Interdisciplinary Description of Complex Systems 22(3), 284-290, 2025

THE EFFECT OF WEATHER-DEPENDENT RENEWABLE ENERGY SOURCES ON THE OPERATIONAL SAFETY OF CRITICAL INFRASTRUCTURE SYSTEMS – CREATION OF AN ANTIFRAGILE ENERGY SYSTEM

Richard Haddad*, Laszlo Ady and Peng Zhang

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.23.3.9
Regular article

Received: 20 February 2024.
Accepted: 28 October 2024.

ABSTRACT

While the ecological footprint of humanity is constantly growing, urbanization has had an exponential growth in recent years. The fundamental concept of green energy is to create liveable and sustainable urban environment. There are several ways to produce completely green energy, whilst focusing on developmental opportunities in certain areas. Fundamentally, there are two main disciplines to develop green energy: one is info-communication and other is the energy systems in parallel. Their focus is on achieving an antifragile system that is less prone to the hectic change of weather-dependent, distributed energy producers. Our research highlights the problem of integrating weather-dependent distributed renewable energy producers into the electrical network in Hungary. This article will cover the opportunities and challenges of the Hungarian electricity system concerning small, household size power plants and unfold how a modern "super-computer" can help or hinder modelling the electrical systems, and what other organizational opportunities can aid integration.

KEY WORDS

renewable energy, safety, antifragile energy system, infrastructure systems

CLASSIFICATION

JEL: Q40

*Corresponding author, η: haddad.richard@kvk.uni-obuda.hu; -
József körút 6., Budapest, 1088, Hungary

INTRODUCTION

When looking for the answer to the question of how to make our electrical systems less fragile, an endless list could be compiled, since this critical infrastructure is integral to the everyday life of every person. A recent slogan by the Budapest Electrical Works stands true: "If there is electricity, there is everything". Unfortunately, the opposite of this sentence, as shocking as it may be, is also true: without electricity very little can be done.

The electrical infrastructure has undergone a major transformation in the past decades, in which the focus has been on the reduction of energy dependence, saturation of green energy, and the preference of distributed energy production. The Hungarian domestic solar production had already reached 2 200 MW of installed capacity by the end of 2023 – according to the Hungarian Energy and Public Utility Regulatory Authority. At the same time, the peak demand in Hungary has been mostly around 7 300 MW. In 2012, the installed solar capacity barely reached 13 MW, but then it grew exponentially and explosively in the following decade. Although this growth slowed down in 2023, the Hungarian electrical system operator predicts up to 10 000 MW of solar-based generation capacity by 2030 [1].

Figure 1 shows that more than 250 000 solar inverters with Internet access are already in operation and connected to the electrical grid in Hungary. In addition, around 500 000 smart meters with two-way data connections and internal disconnector capabilities were installed within the energy network. If predictions are right, the number of these devices will have doubled by 2030, which will impose a further impact on the security of these networks. While the benefits and advantages of digitizing the energy systems are evident, the risk of vulnerabilities and malicious intent to disrupt operation should also be considered. Ripple control systems – ripple control is a common platform of load control, grid management which involves superimposing a higher-frequency signal onto the standard network frequency of the main power signal. When receiver devices attached to time shiftable residential or industrial loads receive this signal, they switch off the load until the signal is switch on again – are prime examples of such sub-systems to be potential victims of attacks and these systems are well established for many simultaneous controls for demand-side management (DSM). Even if the cybersecurity measures of ripple control systems are improved, they will still be the main cause of blackouts.

