COMCERT

APATOR

EXPERT OPINION

Threats to Smart Grid Cyber Security in Poland in Connection with Smart Meter Rollout

Including Recommendations to Counter Threats

The Expert Opinion was created in cooperation between ComCERT SA and Apator SA

August 2023

1. **Executive summary** 03

2. **Introduction** 04

3. **Technological sovereignty** 06

4. **The importance of cyber security in the energy industry** 08

5. **Threats to metering equipment and systems** 12
5.1. Threats to metering equipment and systems 14
5.2. Communication channel attack 15
5.3. Supply chain attack 16

6. **Suggestions for minimising supply chain risks** 19

7. **Recommended actions for supply chain risk minimisation** 28
7.1. Near-term perspective 28
7.1.1. Amendment to the Act on the National Cyber Security System (UKSC) 28
7.1.2. Recommendations of the Government Plenipotentiary for Cyber Security 29
7.2. Long-term perspective 30

8. **Call for action to improve cyber security in the energy sector** 34

1. EXECUTIVE SUMMARY

1. An en-masse replacement of standard electricity meters with Automatic Meter Reading (AMR) solutions is underway in Poland. By 2028, around 16 million meters equipped with a communication module will be installed in the electricity grid. Of the approx. 4 million devices installed so far, more than half come from outside the EEA, from vendors not verified for cyber security.
2. The coming months will be critical for the future and security of smart grids in Poland. The lack of cyber security regulation applicable to AMR meters used in the energy sector threatens the stability and security of the entire system.
3. There is an urgent need for action on the part of the Polish Government and the relevant institutions and services to create optimal conditions for the energy transition, which requires a secure and digitally resilient energy infrastructure.
4. Technological sovereignty should be part of the energy transition process in the same way as information technology.
5. The progressive energy transition process entails the digitisation of the sector as a prerequisite for its dynamic development, while also raising challenges of resilience to physical and digital threats.
6. ICTs have been, are and will continue to be targeted by criminal groups, state-sponsored actors or directly by the intelligence agencies of hostile states.
7. Smart meters are a vital link in the electricity supply chain, and their pre-planned remote disruption can cause widespread power failures in distribution networks, negatively affecting large groups of consumers and businesses.
8. In Poland, the biggest and as-of-yet unaddressed risk in the context of smart meters is a possible attack on the supply chain, i.e. including backdoors or logic bombs in meters supplied to Distribution System Operators (DSOs).
9. Countries that are rival or outright hostile to the broadly construed West, which are successively expanding in the Polish Advanced Metering Infrastructure (AMI) market, have all the motivation and resources necessary to carry out such an attack. Indeed, they have dominated in the recent tenders.
10. The NIS2 Directive on measures for a high common level of cybersecurity across the Union (to be implemented in Poland by October 2024) requires all entities belonging to the so-called "essential entities" (which includes DSOs) to ensure supply chain security.
11. European vendors and cyber security experts (also supported by the position of the National Chamber of Commerce for Electronics and Telecommunications of 4 August 2023[1]) call for proposals for legislative changes in the field of cyber security, including smart meter supply chain security.
12. Considering the significant amount of time required to prepare and implement the regulations in question and the need for URGENT action, it is reasonable to adopt non-regulatory mechanisms (following the example of other European markets) during the transition period. These could include the recommendations of the Government Plenipotentiary for Cyber Security, which serve to draw attention to and counter specific, real threats to Poland's critical infrastructure.

A recommendation that the national power system not use equipment or software from outside the European Economic Area could significantly reduce the risk to the remote reading meter supply chain and contribute to the security of the national power grid in today's extremely challenging and uncertain geopolitical and macroeconomic environment.

1 https://kigeit.org.pl/FTP/if/SIS-SG/230804_Stanowisko_KIGEiT_Bezp_liczn_e.e.pdf — accessed 12 September 2023

2. INTRODUCTION

The "Recommendations on cybersecurity for the energy sector", issued by the Ministry of Environment and Climate, reads as follows: "The development of the Polish energy sector and its ongoing digitisation result in greater vulnerability of the services provided to cyber security threats. The 2021 amendments to the Energy Law define the lines of development of the Polish energy system but also enable its further safe integration with renewable energy sources and synergies in the sector — including increasing the energy system's flexibility and exploiting the potential offered by active consumers. Furthermore, mention should be made of the proposed comprehensive solutions to remove legal barriers to the development of battery storage facilities enabling the further development of distributed (prosumer) energy sources and RES (Renewable Energy Sources).
Yet, crucially from a cyber security standpoint, the solutions that have been prepared are merely a starting point for the **transformation of the energy sector through such things as digitisation, smart grids and smart AMR meters,** as well as providing a legal framework for smart metering in the electricity sector. Investments in smart grid development, including AMR meters, is the overarching approach adopted across the European Union, resulting in an obligation for electric grid operators to install smart meters for at least 80% of their end customers by the end of 2028"[2].

In the context of the energy transition, the issue of technological sovereignty is also emerging as one of the many challenges that should be addressed in this process. This paper aims to examine the phenomenon **of technological sovereignty in the context of Poland's energy security and,** in particular, to analyse how technological sovereignty manifests itself in the energy sector based on the example of smart energy meters, as well as what risks and threats it poses to the National Electricity System, and to present proposals to minimise them.

By no means is this expert opinion intended to target any specific company. It outlines an objectively increasing risk to the supply chain regardless of the vendor's country of origin or business ties.

- **Chapter 2** presents the main conclusions summarising the analyses carried out in this study.
- **Chapter 3** defines technological sovereignty and the challenges of implementing new technologies in the electricity sector.
- **Chapter 4** contains the main risks that may affect the stability, reliability and security of the National Electricity System. It also lists the major attacks against energy sector companies over the past several years. The chapter also provides information on the risk factors and potential consequences of a successful cyber attack on the energy sector.
- **Chapter 5** examines possible attack vectors on the electricity distribution system that could exploit smart metering devices. The chapter also includes a summary of the analysis, which lists the protection measures currently in place against the potential types of attacks and their possible consequences.
- **Chapter 6** contains proposals for minimising supply chain risks. The proposal was developed using the SWOT analysis.
- **Chapter 7** enumerates the recommended actions for minimising supply chain risks. These are broken down into short- and long-term ones.

2 https://www.gov.pl/web/klimat/rekomendacje-dotyczace-dzialan-majacych-na-celu-wzmocnienie-cyberbezpieczenstwa-w-sektorze-energii-oraz-wytyczne-sektorowe-dotyczace-zglaszania-incydentow — accessed 23 August 2023

- **Chapter 8**contains a call for action to improve cyber security in the energy sector.

In this document, the terms "smart energy meter", "AMR meter" and "smart meter" are used interchangeably.

3. TECHNOLOGICAL SOVEREIGNTY

technological sovereignty, which has been going on around the world for several years, has recently intensified.

The concept of "technological sovereignty" is by no means new — it is its precise definition that is a contentious issue. Some view it mainly as retaining control over key sectors of the economy (in terms of economic strategy); others believe that independence, control and autonomy over technology and production solutions (a technical and technological approach) are most relevant.

In the European Sovereignty Index[3], a study by The European Council on Foreign Relations (ECFR), technological sovereignty is defined as: "the ability to shape critical technologies in accordance with the European Union's interests and values. The EU would be technologically sovereign if it developed globally competitive critical technologies, regulated their dissemination and use effectively, and avoided excessive dependence on other powers for technologies that are essential to its economic, political, and societal well-being."

Thus, technological sovereignty construed in this way would mean not only the ability to develop and implement technologies to produce highly advanced equipment or products domestically and independently of foreign vendors but also the ability of an entity (country, organisation or society) to oversee and manage its technologies, infrastructure and data as independently and autonomously as possible (including their distribution).

The EU Sovereignty Index assesses 6 areas: climate, defence, economy, health, migration and technology. In the area of technological sovereignty, the average score of EU member states was as little as 4.8 out of 10 (weighted by population)[4]. This is the lowest average score of all six domains in the Index. Notably, none of the five largest EU countries — Germany, France, Italy, Spain and Poland — ranked in the top three in this respect[5].

In assessing the contribution of member states to European technological sovereignty, the authors of the European Sovereignty Index focused on artificial intelligence, big data, cloud computing, semiconductors, robotics, the Internet of Things, high-performance computing, advanced telecommunications and cyber security. As can be seen, all the fields considered are related to ICT. The reason behind this is the authors' belief that these technologies play a fundamental role in economic and political development in today's increasingly digitised economies and interconnected societies, as well as that they are central to the technological competition between great powers and are at the heart of the European debate on technological sovereignty.

The index measures the technological capabilities of member states and their commitment to technological sovereignty through certain indicators[6]. In the case of technological capabilities, some of those taken into account included:

- contribution to research, patents and standards;
- number of technology companies and specialists;
- market shares of companies;
- venture capital investments in the above technologies;
- technology absorption;
- cyber security capabilities.

3 https://ecfr.eu/wp-content/uploads/2022/06/European-Sovereignty-Index.pdf and https://ecfr.eu/special/sovereignty-index/ — accessed 19 August 2023.
4 Poland's average score in this area is 3.6 — ibid.
5 Poland ranks at the bottom of the pile, in the last five, and is overtaken by such countries as Slovenia, Greece and Lithuania.
6 For a full list, see the "Technology" section and click on the "List of indicators" to expand it: https://ecfr.eu/special/sovereignty-index/#terrain-technology accessed 19 August 2023.

