Establishment of a FramewORk for Transforming current EPES into a more resilient, reliable and secure system all over its value chain

Characterization and classification of EPES threats

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No. 101075665

Executive summary

It is widely recognised that electricity is more than essential for everyday life and the power sector of each country has become the backbone of the its economy. Therefore, any disruption to the energy supply chain will lead to catastrophic impacts on the critical infrastructure across most industries. However, the power sector has been grappling with numerous challengers, arising from natural, technological or human-caused threats, even before the recent disruptions driven by the COVID-19 pandemic and the Russian invasion of Ukraine. Indeed, the experiences of the electricity industry in the last decade highlighted the vulnerability of the sector to extreme events. In this context, apart from the usual operational paradigm to focus on reliability, security, restoration, and emergency planning, energy suppliers should invest in Electrical Power and Energy Systems (EPES) resiliency to bounce back from such events.

Resilient EPES could thrive under changing conditions and withstand, respond to, and recover rapidly from the impacts of threats. Towards this direction, traditional energy systems are upgraded with many advances in the field of industrialisation, digitisation and electricity demand at both commercial and residential level and are thus transformed to smarter ones. This transformation is supported by the integration of Internet of Things (IoT) that is being utilised for the bidirectional flow of information, to form an extensive network of a cyber-physical system capable of monitoring and controlling the various connected devices remotely. While this transition creates many opportunities for achieving energy and cost efficiencies, it also brings new challenges and risks that are more complex, frequent, and less predictable. Thus, cyber-security has been identified as a top power industrial security target. Cyber-attacks targeting EPES have increased over the last five years, and power sector vulnerability will continue to rise as renewable and distributed energy resources (DERs) are added and systems become more complex, digitalized, and decentralized.

Taken all this into consideration, the current study aims to provide a consolidated outlook on threats that may jeopardise the integrity of EPES when exploiting vulnerable energy assets, hence posing risks to the security of supply. The analysis realised within this report is complementary to other activities that will be realised within the eFORT project, targeting the use of dynamic Risk Assessment (RA) tools for EPES threats and vulnerabilities analysis, the assessment of cascading effects that may be triggered from the various threats as well as the development of a resilience planning process to safeguard EPES operation. In this context, the present report realised a comprehensive assessment of the power sector's vulnerabilities to climate and non-climate natural threats and to human and technological threats. The vulnerability assessment involved both an extensive literature survey and the stakeholder engagement through the use of structured questionnaires that have been distributed to energy grid experts across EU. The main goal was to identify the most important threats to the EPES, describe their impact and determine and prioritise among the vulnerabilities that may be exposed.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No. 101075665

For the implementation of the described activities, the identification of prominent technological, natural and human-caused threats has been realised through an extensive literature review of published reports, scientific papers, focusing on climate and historical data, current and/or emerging threats, combined with the analysis of relevant vulnerable assets of the energy system that could be exploited by those threats, generating a risk to the security of energy supply. EPES threats have been then classified according to their type, their quality and possible impacts on EPES. Subsequently, the identification of the vulnerabilities of EPES associated with the various threats and their respective impacts, has been carried out. Finally, for the risk identification phase, a generic bottom-up analysis was followed, focusing on the nature of the various threats and the type of assets they affect, as well as the causal relationships that lead to the materialisation of each risk.

To enhance the RA process and the prioritisation among the various EPES vulnerabilities, a risk scoring process (qualitative scoring from low to high) has been adopted combining the likelihood of a threat to occur and the severity of the potential vulnerabilities, reflecting the magnitude of the consequence of realising each vulnerability or the extent to which each vulnerability may negatively impact EPES. Upon defining the relevant scorings, risk heat maps have been generated, correlating threats and vulnerabilities, and combining scores in a meaningful way, that allowed to rank risks and visualise data through defined colour-coding, thus prioritise among the possible risks. Specifically, by exploiting the results generated within eFORT from the EU energy