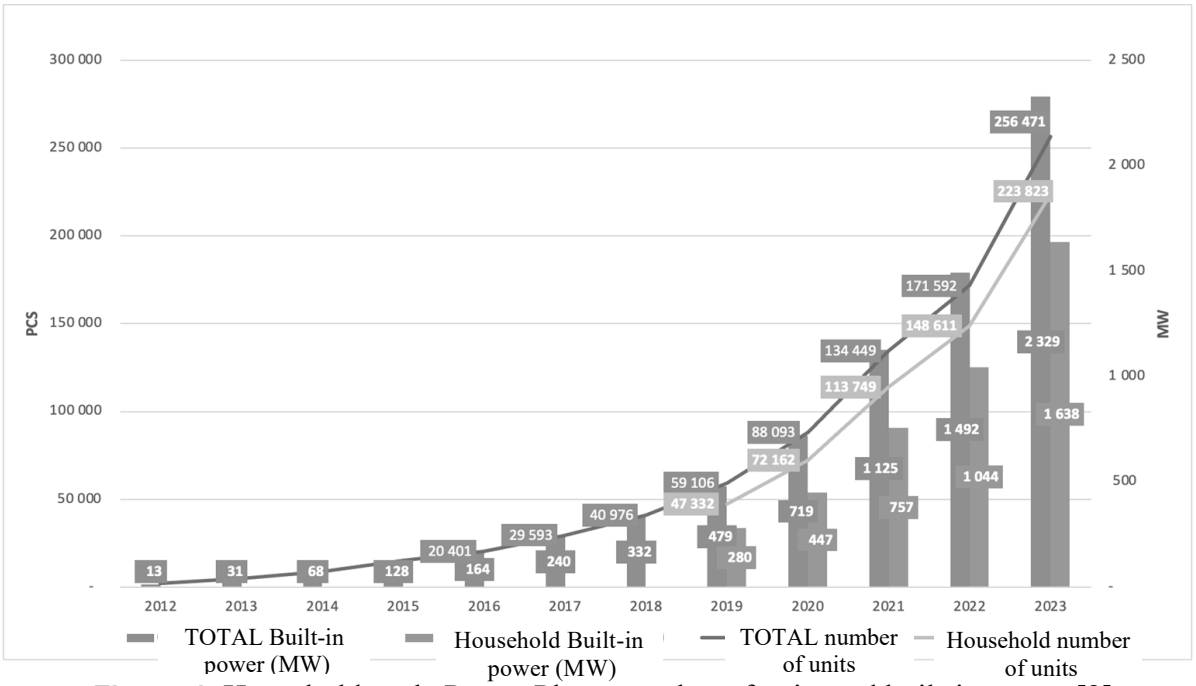

Figure 1. Household-scale Power Plants number of units and built-in power [2].

When analysing the energy system of Hungary today, it can be looked at from two angles: technology capabilities and security – including cyber security. In our case, both angles focus on household-scale, weather-dependent, energy-producing inverters and energy storages together with the related smart metering infrastructure.

SAFETY AND SECURITY ISSUES

Our opinion is that February 24th 2022, is a turning point in critical infrastructure protection. After numerous cyber-attacks, there was an invasion in Ukraine. The primary targets of all attacks were carefully selected to significantly disrupt the country's critical infrastructure. In 2018, Ukraine was ranked 88th in the Human Development Index [3]. With this ranking, the country was in the High Human Development category. Considering Ukraine's energy and information communication technology, technical development, and existing infrastructure, it was on par with what one would find in developed countries.

Cyber-attacks on energy infrastructure are not unheard of. One example from 2010 is the deployment of the first known cyberweapon [4], or in 2012 against oil company Saudi Aramco. Ukraine was also exposed to it in 2015 and 2016.

Concurrently to the military operations in the physical space, attack was launched in the cyber space against the satellite telecommunications company ViaSat to block military positioning and communication capabilities [5]. This attack not only disrupted military capabilities, but also caused a disturbance in the German energy system. The synchronization of offshore wind farms in the German North Sea is done via the same satellite system operated by ViaSat. According to sources the attack paralyzed the platform for almost a month, and the service was fully restored only after March 31, 2022 [6].

In 2023, similar attacks were carried out against Acer and the energy provider HSE, but details of those attacks are yet to be revealed. There are many theories, but no attacker and no motivation has been identified officially. Specialists are working on mitigating the damage, and hopefully the background of these attacks will be revealed.

These recent events have shifted our research to examine a less studied and protected area of the Hungarian energy infrastructure. Previous studies, such as "Digitális Mohács" [7] and its version 2.0, outlined what the potential scenario of a coordinated cyber-attack launched against Hungary could look like. Reviewing parts of these studies. One can examine what risks arise from the vulnerabilities of Household-scale Power Plants, the energy storage connected to them, and the smart meters installed for their energy accounting.

In the United States of America and Canada, the NERC – North American Electric Reliability Corporation standard system is used. This includes NERC-CIP, i.e. the NERC Critical Infrastructure Protection section, which contains 112 standards. Our research identified 5 relatable NERC-CIP reliability standards for small household-sized power plants, energy storage and smart consumption meters.

When examining European standards, it can be concluded that the IEC-62443 standards are the most widely accepted ones. In October 2024, NIS 2.0 [8] will bring further changes to the sector including cross-border capacity of energy systems between international borders.

