WIEDZA OBRONNA
2023, Vol. 283 No. 2
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2023-j285

GRZEGORZ PILARSKI *
Akademia Sztuki Wojennej, Warszawa, Polska

JACEK MICHALIK *
Warszawa, Polska

MARCIN WYSZYŃSKI *
Warszawa, Polska

ANALYSIS OF SELECTED CONTEMPORARY THREATS TO GAS INFRASTRUCTURE

ABSTRACT: Nowadays, companies are increasingly using a risk-based approach to achieve their business goals. A key element of this approach is the identification of threats that may materialize and affect the functioning of the company. Following the example of the gas sector, with the gas infrastructure as the subject of research, the authors presented selected contemporary gas network threats that may occur within the mentioned sector.

KEYWORDS: critical infrastructure, gas infrastructure, energy industry, national security,

INTRODUCTION

Analysis of the threats that may affect a country's distribution network is a key issue from the perspective of energy security. Threats, which can be categorized as natural, technical, terrorist and military, can affect the operational security of the gas infrastructure and the continuity and security of gas fuel supply. In order to develop appropriate methods to protect the distribution network, it is necessary to realize what threats it is exposed to. It is also

* **płk dr hab. inż. Grzegorz Pilarski,** War Studies University, Warsaw, Poland
https://orcid.org/0000-0001-9728-2611 g.pilarski@akademia.mil.pl
* **Jacek Michalik,** Warsaw, Poland
* **Marcin Wyszyński,** Warsaw, Poland

important that the negative consequences of the threats and the lack of continuity of gas fuel supply last as short as possible.

Taking into consideration the aforementioned issues, the main purpose of this article is to analyze the construction of gas infrastructure and the threats to the gas network that may occur within the energy sector. The authors formulated the research problem in the form of the following question: what threats to the gas network can affect the disruption of continuous and secure supply of gaseous fuel?

The authors put forward the following research hypothesis: natural, technical, terrorist threats, dependent and independent of the actions of the Distribution System Operator (DSO) have a significant impact on the security of gas fuel supply. Critical threats to the distribution network include: decapitalization of network assets, corrosion, human error and construction work near the DSO's infrastructure as well as terrorist threats (cyber attack).

The research methods applied in the research process included literature analysis, analysis of Internet sources, analysis of industry documentation, and empirical analysis in the form of a diagnostic survey.

In Poland, the Distribution System Operator's (DSO) obligation to ensure continuous and safe supply of gaseous fuel stems from legal provisions imposed by the Law of April 10, 1997. - Energy Law (Section 9 c - Duties of system operators).

Meeting the obligations imposed on DSOs is fraught with high risk, in view of the volatility, uncertainty, complexity and ambiguity of occurring events, technological developments, legislative considerations (e.g., arising from environmental protection packages) and growing expectations of end users. In the subject literature describing the above determinants of the surrounding world, an interesting concept is VUCA[1], which allows to describe the environment of an organization characterized by rapid changes in a very short time.

Recent years bringing dynamic changes in the environment (VUCA) make it necessary to expand the approach to the operation of the gas network through, among other things, cyclical analysis of risks to develop a package of preventive and reactive methods, adequate to the level and severity of risks affecting the security of gas fuel supply.

---

[1] VUCA is an acronym based on the leadership theories of Warren Bennis and Burt Nanus (book: *Leaders: The strategies for taking charge*. New York: Harper & Row,1985), to describe or to reflect on the volatility, uncertainty, complexity and ambiguity of general conditions and situations. Initially, the term was used by the US Army War College to describe the world under Cold War conditions. Today, this concept of strategic leadership is widely used in many organizations.

The information, analysis and proposals for action contained in this article are intended to fulfill a supportive role for managers (DSOs) in the VUCA era. Today's working environment for managers involves a number of challenges, for it is work under conditions of:

- volatility, i.e. rapid pace, often surprising changes in regulations, rising prices of materials and services or labor costs, required quick decisions and, following that, adequate actions;
- uncertainty, i.e. operating in a reality that is difficult to predict, requiring the use of risk analysis as one of the basic tools for assessing possible risks and evaluating their effects, and thus for building remedial or corrective actions;
- complexity, resulting from the multiplicity of factors, the possibility of simultaneity, the multiplicity of regulations, instructions and information, and therefore the need to take into account many factors, analyze and synthesize information for a quick decision when the situation requires it;
- ambiguity, i.e. the lack of unambiguous solutions, a situation where multiple methods can be applied and there is no clear answer as to which method/solution should be used, and therefore the need to apply risk management, prepare various scenarios for the materialization of risks, and use this knowledge to select the optimal method of operation.