In contrast, commitment to technological sovereignty is assessed through such things as:

- positions on EU regulations and cooperation;
- involvement in international technology forums;
- participation in European research and development;
- contributions to EU international technology initiatives;
- survey data on public support for technological development.

The issue of technological sovereignty was hotly debated along with the discussion on 5G technology (it also came to the forefront in the minds of politicians and the broader public). One can risk the claim that the debates held at the level of the European Union and in the Polish public space have raised awareness of this issue and the dangers of overlooking it or focusing exclusively on the economic aspect of the technologies being implemented in Western countries. The European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP))[7] states that:

- there is no guarantee that the regulations that apply to entities offering 5G technology in the countries of origin [8]are not applied extraterritorially, and they could threaten EU security,
- cybersecurity competence centres and networks of national coordination centres should support the EU in maintaining and developing the technological and industrial cyber capabilities needed to secure its digital single market,
- work should continue on establishing a certification system for equipment (in this case, 5G),
- certification should not preclude monitoring of the supply chain by competent authorities and operators to ensure the integrity and security of equipment operating in critical telecommunications environments and networks.

The challenges of implementing new technologies have also been recognised in the electric power sector. As early as the beginning of the previous decade, the President of the Energy Regulatory Office issued a series of positions on the necessary requirements for smart metering and billing systems implemented by the DSOs, i.e. the so-called positions on AMI[9]. In these positions, AMI (Advanced Metering Infrastructure) is defined as follows: "a metering and billing system comprising a central application, two-way communication infrastructure, metering infrastructure and other elements for remote measurement, transmission, storage and processing of metering data concerning electricity and possibly other utilities, as well as relevant information and commands." The characteristics of AMI (as distinguished from AMR — Automatic Meter Reading) are[10]:

- possibility of two-way communication with the meter,
- compatibility with a Home Area Network (HAN),
- greater network complexity,
- Smart Grid compatibility.

Links between the issues of technological sovereignty and security of the National Electricity System (NES) in the context of smart meters are examined in the subsequent chapters.

7 OJ C 23, 21.1.2021, p. 2 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:C:2021:023:FULL&from=NL— accessed 14 August 2023.
8 The resolution refers to the example of China's State Security Law, which requires all citizens, businesses and other entities to cooperate with the Chinese state in protecting state security, in conjunction with a very broad definition thereof — ibid.
9 e.g. positions of the President of the Energy Regulatory Office of 31 May 2011 and of 10 July 2013.
10https://pl.wikipedia.org/wiki/Zaawansowana_infrastruktura_pomiarowa

4. THE IMPORTANCE OF CYBER SECURITY IN THE ENERGY INDUSTRY

The National Electricity System (NES) is a "system of systems," combining electricity generation, transmission, distribution and consumption systems (or subsystems). There are a variety of threats that can affect the stability, reliability and security of the NES. Some of these are related to technical and weather aspects; others relate to geopolitical issues or the ability to actually manage the NES. Some of the main risks include:

- **Infrastructure failure:** Damage to infrastructure components, such as transmission lines, transformer stations or generators, can lead to power outages, especially if the protection and backup systems in place are insufficient. In the case of an outage, determining the root cause is crucial, as it can be either an equipment failure due to a defect or sabotage that simply appears as one. Failures or disruptions in one area of the network can have a cascading effect on other areas, which can lead to extensive power outages across entire regions.
- **Weather events:** Weather conditions like thunderstorms, windstorms, rainfall and snowfall can damage energy infrastructure and cause power outages.
- **Electromagnetic interference:** Electromagnetic pulse, caused by such things as solar storms or nuclear explosions, can disrupt the power system, damage electronic devices and cause failures. However, it may also be caused by military Electronic Warfare technology.
- **Grid imbalance:** Power shortages may occur during periods of high energy demand, leading to energy supply restrictions or even breakdowns.
- **Import/export dependence:** Poland imports/exports some electricity; this exposes it to energy supply or receipt disruptions, which may destabilise the NES.
- **Ageing infrastructure:** Part of the energy infrastructure is outdated, not in line with the current conditions and requirements of NES operation, and requires modernisation. A mismatch with contemporary standards or using unsuitable and untested solutions can increase the risk of failure and disruption.

The most important aspect of NES security is maintaining grid stability (balancing). Smart monitoring and management systems can help predict and adapt to changes in electricity production and consumption, as well as implement flexible mechanisms such as emergency load disconnections to prevent grid overloading. However, large-scale deployment of smart monitoring and management systems generates new risks caused by the technology itself. An en-masse disconnection of customers due to a fault or intentional actions by external actors can cause grid instability and, if no sufficient regulation and backup mechanisms are in place, it may cause a widespread grid failure known as a blackout.

The deployment of smart monitoring and management technologies in the power sector also creates risks due to conflicting demands between the desire to reduce costs and ensure the safety and effectiveness of technological solutions. To drive down costs, some vendors may choose to use cheaper, non-compliant components or cut costs in areas related to safety or quality. Doing so can lead to failures, cyber-attacks or low energy efficiency. Balancing these requirements is key to ensuring the sector's sustainability while also guaranteeing savings and security for users and government infrastructure. Therefore, it seems reasonable to introduce quality and security requirements (including cyber security) to the procurement process, as discussed later in this paper.
Cyber security is another vital challenge that must be addressed in the context of NES security. Cyber threats are a pertinent issue for any sector of the economy in which the scale of digitisation allows cybercriminals to launch attacks to disrupt it or its components. The energy sector is particularly vulnerable to cyber attacks due to its strategic importance to the functioning of state and local structures, as well as each individual citizen. Over the past few years, both the conventional and renewable energy industries have dramatically increased their degree of digitisation and, consequently, the dispersion of their structures. Energy sector companies are among the most frequently attacked businesses. These attacks are most often carried out by actors supported and financed by

hostile states and seek to disrupt or outright destroy electricity distribution or transmission infrastructure. The largest of these included:

- 2001: – an attack on California Independent System Operator, an electricity supplier — attackers gained access to one of its internal networks. The attack affected the power grid before it was detected, causing a power outage for nearly 400,000 customers. It was likely sponsored by China.
- 2003: – an attack on the Davis-Besse Nuclear Power Station in the US — an attacker used malware to disable the system displaying the reactors' operating parameters for four hours; no data was stolen; no attacker attribution data available.
- 2008: – Edwin I. Hatch Nuclear Power Plant incident — a management software update error led to an error in the reactor control system resulting in a 2-day power outage; no attacker attribution data available; no data on the possible use of malware in the incident.
- 2014: – an attack on Korea Hydro and Nuclear Power (KHNP) in South Korea — the theft of plans and manuals for two reactors, power systems data and results of radiation exposure measurements in the NPP zone, as well as data of more than 10,000 KHNP employees. The attacker then demanded that the three reactors be shut down, or else the stolen materials would be published.
- 2015: – an attack on three Distribution Network Operators (DSOs) in Ukraine — more than 50 power substations were disconnected from the grid. Power shortages affected some 225,000 customers. The industrial automation system was physically damaged. The substations had to be operated manually for several weeks after the incident. The attacker used malware called BlackEnergy; the attack was likely sponsored by Russia.
- 2016: – an attack on a Distribution Network Operator (DSO) in Ukraine — the part of the grid responsible for supplying energy to the Ukrainian capital became the target of the attack. The consequences of the attack were severe power supply restrictions for thousands of customers in the northern part of Kyiv. The attack was likely sponsored by Russia, as shown by an international investigation (2016 saw similar attacks on the US power grid carried out by the same actor).
- 2016: – an attack on Israeli power grids — though the attack resulted in no power outages, it managed to compromise government energy-related systems; no attacker attribution data available.
- 2020: – an attack on Energias de Portugal (EDP), an energy supplier — a ransomware attack, likely using stolen credentials. The attackers stole 10 TB of data, including customers' personal information; no attacker attribution data available.
- 2022: – an attack on Delta-Montrose Electric Association (DMEA), a US electricity supplier — the attack forced the company to shut down 90% of its IT infrastructure due to irretrievable data loss. The attackers deleted databases containing 25 years' worth of information on company operations; attacker attribution unknown.
- 2022: – a series of attacks on wind turbines of various operators in Europe — as a result of the attacks, one operator lost connection to 6,000 wind turbines, one fell victim to a ransomware attack, and another was forced to shut down all remotely managed equipment for 24 hours. These attacks were probably related to the outbreak of war in Ukraine and were enabled by Russian support.

It should be noted that the development of modern ICT also brings threats in the field of espionage. US authorities have warned several German governments against allowing too much Chinese capital into their critical infrastructure[11]. In March 2023, news broke of a "Trojan horse in Hamburg" when it was determined that Chinese container cranes working in the German port were equipped with advanced sensors that could collect sensitive data, including information on military shipments[12].

