# Transforming the energy sector through digitisation

At a time when the energy landscape is undergoing a fundamental change towards decentralisation and decarbonisation, the introduction of new and smarter technologies will make an important contribution. They will help integrate renewable energies from variable and distributed resources in the energy systems and increase efficiency through better monitoring and optimisation of assets.

These technologies can moreover provide an opportunity for the uptake of new energy services and business models enabling consumers in the active participation in the energy system and energy markets. The key issues to promote the digitisation of the energy sector are the following:

* Interoperability of communication to and from the appliance/device in a smart home to enable smart energy services, possibly combined with other services for consumers;
* The ability of the energy sector to handle much larger amounts of data than they currently do and use them to optimise the system, so that small-scale PV, demand-side response, etc can participate in the markets for energy and network services.
* In such a market with a lot more data, and remote control actions linked to them, the reliability of the grid and of the communication channels becomes critical for a secure network operation: It is clear that none of these innovations will take off if the communication is not secure. Cybersecurity is therefore a basic condition to be taken into account in the design and testing of any of the above.

The Energy Challenge contributes to the Focus Areas "Boosting the effectiveness of the Security Union" (SU) and "Digitising and transforming European industry and services" (DT), with the following specific topics (the contribution of the Energy Challenge is matched by a contribution from the SC7 and LEIT-ICT parts of the H2020 programme):

* SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks (SC7);
* DT-10-2018-2019: Internet of Things for Energy: interoperable smart homes & grids (LEIT-ICT);
* DT-11-2019-2020: Pilots for Big data tools and architectures in energy system management (LEIT-ICT);

Other topics may still be added, or, alternatively, more general calls in the ICT part of the programme will be open to the energy sector: further information will still follow.

The proposed topics listed below are part of calls developed in other parts of Horizon 2020. and therefore also subject to the general terms and conditions of those parts, which are not included in this document, but can be shared later and will in any case be shared with the relevant configurations of the Programme Committee in charge of these calls (i.e. LEIT-ICT and SC7).

These proposals are of course also subject to agreement by these configurations of the Programme Committee, and the budget and timing still need to be finalised. The topics that are part of 'transforming the energy sector through digitisation' will be jointly funded by DG ENER and DG CNECT, with an indicative total budget for the Horizon2020 work programme 2018-2020 of between 90-150 million Euro.

## SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks

Specific Challenge: The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity, hence a power outage can have direct impact on the availability of other services (e.g. transport, finance, communication, water supply) where backup power is not available or the power restoration time goes beyond the backup autonomy.

With the transition to a decentralised energy system, digital technologies are playing an increasingly important role in the EPES: they contribute reducing the energy consumption; they enable the integration of higher shares of renewables and promote a more energy efficient system. At the same time, with the growing use of digital devices and more advanced communications and interconnected systems, the EPES is increasingly exposed to external threats, such as worms, viruses and hackers, data privacy breaches and other vulnerabilities.

Without appropriate cyber-defence measures, systems access could be violated with the malware spreading over the system and may cause power outages, damages and cascading effects to interconnected systems, and energy services. Therefore, the EPES is currently facing a range of threats requiring an attentive evaluation of the cyber security risk that allows taking proper countermeasures. For example, the decentralisation process of the EPES will increase the number of access points (e.g. smart meters, IoT), hence increasing the exposure to cyberattacks. Also, the network protocols used by existing SCADA/ICS (Supervisory Control and Data Acquisition System/Industrial Control Systems) were designed in times when cybersecurity was not part of the technical specifications for the system design, hence if a hacker or worm can get access to any control system, it can exploit the protocol to disable or destroy most industrial controllers. On the other side, unlike IT systems, a control system in the EPES that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts. At the same time, with the decentralisation leading to a distributed energy system, the concept of microgrid/islanding is de facto acting and could be further exploited against cyber-attacks and cascading effects in the EPES.

In order to pursue the integration of the renewables and to benefit from the advantages brought by a modern digitalised electricity grid, there is a need for new security approaches detecting and preventing threats with severe impacts and to shield the electric system against cyber-attacks. Without an adequate strategy and measures to protect the energy system, and in particular a decentralised EPES, from cyber-attacks, the energy transition would be more risky, more costly and possibly in danger.