Adopting a research procedure based on an approach linking theory and practice, the authors recognize to what extent the contemporary solutions embodied in procedures, instructions, and good gas practices are sufficient to carry out effective operator activities in times of dynamic change as well as examine to what extent the new approach based on hazard analysis and risk assessment will support effective management of the distribution network.

ESSENTIAL COMPONENTS OF A GAS SYSTEM

The supply of gaseous fuel to end users is carried out by a number of interconnected and cooperating but separate (in terms of ownership and function) systems that make up the national gas system. Along with oil and coal, natural gas is one of the three most essential types of fossil fuel for the current economy. Natural gas is of fundamental importance to national economies, industry, local communities, and households. Natural gas is used to generate electricity and is widely used in heavy industry, chemicals, food, transportation, services, commerce, and other industries. Domestic natural gas is primarily used for space heating, cooking, hot water, and air conditioning.

There are two main sources through which natural gas is brought to the domestic market. The first is extraction from domestic fossil seams. The second source of obtaining natural gas is importing it from abroad. Gas can also enter the system through underground gas storage facilities, LNG regasification stations, and denitrification plants. Another source, the importance of which may change in the near future, are biogas plants that convert biomass into biogas, which, after refinement, can be fed into the gas system. The extraction of gas, its sale, and its transmission to customers, requires the performance of many different activities. Therefore, we can divide the entire gas supply chain by the tasks performed into:

- mine system;
- transmission system;
- storage system;
- distribution system;
- other gas systems.

The mine system includes all the technological systems, together with the field pipelines, necessary for the extraction of gas, its transportation to the place of purification and treatment, and its metering and transfer to the cooperating system. One or more Natural Gas Mines may operate within a single system, from which gas is received at a single delivery point. Mines systems cooperate with the transmission system, distribution system or direct pipelines (a gas pipeline built to directly deliver gaseous fuel to a customer's installation bypassing the transmission and distribution system).

The gas transmission system is a system of gas pipelines and process facilities used to transport gas from points of entry to the system/sources (e.g., Natural Gas Mines, Gas Import Points, Underground Gas Storage Plants, Denitrification Plants) to points of exit, i.e. places where gas is taken from the transmission system (e.g., to other systems, Denitrification Plants, Gas Export Points, Gas Mixing Plants, PMGs). The key task of this system is to transport gaseous fuels through the transmission network throughout the country for delivery to distribution networks and to end customers connected to the transmission system.

The storage system includes technological systems for the temporary storage of gas in Underground Gas Storage Facilities.

The gas distribution system includes gas pipelines and technological systems necessary for the collection of gas from the transmission system and delivery to the end user. The key task of this system is to transport gaseous fuels reliably and safely through the distribution network throughout the country directly to end users and the networks of other local operators.

The natural gas liquefaction system is a liquefied natural gas facility for liquefaction and the import, offloading and regasification of liquefied natural gas, together with auxiliary installations storage tanks[2].

In recent years, there have been significant organizational changes in the structure of the Polish natural gas market, resulting, among other things, from EU law, including mainly Directive 2003/55/EC of the European Parliament and of the Council of June 26, 2003 concerning common rules for the internal market in natural gas and repealing Directive 98/30/EC and Directive 2009/73/EC of the European Parliament and of the Council of July 13, 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC. Among other things, these directives necessitated the reorganization of the natural gas market, i.e. in particular the separation of transmission and distribution activities from trading activities[3]. The sale and purchase of gaseous fuels on the Polish wholesale market takes place primarily on the exchange market operated by the Polish Power Exchange (Towarowa Giełda Energii S.A.). Participants in the exchange market are mainly companies trading in gaseous fuels and the largest end-users, who may act independently after entering into an appropriate agreement with POLPX S.A., becoming members of the exchange, or through brokerage houses or through other entities with the status of an exchange member from their own capital group that may conclude transactions on behalf of other entities belonging to the same capital group[4].

The supply of gaseous fuel to customers may be carried out through the following types of transmission and distribution network connections:

a) source-distribution-consumer;
b) source-transmission-consumer;
c) source-transmission-distribution-consumer;

[2] A. Matkowski: *Vademecum Gazownika*….op. cit., p. 302.
[3] M. Kulesa, P. Rogóż, *Wybrane uwarunkowania liberalizacji sektora gazu w Polsce, https://www.cire.pl/pliki/2/Wybrane_uwarunkowania_liberalizacji_sektora_gazu_p.pdf* [access: 08.03.2023].
[4] Energy Regulatory Office, *Charakterystyka rynku paliw gazowych*, https://www.ure.gov.pl/pl/paliwa-gazowe/charakterystyka-rynku/9662,2020.html [access: 08.03.2023].

d) source-transfer-distribution1-distribution2-consumer;
e) source-distribution1-distribution2-consumer;
f) direct pipeline outside the gas system.

