early prototype of a flexibility marketplace in the distribution grid which has been in operation since March 2017 highlight this necessity. Behind the success of the Pilot project is the collaboration between Agder Energi, Enfo, Powel and Microsoft in finding technological solutions to make the grid smarter.

Further exploiting existing technologies
Existing infrastructure such as smart metering should be further exploited and utilized for use of smart meter events with predictive maintenance purposes. This has been undertaken in the UPGRID [36] 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.

Establishing Innovation/Expert centres – case in point for EV penetration
With new consumer demands aiming to accelerate penetration of EVs, good practice can be to establish an innovation/expert centre for EVs within a TSO/DSO stakeholder, ie. CECOVEL includes software systems that provide Spanish TSO with visibility and manageability in real time of electricity consumed by vehicles in Spain as well as a simulation of the impact of future scenarios with high penetration of electric vehicles.

Data transformation – case of digital twin
The current extent of data digitalization among DSOs, TSOs and other energy stakeholders is uneven; however, benefits have a wide range for digital twins, including the SPARKS project for simulation of large-scale blackouts. In order to create dynamic digital or virtual software replications of physical assets, products and in the future prosumers themselves, further data transformation is needed.

Decomposing blockchain challenges through research
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

[36] UPGRID project, 2015-2017, European Union's Horizon 2020 research and innovation programme grant agreement No 646.531, www.upgrid.eu

consumption, cost and control, security and privacy – as most of these examples are being developed not as open source, integration concerns, and cultural adoption.

Customer empowerment – needs not only technology but behavioural change
Consumer empowerment is not only a matter of being able to choose the best offer from various suppliers or to get a clearer bill, but also to become more active in the energy system as demonstrated with the development of services like Wivaldy in France (in the context of the Enedis Linky project) and Greenely in Sweden. Investments in contribution of behavioural change to the energy transition, aiming at raising people's awareness about energy to progressively lead them towards playing a steering role of the energy transition is one more component needed. Companies -mainly innovative SMEs and start-ups, are developing solutions in this direction to motivate users to change their energy behavior towards efficiency and flexibility.

Democracy by design
Finally, as Digital technologies have been touted as facilitating, enabling and even enhancing democratic processes at the same time they can pose a threat to democratic processes and public values. The complexity of algorithms, for example, can make it difficult to hold decision-makers accountable and the automation of decision-making processes can disadvantage less tech-savvy citizens and reduce their ability to participate in society. Therefore, a framework supporting decision makers is required to address this aspect as highlighted in Democracy by design use case.

2.13 FURTHER RECOMMENDATIONS

"Deliver Flexibility to the market" Flexibility markets need to be profitable for small loads in order to make many of the decentralized use cases, especially for household customers work. Therefore, the market design needs to be reviewed with focus on flexibility markets and the players on those markets i.e. at least 15-minute interval metering and settlement needs to be implemented, which is not the case Europe-wide.

2.13.1 CONGESTION MANAGEMENT

To deal with congestions properly, the following key aspects need to be considered:

- To ensure safe and reliable operation at all levels, information and data exchanges between system operators in all relevant timeframes (network planning, operational planning and scheduling, real-time) should be enhanced. This requires a coherent design of the architecture of IT and data exchange interfaces within a TSO's control area (and can even go beyond the control area and include several TSOs). The architecture of IT and data exchange interfaces should encompass all DSOs in a TSO control area, although this does not necessarily imply that all DSOs (independent of their size and network level) will have a direct interface to the respective TSO.
- It should be ensured that each system operator has sufficient data, both structural, market-related and in real time, on its observability area) needed to maintain safe operation when it comes to congestions.
- System operators should have the necessary information and data to check whether certain flexibility bids, when activated, could create congestions in their grid. Furthermore, if a flexibility bid could indeed create congestion, the respective system operator needs to have the ability to provide the necessary information, define limits for or prevent bids activation in areas that will lead to grid constraints).
- TSOs and DSOs should discuss further how to deal with these issues on a practical level. DSOs are concerned about possible misalignment of actions between TSOs and DSOs and also between other market players in some cases that could lead to a loss of control

of the distribution grid and drive inefficient grid expansion. At the same time, TSOs are concerned about their ability to perform efficient balancing of the overall electricity system, ensuring security of supply and fair market functioning. With the increasing amount of (renewable) generation facilities in distribution networks, both TSOs and DSOs would like to unlock as much of the potential of these distributed resources as technically possible.

- Cooperation between market players in the energy sector and outside the energy sector that create cross sector product bundles are needed. This would provide new players and technologies for the energy sector which could increase performance and lead to development.
- Measurement and data, respectively knowledge is key. The starting point of most business cases is a model of the customer. Use cases that help gathering data and building such models are crucial for new business cases to succeed.

2.13.2 BALANCING:

Exchanges of information between TSOs and DSOs should be reinforced, taking the increased need for cooperation into consideration, e. g, the non-exhaustive list:

- Product;
- Maximum/minimum upwards/downwards flexibility amount (kW) delivered for each relevant balancing period of the day;
- Location (connection point);
- Depending on the level of capacity/assets size, extra information is required.
- Offers (amount of flexibility offered, assets portfolio, etc.);
- Activated offers; and
- Limits needed by the DSO.

From DSOs' points of view, some balancing actions could be devolved to them to procure balancing services on their networks to support the TSOs as a subsidiary activity. This could help manage the impact of distribution generation within specific parameters as set out by the TSO. This assures the TSO that balancing interventions are occurring on the DSO network without the TSO needing to check with the DSO every time a balancing action is needed on the DSO network.

2.13.3 FLEXIBILITY

Coordination between TSOs, DSOs and other stakeholders using distributed flexibility will require extensive cooperation and clear boundaries between TSOs' and DSOs' rights and duties. System operators can use flexibility to manage their grids (responsibility area), but they also need data from part of the connecting grids (observability area) to manage the grid properly, taking into account that the market works as freely as possible.

2.13.4 COORDINATION OF FLEXIBILITY OPTIONS:

Flexibility can be used for different purposes and by different parties:

- TSO for balancing (power balance for frequency control);
- TSO and DSO for congestion management;
- TSO and DSO for power quality control; and
- BRP for portfolio balancing (energy balance).

Therefore, a coordination process is needed to ensure that a flexibility bid can only be activated once and will not cause problems in either the grid they are connected to or in grids that might be influenced (see also congestion management). Flexibility options on the one hand affect TSOs and DSOs, but on the other hand even more directly affect the generators, customers and loads, prosumers and storage operators, suppliers and aggregators that offer them. Those parties thus need to have access to and benefit from certain data being exchanged between TSOs and DSOs, and they own certain data that are being exchanged. This shows yet another advantage of a coherent architecture of IT and data exchange interfaces encompassing all DSOs within a TSO's control area: It lends itself easily to access and partial control by customers, generators, prosumers, storage operators, suppliers and aggregators.

1. Introducing the flexibility marketplace for flexibility trading requires a more active role for the DSOs. DSOs need to be active in information exchange to all market parties.
2. The DSO needs to be able to forecast when and where the congestion will occur.
3. A new flexibility marketplace should be able to coexist alongside current markets.
4. The new market place will provide a way to offer flexibility that is compatible with existing energy products.
5. A product in the new flexibility marketplace is made up of building blocks and a set of parameters. By offering this flexible product design, the flexibility market place can give buyers and sellers the exact desired properties that they are looking for.

Aggregators can play a major role in unlocking flexibility and will play a growing role in the market. The regulatory framework and subsequent data management model should support data exchange needed for such a development, foreseeing the needs of TSOs and DSOs to receive relevant information.

2.13.5 REAL-TIME CONTROL AND SUPERVISION:

Starting at the Member State level, TSOs and DSOs should mutually agree on data management models, data format and communication protocols for these data exchanges. If beneficial to society, this harmonisation should be on the European level.

TSOs and DSOs should proactively develop the TSO – DSO interface to support data acquisition and data exchange between grid operators in real-time for market parties to perform better portfolio optimisation and therefore facilitate the integration of RES and customer connections.

2.13.6 NETWORK PLANNING

TSOs and DSOs should work towards common assumptions for planning purposes (e. g, economic growth, resilience and national carbon reduction plans, etc.) and common parameters for planning methodology (e. g, definition of connection requirements from grid users, simplified electrical grid models, etc.).

Information exchange between TSOs and DSOs supporting long-term network development process could include simplified electrical grid models, including foreseen and planned grid expansion projects as well as annual demand/generation forecasts per physical TSO – DSO interface.

Information exchange between TSOs and DSOs supporting operational planning could include, as long as it respects confidentiality issues, the year-ahead availability plan, outages and business continuity/ emergency plans and information related to upfront activities for operational security analysis. Furthermore, demand/generation forecasts on the TSO – DSO interface could be exchanged and/or published periodically, which also would facilitate integration of RES and new customer connections. The periodicity of these forecast exchanges could evolve over time.

3. CYBERSECURITY - CYBER-ROBUSTNESS (TF3)

3.1 EXECUTIVE SUMMARY

Cyber-security 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 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 documents first chapter considers digitalization use cases of Task Force 1, digitalization technologies of Task Force 2, and this third chapter deals with digitalization cybersecurity topics.

The identified topics were clustered into three areas:

- 9 technical topics (focusing on near-future research needed), either technology related topics in need for cybersecurity research, or can be used for solving cybersecurity and resilience challenges
- 9 policy topics (with near to midterm future research relevance), policy and governance related topics in need for cybersecurity research, or can be used for solving cybersecurity and resilience challenges
- 9 future challenges topics (sharing midterm future research needs identified, leading into 2050, sometimes can seem far-fetched), 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).

Following a brief introduction, background information, and motivation, relevant European cybersecurity covering projects are described. A glimpse into the different needs of cybersecurity considering Information Technology (IT) and Operational Technology (OT) is provided. A deeper look into cyberattacks 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.

The summarized recommendations for research in the three clusters are listed as follows:

- Technology
  1. AI will help cybersecurity industry to efficiently monitor sophisticated threats
  2. Blockchain is considered as a promising technology to address authentication, authorization, consensus, and immutability

3. Blockchain offers a secure decentralized way to guarantee the veracity of various transactions
4. Digitalization enables and relies on the massive deployment of sensors that improve analysis
5. IoT enabled devices will make the energy system more transparent and efficient with analytics
6. For highly networked components, safety is not reachable without cybersecurity
7. Machine Learning enables predictive analytics which helps detecting cyber attacks
8. OT/IT cybersecurity architecture raises the question of on-premise vs cloud-based calculation
9. Grid optimization application are suitable to be deployed in a cloud environment; however, safety or security relevant grid control requires still a decentralized grid asset deployment

- Policy
  1. Metrics and frameworks should be developed for decision making of cybersecurity risks
  2. Stakeholders operating in isolated silos need a communication platform (IT, TSOs, DSOs, ESCOs, Policy)
  3. Cybersecurity research at a meta level should be stimulated among member states
  4. Transparency of data flows and standardized data models are required for GDPR
  5. Cost benefit analyses shall be considered (e.g., black out simulators)
  6. Research on regulation securing cybersecurity investments is recommended
  7. The NIS directive boosts cooperation between Member States for cybersecurity, but the EU should go further following USA NERC example, organizing research of large-scale interdisciplinary attack scenarios, following the motto “Obscurity is not equal to security”
  8. Knowledge databases are used to share, and access known vulnerabilities
  9. Regular trainings are key to make our critical infrastructure resilient against cyber-attacks
- Future challenges
  1. Society and energy users need awareness about cybersecurity in the energy use
  2. 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 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
  7. Bio- and nano-technologies will 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 for energy systems

With a horizon set on 2050, important innovation and research topics in different clusters were identified, that will need results in the next years. Acting on those topics now will close important research gaps with results needed, when creating policies, regulations, and directives to improve cybersecurity and resilience for the future.

3.2 INTRODUCTION TO CYBERSECURITY AND RESILIENCE

There are 250 million energy customers in the EU, a mix of households and a strong, process intensive industry, all relying on its critical power infrastructure. The goal of this task force on digital cybersecurity recommendations (resilience) is to estimate, where we will be in 2050, and what is needed regarding cybersecurity, so that customers equipped with smarter solutions, can rely on a resilient energy system.

Sectors like finance, health, energy, and transport are becoming increasingly dependent on Information Technology (IT). Increasing digitization and customer participation cause 86% of Europeans to believe that the risk of becoming a victim of cybercrime is increasing (pecial Eurobarometer 464a: Europeans, s.d.) and according to (Carpenter & Wyman, 20166), 60% of companies have never estimated the potential financial losses from a major cyber-attack. The European Commission has proposed a portfolio of wide-ranging concrete measures aiming at strengthening cybersecurity structures and capabilities, facing ever-increasing cybersecurity challenges[37]. Building on the Digital Energy System 4.0 document (Vingerhoets, , Chebbo, & Hatziargyriou, 2018) by ETP SmartGrids, the role of task force three on cybersecurity and resilience is to guide research, development, and innovation (RD&I) in the crosscutting issue of cybersecurity to support Europe’s energy transition. We do not create standards in this task force; we highlight existing or missing ones.

As experts contributing to the WGs, we do this on a voluntary basis, and no reimbursement of expenses is foreseen. We are motivated by our individual and institutions research interests but driven by the idea of achieving the global (apart from the USA) climate goals in spite of a growing economy, increasing electricity consumption, and rapid digitization and decentralization of infrastructure for a smart energy system. Our hope is that a renewable, digital power system can provide cybersecurity and resilience enough, for continuous electricity supply at a reasonable cost for everyone in Europe. We do focus on Europe, but we will mention global activities where appropriate.

3.2.1 BACKGROUND

Smart grids have been defined by the European Smart Grid Task Force (set up by the European Commission at the end of 2009) as “electricity networks that can efficiently integrate the behaviour and actions of all users connected to it - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply”.

In the U.S., based on the Energy Independence and Security Act (EISA), the National Institute of Standards and Technologies (NIST) published the Guidelines for Smart Grid Cybersecurity in 2010 (The Smart Grid Interoperability Panel Cyber Security Working Group, 2010) (revisioned 2014 (The Smart Grid Interoperability Panel and Smart Grid Cybersecurity Committee)), providing a starting point and a foundation for a framework for evaluating smart grid-related characteristics, security requirements, risks, and vulnerabilities, and assisting with mitigation. Adopted from (National Infrastructure Protection Plan | Homeland Security., 2018), the proposed components of the cybersecurity strategy were prevention, detection, response, and recovery – all still relevant today. This multiple hundreds of pages report created by hundreds of experts in their related fields is offering a logical reference model spanning open a network of various and different interfaces between actors, systems, and components of all things smart grid related. Interfaces are part of thorough lists of security requirement categories. The European Conceptual Model was an evolution of the NIST model also integrating Distributed Energy Resources, providing different stakeholders viewpoints,

[37] Cybersecurity State of the Union 2017 http://europa.eu/rapid/press-release_IP-17-3193_en.htm

resulting in a Smart Grid Architecture Model (SGAM) framework (Smart Grid Coordination Group, 2012). The SGAM allows a holistic view of documented smart grid use cases. One of these viewpoints is cybersecurity, which requires the right choice and the appropriate use of information security standards. This guidance was provided by the Smart Grid Information Security (SGIS) working group, also under the European Commission Smart Grid Mandate M/490 (Group, 2012). The SGIS working group created the SGIS Framework, a risk analysis method, enabling management to get a granular view of traceable risks and consequences of smart grid incidents, of SGAM mapped use cases (Gottschalk, Uslar, & Delfs).

Current developments on the power networks, such as digital communication between supplier and consumer, intelligent metering and monitoring systems, will allow smart grids to improve the control over electricity consumption and distribution substantially to the benefit of consumers, electricity suppliers, and grid operators. Moreover, not only advanced Information and Communication Technologies (ICT) are at the core of an effective smart grid implementation. Also, Industrial Control Systems (ICS) and related Operational Technology (OT) need to be taken into account. All processes across the whole value chain are heavily based on these infrastructures and technologies. Smart grids give clear advantages and benefits to the whole of society, but a dependency on ICT components (e.g., computer networks, intelligent devices), ICS (e.g., supervisory control and data acquisition systems, distributed control system), OT (e.g., firmware, operating systems) and the internet makes our society more vulnerable to malicious attacks with potentially devastating results on smart grids. These undesired negative outcomes can happen in particular because vulnerabilities in smart grid-related communication networks and information systems may be misused for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants. The mentioned SGIS framework, for example, is an early mitigation tool to identify and visualize these risks pre-emptively. This position paper will describe the many more areas (called topics), which need similar tools, technologies, and concepts researched, to resiliently cope with the new ICT challenges in this cross-cutting issue: cybersecurity.

3.2.2 DIFFERENTIATION TO PARALLEL ACTIVITIES

ETIP-SNET Working Group 4 (WG4) addresses the use and impact of the Information and Communication Technologies as a pervasive tool along the entire value chain of the power generation, transportation, and use. The communication layer is one of the pillars of the smart energy system, enabling system observability, monitoring, control, and protection, explicitly enabling a radical change in the relation between the final user and the energy system. New digital tools (i.e., from smart meters to social networks) linked to the Internet of Things will aim to favour customer participation in all stages of the development and expansion of the energy system thanks to the analysis of big data generated. The widespread use of digital technologies, however, needs to be accompanied by suitable measures for data and information protection from malicious intrusions and attacks (cybersecurity) and uncontrolled use of customers data (data privacy). Within this framework, cybersecurity is an essential requirement to allow the final objective of a highly digitalized energy system which will be able to deliver the needs of European citizens in a reliable and fully participative manner. In particular, WG4 follows on:

- The full digitalization of both the transmission and the distribution networks with new ICT infrastructures cybersecurity-issues linked to using of big data, IoT, and high-performance computing;
- ICT infrastructures and technologies that will allow the involvement of the end customers and the retail market players;
- The retail electricity markets empowering customers (favourable environment to choose electricity suppliers and to better control consumptions through modern services provided by new market players);

- The improvement of public awareness of long-term energy challenges and the need to build and protect transmission infrastructure to increase the social benefit of energy use.

In contrast to ETIP-SNET WG4 supporting the ETIP-SNET Governing Board with recommendations for the near to midterm future, the task of the Energy Expert Cyber Security Platform (EECSP) is to directly assist the European Commission (EC) in the preparation of the next legislative proposals and policy initiatives. The mission of the EECSP-Expert Group is to guide the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies, and nuclear. According to the latest EECSP Report [1], there are two high-level concerns regarding the cybersecurity in the energy sector:

- secure energy systems that are providing essential services to the EU society, and
- protect the data in the energy systems and the privacy of the European citizen.

To resolve the concerns, four strategic priorities are set:

1. Set-up an effective threat and risk management system,
2. set-up an effective cyber response framework,
3. continuously improve cyber resilience, and
4. build-up the required capacity and competencies.

The criteria to evaluate the gaps in security in the EU are summarized into:

1. The importance of the European society and potential economic impact,
2. potential national or cross-border implications related to the ‘weakest link problem’,
3. prospects of a respective level to address the challenges, and
4. real-time and dependence on availability requirements.

Also, in cybersecurity, the three common protection goals are defined: Confidentiality, Integrity, and Availability (CIA). The main sources of security gaps based on the view of the expert energy group are:

- The very vague definition of responsibilities within the three interconnected levels of EU: Operator, nation-state, EU.
- The dependence of third-party countries outside EU that are interconnected to the Energy network and the need to unify the frameworks.
- The fact that no objective criteria, methods, and guidelines are given to neither Member States nor European institutions/organizations; a coordination is inexistent.

The more sensitive subsectors of the energy sector, security-wise, are electric and nuclear since they are real-time dependent. The challenges in the electricity sector in relation to the identified strategic areas are presented in (European Commission) (p. 32, table). The difficulties in the nuclear industry in regarding the designated vital regions are shown in ([10], p. 34, table). The information about the gaps details in all the four strategic priorities are given in ([10], p. 59-63, tables 10-13) respectively. The recommended actions in EC level are proposed in ([10], p. 64-68).

The European Commission Smart Grid Task Force Expert Group 2 (SGTF EG2) on cybersecurity builds on this EECSP report in their latest interim report [11]. The EG2 agreed on Terms of Reference ([11], p. 24) which lead to derived objectives and critical areas to be addressed by a “network code on cybersecurity”. The identified key areas were matched to the previously presented EECSP strategic priorities and gaps, network code objectives derived and resulted in a detailed description of four critical areas for network code on cybersecurity after further analysis:

1. European Cybersecurity Maturity Framework
2. Supply Chain Management
3. European Early Warning System for Cyber Threats
4. Cross-Border and Cross-Organisational Risk Management

The intermediary report promises the preparation work for all those instruments to continue, with the goal of being ready for the network code on cybersecurity. The proposal of SGTF EG2 is to work jointly with T&D Europe, ENISA, ENTSO-E, and relevant stakeholders, also organizations not directly considered by the member states following the NIS Directive (Euroean Commission, 2016), e.g., on sharing energy-related security information or not having necessary CERT capabilities, since the network code will apply to all electricity distribution and transmission system operators equally.

All parallel activities have a secure and resilient smart energy network as their goal and can be visualized as interlocking approaches from different angles to create the necessary momentum and to have the required tools already developed at hand when they will be needed. To differentiate from very near term and concrete measures envisaged by SGTF EG2, the ETIP-SNET WG4 Task Force 3 experts in this report on cybersecurity and resilience (cyber-robustness) suggest near to midterm future relevant research topics up to 2050.

3.2.3 INCREASING CYBER-ATTACKS

While the malicious incidents against the energy sector up to 2010, the year of Stuxnet, was mainly caused by physical attacks or vandalism only, digitisation in the shape of Internet of Things (IoT) and early smart grid appliances do not just open opportunities for customer participation in the critical infrastructure smart grid but also for hackers.

Figure 39 summarizes a (non-extensive) timeline snapshot graphic of power grid infrastructure related cyber-attacks.

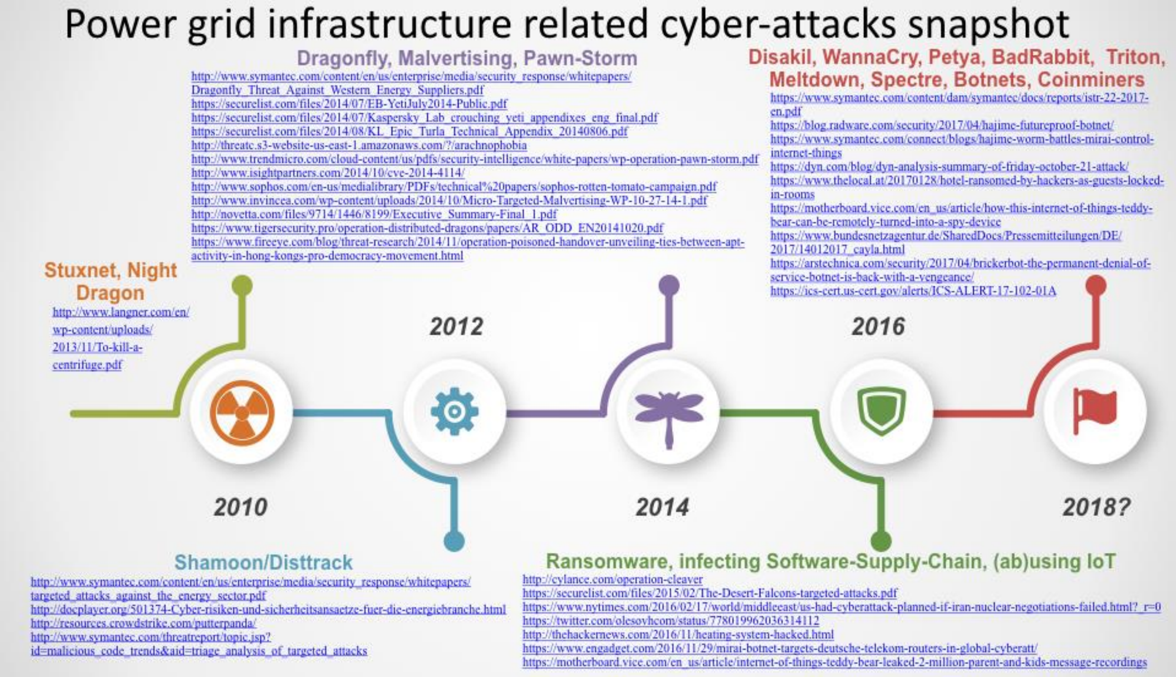

Power grid infrastructure related cyber-attacks snapshot
Dragonfly, Malvertising, Pawn-Storm
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf
https://securelist.com/files/2014/07/Kaspersky_Lab_crouching_yeti_appendixes_eng_final.pdf
https://securelist.com/files/2014/08/KL_Epic_Turla_Technical_Appendix_20140806.pdf
http://threatc.s3-website-us-east-1.amazonaws.com/?/arachnophobia
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
http://www.isightpartners.com/2014/10/cve-2014-4114/
http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-rotten-tomato-campaign.pdf
http://www.invincea.com/wp-content/uploads/2014/10/Micro-Targeted-Malvertising-WP-10-27-14-1.pdf
http://novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf
https://www.tigersecurity.pro/operation-distributed-dragons/papers/AR_ODD_EN20141020.pdf
https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
Disakil, WannaCry, Petya, BadRabbit, Triton, Meltdown, Spectre, Botnets, Coinminers
https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
https://blog.radware.com/security/2017/04/hajime-futureproof-botnet/
https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms
https://motherboard.vice.com/en_us/article/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device
https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html
https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
Stuxnet, Night Dragon
http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
2012
2016
2010
2014
2018?
Shamoon/Disttrack
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf
http://docplayer.org/501374-Cyber-risiken-und-sicherheitsansaetze-fuer-die-energiebranche.html
http://resources.crowdstrike.com/putterpanda/
http://www.symantec.com/threatreport/topic.jsp?id=malicious_code_trends&aid=triage_analysis_of_targeted_attacks
Ransomware, infecting Software-Supply-Chain, (ab)using IoT
http://cylance.com/operation-cleaver
https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf
https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?_r=0
https://twitter.com/olesovhcom/status/778019962036314112
http://thehackernews.com/2016/11/heating-system-hacked.html
https://www.engadget.com/2016/11/29/mirai-botnet-targets-deutsche-telekom-routers-in-global-cyberatt/
https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Figure 39: Power grid infrastructure related to cyber-attacks snapshot

The links cover news reports, security company alerts, and summaries, as well as blogs and dossiers of security researchers over the last years and can be found in the Appendix. It is especially noticeable that complexity of the attacks is rising as is the frequency, impact, and the caused damages. Three significant threat kinds/motivations can be identified:

A. **monetary/ransom**: Attacks can be internal (e.g., a disgruntled employee) or from external sources for financial gain or benefits. These are classical cybercriminals using, e.g., trojans, rootkits, keyloggers, phishing, spear-phishing, viruses, worms, botnets, crypto-lockers, e.g., Erebus, or crypto miners.

