T&D europe

ENSURING THE CYBERSECURITY OF EUROPE'S ELECTRICITY SYSTEM

DIGITALISATION IS AN ESSENTIAL TOOL FOR THE **CLEAN ENERGY SYSTEM**

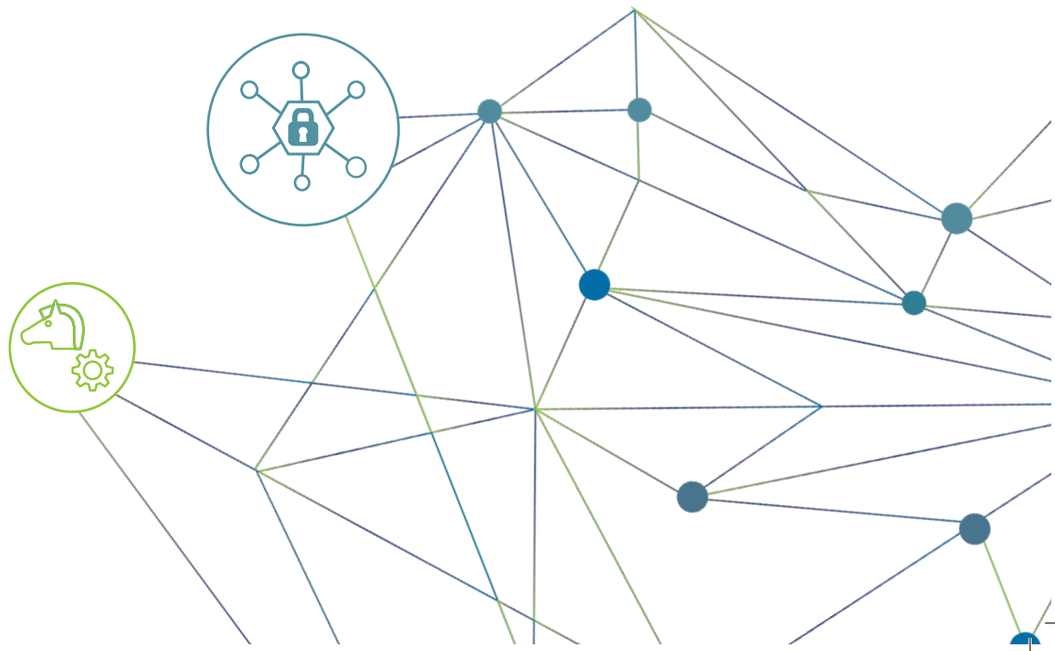
Electricity has become an essential and critical resource of the daily life of Europeans. Few people can imagine living without the benefits of electricity. A temporary or prolonged disruption in our electricity supply touches virtually every part of our society and economy. Without electricity, everyday life is severily disrupted, creating massive impacts on essential services such as transportation, water and food supply, communications, security and health services.

Therefore the challenge is to improve the resilience of the grid by ensuring the quality of service and the continuity of supply under different circumstances. In addition society desires to move to a cleaner energy system, emmiting less greenhouse gases. This shift towards clean and resilient electricity requires a transformation of the electrical grid into a smarter and more efficient network, supported by digitalisation. In parallel with this transformation, new actors such as aggregators and prosumers, re-inforce the need of integrity and availability of information, building a framework of trust among peers.

Cybersecurity is at the top of the agenda of Governments [1], industry and utilities. The EU recognises the importance of cybersecurity for the energy sector and the need to duly assess cyber-risks and their possible impact on the security of supply. EU Member States are developing and coordinating their cybersecurity strategies [2] and are in the process of adopting the so-called Cyber Security Act [3].

Cybersecurity measures need to consider five characteristics that are specific for the electrical grid.

1. There are more than 4 million substations **geographically distributed** across the EU, deployed over the years without cybersecurity in their initial design, which are potentially vulnerable to cyber attacks.
2. The **energy grid assets are very different from one another,** having been deployed over long periods of time with **diverse levels of cybersecurity** functionality.
3. The criticality of substations regarding grid stability is variable, but substations can also be seen as a **potential access** to control center communication networks, leading to a large and dispersed attack surface.
4. Electrical grid instability created at substation OT [4] level can lead into a **domino effect,** creating black out at pan-european level.
5. Digitalisation and **new applications** like e-mobility or renewables amplify the phenomena described under (3) and (4).



