# Energy Policy Studies

IGNACY LUKASIEWICZ
ENERGY
POLICY
INSTITUTE

2(8) / 2021

**Cover design:** Aku Studio

**Typesetting:** Lidia Mazurkiewicz, MSc, Eng.

**Publisher:** Ignacy Lukasiewicz Energy Policy Institute

eps@instytutpe.pl

http://www.instytutpe.pl/eps/

http://www.instytutpe.pl/en/eps-en/



e-ISSN: 2545-0859

The electronic version of the journal is the original version.

Rzeszow 2021

# CONSTENTS

# Outline of using the Energy Cluster potential for the Distribution System Operator

*Marek Sikora*

**Abstract**: The aim of the article is to present the possibility of cooperation between the Energy Cluster and Distribution System Operator (DSO) in order to improve the local grid operation, and indirectly, for the benefit of the National Power System. The possibility of creation and operation energy clusters in Poland, with particular emphasis on contractual relations with the DSO and the position of the cluster in the energy market is discussed at the first stage of the article. The following part analyses the impact of distributed energy sources (DER) on the distribution grid as well as the grid operation problems. The issue of distribution grid flexibility in relation to the development of distributed generation is presented. What is more the possible interactions between the Energy Cluster and the DSOs in this respect is elaborated. Finally, the ways of using the energy potential of the Energy Cluster by the DSOs is analysed, which take the form of specialized services for grid operators.
**Key words:** distributed energy resources, energy clusters, flexibility

## Introduction

Another year has passed since the concept of the Energy Cluster was officially introduced to the Polish energy sector regulations, which found its place in the Renewable Energy Sources Act. At the same time, another year has been passing without full implementation of the REDII Directive (EC Directive 2018/2001) and the Market Directive (EC Directive 2019/944) in terms of "Renewable Energy Communities" and "Citizen Energy Communities" (RES Act).

Despite the initial enthusiasm of many communities, mainly from the renewable energy sector and local governments, as of today, most of energy clusters have not gone beyond the conceptual phase and the growth of new initiatives has been practically stopped. However, it should be emphasized, that most of the established energy clusters, as a goal of their activities have set themselves the construction of new generation sources to meet their own energy needs. Planned generating capacities are characterized by field dispersion, diverse technology of production and significant geographical distance from the places of energy consumption. The share of sources with intermitted generation (PV, wind) is important here; it covers about 2/3 of the planned capacity. The rest are stable sources (biogas, water, cogeneration) (Sołtysik, 2018). Few new initiatives, are based on the pursuit of energy self-sufficiency, mainly by building their own generation sources and even by building their own distribution network (KIKE, 2021).

Energy self-sufficiency, as indicated by clusters, is in fact an attempt to balance energy demand and supply in the cluster over a specified period of time. Clusters assume that such balancing should occur over a longer period of time, with the planned initial level of demand coverage by own production not exceeding 27% (Sołtysik, 2018). Balancing is not considered

from the side of simultaneity of the process of electricity generation and consumption , i.e. real-time balancing is not assumed.

Due to the mentioned instability of generation and low self-balancing (also non real-time), the support of distribution grid is needed, by accepting temporary surpluses of produced energy or supplementing temporary deficiency. In emergency situations, distribution grid will act as a reserve for supplied energy to consumers. On the other hand, the energy potential of clusters can be useful for the DSOs to improve local distribution grid operation for the benefit of other system users and the National Power System (NPS). Such cooperation will always exist, regardless of whether the Energy Cluster has its own grid or is created on the DSO grid.

The purpose of this article is to analyse selected issues of Cluster-DSO cooperation and to answer the question whether a cluster's cooperation with DSOs is possible in the scope of using the Energy Cluster potential for the needs of local Distribution System Operator, and thus the National Power System.

**General remarks on the Cluster-DSO cooperation**

In the case of energy clusters, the purpose of which is to produce energy for the needs of its members, it is necessary to define how clusters would like to use the power system. Is it supposed to be only access to the network in order to transfer energy between clusters members, or they also need access to the Energy Market. Clusters can choose to build own grid connecting theirs participants or use the existing grid of the Distribution System Operator (DSO) located in the area of clusters operation. Regardless of the chosen solution, when building contractual relations in a cluster environment, several important issues should be taken into account, presented below, the proper understanding of which may guide further activities of the interested parties (Sikora, 2013).

From the DSO point of view, a cluster having its own grid is definitely easier to cooperate with because the network must have the right Operator. Therefore, it is a cooperation of two Distribution System Operators, which does not require special agreements, as a cluster is treated as a consumer connected to the DSO grid (Energy Law Act).

In case of clusters created on the DSO grid, both consumers and producers are still connected to the DSO network, which provides them distribution service - the same as before joining to a cluster. In this case, the DSO's task is primarily to enable the participation of entities in the cluster as well as to fix its activities on the network. If cluster participants are treated as independent entities, changes are required in the contractual relations between the Operator and all interested parties.

There is a postulate from both DSOs and Clusters that the cluster area, apart from the geographical limitation, should also have a grid limitation, i.e. points defining a cluster area belong to the grid of the same DSO (WKB, 2019). This postulate is justified by the fact that if cluster’s area includes more than one Operator grid area, firstly, this cluster with each DSO must establish individual contractual relations, and secondly, there is a risk that cluster participants will not have the distribution service provided in the same way. It is also to be considered whether a mixed cluster should be allowed to operate on the DSO grid, i.e. some participants are connected to the DSO grid, and some to the own grid. It seems that this is possible provided that the cluster own grid is connected to the DSO network.

Effective functioning of any cluster requires the exchange of information and metering data with the DSO, which is primarily associated with ensuring the proper status of metering. While generators and some of the consumers are metered correctly from the point of view of cluster needs, i.e., meters with load profile registration, remote and automatic data acquisition, the metering of other consumers, including households, for the most part does not meet these requirements. By 2028, it is planned that each DSO in Poland will have installed Smart-Metering meters for at least 80% of household customers (Energy Law Act), which will significantly increase the possibility of new participants joining to clusters.

If clusters start using energy market mechanisms, e.g. purchase and sale of energy, it is necessary to grant it an appropriate status and define its rights and obligations. Typically, this task is performed by the system operator on which a cluster is connected. The role of the DSO is to legitimize the activity of a cluster in the operator's grid by adopting a minimum framework for cooperation, as is done for example for energy suppliers and the Third Party Access (TPA) principle. The operator should also take into account the energy potential of clusters both from the technical side, associated with distributed generation, as well as from the market side - as customers or providers of new services such as DSR, flexibility.

The applicable national rules (RES Act) do not prejudge contractual relations between cluster members and the DSO on whose networks the cluster was established. In the case of distribution services, they are always provided by the Operator of a grid to which a cluster is connected. As for the delivery of energy, cluster participants are clients of the Electricity Suppliers who sell it or buy energy from them. It is also possible to combine both the purchase of distribution services and energy into one contract, i.e. a master agreement.

Along with clusters development it is natural for the structure of clusters to be changed. Usually there is an increase in the number of consumers and producers. Other elements also appear, e.g. energy storage or the need of changing existing business model in a way of using the potential of a cluster in the energy market - to provide flexibility services to the NPS or DSO. The cooperation agreement with DSO must provide for both, a change in structure and behaviour of cluster participants. Any change, if planned, should be analysed by both - the cluster and the DSO. This reduces the risk that, as a result of a planned change, clusters will cease to function for formal reasons.

The loss or resignation of participation, especially in clusters on DSO grid, need a special protection from a situation where clusters ceases to function. DSO, as a public trust entity, must ensure that customers and energy producers are not left on their own.

**The distributed sources impact on the DSO grid**

According to the latest information, in the last two years in Poland there was a fivefold increase in the number of micro-installations connected to DSOs grid, the number of which has already exceeded the level of 760 000 pcs. and 5 340 MW of installed capacity (PTPIREE, 2021). Such a large number of distributed resources is a challenge for DSOs, both from the technical and organizational point of view. Therefore, the impact of distributed resources on distribution network should be considered as opportunities and threats for the network.

The undeniable advantage of distributed generation is the production of energy near to their consumption, which significantly reduces the need for long-distance energy transmission

(typical transmission is mainly from conventional sources), reducing grid energy losses and the load of grid components. Proper stabilization of source operation by using energy storage or mix of generation technologies strengthens the positive impact of distributed sources on DSO network (PEP 2040, 2021). In the case of energy clusters, sources are in principle supposed to balance the energy demand of customers in a cluster, contributing to the creation of energy balanced areas, usually in the long term.

With the increase of distributed generation in distribution network, phenomena such as appeared (Pijarski, 2018; PTPIREE, 2021) :

- problems with maintaining power quality indicators in the network, mainly voltage level,
- overloading of selected grid sections and elements (e.g. MV/LV transformers) due to excessive local generation,
- export of energy surplus to other network areas or voltage upper levels as a result of mismatched production and consumption or excessive concentration of sources in a given area,
- necessity to maintain power reserve in the system for the sources whose production profile depends on the weather conditions (unstable sources - solar, wind).

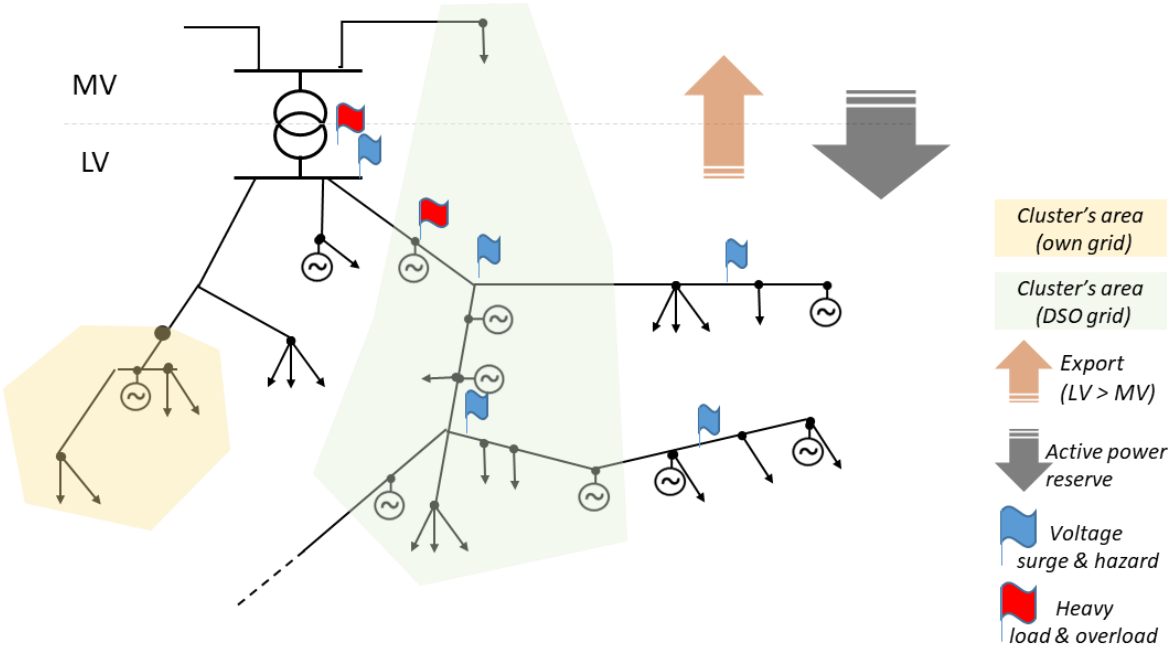


Fig.1 Graphical interpretation of network problems. Cluster areas as background.
Sources: Own Study

One of the reasons for the described problems in distribution grid, is an unprecedented growth of distributed generation in such a short period of time, which cannot be matched by network investments. These investments, which are made in order to improve the grid and accommodate more RES, require sufficient time for implementation and an appropriate level of financing (PEP 2040, 2021).

It should be emphasized here that a development of distributed generation is the main direction of energy decentralization and decarbonization. In such an approach, the role of the DSOs is to broadly support market changes and to reduce or eliminate barriers that prevent this

transformation from taking place. It is necessary to maintain efficiency, security and stability of the electricity grid (Roadmap, 2021)

**Distribution network flexibility**

Saturation of distribution network with distributed energy sources means that DSOs must accept higher variability of energy generation, which in many cases is closely related to weather conditions. This results in moving away from the "generation follows demand" principle to the "demand follows generation" principle. Most of renewable generations are intermittent and (apart from downwards) not controllable. The more type of generation will be connected to the grid, the harder it will be to keep pace with demand by dispatchable generation. Energy storage will play an important role due to fact that not all demand is able to follow renewable. The existing grids are designed to transport and distribute energy from central power plants to local customers. Changing this principle by adding local generation and storage systems will require a total review of their architecture (Vision Paper, 2015). On the other hand, grid users increasingly would like to actively participate in the energy market by adjusting their energy potential (generation, consumption, storage) to the market. In other words, they respond to market signals, e.g. energy prices, by changing their typical behaviour - they optimize energy consumption, produce energy, transforming themselves into Active Consumers (Mataczyńska & Kucharska, 2020).

This unique ability of a power system to respond to most of change in demand and supply, caused by the dispersion of many types of generation resources and/or activating users on the energy market, is called the energy system flexibility.