B. **fun/protest:** These range from single young persons (script kiddies) to large distributed groups, e.g. anonymous or other hacktivists that use cyber-attacks to make a point otherwise not being taken seriously, or not having a voice (whistle-blowers). They use DDoS attacks, redirections, leaks, firewall breaches, data-dumps.

C. **espionage/sabotage**: This includes cyberattacks paid for by a competing company, terrorist groups or a nation states, who try to gain market share, disrupt military or industrial operations, and cause large-scale destruction for political reasons. They use exfiltration for data or complete toolsets such as Night Dragon, Shamoon, Duqu, Prism, Stuxnet, the Dukes, Flamer, Dragonfly, Superfish, Nitro Zeus, Disakil.

Cyber weapons caused the most severe damages to critical infrastructure. All evidence is pointing towards nation states, or state-sponsored actors being their creators and sometimes deployers – unless a cyber warfare codebase “got loose” (WannaCry). Despite all evidence to this day, every involvement is being heavily denied. No actor so far admitted to the use of Stuxnet, Flamer, Prism, WannaCry, Nitro Zeus, or Petya. Nevertheless, there were reactions in countries affected most by Stuxnet, namely Iran, which has invested heavily into educating its students in cybersecurity. National pride is being the primary motivational source to join armed forces in this generation, to the point of becoming the world's top cybersecurity task force, securing their country.

3.3 MOTIVATION FOR FURTHER CYBERSECURITY RESEARCH

This section will provide a brief overview on the current cybersecurity-related work research and is a motivator to define future cybersecurity and resilience challenges (sharing, cost, openness, distributed risks, countermeasures, managing consequences, etc.) to be tackled and solved in the short and medium timeframe leading up to 2050.

3.3.1 EXAMPLE EXCERPT OF EUROPEAN CYBERSECURITY PROJECTS

A shift towards a low-carbon economy calls for increasing digitization of the energy system. As digital developments impact multiple aspects of European policies and its energy system, cybersecurity-related issues shall be taken into consideration in the Research and Innovation programs across Europe. The goal of this section is to summarize the state of development and attention given to cybersecurity aspects inside R&I projects that have been taken place in Europe. Particular attention is given to projects supported by Horizon 2020 programme from European Commission. The timeframe of the projects mentioned in the current section is presented in the following **Table 20.**

project	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
TCLOUDS	▒	▒	▒	▒							
PHYLAWS			█	█	█	█	█				
SPARKS					▒	▒	▒	▒			
ECOSSIAN					█	█	█	█			
ARGOS					▒	▒					

project	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
SEGRID					■	■	■	■			
PRECYSE			▒	▒	▒	▒					
CIPRNet				■	■	■	■	■			
C-DAX			▒	▒	▒	▒	▒				
SMARTIE				■	■	■	■				
SMART-NRG					▒	▒	▒	▒			
PDS4NRJ				■	■						
ELASSTIC				▒	▒	▒	▒				
RASEN			■	■	■	■					
RERUM				▒	▒	▒	▒				
AnyPLACE						■	■	■			
Flex4Grid						▒	▒	▒			
FLEXICIENCY						■	■	■	■	■	
NOBEL GRID						▒	▒	▒	▒		
Smartnet							■	■	■		
WiseGRID							▒	▒	▒	▒	▒
SUCCESS							■	■	■		
DEFENDER								▒	▒	▒	▒
SCOTT								■	■	■	■
InterFLEX								▒	▒	▒	

Table 20: Selected European Research Projects and their timing

The SPARKS[38] project provides innovative solutions in a number of ways, including approaches to risk assessment and reference architectures for secure smart grids. The technology development focuses on three core concepts required for smart grids: cyber-attack resilient control systems; real-time network monitoring of SCADA-based control systems; novel hardware security technologies for smart metering applications. Among the deliverables, the “Smart grid security and risk assessment”, “Security Architectures, Guidance and Standards for the Smart Grid” and “Smart grid security and resilience technologies” have relevant outcomes for cybersecurity applied to smart grids.

[38] SPARKS: http://www.sparksproject.eu/

In ECOSSIAN[39] project, a prototype system was developed which facilitates preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management.

The ARGOS[40] project studied how critical gas and electricity infrastructures can anticipate any threat with the view of avoiding potential disruptions. The capacity to monitor, deter and respond to potential threats was enhanced.

SEGRID[41] project performed a risk management analysis to some smart grid use cases, defining security requirements and determined gaps in technologies, standards and regulations. In PRECYSE[42], it was defined, developed and validated a methodology, an architecture and a set of technologies and tools to improve security, reliability and resilience of ICT systems supporting critical infrastructures.

CIPRNet[43] built a long-lasting virtual centre of shared and integrated knowledge and expertise in critical infrastructure protection. This centre made the use of this protection possible and related knowledge, expertise, and resources in a joint force against cyber-attacks.

Cyber-secure Data and Control Cloud for Power Grids, C-DAX[44] exploited the properties of novel architectures that are by design more secure, resilient, scalable and flexible than conventional information systems. These architectures aimed, among other aspects, the secure, synchronized and timely delivery of measurement and control data and a resilient cyber-secure layer to currently used protocols in the electrical grids infrastructure.

Other projects contributed for studies and improvement of secure personal data management and the resilience of critical information systems: PDS4NRJ[45], ELASSTIC[46,] RASEN[47], RERUM[48].

The SMARTIE[49] project studied the secure exchange of data between IoT devices and consumers of their information within the context of Smart Cities. Results were demonstrated in smart cities in Germany, Serbia and Spain. SMART-NRG50 project proposed a new protocol stack integrating security protocols for optimization for smart metering and analysed the design and the optimization of advanced security and privacy mechanisms for large-scale networks.

The AnyPLACE[51] project developed a modular energy management system capable of monitoring and controlling local devices according to the preferences of consumers. It is currently in test phase in Germany and Portugal. The developed central unit uses a cybersecurity module.

The Flex4Grid[52] project aims at creating an open data and service framework that enables a novel concept of prosumer flexibility management. The project tackles the cybersecurity and

[39] ECOSSIAN: http://ecossian.eu/
[40] ARGOS: http://argosfp7project.blogspot.pt/
[41] SEGRID: https://segrid.eu/
[42] PRECYSE: http://precyse.eu/
[43] CIPRNet: https://www.ciprnet.eu/home.html
[44] C-DAX : https://www.cordis.europa.eu/project/rcn/106390_en.html
[45] PDS4NRJ: https://cordis.europa.eu/project/rcn/109640_en.html
[46] ELASSTIC: http://www.elasstic.eu/
[47] RASEN: http://www.rasenproject.eu/
[48] RERUM: https://ict-rerum.eu/
[49] SMARTIE: http://www.smartie-project.eu/
[50] SMART-NRG: http://www.smart-nrg.net/
[51] AnyPLACE: http://www.anyplace2020.org/
[52] Flex4Grid: https://www.flex4grid.eu/

privacy issues from two viewpoints. The first is organizational and related to procedures that enable security and privacy provisioning. The second are mechanisms and services and their implementation, where classical security services are touched, from authentication, to confidentiality, to access control.

FLEXICIENCY[53] project is addressing cybersecurity and data privacy issues, to its demonstrations of demand response, flexibility, and energy efficiency based on metering data. The project addresses a flexible smart metering architecture, based on cheap and already available components.

In NOBEL GRID[54] project cybersecurity is being carefully addressed, considering firewalls and content filters acting as a RBAC (Role Based Access Control) system. It also considers physical protection for cybersecurity.

SMARTNET[55] project proposes new practical solutions to the increasing integration of Renewable Energy Sources in the existing electricity transmission networks. It considers the risk management process from the SPARK project. The project summarizes EU level ICT requirements for smart grids looking at communication, information, security and component aspects. In the deliverable 3.1 of the project, security related standards are reviewed: IEC 62351-3 (that provides security for any profile that includes TCP/IP), security for IEC 61850 including IEC 62351-6, ITU-T X.500, all parts of IEC 62351 and also ISO/IEC 27019 TR.

Communications related standards are extensibility studied, so that a state-of-the-art communication architecture is applied to project demos.

WiseGRID[56] is working towards a set of solutions and technologies to increase the smartness, stability and security of an open European energy grid.

SUCCESS[57] project is providing concrete guidelines to support the design of energy systems and linked communications networks, including specifications of secure communication solutions complemented by data privacy studies to ensure the acceptability of the results by consumers. Demos are running in Ireland, Italy and Romania.

DEFENDER[58] project is modelling Critical Energy Infrastructures (CEI) as distributed Cyber-Physical Systems for managing the potential reciprocal effects of cyber and physical threats, deploying a novel security governance model, leveraging life cycle assessment for cost-effective security management over the time, addressing: (i) a combination of range of devices/technologies for situational awareness; (ii) intelligent processing for cyber-physical threat detection with (iii) a toolbox for incident mitigation and emergency response and (iv) Human-In-The-Loop for managing people interaction with CEI, while leveraging on blockchain technology for peer-to-peer trustworthiness.

SCOTT[59] is a project with 57 partners from 12 countries that is addressing Internet of Things ensuring safety and security, privacy and trustworthiness / reliability

[53] FLEXICIENCY: http://www.flexiciency-h2020.eu/
[54] NOBEL GRID: http://nobelgrid.eu/
[55] SMARTNET: http://smartnet-project.eu/
[56] WiseGRID: https://www.wisegrid.eu/
[57] SUCCESS: http://www.success-h2020.eu/
[58] DEFENDER: http://defender-project.eu/
[59] SCOTT: https://scottproject.eu/

PHYLAWS[60] project addressed the enhancement of privacy at the radio interface of wireless networks Physical Layer Security and Secrecy Coding in Realistic Test cases using Wi-Fi and LTE.

TCLOUDS[61] project addressed the architecture and prototypes for a federation of trustworthy infrastructure clouds that build on complementary and mutually reinforcing technical approaches.

InterFLEX[62] investigates the INTERactions between FLEXibilities provided by energy market players and the distribution grid, with a particular focus on energy storage, smart charging of electric vehicles, demand response, islanding, grid automation and the integration of different energy carriers (gas, heat, electricity).

All projects named above did or do contribute to cybersecurity with their research activity, however, in most projects the main focus is on decarbonisation and smart grids. So cyber security is not considered "by design", as it should be considered nowadays for staying safe, secure and resilient. Therefore, it will be 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 special needs of the specific application or the energy system in general. The following paragraph will elaborate on these special requirements of energy systems and in the subsequent parts of this document. The recommendations for research activities are discussed in topic clusters.

3.3.2 OPERATIONAL TECHNOLOGY CYBERSECURITY VS. INFORMATION TECHNOLOGY CYBERSECURITY

The world of traditional Information Technology (IT) has morphed greatly over the years into non-traditional areas, such as supporting electricity management and control systems. This evolution has given rise to the need of cybersecurity within Operational Technology (OT). The OT role focuses on the process controls required to manage the operations side of the business. The differences between OT and IT can be confusing for those on either side when it comes to the specific roles each competency plays, but both types of security are necessary to ensure the protection of our critical infrastructure.

The main principles behind a cyber-secure system can be defined using the CIA triad according to ISO/IEC 27001. CIA stands for confidentiality, integrity and availability.

- **Confidentiality**: Protect data from unauthorized access or disclosure.
- **Integrity**: Protect the consistency of information ensuring the actual data is authentic, was sent, and that correctly.
- **Availability**: Ensure that the data and systems are available, and that downtime is avoided or minimized.

In the IT world, the priority for these concepts is typically CIA, while in the OT world the priority is normally inverted as AIC. For example, take the case of a financial company. In the event of a cyber incident, it may be a normal practice to place their system offline to protect the confidentiality of their customers' data, whereas an electric utility would almost never consider taking their protection and control system offline. Doing so could potentially cause unsafe conditions for their personnel or leave a section of the grid in an outage condition.

High reliability and uptime is one of the key principles of an OT system. All security measures and maintenance practices are designed around maintaining this. Secondly, performance and reaction time are also very important. In the electrical grid, the time required to react needs to be in the range of tens of milliseconds. Lastly, OT systems use control methodologies and

[60] PHYLAWS: http://www.phylaws-ict.org/
[61] TCLOUDS: https://www.tclouds-project.eu
[62] INTERFLEX: http://interflex-h2020.com

specialized protocols such as IEC 61850, which require specific domain expertise to both configure and secure. Some other key differences between IT and OT are shown in **Table 21**: Comparison between IT and OT (Source: T&D Europe).

	Information Technology (IT)	**Operational Technology (OT)**
Purpose	Transaction Systems; business systems, information systems, IT security standards, Office IT aspects	Control Systems; control or monitor physical processes or equipment, OT security standards, OT Data Services and applications
Architecture	Enterprise wide infrastructure and applications	Geographically distributed, event-driven, real-time, industrial/ruggedized hardware/software
Interfaces	Personal Computers, Mobile devices	SCADA, protection relays, RTUs, HMIs, switchgear
Ownership	CIO, finance and administration departments, IT managers	COO, electrical engineers, technicians, operators, and operations managers
Connectivity	Corporate network, Internet, IP-based	Control networks, hard-wired twisted pair, fibre optic and IP-based
Responsibilit y	Keeps the enterprise running and protects company assets	Keeps the lights on, protects operational assets and ensures safety

Table 21: Comparison between IT and OT (Source: T&D Europe)

3.3.3 CYBERATTACKS IN INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems (ICS) combine cyber- and physical layers (IT and OT) in order to perform a set of tasks within industrial environments. The latter can be composed of critical infrastructures as energy production and distribution (electricity, water, gas etc.). ICS are organized through a common architecture based on three hierarchical layers according to the processing capacity and decision-making power level. These layers are: the sensor/actuator layer that form the physical layer, the control layer composed of Human Machine Interfaces (HMI) and Programmable Logic Controller (PLC), and the supervision layer integrating the control room. In addition to these three layers, there are the communication networks that connect them together using analog/discrete input/output (I/O) or propriety protocols TCP/IP.
ICS are vulnerable to cyberattacks because as previously explained (AIC vs. CIA), they are designed to solve issues of production and safety without taking into account security issues. These attacks can take different forms according to the affected layer as alteration of control flow by attacking the PLC in the supervision layer or communication removal between two layers impacting in both cases the IPS' availability, or spoofing data coming from sensors or orders sent to actuators impacting their integrity.

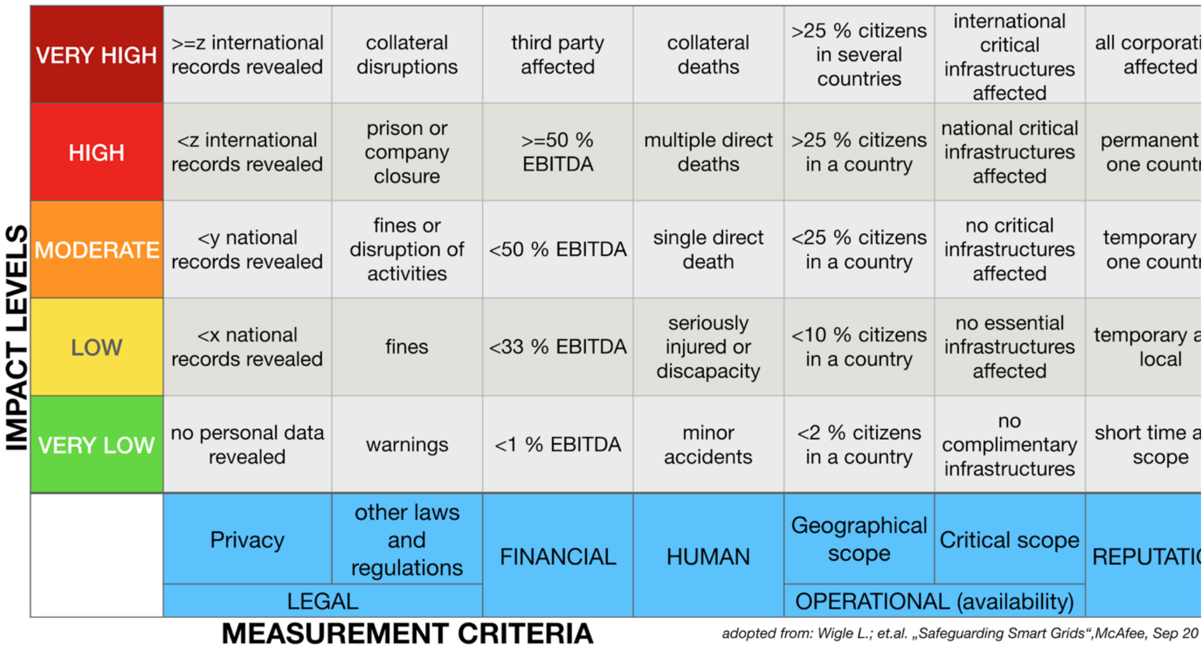
ICS as an Operational Technology (OT) have specificities and constraints that make difficult the use of classical security solutions used in Information Technology (IT). Indeed, ICS have strong real-time constraints, limited resources (memory), heterogeneous protocols and communication technologies, continuous production, and infrequent updates. Therefore, it is important to develop adapted solutions that take into account these aforementioned specificities and constraints in order to improve the security of ICS against cyberattacks. These solutions must generate models able to 1) verify the consistency of each layer output (control commands, sensor outputs, SCADA/reports, etc.) according to the current functioning conditions, 2) determine online the prohibited or dangerous functioning modes (conditions) by observing the sequences (actions/sensor outputs etc.), 3) communicate using an independent and secured network in order to limit the cyberattack size, 4) operate in non-intrusive manner without the need to install new probes in the production system, 5) adapt online their inference engine to new cyberattacks (new prohibited and dangerous modes), and 6) operate in decentralized decision structure in order to be consistent with the ICS distributed nature and to limit the computation complexity. These objectives can be fulfilled by combining approaches and technologies from interdisciplinary domains, ranging from analytical/physical model-based communities through Artificial Intelligence communities.

3.3.4 RISK ASSESSMENT

Growing connectivity and digitisation creates a rapidly increasing amount of assets to protect from cybersecurity threats. To identify which assets to secure first in the energy system one can split these into three layers:

- Hardware: infrastructure (power grid, power plants, transformer stations, fibre networks, radio stations), systems (OT control centres, IT information centres, telecommunication systems, back office), combinations (ICS), and services (emergency response, trading, financial, maintenance);
- Software: virtual machines, applications, sessions, protocols, algorithms, patching security holes;
- Data: private data, metadata of individuals, companies, and government, financial or health records, usage patterns, identities, certificates, keys, codes, and passwords.

Assuming a vulnerability – a security hole of any kind –, the combination of motivation and asset owned, creates a threat vector. Different threat vectors may have different impact levels, but to assign a single impact level for a single threat vector is not complex enough in our interconnected city- and infrastructure-depending societies. A multitude of measurement criteria are used to cover basic social and environmental risks (likelihoods), hence, impacts e.g., Earnings Before Interest, Taxes, Depreciation and Amortization (EBITDA) of cybersecurity on a scenario to analyse (see Table 22: Correlation of impact levels and measurement criteria in an analysis scenario).



IMPACT LEVELS

VERY HIGH	>=z international records revealed	collateral disruptions	third party affected	collateral deaths	>25 % citizens in several countries	international critical infrastructures affected	all corporati affected
HIGH	<z international records revealed	prison or company closure	>=50 % EBITDA	multiple direct deaths	>25 % citizens in a country	national critical infrastructures affected	permanent one countr
MODERATE	<y national records revealed	fines or disruption of activities	<50 % EBITDA	single direct death	<25 % citizens in a country	no critical infrastructures affected	temporary one countr
LOW	<x national records revealed	fines	<33 % EBITDA	seriously injured or discapacity	<10 % citizens in a country	no essential infrastructures affected	temporary a local
VERY LOW	no personal data revealed	warnings	<1 % EBITDA	minor accidents	<2 % citizens in a country	no complimentary infrastructures	short time a scope
	Privacy	other laws and regulations	FINANCIAL	HUMAN	Geographical scope	Critical scope	REPUTATI
	LEGAL				OPERATIONAL (availability)		

MEASUREMENT CRITERIA

adopted from: Wigle L.; et.al. „Safeguarding Smart Grids",McAfee, Sep 20

Table 22: Correlation of impact levels and measurement criteria in an analysis scenario

For example, it is quite important to perform a detail risks analysis for the system or systems to be secured and even keep it updated during their life so as to reassess whatever modification has been introduced. This way, a ransom cryptolocker extortionist can infect a website hosting service providing company and receive a “very low” impact level for legal, human and critical scope criteria, but “high” in financial, geographical, and even “very high” in reputation. To extend the analysed scenario into one more dimension, if the cryptolocker issue affects the **availability** of the technology for different amount of seconds, hours, or weeks, the impact will be different. The assessment will also change with the **integrity** of the data or service (was it manipulated, is it authentic, was data lost, does not working any more), as well as with the status of **confidentiality** in terms of internal or external disclosure in all measurement criteria.

3.3.5 IDENTIFYING CLUSTERS, TOPICS, AND SCENARIOS

The steps described offer a risk-based methodology to analyse cybersecurity and resilience scenarios in a structured way:

1. Find threat motivations and assets using vulnerabilities.
2. Along identified threat vectors assess impact on measurement criteria in the energy systems of the future.

In this position paper we would like to take a step back and offer suggestions for research in three clusters to help identifying the relevant cybersecurity scenarios until 2050, before they become vulnerabilities. The goal is, to provide starting points of exploration, where to enhance funding research of cybersecurity topics for the European energy sector, to have a head-start on vulnerabilities and threat vectors in (unfortunately) possibly likely risk analysis scenarios.

We take an expert group-based approach, trying to represent the widest community of stakeholders, related to the cross section of information technology, smart energy systems, customer participation, and cyber-security. The topic descriptions are assembled into one or more scenario descriptions. Each scenario description should allow readers to identify near to mid-term future research goals necessary for preparing the European energy system to become more cybersecure and more resilient. The descriptions will be either general or on the basis of concrete examples, sometimes motivated by circumstances in practice. The goal of this document is for information purposes only, to spark ideas for research goals, not to suggest further ranking, immediacy, state-of-the art, or importance by the order of suggested topics. The list of topics is not complete and needs to be adapted from time to time with technological developments, as well as societal changes to stay relevant.

3.4 FUTURE CYBERSECURITY AND RESILIENCE CHALLENGES

Future relevant cybersecurity and resilience issues were identified by members of the Working Group 4 task force on cybersecurity over the course of 2017/18. All issues will need collaborative, participatory, and transparent research and development to solve them or to find a way around them ((Gassmann & Sutter, 2016) p.135-145). To provide insights into future challenges for the public, these issues were prioritized, timelined, and clustered with the vision of a secure 2050 energy system in mind. For each paragraph in each cluster one or more short scenario descriptions were presented, to help readers envision the broad cross cutting research topics.

3.4.1 CLUSTER: TECHNOLOGY

The topics of this cluster are already relevant or are expected to be relevant in a near-term time frame. The topics are either technology related topics in need for cybersecurity research or can be used for solving cybersecurity and resilience challenges.

3.4.1.1 T1 ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is a large area. Originally defined by Alan Turing in the 1940s, Artificial Intelligence refers to a branch of computer science that aims to develop intelligent systems that work and react like humans. Nowadays, AI is made up of different core elements including machine learning, deep learning and cognitive systems. It is a multifaceted subject touching many aspects of our lives. In a cybersecurity context, AI can be defined as a set of intelligent technologies that perceive their environment well enough to identify threats and take action against them. For instance, it could be used to detect intrusions in network traffic or log files.