The transmission and distribution networks are supplied with Group E high-methane natural gas and Group L nitrogenous natural gas.

The gas network consists of the following elements: gas pipelines, gas connections, gas compressor stations, gas stations, gas units at the connection, LNG regasification stations, gas storage facilities with piping systems and other associated facilities[5].

Gas pipelines are divided according to[6]:

a) maximum operating pressure (MOP) into:
    - low-pressure gas pipelines up to and including 10.0 kPa;
    - medium pressure gas pipelines above 10.0 kPa up to and including 0.5 MPa;
    - increased medium pressure pipelines above 0.5 MPa up to and including 1.6 MPa;
    - high-pressure gas pipelines above 1.6 MPa.
b) materials used for:
    - steel gas pipelines;
    - PE polyethylene gas pipelines.

Gas stations are divided according to:

a) the maximum operating pressure (MOP) at the station entrance into:
    - medium pressure (for pressures up to and including 0.5 MPa);
    - increased medium pressure (for pressures above 0.5 MPa up to and including 1.6 MPa);
    - high pressure (for pressures greater than 1.6 MPa) .
b) the function performed in the system on:
    - reduction stations (reduction of gas pressure);
    - measuring stations (measurement of volume flow, mass or energy of gas);
    - reduction-measuring stations (a combination of the functions of a reduction and measuring station);

[5] Own elaboration based on: K. Bąkowski, Sieci i Instalacje Gazowe. Poradnik projektowania, budowy i eksploatacji, Wydawnictwo Naukowe PWN SA, Warszawa 2013.
[6] Rozporządzenie Ministra Gospodarki z dnia 26 kwietnia 2013 r. w sprawie warunków technicznych, jakim powinny odpowiadać sieci gazowe i ich usytuowanie. Dz.U.2013.0.640.

- distribution stations (usually with large capacities designed to control the volume of the stream and to measure it);
- treatment stations (which mainly performs the function of hydration of gaseous fuel).

Gas units at the connection are divided according to:

a) the maximum operating pressure (MOP) at the inlet at:
   - medium pressure (for pressures up to and including 0.5 MPa);
   - increased medium pressure (for pressures above 0.5 MPa up to and including 1.6 MPa).
b) the function performed in the system:
   - reducing (reduction of gas pressure);
   - measuring (measurement of volume flow, mass or energy of gaseous fuel);
   - reducing-measuring (combination of reducing and measuring functions).

In the gas industry, one can distinguish three types of gas network interconnection structure[7], for the transmission or distribution of natural gas in municipal areas:

a) tree structure - is an infrastructure that distributes natural gas locally on the territory of municipalities to end users. This system is fed from a single entry point to the system (gas station), which may be the exit point from the transmission system, distribution system, natural gas mine, or LNG regasification station;
b) ring structure - is a system of networks distributing natural gas locally within municipalities to end users, fed from several entry points to the system, hydraulically connected to each other by pipelines in the system. Such a system is characterized by two-way supply due to the possibility of gas flow from different directions in the system;
c) mixed structure - is a gas infrastructure, consisting of elements of a tree and ring structure.

According to the above description, the country's gas infrastructure is a complex system, which directly affects the scale of potential risks that can be identified.

IDENTIFICATION OF GAS INFRASTRUCTURE THREATS

[7] W. Grządzielski, T. Mróz, *Planowanie zrównoważonego rozwoju systemu gazowego*, KAPRINT, Lublin 2017, pp. 28-29.

When identifying risks, it is necessary to answer the question: what adverse events can affect the key infrastructure in the gas sector. This is important, because in order to develop appropriate methods to protect it, it is necessary to realize what the sources of these risks are. If the infrastructure is completely destroyed, damaged or its operation is disrupted, it can endanger the property or even the lives of citizens and lead to the malfunctioning of the state's economy. It is also important that any threats are detected as early as possible, and their negative consequences in the various systems last as short as possible, are easy to remove and do not cause additional losses to citizens and the economy[8].

In this part of the article, the authors have attempted to characterize the threats that can affect the security of operation of gas infrastructure. The catalog of risks (Table 1.) that can occur on the elements of the distribution network was determined on the basis of statistical and historical data and expert estimates. Consideration was given not only to the risks already occurring, but also to those whose occurrence is possible, taking into account the observed processes and geopolitical changes. In their considerations, the authors adopted the following division of threats to gas infrastructure: natural, technical, terrorist and military, and other.

Table 1.

Threats to gas infrastructure

Threats	
Natural hazards	Flooding
	Strong winds
	Tectonic movements
	Landslide
	Epidemic
	Fire
	Severe frost
	Intense snowfall
	Corrosion
Technical hazards	Decapitalization of assets
	Human error
	Construction work near infrastructure

[8] Kolano S., Identyfikacja zagrożeń krytycznej infrastruktury państwa, „Współczesne Problemy Zarządzania", Tom 6, Nr 1(12), 2018.