**Interaction between Energy Clusters and DSO**

Taking into account the previous considerations, clusters and DSO (representing also other grid users) may interact in the following areas:

- the assumption of energy self-consumption of a cluster, results in investments in new generation capacities, which may negative affected on the distribution network, if realized
- due to the territorially limited area of a cluster, there may be a concentration of DER, which may result in sources redispatch ,
- not all network users in a given area are willing or able to participate in clusters. The operator must ensure that everyone has the same level of distribution service, and guarantee the same quality and reliability parameters of supply, including power capacity reserve in the system,
- balancing of an energy cluster through active management of demand, as well as participation in organized forms of the energy market, cause greater variability of flows in the network, which may adversely affect its operation. The operator must increase the flexibility of its own network,
- existing or planned network congestions may effectively prevent clusters from achieving its objectives.

The above outlined Cluster-OSD interaction could be mutually beneficial if the parties find common ground and understand each other's needs.

In the initial phase of development of such initiatives, Cluster-OSD cooperation should occur at least in the following areas:

- location of clusters on the DSO network,
- build new capacity by clusters, including the selection of generation technology,
- support for balancing of clusters by energy storage facilities,
- using the energy potential of cluster participants for the local improvement of grid operation.

In the case a cluster does not plan to build its own distribution grid, i.e. cluster members are connected to the DSO grid, the assumed cluster objectives (related to energy production or ensuring energy self-consumption) must be analysed in terms of the technical capacity of the grid. At least the following aspects need to be taken into consideration:

- whether the geographical area of a cluster coincides with the area of the grid of the same DSO. Otherwise, there is a risk of cluster division into sub-areas, which together will not give the desired effect,
- whether the area of a cluster includes multiple voltage levels e.g. LV, MV, or the area is not too vast. In this case, the location of the sources may be on a different voltage level as the loads or at a considerable distance. This results in additional flows in the network and departure from the principle of production as close to the load as possible,
- whether in the area of a cluster, the Operator has the possibility of connecting new sources.

An important issue for clusters, is the choice of the future energy generation technology. From the Operator's point of view, it is important if the source generates energy stably, is supported by energy storage and if it has the regulatory capabilities. Stable generation allows the DSO to plan grid flows more accurately, which increases the flexibility of the grid and the possibility of connecting new customers without the need for grid expansion (Wasiak, 2015). Furthermore, by appropriately selected the source location, it is possible to significantly reduce technical problems in the grid associated with the expansion of distributed generation (Pijarski, 2018). Operators, on the basis of conducted observations and analyses of the network condition, can indicate locations where it would be advisable to build a new RES. Additional definition of requirements regarding generation stability or control capabilities would allow clusters to build such source on request of DSOs. Benefits from such an action would accrue to clusters - the possibility to build a source for needs of clusters and the Operator - a stable source supports the operation of the network and in some cases, postpones the need for network expansion.

**Clusters as service providers for the DSO**

Activities described as Cluster-OSD interaction, lead to the conclusion that the Energy Cluster can support the operation of distribution system. Properly defining the framework for such cooperation will benefit both clusters and the DSO. This idea of supporting operators in increasing the flexibility of their networks (as defined previously) is reflected in the provisions of the internal market regulation (EC Regulation 2019/943). In line with the provisions of the Regulation 2019/943, to integrate the growing share of renewable energy sources (RES), the

electricity system should make use of all available flexibility resources. The flexibility resources consist of flexible generation, interconnection, demand response and energy storage.

Each network user is entitled to offer its flexibility to the market, and the DSO is entitled to obtain flexibility from entities connected to its network as a service on a market basis (EC Directive 2019/944, Articles 15, 17, 32). In other words, the system user who owns the flexibility resources can, in response to a market signal, commit to a certain behaviour in terms of energy production, consumption or storage. Since the members of a cluster (in the sense of "Citizen Energy Communities") act together, offering flexibility is only possible through aggregation.

The purpose for which the DSO will use the flexibility resources determines the type of service that clusters (or other system user) will provide to the Operator. The referenced Directive 2019/944 and Regulation 2019/943, indicate three types of services that the DSO may use:

(1) flexibility services - defined by the Operator so that the owner of a flexibility resource is able to change of electricity load, generation or storage from their normal or current patterns (reduction or increase) in response to signals (price) from DSO.

Flexibility services can be used for "congestion management", i.e. elimination by DSOs of situations in which all requests from market participants cannot be accommodated, because they would significantly affect the physical flows on network elements which cannot accommodate those flows. A typical example of network congestion is the overloading of power lines or substations caused by excessive concentration of generation on a grid, not adapted to the consumption existing there. Such a situation makes it necessary for the DSO to prevent the negative impact of such a condition (by means of manage the network), reducing the risk of outages. As a result, clusters are unable to achieve its objectives, or this achievement is very limited.

Another area of utilization of cluster resources can be support for planned and unplanned operational activities. As we know, the Operator is obliged to keep the network in good technical condition. Due to the safety of these operation, it is often necessary to switch off the voltage and interruptions in supply. In such cases, energy generation sources or storage facilities in a cluster could provide power to some areas of the grid that are not related to the area of maintenance work but due to network connections have been switched off. The same can be done in case of failure in the grid.

The long-term cooperation of clusters with the DSO may, for a certain period of time, replace the need for network expansion, especially if the new source is built in a location agreed with the Operator. The network development plan shall also include the use of all resources that the distribution system operator is able to use as an alternative to system expansion.

(2) non-frequency ancillary services – services used by a distribution system operator for steady state voltage control, fast reactive current injections, inertia for local grid stability, short-circuit current, black start capability and island operation capability (Directive 2019/944).

The most significant application of this service, is to use technical capabilities of sources operating to control and maintain voltage. This is an important problem in net-

works with high saturation of renewable sources, described in detail above, usually mitigated by proper management of reactive power. Other applications require clusters to have either generation sources stable in production or energy storage. A special case here is "island operation", which can be provided in a given grid area in case of e.g. long-term outages.

(3) redispatching service - means a measure, including curtailment, that is activated by distribution system operator by altering the generation, load pattern, or both, in order to change physical flows in the electricity system and relieve a physical congestion or otherwise ensure system security (Regulation 2019/943).

If the DSO has no other options, it can agree with the network users, including the Cluster, that it is necessary, for example, to reduce generation or stop it altogether. The primary objective here is system security.

The provision of the services outlined above, may take a form of a long- or short-term commitment for which a cluster will receive appropriate remuneration. In principle, the length of the commitment can be determined by the purpose for which the service will be used. For alternatives to network expansion, the duration of the service is calculated in years. For the purpose of congestion management, the periods can be counted either in years - as readiness for service, or in near real time - as countering physical congestion. In the case of voltage control and maintenance, near real-time service times become important (Mendicino, 2021).

## Conclusions

Clusters, as renewable or citizen energy communities, are presented as a new actor in the electricity market. Typically, they aggregate distributed generation, loads or storages over a small network area for self-consumption. They are also places where new technologies can be applied, e.g. energy storage, e-mobility development, smart grid management or local balancing. Clusters have a significant energy potential that comes from distributed resources, therefore they have an impact on the operation of the grid - they can improve or disrupt its operation. This potential, properly used by the operator may support the operation of the power system, i.e. directly the distribution grid and indirectly the National Power System.

The analysis conducted from the perspective of the possibilities of creating a cluster on the DSO network, its potential and possible interactions justifies the thesis that proper Cluster-DSO cooperation supports the operation of the power system. This cooperation should be conducted at least in the scope of considering the needs of the grid when selecting sites for new sources and supporting the flexibility of the grid and the power system through active management of a cluster so that it can provide services to DSOs in a market-based formula. Therefore, it is necessary for the DSO to properly recognize and consider the Energy Cluster as a new market participant with its potential and opportunities. The operator should also develop rules for such cooperation that are non-discriminatory and without unnecessary barriers. Ultimately, the Operator, should design an appropriate local flexibility market to address the problem of congestions in the distribution network and to deliver ancillary services to the power system.

These recommendations are part of the new energy market model, shaped by the ongoing energy transition towards distributed generation.

## Bibliography


1. RES Act - Ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii, (Dz. U. z 2021 r. poz. 610, 1093,1873)
2. Energy Law Act - Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2021 r., poz. 716)
3. Market Directive - Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 20193 on common rules for the internal market for electricity and amending Directive 2012/27/EU, Official Journal of the European Union , L158/125, 14.06.2019.
4. Market Regulation - Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 20192 on the internal electricity market , Official Journal of the European Union , L158/54, 14.06.2019.
5. REDII - Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (recast), Official Journal of the European Union, L 328/82, 21.12.2018.
6. KIKE – Krajowa Izba Klastrów Energii, [online] https://kike.org.pl/ (access: 01-12-2021)
7. Mataczyńska, E., & Kucharska, A. „Klastry energii. Regulacje, teoria i praktyka" Instytut Polityki Energetycznej im. I. Łukasiewicza, (2020), p.46-85
8. Mendicino L., "DSO Flexibility Market Framework for Renewable Energy Community of Nanogrids", Energies 2021, 14, https://doi.org/10.3390/en14123460 (access: 01-12-2021)
9. PEP 2040 – „Polityka Energetyczna Polski do 2040". Obwieszczenie Ministra Klimatu i Środowiska z dnia 2 marca 2021 r. w sprawie polityki energetycznej państwa do 2040 r. Monitor Polski 2021 r. poz. 264.
10. Pijarski P. „Analysis of Voltage Conditions in Low Voltage Networks Highly Saturated with Photovoltaic Micro Installations", Acta Energetica 3/36 (2018) | 4–9
11. PTPIREE, Mikroinstalacje w Polsce, stan na dzień 31 października 2021r. [online], http://www.ptpiree.pl/energetyka-w-polsce/energetyka-w-liczbach/mikroinstalacje-w-polsce (access: 01-12-2021)
12. "Roadmap on the Evolution of the Regulatory Framework for Distributed Flexibility", A joint report by ENTSO-E and the European Associations representing DSOs (CEDEC, E.DSO, Eurelectric, GEODE), 2021, https://www.edsoforsmartgrids.eu/dso-tso-roadmap-on-the-evolution-of-the-regulatory-framework-for-distributed-flexibility-2/ (access: 01-12-2021)
13. Sikora M. „Współpraca Klastra z OSD. Wybrane zagadnienia", Smart Grids Polska, 2/2018 (20), s.39-41
14. Sołtysik M., Klastry energii jako narzędzie budowy energetyki obywatelskiej, Zeszyty Naukowe, Instytutu Gospodarki Surowcami Mineralnymi i Energią Polskiej Akademii Nauk rok 2018, nr 105, s. 15–24
15. Wasiak I., "Wybrane problemy integracji rozproszonych źródeł energii z siecią dystrybucyjną", Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 45, 2015 r.

16. WKB [Wierciński Kwieciński Baehr] „Analiza prawna barier dla rozwoju energetyki rozproszonej na potrzeby tworzenia klastrów energii oraz propozycje zmian przepisów prawnych mających na celu eliminacje zidentyfikowanych barier", na zlecenie Ministerstwa Energii, 2019 r.
17. Vison Paper - "The Journey to 'Green' Energy or 'a Quest for Flexibility'", tech.rep. Eandis 2015, https://www.edsoforsmartgrids.eu/a-journey-to-green-energy-2/ (access: 01-12-2021)

**Marek Sikora** – M.Sc., Graduated from the Faculty of Electrical Engineering and Electronics of Lodz University of Technology and postgraduate studies "Electricity Markets". An expert in the energy industry with many years of professional experience. Professionally, he deals with problems of balancing the power system, energy transition model and with concepts of energy communities.
ORCID: 0000-0001-8328-4042

# Vulnerability of power system to cyberattacks

*Tomasz Chyła, Weronika Maciejewska*

**Abstract:** Electricity significantly determines the possibility of development of technical civilisation, both on a global and local scale. The availability of energy determines the diversity of civilisational development of communities inhabiting particular areas of the earth. The Internet, in turn, as a tool conducive to the human species, induces many opportunities while simultaneously generating threats. The Supervisory Control and Data Acquisition (SCADA) systems used in the power industry are key elements in the operation of industrial facilities and critical infrastructure, while also being vulnerable to cyberattacks. Successful cyberattacks can cripple internal processes, cause financial losses and potentially lead to unwanted block-outs.
**Key words**: SCADA, energetics system vulnerability, cybersecurity

## Introduction

The technological advances that have taken place in the last few decades have made our lives easier in many areas. Social networking sites, GPS navigation, transfers via the Internet, electronic registration for doctor's appointments, or the press available on the Internet. Thanks to the Internet, we can not only do countless things faster and easier, but we can also move with a single click to almost any corner of the world. In counterpoint to the positive side of technological progress come the dangers of the highly computerised modern world. The development of information technology creates not only new opportunities but also a huge number of risks. The aspirations of states to create information societies have made these technologies a source of threat to state security.