Machine learning is an application of AI using algorithms able to receive input data and use statistical analysis to predict an output value, assess if it is in an acceptable range and trigger if the value is considered out of range. It provides systems with the ability to automatically learn and improve from experience without being explicitly programmed. It can be used as a tool to predict outcomes based on past events.

Deep learning, a subset of machine learning, is modelled on artificial neural networks inspired by the workings of the human brain. These networks are capable of learning unsupervised from data that is unstructured or unlabelled. Advancements in processing power and cloud computing brought the possibility to build large neural networks able to learn from massive data sets.

Finally, cognitive systems are another key element of AI that simulate the human thought process using an automated model. These self-learning systems are built using machine learning foundations that perform data mining, pattern recognition and natural language processing.

Artificial intelligence offers new possibilities to improve cycles in the cybersecurity field. It automates tasks and thus speeds up the process of noticing and responding to cyber-attacks. Combined with the expertise of security analysts, the technology will allow organisations to develop predictive measures to protect them from malicious attacks. Unfortunately, AI is also seen as a powerful tool for bad hackers that enables them to build cyber-attacks more efficiently. Ironically, cybersecurity systems based on artificial intelligence technology are and will be, for many experts, best able to defend against "AI-enabled hacking" (Yampolskiy, 2017).

Organisations have begun to incorporate AI into their broader cybersecurity strategy to both detect threats and respond to them. Watson, a computer system developed by IBM, which combines artificial intelligence and sophisticated analytical software, is considered as the first cognitive solution for cybersecurity; it augments an analyst's ability to identify and understand sophisticated threats, by tapping into unstructured data and correlating it with local security offenses (Corbin, 2017).

Artificial intelligence will also allow the cybersecurity industry to tackle one major challenge: there are not nearly enough cybersecurity analysts to identify threats and resolve exploits quickly. The field faces a growing skills gap. By 2020, the number of unfilled cybersecurity positions is expected to reach around 1.5 million [(Booz, Allen, & Hamilton, 2017). The tedious and time-consuming tasks of threat research could be delegated to AI systems, allowing trained human operators to focus on the most difficult tasks.

The research and innovation on the use of AI applied to cybersecurity on energy systems – SCADA, smart meters supervision, energy market places, etc. clearly will lead to increased effectiveness and reaction speed of an energy systems security and could represent a part of the solution to adapt to a changing existing and future cybersecurity risk environment.

Takeaway messages:

- T1.1: AI will help cybersecurity industry to efficiently monitor, identify and understand sophisticated threats, including threats that will themselves be based on AI tools.
- T1.2: AI will be more and more necessary as unfilled security positions and skills gap will be growing during the next years.

3.4.1.2 T2 AUTHENTICATION

Smart grid is an evolving new power system framework with ICT driven power equipment structure and therefore is open to cyberattacks. The importance of reliable energy grid infrastructure demands for an increased level of cybersecurity. As already mentioned, the high-level security objectives for protecting the smart grid are: Confidentiality, Integrity, and Availability (Pandey & Misra, 2016). To be successful on all the above objectives, the communication technologies must be secure, since any failure to the secure transport of the information in the smart grid systems can lead to critical failure in each objective (Yan, Qian, & Sharif, 2012).

A modern technology which could simultaneously solve the problems of authentication and authorization in smart grids is the blockchain technology. Blockchain is a secure and decentralized database technology that can guarantee, under specific circumstances and design, immutability, privacy (Zyskind, Nathan, & Pentland, 2015), authorization (Halpin & Piekarska, 2017), (smart contracts) and authentication (Emmadi & Narumanchi, 2017). By developing a specialized solution for smart grids based on blockchain technology (Dorri, Kanhere, & Jurdak, 2016.).it is possible to address all the problems of cybersecurity in communication intrusion ((Xiao, 2013) p. 269-290) at once. Certainly, blockchain cannot solve all authentication challenges, but before, it seemed utopic for a system to guarantee authentication (Moinet & Darties, 2017) of the data produced by various components that are on the consumer side, that transfer data privately (Halpin & Piekarska, 2017), while forbidding the unauthorized alteration of data by 3rd parties (Emmadi & Narumanchi, 2017) and allow only authorized users (Luu, Chu, & Olickel, 2016) to send commands in the distribution and transmission system.

A wide spread development of immutability could also enable law enforcement or insurance companies to more heavily rely on the trail of electronic evidence. While applications in market systems are very likely, using blockchain in OT systems is difficult. Especially considering the integration of legacy systems, or possible caveats, such as the size of the data overhead and reliability issues in relation to the blockchain nodes. This is why more traditional authentication approaches should also be explored. Besides authentication, authorization is also an interesting question for smart grid systems, in which multiple parties are involved. Especially relevant is authentication and authorization in combination with foreseeable decentralization. The smart grid systems, which will become more open to different parties, will need authentication to span a multitude of different companies, and authorization to be much more fine-grained.

Takeaway messages:

- T2.1: Smart grids development will increase the need for IT components and for users to be strongly authenticated.
- T2.2: Blockchain is considered as a promising technology to address both authentication and authorization needs (see also: Blockchain).
- T2.3: Authentication across devices, companies, or countries borders and fine-grained authorization are foreseeable.

3.4.1.3 T3 VISION CYBERSECURITY CENTRALIZED VS. DISTRIBUTED

The Energy system is being and will remain digitally transformed. The intensive and massive use of digital technologies has started and will happen as its associated efficiency will justify investment either by itself or accompanying energy developments, as the ones referring to the adoption of Distributed Energy Resources (DER), mainly renewable generation of any size and location, storage and demand side management. The big change in transportation, with its clear result in electrification increase, will also heavily impact the energy system.

All of this requires a fundamental understanding, adoption and research of cybersecurity measures to achieve the adequate level of resilience and market effectiveness of the future energy system.

There are two main points of view for this future energy system which result in two different perspectives for every one of its characteristics and requirements, including cybersecurity. On the one side, the prosumers, inherently distributed, especially if taking into account any appliance or device connected to this side of the system. On the other, the view of the network which tends to start with a centralized approach and finalizes necessarily with a distributed one when it delivers the energy service to the user (MIT Energy Initiative, 2016).

The risk analysis which should be the central concept to keep in the design, implementation and operation of the cybersecurity, suggests that if the population of devices to maintain secure increases, a full centralization would increase the risk of being accepted. On the contrary, a decentralization (reverse current trends) with a well limited zone of impact would help to control the risk to be accepted.

However, the economies of scale associated with centralized solutions suggest that a fully distributed security would avoid achieving some efficiencies, impacting the economics of the overall solution. Distributed maintenance is in many cases incrementing OPEX (International Energy Agency, 2017).

Therefore, the proposed topic to research is the comparison of resulting efficiency, for achieving the same level of accepted risk, between centralized and distributed cybersecurity solutions. In all their parts: inherent security by design devices, software upgrades, supply chain agents (equipment suppliers, installers and maintenance responsible ones), authentication and validation, and overall system management, including the security control centers. Decentralized management seems very expensive nowadays but considering the advent of management capable bottom-up decision systems with distributed artificial intelligence solutions, with the right, forward thinking update and patch concepts as background (IETF), these management capabilities could be made cost effective through new systems on chip.

As the measure of efficiency and risk should request heuristic basis, the analysis of the alternatives with the support of demonstrations with enough size to grant scalability and replicability is recommended. The use of existing systems as the Smart metering already deployed in almost all European countries would be a suggested starting point of research, to build up recommendations and tracks to follow with other parts of the energy system.

Takeaway messages:

- T3.1: Digitisation enables future distributed, decentralized energy and IT systems. However, the overall efficiency of decentralized systems has to be measured and compared with centralized solutions.
- T3.1: The scalability and replicability of decentralized energy and IT systems needs further investigation. Smart meter deployment may represent a relevant starting point for research.

3.4.1.4 T4 HUGE SENSOR DATABASES

New digitalization technologies, a growing pervasive telecommunication infrastructure, Internet of Things (IoT), current data retention policies, and cloud computing enable the application of sensors at places in the grid, which were not monitored so far. Additionally, sensor information from devices behind the electricity or gas meter, or even from other domains might become available uncategorized in data lakes or connected with semantic information, already prepared for energy management purposes. Inverters for batteries or photovoltaics may monitor the grid voltage and/or power quality and send this information via a remote service IT-connection (e.g.: OPC-UA) to a cloud service of the inverter manufacturer, who may use this information to create digital twins and offermachine learning powered maintenance predictions, or even provide this information to grid operators. Even car manufactures have started pilot projects to offer the sensor information for the IT-connected cars driving around as so called “mobile weather stations” to grid operators (TenneT, https://www.tennet.eu/de/unsere-kernaufgaben/innovationen/mobile-sensordaten)

We could grasp the size of the volume of the power grid sensor information by mentioning the sampling rate of 4000–12800 samples/sec of the IEC 61850-90-5 Synchronized phasor (synchrophasor) measurement unit (PMU). PMUs widely accepted by the power grid industry and such units are already being deployed at fast pace around the world. Such an increase of sensor information (Big Data) on the one hand side enables much more analytic applications to improve the operation of the energy supply system, on the other hand, new vulnerabilities might arise either due cybersecurity issues or due to mutual dependencies between the energy supply and the IT systems. In connected systems, every actor can initiate communication. Relying on connectivity alone is not a sufficient security measure but demands for semantic interoperability and random offsets (to conquer attackers threshold parameter knowledge), coupled with communication security for control and data signals and granular access rights mechanisms ((Bubolz) p.128-130). A resilient system design of the energy system has to consider this by maximizing the IT security level on the one hand side, while ensuring that the communication of system critical information is secured even during a longer lasting blackout. Restoration plans have to make sure that the communication infrastructure is powered up, before it becomes required. As a conclusion, beside the research on analytical utilization of the increasing sensor data base, cybersecurity issues have also to be considered and mandated for corresponding research projects.

Takeaway messages:

- T4.1: Digitalization enables and relies on the massive deployment of sensors that improve analysis and monitoring capability. Data based systems will depend more from data availability (including communication networks). Cybersecurity should be investigated as specific topic in order make sure that systems remain resilient to attacks.
- T4.2: IoT enabled devices will help to make the energy system more transparent and allow more efficient operation by means of data analytics.
- T4.3: A critical infrastructure like the energy grid still requires a reliable OT communication which might be complemented by IoT.

3.4.1.5 T5 CLOUD COMPUTING

As already mentioned in T4 “Huge Sensor Databases”, cloud technology may facilitate the combination of much more data for various sources to derive knowledge about the performance of the energy system, unlock information, and detect optimization potential. However, certain applications, like the protection of grid assets against damages due to electrical failures, still need to be executed on premise, i.e., in the substation. But the (geographical) fault localization, as input for the repair crew, might be predicted in the cloud. Consequently, the decomposition of current grid automation solutions into functions and the determination whether these functions are cloud compatible or not, is an important research topic. The evaluation of future OT/IT architectures for grid automation by research and demonstration projects will help to avoid inefficiencies in this regard on the one hand and support interoperability between new and legacy technologies and therefore reduce the risk of stranded investments into grid automation technologies on the other. An interesting use case to consider in research is to take automated switching decisions based on cloud data. One can easily imagine, that along the way, the cloud computing systems have more data (data lakes), and hence, a better view on the grid than a single supervisory control and data acquisition (SCADA) system. So new data analysis algorithms could be used for optimizing e.g., electricity flow. It also needs to be said, that cybersecurity in such a centralized approach has to be evaluated at a very severe impact level, since a hack of the cloud system may cause wide area blackouts.

Research in this direction also needs to investigate what are the risks, mitigation strategies, and recovery scenarios.

Due to its scale, an equally important topic to be considered in this regard is data privacy as an additional separate issue to that of data analysis or mining or attack detection. Aggregation of raw data might help to assure data privacy for an individual person, but on the other hand, this might reduce or even eliminate the information value of the data for grid operation purposes. Hence, research projects might focus on defining the right trade-off between data privacy and information demand for grid operation purposes. This might even become a dynamic process, which allows more detailed insights into the data, dependent how endangered the secure operation of the energy system is. Another approach includes techniques toward making the issue irrelevant by making well encrypted data aspects queryable (Wen, Lu, & Liang, 2014) The technology readiness level of techniques such as order-preserving encryption, searchable encryption, bilinear pairing, Public-key Encryption with conjunctive keyword search, Hidden Vector Encryption based query predicates, and special data structure traversal needs to be increased stepwise, up to a deployable architecture component. With necessary research on efficient encryption and decryption algorithms, new indexing technologies for encrypted data, and scaling manageability of analysing large amounts of it, this can allow necessary markets, auctions, or audits of the data and still meet future, very stringent data privacy laws.

Takeaway messages:

- T5.1: The future OT/IT architecture for grid automation raises the question of on-premise or cloud-based calculation. It should be further investigated from a cybersecurity perspective [see also: centralised vs distributed, huge sensor data base].
- T5.2: The trade-off between raw individual data or aggregated / protected data may be found through new encryption/decryption and indexing technologies, to further explore.
- T5.3: Grid optimization applications are suitable to be deployed in a cloud environment; however, safety or security relevant grid control function still requires a decentralized deployment, close to the grid assets.
- T5.4: The demands coming from data analytics and data privacy have to be considered in a way, that both the derived information value for grid operation and the data security level is maximized.

3.4.1.6 T6 SAFETY INTERSECTING SECURITY

Safety nowadays is not concerned with cybersecurity because the malicious causing of accidents is not considered a safety issue during certification. It defines a scenario of normal operation (e.g., components in line of sight) under which all safety relevant functions will work and be certified. It argues that malicious intent, such as putting a car bomb into a car, will still explode the car, and there is nothing car manufacturers can do about it. Since cyber-attacks are also malicious, it is also not a concern. The intersection of Industry 4.0 with operational technology (OT) vendors and Internet of Things (IoT) everywhere, especially also at the customer site might change the perception of safety relevant devices from pure OT towards expectations in IT. There needs to be a difference established related to cybersecurity, abusing components already present and built into the smart grids, to command and control their functions. Of course, safety features overrule security functions, but there is no safety without considering cybersecurity of highly networked components. In industry IEC

62443 is being used as standard and in future, devices and machines are going to be certified towards this. The requirements are comparable to safety from IEC 61508, but extended with security aspects. How much regulation can help companies justifying cybersecurity spending to their shareholders and how much existing certification can cover these issues needs to be analysed – a first step could be, to include cybersecurity in certification processes for digital devices, especially if they are networked.

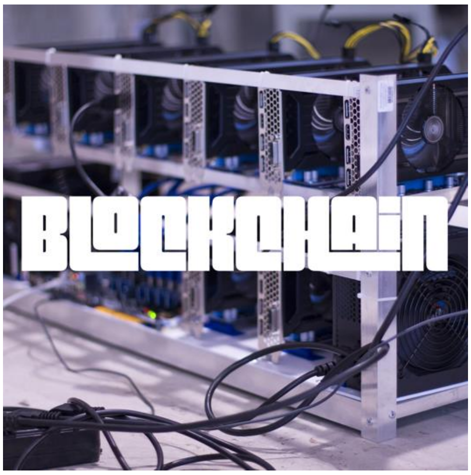
There needs to be research on the modularization of reusable components and technologies, that allow (re-)certification after unavoidable security firmware updates during years of operation. Rolling up the interconnection from the other side, new technologies e.g.: blockchain, can make information public that was background process information before. Safety relevant implications on internal state information need to be addressed and researched.

Noticing safety problems ahead of time, through more research in the area of pre-simulation of control systems, or predictive analytics of digital twins virtually representing different components, devices, systems, or systems-of-systems can also be part of a tighter integration of interdisciplinary efforts in reactive security strategies, trying to detect unwanted changes in production environments. There is generally a need for tool-support in modelling present architectures according to SGAM levels, describing devices and information, their connections and resulting security and safety implications in an extendable, maintainable way, as model-based, interoperable assets. This allows integration of new smart grid applications already inside existing use case models (Gottschalk, Uslar, & Delfs), therefore enabling early assessment of changes to current business. Establishing the toolchain as part of a safety and cybersecurity certification process, could allow sharing of generalized requirements, comparable to common criteria catalogues.

Takeaway messages:

- T6.1: for highly networked components, safety is not reachable without cybersecurity.

3.4.1.7 T7 BLOCKCHAIN



Blockchain has become one of the most disruptive technologies of the past decade. Since its debut in 2008 with the white paper of Satoshi Nakamoto (Nakamoto), this new technology has expanded past its initial use as the base of the first cryptocurrency, Bitcoin, into many other areas (PandaSecurity, 2017). This technology offers a totally new and innovative approach to storing information, making transactions, and performing functions on transaction content.

Blockchain could be defined as distributed and shared databases duplicated across a large network of computers. This technology is a continuously growing list of records made up of blocks which are recorded and added to it in chronological order. Users can submit new records for inclusion, but it will only be included in the database following the agreement of a majority of members. Blocks are secured through cryptography and designed to avoid any kind of modification or alteration afterwards. Once the records have been entered they cannot be removed or changed.

According to many experts, Blockchain technology has an inherent connection to cybersecurity as it concretizes the culmination of decades of research and breakthroughs in cryptography and security (Barzilay, 2017). Blockchain ensure data integrity by using a variety of consensus and messaging techniques. It helps encrypt all the actions performed with a file or object into the code that is inherent in the file. Encryption cannot be removed, altered or omitted. This technology is also completely transparent by design as it allows members to check the veracity of the transaction carried out, while also confirming who it comes from. Because of its decentralized and autonomous structure, a blockchain cannot be controlled by a single entity and has no single point of failure. However, there is a known “51 percent” vulnerability for small blockchains, if one entity takes control over a large percentage of the overall network mining power. It could then control the approval of transactions; based on the majority of miners.

The “almost” inviolability and decentralization of the blockchain could be suitable for environments with high security requirements and mutually unknown actors. Organisations from different sectors have begun applying this technology to prevent fraud and improve protection of information. Guardtime [63], a data security start-up, already operates blockchain systems to keep and protect sensitive records. In 2016, the company reported that it had secured all of Estonia's 1 million health records with this technology. This start-up is nowadays the world’s largest blockchain company by revenue, headcount, and actual customer deployments. Blockstack[64], a company which provides a fully decentralized option for DNS, has implemented the technology in this area to prevent distributed denial of service (DDoS) attacks from occurring. Obsidian, a messaging platform, uses the blockchain-decentralized network to secure information of users. Metadata are randomly distributed throughout a ledger and therefore are not available for gathering in one single point, from which it could then be hacked.

The blockchain is one of the most promising inventions of the past decade with direct cybersecurity application. Some issues still need to be investigated (e.g., 51% vulnerability) in order to confirm its robustness against malicious attacks. Immutability is an advantage of blockchains, but in face of errors and bugs in published smart contracts, there need to be versioning mitigation strategies. Immutability is also a disadvantage, thinking about the right to being forgotten, as stated in the GDPR – and since everyone can write onto the blockchain, no one can stop images of child-pornography being put into the data of the blockchain (Dockrill, 2018) and it being downloaded to every node either; new is the possibility of tracing it back to the perpetrators accounts; again driving home the need for authentication and identity management solutions.

Blockchains need to be further investigated in energy systems as a new technology that could better protect data and be used to certify metering measures, energy transactions, customer consent for data sharing, inherent accounting, consensus-driven location verification [65] and more. Nevertheless, current limitations such as slow transaction amounts (5/second), computation capacities of many complicated contracts, and high gas costs for frequent changes need to be improved. One of the first milestones to solve will be, how to connect identities on the blockchain, which will enable numerous applications affecting every vertical in all sectors, as diverse as voting in smart government, automated accounting services, up to recipes, IP, or prescriptions in medical industry – and of course the legal industry handling relationships of entities in smart contracts, written by lawyers on Ethereum (Wood, 2018) in solidity using openZeppelin and ConsenSys, or hyperledger[66], to name a few starting points.

Takeaway messages:

- T7.1: Blockchain technology offers a promising secure decentralized way to guarantee the veracity of various transactions, such as certifying metering measures, energy transactions, customer consents for data sharing, with regards to the energy sector.

[63] Guardtime: https://guardtime.com
[64] Blockstack https://blockstack.org/
[65] FOAM: https://foam.space
[66] The Linux Foundation Projects: Hyperledger https://www.hyperledger.org/

3.4.1.8 T8 PREDICTIVE ANALYTICS

The increasing fluctuations of wind and sun based renewable energy sources put high demands on prediction models to guarantee a reliable energy grid infrastructure. The faster pace also raises demands for increased levels of cybersecurity. The high-level security objectives AIC (Pandey & Misra, 2016) are the starting point for necessary prediction. To provide situational awareness and detect intrusion of the systems, there are three main types of data analysis systems that can be used: Misuse-based, anomaly-based, and hybrid (A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, 2016) Along all those types, there are three security concepts, differentiated by the time the attack is mitigated: prevention against attacks expected, detection of unexpected attacks happening (e.g., anomaly detection), and forensics of past attacks to learn from and to create more prevention. Potential future smart grid malware is developing strategies to conquer devices despite those concepts: e.g., encryption, modules, authentication, decreased aggressiveness, using unknown (zero-day) vulnerabilities, obfuscation (Eder-Neuhauser, Zseby, & Fabini, 2017), (Vormayr, Zseby, & Fabini, 2017).

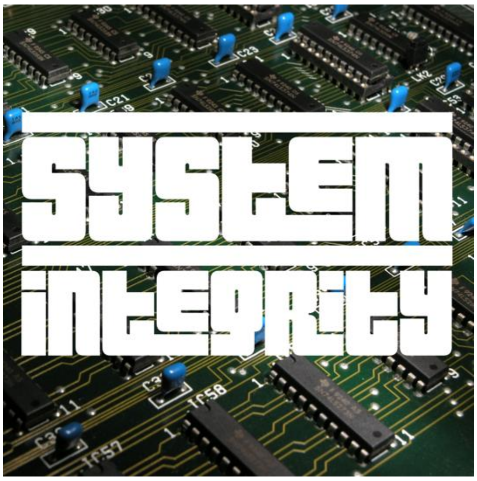
In recent years, the rapid increase of research results in the field of Machine Learning (ML) enables other research fields to benefit from it (Ozay & Esnaola, 2015). The usage of GPU-accelerated containers in cloud services and the development of tools such as TensorFlow [67], Torch [68], and Caffe2 [69] that can profit from this infrastructure, are revolutionizing all the industries in ways that before where not possible. Modern machine learning algorithms excel in pattern recognition, therefore find usage in either detecting specific signatures of attacks (misuse-based systems) or in identifying observations that do not conform to the expected patterns (anomaly detection) and enable the detection of zero-day attacks. The above render ML based systems ideal to detect all the types of intrusion-based attacks and evidence exist that their performance can be greater than algorithms based on statistical learning method (Tan & De, 2017)

Takeaway messages:

- T8.1: Machine learning enables predictive analytics; applied to cybersecurity it helps detecting specific attacks, identify patterns and enables the detection of zero-day attacks [see also: Artificial Intelligence]

[67] Tensor Flow: https://www.tensorflow.org
[68] Torch: http://torch.ch
[69] Caffe2: https://caffe2.ai

3.4.1.9 T9 SYSTEM INTEGRITY



Smart grids are composed of various monitoring and control devices that aim to increase efficiency and reliability in the grid, as well as providing new services for energy consumers. Such a setup will eventually contain critical devices that large parts of the grid will rely on and therefore have high demands on reliability and security. These systems will not be isolated however, they will be connected to various other, possibly less critical, components and will require a certain amount of trust towards these components (Farhangi, 2010). To ensure the reliability of these critical components, research efforts should be directed towards finding and evaluating appropriate methods to secure the correct functionality of these critical systems and their connected component, either via traditional quality ensure methods, or by new, unconventional means, like the hardware trojan detection (Krieg, Rathmair, & Schupfer, 2014).Furthermore, the security concept should be extended towards reactive methods to detect and mitigate malfunctions in a critical system, like the application of biologically inspired artificial immune systems (WANG, LIU, & WANG, 2006). To this end, formulating a general approach to securing critical devices in the smart grid's domain is still a fundamental question and requires research into the validity and applicability of the various existing approaches. The results of this work can then guide further research efforts in refining the available technologies for the use in the smart grids domain and finding new research fields for future interdisciplinary collaboration. As science and industry are already well on the way to develop components for such systems (Hutterer, Hauer, & Meindl), guidance regarding security in order to ensure a safe supply chain is in high demand. In conclusion, we argue that in order to ensure the safety in a smart grid environment we will need to ensure security on the device level. To do so, we will need to secure the supply chains of these devices and either extend this security to all participating components or find methods to deal with violations of the trust contracts between components. The first step on this road is fundamental research into the possible approaches we could take. The field of security and safety is vast and without evaluating its fundamentally different strategies, specifically for the smart grid's domain, we run the risk of ending with unsafe, underestimated components providing gateways to our otherwise highly secure and possibly also highly expensive, critical devices.

Takeaway messages:

- T9.1: System integrity relates to the behaviour of critical devices controlling the grid. 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.
- T9.2: One fundamental possible research track to ensure security of the supply chain is to build trust contracts between components and to control trust contracts violation.