11https://www.euractiv.pl/section/gospodarka/news/czy-chinskie-dzwigi-szpieguja-port-w-hamburgu/ — accessed 17 August 2023
12https://wgospodarce.pl/informacje/124564-chinskie-dzwigi-szpieguja-kon-trojanski-w-hamburgu — accessed 17 August 2023

According to Check Point Research, the number of cyber attacks worldwide is the highest in 2 years, averaging 1,258 per week. Significantly, Q2 2023 alone saw an 8% increase compared to the same period last year. Europe has seen the highest rise in attacks — a more than 21% increase. Meanwhile, in Poland alone, there were 33% more cyber incidents in Q2 2023 than in Q2 2022.[13]

The following risk factors that threaten the energy sector's cyber security are usually mentioned:

- high rate of digitisation in the energy sector — the energy system transition brings with it the need to implement greater access to secure energy. This process is being implemented through the development of new technologies, which additionally bring a new vector of cyber threats. One example is using Smart Grid technology, which is set to improve system efficiency. The main advantages of this solution are improving the security of supply and reliability of the power system, the ability to notify customers about the current electricity prices, facilitating the development of distributed generation sources and their connection to the power grid and improving customer awareness of how to optimise energy use The technology also makes it possible to remotely detect grid failures and fix related problems on the fly. Unfortunately, its biggest drawback is its vulnerability to cyber-attacks. This is why it is necessary to develop and implement effective cyber security strategies in every organisation operating in the energy sector.
- advanced ICT attacks (cyber-attacks) — as technology develops, so do the intensity and sophistication of cyber attack attempts. Cybercriminals are also using more and more sophisticated methods and tools; thus, their actions are increasingly difficult to detect quickly. Further, many security incidents are caused by organised crime groups specialising in cyber attacks, including those sponsored by governments (APT attacks). This is a major challenge not only for energy companies but also for manufacturers and suppliers of equipment and software used in energy systems.
- the energy sector is an attractive target — energy is a strategic aspect of state security while also providing security at the local and individual levels. This makes it a particularly tempting target for cybercriminals, guaranteeing significant benefits in the event of a successful attack. After all, the operations of virtually all public and economic entities depend on the energy sector and the efficient distribution of energy.

The consequences of a successful cyber attack targeting the energy system can be wide-ranging — the victims are bound to face legal, financial and reputational consequences. These consequences should also be considered in economic and even political terms. Attackers want to achieve their goals, which in the case of the energy sector can be characterised as follows:

- financial benefits — typically the ransom that energy sector players will pay to regain access to strategic management systems, distribution systems and service systems;
- causing destabilisation and social unrest by attacking energy industry structures responsible for providing electricity and heat to institutional and private customers. Such actions are usually designed to negatively affect a country's economy or create a political crisis. They are often initiated at the behest of governments or organisations hostile to that country;
- inducing a situation on the stock exchange that is desirable for the attacker but unfavourable for the energy sector players. Cyber attacks can be part of business wars between competing institutions;
- generating financial losses in energy companies while aiming to undermine the given institution's market position and weaken public confidence in its services;
- intellectual property theft.

13 https://crn.pl/aktualnosci/najwyzszy-poziom-cyberatakow-od-dwoch-lat/ — accessed 7 August 2023

Yet, it is the social impact that seems the most significant. The level of dependence of individual consumers and entire industries on electricity means that a blackout caused by a successful cyberattack can immediately affect many millions of people and disrupt the operation and supply of services essential to the functioning of modern societies, e.g., water and sewerage systems, healthcare, public transport, telecommunications. Modern households increasingly rely on electricity due to the rapid development of household technology and, at the same time, the increasing environmental awareness in society. Recently, the tendency to transition to electricity has been reinforced by the risks associated with the supply of natural gas fuels due to the Russo-Ukrainian war. One reason behind increased electricity use is personal transport and the rising prevalence of electric cars, which are becoming a popular alternative to internal combustion engine vehicles and thus help reduce harmful emissions. Heating systems are changing as well. Although natural gas solutions continue to be marketed, modern gas heaters still require a continuous supply of electricity to power their electronics. Due to climate change, Poland is seeing an increase in the use of air-conditioning systems, a solution deemed indispensable in many regions but not previously taken into account as a challenge that the electricity grid would have to face.

Considering the above, cyber security in the power sector is becoming a key issue that must be addressed to ensure the continuity of electricity supply.

5. THREATS TO METERING EQUIPMENT AND SYSTEMS

The National Electricity System (NES) is at the precipice of a transition that must take place in the coming years. By 2030, it will need to be connected to:

- more than 20 GW of solar power sources (excluding prosumer systems set up after 31 December 2021) with an annual output of 21 TWh,
- more than 14 GW of onshore wind power sources with an annual output of 37 TWh,
- nearly 11 GW of offshore wind power sources with an annual output of 40 TWh.

The number of customers connected to the grid is expected to increase by more than 2 million during this period. Due to the growth of the Electric Vehicle sector, it will also be necessary to install more and more electric vehicle charging stations. **By that point, all of Poland's 18 million electricity consumers will have AMI meters** (i.e. smart meters[14]) set up on their premises.

Today, more and more automated or smart solutions are being used as part of the IT infrastructure supporting the electricity distribution system and related metering systems. Artificial Intelligence- and Machine Learning-driven Smart Grid and Smart Metering systems are now used for real-time energy flow monitoring and control. Adapting ever newer, more automated and advanced solutions provides many benefits to the energy sector but also brings additional security risks. The Smart Grid (SG) technology mentioned above is intended to match the scale of the challenges facing the grid infrastructure operated by the Polish power sector. SG is based on modifications to the existing power grid. One of these is the introduction of Advanced Metering Infrastructure (AMI) into the grid. AMI uses one- or two-way communication between suppliers and consumers' smart electricity meters and implements smart data collection solutions.

Smart meters are metering systems that enable the automatic collection, storage and transfer of detailed electricity consumption data. They mainly measure consumers' electricity consumption in real time while also monitoring power supply quality and instantaneous electrical characteristics like voltage and current at customer take-off points, and send this data to electricity providers at a certain frequency. This way, power companies can monitor and adjust short-term energy demand (demand response), provide more accurate billing and use dynamic pricing to help reduce energy consumption during peak demand. They eliminate the need to read meters manually and, through data transfer, allow real-time monitoring of energy consumption data. The fact that smart meters transmit data to strategic entities, i.e. power companies, makes them a target for cybercriminals. The data transmitted by the meters is detailed data on the consumer's electricity consumption, i.e. personal data. If intercepted, this data can be analysed and used to draw conclusions about a household's activities, or even the type of appliances that it uses, which in turn can not only lead to an invasion of the consumer's privacy but also provide cybercriminals with information about their daily schedule, social status and other aspects of their life (profiling).

Personal data leaks are not the only negative consequence of cyber threats facing the energy system. Smart electricity meters are equipped with contactors that allow remote disconnection of the consumer from the electricity grid. While this is practical for Distribution Network Operators, the contactor and the possibility of its remote triggering allows attackers not only to deprive a selected group of victims of power but — if many devices are compromised — to throw the entire electricity grid out of balance. This called a Load Oscillating Attack. Here, the idea is to disconnect electricity consumers en masse when there is high electricity demand (high electricity consumption).

14 https://www.ure.gov.pl/pl/urzad/informacje-ogolne/aktualnosci/10630,Rynek-energii-elektrycznej-historyczne-porozumienie-sektorowe-regulatora-i-opera.html?search=8507173 — accessed 21 August 2023

Since a large number of energy consumers are disconnected from the power grid, the excessive load is automatically transferred to its other segments, tripping excess energy safeguards throughout. This creates a domino effect which can cause a complete blackout across large areas of the country[15].

In its position on AMI of 10 July 2013,[16] in the chapter on risk analysis, the Energy Regulatory Office President pointed to market and operator risks. Among the market risks identified was "the risk of potential petrification of the market of customers (users) of AMI infrastructure (end users and DSOs) through the division of this market among dominant suppliers of infrastructure elements," which could lead to "dependence on a single technology supplier in the area of operations of a given DSO." In turn, the identified operator risks included "the exposure of the AMI communication infrastructure to potential "bottom-up" introduction (by the end customer or a third party) of a signal destabilising the entire system's operation, particularly by blocking the possibility of transmitting useful signals or by introducing false signals/commands; here it should be noted that the risk of "hacking" via physical access in this case is of the same nature as the risk of exploiting a transmitted signal (tapping over-the-air signals)." It is apparent that the potential risks of third-party interference with smart monitoring and management systems were recognised as early as 10 years ago.

To date, there has been no reported campaign or cyber attack focusing solely on smart metering devices or any other Smart Grid component and aiming to disrupt supply or destabilise the entire electricity distribution system. The only attack made public to date that directly used metering devices was of a different nature. The incident took place in Puerto Rico,[17] where the attacker used an optical connection and software to access the memory of smart meters and then, using the credentials obtained in this way, falsified electricity consumption readings, which resulted in under-billing. The losses were valued at several hundred million dollars. This does not mean that the threat does not exist, however. This vector is being analysed and researched [18]and is a genuine threat. An attack aiming to destabilise the energy supply of a country such as Poland could be an element of political pressure or serve other goals pursued by a hostile power.

Equipping smart meters with contactors allows attackers — if they can first add backdoors or logic bombs to the devices — to simultaneously and remotely connect or disconnect a large number of consumers. For this reason, it is crucial to develop appropriate requirements for smart metering devices and to establish procedures for verifying that the devices meet these requirements.

15https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10098782&tag=1 — accessed 17 August 2023

16 Position of the President of the Energy Regulatory Office on the necessary quality requirements of services provided using AMI infrastructure and the framework for interchangeability and interoperability of Smart Grid network elements and Smart Grid-linked home network elements — https://ise.ure.gov.pl/ise/stanowiska-regulatora/5357,Stanowisko-Prezesa-URE-w-sprawie-interoperacyjnosci-sieci-Smart-Grid.html — accessed 17 August 2023.