Nowadays, the state's vulnerability to threats in the area of cyberspace, related to the hostile use of information technology, is increasing. Nowadays the entire critical infrastructure, for example all state institutions, security services, power plants, as well as any kind of transport or water management institutions, use IT systems. Digitization has become an integral part of the development of every area of today's life. Although the benefit it brings is invaluable, it also carries many threats from cyberattacks that are difficult to predict and, in many cases, to identify. They are growing as fast as digitization is progressing. It is difficult to imagine how serious a threat to many sectors of the economy is posed by cyberattacks, especially for those sectors whose infrastructure is considered one of the critical elements of the state functioning.

This paper presents cyberattacks that target networks used in power plants, specifically on the SCADA (Supervisory Control and Data Acquisition) system. To explain the forms and methods of carrying out cyberattacks on power grids, the ways in which the power system in Poland is organised and how the SCADA system works will be presented. This will be followed by an analysis of the cyberattacks carried out against this system and their implications for future attack methods. The main objective of this paper is to look at the vulnerability to cyberattacks of the SCADA systems used in power systems. The research question of the paper is: Is the SCADA system resilient to cyberattacks?

## The power system

The power system is considered as one of the most important components of critical infrastructure. The effective functioning of the entire economy of the country depends on ensuring the continuity and security of electricity supply. Hence, any undesirable, unforeseen and violent phenomena in any element of the power system will have a fundamental impact on all processes curried based on electricity as the primary carrier. (Henning 2015:196).

The power system is a set of interconnected elements used for generation, processing, transmission, and distribution of electricity as well as dispatch centres that control the operation of the system. These elements with IT infrastructure (hardware and software) form a system of functional connections, cooperating under strictly defined rules and are capable of permanently maintaining defined reliability and quality parameters of electricity supply and meeting the conditions applicable to cooperation with other interconnected systems also with other countries by appropriate cross-border connections. Due to the functions performed, the power system could be divided into two main subsystems (Bezel 2018:1):

- generation (power plants),
- transmission and distribution (power lines, stations, and substations).

Proposed division is important from the security of supply point of view, but it is not the only one. It should be remembered that problems with the consumption (load) of power generated by large power plants may have a significant impact on ensuring continuity of supply and power system security.

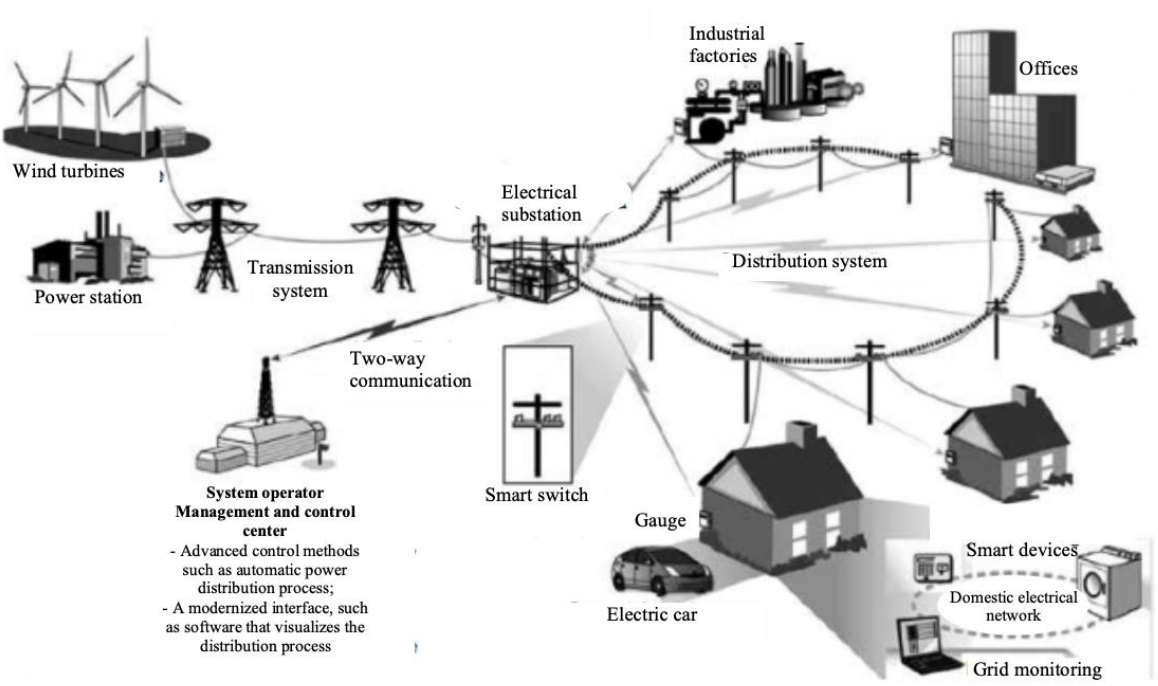


Fig. 1. General overview of the electricity supply infrastructure system
R. Henning, Cyberterrorism vs critical infrastructure part I. The Energy System, Bellona Quarterly 4/2015, p. 199

## The SCADA system

Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems are key elements in the operation of industrial facilities and critical infrastructure. Successful cyberattacks can cripple internal processes, cause financial losses, and potentially result in the loss of human life (Controlengenering 2017).

Many organisations in critical infrastructure have implemented SCADA/ICS to automate process control and data collection. These systems have become important targets for attackers looking to disrupt business operations. Unfortunately, many ICS systems are not designed to be immune to cyberattacks and as a result, cybercriminals are attacking these systems with greater intensity. Therefore, it is important when designing these systems to pay great attention to their preparation in the event of possible cyber attacks.

Today's level of sophistication of SCADA systems and the fact that they have been used in the power industry for several years makes it practically impossible to know whether manual process control would still be possible. In addition, noting the continuous development of information technology, further tightening of the connections between computers and the power system is to be expected. Especially in the light of smart grid projects being put into use (Henning 2015:197). Nevertheless, the high processes automation in the energy sector does not release companies from the need to develop procedures related to the unforeseen inability to perform a given process in an automatic form. Each energy company knows the capabilities of its devices and has action scenarios in case of various problems. In addition, by complying with the provisions of European and national regulations, companies develop the necessary safeguards and separate management methods of maintaining the security of the power system.

Operation of the power system is highly dependent on computers and ICT networks, that is why the power system may become the ideal target for a cyberattack. It is the area of critical infrastructure where SCADA type devices started to be introduced intensively The SCADA systems collect data from machines and measuring devices in real time, which enables supervision of the production process. Visualisation of current data or historical data is also an important feature. The SCADA system allows user to control the production process by setting parameters from the panel enabling alarms detection and sending necessary information to operators In addition, SCADA archives data from the production process. It was mainly introduced to control and supervise remote installations and equipment. Energy companies use SCADA to manage the processes of power generation, transmission, and distribution, switching on and off electrical circuits and setting safety thresholds to protect the installation from overloads (Malko, Wojciechowska 2015:11).

SCADA systems improve the efficiency of a critical industrial system and provide better protection for the equipment used. They also improve staff productivity. SCADA frameworks redirect immediate alert warnings to observation stations using an attested monitoring stage, advanced communications and state-of-the-art sensors (Yadav, Paul 2020:1). It may be considered, at this stage, that this is not a sufficient safeguard. The modernisation of SCADA systems has made them more vulnerable to attacks from anywhere in the world (Miller, Rowe 2012:52). The modernisation of the SCADA system, standardisation of communication protocols, and increasing interconnectivity have drastically increased the number of cyberattacks on the SCADA system over the years. These types of attacks are becoming increasingly sophisticated.

The proper operation of the SCADA framework should be crucial for the enterprise because the result of an outage can be a failure that can be very costly or even cause loss of human life (Cherdantseva 2016:27).

Most attacks on transmission networks are not transparent. Threats can exploit various attack vectors, taking advantage of existing flaws in industrial device configuration and network segmentation, as well as vulnerabilities in operating systems. Security experts involved in testing corporate IT systems reveal that enterprises typically have insufficient perimeter protection against external attacks, and industrial networks are not adequately isolated from corporate systems (TOP20 2018:4). Another reason why the power system can become the target of a cyberattack is that the power system is a highly interconnected and interdependent system and is therefore susceptible to cascading effects. In such a system, it is possible for a system failure to occur at one location, which will spread exponentially and lead to a failure of the entire system. In addition, the chain dependence of processes occurring in the power system translates into the possible occurrence of cascade shutdowns, eventually leading to blackout.

According to reports prepared by specialists, the power system is the most frequently attacked component among all networks included in critical infrastructure systems. A significant proportion of these cyberattacks, particularly over the last few years, have been successful for the attackers. Typically, complex and sophisticated malware is used to carry out these types of attacks. A typical method of infecting a network is carelessness on the part of an employee, such as plugging in an infected USB device. During such a cyberattack, the identity of the attackers generally remains anonymous (Henning 2015:197).

Control systems with SCADA software are the most sensitive systems in the power generation sub-sector. Most of them use human-machine interface software, enabling the user to interact with the plant's devices and equipment. In a situation where a hacker gains access to the control software, this is equivalent to complete transparency of the software.

The vulnerability to cyberattacks stems from the fact that the SCADA architecture was developed before cyberattacks became an issue. Large power plants and energy providers are at risk because these systems were introduced into then existing infrastructures decades ago and were not protected from attacks (Malko, Wojciechowski 2015:22).

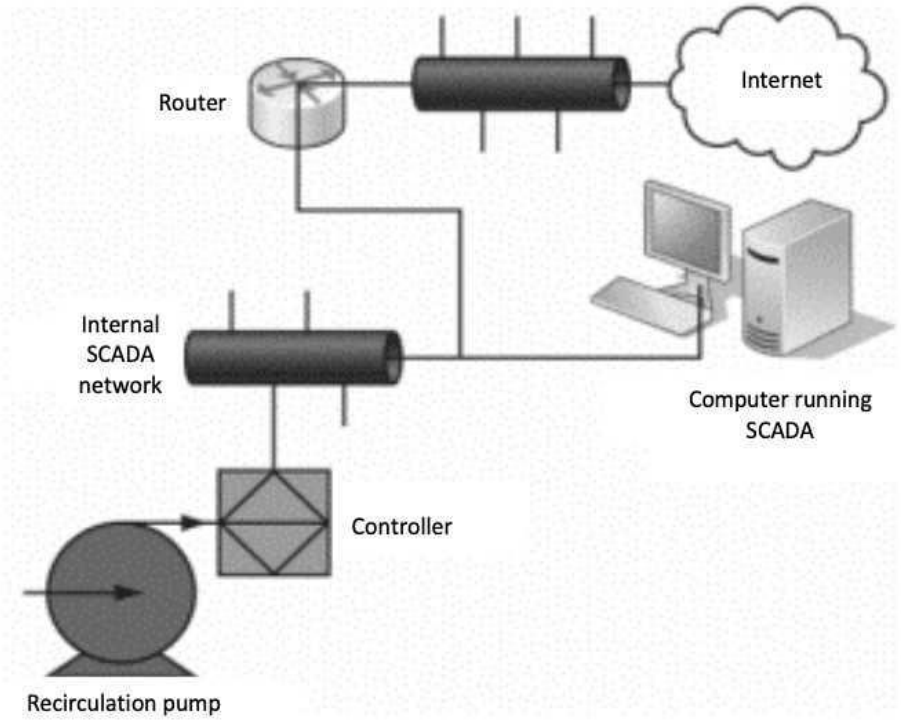


Fig. 2. Information transmission system not secured against cyberattacks
J. Malko, H.Wojciechowski, Sektor energetyczny i cyberbezpieczeństwo, Instytut Energoelektryki, Politechnika Wrocławska, "Nowa Energia" - no. 1/2015

Monitoring tools, as used in SCADA systems, are helpful in integrating networks. In the past 15-20 years, much of the network infrastructure was built to optimise such targeted SCADA systems, but attacking those systems was not expected. This is because we were dealing with realities completely different from those of today (Malko, Wojciechowski 2015:24). Therefore, it is worth considering, how do hackers exploit gaps in systems and break into energy infrastructure systems?

According to a (Symantec 2015) report, many SCADA and ICS systems operate outside traditional security constraints and show vulnerability to hacking attacks. Sometimes it only takes a single click to create danger and protecting against it requires far more complex actions. The attacks are aimed at the weakest points of the systems. The weakest elements could be classified as:

- inadequate, weak protocols – most often this is a result of the fact that during development of communication protocols for SCADA systems, security was not taken into account. Moreover, almost every SCADA system uses the same protocols, making it easy for potential hackers to launch an attack,
- lack of proper training – employees are the most vulnerable element of the entire SCADA system. Social engineering, phishing or spear-phishing attacks are very common. Inadvertently clicking on an infected email can compromise the entire system,
- unsecured SCADA applications – Internet and computer applications are widely used to modify and monitor various SCADA system components. However, many of these applications do not meet modern application security requirements.
- poor separation of IT and OT – it happens that many organisations have an inadequate separation between IT (information technology) and OT (operational technology),

which creates a significant risk. IT is critical to every organisation today, yet not using the same routers and communication networks for IT and SCADA applications is a basic requirement to ensure security. However, many installations lack this segregation.

- lack of maintenance – manufacturers and vendors create products with default configurations that operators can change with each installation. Some operators, due to the lack of awareness or a false sense of security, do not change the default settings. This poses a potential security risk to the system. Moreover, it is often the case that hardware as well as software are not updated to the latest standards, which also poses a risk (Securing SCADA 2020).
- HMIs (Human-Machine Interfaces) display data from various sensors and machines connected to the SCADA system to help users make decisions that they can also implement using the same interface. Because of their capabilities and role in SCADA systems, HMIs are an ideal target for potential cybercriminals seeking to gain control of processes or steal critical information (SCADA Vulnerabilities 2019).