3.4.2 CLUSTER: POLICY

The topics of this cluster are relevant already or are expected to be relevant in a near to mid-term time frame. The topics are policy and governance related topics in need for cybersecurity research or can be used for solving cybersecurity and resilience challenges. In contrast to the technology topics, the policy cluster sometimes does not try to offer solutions on specific directions on how to tackle the challenges since, in many cases, topics will need to be solved on a national level, or even on an organizational level, taking into consideration different cultures, perspectives, and living realities of different individuals.

3.4.2.1 P1 METRICS

The variety of digital threats is on a constant increase day by day. Crafting reliable countermeasures for a wide range of participants in the digital ecosystem (companies, governments, individuals) is a difficult task, especially when it comes to creating policies and recommendations that can be used by all parts of this digital ecosystem. The authors of the Twenty Critical Security Controls for Cyber Security (The CIS Critical Security Controls for Effective Cyber Defense, Center for Internet Security, 2018) address therefore a prioritisation on the first five controls covering for eliminating the vast majority of the organization's vulnerabilities. The remaining fifteen are targeted for today's most pervasive threats, bringing useable metrics and definitions for realization and future use. There is a research need for frameworks that are able to assist any decision making and facilitate the complex area of cybersecurity risks (Liu, Xing, & Wang, 2017). Due to the fact, that deployed software and operating systems grow not only in their number of functionalities, but also in size and complexity, where manual efforts are not enough in terms of scalability and complexity, environments with automated reasoning with a deployed artificial intelligence can assist the overall security and performance in terms of availability.

The authors of (Zheng, Y, & Hou, 2017) list a set of desirable characteristics that shall be considered in order to assess a benchmark performance for network robustness metrics, which can be transferred to other parts of a cyber-physical system. When following the approach by the authors of (Zhang, Wang, & Jajodia, 2016), network diversity can be a key to resilience against Zero-Day attacks (not against state sponsored attackers), with the stated drawback of high manual efforts, which shall be eliminated by decision support. An assessment of the system, creating a situational awareness of each individual branch of different organisations and departments with highly specific directions of threat-reduction can be beneficial.

Takeaway messages:

- P1.1: Metrics, frameworks, and automated tools should be developed and generalized to help and assist decision making in the complex area of cybersecurity risks.
- P1.2: To foster diversity and to avoid monocultures of components, devices, or operating systems increases cybersecurity (not against state sponsored attackers).

3.4.2.2 P2 EXISTING RELATED/BACKGROUND EFFORTS

A major part of the state of the art on cybersecurity research in Europe has been already discussed in the chapter entitled Example Excerpt of European Cybersecurity Research and elsewhere. Regardless of the interesting approaches considered, important efforts devoted, and the stellar consortia involved, it seems that the so far related actions are to a certain extent fragmented. Such fragmentation could be very well expected due the multifaceted nature of the cybersecurity issue. There has been little to no research on a meta level, looking at common findings, and outliers, to identify things that can be done better. There are already first evaluations, looking at general data of past projects[70] or an overview map[71] but research and meta studies could help speed up the process, especially through deduplication of comparing vertical results of different national projects. This can lead to surprising conclusions on the policy or governance level. Considering related work across sectors, such as the Alliance for Internet of Things Innovation (AIOTI) to name just one. The security in IoT is also a concern for smart grids with its expected tens of billions connected devices in the EU by 2020 (Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination FINAL REPORT).

To tackle this topic, there exist the following efforts, contributing to the missing meta-level analysis of the overall studies and outcomes. They lead by these three prominent EC organizations (see Figure 40) and their actions seem to complement each other.

Figure 40: EC organizations contributing to the missing meta-level analysis

In particular:

- The ECS[72] through its dedicated Working Group on “Sectoral demand” in general, and its segment “SWG3.2: Energy (oil, gas, electricity), and smart grids” in particular is focusing towards a true cybersecurity ecosystem, linking supply and demand.
- JRC hosts several energy security efforts. These include:
  - The Incident and Threat Information Sharing EU Centre - Open Source Intelligence for the Energy Sector[73]
  - The electricity supply security and resilience core activity, a layer within the European Smart Electricity Systems and Interoperability[74]

[70] Smart Cities info system: https://www.smartcities-infosystem.eu

[71] Map of Smart Grid Projects: http://ses.jrc.ec.europa.eu/project-maps

[72] ECS: https://www.ecs-org.eu/

[73] JRC ITIS: https://itis.jrc.ec.europa.eu

[74] JRC SES: http://ses.jrc.ec.europa.eu/

- ENISA focuses on several topics[75] with most of them related, at least to some extent, to this position paper. In particular, the subtopic smart grid is the most related one.

As mentioned the above have clear complementarity visions and objectives. As it is apparent (see for example the characteristics of the participating organizations) ECS is focusing much more towards the security industry rather than energy one. JRC has specific actions on cybersecurity issues of the energy sector, they are keen towards observation, assessment, awareness, policies, accidents, rather than cyber-security itself. We should mention here the excellent reports provided in general and the (Fulli, Masera, & Covrig, 2017) in particular. ENISA covers a wide range of topics related to our report in most appropriate ways. The reports found within the Smart Grid Subtopic are of highest quality, but unfortunately a bit outdated.

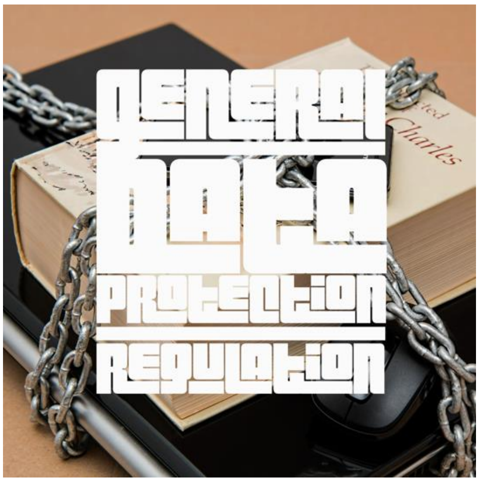
Takeaway messages:

- P2.1: Umbrella studies that unify the various visions mentioned above is needed. They will provide a holistic view that could lead to increase specificity. They will also clearly identify under-studied issues, misconceptions, and overloaded terms.
- P2.2: Stakeholders involved seem to still leave in isolated silos. There is a clear necessity of creating a clear communication platform for all of them and create a core group that the different industry sectors (IT, Transmission grid operators (TGO), distribution grid operators (DGO), Policy).
- P2.3: Privacy issues do not seem to be covered to the extent it demands so far (see also topics P3, P5 and P5 below).
- P2.4: Cybersecurity research at a meta level has been very limited so far and should be stimulated, to consolidate insights, results, knowledge and research needs which have been developed in Member States and through European collaboration projects.

3.4.2.3 P3 GDPR

Nowadays, digitization is transforming everything. The exponential evolution of technology has turned society highly dependent on it. The emerging new concept of, “Digital Transformation”, and it has become a primary goal for all companies. Concerning this, and in order to protect the individual subject in what concerns the treatment of personal data and the free circulation of it, the European Commission updated the so-called General Data Protection Regulation76 (GDPR), which was applied on the 25th of May 2018.

The GDPR has the objective to help Europe embrace the Digital Era, being an essential element of the Digital Single Market and of the European Union Agenda for Security. The main goal is to harmonize the level of data protection across the European Union (EU) thereby eliminating the existent regulatory fragmentation. It harmonizes the processing of personal data from data subjects residing in the Union, regardless of the location where the processing company is located, which is appreciable for the development of new data analytic solutions.



Additionally, the conditions for consent have been strengthened and the notification requirements on data breach have been increased. The new GDPR strengthens the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format and also the “right

[75] ENISA: https://www.enisa.europa.eu/topics
[76] GDPR Portal: https://www.eugdpr.org

to be forgotten" entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. GDPR introduces also data portability – the right for a data subject to receive the personal data concerning them, which they have previously provided in a "commonly used and machine-readable format" and have the right to transmit that data to another controller.

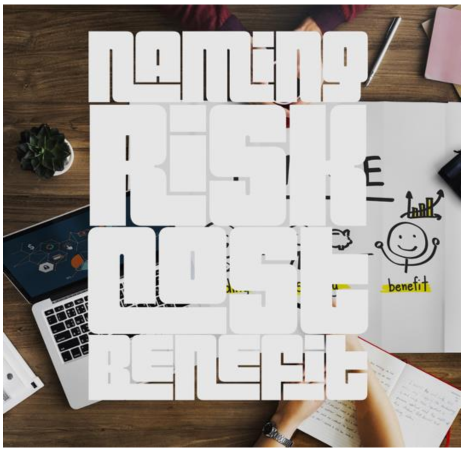
With the GDPR companies will have to review their processes. The high penalties if a breach occurs, the need to implement privacy by design are obligating companies to analyse deeply their methodology.

In total all these new requirements introduced by the GDPR need to be mapped to the current workflows and use cases in the energy supply industry to assure operational continuity while being compliant with the GDPR. As GDPR harmonizes the data privacy regulation throughout the whole European Community, it would be very valuable to work out the GDPR compliant adoption of existing use cases and workflows in joint research and demonstration projects, utilizing the methodologies developed within the M/490 mandate. This would create a very high level of transparency and would also detect issues, where the GDPR might be in conflict with needs required for a secure and reliable power supply and therefore produce also value feedback where the GDPR might need some clarification.

Takeaway messages:

- P3.1: The challenge will be to assure that the workflows assuring the operational continuity in the energy supply industry are being compliant with the GDPR.
- P3.2: Transparency of data flows and standardized data models are required to verify compliance with GDPR

3.4.2.4 P4 NAMING RISK COST BENEFIT



Different nations are in different situations on a development timeline towards a smart energy system, combining existing infrastructure, phasing out technologies with an environmentally big footprint on an overall life cycle. Research is needed to put numbers to whole life cycle impacts of current and new technologies but also procedures and processes assessing good practice examples. Globally oriented international collaboration needs to be put on a comparable landscape of opportunities for the future. To isolate Europe is not an option in a globally connected world. With interdependence comes the interest for everybody in a good outcome. The focus should be on long term solutions, learning from how companies are run with a long-term goal (which is adjusted), and how to calculate the benefits not just in quarter earnings, but factoring in less tangible societal benefits. This will allow to pinpoint costs for necessary cybersecurity audits, certification, requirements of vendors, or possibly mandatory patch & update contracts. Apart of espionage or cyber-warfare making it difficult to identify future risks, research is needed to gain a more holistic picture and start to put names and costs to what is important.

The Blackout Simulator[77] was a very early tool to provide a graspable translation of the importance to avoiding power system blackouts caused by hijacking, communication network devices failure, maintenance interventions, etc. for policy makers in understandable language, increasing transparency for consensus. More research on different scopes should help especially smaller distribution grid operators to be able to justify investments in cybersecurity for transmission/distribution power systems down to the secondary substations levels. In

[77] Blackout Simulator: http://www.blackout-simulator.com

reference to existing simulators in chapter quantifying impacts – this way of testing is needed for policies as well. The necessary cost of additional IT infrastructure to react to possibly maliciously concerted IT networked power consumers and producers on the customer side (e.g., mirai botnet) needs to be weighed against "... lobbyists and trade association representatives claiming that cybersecurity measures are too hard. The truth is, it is not." (Schneier, 2017) To improve cybersecurity for the whole industry, companies need regulation and policies (to blame) for cybersecurity investments, in spite of fiduciary responsibilities to maximize profits and this way, avoid penalization through shareholders losing profits – at the cost of cybersecurity for the whole society.

Today, vigilante individuals are deleting unpatchable, unsecure firmware of connected IoT devices to mitigate DDoS and botnets. Policies need to be evaluated, to bridge the paradox of holding vendors responsible for not patching and at the same time absolving vendors of responsibility, to ensure that cybersecurity risks are reported swiftly and patched. For example, global acting vendors could not be held liable, if they can produce an independent third-party security audit of their hacked system. New kinds of cybersecurity certification need to be defined and agreed on an international level. To pre-emptively deal with huge quantities of cyber-weaponizable IoT devices, research needs to look into the security of small devices (IoT), and especially the used crypto in general, to identify suitable, and banish unsuitable, currently used technologies. New architectures try to solve the secure update process of firmware in IoT devices (Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination FINAL REPORT). Policies can help tremendously in increasing the adoption rate of proven concepts to become state of the art.

Takeaway messages:

- P4.1: Cybersecurity issues handling raises costs that relate to long term goals for the companies and the whole society. Cost benefit analyses shall be considered in this regard for research and be evaluated through large impact quantification tools (e.g., black out simulators).
- P4.2: Research on regulation and policies that could help securing investments related to cybersecurity for organisations is recommended, especially for software vendors (e.g., mandatory patch & update contract offering) and IoT device vendors (responsibility / liability related to cyber-attacks).

3.4.2.5 P5 ANONYMISATION AGGREGATION

As already discussed in topic T5 "Cloud Computing" aggregation of raw data might help to assure data privacy for an individual person, but on the other hand, this might reduce or even eliminate the information value of the data for grid operation purposes. Research projects might highlight, teach and replicate good results of anonymization and aggregation or retention policies which consider the varying sensitivity of the data as well as the varying information detailing requirements for secure grid operation.

The research projects shall also prove the compliance of the developed algorithm and practices with the privacy requirements imposed by the GDPR (see also topic P3). A relatively new approach of querying over encrypted data (Wen, Lu, & Liang, 2014), could allow the coexistence of privacy and full data retention. The applicability on large datasets, even after local aggregation of e.g., metered consumption data in substations, is an open question.

Nonetheless, even after anonymization and/or aggregation, regular functions of the power grid need to be possible (e.g.: the ability to predict supply and demand variations).

Takeaway messages:

- P5.1: The demands coming from data analytics and data privacy have to be considered in a way, that both the derived information value for grid operation and the data security level (anonymisation/aggregation/…) is maximized.

3.4.2.6 P6 PRIVACY LAYER

The digitization process of the Energy sector brings with it new data collection, communication, and information sharing capabilities. While innovative technologies are being developed for 'smarter' grids, new issues for protecting consumers' privacy show up. Increased interconnection and integration introduce cyber-vulnerabilities into the grid which could lead to the leakage of personal information and the invasion of consumers' privacy more easily than before.

Personal information is defined as recorded data that can identify an individual directly or indirectly. According to NIST, it includes information such as name, address, consumption and billing history (The Smart Grid Interoperability Panel Cyber Security Working Group, 2010). Within the smart grid context, the amount of personal data that can be monitored, collected and analysed is significantly increasing. According to the EC, close to 200 million smart meters for electricity and 45 million for gas will be rolled out in the EU by 2020. This expanded information raises added privacy concerns.

First of all, fraud should be considered as customers private data could be intercepted, manipulated and modified for illegal purposes. Security issues need also to be investigated as the information generated by the smart meters introduce new concerns. For example, the "near real-time" data regarding energy consumption could be used for malicious intent to determine whether a residence or facility is occupied, where people are in the structure, what they are doing, and so on (The Smart Grid Interoperability Panel Cyber Security Working Group, 2010). In particular, private sensitive information like practice of religion can be inferred from an electrical consumption load curve analysis. Personal lifestyle information collected from energy use data could also be used for unfair commercial purposes as they are valuable for different parties to develop techniques such as targeted marketing.

All of these potential issues need to be properly addressed as they could significantly threaten customer privacy, especially with regards to GDPR: personal information monitored and collected in the smart energy / smart grid context need to be secured and controlled accordingly, with the use of a "privacy by design" layer in all concerned IT components of the system (from transmission to storage to access).

The security of data is generally ensured via cryptographic techniques. However, future systems may require information protection techniques beyond traditional cryptography. Techniques like signal processing, used for securing physical layer communications, or differential privacy, a method that enables quantifying the exposure (privacy) of any record in a database, might be suitable solutions. State-of-the-art techniques such as anonymity, access control, and accountability might provide their solution to eliminate personal information leakage problems.

Concrete results are expected in design principles to address privacy issues including:

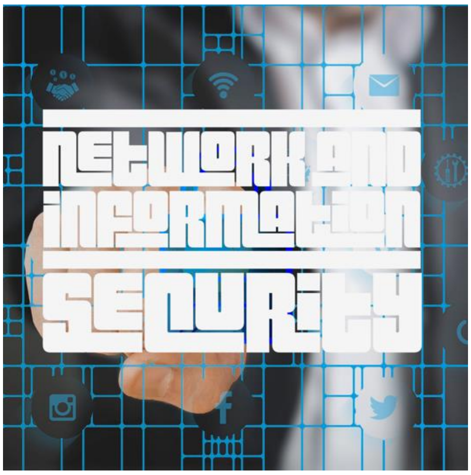
- the “collection limitation principle” which states that personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;
- the “purpose specification principle” suggesting that the intents for which personal data are collected should be specified and information should only be used for the purpose for which it was collected;
- the “data quality principle” which stipulates that personal information should be accurate, complete and kept up-to-date.
- the “security safeguards principle” suggesting that personal data should be protected by reasonable security safeguards against such risks as unauthorized access, modification or disclosure of data.

Additional in-depth studies are required to determine the best mechanisms to prevent privacy violation in the smart energy / smart grid context as failure to address these issues will not be accepted by customers.

Takeaway messages:

- P6.1: Privacy concerns are growing with the transformation of energy systems, in particular, smart meters that are being deployed all over Europe bring sensitive personal data into the system.
- P6.2: 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.

3.4.2.7 P7 NIS DIRECTIVE



The Directive on security of network and information systems (the NIS Directive [78]) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

It provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

1. Member States preparedness by requiring them to be appropriately equipped e.g., via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
2. cooperation among all the Member States by setting up a cooperation group and even a CSIRT Network,
3. a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, among them energy and key digital service providers.

In this context of cooperation increase, a global cyber-attack simulation on European electricity and gas utilities and networks could bring an interesting opportunity to boost the capacity of the many implied companies to coordinate and react quickly. The organisation of a big exercise of such kind would need an important preparation and cooperation effort, but it will be worth for the global resilience of European energy systems.

In comparison, the same kind of simulation is being realized every two years at North American level (USA, Canada, Mexico, …) and coordinated by the North American Electric Reliability Corp (NERC). It involves more than 400 organisations and around 6,000 persons.

[78] NIS Directive: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Hence an equivalent European initiative would prove the ability of Europe to face the global risk of a major cyber-attack occurring simultaneously in several European member states. As there will be many public and private parties at stake, the first step toward a future European cyber-attack simulation is to study and work on the optimal organisation, which entity should be best placed to head and coordinate it, and how to make the most public and private companies embark on the global European exercise.

Takeaway messages:

- P7.1: The NIS directive aims to boost the level cooperation between member states for cybersecurity. In this regard, the organization of a European wide global attack simulation exercise on electricity and gas infrastructure may be fruitful both for the preparedness and the resilience of European energy systems.

3.4.2.8 P8 SHARING OF VULNERABILITIES

Imagining a database (DB) where all attacks are documented/shared is allowing companies to communicate with each other on highly sensitive issues and presumably contributing to a significant reduction of resource intensive multiple intra company solution finding processes. Research in this topic should prepare best sharing practices, to avoid information floods (e.g.: open and collaborative epidemic response in healthcare). For example, IBM shared its DB of 500 TB filled with cyber-attacks and mitigations – a good example but this format is not usable for small (or even most big) companies.

The amount of threats to electronic devices is on a constant increase, as well as the according countermeasures and strategies for closing possible vulnerabilities. Keeping the operating system and working environment up-to-date & secure and apply the according countermeasures requires a well-designed access towards the knowledge for the responsible persons in a compressed but understandable way. So-called knowledge databases are an option of providing the necessary platform for sharing and accessing know vulnerabilities.

For example, one misconception upon password handling has been stated in the mid of 2017 by Bill Burr, responsible for the widely used guidelines for password creation (Burr , Electronic Authentication Guideline) which caused employees to write down the complicated password forced by security algorithms and place them below the keyboard or otherwise nearby.

One of the greatest challenges relies on granting the right amount of useful information for the person in charge, preferably attuned to his level of expertise. A common understanding on the type and functions of the device or system in question is therefore crucial.

The design and proof of concept of an adjustable user (group) specific (transfer-) knowledge database access (or similar technological approaches) or process that enables an integration into everyday working situations whilst enhancing the overall security situation even for small companies, is recommendable.

The correct treatment and containment of a vulnerability needs to be accessible and practicable in terms of available resources, which are inevitable connected to the user or technician, carrying out the task of keeping the operating system alive and secure. This comes hand in hand with bringing together different levels of domain knowledge or varying terminologies for the very same object exposing the vulnerability in question.

The accessibility of the right information and avoidance of redundant solution findings, as well as ongoing documentation in order to avoid common errors are not limited to the domain area of security. The proposed approaches or methods need to prove themselves valuable among different levels of the company, ranging from small to big scale. One of these approaches is handled with the model driven engineering approach in the Smart Grid domain as described in (Christian) with one of the goals being to raise awareness on possible vulnerabilities in a cyber physical system. A similar model driven engineering strategy has also been applied to the field of Industry 4.0 (Weyrich & Ebert, 2016), unmanned aircraft systems (Denney, Pai, & Whiteside, 2017), and healthcare (Gannud, Wu, & Timoney, 2017) for validation purposes and handling the complexity of today's quick developments.

Establishing processes or software for reducing information floods, and allow for teamwork of multi-agent systems ((Dunin-Kiplic & Verbrugge, 2010), p.3) for the end-user is going to be more important than ever in an evolving time of Big Data, whereas the yearly collected data and information surpasses all former accumulated volumes of data collected in human history.

Takeaway messages:

- P8.1: Obscurity is not equal security, and well-meaning solutions without the appropriate technical means to realize them without loss of comfort can have opposite effects.
- P8.2: Knowledge databases are used to share and access known vulnerabilities; To reach maximum efficiency, research is recommended on the way to provide, for the same object/vulnerability, the appropriate level of domain knowledge and terminology given company context (e.g., small vs big company) and user skills (e.g., he may be a standard user, a cybersecurity expert or an IT technician).

3.4.2.9 P9 TRAINING AND POLICY AMENDMENTS

The cyber threats to society are changing. In the past, most cybersecurity risks came from criminal groups seeking financial gain, for instance through attacks on business (e.g., web applications or online payment systems) and personal computers. However, the discovery of Stuxnet showed that malware could be used as a tool for damaging physical equipment essential for functioning of the critical infrastructures. Since then, many nation states have been developing the offensive hacking (cyber-warfare) capabilities targeted at critical infrastructures. The recent attack on Ukrainian power distribution companies have shown that some actors are willing to use these capabilities, and such attacks could cause significant damages to critical infrastructure, also at neighbouring interconnected countries. In the meantime, critical infrastructures have only become more vulnerable because of increasing automation and interconnection with other open systems (e.g., IT system). Because they depend more and more on computers, they often cannot work properly without active remote control. The combination of these trends creates a great risk from cyber-attacks. The infrastructure operators need to prepare their employees to cope with such advanced cyber-attackers. To make our critical infrastructures resilient against cyber-attacks, regular exercises should be held on what to do in different stages of the attack, including stages in which the attack is affecting the physical world. However, trainings in this stage cannot be done on real systems without risking disruptions of critical services. Instead, the best way to hold them would be through simulations. The energy domain will require cyber-security training methods that allow critical infrastructure providers to effectively prepare for major incidents. The training methods should incorporate realistic simulations of the physical world, so that training participants can experience the impact of cyber-attacks and learn how to respond in a real crisis.

Takeaway messages:

- P9.1: Regular exercises and trainings are key to make our critical infrastructure resilient against cyber-attacks. The efficiency of training methods may be improved through research on how the complex physical world of energy systems may be realistically simulated.

3.4.3 CLUSTER: FUTURE

The topics of this cluster are expected to be relevant in a mid-term future. The topics might sometimes seem far-fetched and unrelated today, but we need start to understand these as interdisciplinary research areas, to try to deal with unknown cybersecurity challenges from suddenly exponentially growing sectors (biotech, AI, quantum computing).

3.4.3.1 F1 PROGRESS CONSIDERATIONS

The development of smart grids to overcome future challenges in the energy domain will open up new communication paths that exist in parallel to the energy distribution infrastructure (Farhangi, 2010). The increased use of sensors and implementation of new services for the consumers will potentially generate vast amounts of additional data. These developments put new strains on the security systems involved in this area, as they open up new entry points to the system and therefore offer new opportunities for attacks while increased reliance on the energy grid and the additional personal data that could be available through the additional services, makes it an increasingly tempting target. The problem becomes even more severe if we assume that future automated control concepts will follow distributed approaches (Strasser, 2015).

When considering security and cryptography for the energy grid and its related services we must not neglect how technological advancements in hardware and software can threaten existing solutions at any time, an extreme example here might be the thread caused by quantum computing to existing RSA-key based systems (Mailloux, Lewis, & Riggs, 2016). The core problem here is providing future-proof security measures, or in other words, solutions to problems we do not face yet. Scientific research in new security concepts needs to go beyond “locking” people out, but instead improve security on various levels, some proactive by restricting access and providing intrusion detection, some reactive by providing mitigation and tracing strategies. Various research lanes to this end already exist in the security community and also in the distrusted systems domain. Evaluating these new approaches and integrating them into policies for industrial applications will be essential in allowing the smart grid to grow to its full potential without exposing the energy systems we so rely on to attacks and misuse.

