

INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

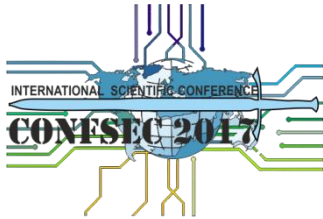
ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

**YEAR VII,
ISSUE 1/2023**



**PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA**



INTERNATIONAL SCIENTIFIC JOURNAL **SECURITY & FUTURE**

PUBLISHER:

SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0

108, Rakovski Str., 1000 Sofia, Bulgaria
tel. (+359 2) 987 72 90, tel./fax (+359 2) 986 22 40,
office@stumejournals.com,
www.stumejournals.com

ISSN (PRINT) 2535-0668; ISSN (Online) 2535-082X
YEAR VII, ISSUE 1 / 2023

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov
New Bulgarian University, Sofia, BG

Members:

Alexander Baranov, Prof.	Higher School of Economics	RU
Alexander Kurbatski, Prof.	Belarusian State University	BY
Alexander Troyanskiy, Assoc. Prof.	Odessa State Polytechnic University	UA
Andrzej Misiuk, Prof.	Warsaw University	PL
Ariana Bejleri, Assoc. Prof.	Polytechnic University of Tirana	AL
Galina Zhavoronkova, Prof.	National Aviation University, Kyiv	UA
Gudrun Biffl, Prof.	Donau University	AT
Dimitar Dimitrov, Prof.	Shumen University	BG
Evgeni Manev, Prof.	University of Library Studies and Information Technologies	BG
Hanáček Petr, Assoc. Prof.	Technical University of Brno	CZ
Iliyan Lilov, Prof., Col.	“Vasil Levski” National Military University	BG
Jaroslav Tureček, Assoc. Prof., Col.	Police Academy of the Czech Republic	CZ
Josef Reitšpís, Prof.	The University of Security Management in Kosice	SK
Juris Borzovs, Prof.	University of Latvia	LV
Kristiina Hakk, Assoc. Prof.	Estonian Information Technology College	EE
Kiril Stoychev, Prof.	Institute of Metal Science – BAS, Sofia	BG
Lev Elisov, Prof.	Moscow State Technical University of Civil Aviation	RU
Milan Popović, Prof.	University of Montenegro	ME
Muhammed Ali Aydin, Assoc. Prof.	Istanbul University	TR
Nebojša Bojanić, Assoc. Prof.	University of Sarajevo	BA
Nikifor Stefanof, Prof.	University of Security and Economics - Plovdiv	BG
Ninoslav Marina, Prof.	University of Information Science and Technology - Ohrid	MK
Nurgali Zaurbekov, Prof.	Almaty Technological University	KZ
Oliver Bacanovic, Prof.	University "St. Kliment Ohridski" - Bitola	MK
Ognyan Ivanov, Assoc. Prof.	Institute of Solid State Physics, BAS - Sofia	BG
Piotr Majer, Prof.	University of Warmia and Mazury	PL
Razvan Rughinis, Prof.	Polytechnical University of Bucharest	RO
Siniša Tatalović, Prof.	University of Zagreb	HR
Stoyan Denchev, Prof.	University of Library Studies and Information Technologies	BG
Tatyana Ejevskay, Prof.	Transbaikalian State University	RU
Valentin Todorov, Assoc. Prof.	Varna Free University „Chernorizets Hrabar“	BG
Vladimir Zakhmatov, Prof.	Academy of Ecological Safety, Kiev	UA
Zelimir Kesetovic, Prof.	University of Belgrade	RS

CONTENTS

THEORETICAL FOUNDATIONS OF SECURITY

Organizational resilience and critical infrastructure security systems

Valeri Panevski 3

A coordinated approach to achieve a higher overall level of resilience and protection of critical infrastructure

Valeri Panevski 6

Model of the Whistleblower Protection System

Veselin Tselkov 9

NATIONAL AND INTERNATIONAL SECURITY

Safety and security measures during transportation of dangerous goods class 7 (radioactive materials), taking into account the requirements of ADR

Lyudmil Nedelchev, Dimitar Dimitrov 12

Safety and security measures during transportation of dangerous goods class 7 (radioactive materials), taking into account the requirements of ADN

Lyudmil Nedelchev, Dimitar L. Dimitrov 15

Maritime piracy and armed robbery evolution in 2008-2022

Adelina Tumbarska 18

TECHNICAL FACILITIES FOR ENSURING SECURITY

Flood risk assessment and management through a water management information system

Sabina Nedkova, Galina Baycheva, Plamena Atanasova, Hristo Bozov 22

Organizational resilience and critical infrastructure security systems

Valeri Panevski

Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre “Acad. A Balevski” at the Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
paneovski@ims.bas.bg

Abstract: *The identification and protection of critical infrastructure (CI), which provides essential services for the national and European markets, especially in key sectors of the economy, requires priority measures to be taken to increase its resilience. The concept of resilience is closely related to the ability of a CI to prevent, defend against, respond to, withstand, mitigate and absorb, adapt to, or recover from risk events. Here, both the organizational measures and the technical part of the security systems, developed according to the specifics of CI, play an essential role.*

In this regard, this publication presents the framework of the author's view on the relationship between organizational resilience and CI security.