Cyberthreats to the power sector can take several variants and be initiated from different sources. Several types of attackers can be singled out due to the crucial importance and specificity of the industry:

- politically motivated actors whose aim is to sabotage the infrastructure by disrupting or destroying or humiliating the victim and causing image damage,
- hacktivists – actors motivated by moral/ideological motives, aiming to publicise an attack and compromise the victim,
- economically motivated actors driven by a desire for profit, with the aim of gaining financial benefits (e.g., from ransomware) (Cyber Security 2019).

Cyberattacks on SCADA software, or targeting industrial automation components, take many forms, and mainly aim to cause physical damage and destruction. These types of attacks are knowledge-intensive and can cause very serious damage, especially to key service providers; an example of such a cyberattack is Stuxnet, which is a computer worm that originally targeted Iran's nuclear facilities and has since adopted and spread to other industrial and power generation facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. After it was discovered in 2010, it generated a flurry of media attention because it was the first known virus capable of damaging hardware and because it appeared to have been created by the US National Security Agency, the CIA and Israeli intelligence.

In order to understand the attacker's thinking and actions, the attack should be broken down into several stages. At the beginning the attacker performs reconnaissance, that is, gathers information about the target. At this stage, the attacker can be helped by a web tool such as Shodan. The web address "shodan hq.com", which is similar to Google, functions as a search engine that is designed to map and collect information about devices and systems connected to the Internet. Shodan is sometimes referred as an Internet of Things (IoT) search engine. Software applications include market research, vulnerability analysis and penetration testing, and hacking. Shodan allows to detect devices connected to the Internet at any time, the location of those devices, and their current users. Such devices can be found in almost any type of system, including business networks, surveillance cameras, industrial control systems (ICS) and smart

homes. Entering this address and finding the SCADA gateways gives a clue to each threat, with the potential user given a name and password. It is easy to access the aggregate site (e.g., South Korea) and request information on e.g., current power level of the units, or unit instantaneous fuel consumption. Once identified, the attacker finds a way to get into the corporate network through, for example, a company website, malicious emails or an infected USB drive. The cyberattack thus becomes trivial. In a corporate network, it looks for information about control systems (ICS networks), these are: controllers, relationships between controllers and certain processes, company procedures, passwords, etc. (Zwalczanie 2020). Metasploit, an open tool for penetration testing and breaking security of ICT systems, can be equally dangerous. It is a tool used to obtain information on the status of various equipment, including monitoring of the turbine control system or the reservoir management system of pumped storage power plants. All elements, covered by common access, are vulnerable to attacks. The history of each attack remains in memory and can be reused. Even a novice hacker can benefit from this (Malko, Wojciechowski 2015:23).

After gaining access to the network, the attacker verifies its architecture and the information acquired earlier. From the attacker's point of view, this stage is critical if they want to make an effective attack. How does the attacker proceed? For example, they may try to send harmless commands to the target controller or try to change the values of some controller parameters. Importantly with this action, to avoid detection, they should ensure that normal values continue to be reported. These actions are intended to cause the attacker on the day of the attack to be able to take control of the system and cause the desired damage (Combat 2020). With the widespread emergence of Smart Grid technologies, ever more new energy supply systems are entering the so-called Internet of Things, which is characterised by a large number of interconnected systems but low security, implying cyberattacks. Attacker activities that take place inside the control network can be categorised as follows:

- Field-to-Field – This is an attack from one infected remote station or peripheral to another,
- Centre-to-Field – An attack that initiates traffic from the control centre designed to harm or take control of a peripheral,
- Field-to-Centre – An attack that initiates traffic from a remote station to a control centre,
- In Field – An attack from one peripheral to another, within the same location.

In addition to exploiting bugs or underdeveloped systems, hackers also use the "human factor" to their advantage. They use a virus similar to Stuxnet, for example. But the primary tool is to steal correspondence and the curiosity on the part of the addressee – the object of the attack – will do the rest. At a completely unexpected point, you can enter a USB link and then make use of it in a workstation. When this happens, the forged program will start broadcasting the data collected in the system to the hacker, who controls the course of the attack with their commands and control program (Malko, Wojciechowski 2015:24).

There is also a class of "certified hackers" or "white hat hackers". Unlike "black hat hackers" who act with malicious intent, ethical hackers seek to find weaknesses in systems, with the goal of defining and eliminating them. The idea is not just to achieve the required level of security, but to act holistically, at the level of the software package and using physical access.

**Examples of cyberattacks on the power system**

According to a Forrester study, 58% of organisations using SCADA/ICS reported a breach between 2018 and 2020. Only 10% indicate that there has never been a breach (Fortinet 2021:3).

The most notorious cyberattack on industrial systems is the aforementioned Stuxnet, a virus designed to prevent Iran from developing a nuclear programme. The virus exploited not only previously unknown operating system vulnerabilities, but also security holes in the PLCs (Programmable Logic Controller) that were an integral part of the systems at Iran's Natanz nuclear facility. As a result of its use, the attackers managed to damage nearly 1,000 centrifuges at the uranium enrichment plant, causing Iran's nuclear programme to be delayed by more than 5 years. The creators of the virus did not achieve their goal at a low cost, because the development of such a complex solution consumed resources exceeding at least tens of millions of dollars. The precision strike required not only the work of programmers, but also experts with knowledge of ICS, SCADA and the Simatic PLCs themselves. Certainly, the virus was thoroughly tested before it struck, so the purchase of the very P1 centrifuges used at Natanz must have been funded by the budget for cyberweapons development.(Warsawinstitute 2020).

Ukraine was one of the first countries to experience cyberattacks on its power generation system. The first major attack targeting critical infrastructure ensuring electricity supply took place on 23 December 2015 in the western part of Ukraine. As a result, nearly half of the 1.5 million inhabitants were without electricity for several hours. The cause of the problems was malware called "BlackEnergy" that found its way into the computer system via an email message. The message was opened by an unknowing employee at the producer and supplier of energy Prykarpattya Oblenergo. The effect of installing the software was to erase data from some of the hard disks and thus render the systems supplying electricity inoperable. Less than a year later, and exactly on 18 December 2016, a similar event was recorded in Kyiv. At that time, the target of the attack became the system transmitting energy to the city, so that for several hours restrictions in supply covered the northern part of the Ukrainian capital (Biznesalert 2020).

The software that has been identified as responsible for the attacks in Ukraine has also been registered in other countries – including Poland, as well as in the USA. As a result, the U.S. cybersecurity services were involved in the investigation after the aforementioned attacks. The Russian Federation was blamed for the attack, pointing to a hacking group linked to the Russian government. In 2018, the head of the Cyber Police, Serhiy Demediuk, in an interview with Reuters, emphasised that 99% of attacks on Ukrainian IT systems come from Russia (Biznesalert 2020).

However, Ukraine and the US are not the only countries that have been affected by attacks on power plants. A similar situation was recorded in June 2017. At that time, hackers (it was not specified at the time from which country) attempted to penetrate the computer networks of nuclear power plants and energy companies in the USA and other countries. An example cited in the media was the attack carried out against Wolf Creek Nuclear Operating Corporation, the operator of a nuclear power plant located near Burlington, Kansas. The information available at the time indicated that the attackers had not gained access to the control

room of the nuclear power plant. Irish media also reported on a successful cyberattack on EirGrid, the operator of Ireland's electricity grids, in April 2017 (Wysokienapięcia 2018).

It should be added that for two massive global ransomware attacks, the perpetrators demanded a ransom in exchange for decrypting the content – the US, as well as British intelligence blamed North Korea (May's WannaCry attack) and Russia (June's NotPetya attack). NotPetya reached, among others, computers in Ukrainian power companies, but did not lead to disruptions in the operation of power plants and the power system. However, there was an interruption of the radiation monitoring system at the nuclear power plant in Chernobyl (Wysokienapięcia 2018).

Another attack that became the first known cyberattack to directly interact with a governmental security system (SIS – the last line of automated security protection for industrial facilities designed to prevent equipment failures and catastrophic events such as explosions or fires) is Triton, also referred to as Trisis or Hatman. Triton was first discovered in 2017 in Saudi Arabia when it was noticed that the plant's security systems had been breached (Triton 2018). Computer security firm Symantec claimed that the malware known as Triton exploited a vulnerability in computers running the Microsoft Windows operating system (The Guardian 2017). In 2018, FireEye, a cybersecurity research firm, reported that the malware most likely came from the Central Scientific and Research Institute of Chemistry and Mechanics (CNIIHM), a research unit in Russia. Interestingly, traces of the hacking group behind this destructive malware have recently been found. Researchers at FireEye say that this failed attempt did not deter the group that was discovered at the new location. However, the name of the company was not disclosed. Although researchers have relayed that the victim was also a "critical infrastructure facility" and that Triton operators were present on the victim's systems for nearly a year. FireEye's Mandiant cyberforensics department was involved in investigating the breach, but the company was silent on what damage – if any – was done (ZD Net 2019).

In 2014, Symantec reported cyberattacks on about 1,000 companies in more than 80 countries between February and July 2013. In Poland, energy and raw materials companies were targeted. The purpose of this attack was to steal information, but – as Symantec representatives claimed – the infected software was also capable of taking control over the infrastructure managing the production and sabotage. The variety and intensity of cyberattacks carried out indicate an increase in activity and adapting the forms of attacks to changing environmental conditions. This means that SCADA systems should be continuously adapted and secured against potential intrusion into them.

**Ways to protect SCADA systems from threats**

One of the most effective solutions to protect against cyberthreats is to physically disconnect from the Internet and external devices. However, this is currently not a viable solution, if not impossible, as Internet access is critical to the day-to-day operations of most businesses. However, this should be included in the country's critical infrastructure, such as power plants. It is also possible to implement security without compromising internet connections. Such methods include (Securing SCADA 2020):

- Security training for employees – as you could see in the examples given above, most attacks are initiated by employees responding to messages sent by attackers. Employees

should also be trained on the social engineering ploys that hackers can perform. And above all, they should be knowledgeable and follow the rules of secure passwords.

- Strong segregation of IT and OT infrastructure – routers and communication infrastructure used for IT and OT communications should be separated. Strong segregation limits the access of potential intrusion into IT systems, OT will be safe from attacks conducted over the Internet.
- Access control – as mentioned above, personnel are the biggest weakness in any system. Not every SCADA user needs the same scope of knowledge and access to all system components. Implementing user controls will help reduce potential attacks from rogue employees.
- Fibre optic cables – attacks that rely on eavesdropping are quite common in cyberwarfare. If the network is breached, fibre optic cables provide a higher level of security. When a fibre optic cable breaks, the loss of signal is so great that the attacker will not get enough data.
- Firewalls – having firewalls is a basic form of internet security, even if we are talking about regular internet users. However, it must be remembered that the firewall put in place should be strong enough and regularly updated to avoid the emergence of new threats.
- Unidirectional Security Gateways (USG) – however, firewalls alone are not the safest option because it is known that every software has vulnerabilities that can be exploited. USGs provide an additional layer of security by using hardware with limited capabilities that can only send information in one direction. Cyberattacks require two-way communication to launch an attack, and USGs prevent this communication.
- Network Security Procedures – regular audits and penetration testing should be conducted to verify the security measures implemented to ensure network security. This will make security a way of thinking for the organisation rather than an afterthought.

The need to implement optimized anti-virus programs.

## Conclusions

It is indisputable that as digitalisation and technological advances increase in the coming years, the importance of cyberspace in the lives of individuals, societies, countries, and businesses will continue to grow. However, this is a sphere that for the classical concept of defence, given the blurring of boundaries, is still not quite normalised. Nevertheless, effective protection of the most important components of the state, i.e. the national critical infrastructure, against cyberattacks should be a priority nowadays, as well as securing the physical land, sea and air borders.

Research analysis of cyberattack examples show that cyberattacks are a real threat not only to ordinary Internet users, but also to critical infrastructure, including all power system. Cybersecurity experts agree that the SCADA systems used in power system are now more vulnerable to cyberattacks than before. This is because, firstly, the functioning of the power system is highly dependent on computers and ICT networks. Secondly, the modernisation of SCADA systems has made them more vulnerable to attacks from anywhere in the world. The moderni-

sation of the SCADA system, standardisation of communication protocols, and increasing interconnectivity have drastically increased the number of cyberattacks on the SCADA system over the years. Moreover, these types of attacks are becoming more sophisticated.

It is true that the attacks so far have not caused large-scale physical damage. Among other things, this is due to the fact that such an advanced attack requires not only considerable skills, but also technical knowledge and large financial resources. However, this doesn't mean that such attacks won't happen more often, because the stakes are high. Over the years, the number of attacks on industrial systems is clearly increasing, although certainly many of them, especially those aimed at industrial espionage, remain in deep cover. Looking at the evolution of cybercriminal activities, however, we can be sure that we will hear bout similar incidents increasingly often.