17https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ — accessed 7 August 2023

18 e.g. Security analysis of the OSGP protocol/meters by Philipp Jovanovic and Samuel Neves — https://www.iacr.org/archive/fse2015/85400109/85400109.pdf (accessed 16 August 2023), which led to a change in encryption algorithms from RC4 to AES128

One can distinguish three possible attack vectors on the electricity distribution system that could exploit smart metering devices:

1. Physical attack

Description	Threats	Security
A physical breach of the device's hardware components and firmware.	Unauthorised access to measurement data, manipulation of meter data, unauthorised disconnection from the grid or damage to the device.	Tamper event detection and registering, signalling unauthorised access to the AMI supervision centre or a power company employee.

2. Communication channel attack

Description	Threats	Security
Exploiting vulnerabilities in communication protocols or firmware.	Interception or manipulation of data sent to and from the meter, including unauthorised disconnection from the grid and potential access to other grid systems.	Encrypting communications or data sent over communication channels, using robust authentication mechanisms for management activities and regular firmware updates to patch known vulnerabilities.

3. Supply chain attack

Description	Threats	Security
Exploiting backdoors or logic bombs that are implemented in the meter's firmware during the manufacturing process.	Unauthorised access to data transmitted to and from the meter or to its functions, unauthorised disconnection from the grid, potential meter damage or deactivation and possible attack on other grid elements.	Rigorous screening of equipment vendors and security practices used in the manufacturing process, regular firmware security audits and device security testing, implementation of mechanisms to protect firmware and detect and respond to unauthorised firmware modifications.

5.1. Physical attack

It is widely believed that smart electricity meters are protected against the first vector of attack — most meters, if their housing is opened in an unauthorised manner, record the tamper event and notify the AMI supervision centre or signal this issue to the power company employee during a maintenance visit. Moreover, this requires physical access to the device, effectively limiting the scale of the potential attack.

Electricity meters, including smart meters, typically utilise microprocessors and dedicated, proprietary firmware. As such, it comes with no instructions or commands that would allow an attacker to perform complex operations like reading or accessing processor or non-volatile memory. By default, the meter provides data related to the reading of electricity consumption and quality, which are transmitted in pull mode once the electricity supplier's monitoring system has established a connection with the meter. Establishing a connection session involves authorisation, negotiating the parameters of the communication channel and encrypting the channel itself. Yet, this does not discourage cybercriminals and avid hackers. A lot of content and research data on attempts to modify smart meter firmware[19] have been made available online; these include, e.g. putting the microprocessor into a transient state

19 https://www.youtube.com/watch?v=O-J9H2XrZgE

to cause it to malfunction due to repeated brief power outages. Here, the attacker's intention is to obtain the full content of the meter's processor memory through a power outage. Upon obtaining the data, the attacker can analyse it to find vulnerabilities. This can facilitate an attack through a communication channel, e.g. by allowing the attacker to acquire the cryptographic keys stored in the device's memory. This type of attack requires acquiring the device. Attackers typically source the meters through online auction websites and, less commonly, through theft.

Such an attack requires specialised knowledge and equipment. It is also time-consuming due to its methodology and the need to gather information on the electronic components used to build the specific meter model. Attackers can obtain these by analysing the meter's documentation published or made available by the manufacturer, as well as certification documentation and documentation of the electronic systems installed in the meter. Yet, the above difficulties are just one reason why the physical attack vector against smart meters seems unlikely. An additional factor is the limited scale effect — this attack method requires physical interference with a device located on the user's premises. Gaining control over one or several devices does not threaten the entire electricity distribution system.

Instead, the risk to be considered is the attacker gaining knowledge of possible vulnerabilities in the meter's firmware, which could lead to a successful exploitation of the communication layer attack vector.

5.2. Communication channel attack

The second identified attack vector against smart metering devices is using their communication layer to intercept or modify transmitted data or to take over the devices.
Smart metering devices communicate with the outside world in several ways. The first plane of communication is usually 3G and 4G cellular networks, which offer wide bandwidth and high availability. General Packet Radio Service (GPRS) and 2G solutions are used much less frequently. Notably, the connection between the measuring device and the management centre does not use the Internet or any other publicly available network for transmission. The SIM cards used to open communication channels to the management centre only enable connection with the electricity supplier's dedicated network. These restrictions are put in place by the Mobile Network Operator, which determines the connection setup parameters (APN) when configuring its devices and programming SIM cards.

It appears that these restrictions can likely only be overcome using potential vulnerabilities or bugs in the meter's firmware or using backdoors intentionally included in the firmware by the manufacturer. Backdoors and possible vulnerabilities can allow attackers to reroute the connection to their own command & control server by modifying the meter's connection set-up parameters. Attackers can also launch a Denial-of-Service (DoS) attack on a wireless communication module, effectively disrupting communication with the management centre. However, this type of attack requires an attacker to have considerable resources, making it less likely to occur.
Another possible risk is having individual devices using a cellular network connected to a separate network that is not segmented in any way. In such a situation, compromising one device exposes others on the same network, including the management system, to a potential threat. This can happen if outdated communication protocols are used, the transmission is not encrypted or uses identical encryption keys on every device. If all meters have the same set of encryption keys implemented across the system, data transmission is most often encrypted symmetrically. Thus, acquiring a single key allows an attacker to see the data transmitted across the measurement network. This, in turn, can lead to data interception or falsification through a Man-in-the-Middle attack[20], the purpose of which can be to destabilise the electricity distribution system by tricking the management centre into making incorrect decisions (based on false data).

20 A cryptographic attack that involves eavesdropping on and modifying messages sent between two parties without their knowledge

The second layer of communication for smart meters is power line communication technology (Power Line Communication or Power Line Carrier — PLC). This technology is based on transmitting a data signal with a much higher frequency alongside the standard 50 Hz voltage[21]. Since the data is transmitted over the power line, an attacker can gain access to the data by using a hacked metering device. Like in the previous case, this can be done, for example, through a firmware backdoor implemented in the meter's manufacturing process.

The third communication layer for smart meters is short-range communication. Smart meters used in Poland must feature a wireless M-bus radio module,[22] an optical connection and a serial port. In the case of the wMbus radio module, the meter broadcasts the datagram of electricity consumption in the ISM band at intervals defined by the energy supplier or meter manufacturer. Communication is one-way and, if properly configured, it is impossible to set up a two-way channel to connect to the meter's operating system.
The meters are also equipped with local communication ports, such as an optical connection or RS-485 serial port. Compared to the wMBus module, these ports typically offer much greater functionality — their capabilities are similar to those of the remote channel (LTE, PLC), including device configuration and firmware replacement. Establishing communication requires the operator and the receiver to be physically present near the meter. Serial ports can be used to upgrade meters that do not have built-in communication modules. Short-range communications can be used to launch a cyber attack on a metering system, provided the attacker exploits a backdoor, vulnerabilities or bugs in the meter's firmware.

5.3. Supply chain attack

The third attack vector is an attack on the supply chain related to the device manufacturing process. **This is a highly complex problem. At the same time, it is extremely important, especially from the perspective of a cyber attack effected by compromising multiple smart metering devices simultaneously**.

A supply chain attack is an attack in which the targeted entity or infrastructure is not directly attacked; instead, attackers focus on their suppliers. The attackers' rationale is that the latter may be less sophisticated in terms of cyber security and have weaker security monitoring and management mechanisms in place. A supply chain attack may aim to compromise software and hardware alike. Such supply chains are highly vulnerable to attacks because modern organisations do not develop software completely in-house and from scratch. They also use many off-the-shelf components purchased from the market, with the primary criterion often being the lowest price. In the case under consideration, remote reading meters supplied by third-party vendors may be compromised through such an attack.

Below are examples of notable supply chain attacks from recent years:

1. 3CX Phone System — the attackers compromised the 3CX (VoIP PBX) software by adding a backdoor and including it in a legitimate update signed with the software developer's valid certificates. The backdoor enabled access to the victims' networks. According to a Shodan database scan, more than 244,000 instances of 3CX Software had been compromised by the time the incident was detected. Interestingly, the initial compromise also occurred through a supply chain attack — the entry vector was discontinued commercial software that had been previously compromised[23][24].

21 European DSOs can use the Cenelec A band, ranging from 3 to 95 kHz; however, only frequencies between 40 and 95 kHz are used in practice. Frequencies between 95 and 150 kHz are reserved for other purposes (DSOs are not allowed to use them), and the use of frequencies higher than 150 kHz by DSOs is disputed due to possible interference with radio beacons, AM radio, etc.
22 Communication between the master system and the meters (slaves) is done wirelessly in the 169MHz, 433MHz and 868MHz bands. A detailed description of the protocol and physical layer is included in the European standard PN-EN 13757-4 "Communication system for meters and remote reading of meters."
23 https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise — accessed 23 August 2023
24 https://news.sophos.com/en-us/2023/03/29/3cx-dll-sideloading-attack/ — accessed 23 August 2023

2. UAparser.js — the attacker acquired credentials for a software developer's account on the NPM portal and proceeded to insert a backdoor into the UAparser.js package, enabling it to read credentials stored in victims' browsers and session cookies. The attacker also added cryptomining malware to the package. The UAparser.js package is used by the largest and most popular websites, including Facebook, Amazon, Microsoft, Google, Instagram, Mozilla, Elastic, Intuit, Slack and Reddit[25,26].