Key words: RESILIENCE, SECURITY SYSTEMS, CRITICAL INFRASTRUCTURE

1. Introduction

Critical infrastructure (CI), as a provider of essential services, has an indispensable role in maintaining vital societal functions or economic activities in an increasingly interconnected economy. Therefore, it is extremely important to establish at national level a framework which, on the one hand, strengthens the resilience of CIs on the market by establishing harmonized minimum rules, and on the other hand, assists them through consistent and targeted support measures and management.

Due to the increasingly interconnected nature of the activities in which CIs are involved, precautions related only to individual assets are not sufficient to prevent the occurrence of all types of uncertainties. It is therefore necessary to reorient the approach to ensure better risk reporting, better definition and greater consistency in the role and obligations of CIs as providers of services that are fundamental to the functioning of the market. It is necessary to take into account the importance of CI resilience, as it should be able to improve its ability to prevent, respond to, withstand, mitigate, incidents that may disrupt the provision of essential services to absorb them, adapt to them and recover from the impact of such incidents.

Also, as a result of the dynamic threat spectrum, which includes evolving hybrid and terrorist threats, and the increasing interdependence between infrastructure and sectors, more should be done to enhance CI preparedness. In addition, there is an increased physical risk due to natural disasters and climate change, which increases the frequency and magnitude of extreme weather events and induces long-term changes in climate conditions, which can reduce the capacity, efficiency and life cycle of a certain type of CI if no measures are taken to adapt to climate change.

Harmonized minimum rules should be established to ensure the provision of essential services to the market, increase the resilience of CIs and improve cross-border cooperation between competent authorities. It is important that future needs are taken into account in the development and implementation of these rules, ensuring the necessary flexibility. It is crucial to improve the capacity of CIs to provide essential services in the presence of a diverse range of risks. Therefore, in order to achieve a high level of resilience, CIs should be established to which special requirements and supervision will apply, but which will also receive special support and guidance when any relevant risks arise.

Proven experience in the development of CI security systems, which complement its capabilities to improve organizational resilience, has leading researchers from the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Center “Acad. A. Balevski” at the Bulgarian Academy of Sciences [1÷5].

2. Resilience and security of the organization

2.1 Definitions of resilience and security

For the purposes of this publication, the following definitions apply:

- ‘resilience’ means a critical entity’s ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident; [6]

- ‘resilience’ - ability to absorb and adapt in a changing environment; [7]

- ‘organizational resilience’ - ability of an organization to absorb and adapt in a changing environment; [7]

- ‘security’ - state of being free from danger or threat where procedures are followed or after taking appropriate measures.[7]

2.2 Threats and hazards

International governmental and private organizations developing policies, procedures and systems in the field of CI security, especially in the implementation of the all-hazards approach to CI security and resilience [8], make a significant contribution to the process of timely identification of CI hazards and threats.

Both natural and man-made (intentional or accidental) incidents have the potential to damage, disable or destroy CIs. Rather than focusing on one type of threat or hazard at a time, such as hurricanes or terrorism, management should identify all threats and hazards that pose the greatest risks to CI, allowing for more effective and efficient planning and resource allocation.

CI is subject to risks related to physical threats and natural disasters, and is also now increasingly exposed to cyber risks. These risks stem from the increasing integration of information and communication technologies into CIs and the presence of likely adversaries focused on exploiting potential cyber vulnerabilities. As physical infrastructure becomes increasingly dependent on complex cyber systems for operations, CI may become more vulnerable to certain cyber threats, including transnational ones.

The links and interdependencies between infrastructure elements and sectors mean that damage, disruption or destruction of one infrastructure element can cause cascading effects, affecting the continued operation of another. Identifying and understanding interdependencies or dependencies between infrastructure elements and sectors are important for assessing risks and vulnerabilities and determining steps that can be taken to increase security and resilience of the CIs.