## Bibliography


1. (Henning 2015) R. Henning, *Cyberterroryzm vs infrastruktura krytyczna cz. I. System energetyczny*, Kwartalnik Bellona 4/2015.
2. (Bezel 2018) System elektroenergetyczny https://bezel.com.pl/2018/08/01/system-elektroenergetyczny/ (accessed 05.11.2021).
3. (Controlengenering 2017) Kluczowe elementy i strategie bezpieczeństwa przemysłowych systemów sterowania ICS https://www.controlengineering.pl/kluczowe-elementy-i-strategie-bezpieczenstwa-przemyslowych-systemow-sterowania-ics/ (accessed 02.11.2021).
4. (Malko, Wojciechowska 2015) J. Malko, H.Wojciechowski, Sektor energetyczny i cyberbezpieczeństwo, Instytut Energoelektryki, Politechnika Wrocławska, "Nowa Energia" - nr 1/2015.
5. (Yadav, Paul 2020) G. Yadav, K. Paul, Architecture and Security of SCADA Systems: A Review 2020, p.1.
6. (Miller, Rowe 2012) B. Miller, D.Rowe, A survey scada of and critical infrastructure incidents. In Proceedings of the 1st Annual Conference on Research in Information Technology, RIIT '12, New York, NY, USA, 2012, p. 52.
7. (Cherdantseva 2016) Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart, A review of cyber security risk assessment methods for scada systems, [in:] Computers & Security, 56:1-27, 2016.
8. (TOP20 2018) THE TOP 20 CYBERATTACKS on Industrial Control Systems Andrew Ginter, VP Industrial Security, Waterfall Security Solutions Version 1.1, May 2018 https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf (accessed 02.11.2021).
9. (Securing SCADA 2020) Securing SCADA Systems from Cyber Attacks 2020, https://control.com/technical-articles/securing-scada-systems-from-cyber-attacks/ (accessed 07.11.2021).
10. (Vulnerabilities SCADA 2019) One Flaw too Many: Vulnerabilities in SCADA Systems 2019 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (accessed 07.11.2021).
11. (Cyberbezpieczeństwo 2019) Cyberbezpieczeństwo sektora elektroenergetycznego 2019 https://www.muratorplus.pl/technika/elektroenergetyka/cyberbezpieczenstwo-sektora-elektroenergetycznego-aa-2yeU-fL5b-bbLk.html (accessed 06.11.2021).

12. (Zwalczanie 2020) Zwalczanie cyberataków w przemyśle i energetyce 2020 https://automatykab2b.pl/prezentacje/46591-zwalczanie-cyberatakow-w-przemysle-i-energetyce (accessed 07.11.2021)
13. (Fortinet 2021) Report Fortinet Independent Study Finds That Security Risks Are Slowing IT-OT Convergence 2021 p.3 (accessed 07.11.2021)
14. (Wysokienapięcia 2018) Energetyka na celowniku rosyjskich hakerów https://wysokienapiecie.pl/8966-rzad-usa-energetyka-na-celowniku-rosyjskich-hakerow-cyberatak-wysokienapiecie/ (accessed 08.11.2021).
15. (Triton 2018) PROJECT TRITON The First ICS Cyberattack on Safety Instrument Systems 2018 https://www.nozominetworks.com/labs/research-projects/triton/ (accessed 07.11.2021).
16. (The Guardian 2017) https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant (accessed 07.11.2021).
17. (ZD Net 2019) https://www.zdnet.com/article/triton-hackers-return-with-new-industrial-attack/ (accessed 07.11.2021).
18. (Securing SCADA 2020) https://control.com/technical-articles/securing-scada-systems-from-cyber-attacks/ (accessed 07.11.2021).
19. (Symantec 2015) New Energy Report (43)/2015 ISSN 1899-0886 p.11
20. (Warsawinstitute 2020) Witajcie W cyberwojnie, Raport Specjalny — Wiktor Sędkowski 17/12/2020 p.8-10

**Tomasz Chyła** – M.Sc. lieutenant commander, works as a senior lecturer in the Faculty of Command and Naval Operations of Polish Naval Academy in Gdynia. His scientific interests focus on energy development (especially renewable energy sources and gas) in national security context and implementation of modern energy technologies.
ORCID: 0000-0002-3489-1185

**Weronika Maciejewska** – received a master's degree in National Security from the University of Gdansk. Currently, she is a student of MA studies in the field of Information Systems in Security with a specialization in Cybersecurity. While working in the Pomeranian Office of Personal Data Inspectors, she is constantly developing in the field of information protection and cybersecurity by conducting training courses and workshops for students and companies.
ORCID: 0000-0003-3712-7833

# New Trading Hub Europe (THE): A review

*Tomasz Chrulski*

**Abstract**: There As of 1 October 2021, the existing market areas in Germany, GASPOOL (GPL) and NetConnect Germany (NCG), have been merged into a new German national gas market called Trading Hub Europe, or THE for short. This market, as a result of the merger, could become a competitive and even the most important gas hub in the European gas market. The background to this is that the transmission and storage infrastructure in Germany is very well developed. Another fact is the fact that Germany in 2021 consumed the most natural gas in comparison with other European countries. This article presents a review of the literature on gas hub and specifically examines the new gas hub in Germany. Natural gas prices on THE in the early days of its launch indicated that they were not out of line with prices on other European gas hubs. The article notes the fact of the merger and reminds other developing European countries of the importance of having their own gas hub.
**Key words**: THE, European Gas Hub, natural gas, ENTSOG

## Introduction

As of 1 October 2021, the existing market areas in Germany, GASPOOL (GPL) and NetConnect Germany (NCG), have been merged into a new German national gas market called Trading Hub Europe, or THE for short. The market is the result of the merger of the existing market area managers GASPOOL Balancing Services GmbH and NetConnect Germany. By merging together THE can become a major competitor to the Dutch and UK exchanges. THE's core business areas include the management of balancing groups, the operation of virtual trading points and system balancing. The merger has resulted in one of the largest natural gas hubs in Europe which should be noted and presented to a wider audience. In the further part of the article, an analysis of the literature review related to the functioning of gas hubs was undertaken and the new THE's gas hub was characterised and the gas price in the first week of the new hub's operation was presented.

## Review of the literature

At the current time, the natural gas market is developing dynamically, new transmission networks are being built and many consumers are switching from coal to natural gas. Perhaps this is due to the fact that gaseous fuel is presented as a transitional fuel in the pursuit of the Fit for 55 targets. The regulatory and infrastructural overhaul of the natural gas market is expected to lead to the creation of some kind of commercial centre in a specific territory, which will make it possible to reduce the price of gaseous fuel for consumers. A gas hub is such a centre. A physical hub is an ageographical (centrally located and sufficiently inter-connected) point in the network where a price is set for naturalgas delivered at that specific location (IEA, 2013). In contrast, the European Energy and Gas Regulators Group defines a gas hub as a trading platform for physical and or financial transactions in natural gas. It can be a physical point at which a number of networks across pipelines meet or it can be a virtual (balancing) point. The

hub should provide access for customers in the short, medium and long term. Price transparency should be an important characterising factor (CER). The operation of gas hubs arose from market liberalisation and a change in the gas pricing mechanism to create competitive and transparent markets (Xunpeng, 2017).

In regulatory aspects, for quite a relatively long time there were no detailed guidelines in the area of legal mechanisms defining the functioning of gas hubs. This conclusion was already reached in 2014. (Mirello, 2014). It was only in 2018 that the implementation of the third energy package in the gas sector attempted to introduce some regulation. More precisely, the third energy package introduced the idea of a balance of European gas hubs. It was subsequently detailed in the Gas Target Model. The balance was supposed to guarantee competition (Pikus 2019).

Academic publications often indicate that gas hub maturity is achieved in a 10-15 year process. Through third-party access to infrastructure (unbundling of infrastructure capacity), bilateral trading, price transparency, OTC intermediation, entry of non-physical players, creation of exchange products based on underlying physical contracts. The literature indicates that liquidity in general, which is defined as the ability to buy and sell goods quickly without significant price fluctuations, is also very important. Volatility, as a measure of price movement in transactions, transparency, reliability, timeliness, trading volume are also important characteristics (Costescu *et. al*., 2018)

Other publications also highlight that creating a gas trading hub takes time, but also investment inputs, political will (Reuters, 2017). The basic and obvious factor is an infrastructure consisting of an extensive network of gas pipelines with a large coverage and density, with the technical capacity to transport natural gas in a short time. Other elements of gas infrastructure, such as domestic production, connections to neighbouring countries, underground gas storage facilities and LNG terminals, are also important. All these elements make the market broadly diversified, which is beneficial to avoid the market being dominated by a few players.

**Gas hubs in Europe**

Gas hubs in the gas industry first emerged in the US market, operating as physical locations, typically where multiple pipelines cross, often near storage facilities (Fulwood). Gas trading hubs emerged in Europe in the 2000s, with the oldest and most mature gas trading hub in Europe being the UK's National Balancing Point (NBP) (Heather, 2021).

The other leading gas trading hubs in Europe can also be mentioned here. Specifically in Central and Eastern Europe, such a hub is the Central European Gas Hub AG . As a Virtual Trading Point operator, it opens the gateway for traders to trade in the entry/exit zone of the Austrian market (CEGH). Also in cooperation with Powernext and Austria's Central European Gas Hub AG (CEGH), PXE operates the PEGAS CEGH Czech Market for gas trading in the form of derivative products delivered to the Virtual Trading Point on the Czech market (PXE). Another important gas hub in Europe is Point d'échange de gaz - Nord, commonly known as PEG Nord, is one of the 3 virtual trading venues for the sale, purchase and exchange of natural gas and LNG in France. It is one of the pricing and delivery points for Powernext natural gas futures contracts. It is the 6th most liquid gas trading point in Europe. Gas at PEG Nord is traded

on the Powernext exchange (Energy Delta Institue). Other important markets that should also be mentioned are the gas hubs: PVB, TTF, ZEE, ZTP, PSV (EEX).

## The role of the gas hub

Joskow (2013) highlights the important role that gas hubs play in allocating scarce network capacity and ensuring an effective balancing of supply and demand in electricity markets (Joskow, 2003). Despite the fact that EU legislation does not mandate the creation of gas hubs and the EU Directives do not explicitly specify the definition of a gas hub.

Another valuable observation is that instruments such as gas futures allow for the development of a spot market for natural gas, which ensures that the price of natural gas reflects supply and demand issues. This translates into the availability of natural gas in the market, the level of natural gas storage, the price of oil, the external temperature, the degree of infrastructure development (Fang-Yu)

It is important to know that fully developed mature trading facilities are characterised by a gas hub and/or a virtual trading point in combination with a functioning spot and forward market (OXFORD trading )

## Analysis of THE

The main objective of creating a single gas hub (Fig. 1) was to have a single German reference price in order to avoid regional price discrimination for consumers. Another important idea was to increase liquidity in the German natural gas market, security of supply of gaseous fuel and increase the competitiveness of the market. (EEX Customer information, 2021)

Importantly, the new hub includes 40,000 km of high-pressure pipes connecting more than 700 distribution networks in Germany, the largest consumer and importer of gas in Europe (Reuters, 2021). The expected increased tradable gas volumes and increased liquidity across the EU should benefit trading platforms. Hub development and market mergers through the implementation of this proposal. Therefore, this scenario represents an opportunity for trading platforms (European Commission, 2018). Spot contracts on THE hub are executed on the EEX spot market. In addition, local spot contracts are also available, developed in cooperation with the main European transmission system operators (TSOs) and market area managers to support physical balancing. We currently offer such products for TTF and PEG hubs but also for THE. Hub THE enters the futures market segment on the EEX exchange. Derivatives market products, Financial Gas Futures also enter THE.

Exchange trading and physical effect "Physical trading products" are products that are tradable on the European Energy Exchange (EEX), require physical delivery on the Trading Hub Europe (THE) market area and are subject to certain physical delivery restrictions. physical delivery in the market area of Trading Hub Europe (THE). Furthermore, THE uses these physical traded products for system balancing in its Market Area Manager (MAM) function in order to balance the physical imbalance in THE's market area and as Market Based Instruments (MBIs) to eliminate network capacity constraints in order to eliminate network capacity constraints (Impementation Guide).

For the purpose of this article, the physical transmission realised by two German natural gas transmission operators is summarised (Fig. 2): Open Grid Europe GmbH and GRTgaz

Deutchland GmbH, during the first week of operation of the new hub. The actual amounts of transmitted gas are practically constant, which may prove stability and continuity of the systems. Also (Fig. 3, 4) indicate that natural gas prices on the new Hub did not deviate from the natural gas prices on the other European gas hubs, which further proves that despite the start of THE operation, no surprising deviations were found.