Critical infrastructure protection is an important element right from the planning, design and implementation of infrastructure investments. In the US, the framework set by the FCC (Federal Communications Commission) regulation excluded the use of hardware and software by vendors such as Huawei, ZTE, Hytera, Hikvision, Dahua Tech within the security perimeters of critical infrastructure, and solutions provided by these vendors will not be granted a Supplier's Declaration of Conformity.

Well established policies, procedures, and supply chain risk mitigation are equally important. Industry peers have reported an incident when some industrial network equipment failed at a plant. Plant operators did not pay attention to the safety stock of this equipment and reached out to the OEM to procure a new unit. They were quoted an approximate of 2-4 weeks delivery. Technicians took it on themselves to procure the item outside the corporate procurement channels by ordering a device from eBay. The device was installed with the default configuration and production was restarted. Years after installation, the manufacturer released upgrades for that particular model. When the technicians attempted to apply the said upgrades, the device would fail mid-process. Upon further inspection it was revealed that while externally the housing of the device was identical to the OEM model, the inners were vastly different built to mimic the function of the original equipment. The device was a counterfeit and had lived in an operational environment for years before it was identified

The presented example highlights the importance of understanding risks related to third parties. Third-party or N+1 party risk assessment and management have become essential for the safety of energy systems.

ARTIFICIAL INTELLIGENCE AND THE EMERGENCE OF QUANTUM TECHNOLOGY IN THE CYBERSPACE

Targeted attacks and individual actions are plausible, but a coordinated attack against many endpoints is less expected at the current level of development. The geographical penetration of system elements and the capacity of current computing devices do not yet allow for an effective attack on distributed systems [9].

The simultaneous development of two technologies may override the status. One is artificial intelligence (AI), and the other is the emergence of quantum computers in cyber-attacks [10].

AI can independently help determine the target and the attack vector to maximize the efficiency of the breach. However, if an adequate computing capacity is not available, AI is more the subject of science fiction than a real social danger.

Quantum technology can achieve multiple times the computing capacity and communication of our current computing devices. Using Quantum technology, the breaking time of the current encryption technology is reduced to a fraction. When supplemented with AI, it can pose a serious threat and human abilities will no longer set the limitations.

LEGAL BACKGROUND OF CRITICAL INFRASTRUCTURE

The identification, designation and protection of critical infrastructure are regulated by multiple laws in Hungary:

- Act CLXVI of 2012,
- Government Decree 65/2013. (III. 8.) on the implementation of Act CLXVI of 2012,
- Its decree CLXVI of 2012 on the identification, designation and protection of vital systems and facilities. 65/2013 on the implementation of the Act (III. 8.) on the amendment of the Government Decree.

The law collects basic public services in several systems. The first critical system is the energy system, which includes not only the electrical system, but also crude oil, natural gas and district heating infrastructures.

The next infrastructure involves the info-communication technologies, and it is often identified with cellular technology, although it is much more than that. It includes the Internet as a service and the Internet infrastructure itself and other electronic communication services, electronic communication networks, such as broadcasting or even postal services.

Strategically, logistics follow this, as do transportation systems (road, rail, air or water). Even logistics centres that are distribution hubs for consumers are part of critical infrastructures.

The COVID-19 pandemic also showed in 2020-2021 how vulnerable the food and pharmaceutical industries are, and they shall be considered as critical infrastructures.

In addition to the above listed infrastructures, it can be seen how the number and distribution of attacks among various critical infrastructures changed in physical space between February and August 2022 in the conflict in Ukraine, Figures 2 and 3.