Takeaway messages:

- F1.1: Technological progress is continuously ongoing in various domains and will impact energy systems in a way that we cannot fully anticipate today; evaluating new approaches (e.g., sensor data infrastructure, quantum computing, …) will be essential to maintain an adequate level of protection in energy systems against cyber-attacks.
- F1.2: Research based on prediction scenarios should also include relevant technology progress variations in their conclusions.

3.4.3.2 F2 SOCIETAL IMPACT

Digitisation is impacting a great number of human activities and, as a result, our society will be changing as well. Energy, which is being profoundly transformed and leveraged ((Gassmann & Sutter, 2016) p.229-240), will retain its essential characteristic in society. It is quite relevant to facilitate the involvement of the energy users in the cybersecurity good practices through training, and information exchange.

Energy in general, but Electricity in particular, will increase its relevance and importance for human beings. The trend of guaranteeing electricity use to the whole population of the world is clearly defined and supported, being even accelerated by the use of renewables and microgrids in the locations where traditional electrical networks are not existing, as can be seen at the example of China ((Rogers & Wang,, 2012) p.92-99). Digitisation is accompanying the evolution and cybersecurity has to be a factor to always take into account. Particularly in cities, as places where most of the people will live, the special impact on energy resilience needs citizens involvement, also in cybersecurity research and decisions.

The society as a whole and the energy users have to acknowledge the importance of cybersecurity as they already recognize the need for appropriate physical protection. Moreover, when in many cases users of electricity will play an active role in the electrical system supplying their production and supporting ancillary services. As it has been proposed in P9, training of energy users with special content of cybersecurity will be needed, establishing the base for playing even an active role within the overall cybersecurity measures as informing threats, alerting attacks and even updating the firmware/software of their systems/devices to get the desired level of protection within the accepted risk.

In general, there are cybersecurity relevant privacy and societal impacts to be considered for data, data streams, or sensory recordings, depending on their transparency or agreement for recording and evaluation, their encryption during transport, their secure storage, their value reselling, ownership, and attributable analytical post processing allowing near-certain predictions of individual situational behaviour. Cybersecurity societal impacts need to be researched ranging from miniaturized swarms of drones, car generated sensor data, to single-purpose robotic helpers in supermarkets (MIT Technology Review), offering videoframe surveillance without regulation. Depending on the sophistication of attacks, it can be a new threat vector to exploit[79]. Big data and statistically honed algorithms providing a powerful microscope, together with social mining is revolutionizing scientific research (measuring and monitoring the wellbeing and trends of our society), but has implications on societal levels as well ((Qiu & Antonik) p.2), not just the cybersecurity aspect of “losing” the data (theft) or access to it (ransomware). Cyborgs – people enhancing their physical abilities with technologies (infrared vision, Wi-Fi feeling, exoskeleton muscles, etc.). Societies acceptance of robotics or autonomous vehicles is given with little helpers (MIT Technology Review) but relies on the transparency of an available decision-making process – that was proven having been not altered by artificial intelligence (lying) – after accidents and deaths, e.g., (Bhuiyan, A federal agency says an overreliance on Tesla’s Autopilot contributed to a fatal crash.) or (Bhuiyan, Police have released the first video from inside the Uber self-driving car that killed a pedestrian). This immutable history will need research transcending blockchain as a single word answer technology.

[79] Shodan looking for webcams: https://www.shodan.io/explore/tag/webcam

A very underappreciated fact about safety and security is, that in general, humans are not psychopathic murderers trying to kill you and everyone at any chance they can get, drawing wrong lines on concrete to mark misleading roadways, welding heavy iron ramps on train tracks to derail them, steering trucks in the midst of a crowd or shooting at school children. Nonetheless, these attacks do occur and are tragic losses. It has to be a goal of society to create a framework, where these acts do not happen because of avoidable causes such as despair, loose gun laws, tolerated mistreatment in childhood, and ignored warnings of concerned friends, neighbours, citizens, or systems – keeping privacy-by-design principles in mind.

In Energy, the trend is that users will rely more on home/local systems operated by service companies different than the networks (which for electricity will remain needed) and data collection, transport and analysis will be the pillars of the digital transformation. This might become an easier way to request a compulsory compliance of minimum cybersecurity requirements and even to establish the appropriate “knowledge network” to keep the risk under control. In summary, research has to be done in measuring the societal impact of unsecured (cyber) energy supply systems as well as in the most efficient layout to achieve the needed involvement of the users (e.g., supporting multimedia cybersecurity education and awareness programs[80] of consumers to collaborate in preserving acceptable levels of cybersecurity; fostering international cooperation for experts and stakeholders groups to work together, not just overarching Europe, and transparently motivating more countries to follow good examples[81]).

Takeaway messages:

- F2.1: Society and in particular energy users need to be aware of the importance of cybersecurity in the energy use of the future.
- F2.2: Involvement of energy users is necessary to achieve the desired level of risk protection.

3.4.3.3 F3 QUANTUM PROCESSING

Intercontinental quantum communication was demonstrated early 2018 among multiple locations on Earth with a maximal separation of 7,600 kilometres (Liao) enabling the transmission of highly sensitive keys, ensuring no man-in-the-middle was present. But in the near future, the increased processing speed of quantum computers will offer extended capabilities and possibilities to crack protocols that are currently too computationally difficult to unravel. With the use of Quantum (Q) Qbits, units that can be in 3 states (either set to 0, 1 or “superposed”) quantum machines can theoretically compute exponentially faster than current systems. IBM announced the end of 2017 the achievement of a 50 Qbit-based quantum computer, that could “surpass the capabilities of a supercomputer,” according to Google. Lastly, in December 2017, Microsoft made available a “Quantum Development Kit82” for everyone wanting to write quantum programs and simulate up to 40 Qbits in Azure. Experts have suggested that quantum computers could break in the coming 5 to 10 years the toughest mainstream encryption strategies in use today (Wired, 2010). Last

[80] Security Now: https://www.grc.com/securitynow.htm
[81] Good Country: http://goodcountry.org
[82] QDK: https://www.microsoft.com/en-us/quantum/development-kit

year, the IEEE Spectrum, a magazine edited by the Institute of Electrical and Electronics Engineers, reported that quantum computers were close to cracking RSA encryption [83], an algorithm used by modern computers to encrypt and decrypt messages. Some other encryption technologies like AES are still considered – so far – as able to resist to quantum attacks, provided the encryption key is long enough (AES256 seems fine, but AES128 may be broken[84]).

Many of our business activities using the internet such as sending emails, checking online accounts, updating the software, rely on cryptography methods highly vulnerable to attacks from quantum computers which could represent a "free for all" tool for cybercriminals. All industrial and commercial systems could become potentially vulnerable: protected communications between power stations and central IT supervision & control systems. Between connected objects – among them smart meters - and IT central systems. Big encrypted databases. Sensitive data could be leaked, leading to severe consequences for the user and the entity responsible for protecting that data (Totzke, 2017).

Corporations and governments need to adopt approaches to cybersecurity that will allow them to protect their critical information from quantum computing attacks. They must act now as experts have estimated it would take at least ten years to modify existing cryptographic infrastructure (Butterfill).

Indeed, the potentially drastic repercussions of quantum computing on cybersecurity necessitate a complete redesign of the algorithms involved in online encryption which has led to the recent focus on quantum-safe cryptography. Also known as "post-quantum" cryptography, such techniques aim to develop cryptographic algorithms that could withstand breaking by quantum computers (ABI Research). In 2016, Googles experimented a real-world post-quantum cryptography algorithm with its browser Chrome, basing on a specification proposal called "new Hope Key Agreement"[85]. Lattice-based systems, multivariate, hash-based cryptography and quantum key distribution (QKD) are examples of those new quantum-safe techniques that are being developed and experimented.

Agencies such as the ETSI (European Telecommunications Standards Institute) and the NIST (National Institute of Standards and Technology) are attempting to coordinate and homogenize the approach to post-quantum cryptography by developing new encryption standards. The NIST has, in particular, determined the minimum standards for cryptographic technologies used by the United States government. This includes recommended NIST-approved algorithms used to secure data, communications, and identity (Kumar, 2016).

The transition to quantum-safe cryptography is going to take time. It will indeed start with the implementations of "hybrid solutions" that allow for agile cryptography designed to improve the traditional encryption in use today (Totzke, 2017). To tackle this challenge of computing science and cybersecurity from now, it is highly recommended to encourage research and innovation in Europe, and not to let all knowledge and know-how be 'trusted' by major companies like IBM, Google, and Microsoft.

Takeaway messages:

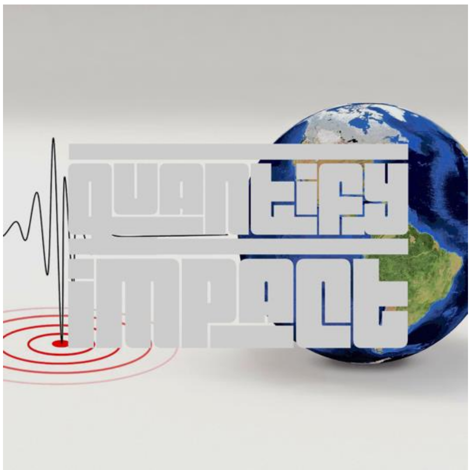
- F3.1: Quantum cryptography is a promising disruptive computing technology that will impact many calculation processes, among them encryption. Research in this field, currently mainly financed and mastered by US companies, is strongly encouraged.

3.4.3.4 F4 QUANTIFYING IMPACTS

[83] Close to cracking RSA: https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

[84] https://crypto.stackexchange.com/questions/6712/is-aes-256-a-post-quantum-secure-cipher-or-not

[85] new Hope Key Agreement: https://www.thesslstore.com/blog/googles-post-quantum-cryptography-experiment-successful/



Stakeholders in the energy sector are well aware of the increasing demand put on the energy infrastructure but fully comprehending the impacts and risks involved in these developments is very hard, especially since some problems, like widespread use of electric vehicles, are only foreseen, but have not yet manifested themselves. For such developments, mainly theoretical contemplations exist ((Pieltain Fernande, Gomez San Roman, & Cossent, 2011), (Reichl, 2013)), that often focus on illustrating relations and impacts theoretically, but fail to deliver information about the actual effects of a technological change to the grid. Supporting stakeholders and decision makers in their process will be necessary to put these theoretical models and predictions into a more relatable form, for example by simulation. Simulators for grid failures already exist in various types (Yao, Huang, & Sun, 2016) but lack integration of the new usage scenarios, like electric vehicles and massively distributed photovoltaics. To make the simulation results serviceable it will be necessary to further ground the results in existing grid infrastructure and provide monetary estimations to the provided simulation results, methodologies for these estimations exist, e.g., (Reichl, 2013) and need to be considered when developing new simulators examining concepts such as serious games.

A sophisticated blackout simulation that integrates estimation of risks and costs for the different actors in the electricity domain will help stakeholder to develop a better understanding for the impact technological developments will have on their domain (Kleineidam, Jung, & Woeltche, 2017) Providing simulation results that are related to the "real" European energy market and consider the new scenarios mentioned above will make the risks more relatable and can be invaluable for stakeholders and decision makers. Putting reliably derived (simulated) numbers to the problems will set the costs for infrastructure development into perspective and give researchers, engineers and analyst's additional arguments and exemplifications to present their ideas and approaches to the decision makers. On the level of energy providers and distributors, the simulation results will introduce a new awareness for the impact of upcoming changes which should help to steer the energy sector towards higher standards of security and stability, in light of ongoing and forthcoming changes in the energy consumer, producer, and distributor landscape.

Takeaway messages:

- F4.1: Simulation is a promising approach to assess and quantify cyber-attack impacts on energy systems. Although simulators for grid failures already exists, they need research and improvement to be adapted to future distributed energy systems (PV, EV, flex, ...).

3.4.3.5 F5 NEW CRYPTO ENVIRONMENTS

Cryptography is an ongoing hare and hedgehog race since the continuously increasing computing power may already tomorrow enable the hacking of crypto algorithms, which today are considered as secure (see also F3 Quantum Processing). For this reason, ongoing research needs to improve cryptography technology to stay ahead of hacking techniques.

However, in the energy management infrastructure, the priority regarding cybersecurity is as follows:

1. availability,
2. integrity, and
3. confidentially.

Therefore, newfound cryptographic solutions need to be given the time to run, being pounded on and tested sufficiently before something is considered secured. Formal verification alone does not cover the whole environment, solutions are deployed inside their new crypto environments. Current crypto needs to be future „proof", formal verification of the software might not be enough.

Also, it will not be possible to roll out new cryptographic solutions simultaneously throughout the whole energy system. Hence, the reliable operation of a heterogeneous cryptographic system and its incremental update needs research too.

Finally, research programs in this regard, should always include field demonstrations to verify, if the technology developed and tested initially within labour environments are also working reliably and securely under field conditions, and all newfound cryptography should be designed with open protocol and not in a closed consortium, not allowing cryptography researchers to validate approaches, or already early on responsibly disclose problems.

Takeaway messages:

- F5.1: For a critical infrastructure availability has the highest priority, this has to be also considered for the development of cybersecurity concepts.
- F5.2: Research programs should include instruments for field demonstrations testing and verifying technology developments in lab and field conditions, with cryptographic open protocol solutions preferred.

3.4.3.6 F6 DATA STREAM CHALLENGES

The ongoing improvements of computing power and communication bandwidth enable the transition from a cyclically to a more continuous monitoring of the grid state, e.g., phasor measurement data instead of cyclic RTU measurement telegrams. Thus, data streaming like monitoring communication allow the control of transient effects, which becomes more and more critical due to the increasing dynamics caused, by the fluctuation of renewable infeed as well as shorter market cycles and the decreasing grid inertia due to the replacing of large generation by synchronous machines with decentralized generation connected via power electronics.

From the cybersecurity point of view, such data streaming like communication requires special attention, as they will become the base for future grid stabilizing applications, e.g., the damping of power swings utilizing the capabilities of power electronic based grid elements like HVDC-Inverters or FACTS. Security measures like for example the cyclic exchange of the encryption key becomes more complex, as the data stream communication must not be interrupted during the change of the encryption key. Also, the protection against Denial of Service attacks might need special solutions to ensure sufficient availability of the data stream communication. Another challenge is sharing symmetric keys in multicast groups, as it is suggested by IEC 62351 with HMAC, which is used as standard solution in Phasor Measurement Unit (PMU) installations, to provide Wide Area Monitoring Protection and Control (WAMPAC). This can be solved with streamable authentication protocols, for example, TESLA (Perrig, Canetti, & Song, Proc. Internet Soc. Netw. Distrib. Syst. Secur. Symp), or newer inf-TESLA (Câmara, Anand, & Pillitteri, 2016).

The volume of streaming data, used, for WAMPAC purposes is rapidly growing but dwarfed, compared to the streaming data volume produced by other application like video on demand, or Massively Multiplayer Online Role-Playing Games (MMORPGs).

Consequently, research is needed to assure, that future communication technologies, developed by the telecom industry, like 5G, can also be utilized for grid management purposes and therefore reduce the need for costly dedicated communication for the grid management. To minimize data streams, not only because of privacy considerations, but also resilience, the development of local intelligence, acting on data that does then not need to be streamed is very important. This local intelligence is not replacing top-down decisions but allowing bottom-up decisions in a decentralized way. Research towards a decision-making unit can be necessary for resilience in a highly distributed cyber-physical system.

Takeaway messages:

- F6.1: The decreasing grid inertia requires to improve the grid monitoring to measure also transient effects. New monitoring technology has to have the same reliability as today's grid monitoring technology.
- F6.2: New communication technology, like 5G need to provide a minimum, but guaranteed service level for critical infrastructures

3.4.3.7 F7 BIO-NANO CHALLENGES

New nano-materials will offer many opportunities in High Voltage Direct Current (HVDC) transmission applications (Stevens , IEEE Electrical Insulation Conference (EIC),). As described at the beginning of this paper, the need for cybersecurity in operational technology is not expected to stop at the operational technology domain.

New developments in bio-technologies, make it easier to create new organisms and to change present ones, call upon every domain, interdisciplinarily, to analyse potential impacts in their fields and across fields. Bio-/Cyber-enhanced humans working with smart grid OT are expected to have different cybersecurity relevancies (ENISA , s.d.).

Like every technology, the dual-use challenge of hackers using new or repurposed bio/nano technologies as easy to order (Mullin, s.d.) malicious weapons for extracting ransom, targeted attacks, or distributed warfare, are calling for resilient protocols and procedures, being able to assume a reduced "normal" operation in case of human emergencies.

New organisms (Gibson, 2010), biological computers (Elowitz & Leibler, 2020), biosensors, transformed cells [82] or industrial enzymes for biofuels (Ball, 2016) made, developed e.g., as alternatives to finite resource based (Lithium) battery storage technologies, apart from well-known awareness for inevitable programming/testing bugs and errors (Green, Kim, & MA, 2017), are expected to be a cybersecurity challenge as well, assuming that for example moderate temperature changes – unnoticed remote intruders in such a storage power plant could influence building automation to target temperature control – could render those storage organisms useless, explosive, or contagious.

The Pentagon and UC Berkeley is successfully exploring how to merge alive insects (bees, cockroaches, etc.) with hardware components to allow remote control, relay audio, or more (Shachtman) – and kids can order a DIY kit online [86]. These remote-controlled insects can, e.g., spy passwords while typed, provide biometrically locked access for perpetrators safe and far away.

The concept of man-in-the-middle attacks is also applicable to malicious changes to organisms' code, production recipes, and DNA/RNA based programs, or the displaying of modified CRISPR results to achieve different conclusions, outcomes, or malicious setbacks. To establish ethical principles, technical solutions, to provide recommendations and public involvement, it is necessary to foster platforms for public-private partnerships, conferences for researchers, symposiums to aid discussions of crosscutting risks of biotechnology and share ideas about cybersecurity as done in the European initiatives SYNBIOSAFE[87] or COSY[88,].

Takeaway messages:

- F7.1: Bio- and nano-technologies will create more and more applications in the future and will raise, the same time, the number of cyber threats (e.g., bio-attacks against bio-components like bio-fuel cells, man-in-the-middle attack). Research should be utilized to establish ethical principles, technological methods, provide recommendations, and allow for public involvement.
- F7.2: It is an interdisciplinary research challenge for information security and cybersecurity. Risks and implications of technologies are not understood. Existing security techniques are not fit to achieve the required protection needed.
- F7.3: Programming tools need to offer new testing and simulation frameworks for evaluating long-term inheritance, mutation, and selection effects. Security and safety protocols for engineered life forms need to be able to guide customers at home working with DIY CRISPR Kits [89.]

3.4.3.8 F8 ROBOTICS SAFETY IMPACT

There needs to be kept a cybersecurity motivated balance between highly-secure solutions, economically affordable ways, and monocultures of operating systems, concerning robotics and safety (ENISA , s.d.).

Increasing demand for collaborating robots ranging from battlefields to factory maintenance (e.g., lifting a heavy load, while collaborating human is adding their labour part) is decreasing physical safety margins. There is ample need for new materials research in damping contacts, research for new sensors to increase robots' awareness of their surroundings, and new control concepts smartly adapting safety parameters dependent on situations. Keeping Asimov's laws of robotics in mind – or stimulating the research for newer versions (Murphy & Murphy, 2009) – could spawn solutions for algorithmic transparency, the ability of systems to explain its decision making; or solutions of trusted identification to the public. Switching the viewpoint, robots are equipped with sensors,

[86] DIY Cyborg Cockroach: http://www.wired.com/dangerroom/2009/01/pentagons-cybor/
[87] SYNBIOSAFE: http://www.synbiosafe.eu/
[88] COSY: http://www.synbio.at/
[89] DIY CRISPR Kits: http://www.the-odin.com/diy-crispr-kit/

processing, and recording power to perceive their surroundings. This raises privacy, ethical, and legal concerns when considering their use for surveillance or efficiency as social robots in consumer marketing. Learning from IT, roboticists might begin to create privacy-enhancing robots, aiding companies or people to preserve privacy in a mid-term future complex world ((Lin, Abney, & Abney, 2012) p. 187-198). Comparable to IT, many commercially available home robots are insecure and can be hijacked by hackers, shifting the privacy problem towards a safety problem – especially considering existing search engines for robot feeds on the Internet, and military robots hacked by terrorists.

Apart from a "design responsibility", ethical codes of collaborative robotics could be cryptographically implemented in hardware as Physical Unclonable Functions (PUF) but verifiable wirelessly. While complex ethical codes are a future topic, PUFs can already offer electronic devices an efficient, secure, and cheap way for authentication and identification (Morozov, Maiti, & Schaumont). In Field Programmable Gate Arrays (FPGA) devices, PUFs may be instantiated during fabrication to exploit variations of the manufacturing process, but they may produce different results each time. Therefore, proficient error correction algorithms need to be found, ID generation needs to be refined, and the potential reliability improvement investigated (Xin, Xin, & Gaj, 2011).

Formal verification of Hardware can be a tool during the manufacturing process to guarantee the functionality of hardware-software chips during production. Self-protection measures or emergency communication need research on kinds of trust models, redundant channels, not jammable.

5G using a spectrum of 30-300 GHz has more bandwidth capabilities but cannot get around obstacles easily. This will need smart cells, coordinating their smaller coverage through offering many more businesses an opportunity to share the infrastructure at the cost of not yet known cybersecurity. For example, inside factories, using small cells or even femto-cells indoors of small to medium-sized companies, or more mobile ecosystems offering mobile connectivity for collaborative-robots or more traditional industrial M2M communication of various interoperable vendors, necessary for new IoT services. These new possibilities will grow the overall coverage, but from the cybersecurity point of view, demands research in enabling synergies of communication infrastructure and at the same time find a secure separation of services, as it is done today with the three dumb routers principle[90] in Wi-Fis at home.

Takeaway messages:

- F8.1: Robotics is a dynamic domain that brings each year new products to life, for public or military use; this domain brings along new threats (hacking of military robots, home robots and enterprise assistants). Research shall be conducted on these new threats to secure both components and infrastructure (e.g., 5G).
- F8.2: a promising research field to secure components relates to the implementation of ethical codes into robots' core components, such as Physical Unclonable Functions (PUF).

[90] Three Dumb Routers: https://twit.tv/shows/security-now/episodes/545 revsited by: https://www.pcper.com/reviews/General-Tech/Steve-Gibsons-Three-Router-Solution-IOT-Insecurity

3.4.3.9 F9 AUTONOMOUS VEHICLES REGULATION

Drones inspecting power lines and cleaning wind turbines[91] are used already today. Growing weights can be transported, people are building their own drones, lifting themselves inside modified bathtubs[92.] The cybersecurity implications of causing power outages through earth faults by drones carrying grounding cables onto high voltage power lines, or simply cutting them in a coordinated synchronized way, need to be addressed already. Especially for consumer products, in the categories below 150kg, 25kg, 5kg, or even 250 g, currently every country has their own interpretation and criminalizing hurdles in the name of air safety. Already 2016 EASA published a consultation document, proposing an important unified regulation for the European Parliament and the Council[93]. Without a common regulation, companies and people have to follow national laws, and stay in grey or safe zones, which does not necessarily increase safety, but stops potential business models and halts European innovation in this domain. Furthermore, regulation needs to keep a balance. People will find ways around unnecessarily strict regulation, e.g., instead of putting cameras on drones, they will put motors/engines on cameras to stay below weight limits, or use remote controlled flying animals or insects with cameras, which are again unregulated. There needs to be a certain freedom for people to creatively use new technologies, and appropriate technological measures assisting safety for life and property.

Autonomously driving cars, hacked, trying to crash into substations in a concerted fashion is supposed to be prevented before the hack happens. Autonomous trains, transporting container loads of batteries across Europe to help stabilize local distribution grids coping with geographically moving events can also be a threat for safety on multiple dimensions, that needs to be dealt with at the cybersecurity level, before malicious attacks happen. The intersection of multimodal autonomous transportation is the most safety-critical area. Hence, there is the research need for trust and credibility between machines (social ICT system architecture) and redundant cybersecurity control measures being found in the following years, since less reliable devices are serving as input as well ((Mitleton-Kelly, 2013) p.141-184).

There is a need to define regulation for affordable minimum cybersecurity reference realizations as open blueprint, to define protocols for immediate patching duties for vendors, depending on severity of adaptable impact assessments, and to offer mostly automated platforms for exchanging new threats and possible ways to cope across domains (IT, banking, smart grid, automotive, aviation, health, rail, etc.). There is a need to identify certification criteria meeting or surpassing minimum cybersecurity measures, which need to provide secure remote update capabilities. This will lead to a higher resilience needed for various application domains. Imported autonomous vehicles need to provide independent certification fulfilling sets of minimum requirements. Research is needed, creating frameworks for critical infrastructure to provide signals of no or slow flight/drive zones for autonomous vehicles, to hardware-based immutably override crash-trajectories to help avoiding accidents (ENISA , s.d.) p14).

[91] Wind Turbine maintainance drone: https://plus.google.com/photos/photo/114077525644661833984/6530562847886426082
[92] Flying to the bakery in a bathtub: https://www.youtube.com/watch?v=EQK9m_OBVgY
[93] EASA drone consultation https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf

Takeaway messages:

- F9.1: Autonomous vehicles, especially drones and cars, bring new threats for energy grids and systems; in this respect research is needed especially on multimodal autonomous transportation that amplify the risks.
- F9.2: Research and inclusion of all relevant stakeholders is needed on regulation perspectives to limit risks through minimum cybersecurity measures and certification, still allowing creative new business models without unnecessary criminalization.