[1] Energy sector on alert for cyber attacks on UK power network, Financial Times 18 April 2018, https://www.ft.com/content/d2b2aaec-4252-11e8-93cf-67ac3a6482fd

[2] 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 (NIS) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[3] http://www.consilium.europa.eu/en/policies/cyber-security/

[4] Operational Technology (OT) – the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc. (Source Wikipedia)

TO SECURE EUROPE'S POWER SYSTEM AND ENSURE A CONTINUED RELIABLE PROVISION OF ELECTRICITY A **HIGH LEVEL OF CYBERSECURITY IS ESSENTIAL**

CYBERATTACKS: ALREADY A REALITY

There have been several well documented incidents that cover almost every aspect of life, from hacking into automotive systems [5] and financial organizations, theft of personal data from companies [6] and government departments [7], to the wilful interruption of industrial processes [8] and public services [9]. As demonstrated by an incident in Ukraine [10], where a cyber attack left 225,000 customers of three distribution utilities without electricity for up to four hours, it is possible for attackers to infiltrate a system months or years before, gain knowledge of the system and then attack. Compromised systems lay undetected until triggered by a signal or external event. In this case, even power backup systems were compromised so that when power was cut to the control centre, the backup supply did not turn on.

THE EU NEEDS A ROBUST, EFFECTIVE AND AGILE CYBERSECURITY APPROACH

[5] Andy Greenberg. (2016, March) Wired Magazine. [Online]. https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/

[6] Suzanne Philion. (2016, Septmeber) Business Wire. [Online]. http://www.businesswire.com/news/home/20160922006198/en/

[7] Ellen Nakashima. (2015, July) Washington Post. [Online]. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[8] ENISA. (2010, October) [Online]. https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis

[9] Alan Martin. (2015, February) We Live Security. [Online]. http://www.welivesecurity.com/2015/02/24/british-hacker-due-sentencing-public-service-ddos-attacks/

[10] Robert Lee. (2016, March) SANS. [Online]. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

PRACTICAL STEPS TO INCREASED CYBERSECURITY

The Smart Grids Task Force - Expert Group 2 – Cybersecurity (SGTF EG2) has drafted its recommendation for the implementation of a Network Code on Cybersecurity, which proposes a harmonized cybersecurity baseline across the European Union. A baseline protection is defined by two building blocks, operator conformance to ISO/IEC 27001 and Minimum Security Requirements for products, services and processes using the EU Cybersecurity Act as an instrument.

International standards are hereby forming the common language of cybersecurity used by all actors in the energy value chain. EU harmonization of security requirements directly benefits the economy by lowering implementation costs while supporting the European Commission's Digital Single Market strategy with products and systems deployable in all Member States. When defining minimum security requirements for all critical infrastructures, EU cybersecurity policy and mandates should reference to the key basic standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019, IEC 62443, and IEC 62351, covering security management, systems security and communication security aspects for the T&D industry.