And what has been said so far is directly related to the possible threats and hazards, specific to geographical regions or to an entire country, which can affect organizational resilience (Figure 1).

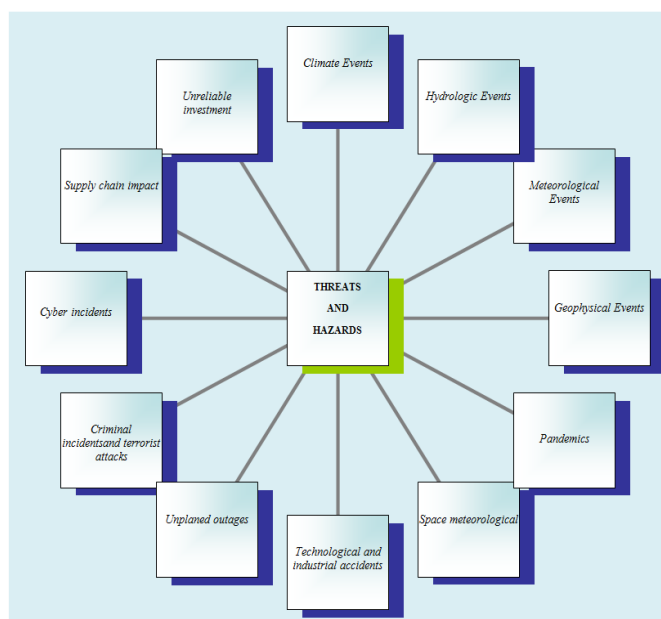


Figure 1: Threats and hazards (option)

- Climate events - extreme temperatures, drought, forest fires;
- Hydrological events - floods;
- Meteorological events - severe storms, winter storms;
- Geophysical events - earthquakes, volcanic eruptions;
- Pandemics - global disease outbreaks;
- Space weather events - geomagnetic storms;
- Technological and industrial accidents - structural damage, industrial fires, release of hazardous substances, chemical spills;
- Unplanned outages - aging infrastructure, equipment failure, large-scale power outages;
- Criminal incidents and terrorist attacks - vandalism, theft, property damage, active shooter incidents, kinetic attacks;
- Cyber incidents - denial of service attacks, malware, phishing;
- Supply chain attacks - using vulnerabilities to cause system or network damage;
- Unreliable investment - potentially to provide external undue influence on CI.

Thus presented threats and hazards must be analyzed to determine their potential impact on CI and how likely they are to occur.

Effective risk management depends on CI management's ability to engage cross-sector to facilitate a shared understanding of risk and to integrate a broad range of risk management activities. By identifying what is truly critical at the functional level and where the key dependencies and interdependencies lie, the risks that are considered unacceptable to the CI can be determined. This approach makes it possible to more effectively determine the risks to the security and sustainability of CIs.

3. CI resilience and security

3.1 Relation between resilience and security

Resilience refers to the ability to prepare and adapt CI to changing conditions. This means being able to withstand and recover quickly from outages, deliberate attacks, accidents or naturally occurring threats or incidents. Sustainable CI also needs to be flexible and adaptable.

Security is directly related to reducing the risk to CIs of threats, attacks, or the effects of natural or man-made disasters through the application of physical means or cyber security measures.

A good CI security and resilience approach is based on cooperation and information sharing.

Cooperation is facilitated by establishing the structures and processes necessary for government entities and the private sector to communicate freely: without disclosing private information or providing an unfair advantage; by maintaining a trusted information environment where stakeholders share information to strengthen security and resilience; and ensuring that relevant stakeholders are fairly represented and engaged by all levels of government (both public and private).

Successful information sharing requires established mechanisms or channels to sustainably reach stakeholders - before, during and after an incident. Information sharing can take many forms, including training, briefings, e-mail alerts, conference calls or meetings in secure locations to discuss classified material about specific threats or hazards, and documents and forums that encourage the sharing of lessons learned. The latter category improves planning for dealing with future risk events.

3.2 Strengthening the security and resilience of critical infrastructure against cyber attacks and other threats

The concept of considering CI as an aggregation of separate physical assets is outdated, as connectivity in contemporary infrastructures takes place in a cybernetic environment. This convergence of cyber and physical assets and activities has transformed CI risks in sectors ranging from energy and transportation to banking, healthcare and agriculture.