3.5 CONCLUSION

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. 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 [92], and the NIS Directive [35], are providing important steps to increase fragmented cooperation, the EU wide sharing of knowledge, transparency for markets. The proposed Cybersecurity Package (European Commission, 2017) wants to go an important 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. This will introduce liability for 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 our horizon set on 2050, we identified important innovation and research topics in different clusters that will need results in the next years, to be able to have many research gaps closed, when creating policies, regulations, and directives to improve cybersecurity and resilience for the future.

3.5.1 CYBERSECURITY RESEARCH TOPICS RECOMMENDATIONS

Digitisation 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 obvious that know-how and expertise from of related domains information security, telecommunications, automotive, healthcare, is essential for the development of cybersecurity and resilience.

Along the famous quote of Niels Bohr “Prediction is very difficult, especially about the future.” (Teaching an Learning Elementary Social Studies, 2013), p. 431), this position paper takes the approach of offering topics and described scenarios with the aim of sparking research ideas. We hope, this will create more interdisciplinary research teams, trying to tackle issues imaginable through the topic and scenario descriptions, but not possible if we already were to match specific stakeholders to formulated research recommendations.

After the description of each topic, a list of takeaway messages was provided, labelled with the first letter of their cluster, the topic number, and followed by a number representing a scenario described within the topic.

The summarized takeaway messages are research topic recommendations in the three respective clusters listed as follows:

- Technology
    1. AI will help cybersecurity industry to efficiently monitor sophisticated threats
    2. Blockchain is considered as a promising technology to address authentication, authorization, consensus, and immutability
    3. Blockchain offers a secure decentralized way to guarantee the veracity of various transactions
    4. Digitalization enables and relies on the massive deployment of sensors that improve analysis
    5. IoT enabled devices will make the energy system more transparent and efficient with analytics
    6. For highly networked components, safety is not reachable without cybersecurity
    7. Machine Learning enables predictive analytics which helps detecting specific cyber attacks
    8. OT/IT cybersecurity architecture raises the question of on-premise vs cloud-based calculation
    9. Grid optimization application are suitable to be deployed in a cloud environment; however, safety or security relevant grid control requires still a decentralized grid asset deployment
- Policy
    1. Metrics and frameworks should be developed for decision making of cybersecurity risks
    2. Stakeholders operating in isolated silos need a communication platform (IT, TSOs, DSOs, ESCOs, Policy)
    3. Cybersecurity research at a meta level should be stimulated among the EU member states
    4. Transparency of data flows and standardized data models are required comply with GDPR
    5. Cost benefit analyses shall be considered (e.g., black out simulators)
    6. Research on regulation securing cybersecurity investments is recommended
    7. The NIS directive boosts cooperation between Member States for cybersecurity, but the EU should go further following USA NERC example, organizing research of large-scale interdisciplinary attack scenarios, following the motto “Obscurity is not equal to security”
    8. Knowledge databases are used to share, and access known vulnerabilities
    9. Regular trainings are key to make our critical infrastructure resilient against cyber-attacks
- Future challenges
    1. Society and energy users need awareness about cybersecurity in the energy use

2. 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 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
7. Bio- and nano-technologies will 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 for energy systems

The identified topics of the clusters can be mapped back to four actors of a typical set of security services in smart energy systems (Xiao, 2013):

- Technology (improve compliance with standards, firewalls, gateways, antivirus, whitelisting, reactive security patterns, artificial intelligence learning, materials, crypto, progress)
- Policy (international platforms, EU wide regulations, laws, or guidelines, national frameworks, the local movements, expenditure in local economy, sector-specific taxes borne & collected and compliance)
- Process (audits, consulting, modelling tools, cloud applications, jobs and working conditions, on and off the job training and educational assistance, a communication network)
- People (training, certification, transparency, international exchange, awareness for flexibility)

These surrounding services help actors to identify, control, and manage security risks: Security Assessment, Secure Design and Implementation, Risk Management, Security Policy, Managed Security, and Incident Response Planning.

Being able to map topics to existing security services does not mean, current research and innovations in cybersecurity are obsolete. On the contrary. Our vision was to think forward to 2050 and from current trends and open issues try to identify important 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 will need to be adapted and revaluated. Also, the importance of each topic will vary from stakeholder to stakeholder. Our prioritization of the topics provided could be seen as a starting point and is as follows – but, due to the nature of a cross-cutting issues such as cybersecurity, this list will be different for each field, domain, or team of experts and time undertaken:

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. One thing we are certain about is that there will be no one-size-fits-all solutions and hence, the need for increasing cybersecurity research along every development of technology and society, now and in any foreseeable future.

A recent analysis and survey work (van der Meulen & Pettey, 2017), predicts that the cybersecurity market is expected to grow 19% to USD $90 billion this year. It also predicts that the top areas of security spending over the next year will be around cloud security, next-generation firewall technology, email security, cyber asset and threat vulnerability, and identity access management. Although this is not explicitly referred in the report, these areas are evidently related to the energy industry. In fact, these areas need to be carefully interrelated with other areas of the energy sector.

In other words, and as already mentioned in our report above, the interdisciplinary nature of the cybersecurity issue for smart grids is apparent if not obvious. This accounts into several general or specific actions, out of whom we state the following as the ones not appropriately addressed so far:

- Energy Markets and Energy Cybersecurity: Next generation Power Grid allows any size of a renewable energy source as well as any consumer to participate in the energy market as a price-maker. This tightens and further strengthens the interlink between the existing economic and the power systems. Economic fluctuations may significantly affect the resilience of power infrastructure and vice versa. Studies that relate the emerging economic models and practices, in particular from their social and behavioural viewpoint to cybersecurity issues of energy systems are well justified.
- Internet and power grid: There exist a plethora of studies on the interplay between the internet and the power grid. This interplay involves common essential concepts but differ on crucial subjects ranging from conceptual ones to technical ones. For example, the internet is capacity-driven while the smart grid is demand driven while both data and power may be transferred on the same physical layer and benefit from the same emerging technologies like blockchain. The existing studies could provide the background for searching cybersecurity solutions through concrete research efforts along their lines and a clearer view.

3.6 OUTLOOK – ETIP SNET – IMPLEMENTATION PLANS

As stated in the introduction ETIP SNET is the main consultation body for the EC to get the advice from the industry, academia, research community, etc. and, in brief, all the stakeholders involved in the research, development and innovation (RD&I) need to achieve a European energy system which will ensure a sustainable economic growth.

As per the following pyramid schematic, once a Vision for 2050 is agreed upon, a road map of RD&I needs for the next 10 years should be established with the purpose of creating the appropriate framework and comprehensive catalogue so as to set up the Implementation Plans[94] for three year period as the main practical tool to be used by the EC and the member states in deciding/updating the SET PLAN within the H2020 overall program.

[94] SET PLAN: https://setis.ec.europa.eu/actions-towards-implementing-integrated-set-plan/implementation-plans

As the period of consideration is shortening (32, 10, 3 years), the accuracy of establishing the targets is increasing. Therefore, the Vision will be a description of what the platform would like to have in 2050, rather than a prediction of that future. Based significantly on the three pillars of our Energy system (i.e., sustainability, market competitiveness and security of supply), the Vision is going to be completed in a short-term, targeting its official publication by June 2018.

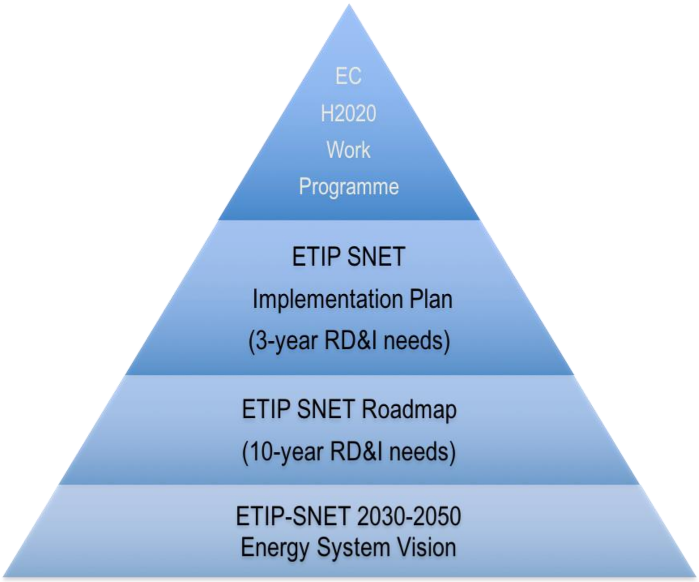


Figure 41: Overview of the ETIP SNET documents

Furthermore, the drafting of the 10 years road map will commence within the year, once its structure is discussed and agreed. The update of an improved knowledge sharing platform will be instrumental to facilitate the work, which, at the end, will be covered by the platform working groups (WG):

- WG1: Reliable, economic and efficient smart grid system
- WG2: Storage technologies and sector interfaces
- WG3: Flexible Generation
- WG4: Digitalization of the electricity system and Customer participation
- WG5: Innovation implementation in the business environment

Each of these groups' members will contribute with their activities and documents, within their assigned area, to the overall aforementioned platform plan.

4. DIRECTORIES

4.1 REFERENCES

A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. (2016). *IEEE Commun. Surv. Tutorials, 18*(2), 1153–1176.

ABI Research. (n.d.). *Modern Cybersecurity Totally Futile in Quantum Computing Era.* Retrieved from https://www.prnewswire.com/news-releases/modern-cybersecurity-totally-futile-in-quantum-computing-era-300541567.htm

Ball, P. (2016). Man Made: A History of Synthetic Life | Science History Institute. *Science History Institute," Distillations, 2*(1), 15–23.

Barzilay, O. (2017). *3 Ways Blockchain Is Revolutionizing Cybersecurity,.* Retrieved 03 2018, from https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-blockchain-is-revolutionizing-cybersecurity/#28e7c4352334.

Bhuiyan, J. (n.d.). *A federal agency says an overreliance on Tesla's Autopilot contributed to a fatal crash.* Retrieved 03 2018, from https://www.recode.net/2017/9/12/16294510/fatal-tesla-crash-self-driving-elon-musk-autopilot

Bhuiyan, J. (n.d.). *Police have released the first video from inside the Uber self-driving car that killed a pedestrian.* Retrieved 03 2018, from https://www.recode.net/2018/3/21/17149428/uber-self-driving-fatal-accident-video-tempe-arizona.

Booz, Allen, & Hamilton. (2017). 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk. *Frost & Sullivan*, p. 8.

Bubolz, M. (n.d.). *Digitalisierung und Transformation in Unternehmen: Strategien und Konzepte.*

Burr, W. (Electronic Authentication Guideline). Electronic Authentication Guideline. *2*.

Butterfill, J. (n.d.). *Quantum computing brings cyber security apocalypse.* Retrieved 03 2018, from http://www.investmenteurope.net/opinion/quantum-computing-brings-cyber-security-apocalypse/.

Câmara, S., Anand, D., & Pillitteri, V. (2016). Multicast delayed authentication for streaming synchrophasor data in the smart grid. *IFIP Adv. Inf. Commun. Technol.,, 471*, 32–46.

Carpenter , G., & Wyman, O. (20166). *Continental European Cyber Risk Survey 2016 Report.*

Christian, N. (n.d.). A Domain-Specific, Model Driven Engineering Approach for Systems Engineering in the Smart Grid.

Corbin, J. (2017). *Bringing the Power of Watson and Cognitive Computing to the Security Operations Center," IBM, SecurityIntelligence, 2017.* Retrieved from https://securityintelligence.com/bringing-the-power-of-watson-and-cognitive-into-the-security-operations-center/

D'Arco, S., Suul, , J., & Guidi, G. (2016). Virtual Synchronous Machine-Based Control of a Single-Phase Bi-Directional Battery Charger for Providing Vehicle-to-Grid Services. *IEEE Transactions on Industry Applications, 52*(4), IEEE Transactions on Industry Applications.

Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination FINAL REPORT. (n.d.).

Denney, E., Pai, G., & Whiteside, I. (2017). Model-driven Development of Safety Architectures. *20th International Conference on Model Driven Engineering Languages and Systems.*

Dockrill, P. (2018). *Bitcoin Could Become Illegal Almost Everywhere, After Shocking Discovery in The Blockchain.* ScienceAlert.

Dorri, A., Kanhere, S., & Jurdak, R. (2016.). *Blockchain in internet of things: Challenges and Solutions.*

Dunin-Kiplic, B., & Verbrugge, R. (2010). Teamwork in Multi-Agent Systems. Chichester, UK: John Wiley & Sons, Ltd,.

Eder-Neuhauser, Zseby, T., & Fabini, J. (2017). Cyber Attack Models for Smart Grid Environments, In Sustainable Energy," Sustain. Energy, Grids Networks. *Sustain. Energy, Grids Networks, 12*.

Elowitz, M. B., & Leibler, S. (2020). A synthetic oscillatory network of transcriptional regulators. *Nature, 403*(6767), 335–338.

Emmadi, N., & Narumanchi, H. (2017). Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure. *Proceedings of the 18th International Conference on Distributed Computing and Networking - ICDCN '17*.

ENISA . (n.d.). *ENISA looks into the Crystal Ball: a report on emerging technologies and security challenges*. Retrieved 03 2018, from https://www.enisa.europa.eu/news/enisa-news/enisa-looks-into-the-crystal-ball.

ETIP SNET. (n.d.). *ETIP SNET website*. Retrieved from https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf

Eurelectric. (2011). *Flexible generation: Backing up renewables.* Retrieved from https://www.google.com/search?q=EURELECTRIC+%282011%29+%3A+%E2%80%9CFlexible+generation%3A+Backing+up+renewables&ie=utf-8&oe=utf-8&client=firefox-b

Euroean Commission. (2016, 07). *DIRECTIVE (EU) 2016/ 1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 6 July 2016 - concerning measures for a high common level of security of network and information systems across the Union.* Retrieved 03 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

European Commission. (n.d.). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF THE REGIONS AND THE EUROPEAN INVESTMENT BANK A Framework Strategy for a Resilient Energy Union with a Forward-Looking* . Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:80:FIN

European Commission. (2005, 01). *Directive 85/2009 EC concerning measures to safeguard security of electricity supply and infrastructure investment.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0089

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Retrieved 03 2018, from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2016). *A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate* . Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0001.03/DOC_1&format=PDF

European Commission. (2016, 02). *An EU Strategy on Heating and Cooling.* Retrieved 07 2018, from https://ec.europa.eu/energy/sites/ener/files/documents/1_EN_ACT_part1_v14.pdf

European Commission. (2016, 11). *Clean Energy for All Europeans* . Retrieved from https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans

European Commission. (2017). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the &quot;EU Cybersecurity Agency&quot;, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity.* Retrieved 03 2018, from https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

European Commission. (n.d.). *Action of the European Commission on Digital Single Market*. Retrieved from https://ec.europa.eu/digital-single-market/en/policies/76026/3786.

European Commission. (n.d.). *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 Energy Research Knowledge Centre. (2014). *Research Challenges to Increase the Flexibility of Power Systems.* Retrieved from https://setis.ec.europa.eu/energy-research/sites/default/files/library/ERKC_PB_Flexibility.pdf

European Commission. (n.d.). *Winter Package of the European Commission*. Retrieved from https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/clean-energy-all-europeans

Farhangi, H. (2010). The path of the smart grid. *IEEE Power Energy Mag, 8*(1), IEEE Power Energy Mag.

Fulli, G., Masera, M., & Covrig, C. (2017). The EU electricity security decision-analytic framework: Status and perspective developments. *Energies, 10*(4), 1–20.

Gannud, H., Wu, H., & Timoney, J. (2017). Applying a MDE approach to a healthcare environment: A case study of an AE dept,. *28th Irish Signals and Systems Conference (ISSC).*

Gao, X., Sossan, F., Christakou, K., Paolone , M., & Liserre, , M. (2018). Concurrent Voltage Control and Dispatch of Active Distribution Networks by Means of Smart Transformer and Storage. *IEEE Transactions on Industrial Electronics, 65*(8), 6657-6666.

Gassmann , O., & Sutter, P. (2016). *gestalten Gescha¨ftsmodelle, Erfolgsfaktoren, Handlungsanweisungen, Fallstudien Hanser, .*

Gerard , H. (2016). *D.1.3 Basic schemes for TSO-DSO coordination and ancillary services provision*. Retrieved from http://smartnet-project.eu/wp-content/uploads/2016/12/D1.3_20161202_V1.0.pdf

Gerossier, A. (2017). Probabilistic day-ahead forecasting of household electricity demand. *CIRED - Open Access Proceedings Journal, IET*.

Gibson, D. G. (2010). Creation of a bacterial cell controlled by a chemically synthesized genome. *Science, 329*(5987), 52–6.

Gottschalk, M., Uslar, M., & Delfs, C. (n.d.). *The use case and smart grid architecture model approach : the IEC 62559-2 use case template and the SGAM applied in various domains.*

Green, A. A., Kim, J., & MA, D. (2017). Complex cellular logic computation using ribocomputing devices. *Nature, 548*(7665), 117–121.

Group, S. G. (2012). *Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deploymen.*

Halpin , H., & Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain. *IEEE European Symposium on Security and Privacy Workshops* , 1-3.

Hutterer, S., Hauer, W., & Meindl, J. (n.d.). Secure Integration and Rollout of IEC 61850-Based Smart Components Within the iniGrid Project. *2015*, 15–18.

IDE4L project . (n.d.). *IDE4L project final report.* Retrieved from http://www.tut.fi/eee/ide4l/D3.2/ide4l-d3.2-final.pdf

IETF. (n.d.). *A Firmware Update Architecture for Internet of Things Devices.* Retrieved 03 2018, from IETF

International Energy Agency. (2017). Digitalization and Energy.

J. Rocabert, Luna, A., Blaabjerg , F., & Rodriguez, P. (2012). Control of Power Converters in AC Microgrids. *IEEE Transactions on Power Electronics, vol. 27*(11), 4734-4749.

Kariniotakis, G. (June 2017). Renewable Energy Forecasting – From Models to Applications. *Woodhead Publishing/Elsevier*.

Kleineidam, G., Jung, G., & Woeltche, A. (2017). Cost Impact Simulation of Blackouts within the Electrical Grid. *International ETG Congress.*

Krieg, C., Rathmair, M., & Schupfer, F. (2014). A Process for the Detection of Design-Level Hardware Trojans Using Verification Methods. *IEEE Intl Conf on High Performance Computing and Communications.*

Kumar, M. (2016). *NIST Calls Development of Quantum-Proof Encryption Algorithms.* Retrieved from https://thehackernews.com/2016/12/quantum-computing-encryption.html.

Liao, S. (n.d.). Satellite-relayed intercontinental quantum network.

Lin, P., Abney, K., & Abney, G. A. (2012). Robot ethics?: the ethical and social implications of robotics. *George A*.

Liu, Q., Xing, L., & Wang, C. (2017). Framework of Probabilistic Risk Assessment for Security and Reliability. *IEEE Second International Conference on Data Science in Cyberspace (DSC)*, (pp. 619–624).

Luu, L., Chu, D., & Olickel, H. (2016). Making Smart Contracts Smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, 254–269.

Mailloux, L., Lewis, C., & Riggs, C. (2016). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals,. *IT Prof, 18*(5), 42–47.

McArthur , S. (2002). Multi-Agent Systems for Power Engineering Applications—Part I: Concepts, Approaches, and Technical Challenges. *IEEE Transactions on Power Systems, 22*(4), 1743-1752.

Michiorri , A. (2015). Forecasting for Dynamic Line Rating. *Renewable &Sustainable Energy Reviews, 52*, 1713-1730.

MIT Energy Initiative. (2016). *UTILITY OF THE FUTURE.*

MIT Technology Review. (n.d.). *Walmart's new robots are loved by staff—and ignored by customers.* Retrieved 03 2018, from MIT Technology Review

Mitleton-Kelly, E. (2013). *Co-evolution of intelligent socio-technical systems?: modelling and applications in large scale emergency and transport domains.* Springer.

Moinet, A., & Darties, B. (2017). *Blockchain based trust &amp; authentication for decentralized sensor networks.*

Moreno-Munoz, A., Bellido-Outeirino, F., & Siano, P. (2016). Mobile social media for smart grids customer engagement: Emerging trends and challenges. *Renewable and Sustainable Energy Reviews, 53*, 1611-1616.

Morozov, S., Maiti, A., & Schaumont, P. (n.d.). Comparative Analysis of Delay Based PUF Implementations on FPGA.

Mullin, E. (n.d.). *A biotech CEO explains why he injected himself with a DIY herpes treatment on Facebook Live - MIT Technology Review*. Retrieved 03 2018, from https://www.technologyreview.com/s/610179/a-biotech-ceo-explains-why-he-injected-himself-with-a-diy-herpes-treatment-live-on-stage/

Murphy, R., & Murphy, D. D. (2009). Beyond Asimov: The Three Laws of Responsible Robotics. *IEEE Intell. Syst, 24*(4), 14–20.

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

National Infrastructure Protection Plan | Homeland Security. (2018, 03 22). Retrieved from https://www.dhs.gov/national-infrastructure-protection-plan#0

Ozay, M., & Esnaola, I. (2015). Machine Learning Methods for Attack Detection in the Smart Gri.

PandaSecurity. (2017). *The Impact of the Blockchain on Cybersecurity,.* Retrieved 03 2018, from PandaSecurity

Pandey , R., & Misra, M. (2016). Cyber security threats — Smart grid infrastructure. *National Power Systems Conference (NPSC).*

pecial Eurobarometer 464a: Europeans. (n.d.). Retrieved 03 22, 2018, from https://data.europa.eu/euodp/data/dataset/S2171_87_4_464A_ENG.

Pedro, , H., Inman, R., & Coimbra, , C. (Woodhead Publishing/Elsevier). Mathematical ethods for optimised solar forecaqsting. *Renewable Energy Forecasting – From Models to Apllication, June 2017*.

Perrig, A., Canetti, R., & Song, D. (Proc. Internet Soc. Netw. Distrib. Syst. Secur. Symp). Efficient and Secure Source Authentication for Multicast. *2001.*

Pieltain Fernande, L., Gomez San Roman, T., & Cossent, R. (2011). Assessment of the Impact of Plug-in Electric Vehicles on Distribution Networks. *IEEE Trans. Power Syst, 26*(1), 206–213.

Qiu, R., & Antonik, P. (n.d.). *Smart grid using big data analytics. .*

Reichl, J. (2013). Power Outage Cost Evaluation: Reasoning, Methods and an Application. *J. Sci. Res. Reports, 2*(1), 249–276.

Rogers , J., & Wang,, A. (2012). Peer to peer electricity. *AXL, Inc*.

Schneier, B. (2017). *Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection.* Retrieved from https://www.schneier.com/essays/archives/2017/11/testimony_before_the_1.html

Shachtman, N. (n.d.). *Pentagon’s cyborg beetle spies take off,” Wired.com, 2009.* Retrieved 03 2018, from Shachtman

Smart Grid Coordination Group. (2012). *Smart Grid Coordination Group - Smart Grid Reference Architecture.*

Smart Grids Task Force - Expert Group 3. (2015). *Regulatory Recommendations for the Deployment of Flexibility: SGTF-EG3 Report,.* Retrieved 07 2018, from https://ec.europa.eu/energy/sites/ener/files/documents/EG3%20Final%20-%20January%202015.pdf

SmartNet project. (2016-2018). *SmartNet project*. Retrieved from http://smartnet-project.eu/

Stevens , G. (IEEE Electrical Insulation Conference (EIC),). Balanced nanocomposite thermosetting materials for HVDC and AC applications. *2015.*

Strasser, T. (2015, 04). A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems. *IEEE Trans. Ind. Electron.*,, pp. 2424–2438.

Tan, S., & De, D. (2017). Survey of Security Advances in Smart Grid: A Data Driven Approac. *IEEE Commun. Surv. Tutorials, 19*(1), 397–422.

Teaching an Learning Elementary Social Studies, A. K. (2013). Teaching an Learning Elementary Social Studies.

TenneT. (https://www.tennet.eu/de/unsere-kernaufgaben/innovationen/mobile-sensordaten, 2018 03). *Mobile Sensordaten - TenneT.*

The CIS Critical Security Controls for Effective Cyber Defense, Center for Internet Security. (2018, 03). Retrieved from https://www.cisecurity.org/controls/.

The Smart Grid Interoperability Panel and Smart Grid Cybersecurity Committee. (n.d.). *NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 1 -Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirement.*

The Smart Grid Interoperability Panel Cyber Security Working Group. (2010). *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security.*

Totzke, S. (2017). *How quantum computing increases cybersecurity risks.* Retrieved 03 2018, from https://www.csoonline.com/article/3197366/security/how-quantum-computing-increases-cybersecurity-risks.html

van der Meulen, R., & Pettey, C. (2017). Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017. Pettey.

Vingerhoets, , P., Chebbo, M., & Hatziargyriou, N. (2018, 03 22). *The Digital Energy System 4.0 – ETP Smartgrids.* Retrieved from https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf

Vormayr, Zseby, T., & Fabini, J. (2017). Botnet Communication Patterns. *IEEE Commun. Surv. Tutorials,*.