Terrorist and military threats	Military threats
	Threats of a terrorist nature
	Cyber attack
	Sabotage
Other threats	Disruption of the energy system
	Disruption of the supply of materials and services
	Disruption of the gas fuel supply chain
	Traffic incidents
	Action of state authorities
	Intra-organizational factors
	Financial
	Events in the international environment

Source: own elaboration.

Natural hazards are occurring in the natural environment and can trigger an emergency situation. They include:

1. Flooding.

   During a flood, a gas pipeline may be exposed or ruptured as a result of a strong flow of water, which may cause interruptions in the supply of gas fuel or a threat to health, property or life. In addition, water may penetrate gas pipelines or equipment, resulting in improper operation (e.g., gas regulators).

2. Strong wind.

   Strong winds can lead to disruptions in electricity supply. Lack of electricity supply may cause disruptions in the operation of some network components, e.g. gas stations (lack of gas heating, lack of operation of the telemetry system and automation system).

3. Tectonic movements.

   Earthquakes or bumps associated with the subsidence of mine workings can lead to stresses in the gas pipeline, resulting in its unsealing, which affects the continuity of gas fuel supply and threatens health, property, and life.

4. Landslide.

   Moving earth masses may cause gas pipelines to float and lead to stresses in the pipeline, consequently causing it to unseal, which affects the continuity of gas fuel supply and threatens health, property, and life.

5. Epidemic.

   Mass illnesses caused by infectious diseases, may involve death or temporary incapacitation of workers responsible for maintaining gas infrastructure or responding to emergency calls. This can lead to late response to emergency reports. Consequently, the supply of gas fuel could be affected. An outbreak could also upset the supply chain of spare parts and equipment used in gas network facilities.

6. Fire.

   Fire is particularly dangerous inside process facilities such as gas stations. It can lead to their partial or complete destruction, which can cause disruptions in the supply of gas fuel, as well as a threat to health, property, and life.

7. Severe frost.

   Prolonged severe frosts can cause increased gas fuel intake, resulting in gas fuel supply disruptions due to shortages. They can also contribute to malfunctions on the gas network due to large temperature fluctuations. Minimum operating temperatures declared by manufacturers of equipment may be exceeded and lead to disruptions in their proper operation or contributing to permanent damage.

8. Intense snowfall.

   Intense snowfall may lead to disruptions in electricity supply. Lack of electricity supply may cause disruptions in the operation of some network components, such as gas stations (lack of gas heating, lack of operation of odorization system and telemetry or automation system). A large snow cover also means communication difficulties to facilities and shut-off fittings on the gas network located in forest and agricultural areas.

9. Corrosion.

   Underground steel gas pipelines are primarily subject to uneven ground corrosion. The most destructive corrosion effects are those caused by stray currents and by alternating current induced from high-voltage power lines. To a somewhat lesser extent, gas pipelines are affected by galvanic corrosion, biological corrosion, and stress corrosion. The causes of corrosion include:

   - stray currents;

corrosion caused by stray currents occurs at intersections, approaches, and parallel runs of gas pipelines with electrified railroad and tramway traction.

- alternating currents;

  prolonged exposure of alternating currents (power lines above 110 kV) to steel underground gas infrastructure, can cause corrosion at the site of leaks in the insulation coating, because of the flow of alternating current.

- galvanic corrosion;

  galvanic corrosion is a typical corrosion process of a local nature, formed by corrosion cells in contact in the same soil or water electrolyte. The metal with more negative potential is corroded. On steel distribution networks, such cells occur, among other things, as a result of connections to foreign metal underground infrastructure.

- microbial corrosion;

  corrosion caused by the activity of microorganisms (bacteria) is particularly dangerous in poorly oxygenated environments with a pH between 5.5 and 8. Microbial corrosion often proceeds at a rate much higher than the rate of typical general corrosion in soil electrolytes.

- stress corrosion corrosion;

  a special type of corrosion, visible as corrosion cracks. The corrosion process develops slowly, leading to the unsealing of gas networks. The prerequisite for the initiation of corrosion cracking is the simultaneous action of two factors: internal or external stresses and corrosion caused by the interaction of the electrochemical environment.

- hydrogen corrosion;

  the process of destroying the structure of a metal due to the penetration of hydrogen into its structure. The effect of this process is the loss of plastic properties including a reduction in tensile strength parameters, leading to so-called hydrogen embrittlement.