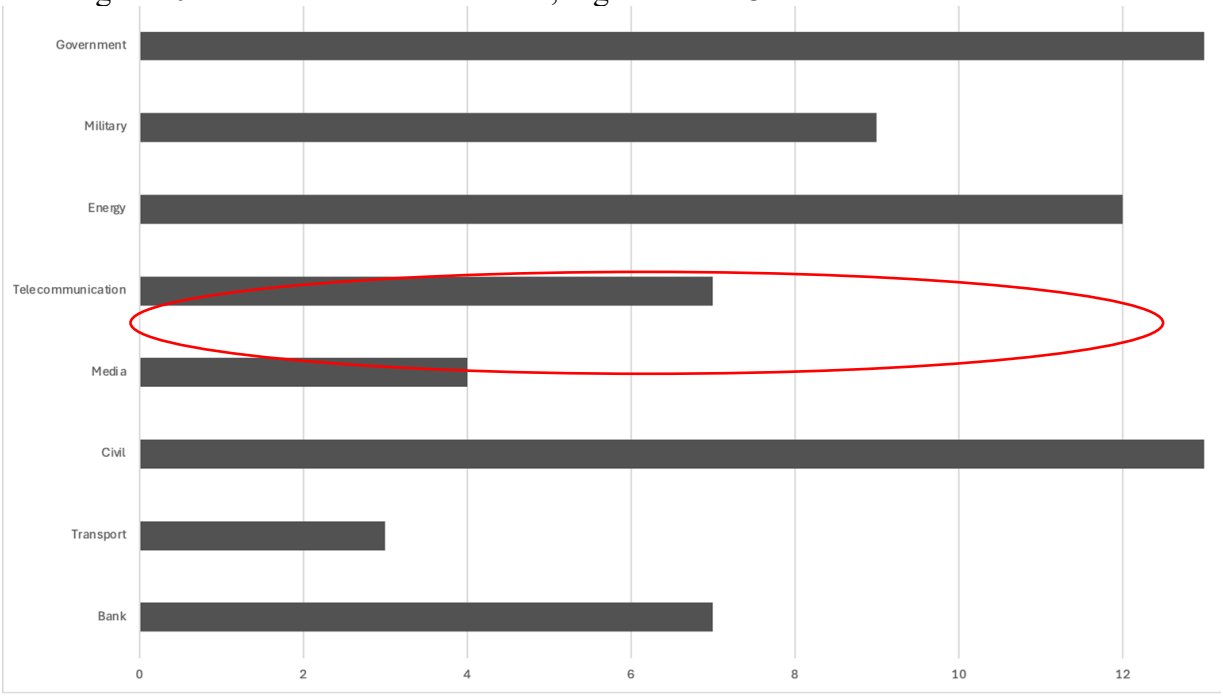

Figure 2. Distribution of targets in the conflict in Ukraine in February 2022 [11].