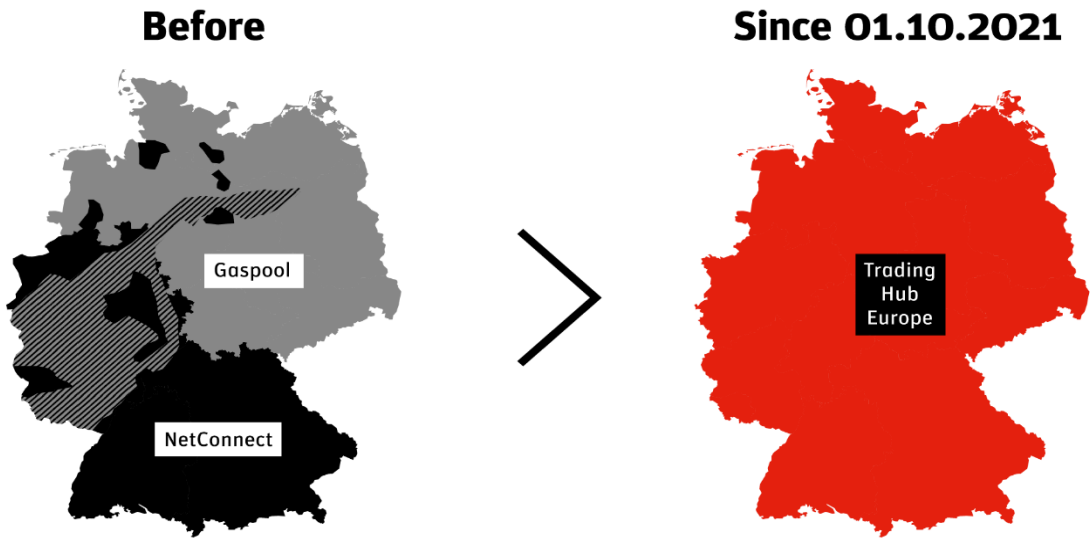


Fig. 1. Area of activity THE. Source: EEX

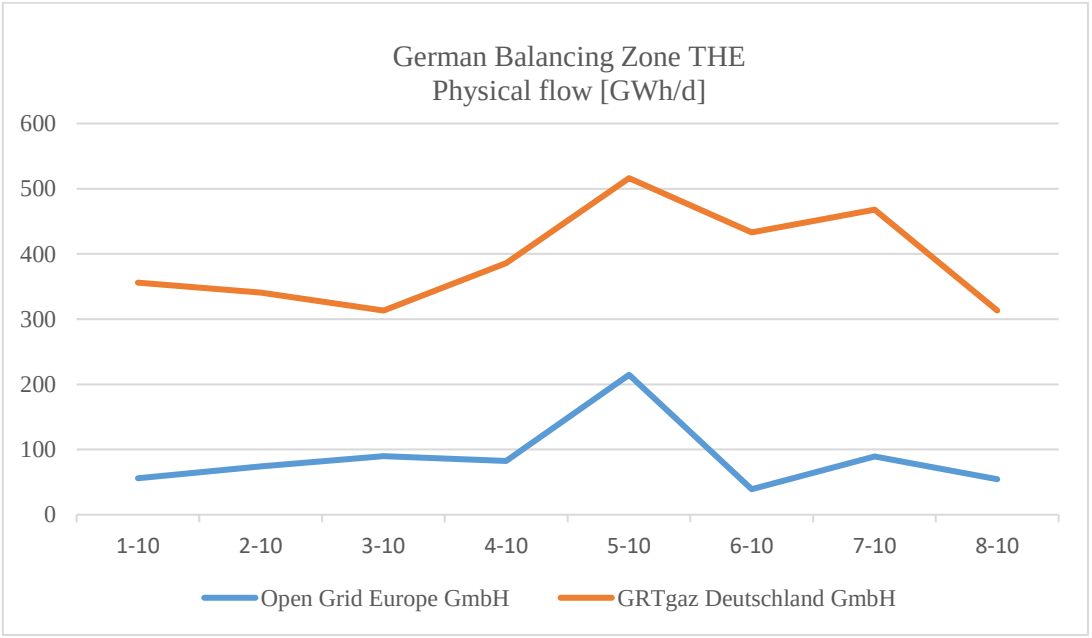


Fig. 2. German Balancing Zone THE Physical flow. Compiled by the author based on (EEX)

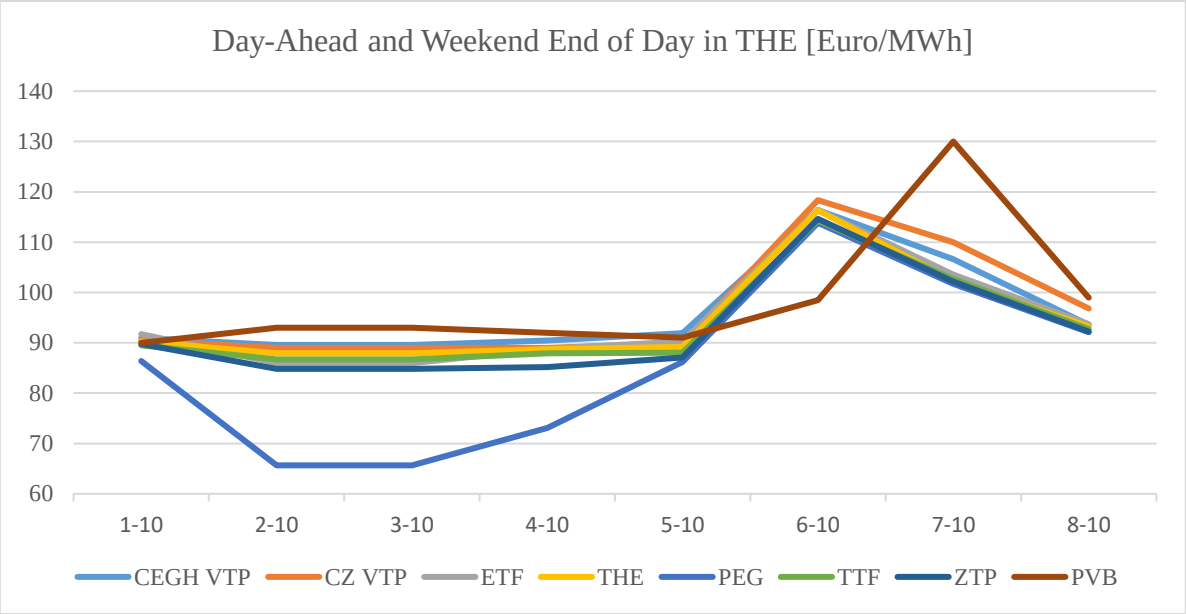


Fig. 3. Day-Ahead and Weekend End of Day in THE. Compiled by the author based on (EEX)

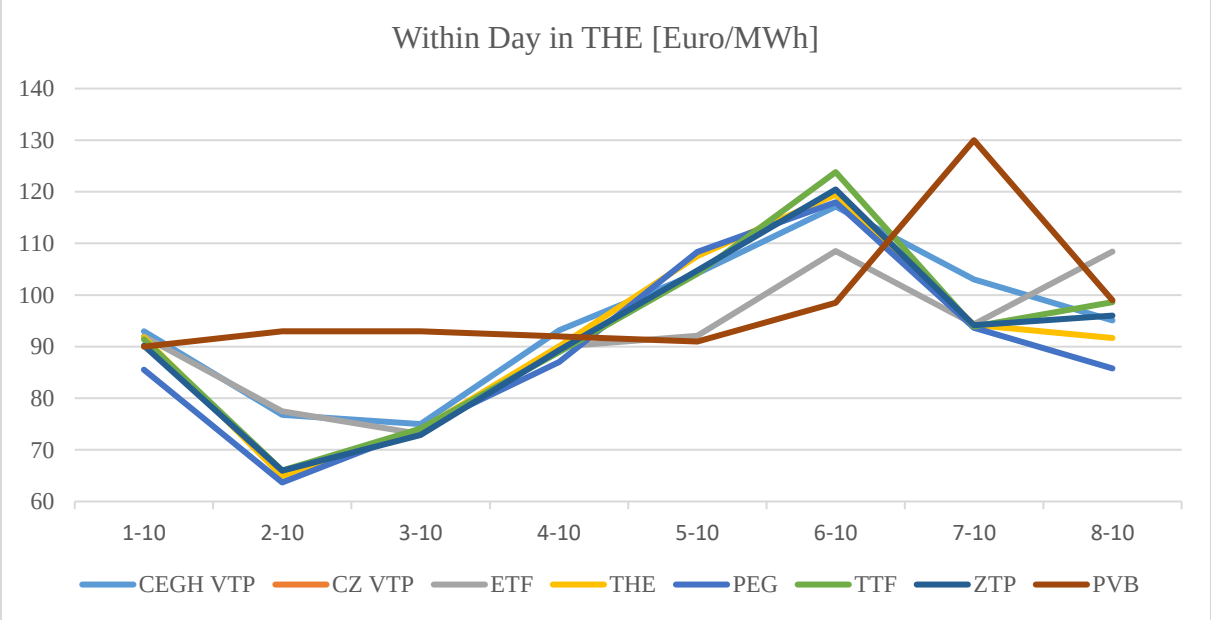


Fig. 4. Within Day in THE. Compiled by the author based on (EEX)

The German economy is among the leading European countries in natural gas consumption (Fig. 5). The supply of natural gas to industry and end consumers makes Germany an important player in the European natural gas market. Moreover, in the first half of 2021 Germany consumed the most natural gas in the European Union. The German system consists of 5 physical interconnectors, Brandov-OPAL (Germany-Czech Republic), Obergailbach (FR)/Medelsheim (DE) (Germany-France), Waidhaus (Germany-Czech Republic), Oberkappel (Germany-Austria), Gernsheim (German transmission-DE THE BZ). In addition, VIP Oberkappel, VIP France-Germany, THE VTP (DE) There are 5 transmission system operators in Germany that belong to the European association of natural gas transmission system operators:

GASCADE Gastransport GmbH, Thyssengas GmbH, ONTRAS Gastransport GmbH, GRTgaz Deutchland, Gasunie Deutchland Transport Services GmbH. All of these form the body that has given Germany the opportunity to create a gas hub.

| TIME | 2021-01 | 2021-02 | 2021-03 | 2021-04 | 2021-05 | 2021-06 | Total |
|---|---|---|---|---|---|---|---|
| Belgium | 2 459,400 | 2 035,100 | 1 959,800 | 1 733,300 | 1 285,000 | 953,500 | 10 426,100 |
| Bulgaria | 381,380 | 347,362 | 377,433 | 294,204 | 234,655 | 230,255 | 1 865,289 |
| Czechia | 1 279,051 | 1 172,943 | 1 092,541 | 881,416 | 590,599 | 415,464 | 5 432,014 |
| Germany | 13 130,666 | 11 238,430 | 10 149,760 | 8 456,133 | 6 311,638 | 4 273,432 | 53 560,059 |
| Estonia | 65,000 | 70,600 | 52,600 | 39,200 | 25,700 | 16,800 | 269,900 |
| Ireland | 553,688 | 439,708 | 500,179 | 462,687 | 391,530 | 371,718 | 2 719,510 |
| Greece | 628,402 | 448,668 | 540,101 | 551,048 | 403,431 | 549,260 | 3 120,910 |
| Spain | 3 419,000 | 2 523,000 | 2 848,000 | 2 693,000 | 2 406,000 | 2 436,000 | 16 325,000 |
| France | 6 068,591 | 4 649,302 | 4 547,173 | 3 544,711 | 2 561,115 | 1 655,117 | 23 026,009 |
| Croatia | 313,400 | 295,000 | 321,600 | 270,600 | 182,300 | 131,300 | 1 514,200 |
| Italy | 9 823,000 | 7 677,500 | 7 638,000 | 6 161,000 | 4 215,000 | 4 317,000 | 39 831,500 |
| Cyprus | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| Latvia | 183,509 | 178,833 | 136,977 | 79,661 | 45,803 | 42,409 | 667,192 |
| Lithuania | 321,100 | 273,000 | 226,900 | 216,300 | 204,000 | 152,300 | 1 393,600 |
| Luxembourg | 101,417 | 83,134 | 81,899 | 68,398 | 57,590 | 36,079 | 428,517 |
| Hungary | 1 543,542 | 1 330,476 | 1 231,594 | 953,549 | 634,348 | 426,477 | 6 119,986 |
| Malta | 26,759 | 27,039 | 29,024 | 32,750 | 32,040 | 36,842 | 184,454 |
| Netherlands | 5 846,166 | 4 874,130 | 4 652,755 | 3 856,979 | 3 142,287 | 2 434,313 | 24 806,630 |
| Austria | 1 249,298 | 1 024,985 | 1 005,607 | 828,029 | 568,365 | 397,566 | 5 073,850 |
| Poland | 2 731,659 | 2 513,831 | 2 395,204 | 2 020,853 | 1 593,402 | 1 332,069 | 12 587,018 |
| Portugal | 527,035 | 386,643 | 435,485 | 521,285 | 439,409 | 534,458 | 2 844,315 |
| Romania | 1 650,000 | 1 458,000 | 1 472,000 | 1 039,000 | 616,000 | 526,000 | 6 761,000 |
| Slovenia | 113,212 | 97,559 | 99,389 | 86,458 | 66,908 | 53,660 | 517,186 |
| Slovakia | 498,009 | 613,790 | 561,104 | 732,175 | 449,765 | 225,910 | 3 080,753 |
| Finland | 358,900 | 359,900 | 267,900 | 227,900 | 101,900 | 119,895 | 1 436,395 |
| Sweden | 184,000 | 155,000 | 116,000 | 100,000 | 63,600 | 103,700 | 722,300 |
| Norway | 408,562 | 376,001 | 410,412 | 382,296 | 347,406 | 354,238 | 2 278,915 |
| North Macedonia | 47,500 | 42,247 | 45,724 | 11,904 | 10,123 | 17,458 | 174,956 |
| Albania | 3,978 | 3,569 | 3,849 | 6,972 | 4,768 | 5,063 | 28,199 |
| Serbia | 408,000 | 347,000 | 346,000 | 280,000 | 157,000 | 148,000 | 1 686,000 |
| Turkey | 6 618,620 | 5 716,650 | 6 641,830 | 4 494,010 | 3 259,620 | 3 810,590 | 30 541,320 |
| Moldova | 191,700 | 186,600 | 165,200 | 98,300 | 42,300 | 29,500 | 713,600 |
| Ukraine | 4 278,000 | 4 048,000 | 3 544,000 | 2 239,000 | 1 340,000 | 1 340,000 | 16 789,000 |
| Georgia | 350,780 | 313,630 | 299,670 | 164,080 | 99,010 | 92,410 | 1 319,580 |

Fig.5. Inland consumption in Germany [mln $m^3$]. Compiled by the author based on (Eurostat)

## Conclusions

1 October 2021 will remain an important date in the calendar of the European natural gas market for a long time. The merger of two companies has given life to THE. Germany could become one of the major players in the European natural gas market. The new Gas Hub, together with the potential commissioning of the Nord Stream 2 pipeline, could additionally result in Germany playing an important role in the European transmission system. Germany's largest

natural gas consumption in the first half of 2021 positions the country as a leader in the European natural gas market. Furthermore, this merger may inspire other developing countries in the European gas market to create leaven for the eventual creation of a gas hub in their own country. The positive aspects of creating a gas hub should further encourage other countries. What is important is the maturity of the domestic gas market, which lays the foundations for the creation of natural gas. Another important aspect is that, at the time of the potential commissioning of Nord Stream 2, there is already a strong German natural gas market.