Technical hazards are sudden and unforeseen damage or destruction of gas facilities causing interruption of their operation or loss of functionality. They mainly result from inadequate technical condition or human activity. They include:

1. Asset decapitalization.

Decapitalization is a process that means a reduction in the value of the capital held in the form of fixed assets. The reason is their wear and tear not balanced by sufficient investment. The problem of decapitalization was noted by the authors of the "National Security White Paper." Significant strategic dilemmas that Poland will face in the coming two decades are also related to the need to ensure security in cyberspace and to counteract the decapitalization of industrial and transportation infrastructure. Decapitalization, and often the devastation of infrastructure, cause the risk of industrial and technical disasters to increase every year[9]. In the coming years, the most significant risks in the area of energy security affecting security policy will be related to the decapitalization of generation infrastructure, transmission and distribution networks (almost 70 percent of this infrastructure is affected) [10].

According to the Decree of the Minister of Economy on the technical conditions to be met by gas networks and their location (Journal of Laws 2013, item 640), gas pipelines can be built of steel and polyethylene. Steel networks were built until the 1990s (nowadays steel is used mainly for high-pressure gas pipelines). Steel pipelines from this period, due to poorly developed corrosion protection, are prone to corrosion and are a much greater source of leaks compared to polyethylene pipelines, the use of which became widespread in Poland in the second half of the 1990s. The success of polyethylene as a material for the construction of medium- and low-pressure gas networks has been determined by several factors, which include durability (resistance to corrosion) as well as ease of installation (to which the high degree of automation of the splicing process contributes). The rate of restoration of the gas infrastructure has not kept pace with its year-to-year aging process and, consequently, its gradual deterioration. This can consequently lead to a significant increase in the number of incidents and failures. This state of affairs may result in services not having sufficient personnel and equipment resources to handle these incidents in a timely manner, i.e. secure the scene and eliminate the danger.

2. Human error.

---

[9] National Security Bureau, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, p. 13, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf, [access: 25.01.2023].

[10] *Ibd.*, p. 141.

As a result of human error (an employee of the operator or a subcontractor), inattention or incompetence, disruption or failure of the gas network can occur. During the process of construction or modernization of gas infrastructure facilities, mistakes can be made at both the design and construction stages of the gas network. Implementation of works not in accordance with guidelines and procedures, construction errors, quality errors in the materials used, which cannot always be noticed and eliminated at the stage of acceptance, may cause that over the years (at the stage of use of the gas network) there may be failures or disruptions in its operation. In addition, during operation or repair work, as a result of human error, failure to follow procedures, damage may occur, misconnection and misconfiguration of equipment on the gas network, which may consequently lead to disruption of gas fuel supply.

3. Conducted earthwork/construction work in the vicinity of gas infrastructure.

   It is incumbent on the owner or manager of third-party construction facilities/networks (water supply, sewerage, telecommunications, district heating, power supply) to exercise due caution when carrying out construction work in the vicinity of gas networks. As a result of industry agreements at coordination meetings held at district offices, rules for the mutual location of technical infrastructure, including gas networks, are determined. However, these rules are not always observed, and then situations arise where gas pipelines are damaged or interrupted during earthworks.

Terrorist and military threats involve the use of force or violence, aimed at causeing harm for political or ideological motives, especially to economically vital infrastructure. We can include:

1. Military threats.

   Military threats can take the form of political-military crises in particular, provoked for the purpose of exerting strategic pressure within the framework of current politics, without crossing the threshold of war. However, direct armed threats cannot be excluded either. Among them, two types should be distinguished: first - threats that can most generally be described as aterritorial, that is, point strikes of deliberately limited scale and scope, and second - threats of large-scale war[11].

2. Terrorist threats.

[11] National Security Bureau, *Biała Księga…*, op. cit., p. 13.

Terrorism is one of the most significant threats of the current world. It reduces both the state and the sense of security of any state and citizens. It involves the use of force or violence against individuals and organizations and the threat of destruction of facilities. Each gas system is vulnerable to terrorist attack. In particular, key components of the gas network may be the targets of attacks, the destruction of which poses a serious security threat.

3. Cyber attack.

The energy sector has become a target for cyber attacks with the advent of smart grids and automated equipment. In extreme cases, cyber attacks can disable the entire transmission or distribution infrastructure, causing massive economic and financial losses, casualties, and environmental damage. There have been a number of hacker attacks on energy infrastructure in recent years. In 2003, one of the U.S. nuclear power plants in Davis-Bess, was infected with the Slammer virus. The virus blocked the SCADA system that collected data on the reactor's cooling plant and radiation meters. In December 2015, there was a cyber attack on critical infrastructure in Ukraine, which resulted in hundreds of thousands of people losing access to electricity for hours. Another example is the 2021 attack on the critically important Colonial Pipeline, which supplies nearly half of the US East Coast's energy needs. The attack caused delays in fuel deliveries, which in turn led to an increase in gasoline futures. These types of cyber attacks are sometimes carried out by APT (Advanced Persistent Threat) groups.