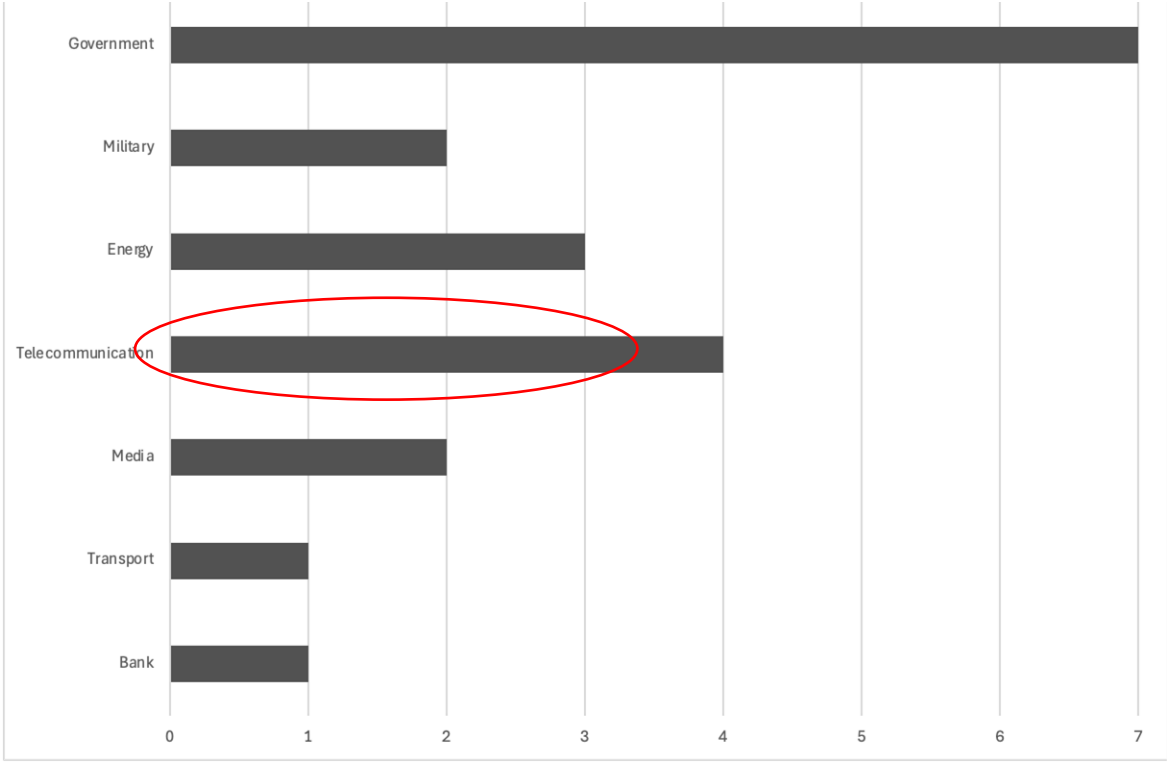

Figure 3. Distribution of targets in the conflict in Ukraine in August 2022 [11].

Figures 2 and 3 show a shift in emphasis on different targets. At the same time, the intensity of the attack on energy systems did not decrease at all.

The 1977 total blackout in New York showed how a long blackout can result in severe civil unrest. Can the devices, facilities and the current energy system or its parts be identified as national/European critical system elements?

Are there any Hungarian or international sector criteria that influence identifying as such?

What are the critical system elements in energy systems? Based on our research, how can these be expanded?

CONCLUSION

Our research shows that protection of the energy sector is still very much in its infancy. Strategic thinking or even cross-sector integration has not yet come together at the regulatory level. It is encouraging to see that the level of preparedness of the sub-sectors is more advanced, and the directions vector of harmonization at the international level is the same. The singularity problem is valid, i.e. until the advent of artificial intelligence and quantum computers, the human mind and its capacity will most likely be the bottleneck in resolving the outlined problem *en masse*. Only introducing new technologies will allow to overcome this. In the meantime, for the rest of our investigations, the main question to answer is that, although the new regulations provide guidelines for the applicable cyber security actions in relation to new systems, how the systems that have already been deployed and are currently operating can be managed. The goal is to create an anti-fragile energy system, considering that digitalization and the emergence of new technologies will continue. Meanwhile, all these processes need to be further strengthened taking into account the constantly decreasing number of qualified personnel.

REFERENCES

[1] Batta, G.: *Current issues of electricity supply from a regulatory perspective.* In Hungarian. https://www.mee.hu/cikk/a-villamosenergia-ellatas-aktualis-kerdesei-szabalyozasi-szempontbol, accessed 31st January 2024,

[2] MEKH: *HMKE Adatok.* https://mekh.hu/download/3/64/61000/HMKE_adatok_2023.xlsx, accessed 31st January 2024,

[3] United Nations: *Human Development Indices and Indicators.* https://hdr.undp.org/system/files/documents/2018humandevelopmentstatisticalupdate.pdf, accessed 31st January 2024,

[4] Baezner, M. and Robin, P.: *Stuxnet*. ETH Zürich, Zürich, 2017,

[5] Vasquez, C. and Groll, E: *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault.* https://cyberscoop.com/viasat-ka-sat-hack-black-hat, accessed 31st January 2024,

[6] Nordex SE: *2022 Together for change – Wind for a sustainable future Sustainability report 2022.* https://www.nordex-online.com/wp-content/uploads/sites/2/2023/03/SustainabilityReport_Nordex_EN_2022-s.pdf, accessed 31st January 2024,

[7] Kovács, L. and Krasznay Cs.: *Digital Mohács: A cyberattack scenario against Hungary*. In Hungarian. Nemzet és Biztonság **3**(1), 44-56, 2010,

[8] European Parliament: *The NIS2 Directive.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, accessed 30th July 2024,

[9] Qi, J.; Hahn, A.; Lu, X.; Wang, J. and Liu, C,-C.: *Cybersecurity for distributed energy resources and smart inverters.*
The Institution of Engineering and Technology **1**(1), 28-39, 2016,
http://dx.doi.org/10.1049/iet-cps.2016.0018,

[10] Said, D.: *Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid.*
Energies **16**(8), No. 3572, 2023,
http://dx.doi.org/10.3390/en16083572,

[11] Kovács, L. and Görgey, P.: *Cyber Defense and Cyber Operations in the Shadow of War: Cyber Warriors, Artificial Intelligence, and Quantum Technology.* In Hungarian.
https://www.mee.hu/cikk/kibervedelem-es-kibermuveletek-a-haboru-arnyekaban-kiberharcosok,-a-mesterseges-intelligencia-es-a-kvantum-technologia, accessed 30th July 2024.