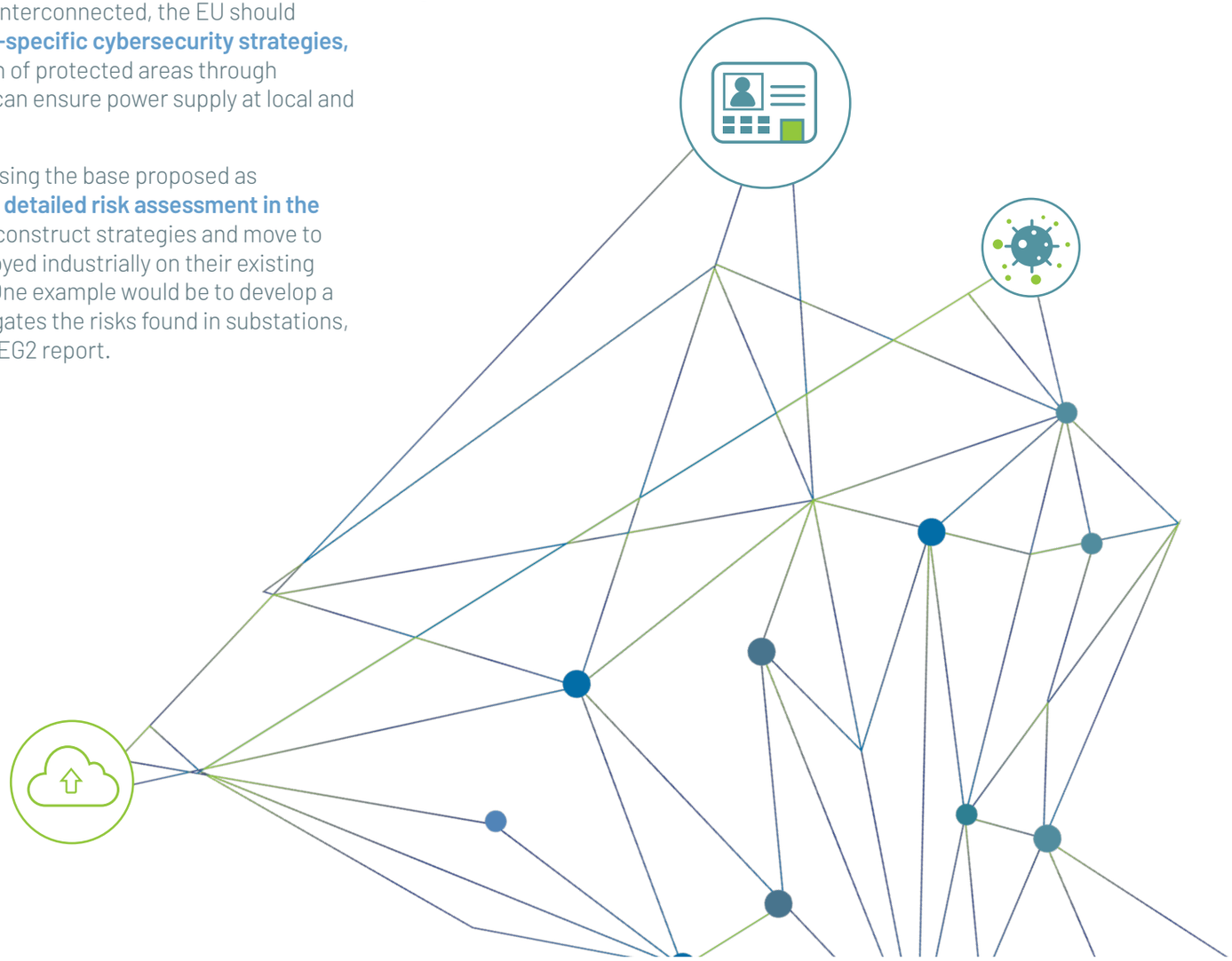
Furthermore, the energy grid consists of complex systems interacting with life-times of 40 years and more. Consequently, certification should be focused on processes and not components, such as ISO/IEC 27001 which focuses on the management of security and IEC 62443-2-4 which focuses on the process of a system integrator.

For operators of critical infrastructure it is essential that the components from different suppliers, integrators, and service providers can work together. To strengthen interoperability the EU should consider funding an **EU interoperability platform,** tasked with the development and implementation of international standards such as **IEC 62351 and IEC 62443.** Such an initiative would concretely help the EU to achieve the ambition to make Europe a leader in cybersecurity by 2025.

As the electricity grid is more and more interconnected, the EU should facilitate the development of **electricity-specific cybersecurity strategies,** including the design and implementation of protected areas through **microgrids and back-up solutions** that can ensure power supply at local and regional levels.

Grid actors can build on this inititive by using the base proposed as **suggested by EG2 report and perform a detailed risk assessment in the IT and OT enviroment,** use the result to construct strategies and move to standardized solutions that can be deployed industrially on their existing infrastructure, including field systems. One example would be to develop a standardized upgrade solution that mitigates the risks found in substations, based on the security profile defined by EG2 report.