Scope: The proposals shall demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders. The proposals shall demonstrate the resilience of the EPES through the design and implementation of adequate measures able to make assets and systems less vulnerable, reducing its expositions to cyberattacks. Different scenarios of attacks with the relative counteracting measures have to be designed, described and tested on the field to verify effectiveness. Depending on the specific application, the proposal shall apply measures to new assets or to existing equipment where data flows were not designed to be cyber protected (e.g. SCADA, ICS). The proposals shall implement the following series of activities concurring to make the electric system cyber secure: (i) defining cybersecurity design principles and standards with a set of common requirements to inherently secure EPES; (ii) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy provision supply chain); (iii) on that basis, designing a secure network architecture with defence in depth approach implementing segmentation and security levels mechanism considering a functional hierarchical model; (iv) implementing the measures in real life demonstration testing the cyber resilience of the system with simulation of different types of attacks and severity; and (v) demonstrating the effectiveness of the measures with a cost-benefit analysis.

The proposals shall also (i) develop security information and event management system collecting logs and other security-related documentation for analysis that can also be used for information sharing across operators of essential infrastructures and CERTs; (ii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and (iii) propose policy recommendations on EU exchange of information.

The dimension of a pilot/demonstrator within the proposal shall be at city level, involving generators, one primary substation, secondary substations and end users. The proposals shall include the following types of entities: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers.

The proposals may refer to Industry 4.0 and other proposals and/or projects dealing with cybersecurity in energy.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 6 and 8 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other

Expected Impact:

1. Built resilience against different levels of cyber and privacy risks.
2. Ensured continuity of the critical business energy operations.
3. The energy sector is better enabled to easily implement the NIS directive.
4. Increase the resilience of the electric system to different levels of attack.
5. The cyber protection measures will be easily reconfigurable to new threats.
6. A set of standards and rules for certification of cybersecurity components, systems and processes will be made available.
7. Cyber protection policy design and uptake at all levels from management to operational personnel.
8. Manufacturers are encouraged in providing accountability and transparency, enabling third parties monitoring and auditing the privacy and security of their energy devices and systems.

Type of Action: Innovation action

## DT-10-2018-2019: Internet of Things for Energy: interoperable and smart homes & grids

Challenge:
When energy production is becoming decentralised and ICT is increasingly present in homes, the integration of Renewable Energy Sources and promotion of energy efficiency should benefit from smarter homes, buildings and appliances. Smart homes and buildings are one crucial element because system integration and optimisation of distributed generation, storage and flexile consumption will require interoperable smart technologies installed at building or home level. IoT enables a seamless integration of home appliances with related home comfort and building automation services allowing to match user needs with the management of distributed energy across the grid and to gain access to benefits from Demand Response. Novel services should lead to more comfortable, convenient and healthier living environment at lower energy costs for consumers whilst enabling an active participation of consumers in the energy system and energy markets.

Scope:

The aim of the pilot is to exploit IoT reference architectures models that allow for combining services for home or building comfort and energy management, based on platforms that enable the integration of relevant digital technologies like IoT, AI, cloud and big data services. Energy services, where appropriate, can be combined with additional non-energy services and foster the take-up of smart energy communities (in particular peer-to-peer energy markets). The aim is also to demonstrate these platforms under real-life conditions in interaction with the electricity system, and to demonstrate the benefits of energy management through IoT application and services. The envisaged architecture should allow for third party contributions that may lead to new value added services both in energy and the home domain.

The scope is to develop interoperability and seamless data sharing across the devices and systems to enable innovative building energy management services; with the aim to save costs to consumers, to facilitate the integration of renewable energy from distributed intermittent sources and to support energy efficiency. The pilot needs to demonstrate plug-and-play energy management solutions, by taking into account legacy of existing smart home or building solutions, mapping their approach to common architecture models and implementing relevant standards (such as SAREF) within the home and towards the grid (smart meter)/aggregators. Pilots need to ensure interoperability in the communication interfaces between smart devices and from the smart device to the gateway/energy manager and/or to the cloud, i.e. a service provider that uses the data generated from the device. Selected pilots should promote the use of these interoperable solutions as widely as possible involving many different types of appliances (e.g. including white-goods, heating, cooling and ventilation, home & building automation energy management and control, batteries, PV panels, charging for electric vehicles), and explore the need for further standardisation and legislation.