3. Solar Winds — the attackers injected a backdoor into a SolarWinds software update (SolarWinds is a popular networking tool used by many high-profile companies and government agencies). The backdoor allowed attackers to remotely access thousands of corporate and government servers. The attack ultimately led to a leak of sensitive data from many government agencies and other security incidents[27].

4. NotPetya — a malware attack that targeted Ukraine's government and critical infrastructure and spread to other countries through a supply chain attack on software company MeDoc. It spread through an update to MeDoc, a tax accounting program commonly used by Ukrainian companies.

5. CCleaner — a popular operating system maintenance/optimisation tool; it was hacked and used to distribute malware. .

Placing backdoors in electronic components is a significant risk factor in the context of smart meter supply chain attacks. **Backdoors are deliberately inserted software or hardware vulnerabilities that allow unauthorised access to or control of the entire system or its selected components.** Vendors (or attackers) may intentionally introduce backdoors into shipped products for later use in espionage, sabotage or hacking. In this way, attackers can manipulate the energy supply, cause outages or disable the power supply altogether.

Another significant risk is logic bombs. **A logic bomb can be placed in the software or operating system and activate spontaneously under certain conditions** (e.g. on a certain day or time, after a defined number of system launches or once a user performs some action or change in the system). Thus, the essence of a logic bomb is that it requires no connection to "command & control" servers or, indeed, any online connection at all. The logic bomb stores commands that are run automatically upon its activation. These can trigger destructive actions like deleting or altering data and damaging the operating system or other components. Logic bombs used in the energy sector can aim to weaken, deactivate or even destroy power grid or distribution control and management systems, or in the case of smart meters, simultaneously disconnect customers en-masse.

The table below summarises the threats to metering equipment and systems.

	Current safeguards	Potential consequences
Physical attack	medium	low
Communication channel attack	high	medium
Supply chain attack	low	high

Table 1 — Summary of potential attack vectors

25 https://www.truesec.com/hub/blog/uaparser-js-npm-package-supply-chain-attack-impact-and-response — 23 August 2023
26 https://www.cisa.gov/news-events/alerts/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js — accessed 23 August 2023
27 https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/ — accessed 22 August 2023

The potential consequences of a physical attack and a communication channel attack, as presented in the table, were estimated to be relatively less severe. Nevertheless, it must be noted that the lack of standards in this area has prevented the authors of this study from fully assessing the potential risks in the medium and long term.

6. SUGGESTIONS FOR MINIMISING SUPPLY CHAIN RISKS

The authors of this study believe that the supply chain risks are currently the most serious in terms of their implications for the security of advanced metering infrastructure. Accordingly, the subsequent sections of this paper outline various potential measures to reduce these risks.

The SWOT (Strengths, Weaknesses, Opportunities, Threats) technique was used to present the results of the analysis of supply chain risk minimisation methods in an orderly manner.

While each of the proposed solutions may lead to an increase in the price of AMI components, such expenses are necessary to improve critical infrastructure security.

6.1. Introduction of certification schemes [28]for AMI components, including smart meters in particular

A reliable method of assessing product conformity with specific standards is product testing by authorised and accredited testing laboratories and certification by certification bodies. In this case, assessment bodies always use a certification scheme (programme), i.e. a set of standards and test procedures, that is, criteria and methodologies whose application gives confidence in the objectivity of the assessment. Such schemes have been and are being created for various fields of technology, industrial food production, etc. One example is the Common Criteria,[29] additionally established as International Standard ISO/IEC 15408:2022.

S Strengths:

- accessible — any manufacturer can certify its product;
- objective — the criteria used are the same for all products; evaluations are conducted according to the same methodology;
- multilevel — multiple evaluation assurance levels can be defined (e.g. EAL1–EAL7 in the Common Criteria); the manufacturer can choose which level it pursues while the users (based on these levels) have confidence in what they are getting. Also, the purchaser can choose different levels of confidence for different categories of products or their components;
- versatile — enabling the evaluation of different types of products; the manufacturer declares safety features specific to its product type;
- ensuring confidence in the assessed products — certification schemes are a mature and widespread solution.

W Weaknesses:

- labour-intensive and time-consuming for the entity undergoing the assessment due to the need to develop many formal documents and detailed technical documentation, as well as the use of complex testing procedures by the laboratory, which affects the high cost of the assessment;
- time-consuming development of new schemes, resulting from the need to coordinate them through technical committees (or other forums) and the vested interests of standards organisations (ISO/IEC, CEN-CELEC, ENISA), national, business or other delegating members to these bodies.

28 The call for the creation of a national cyber security certification scheme was included in the draft amendment to the Act on the National Cyber Security System (UKSC). https://orka.sejm.gov.pl/Druki9ka.nsf/0/C974DE0E6799563DC12589E40030360D/%24File/3457.pdf

29 https://commoncriteriaportal.org/cc/ — accessed 23 August 2023

Opportunities:

- simplification of existing certification schemes, e.g. the Common Criteria, by reducing the criteria to a minimum that ensures fixed-time testing and certification, i.e. the so-called lightweight certification schemes — a proposal in this respect has already been submitted in the form of European Standard EN 17640;
- electricity meters must comply with the requirements of the Regulation of the Minister of Climate and Environment of 22 March 2022 on the Metering System[30] and must be periodically verified by accredited testing laboratories;
- if the cost of certification according to lightweight certification schemes is not excessively high and the testing time is limited, meter certification provisions can be introduced through the new Act on the National Cyber Security System (UKSC), under the National Cyber Security Certification System;
- creating a competitive advantage for certified European and Polish products in countries that are concerned about the lack of verification of security aspects in products supplied even by major foreign suppliers;
- growing awareness of the risks facing the smart meter supply chain and the electric power system.

Threats:

- high assessment costs will have to be included in the price of the meter, which may increase the cost of implementing Automatic Meter Reading solutions, as well as the overall transition costs;
- some vendors may withdraw from the market;
- reducing Poland's attractiveness for both European vendors and non-EU players;
- introducing legislation with an appropriate vacatio legis, which in practice means implementing the scheme over a long time — in practice, at or after the end of the planned roll-out of remote reading meters;
- whenever a change is made to the software or hardware, the certification procedure must be repeated.

6.2. Introduction of legislation to regulate or exclude High-Risk Vendors from the smart meter market

High-Risk Vendors are entities whose products, services or processes used in critical industries may pose economic, intelligence and terrorist threats to national security. In Poland, such a category of vendors is provided for by the provisions of the draft act amending the Act on the National Cyber Security System and Certain Other Acts[31]. Providers of ICT products, services or processes may be considered High-Risk Vendors if those ICT products, services or processes are used by such entities as key service operators and critical infrastructure operators. Before an entity is declared a High-Risk Vendor, a multi-criteria assessment is made taking into account the following, among other things:

- the likelihood that a hardware or software vendor is under the control of a country outside the territory of the European Union or the North Atlantic Treaty Organisation;
- the number and types of detected vulnerabilities and incidents relating to the types of ICT products, services or processes provided by the hardware or software vendor, and how and when they were addressed;
- the manner and extent to which the hardware or software vendor oversees the hardware or software manufacturing and supply process.

Being designated as a High-Risk Vendor results in the inability to put into use the specific ICT products, services and processes listed in the decision on such designation. Further, the users of such CT products, services and processes covered by the decision must decommission them.
Other EU countries as well as the US and the UK also have similar regulations, though not as restrictive.

30 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000788 — accessed 24 August 2023
31 https://orka.sejm.gov.pl/Druki9ka.nsf/0/C974DE0E6799563DC12589E40030360D/%24File/3457.pdf

S Strengths:

- increasing national security and consumer safety — the state eliminates potentially dangerous or defective products from the market (High-Risk Vendors abandon their plans to expand on the Polish market);
- gaining political leverage against other countries, which can lead to improved standards and practices in their operations;
- legislative nature — firmly established in law and able to be introduced relatively quickly.

W Weaknesses:

- relatively higher costs required to manufacture products in Europe compared to High-Risk Vendors, which may lead to higher prices for DSOs and residential customers;
- potential enforcement issues — prolonged legal cases may occur, de facto suspending the application of the new regulations;
- requiring a separate authority to assess the safety impact of High-Risk Vendor and the need for the staff of such an authority to acquire the necessary competencies, or burdening the existing authorities with excessive workload;
- possible retaliation by host countries of excluded High-Risk Vendors against Polish entities; exclusion of High-Risk Vendors may cause diplomatic tensions or lead to a loss of potential trading partners;
- possibility of High-Risk Vendors taking legal action, which could lead to paralysis of DSO purchasing processes and problems across the sector.

O Opportunities:

- increasing demand for European products, which can help stimulate the European economy, effectively boosting employment, creating new jobs and strengthening European companies (both manufacturers and their many local suppliers and collaborators);
- developing local businesses whose operations focus on supply and production, which can support the national economy and increase the national technological sovereignty;
- boosting the scale of operations and income of local producers, resulting in increased taxes paid to the state budget;
- research advancements in the development and implementation of national AMI solutions (devices);
- developing technological competencies and increasing the level of innovation in European and national R&D centres run by local manufacturers.