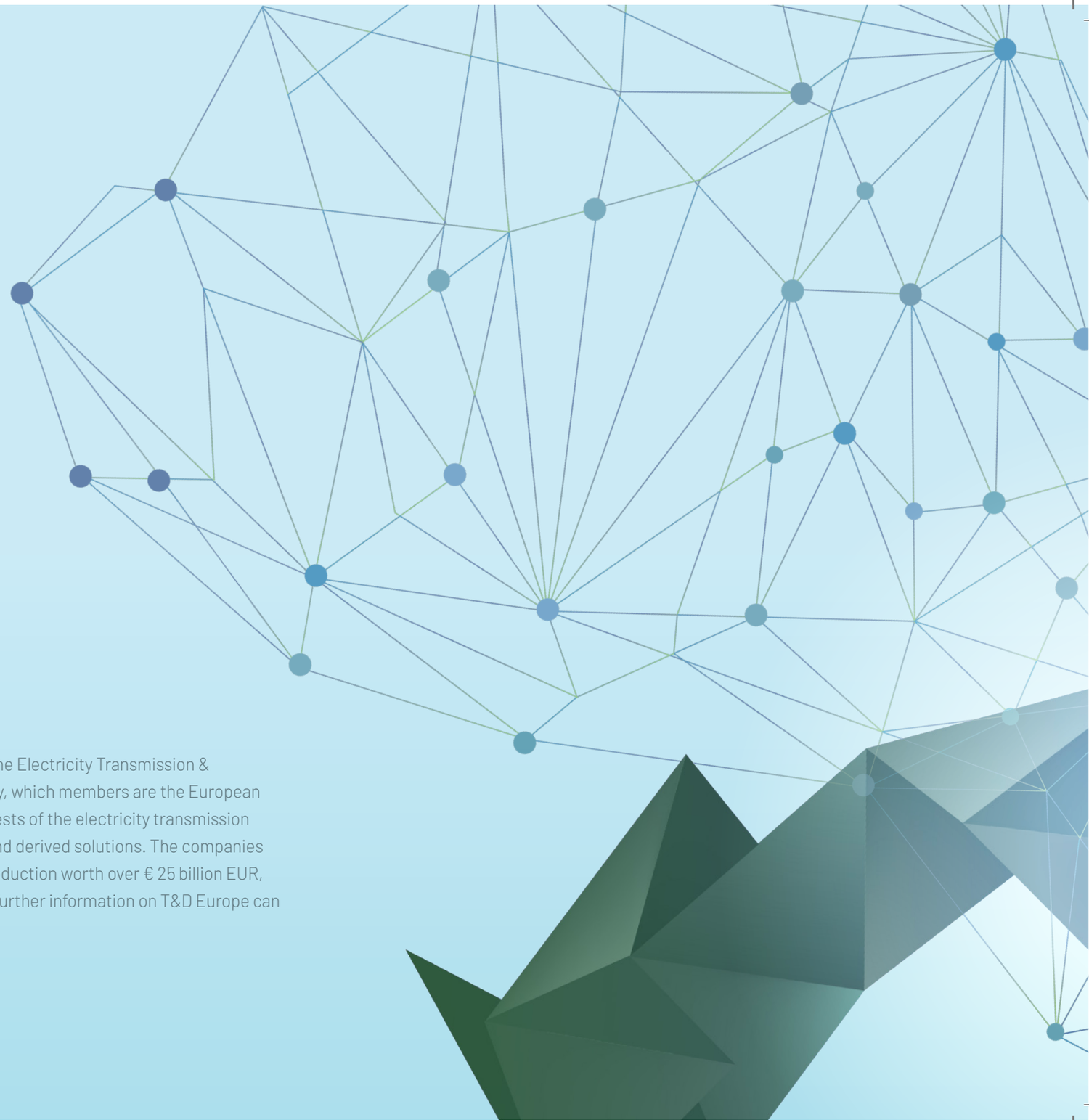
The new clean energy system offers many advantages for consumers and the environment. Digital technologies are essential for the management of this system. This brings potential vulnerabilities to cyber attacks. The EU can be at the forefront and become a global leader for cybersecure energy systems. It is therefore essential to ensure a robust framework for cybersecurity based on international standards.



T&D Europe
BluePoint Building
Boulevard A Reyers 80
B1030 Brussels
Belgium

+32 (2) 206 68 67
email: secretariat@tdeurope.eu

Follow us
T&D Europe
@BetterGrids



ABOUT T&D EUROPE

T&D Europe is the European Association of the Electricity Transmission & Distribution Equipment and Services Industry, which members are the European National Associations representing the interests of the electricity transmission and distribution equipment manufacturing and derived solutions. The companies represented by T&D Europe account for a production worth over € 25 billion EUR, and employ over 200,000 people in Europe. Further information on T&D Europe can be found here:

www.tdeurope.eu

June 2019