Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

The proposals should demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches (including personal data breaches) taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders. The proposals should 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 expected potential disruptive effects on the EPES should be envisaged and the relative counteracting measures should be designed, described, tested (sandboxing, simulations) on a representative energy demonstrator to verify effectiveness. Depending on the specific application, the proposal should 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 to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain); (ii) on that basis, designing adequate security measures to ensure a cyber-secure system and describing the advantages of the solutions adopted compared to others and which aim to guarantee the level of cybersecurity and resilience vital for EPES in an evolving system; (iii) implementing both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity; and (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis. The activities may include the testing of micro-grid and/or islanding as a means to reduce the vulnerability to cyber-attacks.
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) define cybersecurity design principles with a set of common requirements to inherently secure EPES; (iii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and (iv) propose policy recommendations on EU exchange of information.

The dimension of a pilot/demonstrator within the proposal should be at large scale level (e.g. neighbourhood, city, regional level), involving generators, one primary substation, secondary substations and end users. The proposals are encouraged to 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.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020, in particular under the BRIDGE initiative[[http://www.h2020-bridge.eu/]].

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 amounts.

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, hackers and data privacy breaches.
Without appropriate cyber-defence measures, systems access could be violated (e.g. with the malware spreading over the system) and may cause power outages, damages and cascading effects to interconnected systems, and energy services. Therefore, with increased digitalisation, the EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk that allows taking proper countermeasures. For example, the growing use of interconnected smart devices in the EPES will increase the number of access points (e.g. smart meters, IoT), hence increasing the exposure to cyberattacks. Also, even if security improvements may have been made since, older technologies used in legacy systems such as 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.

On the other side, a control system in the EPES that is under attack might not 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, microgrid operations and/or islanding could be further exploited against cyber-attacks and cascading effects in the EPES.

In order to pursue the integration of the renewables within the existing EPES and to ensure that it benefits 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 from cyber-attacks, the energy transition would be more risky, more costly and possibly in danger.

- Built/increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.
- Ensured continuity of the critical business energy operations.
- The energy sector is better enabled to easily implement the NIS directive.
- A set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector will be made available.
- Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector.
- Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.