To strengthen the security and resilience of CIs against identified and/or probable threats and hazards, the following strategies are applicable, but not limited to:

- Improving the exchange of information and obtaining data on CI risks and developing real-time situational awareness capabilities that ensure interpretation and visualization of the risk event by increasing the volume, timeliness and quality of threat and hazards reporting (see Fig. 1);
- Establishing a security and sustainability partnership (between CI owners and operators), for the provision of essential services and functions, and for defining a national focus for collective action carried out in support of local and regional partners, as well as using incentives for improving security and resilience;
- Identifying and understanding the interdependencies and cascading impacts between critical systems through the use of risk assessment programs specific to the CI, its assets and networks, and cross-sector risk assessments;
- Building cooperation between government structures and the private sector to determine the need to develop effective policies and best practices for security and protection of CI, incl. and cyber security;
- Reducing vulnerabilities through the development of resilient design of CIs while identifying and promoting opportunities to build security and resilience of CIs as they are developed and updated, rather than focusing solely on mitigating vulnerabilities inherent to existing CIs.

4. Some challenges to CI security systems

In a rapidly changing threat environment and risk dynamics, it is essential to have an accurate, up-to-date and complete picture of the most important risks facing CI operators, with a particular focus on CIs with cross-border meaning. For this reason, measures should be taken to carry out and/or update assessments of these risks, while at the same time efforts to address climate change and environmental risks should continue, in particular where natural phenomena may further exacerbate human-caused risks.

Consequently, in line with existing threats, it is necessary to prioritize measures to increase resilience in the key sectors of energy, digital infrastructure, banking, health, transport and space, and these measures should focus on increasing the resilience of entities, governing CIs, in relation to human-caused risks. Priority should be given to a national CI that has cross-border links, which is related to the possible consequences of the occurrence of risks.

Also, malicious actions in cyberspace targeting critical areas, including CIs, can disrupt or damage physical infrastructure, and sabotage against it can make digital services unavailable, demonstrating the growing interdependence of physical and digital infrastructure.

Another important challenge for CIs is the fact that they are becoming increasingly complex and interdependent. These infrastructures are under pressure and have become vulnerable due to fragmented management and lack of investment in system maintenance. From climate change to cyber-attacks, CIs operate in an increasingly uncertain future where not all threats and dangers can be predicted or avoided. Therefore, it is essential that CIs are prepared for the threats that can be foreseen and are able to respond to the unexpected so that they continue to provide the essential services that society depends on.

Last but not least, special attention should be paid to CIs as “undersea critical infrastructure or offshore energy infrastructure” [9].

To overcome security environment challenges, infrastructural deficits and to repair and modernize existing CI security systems in the context of dynamic changes in climate and digital communications and human-induced risk events, investments need to be planned. Furthermore, accelerated urbanization requires significant investment in new CIs to meet the growing demand and consumption of their services and products. This creates a huge opportunity to plan and build CI security systems that will continue to function under various risk events and, if they fail, do so in a safe manner.

4. Conclusion

Developing a comprehensive policy framework is the initial step towards increasing the CIs resilience, and whether the infrastructure will indeed be resilient depends on the fulfillment of the objectives and requirements set out in these policies. Accountability mechanisms need to be developed to ensure that intended resilience measures are implemented, such as conducting criticality and vulnerability assessments, preparing business continuity plans, providing backup operating systems, conducting exercises and stress tests, entering into mutual assistance agreements, retooling assets or implementing risk financing mechanisms. Implementation of monitoring can take various forms, including regular reporting, inspections and performance evaluations or peer reviews. Regular evaluations are also useful for determining the effectiveness of policy instruments in strengthening the resilience of CIs and adapting them to keep up with the pace of innovation and emerging risk patterns.

ACKNOWLEDGMENTS

This paper is the result of implementation of the scientific work of the IMSETCH-BAS team, participating in Work package 2. “Intelligent security systems”, Project BG05M2OP001-1.002-0006 Competence Centre “Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)”, funded by the European Regional Development Fund through the Operational Programme “Science and education for smart growth” (SESG), co-financed by the European Union through the European Structural and Investment Funds.

References:

- [1] Dimitrov D., „Some examples of a nuclear security contingency plans, designed for nuclear facilities“, Proceedings of the Annual University Scientific Conference, 5, Publishing House of Vasil Levski National University, 2021, ISSN: 2367-7465, pp. 78-86;
- [2] Dimitar Dimitrov, “Comparative evaluation of techniques for modeling and simulation of interdependent critical infrastructures”, Proceedings of the Annual University Scientific Conference, 10, Publishing House of the National Military University “Vasil Levski”, 2020, ISSN: 1314-1937, pp. 231-241;
- [3] Dimitrov D., „Some examples of a nuclear security contingency plans, designed for nuclear facilities“, Proceedings of the Annual University Scientific Conference, 5, Publishing House of Vasil Levski National University, 2021, ISSN: 2367-7465, pp. 78-86;
- [4] Dimitrov D., „Developing the opportunities for building nuclear security“, Technics. Technologies. Education. Safety. 2021. , Military sciences and national security., Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering “Industry - 4.0”, 2021, ISSN: 2535-0315 (Print), 2535-0323 (Online), pp. 208-211;
- [5] Ventsislav Pehlivaniski, “Tests in the process of designing protection systems”, IMSETHC-BAS, 2020, ISBN: 978-619-188-359-2, pages 169;
- [6] DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC ;
- [7] ISO 22300:2021(en) Security and resilience — Vocabulary;
- [8] A Guide to Critical Infrastructure Security and Resilience, November 2019,
<https://www.cisa.gov/resources-tools/resources/guide-critical-infrastructure-security-and-resilience>;
- [9] COUNCIL RECOMMENDATION of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, EN Official Journal of the European Union 20.1.2023, C 20/1.

A coordinated approach to achieve a higher overall level of resilience and protection of critical infrastructure

Valeri Panevski

Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski" at the Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
paneovski@ims.bas.bg

Abstract: Developing a coordinated and effective response to critical infrastructure (CI) threats, current and anticipated, requires achieving a higher overall level of resilience and protection. The growing interdependence between physical and digital infrastructure creates opportunities for malicious cyberspace actions targeting critical areas to disrupt functionality or damage physical infrastructure. In this regard, through the application of specific approaches to strengthen the resilience of CIs, it is possible to improve the capabilities to counter physical and hybrid threats.

Presenting an option for an effective response against CI threats through the development of security systems is the content of this publication.

Keywords: RESILIENCE AND PROTECTION, CRITICAL INFRASTRUCTURE

Introduction

Natural disasters and malicious attacks on critical infrastructure (CI) pose a serious risk to society and the economy. The interconnectedness of supply chains and technological and financial systems in the global economy increases the vulnerability of CIs to exposure to risk events. When shocks and disruptions occur, their negative impacts can cut across sectors and national boundaries.

At the same time, the global increase in infrastructure investment and the digital transformation of service offerings provide opportunities to rethink CI sustainability. The changing context of the security and business environment necessitates policies and CI governance models that favor investment in resilience. The progressive shift in the focus of CI security policies from asset protection to system resilience is noticeable, which necessitates the implementation of a systemic approach. Rather than focusing only on asset protection, using the systems approach allows infrastructure operators to address asset interdependencies and prioritize resilience measures for those CIs (as a whole or at their critical assets) whose failure would cause the most a lot of damage. Contemporary standardized approaches have been developed to determine the objectives and / or requirements for a higher overall level of resilience and protection, in accordance with the specifics of CI and to prevent any level of potential consequences both in the sites and for the population in the neighboring areas [1,2,3,4,5].

1. Making CI sustainability a management priority

CIs structure the backbone of the functioning of our modern and interconnected societies. Disruption of telecommunications services, energy supply, water supply, transportation or financial systems can cause significant damage to the welfare of citizens and cause adverse economic effects that affect beyond the perimeter of the directly affected area.

Major upheavals of all kinds, from natural disasters to industrial accidents, terrorist or cyber-attacks, demonstrate the vulnerability of CIs, as their destruction or disruption can lead to cascading effects across sectors not only nationally but also internationally. Therefore, ensuring the sustainability of the CI to manage the business continuity of its activity should be an essential part of the developed policies at the national and international level.

1.1 Resilience of the CI

In general, resilience can be defined as the ability of CI to absorb the impact of risk events, recover from them and adapt to changing conditions, while maintaining the same function as before the risk event. In this way, attention is paid to the CI's ability to withstand shocks without loss of functionality, limiting the duration of the interruption and minimizing recovery time.

Thus, upon the occurrence of a given risk event (sudden or gradual), CI resilience objectives can be measured, namely:

- Limiting the extent of damage;
- Limiting the duration of business interruption.

It is also important to note that recovery does not necessarily mean the exact resumption of the state as before the risk event, but may involve change leading to adaptation to new conditions and improvement of the CI's functionality.

In this context, ensuring CI sustainability can be done by providing a combination of several key qualities [6]:

- *Resilience:* Designing CIs robust enough to withstand a foreseeable risk event or investing in CI elements to withstand low-probability but high-consequence events.
- *Redundancy:* Continuation of CI operation through the use of replacement or backup systems that can be activated in the event of the impact of a risk event.
- *Resource assurance:* Management of a risk event by: identifying options; prioritizing what needs to be done to control the damage and initiate mitigation, and informing staff of the documented solutions to be implemented. Intelligence depends primarily on people, not technology.
- *Adaptability:* Reviewing plans, modifying procedures, and introducing new tools and technologies needed to improve resilience, resource security, and recovery capabilities before the next crisis occurs.