**The selected large-scale pilot shall in particular address all of the following issues:**

* demonstrate scalability and stimulate spill-over effects; demonstrate that such platforms lead to a marketplace for new services in EU homes and buildings .
* make use of cascading funds: for the incorporation of users of the pilots, developers of additional applications, replication of the pilot through new sites or new connected devices, and complementary assessment of the acceptability of the use case where appropriate.
* the consortia should cover the whole value chain for IoT-based services: appliance manufacturers and technology providers, ICT suppliers, energy sector (energy suppliers, aggregators, ESCOs, TSOs and DSOs);
* cooperate with other Large-Scale Pilots under the IoT Call and Big Data for Energy Call [Ref]; a duration up to 4 years should be considered allowing the project to contribute to CSA under the call DT-13-2019 and in the BRIDGE project;
* link with Member States' initiatives in this area;

Expected impact:

* Increasing number of energy apps/services and home devices and appliances that are connected through the Internet allowing to shift consumption when energy rates are low, renewables are abundant, etc.
* Validation of user acceptance, as well as demonstration of viable concepts that ensure privacy, liability, security and trust in connected data spaces;
* Accelerated wider deployment and adoption of IoT platforms in smart homes and buildings in Europe and development of secure, cost-effective and sustainable European IoT ecosystems and related business models.
* Demonstration that such platforms lead to a marketplace for new services in EU homes and buildings with opportunities also for SMEs and start-ups.

Type of Action: Innovation Actions. The Commission considers that proposals requesting a contribution from the EU up to EUR 30 million with a duration of up to 4 years for Innovation Actions would allow the areas to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

## DT–11-2019-2020: Pilots for Big data tools and architectures in energy system management

Specific Challenge:

Tomorrow's energy grids consist of heterogeneous interconnected systems, of an increasing number of small-scale and of dispersed energy generation and consumption devices, generating huge amounts of data. The electricity sector, in particular, needs big data tools and architectures for optimized energy system management under these demanding conditions.

Scope:

**Innovation Actions** targeting large-scale pilot test-beds for big data application in the electricity sector. The aim is to develop/pilot and deploy a reference architecture for large-scale data exchange, management and processing in the electricity sector and to translate this reference architecture into an open, modular data analytics toolbox for the safe and effective operation of grids and provision of innovative energy services. The reference architecture should ensure compatibility with legacy formats, interfaces and operating systems of the energy system, allow replication and scale-up, be compliant with applicable EU standards, and should enable the integration of relevant digital technologies like IoT, AI, cloud and big data services. The analytics toolbox shall be able to handle a wide variety of data and support the development of a wide range of energy services, at least to increase the efficiency and reliability of the operation of the electricity network, to optimize the management of assets connected to the grid (in particular small-scale generation and those used for demand response), to increase the efficiency and comfort of buildings, and to de-risk investments in energy efficiency (e.g. by reliably predicting and monitoring energy savings). Proposers must demonstrate that they have access to appropriate large-scale and realistic datasets, and shall involve TSOs, DSOs, suppliers, aggregators, ESCO's, building management and renovation sectors, software integrators/developers, analytics, simulation, prediction, cloud computing, as appropriate. Projects shall collaborate with the Bridge project (SC3).

The Commission considers that proposals requesting a contribution from the EU of around 10 million EUR would allow this area to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

All grants under both subtopics will be subject to Article 30.3 of the grant agreement (Commission right to object to transfers or licensing).

Expected Impact:

Proposals should address the following impact criteria, **providing metrics to measure success** where appropriate:

* Effective integration of relevant digital technologies in the energy sector, resulting in integrated value chains and efficient business processes of the participating organizations;
* Enhancing energy asset management, increasing consumer participation and innovative network management, creating new data-driven business models and opportunities and innovative energy services;
* Offering access to cheaper energy for the consumers and maximising social welfare;

Type of Action:

Innovation Actions (IA)