## Bibliography


1. International Energy Agency, Paris (2013)
2. https://www.ceer.eu/documents/104400/-/-/06c748a0-6867-e345-f25e-ab0fe7ee9d5b) [Accessed: 2021-10-20].
3. Mirello C., Polo M. *The Development of Gas Hubs in Europe.* DOI: 10.13140/2.1.4048.2243
4. Third Energy Package-security dilemmas. Vienna Forum on Euopean Energy Law. Paweł Pikus. 2019
5. Costescu A., Manitsas E., Szikszai A. *State of implementation of the Third Energy Package in the gas sector*. JRC SCIENCE FOR POLICY REPORT, 2018).
6. https://www.reuters.com/article/us-china-gas-exchange-q-a-idUSKBN1EN0I1
7. Fulwood M., *The Singaporean natural gas hub: reassembling global production networks and markets in Asia, Journal of Economic Geography,* Volume 20, Issue 5, September 2020, Pages 1241–1262, https://doi.org/10.1093/jeg/lbaa011
8. Heather P., *European Traded Gas Hubs: German hubs about to merge*. The Oxford Institute for Energy Studies. 2021, No. 286084
9. CEGH, https://www.cegh.at/, [Accessed: 2021-10-20].
10. PXE, [Online] https://www.pxe.org/ [Accessed: 2021-10-20].
11. Energy Delta Institute, [Online] https://web.archive.org/web/20140407200551/http://www.energydelta.org/mainmenu/energy-knowledge/country-gas-profiles/country-gas-profile-france
12. EEX, [Online] https://www.eex.com/en/ [Accessed: 2021-10-20
13. Joskow P., Natural Gas: *From Shortages to Abundance in the United States*. American Economic Review, vol. 103, no. 3, 2013
14. Joskow P., *The Difficult Transition to Competitive Electricity Markets in the U.S*. Center for Energy and Environmental Policy Research, 2003.
15. Fang-Yu L., Ryvak M., Sayeed S., Zhao N., *The role of natural gas as a primary fuel in the near future, including comparisons of acquisition, transmission and waste handling costs of as with competive alternatives*. Chemistry Central Journal 6, S4, 2012.
16. [Online] https://www.europeangashub.com/tag/oxford/ [Accessed: 2021-10-20]
17. EEX Customer information 24/03/2021 [Online] https://www.eex.com/fileadmin/EEX/Markets/Natural_Gas/Trading_Hub_Europe_THE/20210324_EEX_Customer_Information_Further_Information_related_to_the_German_Gas_Market_Merger_on_1_Oct._2021.pdf/ [Accessed: 2021-10-20]

18. Reuters 2021, [Online] https://www.reuters.com/business/energy/germany-launches-nationwide-gas-trading-hub-2021-10-01/)/ [Accessed: 2020-01-12].
19. European Commision, [Online] https://ec.europa.eu/energy/sites/ener/files/documents/quo_vadis_report_16feb18.pdf/ [Accessed: 2021-10-20]
20. Implementation Guide, Trading Hub Europe – implementation Guide: Case Studies ad Explanatory Information on the Physical Trading Products Pursuant to Section 25 of the Balancing Group Contact.

**Tomasz Chrulski** – PhD student at the Doctoral School of AGH , Faculty of Drilling, Oil and Gas, AGH University of Science and Technology, Kraków, Poland.
ORCID: 0000-0002-8842-518X

# Book Review: The Nordic Dimension of Energy Security[1]

*Özgenur Aktan*

**Abstract:** *The Nordic Dimension of Energy Security* aims to problematize the narrow conceptualization, contextualization and fossil fuel-based practices of energy security in the context of climate security. Energy has a key role in political, economic, social, cultural, environmental, ontological and climate security issues. The connection between energy and security contains various concepts, contexts and affects the civilizational development of human societies. The author demonstrates that the Nordic states pursue sustainable energy security policies and energy cooperation strategies with the Baltic states and European Union member states, while actively engaged in peace building activities. In this regard, the Nordic states have been evaluated as reference role models to remedy the narrow and traditional energy security approaches and to internalize renewable energy sources.
**Key words:** energy security, Scandinavia, Multi-dimensional threats

## Introduction

Energy security and the energy sector of the Nordic states, formed by Denmark, Norway, Sweden, Finland and Iceland, deserve careful elaboration and attention in the context of the climate crisis. In this spirit, the author provides detailed, historical and comparative analysis of the energy vision of the Nordic states to provide critical criteria for policy decision-making processes. The Nordic states have an important role in the energy integration, cooperation and active participation processes with environmentally friendly tendencies and methods. Pursuing a balance between energy security and climate security, while focusing on the social awareness and social acceptability aspects of the energy security and stimulating the industries to develop ecologically appropriate technologies has been evaluated as critical Nordic strategies to contribute to sustainable energy security in the long term.

There are political, economic, industrial and social challenges to actualize the total independence from fossil fuels. But still, engaging with the energy and environmental security-related experiences of the Nordic states may demonstrate ways and means to construct laudable conditions in the context of the climate crisis. The author focuses on the energy security and energy vulnerability of the European Union (EU) and Baltic states, while evaluating the Nordic states as reference cases to harmonize the relationship between energy security and climate crisis. Descriptive and comparative analysis of the energy security of the EU, Baltic and Nordic region may be evaluated as valid and sound to demonstrate transnational and solidarity-oriented approach in International Relations (IR).

Multi-dimensional risks and threats, which are associated with the impacts of the climate crisis may be evaluated as the starting point to problematize traditional approaches, to develop an appropriate definition of energy security and to contribute to energy cooperation. Attention

[1] Ryszard M. Czarny, The Nordic Dimension of Energy Security, Switzerland, Springer Nature, 2020.

should be drawn to the relationship between energy security and climate security to dissolve the problem of various explanations in IR and to challenge traditional approaches. The climate crisis, in this respect, may be evaluated as the starting point to redefine and reconceptualize energy security, as exemplified by the Nordic states. Environmental well-being as the reference subject of the energy security may be effective to provide joint undertakings, comprehensive responses and timely resolutions against the impacts of climate crisis. The author argues that linking energy security and climate policy requires transforming the global energy system and changing taken-for-granted assumptions about the concept of security. In this regard, he examines the characteristics and challenges, resulting from the Nordic energy model and culture.

**Summary and Evaluation of the Chapters**

In the first chapter, the author argues that concerns about national security, economic interests and adequate supply of energy resources have dominated energy security policies. Explanations about energy security have thus been subject to different approaches and prioritizations. The differentiated or specialized conditions and interests may obstruct efforts to develop a working definition that satisfies the needs, demands and policy choices of all of the agents in IR. But still, it is necessary and rational to develop a more comprehensive perspective in which environmental impacts of energy resources, integration and cooperation mechanisms in the energy market and infrastructure security are also analyzed.

In the second chapter, the author formulates the justificatory reasons to internalize Renewable Energy Sources (RES) from political economic and sustainable development perspectives. The brief history of energy alterations, changes in the energy availability and capacity conditions of the states, impacts of energy poverty, energy inaccessibility and electricity insecurity, water security, technological and economic inequalities, which may jeopardize to compensate fossil fuels and to obtain energy from solar, wind and water are also explained and analyzed. The author examines the dimensions of energy security, including affordability, reliability and sustainability, with an emphasis on the sectoral interactions and dynamics. Engaging with the dimension of energy security also allows us to appreciate the role of geopolitical, geoeconomics and environmental perspectives.

The author addresses the risks and threats in demonstrating the problematic aspects of traditional energy security. Environmental insecurities, pollution, increasing energy demand, especially from Asia, increasing energy prices, political instabilities and energy injustices have been evaluated as important challenges in the context of the global energy system. Apart from the emphasis on state, market and environmental-centric perspectives, a marxist critique of traditional energy security may also allow us to appreciate the competing paradoxes and dilemmas in the context of energy security. Engaging with the IR theories might have enriched discussions about dilemmas in energy markets. But the author does not focus on the concept of energy security through the premises of IR theories and does not elaborate on a marxist critique, when mentioning energy poverty, inaccessibility and injustice issues.

Energy security is also intertwined with the gap between the rich and poor in the international system. The author explains how climate policies may produce economic pressures

and developmental restrictions for developing states and poor societies. Technological and capital-intensive policies and costly investments, which are based upon the internalization of renewables, may not be compatible with economic realities and may produce obstacles in achieving a balance between energy security and climate security. Inequalities and injustices may produce challenges for the formation of a solution, which satisfies and unites all of the agents in IR. But still, the author suggests that the policies of governments should focus on energy efficiency solutions and transitions towards RES to mitigate and to shape the future of the global energy system in line with the requirements of climate security. The author also provides case studies and reports to demonstrate the contradiction between energy policies and climate security and shares some estimations and scenarios, which indicate the primary role of coal, oil and natural gas in energy mix policies.

In the third chapter, the interactions between energy supply and energy demand are analyzed with an emphasis on exporting and importing activities. The impacts of the concentration of the proven reserves, discoveries and explorations of coal, oil and natural gas on energy markets and policies are also shared and discussed. The author provides comparative estimations, which indicate the increasing role of natural gas in energy mix policies. Information and analysis about the energy production, consumption and trade by regions, international organizations, states, sectors and fuels are also given to provide a comprehensive approach.

In the fourth chapter, the energy security and climate policies of the EU are examined through a close look into its relationship with Russia. This chapter elaborates that natural gas is a key issue for the energy security of the EU. The security of natural gas supply, energy relations between the EU and Russia, energy dependency and environmentally problematic energy-intensive industries of Eastern and Central Europe, fragmentation and integration trends in the EU energy markets, investments and projects to contribute to cooperation, efficiency and energy stability in the EU have also been analyzed. Ensuring the security of natural gas supply from Russia and conflict in Ukraine have been evaluated as critical components that may reveal the vulnerability and divergence of the EU's policy framework and institutional design at large.

The author emphasizes the viability of a game theory approach to demonstrate the strategies of Gazprom through the pressures of Russia to provoke natural gas competition and to undermine energy solidarity within the EU. These strategies have been exemplified as price maximization policies, differentiated pricing choices, check and control mechanisms aimed at jeopardizing the introduction of alternative energy resources and infrastructural investments in securing natural gas supply. In response to these strategies, diversifying natural gas suppliers and energy resources, developing energy interconnectivity and infrastructure security have been emphasized as important strategies of the EU against the adverse impacts of natural gas dependency.

Supplying natural gas from Caspian Basin and the Middle East, diversifying the transmission routes and trading partners, liquefied petroleum gas and natural gas, while adopting regulatory policies to undermine the divergence and unilateral decisions of the EU member states have been important to contribute to energy security of the EU and to mitigate the threats, exemplified by the relationship between the EU and Russia. The author also explains how the relationship between the EU and Russia is defined by various problems, including

dependencies, different values and unilateral policies of Russia, aimed at pursuing international influence through the instrumentalization of energy resources, especially natural gas.

The author argues that deteriorating the cohesion of the EU may produce disagreements among the member states, concerning the viability of cooperation with Russia. In this context, it is important to strengthen EU's internal energy market, which is aimed at facilitating energy trade and energy access, converging pricing and taxation, protecting the energy security and rights of European citizens, supporting the interconnectivity, harmonizing the internalization of RES process and introducing binding rules to contribute to environmental security, resilience, development of RES and energy solidarity.