These groups use sophisticated ICT attacks against political, economic, industrial, technical, and military targets. APT groups are often identified with specific countries, as there are indications that certain cybercrime groups act on behalf of specific countries carrying out pre-planned activities. Examples include groups with the acronyms APT1 identified with China or APT28 or APT29 identified with Russia[12].Of course, pinpointing the affiliation of specific attribution entities is not straightforward and requires advanced cyber investigative efforts.

In its report, the European Cyber Security Agency - ENISA in particular highlights the rise of ransomware threats. The trend is being fueled by the increasing digitization of society, as well as companies moving from traditional infrastructure to online solutions. During the

[12] cf. G. Pilarski, Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warsaw 2020, p. 69.

reporting period, ENISA also observed increased attempts by cybercriminals to attack critical infrastructures[13].

Experts unequivocally identify critical infrastructure facilities as one of the most important targets for cyber attacks. 70% of experts participating in the quantitative survey conducted for ‘the Future of crime report’ identified the negative impact of an attack on critical infrastructure as a critical threat, giving it a rating of "10" on a 10-point scale[14].

4. Sabotage.

   The conscious and faulty performance of assigned duties by an employee or subcontractors, or deliberate and planned damage to equipment, can lead to disruption of infrastructure operations.

Other threats include disruptions in cooperating systems as well as adverse events at the level of the organizations concerned, countries and in the international environment.

1. Disturbances in the electric power system.

   Electricity plays a very important role in the functioning of society and the state. Power outages in the electricity grid mean serious consequences for companies, industrial plants, public institutions, etc. The same is true of gas network components, some of which require uninterrupted supplies of electricity to function properly. This applies to LNG regasification stations and gas stations, where electricity is used to heat gas in the process of pressure reduction, gas fuel odorization and its constant monitoring, monitoring of explosion hazard zones, control of gas pressure, temperature and flows, automatic control of equipment. Also, information systems at dispatching stations require access to electricity for constant monitoring of gas network parameters and taking immediate action in the event of an emergency or threat to human health and life.

2. Disruption of the supply of materials, equipment, and services.

   Increasing globalization is significantly affecting the operation of businesses and the flow of goods and services. Supply disruptions are a major challenge for both consumers and companies. The Covid 19 pandemic or the blockade of the container ship Ever Given in the

---

[13] Gov.pl, *Krajobraz (cyber)zagrożeń 2021 - raport Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA),* https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberzagrozen-2021---raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa, [access: 24.02.2023].

[14] Infuture Institute, *Cybersecurity*, https://infuture.institute/trendy/future-of-crime/future-f-crime-infrastruktura-krytyczna/, [access: 24.02.2023].

Suez Canal showed that many companies around the world were not ready for the materialization of risk in terms of supply chain disruption. Also, for gas companies, disruptions in the supply of materials, equipment or services can cause a threat to the continuous and reliable operation of gas infrastructure.

3. Disruptions in the gas fuel supply chain (cooperating operators).

   The extraction of gas and its transportation to customers, requires the execution of many integrated activities. For this reason, we can divide the entire gas supply chain, based on the tasks performed, into the following systems:

   - mining;
   - transmission;
   - storage;
   - distribution.

   The various systems are interconnected and must cooperate with each other in order to be able to deliver gaseous fuel to the end user. The effects of a serious disruption of one system (failure, drop in gas pressure, lack of sufficient gas fuel) can be felt and have an impact on the proper operation of other gas systems.

4. Traffic incidents.

   Above-ground elements of the gas network, such as gas stations, LNG stations, gas units at the connection, may be located near roads, streets on which vehicular traffic travels. As a result of the driver's intentional or unintentional action, a wheeled vehicle driven by the driver may damage aboveground elements of the gas network.

5. Action by state authorities.

   We can mention here the implementation of proceedings for the revocation of the operator's license, the issuance of a normative act by authorities publicly adversely affecting the activities of entities and infrastructure.

6. Intra-organizational factors.

   As examples of risks, we can mention erroneous decisions of managers, irregularities in the functioning of the company's structures, inconsistent procedures, errors in personnel policy (e.g. lack of qualified staff).

7. Financial.

   As threats we can mention the lack of funds to maintain infrastructure, lack of liquidity, insolvency of the company, threat of bankruptcy.

8. Events of international significance.

The events may include, among others, political-economic conflicts in countries that supply or transit natural gas, resulting in restrictions or interruptions in gas supply, blackmail and pressure on energy security, threats of disinformation.

The aforementioned threats may adversely affect various elements of the country's gas infrastructure.

CRITICAL THREATS TO THE DISTRIBUTION NETWORK

Based on their research, the authors identified critical risks that affect key elements of the distribution network. As a result of the risk analysis, the authors assumed that very high-risk events affect the following elements of gas infrastructure:

- high-pressure steel pipelines and connections;
- elevated medium-pressure gas pipelines and steel connections;
- high-pressure gas stations;
- elevated medium pressure gas stations;
- medium pressure gas stations;
- LNG stations.