WANG, J., LIU, X., & WANG, X. (2006). Artificial Immune System and Analysis of Its Models. *Comput. Technol. Dev, 7*, 35.

Wen, M., Lu, R., & Liang, X. (2014). *Querying over Encrypted Data in Smart Grids.* Springer International Publishing.

Weyrich , M., & Ebert, C. (2016). Reference Architectures for the Internet of Thing. *Ebert, 33*(1), 112–116.

Wood, G. (2018). *Ethereum: A secure decentralized transaction ledger byzantium version.*

Xiao. (2013). *Security and Privacy in Smart Grids.* CRC Press.

Xin, X., Xin, J. P., & Gaj, K. (2011). A Configurable Ring-Oscillator-Based PUF for Xilinx FPGA. *14th Euromicro Conference on Digital System Design.*

Yampolskiy, R. (2017). *AI Is the Future of Cybersecurity, for Better and for Worse.* Harvard Business Review.

Yan, Y., Qian, Y., & Sharif, H. (2012). A Survey on Cyber Security for Smart Grid Communications. In *IEEE Commun. Surv. Tutorials* (pp. 998–1010).

Yao, R., Huang, S., & Sun, K. (2016). A Multi-Timescale Quasi-Dynamic Model for Simulation of Cascading Outages. *IEEE Trans. Power Syst., , 31*(4), IEEE Trans. Power Syst., .

Zhang, M., Wang, L., & Jajodia, S. (2016). Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks. *IEEE Trans. Inf. Forensics Secur, 11*(5), 1071–1086.

Zhao, J., Mili, F., & Milano, F. (n.d.). Robust Frequency Divider for Power System Online Monitoring and Control. *IEEE Transactions on Power Systems*.

Zheng, J., Y, L., & Hou, Y. (2017). BMNR: Design and Implementation a Benchmark for Metrics of Network Robustness. *IEEE International Conference on Big Knowledge (ICBK).*

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, 180–184.

4.2 ABBREVIATIONS

3-D	3 Dimensional
3GPP	3rd Generation Partnership Project
4G	4th Generation (wireless systems)
5G	5th Generation (wireless systems)
6LoWPAN	Internet Protocol version 6 over Low-Power Wireless Personal Area Networks
AC	Alternating Current
AEC	Advanced Encryption Standard (128/256)
aFRR	automatic Frequency Restoration Reserve
AI	Artificial Intelligence
AIC	Availability, Integrity, Confidentiality
AIOTI	Alliance for Internet of Things Innovation
AL	Adapters Layer
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Augmented Reality
ART	Accountability, Reliability and Transparency
ATIS	Alliance for Telecommunications Industry Solutions
BES	Bulk Electricity System
BiDi	Bidirectional
BPL	Broadband over Powerline
BR/EDR	Basic Rate/Enhanced Data Rate
BRP	Balance Responsible Party
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPEX	Capital Expenditures
CCGT	Combined-Cycle Gas Turbine
CECOVEL	Control Centre for Electric Vehicle
CEI	Critical Energy Infrastructures
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Computer Emergency Response Team
CHP	Combined Heat and Power
CIA	Confidentiality, Integrity, Availability
CIP	Critical Infrastructure Protection
CoAP	Constrained Application Protoco
CPS	Cyber Physical Systems
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSS	Cascading Style Sheet
CWDM	Coarse Wave Division Multiplexing
DALL	Data Access Logic Layer
DB	Database
DBPSK	Differential Phase-Shift Keying
DC	Direct Current
DDoS	Distributed Denial of Service (attack)
DEP	Data Exchange Platform
DER	Distributed Energy Resources

DLC	Direct Load Control
DLR	Dynamic Line Rating
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DQPSK	Differential Quadrature Phase Shift Keying
DR	Demand Response
DSL	Digital Subscriber Line
DSLL	Data Storage Logic Layer
DSO	Distribution System Operator
DSSS	Direct Sequence Spread Spectrum
DTLS	Datagram Transport Layer Security
DWDM	Dense Wavelength Division Multiplexing
EBITDA	Earnings Before Interest, Taxes, Depreciation, and Amortization
EBS	Eurobarometer on Cybersecurity
EC	European Commission
EDFA	Erbium Doped-Fibre Amplifier
EECSP	Energy Expert Cyber Security Platform
EG	Expert Group
EGPRS	Enhanced General Packet Radio Service
EHF	Extremely High Frequency
EISA	Energy Independence and Security Act (in the USA)
EMS	Energy Management System
ENISA	European Network and Information Security Agency
ENTSO-E	European Network of Transmission System Operators-Energy
EPON	Ethernet Passive Optical Network
ESCO	Energy Service Company
ETIP	European Technology & Innovation Platform
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
EXE	Energy Exchange Enablers
FACTS	Flexible Alternating Current Transmission System
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FLISR	Fault Location Identification and System Restoration
FR	Far Range
FSS	Fixed-Service Satellite
FTTC	Fiber to the Curb/Cabinet, Closet
FTTH	Fiber to the Home
G3-PLC	Generation 3 Power Line Carrier
GA	Genetic Algorithms
GDPR	General Data Protection Regulation
GEO	Geostationary Orbit
GMSK	Gaussian Minimum Shift Keying
GOOSE	Generic Object Oriented Substations Events
GPU	Graphics Processing Unit
GSM	Groupe Spécial Mobile (engl. Global System for Mobile Communications)
GSMA	Global System for Mobile Communications Association
H2020	Horizon 2020
HaLow	IEEE 802.11ah, pronounced "HEY-Low"
HART	Highway Addressable Remote Transducer
HD-PLC	High Definition Power Line Communication

HEMS	Home Energy Management System
HMAC-SHA256	Hash-based Message Authentication Code-Secure Hash Algorithm with key length 256
HTML	Hypertext Markup Language
HTS	High-Throughput Satellite
HVDC	High-Voltage, Direct Current
IBM	International Business Machines
ICO	Initial Coin Offering
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IDE4L	Ideal Grid for All
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMT	International Mobile Communications
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	(NIST) Internal Report
ISA	International Society of Automation
ISO	International Organization for Standardization
ISOC	Integrated Security Operation Centre
IT	Information Technology
ITU	International Telecommunications Union
JOIN	Joint Communication (of the European Commission and the European External Action Service)
KPI	Key Performance Indicator
LAN	Local Area Network
LE	Low Energy
LEC	Local Energy Communities
LIDAR	Laser Detection and Ranging
LoRaWAN	Long Range Wide Area Network
Low Earth Orbit	Low Earth Orbit
LPWA	Low Power Wide Area
LPWA	Low-Power Wide-Area
LR	Long Range
LTE	Long Term Evolution
LTE-M	Long Term Evolution – Mobile
LV	Low Voltage
M/490	(Smart Grid) Mandate 490 (of the European Commission)
M2M	Machine to Machine (communication)
MAC	Medium Access Control
MDF	Medium Dispersion Fibre
MEO	Medium Earth Orbit
MMORPG	Massively Multiplayer Online Role-Playing Game
MSS	Mobile-Satellite Service
MSS	Mobile-Satellite Service
MV	Medium Voltage
MVP	Minimum Viable Product
NB PLC	Narrow Band Power Line Carrier
NB-IoT	Narrow Band-Internet of Things
NFV	Network Function Virtualisation
NILM	Non-Intrusive Load Monitoring

NIPP	National Infrastructure Protection Plan
NIS	Network and Information Security (Directive)
NIST	National Institute of Standards and Technologies
NN	Neural Networks
NR	New Radio
NRA	National Regulatory Authorities
NSA	Non-Stand Alone
NZ-DSF	NonZero Dispersion-Shifted Fibre
O-QPSK	Offset Quadrature Phase Shift Keying
OC	Optical Carrier
OCSP	Online Certificate Status Protocol
OFDM	Orthogonal Frequency-Division Multiplexing
OFDM	Orthogonal Frequency-Division Multiplexing
OHL	OverHead Lines
OPC-UA	Open Platform Communications Unified Architecture
OPERA	Open Power Line Carrier European Research Alliance
OPEX	Operating Expenses
OT	Operational Technology
OTN	Optical Transport Network
PFR	Primary Frequency Response
PHY	physical layer of the Open Systems Interconnection model
PLC	Power Line Carrier
PMU	Phasor Measurement Unit
PoC	Proof of Concept
PoH	Point on the Horizon
PPP	Public Private Partnership
PRIME	PoweRline Intelligent Metering Evolution
PUF	Physical Unclonable Functions
PV	Photovoltaic
Q/V	Volumetric Flow Rate
Qbit	Quantum bit
QKD	Quantum Key Distribution
QoS	Quality of Supply
R&D	Research and Development
R&I	Research and Innovation
RBAC	Role Based Access Control
RD&I	Research, Development & Innovation
REC	Regional/Renewable Energy Communities
RES	Renewable Energy Resource
RF	Radio Frequency
RL	Reinforcement Learning
RNA	Ribonucleic Acid
ROCOF	Rate of Change of Frequency
RSA	Rivest Shamir Adleman
RTDS	Real Time Dynamic Simulation System
RTU	Remote Terminal Unit
SAAS	Software As A Service
SAIDI	System Average Interruption Duration Index
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Networks
SEP	Smart Energy Platform
SET Plan	Strategic Energy Technology Plan

SFR	Secondary Frequency Response
SGAM	Smart Grid Architecture Model
SGIS	Smart Grid Information Security
SIG	Special Interest Group
SME	Small and Medium Enterprise
SNET	Smart Networks for Energy Transition
SOA	Service-Oriented Architecture
SONET	Synchronous Optical NETwork
SPARKS	Smart Grid Protection Against Cyber Attacks
SR	Short Range
SUN	Smart Utility Networks
SVG	Scalable Vector Graphic
T&D Europe	European Transmission and Distribution (association)
TB	Terabyte
TCP	Transport Control Protocol
TDM	Time Division Multiplexing
TDMA	Time-Division Multiple Access
TF	Task Force
TLS	Transport Layer Security
TSDB	Time Series Database
TSG	Technical Specification Group
TSO	Transmission System Operator
TTF	Title Transfer Facility
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UE	User Equipment
UHF	Ultra High Frequency
USA	United States of America
V2G	Vehicle to Grid
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VHF	Very High Frequency
VR	Virtual Reality
vRES	variable Renewable Energy Sources
VSAT	Very Small Aperture Terminal
WDM	Wavelength Division Multiplexing
WG	Working Group
Wi-Fi	Wireless Fidelity
WiGig	Wireless Gigabit Alliance
WPAN	Wireless Personal Area Network
XML	eXtensible Markup Language
ZigBee	ZigZag like a Bee

4.3 APPENDIX CYBERSECURITY

To provide further information on cybersecurity and relevant issues and recommendations, technologies, and contacts, this section put together relevant documents in categories, providing vertical information on current policy situations, technology standards, and organizations to contact for current developments.

4.3.1 RECOMMENDATIONS AND GUIDELINES

NERC CIP	www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
BDEW White Paper Requirements for Secure Control and Telecommunication Systems – defining basic security measures and requirements	https://www.bdew.de/media/documents/Awh_20150331_OE-BDEW-Whitepaper-Secure-Systems.pdf
CEN-CENELEC-ETSI SG-CG report on Smart Grid Information Security (M/490)	ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf
CIGRE JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems	https://e-cigre.org/publication/317-security-for-information-systems-and-intranets-in-electric-power-systems
EECSP-Final Report Cyber Security in the Energy Sector	http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=30396&no=1
EG2: General Data Protection Regulation (GDPR)	http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
NIST Cyber Security Framework	www.nist.gov/cyberframework
NIST IR 7628 (from Smart Grid Interoperability Panel – Cyber Security WG),NIST Guidelines for Smart Grid Cybersecurity	http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
NIST Second Draft Update to Cybersecurity Framework	https://www.nist.gov/cybersecurity-framework/cybersecurity-framework-draft-version-11
NIST SP 1108R2, NIST Framework and	https://www.nist.gov/sites/default/files/documents/smartgrid/NIST_Framework_Release_2-

Roadmap for Smart Grid Interoperability Standards	0_corr.pdf
NIST SP 800-184 Guide for Cybersecurity Event Recovery	http://doi.org/10.6028/NIST.SP.800-184
NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security	https://doi.org/10.6028/NIST.SP.800-82r2
NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53.pdf
Report of the Task Force Smart Grid Expert Group 2 – Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection	https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf
SG3 - SMB/4175/R - Smart Grid Standardization Roadmap	http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf
U.S. Department of Homeland Security: The Catalog of Control Systems Security - Recommendations for Standards Developers	https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf
WG D2.22, Information Security for Electric Power Utilities	https://e-cigre.org/publication/D2-206_2010-information-security-for-electric-power-utilities--results-of-cigre-wg-d222

4.3.2 CONTACTS AND ORGANIZATIONS

This subsection should provide further points of contact to get in touch with more experts on the topic, new research around cybersecurity, as well as provide more information on currently used technologies in running or successful projects:

European Energy – Information Sharing and Analysis Center	www.ee-isac.eu
International Electrotechnical Commission - IEC	http://www.iec.ch
National Institute of Standards and Technology – NIST	https://www.nist.gov

International Organization for Standardization – ISO	https://www.iso.org/
Deutsches Institut für Normung – DIN	https://www.din.de/en
IEC Smart Grid Strategic Group – SG3	http://www.iec.ch/smartgrid/development/
IEC Technical Committee 57 Working Group 15 (ISO/IEC TC57 WG15)	data and communication security for power system management http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2389,25#
International Society of Automation - ISA	https://www.isa.org
The International Council on Large Electronic Systems -– CIGRE	www.cigre.org
North American Electric Reliability Corporation – NERC	https://www.nerc.com/
U.S. Federal Energy Regulatory Commission	https://www.ferc.gov/
Internet Engineering Task Force – IETF	https://www.ietf.org
World Wide Web Consortium – W3C	https://www.w3.org/
Bundesverband für Energie- und Wasserwirtschaft – BDEW	https://www.bdew.de/
European Union's Task Force Smart Grid	https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force
CEN/CENELEC/ETSI Smart Grid Coordination Group	https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx
European Committee for Standardization – CEN	https://www.cen.eu/
European Committee for Electrotechnical Standardization – CENELEC	https://www.cenelec.eu/
European Telecommunications Standards Institute – ETSI	www.etsi.org/

4.3.3 RELEVANT STANDARDS

IEC 62443	System Security in industrial communication
IEC 62351-1 to 11	Communication Security
ISO/IEC 27001/27019	Security Management
ISO/IEC TR 27019	Information security management guidelines ISO/IEC 27019:2017
IEEE C37.240	IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
IEC 62056	Electricity metering data exchange, DLMS/COSEM

IEEE 1686	Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
IETF GDOI Enhance	The Group Domain of Interpretation
ISO/IEC 15118	Road vehicles -- Vehicle to grid communication interface
IEC 62743	Radiation protection instrumentation - Electronic counting dosemeters for pulsed fields of ionizing radiation
ISO/IEC 61850-8-1	Specific communication service mapping (SCSM) - Mappings to Manufacturing Message Specification MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
ISO/IEC 27001/2	Information security management / Information technology -- Security techniques -- Code of practice for information security controls
ISO/IEC 19790	Information technology -- Security techniques -- Security requirements for cryptographic modules
IETF RFC 7252 CoAP	The Constrained Application Protocol (CoAP)
IETF RFC 6960 OCSP	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
IETF RFC 7030 EST	Enrollment over Secure Transport
IETF Draft TLS v1.3	The Transport Layer Security (TLS) Protocol Version 1.3 https://tools.ietf.org/html/draft-ietf-tls-tls13-28
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
IEC 62559	Use Case Template
ISO 27011	Mapping ISO27002 to telecomunication
DIN SPEC 27009	Mapping ISO27002 to electric utility domain
IEC 60870-x	Energy Automation
ICCP	TASE.2, Control Center Communication
ISO 9506	messaging real-time process data and control
RFC 5246	Request for Comments TLS v1.2, Layer 4 security
ISA 99	Security for Industrial Automation and Control Systems
IEEE 802.1X	Port Based Network Access Control
ISO/IEC 17799	predecessor of ISO 27000
CIP-002 to CIP-011	Critical Infrastructure Protection Cyber Security Standards
RFC 6272	Internet Protocols for the Smart Grid
RFC 3711	Secure Real-Time Transport Protocol (SRTP)
RFC 4101 4102 4103	base standards for IPSec, Layer 3 security
RFC 4962	Authentication, Authorization, and Accounting (AAA)
RFC 5247	Extensible Authentication Protocol (EAP)
RFC 5746	Datagram Transport Layer Security (DTLS)
RFC 6407	Group Domain of Interpretation (GDOI)
IETF Draft moran-suit-architecture	A Firmware Update Architecture for Internet of Things Devices https://tools.ietf.org/html/draft-moran-suit-architecture-03

IEC 61850-90-5	Addresses security for synchrophasor communication in terms of integrity (based on HMAC) and optional confidentiality (using AES) for key management

4.3.4 CYBER-ATTACKS REPORTS LIST

Covering the contents of the picture in chapter “Increasing cyber-attacks”, this is a non exhaustive list of reported and discovered cyber-attacks, mostly related to the energy sector over the last years:

- http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf
- http://docplayer.org/501374-Cyber-risiken-und-sicherheitsansaetze-fuer-die-energiebranche.html
- http://resources.crowdstrike.com/putterpanda/
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
- https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf
- https://securelist.com/files/2014/07/Kaspersky_Lab_crouching_yeti_appendixes_eng_final.pdf
- https://securelist.com/files/2014/08/KL_Epic_Turla_Technical_Appendix_20140806.pdf
- http://threatc.s3-website-us-east-1.amazonaws.com/?/arachnophobia
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
- http://www.isightpartners.com/2014/10/cve-2014-4114/
- http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-rotten-tomato-campaign.pdf
- http://www.invincea.com/wp-content/uploads/2014/10/Micro-Targeted-Malvertising-WP-10-27-14-1.pdf
- http://novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf
- https://www.tigersecurity.pro/operation-distributed-dragons/papers/AR_ODD_EN20141020.pdf
- https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
- http://cylance.com/operation-cleaver
- https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf
- https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?_r=0
- https://twitter.com/olesovhcom/status/778019962036314112
- https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
- https://blog.radware.com/security/2017/04/hajime-futureproof-botnet/
- https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
- https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
- http://thehackernews.com/2016/11/heating-system-hacked.html
- https://www.engadget.com/2016/11/29/mirai-botnet-targets-deutsche-telekom-routers-in-global-cyberatt/
- https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings
- https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms

- https://motherboard.vice.com/en_us/article/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device
- https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html
- https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/
- https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
- https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/
- https://www.symantec.com/blogs/threat-intelligence/triton-malware-ics
- https://www.symantec.com/security-center/threat-report
- https://twit.tv/episodes?filter[shows]=1636

4.3.5 FURTHER READING

This is a non-exhaustive list of additional reading of scientific literature, describing further, more detailed, orthogonal, or adjacent related work to the topics presented in this position paper.

L.T. Berger and K. Iniewski. Smart Grid Applications, Communications, and Security. Wiley, 2012.
J.B. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama. Smart Grid: Technology and Applications. Wiley, 2012.
S. Jasanoff. The Ethics of Invention: Technology and the Human Future. W. W. Norton, 2016.
M. Sashinskaya. Smart Cities in Europe: Open Data in a Smart Mobility Context. CreateSpace Independent Publishing Platform, 2015.
L.L. Thomson and American Bar Association. Section of Science & Technology Law. Data Breach and Encryption Handbook. American Bar Association, 2011.
I. van de Poel and L. Royakkers. Ethics, Technology, and Engineering: An Introduction. Wiley, 2011.
B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen. A video game for cyber security training and awareness. Computers & security, 26(1):63–72, 2007
Y. Hong, S. Goel, and W. M. Liu. An efficient and privacy&#8208;preserving scheme for p2p energy exchange among smart microgrids. International Journal of Energy Research, 40(3):313–331, 2016
B. S. Rawal, S. Liang, A. Loukili, and Q. Duan. Anticipatory cyber security research – an ultimate technique for the first-move advantage. TEM Journal, 5(1):3–14, 2016
I. ARMENCHEVA. Aspects of policies and strategies for cyber security in the european union. Journal of Defense Resources Management, 6(2):37–44, 2015
J. Ferdinand. Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. Journal of Business Continuity & Emergency Planning, 9(2):185–195, 2015
Y. Wang, D. Ruan, J. Xu, M. Wen, and L. Deng. Computational intelligence algorithms analysis for smart grid cyber security. LECTURE NOTES IN COMPUTER SCIENCE, 1(6146):77–84, 2010
N. J. Hewitt. Contributing to a resilient energy union: an integrated energy storage and smart grid strategy? International Journal of Ambient Energy, 36(4):155–155, 07 2015.
C. Armour. Cyber resilience: Leadership matters. Cyber Security: A Peer-Reviewed Journal, 1(2):134– 146, 2017
M. Taddeo. Cyber security and individual rights, striking the right balance. PHILOSOPHY & TECHNOLOGY, 26(4):353–356, 2013
I. Nai Fovino, L. Guidi, M. Masera, and A. Stefanini. Cyber security assessment of a power plant. Electric power systems research, 81(2):518–526, 2011

Cyber security report 2013: Fast alle unternehmen schon mal von hackern attackiert. DATENSCHUTZ UND DATENSICHERHEIT, 38(1):64–64, 2014

Cyber-security needs attention now and not later. Computer fraud & security, 2002(2):5–5, 2002

B. Genge, P. Haller, C. Dumitru, and C. Enachescu. Designing optimal and resilient intrusion detection architectures for smart grids. IEEE TRANSACTIONS ON SMART GRID, 8(5):2440–2451, 2017

F. S. Tsai and K. L. Chan. Detecting cyber security threats in weblogs using probabilistic models. LECTURE NOTES IN COMPUTER SCIENCE, 1(4430):46–57, 2007

R. Fisher, M. Norman, and M. Klett. Enhancing infrastructure resilience through business continuity planning. Journal of Business Continuity & Emergency Planning, 11(2):163–173, 2017

M. T. Holzleitner. European provisions for cyber security in the smart grid; an overview of the nis-directive. ELEKTROTECHNIK UND INFORMATIONSTECHNIK, 134(1):14–18, 2017

J. Zerlang. GDPR: a milestone in convergence for cyber-security and compliance. Network security, 2017(6):8–11, 2017

H. Rosoff, J. Cui, and R. S. John. Heuristics and biases in cyber security dilemmas. ENVIRONMENT SYSTEMS & DECISIONS, 33(4):517–529, 2013

J. Botelho. How automating data collection can improve cyber-security. Network security, 2017(6):11–13, 2017

W. Boyer and M. McQueen. Ideal based cyber security technical metrics for control systems. LECTURE NOTES IN COMPUTER SCIENCE, 1(5141):246–260, 2008

N. Choucri, S. Madnick, and J. Ferwerda. Institutions for cyber security: International responses and global imperatives. Information Technology for Development, 20(2):96–121, 2014.

J. A. Renjit and K. L. Shunmuganathan. Multi-agent-based anomaly intrusion detection. Information Security Journal: A Global Perspective, 20(4-5):185–193, 2011

J. Shea. Nato: Stepping up its game in cyber defence. Cyber Security: A Peer-Reviewed Journal, 1(2):165–174, 2017

J. Xie, A. Stefanov, and C. Liu. Physical and cyber security in a smart grid environment. Wiley Interdisciplinary Reviews: Energy and Environment, 5(5):519–542, 2016.

Zhang, Ou, and Caragea. Predicting cyber risks through national vulnerability database. Information Security Journal: A Global Perspective, 24(4-5):194–206, 2015

X. Ye, J. Zhao, Y. Zhang, and F. Wen. Quantitative vulnerability assessment of cyber security for distribution automation systems. Energies, 8(6):5266–5286, 2015.

A. A. OUAHMAN. Security and privacy issues in cloud computing. Journal of Defense Resources Management, 5(2):99–108, 2014

S. Saran. Striving for an international consensus on cyber security: Lessons from the 20th century. Global Policy, 7(1):93–95, 2016

A. Sokolov, V. Mesropyan, and A. Chulok. Supply chain cyber security: A russian outlook. Technovation, 34(7):389–391, 2014

T. Scully. The cyber security threat stops in the boardroom. Journal of Business Continuity & Emergency Planning, 7(2):138–148, 2014.

I. Atoum, A. Otoom, and A. A. Ali. A holistic cyber security implementation framework. Information Management & Computer Security, 22(3):251–264, 2014.

S. Purser. The european cooperative approach to securing critical information infrastructure. Journal of Business Continuity & Emergency Planning, 5(3):237–245, 2011

R. Gustavsson and S. Hussain. The proper role of agents in future resilient smart grids. Communications in computer and information science, 1(430):226–237, 2014

Uk launches new cyber security strategy. Computer fraud & security, 1(12):3–3, 2011

K. Julisch. Understanding and overcoming cyber security anti-patterns. Computer networks, 57(10):2206– 2211, 2013
F. Hult and G. Sivanesan. What good cyber resilience looks like. Journal of Business Continuity & Emergency Planning, 7(2):112–125, 2014

5. ABOUT THE AUTHORS

The production of this document required us to look into the future, declaring our points of view on what areas of research we, as Europeans need to invest in now, for a digital, cyber secure, robust future energy system in the future. The authors want to thank the many experts and colleagues who were involved in the creation of this document, checking references, and providing review comments and feedback.