EU regulations, resolutions and rules have also been briefly given and interpreted as the representation of the energy autarchies among the member states in practice. Different conditions and policy choices, technical, economic and regulatory barriers within the EU have been analyzed in the context of energy policies. The author explains how Germany, for instance, has pursued wind and solar energy-oriented strategies and green technologies, while France has focused on the development of nuclear energy and technological strategies. Poland, on the other hand, has focused on coal. In this regard, it is observable that energy and environment-related concerns have a critical role for European integration and cohesion processes. The main idea is that pursuing a common policy and complete integration in the energy market, while ensuring environmental protection may be evaluated as critical challenges for EU integration in the context of energy security.

In the fifth chapter, Nordic states have been analyzed from political, geographical, socio-economic, technological, cultural and ecological perspectives. The author identified the similarities and distinctions between the Nordic states and Baltic states in terms of the energy, electricity and climate security-related conditions, availability of the energy resources, RES potentialities, practices and policies of the EU. In this regard, both opportunities and challenges have been emphasized to expand cooperation between the Nordic states and Baltic states in the context of the energy security and climate crisis. The Nordic energy market has been explained in terms of the liberalization and integration of energy markets, research and development processes, innovation and ecological resolutions. Energy security policies, potentialities and challenges of the Nordic states have been analyzed compared to the EU and Baltic states.

The author explains mutually supportive components to achieve Baltic Sea cooperation (Czarny, 2020: 111) as follow:

*"– liberal model of the internal market;*
*– sustainable development;*
*– security of supply".*

Given such components, energy cooperation in the Baltic Sea region has been evaluated as critical to contribute to energy security and interconnectivity of the EU and Nordic states and to challenge the military presence of Russia in the Baltic Sea (Czarny, 2020: 112-113, 115). Energy cooperation between the Nordic states and Baltic states has been evaluated as important to undermine the energy isolation and dependency of the Baltic states and to contribute to EU targets as well. Thus, the energy security of the Nordic states is also intertwined with the energy security of the EU and Baltic states. The author also shares the energy conditions and RES potentiality of the Baltic states, while looking at the possible energy and environment-related implications of the infrastructural investments and projects. The author suggests to assess

energy security of the Baltic states with the inclusion of both EU membership and distinctive political and civil cooperation programs and initiatives with the Nordic states. This suggestion implies to develop further cooperation and integration.

In the sixth chapter, the author examines the transformation of the energy security, energy balance and energy market structure of Denmark. The author shares compiled data about the energy production, consumption, importing and exporting activities of Denmark, while evaluating Denmark as a critical case study to observe various energy security strategies. Coal, oil and natural gas still have an important share in the energy mix policies of Denmark. But still, integration of RES has also been supported to achieve sustainable energy security and electricity security. The fuel crisis of the 1980s has produced anxieties in decreasing dependency on fossil fuels and in mitigating environmental impacts. In this regard, Denmark has pursued policies to diversify energy resources through the integration of RES, especially wind energy, modernization and liberalization of energy market, promotion of investments regarding infrastructural connectivity, smart grids and energy technologies in the context of the climate crisis.

In the seventh chapter, structural changes in the energy security of Finland have been analyzed. The impacts of the oil crisis of the 1970s, energy balance and climate policies have been explained from historical and comparative perspectives. The author also shares how EU membership has allowed Finland to accelerate market competition and to integrate with the European energy and electricity market. Cooperation with the Nordic and Baltic states also contributed to integration and interconnectivity in the context of energy security.

Pursuit of reliable energy trade, diversification strategies, compensation of fossil fuels by RES, bioenergy, nuclear energy, innovation in the transportation and aviation sectors have been critical to achieve energy security and to provide a balance between economic growth and environmental security. The author notes the role of public awareness for the internationalization of sustainable development at large as well. Apart from the emphasis on the societal level of energy security, the Arctic identity also compels Finland to develop policies, which integrate energy and climate-related insecurities. The author also suggests that the Nordic cooperation may expand to the Arctic region as well.

In the eighth chapter, the energy transition process in Iceland is analyzed. The author notes that the increasing oil prices of 1973-1974 were effective in compelling Iceland to focus on geothermal energy-related policies (Czarny, 2020: 168). Economic and sustainable utilization of geothermal energy has been effective in reducing energy dependency and the share of fossil fuels and in contributing to electricity security. In this regard, concerns about competitive prices and affordability may also be evaluated as critical to focus on RES. Explorations in the volcanic islands also confirm the high level of geothermal energy potentiality in Iceland. The author also explains the economic and environmental-related reasons to develop RES and to expand energy cooperation with Europe.

In the ninth chapter, changes in the energy security, energy balance, energy opportunities and challenges of Sweden have been analyzed. In the 1970s, there has been a heavy emphasis on the fossil fuel-based production policies. But the oil crisis of 1973, pursuit of reliable energy supply, energy dependency and environmental impacts compelled Sweden to adopt ecological and efficient resolutions and appropriate waste management mechanisms. In this context, electricity, water energy and bioenergy play a critical role in the achievement of

environmental protection. The author also explained the similarities between the security of natural gas-oriented resilience mechanisms of Sweden and EU.

There have been efforts to increase public awareness during the internalization of the RES transition process. In this context, Sweden also takes the social acceptability of RES into account to facilitate the energy transition process, while limiting the use of fossil fuels. Although fossil fuels are still used and traded, Sweden pursuits policies in line with the development of sustainable energy security and supports projects to develop solar energy. The author also explains the resilience mechanisms and emergency responses of Sweden against the impacts of energy disruptions and crises, with an emphasis on the security of natural gas and oil. In this regard, the pursuit of cooperation with the EU may also be evaluated as a resilience mechanism in terms of secured, uninterrupted and cost-effective energy supply, sustainability and RES.

In the tenth chapter, Norway's energy and climate policies are analyzed. The author explains that oil and natural gas production and exportation activities play a critical role in state revenue and trade balance in Norway. Norway also conducts oil and natural exploration operations in the North Sea, Norwegian Sea and Barents Sea to support the sales of fossil fuels and the flow of income. Natural gas cooperation between Norway and the EU also requires strengthening infrastructure security, interconnectivity and market integration, which are critical components of energy security.

Norway pursuits RES-based policies and hydropower projects to sustain domestic consumption, while exporting fossil fuels. The author explains how electrification of energy security in Norway is also extended compared to other Nordic states. The integration of the electricity market by Norway, Sweden, Finland, and Denmark also contributed to achievement of energy security in the Norway and Nordic region. The author recommends that modernization of RES, cross-border interconnectivity and effective distribution and transmission of electricity are required to contribute to energy security, flexibility and resilience.

In the final chapter, the author discusses the energy security accomplishments and challenges in the Nordic region, with an emphasis on environmental protection, climate security and development of deeper cooperation. A comparative perspective is employed in analyzing energy security in the Nordic states. The energy sector is inevitably intertwined with policies to mitigate climate change. Even in Nordic states, with high levels of socio-economic development and prosperity, actualization of the RES transition process is a challenge. In this regard, the author evaluates liberalization and integration of energy markets, innovative resolutions, technological developments and public awareness as important to undermine the challenges of the RES transition process.

The author asserts that Nordic states have a leading role for environmental security and well-being at national, European and international levels (Czarny, 2020: 238). In this context, a Norden approach has been emphasized as a reference model to conceptualize the relationship between energy security and climate crisis. The author explains that the Nordic interpretation of sustainable development needs to be read as a role model to be followed by others in pursuing to provide a balance between energy, ecology and climate protection, economic and social welfare.

## Concluding Remarks

Overall, the book examines the energy security activities and policies of the Nordic states, both nationally and in the European context to demonstrate a holistic approach in the context of the climate crisis. Energy has a critical role in redefining the relationship with the environment at political, industrial and societal levels. In this regard, the idea is to transcend beyond mere material and profit-seeking perspectives in favor of environmental well-being and RES. The author contends to favor liberalization of the energy markets. But he does not elaborate on problems that cannot be resolved through liberalization processes. The problems about energy poverty, inaccessibility and injustice are not explained in detail and in comparison to the Nordic model, which has been evaluated as an inspiration for social cohesion and economic welfare (Andersen et al., 2007: 11-12).

The author calls for the recognition and dissemination of *"Nordic ecological culture"* and *"Nordic energy culture"* (Czarny, 2020: 241), which may contribute to environmental compatibility of energy security. The author also emphasizes that the Nordic interpretation of energy security and energy cooperation are highly involved in the energy policies of the EU and also capable of affecting *"the ongoing Europeanisation and globalization of energy policy processes"* (Ibid, 2020: 256). This kind of a holistic and comparative perspective may be evaluated as a critical strength of this book.

Despite the inner contradictions and pressures, which have been associated with the globalization process and emerging economies in Asia and Latin America, Nordic model has been accentuated as an inspiration and ideal paradigm in searching for a better system in terms of economics, social welfare, egalitarian distribution and peace. The Nordic model has been described as an ideal combination in between the characteristics of the welfare state and globalization (Andersen et al., 2007: 11-12). Therefore, it would have been important to provide a detailed analysis of liberal understandings of energy security in engaging with the Nordic states as case studies and in favoring the liberalization of energy markets.

A balance between economic prosperity and environmental well-being requires to adopt both industrial and societal policies. A marxist critique of energy security and energy justice perspectives should have been elaborated by taking into account the experiences of developing states and poor societies as well. In this spirit, both mainstream and critical analysis might have been employed for the achievement of energy security. Apart from the emphasis on a marxist critique, the author does not provide the critique of Anthropocene or Capitalocene, which briefly emphasize *"Nature/Society dualism"* (Moore, 2016: 3), when addressing the need for a change in the relationship between humanity and the physical environment. But still, the author acknowledges the role of shared identity in harmonizing energy security policies.

It is important to note that the historical, cultural and linguistic ties among the Nordic states, which underpin the development of joint Nordic identity (Hagemann and Bramsen, 2019: 10; The Nordic Council and the Nordic Council of Ministers, 2019) may also be connected with the development of holistic approaches in the context of energy security. In 2019, the Nordic states shared their vision and commitment, concerning a deeper integration and cooperation in terms of sustainability, climate crisis and environmental well-being by 2030. In this spirit, it has been acknowledged that the Nordic Council of Ministers may play an essential role in actualizing the shared vision. Nordic identity and Nordic solutions, which have been

intertwined with the peace, democracy, mobility, cooperation, close relationship with the sea etc. have been emphasized as critical to contribute to climate action and harmony with the nature (The Nordic Council and the Nordic Council of Ministers, 2019).

Consequently, the book offers critical insights and reference cases to problematize the narrow conceptualization of the relationship between energy and security. Focusing on the connection between energy security and climate security, with an emphasis on the Nordic states in comparison to the EU and Baltic States may be evaluated as one of the key benefits of this publication. The normative, cooperative, integrative, mediative and efficient aspects of the Nordic identity may be employed and further analyzed to provide a constructivist approach to energy security in line with the requirements of climate security. Therefore, the characteristics of the Nordic states may be important in demonstrating an ideal model and a normative force that need to be preserved and disseminated in the international society.

## Bibliography

**Reports and Official Papers from Institutions:**

1. Andersen, T. M., Holmström, B., Honkapohja, S., Korkman, S., Söderström, H. T., & Vartiainen, J. (2007). "The Nordic Model: Embracing Globalization and Sharing Risks". *The Research Institute of the Finnish Economy (ETLA).* Yliopistopaino, Helsinki, Taloustieto Oy Publishing. Retrieved from https://www.etla.fi/wp-content/uploads/2012/09/B232.pdf (Access Date: 11.11.2021).
2. Hagemann, A., & Bramsen, I. (2019). "New Nordic Peace: Nordic Peace and Conflict Resolution Efforts". Nordic Council of Ministers. Retrieved from https://norden.diva-portal.org/smash/get/diva2:1302296/FULLTEXT01.pdf (Access Date: 10.11.2021).
3. The Nordic Council and the Nordic Council of Ministers (2019). "Our Vision 2030". Retrieved from https://www.norden.org/en/declaration/our-vision-2030 (Access Date: 08.11.2021).

**Books:**

1. Czarny, R. M. (2020). *The Nordic Dimension of Energy Security,* Switzerland, Springer Nature.
2. Moore, J. W. (2016). "Introduction: Anthropocene or Capitalocene?: Nature, History, and the Crisis of Capitalism". In Jason W. Moore (Ed.), *Anthropocene or Capitalocene?: Nature, History, and the Crisis of Capitalism* (pp. 1-11). Kairos PM Press.

**Özgenur Aktan** – B.A. in Political Science and International Relations (2017) from Istanbul University and M.A. in Political Studies (2020) from Istanbul Technical University in Turkey. Completed her master thesis, entitled as "Understanding Planetary Security: A Post-humanist Paradigm in Approaching Energy Security and Climate Crisis", under the supervision of Assoc.Prof. Asli Calkivik. Currently a PhD Student in the Department of International Relations at the Galatasaray University in Istanbul, Turkey. Her scientific interests focus on international relations theories, energy policy, critical security studies, conflict resolution and negotiation strategies and effects of climate change on island states.
ORCID: 0000-0003-1026-2445

ISSN: **2545-0859**