Accordingly, we can consider these to be key components of the distribution network. A summary of the results of the carried out risk analyses is presented in the table below.

Table 2.

Identification of risks on distribution network elements

	Risk			
Gas infrastructure element	Low	Medium	High	Very high
High and increased medium pressure steel pipeline/connection		Z, O, C	P, T	B, D, K
Gas pipeline/polyethylene connection of increased medium pressure		Z, O, C	B, D, P, T	
Medium pressure steel pipeline/connection	T	Z, O, C, B	D, K, P	
Gas pipeline/polyethylene connection of medium pressure	T	Z, O, D, C,B	P	

Gas pipeline/low-pressure steel connection	Z, C, T	B, O, P	D, K	
Low pressure gas pipeline/polyethylene connection	Z, C, T	B, O, D	P	
LNG station, High/ increased medium pressure gas station		W, Z, F, C	T	D, B
Medium pressure gas station	T	W, Z, F, C		D, B
Gas unit at the connection	Z, C, T	W, F, B	D	

Source: own elaboration.

Legend to Table 2.

O - Landslide, Flood, Mining damage	D - Decapitalization of assets	K - Corrosion	B - Human error	W - Strong wind
P - Construction work in the vicinity of a gas pipeline	T - Terrorist and military threats	Z - Lack of resources	C - Disruption of the gas fuel supply chain	F - Fire

The analysis shows that very high-risk threats include:

- asset decapitalization;
- corrosion;
- human error.

High-risk threats include:

- construction work near gas infrastructure;
- terrorist threats (cyber attack).

With a view to the reliability of the distribution network to ensure the continuity of gas fuel supply for end customers, the authors assumed that the most significant critical threats to the distribution network are those with very high and high risk of occurrence and consequences.

Recent years have brought dynamic changes in the environment, with new risks such as the COVID 19 pandemic, the war in Ukraine, disruption of the supply chain of gas fuels and materials, floods, and high winds. This makes it necessary to expand the approach to the operation of the gas network, taking into consideration, first of all, risk analysis. On this basis, the Distribution System Operator can consciously introduce additional measures adequate to the level and severity of risks affecting the security of gas fuel supply. A key issue, therefore, in a dynamically changing environment, becomes cyclical risk analysis.

In view of the dynamically changing environment in the gas sector, the authors propose to use the methodology of hazard and risk analysis, which can be helpful in ongoing and planning local operational decisions. The following are six groups of tasks that are proposed to be performed during the hazard and risk analysis:

1 – Determination of the position of distribution network.

In the first step, the number of individual gas network elements should be determined at the DSO level. In addition, the number of entry points to the system and exit points from the system should be determined, along with the identification of key customers.

2 - Identification of threats to the distribution network.

In the second step, it is necessary to analyze the risks and select the most significant risks that may affect the security of operation of the gas infrastructure on the territory of the DSO (taking into consideration the catalog of risks). When identifying and selecting the most significant threats, statistical and historical data found in the failure registers, among others, should be taken into account. In addition, when analyzing the hazards, the specifics of the area should be considered, e.g., existing landslides, mining areas, floods, etc. It is necessary to consider the risks that have already occurred and those that are likely to occur, with the view of the observed processes and geopolitical changes.

3 - Conducting a risk analysis and identifying critical threats to the distribution network.

In the third step, a risk analysis, that is, a determination of the probability of occurrence of the risks identified in step two and an assessment of the consequences of their occurrence, should be carried out. The results should be presented in the form of a risk assessment matrix. After the risk analysis, it is necessary to identify critical threats to the distribution network, i.e. threats with very high and high risk of occurrence and consequences.

4 – Identification of key elements of the distribution network.

In the fourth step, the key facilities of the distribution network of a given DSO should be selected. To do this, the key facilities selection algorithm is used. The selection of key facilities should take into consideration, among other things, the way the gas pipeline is supplied, the functions and type of operation of the substation, and the number of customers including key customers.

5 – Determination of the level of risk acceptance for key elements of the distribution network.

In the fifth step, the risk levels for key network elements diagnosed above should be translated into risk acceptance categories. It is recommended that the DSO respond and implement actions to minimize risks posing high and very high threat to key elements of the distribution network.

6 - Selection of actions at the prevention and response stages.

In the sixth step, the applied actions to be used at the prevention stage and at the time of the incident should be reviewed in terms of adaptation to the diagnosed critical risks and the possibility of introducing new, previously unused solutions.