T Threats:

- restricting access to High-Risk Vendors can lead to temporary shortages of products on the domestic market and an increase in their prices, or even the emergence of a grey market for recertified products;
- potential diplomatic conflicts (political and commercial) with High-Risk Vendor countries, which may affect other areas of cooperation;
- reducing the range of products on the market that meet DSO requirements;
- restricting competition, which may result in reduced innovation in the smart meter market;
- the emergence of a "grey area" of companies circumventing the ban — formally compliant but actually still under High-Risk Vendor control;
- temporary problems with equipment and component availability until domestic suppliers increase capacity or find alternative supply sources that meet the new requirements.

6.3. Mutual DSO arrangements on AMI component security

The assumption is that the DSOs would assess the mutual impact of an infrastructure disruption as a result of an attack on the supply chain as high and jointly decide to mitigate this risk through mutual arrangements on a specific issue, i.e. the security of the AMI components.

S Strengths:

- the arrangement would enable DSOs to share experience, knowledge and best practices related to component security, making them functional and secure by allowing operators to focus more resources on analysing threats and implementing security measures;
- enabling the possibility of developing common safety standards or rules for the procurement of advanced metering infrastructure components;
- non-regulatory nature — the lack of regulation can encourage joint initiatives;
- fewer actors requiring consultation, which encourages joint decisions/proposals.

W Weaknesses:

- different requirements and needs can lead to a compromise that would reduce security to the lowest level acceptable by each party;
- conflicts of interest between DSOs affecting the content of the arrangement — difficulties in work coordination;
- no possibility of verifying compliance with the arrangement;
- unsanctioned nature — the voluntary nature of the arrangement may lead to waivers resulting from management decisions motivated, e.g. by economic factors.

O Opportunities:

- enabling co-funded research cooperation, e.g. laboratories that would be able to work towards improving national security and consumer safety thanks to the newly provided funding;
- entering into a sectoral arrangement as an expression of shared interests;
- enabling the possibility of setting up other structures more quickly and easily, e.g. ISAC (Information Sharing and Analysis Cell), PSIRT (Product Security Incidents Response Team) or building a Competency Centre.

T Threats:

- long decision-making process and frequent changes in the governing bodies of individual DSOs, which may represent different interests;
- varying levels of DSO involvement, and sometimes a paralysing lack thereof;
- competition between DSOs can result in decreased trust and a limited flow of complete, authentic information regarding the security of AMI components;
- leaving the security of AMI components to the DSOs may discourage state authorities from taking responsibility for security issues, resulting in their relying solely on the DSO arrangement and hoping for its effectiveness;
- DSOs' focus on economic aspects — lack of interest in enhancing the security of AMI components.

6.4. Introducing the principle of mandatory split of tendered equipment between different vendors

Introducing the principle of a mandatory split of tendered equipment between European and non-European manufacturers, e.g. on a 50/50 basis (50% European/50% non-European equipment) or otherwise (whether through legislation or a binding DSO arrangement).

S Strengths:

- reducing High-Risk Vendor's market share without being accused of eliminating competition;
- no risk of destabilising the market (no risk of shortages);
- more acceptable to the market and High-Risk Vendors;
- reducing the impact of a potential cyber attack on the supply chain regardless of the vendor.

W Weaknesses:

- complicating procurement procedures by increasing the administrative burden on contracting authorities;
- requiring purchasing procedures to be carried out in compliance with quotas may risk reducing the importance of other criteria, such as safety and quality of products and services, in favour of the vendor's country of origin;
- difficulties in verifying compliance with the requirements (relying on contractor statements is not a sufficient condition) and the need to introduce means to verify the vendor's statements in this regard;
- difficulties in monitoring and enforcing the quotas;
- issues related to defining the product's country of origin.

O Opportunities:

- reducing reliance on non-European vendors, which can help minimise the risk of disruption to equipment supply chains;
- greater resilience of the given country in the event of an international political or trade crisis or other unpredictable situations if it has its own production facilities;
- boosting production in Europe and Poland, which can increase employment and strengthen local companies;
- stimulating development and investment for Polish companies, increasing their chances to sell their products and services;
- "blazing a trail" and a positive example of proactive safety measures that can also be implemented in other sectors and industries where High-Risk Vendors are prevalent.

T Threats:

- High-Risk Vendor countries establishing or taking over entities that meet the national requirements but in fact offer High-Risk Vendor solutions;
- entities of Polish or European origin importing solutions purchased from High-Risk Vendors and then rebranding and offering them as products of Polish or European origin;
- reducing the price or quality competitiveness of products available to DSOs in Poland and Europe;
- limiting access to more innovative or attractive products that do not meet the country of origin criterion;
- risking an uptick in production costs in some cases, which may increase prices for customers and limit their choice;
- risking political or trade disputes with other countries and limiting the potential for global cooperation.

6.5. Developing methodologies and tools for testing security requirements

The smart metering industry is growing rapidly and ensuring the safety and reliability of smart metering equipment is becoming increasingly important. This is reflected by the safety requirements it has developed. Developed by different organisations and included in various documents, these requirements take the form of guidelines, recommendations and even regulations. However, there is a lack of standardised methodology and tools for testing remote reading meters. There is also no widely accepted and publicly accessible test environment.

S Strengths:

- consistency — applicable to all vendors and the products they offer;
- objectivity — standardisation of tests.

W Weaknesses:

- difficult to agree upon;
- costs when commercial tools are used in a test environment.

O Opportunities:

- possible use in certification schemes — allowing the results to be related to ready-made certification schemes and making certification possible;
- possible use by multiple centres, laboratories and by the DSOs themselves;
- filling an obvious gap in AMI security assurance;
- enabling the possibility of using open-source tools;
- enabling the possibility for vendors to independently verify that the security criteria of the smart meters they offer are met by the DSO.

T Threats:

- difficulties in coming to an agreement and the unknown manner of the methodology's introduction (Who is supposed to introduce it and on what terms?);
- challenging the test results in the event of an independent assessment by the DSO.

6.6. Introduction of strict regulations defining vendor responsibility for securing the supply chain

The vendor winning the purchasing procedure would have to provide a deposit or other security to guarantee that its product will remain free of supply chain risks for the duration of the contract. The deposit would be held by a public trust institution or a national bank, e.g. Bank Gospodarstwa Krajowego, and returned on the expiry of the contract or used to cover the cost of removing the consequences of a supply chain attack.

S Strengths:

- introducing strict regulation will increase the security of energy networks by minimising the risk of potential cyber-attacks;
- requiring safe and reliable smart meters would stimulate innovation in the energy sector;
- vendor product liability — the potential loss of the deposit is bound to encourage vendors to maintain strict quality and safety standards;
- simplicity — the deposit mechanism is easy to understand and implement;
- increased public confidence in the sector and the state.

W Weaknesses:

- difficulties in determining the deposit amount;
- long meter life, forcing the vendor to wait a long time for the deposit to be returned,
- depreciation of the deposit over time — it may be insufficient to cover the cost of repairing potential faults;
- additional costs for the vendors, which may be passed on to DSOs in meter sales and, subsequently, to customers through higher charges;
- significant resources on the part of both vendors and regulators/state authorities that would be required to manage the deposits.

O Opportunities:

- withdrawal of some vendors from participating in tenders due to the high risk of sanctions for failure to meet the high product safety standards;
- development of new technological solutions to enhance the security of grids and smart devices.

T Threats:

- resistance from vendors, both High-Risk Vendors and others, who may oppose such a solution;
- the detrimental impact of high participation costs on the liquidity of some entities — tenderers may find freezing significant sums of money for many years unacceptable;
- tenders becoming dominated by vendors with substantial equity and effective elimination from the market of vendors who cannot afford to pay the deposits;
- admitting entities sponsored by hostile states, which do not care about profit but about gaining market position;
- stifling the growth of smaller smart metering companies that would be unable to pay the deposits.

6.7. Amendments to the Public Procurement Law

Legal amendments may also apply to other provisions, e.g. the Act on Crisis Management (Dz.U. /Journal of Laws/ of 2007 No. 89, item 590) or the Act on the National Cyber Security System (Dz.U. /Journal of Laws/ of 2018, item 1560, hereinafter: "UKSC").
Potential amendments to the current laws and regulations could aim to add provisions on the need for AMI vendors to have an ISO/IEC 27001-compliant Information Security Management System (hereinafter: "ISMS") covering the smart meter manufacturing process. The ISMS compliance audit should be carried out by an entity accredited by the PCA in the OECD or EU area.

S Strengths:

- increased confidence in the meter manufacturers, as well as in the product itself;
- a fast-track legislative route as a result of the amendments to the UKSC that need to be made in relation to the implementation of the NIS2 Directive, which requires member states to regulate supply chain issues, including in the energy sector;
- legislative nature — firmly established in law;
- consistency and objectivity — the regulations would be applicable to all vendors and the products they offer;
- circumvention or non-compliance would be sanctioned under the law, making it impossible to avoid punishment for failure to apply the new legal requirements;
- basing the legislation and its implementation on EU law, which enjoys greater authority in the national and international arena.

W Weaknesses:

- difficulties in defining the overall production process and taking into account both physical meter components and software issues;
- no technical verification of the product — the compliance assessment would be based mostly on the risk analysis process and the mechanisms applied to minimise the risks identified;
- a lack of proper identification of the actual manufacturer and production site, e.g. the share of components supplied by the vendor's sub-suppliers, and thus the correct entity to be audited.

O Opportunities:

- limiting the participation in tenders of entities that do not ensure adequate product safety requirements;
- proliferation of Information Security Management Systems across an increasing number of entities;
- increasing the awareness and safety of the production process in general among businesses and individuals alike.