1.1 Natural hazards, industrial accidents and pandemics

CI has a specific vulnerability to potential risks, such as natural hazards. Windstorms can bring down overhead and power distribution lines, earthquakes can destroy bridges or tunnels, rupture water mains, water-related disasters (flooding, etc.) can have major impacts on roads, railways, water supply and sanitation facilities as well as storm surges and tsunamis affect ports, energy facilities and other infrastructure located in coastal areas. Space weather events (e.g. a solar storm) can also put power grids at risk of blackouts and threaten satellites and geo-positioning systems with potential implications for transportation and other activities. Significant disturbances can cause industrial accidents.

When a critical infrastructure asset or network is affected by a risk event, disruption of the service provided can quickly lead to major economic or social impacts. In addition to the direct damage of a disaster, service interruptions can last longer and affect a wider area than where the disaster itself is realized. As a result, firms and households may suffer from a loss of services, which affects production, demand and welfare. In some cases, *business continuity of infrastructure operators* may also be significantly affected,

including emergency response, which may further delay economic recovery after a disaster.

With a high degree of probability it can be argued that climate change and the associated risks of sea-level rise will increase the vulnerability of many critical infrastructure systems located on the seashore and within waterways, especially in energy and transport.

1.2 Digital security threats and terrorist attacks

Individuals with probable intentions for terrorist impacts have also identified CIs as potential targets in terms of the high impact their disruption could generate. This is true both for acts of terrorism and, increasingly, for digital threats. The emerging risk of hybrid threats, characterized by malicious actors playing on the vulnerabilities of civil activities as essential lifelines to impact public trust in open and democratic societies, has also received increased attention from risk managers.

Digital threats can affect CI in different ways - through software, through hardware or through the market realization chain. The rapid development of technology and the increasing digitization of many critical infrastructure processes require constant monitoring of digital security threats and regular assessment of emerging opportunities for malicious impact.

In terms of the risk of terrorism, transport infrastructures (eg. air, sea, rail and metro) are highly vulnerable targets for terrorist attacks that can be complex to defend. If CIs are attacked, the negative impacts may go beyond the loss of human life, as systems may be disrupted for a longer period and the effects on public trust may be difficult to recover from. Nuclear power plants and chemical plants can also be the target of terrorist attacks, resulting in large-scale spills of chemical elements and compounds and releases of radioactive elements into the air, potentially rendering certain areas uninhabitable for long periods of time. Terrorists may also target water systems with bacterial or chemical contamination.

For both, digital security risk and terrorism, insider threats are a significant concern for CI operators. Access to facilities and knowledge of security measures provide a significant advantage to malicious actors wishing to carry out such actions.

2. A possible approach to achieve a higher overall level of CI security

In the current dynamic risk landscape, the portfolio of risks that stakeholders will have to deal with requires increased attention to CI vulnerability, in the context of its security and resilience. Disaster risks, compounded by climate change, present a set of challenges to CI sustainability. In addition, the rise of hybrid threats and associated digital security risks requires increased CI resilience to digital security incidents. Security measures against the risk of terrorism must also include CI resilience. This variety of hazards facing CI requires an all-hazards and threat approach to achieving CI security by improving its resilience.

2.1 Adopting a systemic approach to CI sustainability

The shift from CI protection to resilience aims to address key changes in the risk environment marked by increased uncertainty. To better integrate the complexities, interdependencies and interconnectedness of CIs, adopting a systems approach to CI sustainability provides complementary perspectives. The complex and multifaceted nature of CI sustainability requires the application of a risk-based, multi-layered approach that considers the interdependencies of complex infrastructures while considering potential solutions applicable throughout the life cycle of the infrastructure system (i.e. design, construction and operation). Therefore, resilience is defined not as a discrete outcome or exclusively the ability to recover from a disaster, but rather as a dynamic process that applies a risk-based and life-cycle approach to addressing CI vulnerabilities, making systems more fault-tolerant, more efficient and better able to adapt to unexpected challenges.

The Organization for Economic Co-operation and Development (OECD) expanded this notion of a systems approach applied to CI sustainability [6] and proposed a series of key attributes that public policies should consider in this area:

➤ All hazards and threats

Single hazard policies are not sufficient to build CI resilience. Taking an all-hazards and all-threats approach to UR sustainability allows policymakers and CI operators to better prepare for the unexpected.