Aitor Amezua (ZIV, Spain) received his MSc. in Telecommunication Engineering from the University of the Basque Country in Bilbao in 1995. He has been working in the energy sector since 1992, always with a high component of innovation, new product and business development, especially in the field of renewable energy, energy efficiency, AMI, monitoring and distribution automation. Aitor has held several positions, among them, Customer Technical Assistance Engineer at Iberdrola Distribution, Energy Systems Manager at Millennium Energy, and Technical Manager of the power electronics and AMI business units at Ormazabal. In 2017 he joins ZIV and is now the Distribution Automation Business Unit Development Manager. He is an active member in the electric power community participating in many working groups, among them: WG SmartGrids&microGrids of T&D Europe, WG SmartGrids of AFBEL, WG4 Digitisation of the electricity system and Customer participation of the ETIP SNET, UNE CTN217, IEC SC8B Decentralized Electrical Energy Systems and has also been member of the Experts Group 1 dealing with interoperability of the SmartGrids Task Force of the European Commission.

Angel Conde (Ikerlan, Spain) IK4-Ikerlan is a leading knowledge transfer technological centre providing competitive value to companies.

Antonello Monti (RWTH Aachen University, Germany) received his M.Sc degree (summa cum laude) and his PhD in Electrical Engineering from Politecnico di Milano, Italy in 1989 and 1994 respectively. He started his career in Ansaldo Industria and then moved in 1995 to Politecnico di Milano as Assistant Professor. In 2000 he joined the Department of Electrical Engineering of the University of South Carolina (USA) as Associate and then Full Professor. Since 2008 he is the director of the Institute for Automation of Complex Power System within the E.ON Energy Research Center at RWTH Aachen University. Dr. Monti is author or co-author of more than 300 peer-reviewed papers published in international Journals and in the proceedings of International conferences. He is a Senior Member of IEEE, Associate Editor of the IEEE System Journal and Associate Editor of IEEE Electrification Magazine. Dr. Monti is the recipient of the 2017 IEEE Innovation in Societal Infrastructure Award.

Antonio Moreno-Munoz (Universidad de Córdoba, Spain) Antonio Moreno-Munoz (IEEE SM'09) is Professor at the Department of Electronics and Computer Engineering, Universidad de Córdoba, Spain where he is the Chair of the Industrial Electronics and Instrumentation R&D Group. From 2005 to 2017, he was the Director of the Department. He received his Ph.D. and M.Sc. degrees from UNED, Spain in 1998 and 1992, respectively. From 1981 to 1992 he was with RENFE, the Spanish National Railways Company. Since 1992 he has been with Universidad de Córdoba. He is currently Member of the Technical Committee on Smart Grids IEEE-IES. CIGRÉ-CIRED JWG-C4.24 committee member. R&D projects Auditor for European Quality Assurance Ltd. (EQA) and DNV-GL-Business Assurance. Springer Science consultant. Editor in Intelligent Industrial Systems Journal, (Springer Science), Guess Editor in Energies journal MDPI-AG and reviewer for numerous journals of IEEE, IET, and Elsevier. His main areas of research interest are Smart Grids, Power Quality, Electronic Instrumentation, and usability of complex systems, with over 130 technical publications.

Aris Dimeas (National Technical University of Athens, Greece) is a researcher at the Electrical and Computers Engineering Department of NTUA.

Arjan Wargers (**ElaadNL, Netherlands**) received a MSc degree in 2001 from the University of Groningen, Netherlands. Currently he is employed as Manager Innovation and Development Electric Mobility at ElaadNL and as DSO architect at Dutch DSO Enexis. Since 2010, his main research interests are in the field of Electric Vehicles, primarily aimed at grid integration of EV, Smart Charging and EV related protocols. He is a driving force behind the innovation and practical research executed at ElaadNL over the last seven years.

Asier Moltó (Red Eléctrica de España, Spain) in 2008 and since 2008 has been working in the Demand Side Management and Smart Grid field. More precisely he leads projects and initiatives aiming at preparing the operation of the electric system to the new energy model. He is an Industrial Engineer from the Universidad Politécnica de Madrid and completed his formation in the École Nationale des Ponts et Chaussées in Paris, where he started his professional career as strategy consultant in the European energy markets

Bruno Miguel Soares (R&D Nester, Centro de Investigação em Energia REN – State Grid S.A., Portugal) holds a master’s Degree in Electrical and Computers Engineering in Power Systems from the Faculty of Engineering of Porto University (FE/UP). His Master Thesis was developed in Protection and Automation Systems Department of REN (Portuguese TSO) and was focused in asset management related with protection relays. Bruno worked at the FE/UP where he was Teaching Assistant in Digital Systems Laboratory until January 2015. Since September 2015, Bruno is working in R&D Nester in one of its projects, called “Substation of the Future”. The scope of this project is to develop the technical specification for the near future PAC system of transmission substations (fully IEC61850) and performing the proof-of-concept of the designed system, using a testing platform that was developed by R&D Nester, the Real-Time Power System Simulation Laboratory. Bruno works in this experimental platform, where equipment and design can be tested with real-life conditions, but without effects in power grid. Bruno is member of CIGRE Working Group B5.60 (Protection, Automation and Control Architectures with Functionality Independent of Hardware). His main areas of research are substation’s Protection and Automation (secondary) systems and communication networks.

Christian Lechner (EVN AG, Austria) is working in the **Energy Planning Department** of a leading, international and publicly listed energy and environmental services company, with headquarters in Austria. Christian started working for EVN in 2015 with a Traineeship in Bulgaria. After that he continued as Project Manager responsible for Projects in the field of Demand Side Management, Virtual Power Plants and Smart Grids. Christian has a background in Electrical Engineering and studied at the Vienna University of Technology and at the Technical University of Lund.

Daniel Mugnier (TEC SOL, France) PhD. is head of the research department for solar-thermal and photovoltaic engineering. Moreover, he is the Vice Chairman of the IEA Solar Heating and Cooling program. He has been involved in numerous EU project on solar energy and has a long experience in developping solar thermal and PV projects from the engineering side. He coordinates from 2017 a specific French R&D project dedicated to photovoltaic distributed self-consumption using blockchain.

Elena Boskov-Kovacs (Blueprint Energy Solutions, Austria) Managing Director and co-founder of the Austrian think-tank, services and consulting company focused on bringing innovation and transformation to energy utilities and energy consumer services market. She has 15+ years of consulting and management experience, working for some of the biggest energy industry vendors, consultancies and smart grid system integrators across EMEA region. Working on several projects in Europe with gas and electricity system operators in designing framework for their digital strategy and new business services. She graduated at Department of Power Systems, Faculty of Electrical Engineering and holds an MSc on Electrical Engineering and IT and an MBA from Cotrugli Business School.

Eric Suignard (EDF R&D, France) Eric Suignard received an engineering degree in 1993 from Ecole Nationale Supérieure de Physique de Strasbourg engineering school and a post graduate university degree from Strasbourg Louis-Pasteur university. From 1994 to 2009, he worked in several IT consulting companies (e.g. Cap Gemini) and was involved in IT projects in several domains (e.g. defense, telecom manufacturer, telecom operator, retail banking, energy). In 2009, he joined EDF R&D as an enterprise architect. He currently works on research projects for EDF group entities such as French DSO Enedis.

Esther Hardi (Alliander, Netherlands) strategist and innovation manager with the largest regional infrastructure provider for electricity, gas and heat in the Netherlands. For 20 years she has been working in the energy business in the field of competitive strategy, innovation and business development. She has been a pioneer in biogas injection in the Dutch gas grid, in local energy solutions, and is actively involved in renewable sustainable energy supply. She supervises a number of major systems integration pilot projects, such as Power2gas, EBay for Energy, and Heat systems 2.0 in neighbourhoods. She co-chairs WG 4 of ETIPS NET - the European Technology and Innovation Platform “Smart Networks for Energy Transition” which aims to ensure that all energy customers and market actors can rely on optimally integrated networks, systems and markets. Esther holds an MSc in applied mathematics (Technical University of Delft) and is currently afilioated with TU Delft as a PhD research fellow. Prior to her career in Alliander, she worked for Schlumberger Offshore and with Nuon (Vattenfall).

George Huitema (TNO, The Netherlands) George Huitema holds a Master Degree (Cum Laude) in Mathematics from the University of Groningen and received his PhD in 1988. He then joined KPN Research. Since 2003, by the transfer of the R&D of KPN, he works for TNO where he is senior research scientist and project manager in the area of smart energy systems. At the development and innovation side he is one of the initiators of the Hybrid Energy System Integration (HESI) Facility in Groningen. George is professor of Telematics (ICT and Business) within the Faculty of Economics and Business of the University of Groningen. His research deals with service development and operations within businesses exploiting large infrastructures (like e.g. utilities, data, tele-communications). He currently supervises PhDs focusing on facilitating the growth of energy communities, assessment of energy flexibility, viability of energy enterprises in a business eco system, operationalization of flexibility services and adaptive logistics in circular economy.

George Kariniotakis (Centre PERSEE of MINES ParisTech, France) George Kariniotakis received his Eng. and M.Sc. degrees from Greece in 1990 and 1992 respectively, and his Ph.D. degree from Ecole des Mines de Paris in 1996. He is currently Professor at MINES ParisTech. He is with the Centre PERSEE of MINES ParisTech as a senior scientist and head of the Renewable Energies and Smartgrids Group. He has authored more than 220 scientific publications in journals and conferences. He has been involved as participant or coordinator in more than 40 R&D projects in the fields of renewable energies and distributed generation. Among them, he was the coordinator of some major EU projects in the field of wind power forecasting and integration such as Anemos, Anemos.plus and SafeWind projects. His scientific interests include among others timeseries forecasting, decision making under uncertainty, modelling, management and planning of power systems. He is Senior IEEE Member and member of several expert groups like ETIP SNET.

Gerhard Kleineidam (Competence Network Water & Energy, Hof, Germany) is an expert in system engineering and automation technologies. He lectures “Automation in Energy Supply” and operates the field test lab in the territory of the utility and DSO SWW Wunsiedel GmbH in Northern Bavaria. He has been head of the E|Home-Center at the University of Erlangen Nürnberg before, where he has done research on smart home technologies and micro power plants. He was also CEO and founder of InReCon AG, a company developing high tech solutions in automation. Previously,
he was a senior manager at Infineon Technologies for semiconductor backend automation and a project manager at Siemens Automation Group, where he was responsible for managing huge turn-key automation projects. Gerhard Kleineidam is an active member at VDE and heads the VDE working group “Energy Supply 4.0” www.vde-nordbayern.de/ak-EV-40 .

Guillaume Giraud (RTE, France) Guillaume Giraud received a master’s degree in Electrical and IT Engineering in 1996 from CentraleSupelec, France. He is currently managing an internal task force at RTE on the Digitalization of the substations and control centers. During 20 years in RTE, he held expert and management positions in maintenance, telecom, automation and IT for market and control centers.

Hengxu Ha (GE grid solutions) was born in Penglai, China, on 3rd, Nov. 1972. He obtained his bachelor, master and PHD in electrical engineering in Gezhouba institute of hydro-electrical engineering, Shandong University and Xian Jiaotong University in 1993, 1999 and 2002 respectively. He is now Technical Lead (senior emerging technologies manager) in Department of Innovation and technology, Grid automation solutions, Grid solutions, A GE and Alstom Joint Venture. His research interest is in the area of innovative conception, algorithms and methods in protection, control and automation for electric power system

Henric Larsson (Vattenfall Eldistribution AB) is a business strategist and holds a Master of Science in Pedagogy. 10 years’ experience of the utility industry with a focus on digitalization and the digital customer for the past 4 years. Responsible for implementing digital solutions within the business such as electronic signatures, improved errand handling and more realtime information regarding outages.

Ioannis Vlachos (National Technical University of Athens, Greece) Dr Vlachos is a seasoned professional with more than 15 years of experience working with some of the biggest energy companies, consultancy firms, and system integrators worldwide. He is also working closely and actively with both academia and industry in well-known projects in Europe, South America, and MENA region that merge the worlds of energy and ICT. Dr Vlachos has been awarded with the “Ericsson Award of Excellence in Telecommunications” and has authored more than 40 scientific publications in international journals and conferences. His current interests are focused at the crossroads of Internet of Things, blockchains, distributed ledger technologies, and cybersecurity with the energy sector. Dr Vlachos holds and MSc and PhD from the Department of Electrical and Computer Engineering, School of Engineering of the Aristotle University of Thessaloniki, Greece.

Jan Pedersen (**Agder Energi AS, Norway)** has been Vice-President and a member of the executive management group and responsible for business development, implementation of the innovation system and development of the service business area in the group before becoming a Director in 2011. Mr. Pedersen was CEO of Kristiansand Energiverk for 5 years before the utility merged with 2 other utilities into Agder Energi. Mr Pedersen has had 10 years of experience as a hydropower consultant working in Norway, but also involved in several projects located in Africa and Central America, and more than 20 years as member of the executive management team, including various assignments abroad. He holds a degree in Civil Engineering from University of Trondheim, the Norwegian Institute of Technology.

Jeff Montagne (Enedis, Think Smart Grids Association, France) is working as Chief Data Governance Officer for Enedis. He is also member of Smart Grid Task Force-EG1/WG “Data Format & Procedures” and of ETIP/SNET WG4 “Digitisation of the electricity system and customer participation”. Jeff has 18 years of experience in IT systems and Controlling for utilities. He has been successively working on SCADA communication protocols for EDF R&D Labs, on market exchange platforms for the French TSO, on modernizing security and architecture policies for EDF IS Group, then on digitalization for Enedis. He also spent several years in finance within EDF Group. He graduated as Engineer from Telecom ParisTech / Stuttgart university and holds an MBA from ESCP Europe.

Liam Beard (Vodafone Group, UK) is IoT (Utilities) Development Manager at Vodafone Group. He has 20+ years of experience working in Utility private, VPN and public shared communications. Predominantly focused on strategy development, design, implementation, operation, refresh and recovery of telecommunications and data solutions. Graduate of University of Portsmouth with BSc (Hons) in Computer Studies. Chartered Engineer and FEANI member. Past technical roles in Mercury Communications, Energis, Cable&Wireless (Technical lead and Managing Architect for National Grid Operational Telecoms outsource) and now Vodafone. Current Role - Responsible for Smart Grids and Smart Utility Networks development in IoT across Vodafone's global operating companies. Technical board member at Power Networks Demonstration Centre (University of Strathclyde). Steering board member at TechUK-SmarterUK industry group.

Liliana Ribeiro (EDP Distribuição / EDP, S.A.., Portugal) has a degree in Electrical and Computer Engineering, specialized in Energy, and now is doing a post-graduation in Cyber Security. The combination between smart grid and cybersecurity is what she is really interested in. At the moment, she works at the Portuguese DSO but she will change the group. She will be part of the EDP, S.A.. in the Portuguese DSO, where she will work in the process of connecting to the electrical grid energy producers.

Ludwig Karg (B.A.U.M. Consult, Germany) Ludwig Karg graduated with a master (Dipl. Inf. univ.) in computer sciences at the Technical University of Munich (1981). He gained practical experience in software engineering and held German and international positions in Intel Corp. for multimedia and network products. He is Managing Director of B.A.U.M. Consult GmbH (since 1993) and Chairman of INEM (International Network of Environmental Management). Mr. Karg led various research and development projects on sustainability and renewable energy usage in enterprises, municipalities and regions. Leading an international team of experts, he supports the ERA-Net Smart Energy Systems Initiative in more than 20 European countries.

Maher CHEBBO (General Electric - Global Digital Energy Solutions) PhD Energy joined General Electric as Senior Executive SVP, Chief Commercial Officer Globally for Power Digital Solutions in May 2017 based in Paris, France. He led the Power Digital Transformation P&L Business within Power transforming GE Industrial Customers to become full Industrial Digital, leveraging his 30 years of Digital experience in the market. Maher Headed a Digital Cloud IOT Business of 2 B$. Currently 20% of the current GE Power installed business has adopted Digital based on Financial, Value and Return on Investment justification. Since January 2018, Maher is leading GE Global Digital Energy Solutions as Senior Executive SVP, Chief Business Innovation Officer, covering Power Generation, Grids, Storage, Renewables & Energy Efficiency Services. Beside his permanent role at GE, Maher is Chairman of the GB of REEEP (as of 21st of April 2018), President of ESMIG, Vice-Chairman of ETIP SNET Executive Committee and Chairman of its Digital Energy group. Maher is also member of the Scientific Audit Committee of TNO. Before GE, Maher spent 21 years with SAP where he had several local, regional and global leadership positions focusing on Solution Engineering, Global Field Operations, Software innovation & development through incubating new products (Corporate in-Venturing), Industry business development, Value Engineering and General Management.

Manolis Vavalis (University of Thessaly and CERTH, Greece) is a Professor of Electrical & Computer Engineering at the University of Thessaly and a senior researcher at the CERTH. Before coming to Thessaly, he has been with the faculty of the Department of Computer Sciences at Purdue University, USA and Senior Researcher at FORTH. He has been participating in several EU funded R&D projects, had been coordinating few of them. His main current research interests are in the areas of Energy Markets and Power Stability in Next Generation Power Grids.

Marco-Robert Schulz (**Siemens Power Generation, Germany)** is Project Manager at DAAC (Data Analytics and Applications Center) **of Service Division** in Berlin. With 16 years of experience in business process engineering and project implementation for internal and external business processes, IT tool implementations and digitalization projects, he is an integral part of the ETIP SNET community and contributes to the WG4 TF2 - Digitalization Use Cases. Marco holds a master's degree in Mechanical Engineering (Dipl.-Ing. / M.Eng.) from Beuth University of Applied Science in Berlin.

Marcus Meisel (Institute of Computer Technology, TU Wien, Austria) MSc. BSc. since 2007 in the Energy&IT Group at the Institute of Computer Technology at the TU Wien and currently works there as Assistant Professor, teaching five courses, as project manager, leading five projects: RASSA-Architecture, Spin.OFF, iniGrid, eNDUSTRIE 4.0 and SIRIUS+, and for the European Technology Innovation Platform (ETIP-SNET WG4) leading the cybersecurity task force. He graduated in the Software & Information Engineering class of 2009 and Software Engineering & Internet Computing class of 2015. Apart from teaching, writing publications and proposals as head of his research group, his current responsibilities are gender equality and developing new research domains in the area of distributed communication technologies, Internet of Things, Industry 4.0, general Artificial Intelligence, and Smart Energy Systems.

Miguel Angel Sánchez Fornié (University of Comillas, ICAI, IIT, Spain) was former Director of Smart Grids in Iberdrola group (reporting to Global Networks CEO). He graduated in Electrical Engineering (ICAI Universidad de Comillas) in 1974. M.I.T. (U.S.A.) Nuclear safety degree in 1977. Several positions in Generation, Transmission and Distribution business of Iberdrola. In 1991, he was entrusted with Iberdrola's telecommunications, involving himself in all its business aspects. Since 2,003 he also became responsible for real time Control Systems in Networks. Former member of the UTC (US Utilities telecommunications Council) Board of Directors and President of its European division. Member of the Board Committee of the European Technology Innovation platform (ETIP SNET) Member of the Advisory Committee of the M.I.T. Future of the Electric Grid Study and the M.I.T. Utility of the Future project. General secretary of PRIME Alliance. He is an associate researcher and professor in some courses in the University of Comillas and visiting professor in University of Strahtclyde at Glasgow.

Miguel Carvalho (Watt-IS, Portugal) CEO and co-founder of the start-up company focused on developing intelligent analytics from smart metering and other related data, with the objective of providing value to energy utilities and energy consumers. He has 12+ years of management experience, leading teams towards the development of renewable energy and data analytics projects in Portugal, Spain, UK, Poland and Cyprus. He has extensive experience with EU and national funded R&D projects and from 2016 onwards actively participates on several EU working groups on topics related with Smart metering, Data Analytics, Digitalization of the Electricity System and User Engagement. Miguel graduated in computer engineering from Instituto Superior Técnico (IST) and holds an MSc on Technology Management from IST and an MBA from AESE/IESE Business School.

Moamar Sayed-Mouchawe (School of Mines Telecom Lille Douai, France) Moamar Sayed-Mouchaweh is working since September 2011 as a Full Professor in the High National Engineering School of Mines Telecom Lille Douai in France. His major research interests include Machine Learning for Big Data challenges, Data-driven/Data-centric modelling, Evolving intelligent autonomous systems, and Incremental, on-line, active and self-adaptive learning. His application domain is related to the development of decision support tools to address the challenges of Energy transition (Proactive Maintenance of Large-scale Offshore/Onshore Wind Turbines, Active Demand Side Management in Smart Grid, Dynamic Scheduling Problems in Smart Homes in the Presence of PV-WT Resources, Intrusion detection and misuse of information). He edited several Springer books, wrote two Brief Springer books, published more than 100 papers and co-organized a dozen of special sessions/tutorials/special issues/workshops in international journals and conferences and chaired several international conferences and IPC. He is working as an expert for the evaluation of European and industrial projects and as an associate editor for several international journals.

Norela Constantinescu (ENTSO-E, Belgium) is coordinating the Research and Innovation activities at ENTSO-E including with TSOs members. She is a member of the Governing Board of European Technology and Innovation Platform Smart Networks for Energy Transition and member of the WG4 Digitalization and Customer Integration. Previously she worked for 6 years with European Commission DG Energy leading on the Strategic Energy Technology Plan activities, on low carbon technologies focus on wind sector and Smart Cities and Communities. She has a long experience in energy sector acquired both in private and public sectors nationally and internationally. She obtained a master’s degree in energy engineering from University Politechnica Bucharest and she holds an MBA from Vrije Universiteit Brussels Solvay School

Peter Nemcek (cyberGRID, Austria) is a co-founder and Vice President of Research and Development at cyberGRID GmbH & Co. KG. Peter received M.Sc. in electrical engineering from University of Ljubljana, Slovenia in 2003. He is an expert in the development and deployment of electrical flexibility systems, like Virtual Power Plants, Demand Response Systems and Micro-grids. He is a member of the ETIP SNET WG4, BRIDGE initiative, Slovenian Smart Grids Technology Platform and SmartNet advisory board.

Pierre Serkine (**EIT InnoEnergy, Belgium)** is Energy and Innovation Adviser in the **EU Business Unit** in Brussels. He joined InnoEnergy in 2014 and worked on the development and implementation of the societal appropriation strategy of InnoEnergy to accelerate the shift toward a consumer-centric European energy system, dealing with consumer empowerment (behavioural change, prosumers, active consumers) and digitalization of energy matters. Prior to that, he worked for the European diplomacy on energy, climate change and raw materials issues, on adaptation to Climate Change for the French Ministry of Environment and Energy, and as an analyst in cleantech in a Private Equity funds. He graduated from an engineering school (Arts & Métiers ParisTech, France), he holds an MSc in Aerospace Dynamics (Cranfield Univ., UK), a M. Econ in Energy and Climate Economics (Paris-Dauphine Univ., France), and a MA in European Studies (College of Europe, Belgium).

Rolf Apel (Siemens AG, Energy Management Division, Technology & Innovation, Technology Strategy, Transmission, Distribution, Infrastructure & Industry, Germany) PhD. is Principal Key Expert for smart grid solution within the Siemens AG. He is head of the Technology & Innovation Strategy department for the energy management division. As an experienced expert, he had been member of the CIGRE working group D2.24: “EMS Architectures for the 21st Century” and is steering committee member of the EPCC International Workshops on Power Control Center. He is the German representative in the CAG of the IEC System Committee “Smart Energy” and also the Convener of SyC SE/WG5. On European level he had been working in the use case team for European Union Smart Grid Standardization Mandate (M490) and is currently member of the T&D Europe Task Force Smart Grid. Additionally, he is member of several expert committees in the German organizations VDE/ETG/DKE and ZVEI.

Sandra Riaño (TECNALIA, Spain) holds a BSc and a MSc in Automatics and Industrial Electronics Engineering (University of Deusto, Bilbao, 2006). She is a Researcher in the Smart Grids Area of TECNALIA since 2008. Her main research activities are related to DER integration, Demand Response, Energy Efficiency, Smart Metering and communications for Smart Grids. In these areas, she has worked closely with electrical manufacturers and utilities.

Theo Borst (DNV GL, The Netherlands) Theo Borst is Business Director Digital Grid and principal consultant at DNV GL Energy and is responsible for DNV GL’s service portfolio related to digital grid operation. This portfolio includes services related to SCADA EMS/DMS replacement, Smart Metering, Substation Automation, Energy Data Analytics, Utility Telecommunication, Data modeling/quality services and digital transformation of grid operators using emerging technologies like cloud computing, mobile technology and blockchain. Theo is responsible for strategy- and business development as well as sales and contract management on these topics, in addition, Theo is active as principal consultant, project manager and contract manager Theo has an electrical engineering / computer science background and an MBA degree. He has more than 23 years of (international) experience in system- and software engineering, enterprise architecture, solution architecture, business consultancy, business development, product management, project management (PRINCE II and IPMA-C), team management and QA. He is a member of CIGRE JWG CD2/C2 and of ETIP/SNET.

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.