CONCLUSION

This article provides diagnosis of threats to gas infrastructure and describes their impact on various components of the distribution network. Some of the risks are independent of the Distribution System Operator (DSO) e.g. natural hazards, while others can be influenced by the operator e.g. human error, decapitalization, etc. The emergence of threats, e.g., disruptions to the supply of materials, equipment and services caused by the pandemic and conflict in Ukraine, or military threats and cyber attacks caused by the current geopolitical situation, show the great dynamics of change in this area. Just some time ago, these threats would not have been considered. This indicates that the Distribution System Operator must conduct a cyclic update of the threats and take appropriate measures to eliminate or minimize them. The identified and described natural, technical, terrorist threats affect elements of the gas network, which is also confirmed by the conducted risk analysis. Therefore, the hypothesis that natural, technical, terrorist threats, dependent and independent of the DSO's actions, have a significant impact on the security of gas fuel supply is true. As a result of the risk analysis, threats that have a critical impact on the distribution network have been identified. These include asset decapitalization, corrosion, human error and construction work in the vicinity of gas infrastructure, as well as terrorist threats (cyber attack).

In addition, the carried-out risk analysis indicated that the catalog of key components of the distribution network includes a high-pressure gas pipeline, an increased medium-pressure gas pipeline, a high-pressure gas station, an increased medium-pressure gas station, an LNG station, and a medium-pressure gas station. The main threats to medium-pressure and LNG stations are asset decapitalization and human error. Medium-pressure gas stations are facilities that supply gas fuel to parts of cities or smaller towns. Their failure can lead to a situation where many thousands of customers, including key customers, can be deprived of gas fuel supply for a long period of time. Based on the risk analysis, it has been proven that threats posing very high and high risks to key elements of the distribution network have an impact on ensuring continuity of supply, which directly translates into energy security.

The application of the threat and risk analysis methodology as proposed by the Authors will allow the implementation of the DSO's responsibilities in the distribution system in the face of dynamically emerging threats. It is the intention of the Authors that the individual steps of the methodology will constitute coherent actions, which, adapted to local conditions, will ultimately be an operational management tool for managers and employees of technical services of DSOs in times of VUCA, i.e. times of dynamic threats and uncertainty.

REFERENCES LIST

LITERATURE

Barczyński A., Vademecum gazownika – Tom II Infrastruktura przesyłowa i dystrybucyjna gazu ziemnego. Praca zbiorowa, Stowarzyszenie Naukowo-Techniczne Inżynierów i Techników Przemysłu Naftowego i Gazowniczego, Kraków 2013.

Bąkowski K., Sieci i Instalacje Gazowe. Poradnik projektowania, budowy i eksploatacji, Wydawnictwo Naukowe PWN SA, Warszawa 2013.

Grządzielski W., Mróz T., Planowanie zrównoważonego rozwoju systemu gazowego, Wydawnictwo KAPRINT, Lublin 2017.

Matkowski A., Vademecum gazownika – Tom IV Gaz ziemny: rynek, efektywność, bezpieczeństwo. Praca zbiorowa, Stowarzyszenie Naukowo-Techniczne Inżynierów i Techników Przemysłu Naftowego i Gazowniczego, Kraków 2012.

Pilarski G., Cyberprzestrzeń : relacje w wojnie hybrydowej, ASzWoj, Warsaw 2020.

SOURCES

Energy Regulatory Office, Charakterystyka rynku paliw gazowych, https://www.ure.gov.pl/pl/paliwa-gazowe/charakterystyka-rynku/9662,2020.html [access: 08.03.2023].

Gov.pl, Krajobraz (cyber)zagrożeń 2021 - raport Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA), https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberzagrozen-2021---raport-europejskiej-agencji-ds-cyberbezpieczenstwa-enisa, [access: 24.02.2023].

Infuture Institute, Cybersecurity, https://infuture.institute/trendy/future-of-crime/future-f-crime-infrastruktura-krytyczna/, [access: 24.02.2023].

Kolano S., Identyfikacja zagrożeń krytycznej infrastruktury państwa, „Współczesne Problemy Zarządzania", Tom 6, Nr 1(12), 2018.

Kulesa M., Rogóż P., Wybrane uwarunkowania liberalizacji sektora gazu w Polsce, https://www.cire.pl/pliki/2/Wybrane_uwarunkowania_liberalizacji_sektora_gazu_p.pdf [access: 08.03.2023].

National Security Bureau, Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf, [access: 25.01.2023].

Rozporządzenie Ministra Gospodarki z dnia 26 kwietnia 2013 r. w sprawie warunków technicznych, jakim powinny odpowiadać sieci gazowe i ich usytuowanie (Dz.U. 2013 poz. 640).

Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz. U. 1997 Nr 54 poz. 348).

Contribution to the creation of the article: management of works, scientific editing, introduction, summary – GP; theoretical approach, research – JM, MW.