➤ System level

CI assets are components of a wider complex system that must be considered in its entirety in a resilience strategy. Some system assets are more critical than others. A systems approach enables prioritization of the most critical components through dependency modeling and criticality assessments, as well as addressing weaknesses that create CI vulnerabilities.

➤ Multi-sectoral

Addressing interdependencies requires policy makers and CI operators to go beyond a systems-level approach and jointly target CI sectors to structure a comprehensive resilience policy. From mapping interdependencies to developing shared business continuity objectives, a multi-sector approach is essential for a comprehensive CI resilience policy.

➤ Cross-border dimension

Dangers and threats do not stop at national borders. In some cases, CI systems cross national borders, providing services in multiple countries, and their operators may also operate CIs in several countries. Sharing good practices, adopting common approaches, developing joint standards for CI resilience are some of the policy options that can promote cross-border cooperation in this area.

➤ Life cycle approach

Different resilience and security measures can be applied to the different phases of the CI life cycle: integrating resilience and redundancy requires investment in the design phase, while developing business continuity planning is more about the phase of operation and adaptability can be based on CI renewal. Therefore, it is important to create a comprehensive policy that enables resilience throughout the CI life cycle, applicable from the design phase to its operations and maintenance and retrofitting.

➤ The entire risk management cycle

A common resilience policy should include measures throughout the disaster risk management cycle, from risk assessment, risk prevention, emergency preparedness and response, to recovery. The resilience of CI has specifics in each of these phases. Risk assessment should include assessments of dependencies and criticality. Risk prevention includes resilience measures in the design phase as well as special awareness-raising dialogues with infrastructure operators.

➤ Risk-based and multi-layered approach

Given the significant degree of uncertainty about the intensity and complexity of future disasters, the multiple dimensions of vulnerability of infrastructure systems and all the interrelationships between these systems, prioritizing resilience measures is essential. Only a risk-based and multi-layered approach can account for the interdependencies of complex infrastructures, while also considering potential solutions applicable through infrastructure systems throughout the life cycle.

2.2 CI transformation through innovation and digitization

Innovations are transforming infrastructure systems at a rapid pace, with consequences for risks and vulnerabilities that CI resilience and security policies must integrate. From the energy to

the transport or information sectors, major transformations are underway. The energy sector offers opportunities for significant innovation with the growing share of renewable resources, the development of smart grids and more decentralized and localized approaches to energy production and consumption. The rapid development of autonomous vehicles along with advances in artificial intelligence promises to radically change the transportation sector. Information and communication technologies have significantly changed the way we exchange data and communicate in our daily lives. Smart cities, driven by a data-driven approach, aim to combine the data revolution with innovative and interconnected urban services, reshaping the metropolitan areas where the majority of the world's population lives.

3. Some challenges to CI sustainability management

3.1 Identification of critical assets and assessment of their vulnerabilities

An important point of a comprehensive CI policy is to define a systematic analytical approach for prioritizing sustainability measures that will provide accurate information for target planning and investment decisions. It needs to be recognized that not all infrastructure assets have the same level of criticality and criticality assessments should be carried out to identify assets that are truly critical.

3.2 Vulnerability analysis to identify weak points

Once the critical assets are accounted for and hierarchically classified, vulnerability assessments enable the identification of weak points where potential failures are likely to occur. An in-depth CI vulnerability assessment provides an insight into the most important risks, threats, vulnerabilities and the level of resilience of this infrastructure. In order to do this, it is essential to stress-test the CI's vulnerability to a series of risk scenarios of varying probability, magnitude, or their combination, across a range of potential hazards and threats. These assessments consider the most likely scenarios, in addition to those that are less likely, but could nevertheless come to pass.

A comprehensive, all-hazards approach can help uncover complex vulnerabilities while facilitating the integration of CI management system vulnerabilities into business impact analysis, as these errors are common. The European Commission's Joint Research Center has, for example, developed a stress test tool that focuses on these complex aspects of governance with application to the nuclear and banking sectors [6].

CI vulnerability assessments can be performed using a variety of methodologies that range from deterministic approaches to probabilistic methods. Deterministic approaches analyze and interpret past disaster events and available retrospective data in light of new developments. Scenarios and disaster simulations extend retrospective analyses.

3.3 Risk assessment as a basis for investment in resilience

A number of threat and hazard assessment approaches are available to help CI owners and operators understand potential incidents and the ways in which they could affect infrastructure and the surrounding urbanized area. Risk assessments provide decision makers with better information to determine which mitigation and risk management measures are most critical, for which critical assets different types of action are most appropriate, and the range of measures available could include: coordination with other stakeholders; provision of additional response or recovery equipment; changes in the design of CI elements; restrictions on operations and hiring and training of personnel. Risk assessments encourage consideration of a range of more likely events, the impact of which could nevertheless have significant consequences.