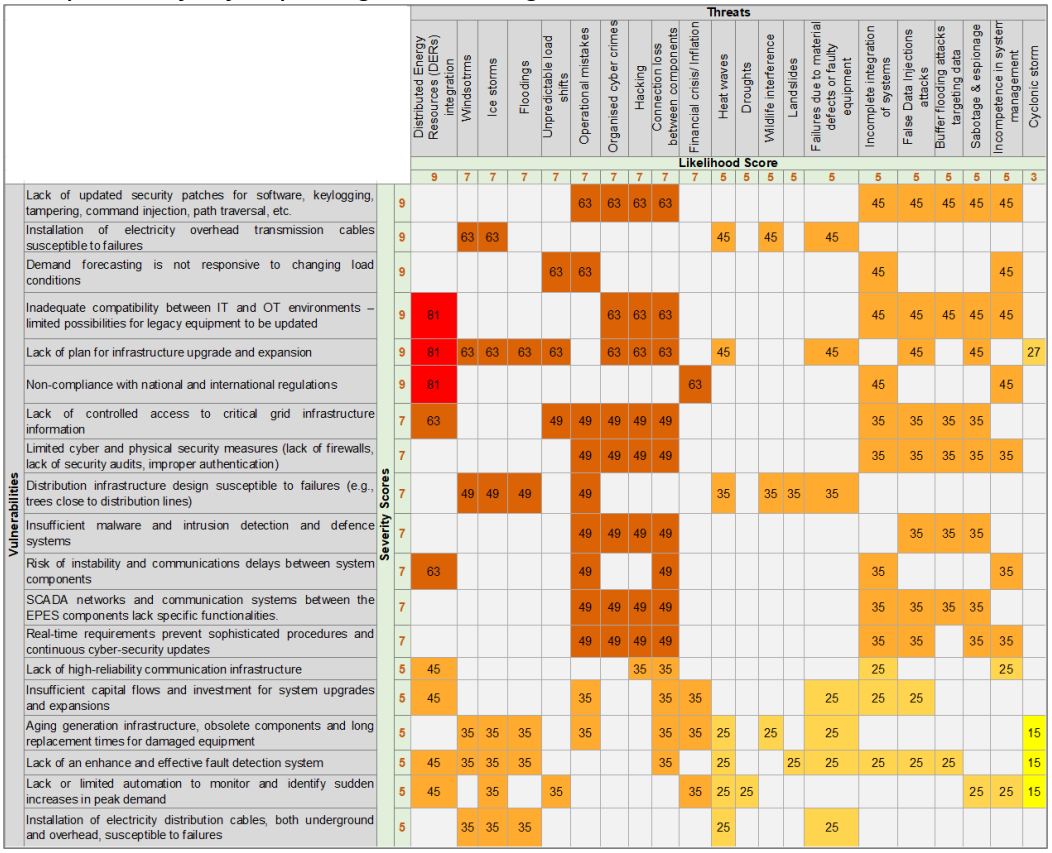

Figure 1. Risk heat map based on the data gathered from the energy experts' questionnaires analysis.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No. 101075665

grid experts' responses, two lists have been formed, incorporating the identified vulnerabilities along with their severity score as well as the respective threats and the likelihood of occurrence score. Based on these lists, a Risk criticality heat map (Fig. 1) has been generated to visualise risk rating and enable the prioritisation among risks.

The analysis realised based on data collected from the energy grid experts across EU, indicated that apart from the risks related to natural/meteorological phenomena due to climate change impacts, that mainly affected EPES resilience and integrity in the previous years, currently the main attention has been shifted towards cyber threats as well as to the risks arising from DERs integration, that has been significantly progressed in order to meet the growing electricity demands and the adoption of green energy sources. Undeniably, DERs integration and the transformation of the traditional energy grid to a smart grid, paved the way for many technological advancements and the incorporation of energy management and operations techniques, that have positively impacted EPES, however they have also opened pathways for attackers to exploit vulnerabilities and introduced additional threats. Based on this analysis, the most critical threats that have been identified, based on the answers provided by the energy grid experts across EU are: DERs integration; Organised advanced cyber-crimes from assemblies of people with advanced technical skills and adequate financial resources; Hacking into cyber system to control EPES with the intention to cause harm; Connection loss between components; Operational faults; Windstorms; Ice storms; and Unpredictable energy load shifts from peak hours to off-peak hours.

In line with the previously mentioned increased adoption of IoT devices in EPES and the challenges they entail from the cybersecurity perspective, the current study also includes an annex on threats associated to IoT devices that may be used for the so-called demand side attacks or manipulation of demand via IoT (MaD IoT) attacks. The devices considered traditionally in this kind of attacks are high wattage IoT devices like heating, ventilation, and air conditioning (HVAC) or electric vehicles (EV) charging posts. Within the eFORT project, the impact of generation is going to be also analysed, so photovoltaic (PV) inverters are considered too. The cybersecurity threats associated to such consumption and generation devices are especially important because: (i) they are the weakest link in the chain; (ii) they are typically out of the control of the distribution system operators (DSO); and (iii) although they may not be considered a threat for the power infrastructure individually, if they were massively compromised and orchestrated attacks were organized, the impact in the operation of the power grid (e.g., in terms of stability) might be very important.

Regarding connected HVAC systems, the components that can be compromised can be classified in: sensors and actuators, and control server. The so-called smart home plugs stand out within the first category, since they are becoming very popular to remotely control and monitor home devices. Compromising this kind of devices may entail from sending fake measurements to powering on or off the devices powered through them. Control servers represent nevertheless the key elements in the architecture, since they are more complex and are responsible for receiving and processing measurements and making decisions and sending commands accordingly. In EV charging infrastructures,

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No. 101075665

five main components were identified as susceptible to being attacked: EV, DC fast charging points (DCFC), AC charging points, protection devices, and transforming devices, although the latter two are embedded in the power grid itself. DCFC are especially relevant due to the large loads they handle. Charging point operators (CPO), that manage both DCFC and AC charging points, and vehicle to grid (V2G) connections are also identified as key for the RA of EV charging infrastructures. Finally, inverters are considered the most critical components of PV installations. The potential attacks to these devices range from physical attacks to hall-effect sensors that provoke failures to cybersecurity attacks that may produce complete failure of the infrastructure.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No. 101075665