T Threats:

- lengthening the supply chain in a way that makes it difficult and expensive to reach and audit the real manufacturer;
- difficulty for manufacturers to comply since some of their sub-suppliers will be unwilling to conform to such requirements (e.g. processor vendors);
- no real possibility of assessing the effectiveness of the subcontractor verification process.

6.8. Recommendations by the Government Plenipotentiary for Cyber Security on High-Risk Vendors in the area of smart energy meters

The current Act on the National Cyber Security System allows the Government Plenipotentiary for Cyber Security to make recommendations on the use of IT devices or software, particularly with regard to the impact on public safety or a vital national security interest. Guided by the vital interest of state security, the Plenipotentiary may issue a recommendation to DSOs in the form of a warning against a cyber security threat involving the use in Poland of advanced metering equipment hardware or software originating from outside the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development or the North Atlantic Treaty Organisation.

S Strengths:

- the recommendations require no complicated and lengthy legislative process but are nonetheless firmly established in statutory provisions;
- increased confidence in the meter manufacturers, as well as in the product itself;
- supporting meter manufacturers from the territory of the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development or the North Atlantic Treaty Organisation;
- reducing/eliminating High-Risk Vendors' market share;
- supporting national technological solutions, as well as those offered by allied states.

W Weaknesses:

- no sanctions for disregarding the recommendations — where a potential shortage of vendors in the market may occur due to exclusion based on the recommendations, DSOs may seek to avoid applying them;
- the recommendations must be reviewed by the Cyber Security College, which may find it difficult to issue a consistent position;
- no deadline is specified for the College to issue its opinion, and as such, the College may take a long time to do so.

O Opportunities:

- greater awareness of the risks to the smart meter supply chain;
- introducing similar recommendations in other countries of the European Union, the European Economic Area, the Organisation for Economic Cooperation and Development and the North Atlantic Treaty Organisation (such recommendations are already in place, e.g. in the Czech Republic);
- reducing reliance on High-Risk Vendors;
- stimulating the domestic market, resulting in greater technological sovereignty and self-sufficiency;
- improving the economic situation by increasing domestic production and providing jobs.

T Threats:

- excluding High-Risk Vendors carries the risk of limiting the availability of AMI components and, as a result, the risk of problems in ensuring a stable energy supply;
- identifying High-Risk Vendors and implementing recommendations can lead to delays in energy-related investment projects;
- entities of Polish or European origin importing solutions purchased from High-Risk Vendors and then rebranding and offering them as products of Polish or European origin;
- risking political or trade disputes with other countries and limiting the potential for global cooperation;
- recommendations would require regular updates due to the rapidly evolving cyber security environment.

7. RECOMMENDED ACTIONS FOR SUPPLY CHAIN RISK MINIMISATION

As indicated in Chapter 5, an attack on the smart meter supply chain poses the greatest risk to the stability of the NES. For this attack vector, current protection measures are the weakest and the potential consequences the highest. Chapter 6 of this paper outlines some measures to minimise the risk of adverse cyber-security impacts on advanced metering infrastructure through the supply chain. Nonetheless, as shown by the SWOT analysis in that chapter, there is no single measure that would be superior to the others and exclusively applicable to ensure the safe use of energy system metering infrastructure. The NIS2 Directive, which should be implemented by EU countries by October 2024 (in Poland, this will most likely happen through an amendment to the Act on the National Cyber Security System[32]), requires all entities subject to its provisions,[33] i.e. DSOs, to ensure supply chain security.

To ensure the stability of the NES until the NIS2 Directive is implemented, the following measures are recommended to minimise the risks associated with the advanced metering infrastructure supply chain.

7.1. Near-term perspective

7.1.1. Amendment to the Act on the National Cyber Security System (UKSC)

Proposals for AMI legislation should be tabled as part of the current legislative process to amend the UKSC. The new UKSC, in addition to the existing arrangements (requiring each key service operator to have an ISMS in place), should include provisions establishing the following requirements:

- obliging producers of IT hardware and software that will be used in critical social or economic activities, thus also in the electric power industry, including that incorporated into advanced metering structures, to have an ISMS;
- obliging the above entities to comply with all the requirements detailed in (a) to (l) below, which would prevent them from being excluded from the scope of the ISMS;
- establishing a requirement concerning UKSC compliance audits to be carried out by accredited certification bodies or cyber security services organisations (except where a conflict of interest exists, e.g. where such an entity provides SOC or CERT services).

IT product security is derived from the organisational, personal, physical and technical security of the manufacturer and its vendors (e.g. supplying software or hardware components). Besides the generally known aspects of information security (IT system hardening, access control, network security, transmission encryption, etc.), those that directly affect the development, execution and operation of security features in the target IT product are also extremely important. These include:

a) Developing a secure system architecture and applying the relevant engineering principles;
b) Applying a secure software development cycle;
c) Considering the application's security requirements;
d) Secure software development;
e) Development and acceptance phase security tests;

32 The draft act amending the Act on the National Cyber Security System and Certain Other Acts is currently being processed. https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=3457
33 Art. 21(2)(d) — supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

f) Outsourcing software development while maintaining security;
g) Separating development, test and production environments;
h) Using Cyber Threat Intelligence;
i) Integrating information security into project management;
j) Ensuring information security in vendor relations;
k) Information security management in the ICT supply chain;
l) Monitoring, reviewing and managing changes to vendor services.

The new ISO/IEC 27001:2022 (requirements) and ISO/IEC 27002:2022 (recommendations) standards contain many requirements and recommendations that cover all of the above aspects. It is thus essential that all organisations involved in the smart meter production process implement an ISMS that complies with these standards.

7.1.2. Recommendations of the Government Plenipotentiary for Cyber Security

The current Act on the National Cyber Security System allows the Government Plenipotentiary for Cyber Security to make recommendations on the use of IT devices or software, particularly with regard to the impact on public safety or a vital national security interest. Guided by the vital interests of state security, the Plenipotentiary may make the following recommendation:

"Following the opinion of ... issued by the Cyber Security College, I recommend that National Cyber Security System entities avoid using in the energy systems any hardware or software not originating from the countries of the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development or the North Atlantic Alliance to implement technologies compliant with category B1 and C1 direct measurement level as per the Regulation of the Minister of Climate and Environment of 22 March 2022 on the Metering System (Dz.U./Journal of Laws/ of 2022 Item 788); this is due to possible cyber security vulnerabilities in such hardware or software."

The proposal is based on a solution used in the Czech Republic to limit High-Risk Vendor expansion in the market. It involved issuing a cyber threat warning on the use of hardware or software from outside the European Union, the European Economic Area, the Organisation for Economic Co-operation and Development or the North Atlantic Alliance to implement technologies that enable the required level of direct measurement, i.e. B, C1, C2 or C3, as per the Czech electricity metering regulations. The warning was published by the Czech National Cyber and Information Security Agency. As per the information available at https://www.nukib.cz/en/, the Agency is responsible for various aspects of security of both classified and public information in ICT systems, cyber security (it runs a CERT team for state bodies and critical infrastructure). Poland has no single equivalent body since these competencies in Poland are divided between the Internal Security Agency's ICT Security Department and CERT, the Ministry of Digital Affairs and CERT NASK. Accordingly, given the strong mandate of the Government Plenipotentiary for Cyber Security and its powers in the legislation, it appears to be the best entity to make such recommendations.
This would not set a precedent either. In the past, the Government Plenipotentiary for Cyber Security issued a recommendation not to use software produced by Moscow-based Kaspersky Lab in information systems.[34] The legal basis for making such recommendations is Article 33(4) of the UKSC and the substantive basis is the opinion of the Cyber Security College referred to in Article 64 of the UKSC. Most importantly, however, in the context of supply chain security, this would directly impact the procurement processes carried out by DSOs. Article 226(1)(17) of the PPL states that the Contracting Authority must reject a bid if it includes IT hardware or software indicated in

34 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-oprogramowania-kaspersky — accessed 23 August 2023

the recommendation referred to in Article 33(4) of the Act of 5 July 2018 on the National Cyber Security System, stating their negative impact on public security or national security. The recommendation proposed in this chapter fulfils this condition.

7.2 Long-term perspective

A long-term solution (not yet practically available in Poland) for ensuring the cyber-security of smart meters could be their certification based on so-called lightweight certification schemes. The idea of introducing such schemes is linked to the European Cyber Security Act[35] (hereafter CSA), which introduces three assurance levels in ICT services, products and processes:

Basic

- the subject of the assessment minimises the known basic risks of incidents and cyberattacks;
- the assessment attestation is issued either by an accredited conformity assessment body (in the form of a certificate) or based on a self-assessment by the manufacturer or vendor, in the form of a declaration of conformity;

Substantial

- the subject of the assessment minimises the known basic risks of incidents and cyberattacks and the risk of incidents and cyberattacks carried out by actors with limited skills and resources;
- the attestation (certificate) that the subject of the assessment has been assessed to meet cyber security requirements is issued by an accredited conformity assessment body;

High

- the subject of the assessment minimises the risks of state-of-the-art cyberattacks carried out by actors with significant skills and resources;
- the attestation (certificate) that the subject of the assessment has been assessed to meet cyber security requirements is issued by an accredited conformity assessment body, either a public entity or a private entity to which the task has been delegated: in both cases, these bodies are additionally authorised by the national supervisory authority for cyber security certification[36].

35 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Cyber-Security Agency) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

36 The latest draft amendment to the UKSC includes a new Art. 59b with the following proposal: "The government administration body responsible for cyber security certification shall be the minister responsible for information technology."

"Lightweight" cyber security assessment schemes began to be implemented in several European countries, including France, the Netherlands, Spain and Germany, leading to the development of European Standard EN 17640[37] as their generalisation. This standard is a considerable simplification of the Common Criteria and CEM methodology and can be used in programmes where limited resources and time to perform the study are key factors.

Table 2 lists the recommended and required tasks for the assessment of an IT product according to the manufacturer's declared assurance level.

		CSA declaration of conformity		
Assessment purpose	**Reference**	**Basic**	**Substantial**	**High**
Completeness check	6.1	Required	Required	Required
Security functions review	6.3	Required		
FIT Security Target assessment	6.4		Required	Required
Project documentation assessment	6.5	Required	Required	Required
TOE assessment	6.6	Recommended	Required	Required
Conformity testing	6.7	Recommended	Required	Required
Security vulnerability review	6.8	Recommended	Required (or executed in 6.9)	
Vulnerability testing	6.9		Recommended	
Penetration testing	6.10			Required
Basic cryptanalysis	6.11	Recommended	Recommended	
Expanded cryptanalysis	6.12			Required

Table 2 — Assessment tasks vs. CSA declaration of conformity

37 EN 17640:2022 Fixed-Time Cybersecurity Evaluation Methodology for ICT Products

Similar to Common Criteria testing, the manufacturer must create a Security Target document in accordance with EN 17640.[38] See Annex A of the standard for the model form and content.

Notably, the Introduction section of EN 17640 makes it clear that the standard cannot be used on its own. Each domain (certification programme) must provide domain-specific cyber security requirements formalised in technical specifications for the products to be assessed and certified. Thus, the methodology described in EN 17640 is intended to be used in conjunction with technical specifications containing cyber security requirements. This is illustrated in Figure 1.

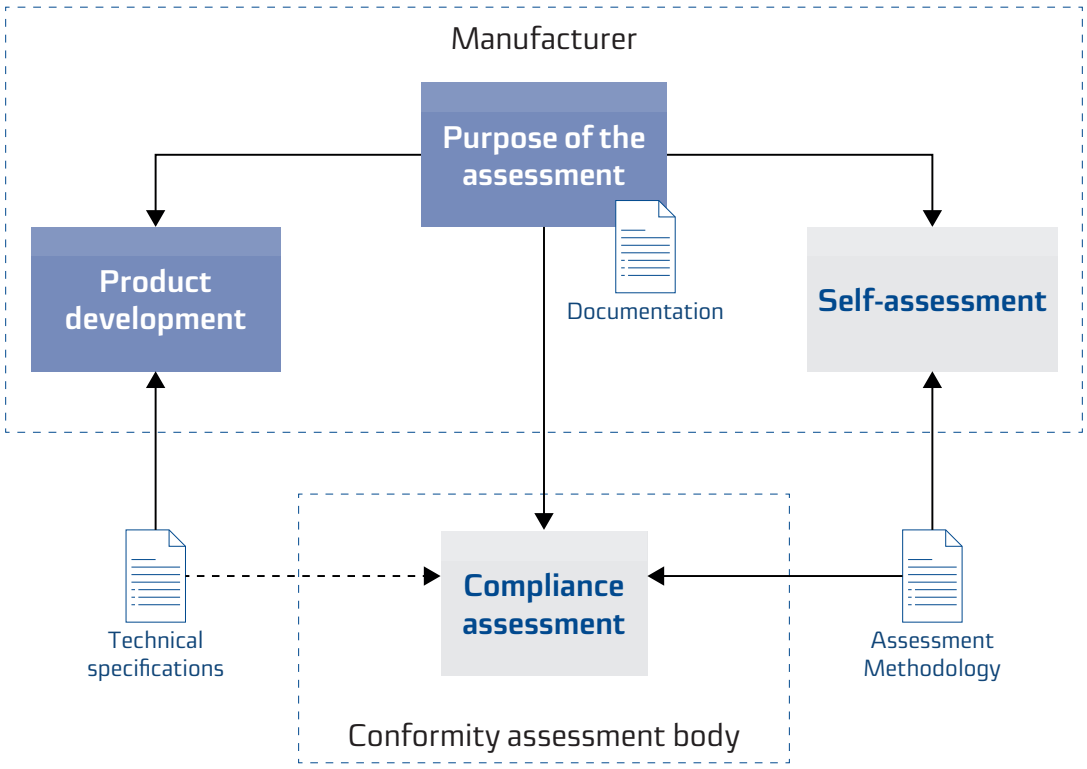

Figure 1 — Product conformity assessment activities under EN 17640

The following issues will need to be addressed in the future (possibly in the relevant legislation):

- At what level of detail should technical specifications be developed for the different types of IT products that can or should be certified based on EN 17640?
- Should such a technical specification for smart meters be Annex 1 to the Regulation of the Minister of Climate and Environment of 22 March 2022 on the Metering System or rather a set of requirements developed at the European level?
- What CSA level certificate (Basic, Substantial, High) should a smart meter manufacturer apply for? The higher the level, the more effective the High-Risk Vendor restriction, but also the greater the restrictions on manufacturers intending to have their devices certified.

38 While there is no suitable translation of this term into Polish, we propose "Specyfikacja zabezpieczeń" (Security specification) as a possible option.

Poland currently has no accredited laboratories for carrying out assessments according to EN 17649. The existing accredited laboratories and certification body carrying out Common Criteria-based assessments could expand their scope of activities, but this must also be done by the PCA within the scope of their accreditation. Although there is news about lightweight certification programmes in Germany, Spain, France and the Netherlands, the authors found no information about such an accredited laboratory in the EU. The matter is likely being held up by ENISA's unfinished work on a suitable European certification scheme. The website https://certification.enisa.europa.eu/ mentions three agreed-upon schemes (for Common Criteria, cloud services and 5G), but none for EN 17640.

In summary, based on the CSA and EN 17640, applying the Common Criteria is not necessary for the testing and certification of devices such as smart meters. The basis can be European Standard EN 17640, which defines what is to be provided by the manufacturer and what the activities of the testing laboratories are to be. However, it is necessary to outline what will serve as an additional technical specification and define the implementation of formal steps — the accreditation of laboratories and certification bodies — which determines this solution's long-term feasibility.

8. CALL FOR ACTION TO IMPROVE CYBER SECURITY IN THE ENERGY SECTOR

With rapid technological development and ever-increasing electricity demand, the energy sector is undergoing significant changes that bring with them many benefits, as well as new challenges and threats. These challenges and threats arise not only from technological developments but also from the current geopolitical situation.

One technological advancement and a symbol of the changes in electricity sector management is smart meters, which offer undeniable benefits in terms of more efficient management, ongoing monitoring of consumption and sustainable use. However, there is concern related to possible insufficient security measures installed in these meters or their components by their manufacturers or High-Risk Vendors, which carries many risks, as discussed earlier in this document. **Hacking attacks, backdoors or logic bombs can compromise citizens' privacy and destabilise the entire power grid.**

The introduction of 5G technology has drawn widespread attention to the issue of technological sovereignty and the real dangers of failing to recognise its importance or focusing solely on the economic aspect of technologies deployed in Western countries. We cannot afford to neglect cyber security since improvements in this area in the energy sector are not just about protecting the interests of our citizens but also about guaranteeing the stability of Poland's critical infrastructure.

Cyber security cannot be guaranteed without properly and institutionally assured supply chain security. The state must have appropriate, effective legal and technical instruments, not only in the electricity sector but across the entire economy and citizens' lives, with particularly strengthened resilience in the public sector and critical infrastructure. As such, this expert opinion calls for the necessary, expected, reasonable and effective measures to ensure a safe, modern and sustainable future.

GLOSSARY

AMI	Advanced Metering Infrastructure
Backdoor	— a system security vulnerability created deliberately for later use to gain unauthorised access
Logic bomb	Malware that launches when certain conditions are met (e.g. on a certain date, when a specific user logs in or after a set number of software launches)
CERT	Computer Emergency Response Team
CSA	Cyber Security Act
Common Criteria - ISO/IEC 15408:2022	A standard to formally verify the security of ICT systems
EN 17640	A document describing a methodology for assessing the cyber security of ICT systems that can be implemented using predefined time and load resources
ENISA	The European Union Agency for Cybersecurity
EEA	European Economic Area
Hardening	The reconfiguration of ICT systems to enhance their security
ISO/IEC 27001	An international standard for Information Security Management Systems
NES	National Electricity System
AMR	Automatic Meter Reading
Man-in-the-Middle	An ICT attack that involves eavesdropping on and modifying messages sent between two parties without their knowledge
NIS2	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union
OECD	Organisation for Economic Co-operation and Development
DSO	Distribution System Operators
PCA	Polish Centre for Accreditation
SOC	Security Operations Center
ISMS	Information Security Management System
UKSC	Act on the National Cyber Security System
ERO	Energy Regulatory Office

Prepared by:

ComCERT SA
ul. Adama Branickiego 13
02-972 Warsaw

Apator SA
ul. Gdańska 4a lok. C4
87-100 Toruń
e-mail: rzecznik.prasowy@apator.com
www.apator.com

2023.133.EN