Identifying the weak points (vulnerable assets) of CIs allows targeting resilience efforts to those that would have the most severe consequences for the infrastructure. Such prioritization can ensure

targeted planning and adequate investment decisions for infrastructure assets, namely which should be strengthened or relocated first, or which asset should receive priority post-disaster recovery to ensure rapid recovery of CI functionality. Also, by comparing the benefits of different resilience measures related to reducing the risk of failures, cost-benefit analysis can support appropriate resilience investment decisions.

4. Conclusion

The protection of CI has become a priority of national and international importance. To be effective, resilience and risk analyzes must be conducted based on new, expanded paradigms. The high degree of connectedness of CIs, both internal and external, can make them vulnerable to global disruptions when subjected to impacts of various natures, from accidental technological failures to natural events, software failures, deliberate malicious attacks, human and organizational errors. It is widely recognized that this wider range of likely risk events requires an all-hazards approach to understanding the failure behavior of CIs in order to achieve their effective protection.

ACKNOWLEDGMENTS

This paper is the result of implementation of the scientific work of the IMSETCH-BAS team, participating in Work package 2. "Intelligent security systems", Project BG05M2OP001-1.002-0006 Competence Centre "Quantum Communication, Intelligent Security and Risk Management Systems (Quasar)", funded by the European Regional Development Fund through the Operational Programme "Science and education for smart growth" (SESG), co-financed by the European Union through the European Structural and Investment Funds.

References:

- [1] Dimitar Dimitrov, "Comparative evaluation of the modeling and simulation techniques of interdependent critical infrastructures", Collection of reports from the annual university scientific conference, 10, Vasil Levski National University Publishing Complex, 2020, ISSN: 1314-1937, pp. 231÷241;
- [2] Dimitrov D., "Developing the opportunities for building nuclear security", Technics. Technologies. Education. Safety. 2021, Military sciences and national security., Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering "Industry - 4.0", 2021, ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 208÷211;
- [3] Dimitrov, D. "Engineering solutions to ensure protection of nuclear power plants against sabotage", International Scientific Journal "Security&Future", 6, 1, STUME, 2022, ISSN:(PRINT) 2535-0668, (ONLINE) 2535-082X, pp.18÷21;
- [4] Kolarov A.P., Naydenov R.V., "An approach to provide operational information on the hydrological condition in sea spaces", VI INTERNATIONAL SCIENTIFIC CONFERENCE CONFSEC, 05-08. DECEMBER 2022 BOROVETS, BULGARIA, YEAR 6, ISSUE 1 (8), Scientific technical union of mechanical engineering "Industry - 4.0", 2022, ISSN:ISSN PRINT 2603-2945, ISSN ONLINE 2603-2953, 74-77;
- [5] Kolarov A.P., Georgiev N.L., Boychev Ya., "The magnetic signature of ships in managing the security and safety environment", Collection of reports VII International scientific conference "HIGH TECHNOLOGIES. BUSINESS. SOCIETY 2022", YEAR VI, ISSUE 1 (10), STUME, 2022, ISSN:2535-0005(PRINT), 2535-0013 (ONLINE), pp. 24÷27;
- [6] OECD (2019), *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, <https://doi.org/10.1787/02f0e5a0-en>.

Model of the Whistleblower Protection System

Veselin Tselkov
University for Library Studies and Information Technologies
v.tselkov@unibit.bg

Abstract: The construction of the system for the protection of whistleblowers is in accordance with the legal framework of the Republic of Bulgaria and the EU Directive.

The report defines a multi-layered model of the protection system, including:

- Information on violations;
- Persons who granted protection:
- Obligated entities, including:
 - Employers in the public and private sector;
- Institutions, bodies, services and agencies of the EU;
- European Commission.

Signaling channels, duties and functional interactions between the main elements of the model are structured. A mechanism for synchronizing and controlling signal processing activities is presented. The model is a theoretical basis for the construction and functioning of the whistleblower protection system.

Keywords: WHISTLEBLOWER PROTECTION, SYSTEMS MODELING, FUNCTIONAL INTERACTIONS, SYNCHRONIZATION AND CONTROL.

1. INTRODUCTION

The establishment of the Whistleblower Protection System (WBPS) is in accordance with the legal framework of the Republic of Bulgaria (Law on the Protection of Whistleblowers or Publicly Disclosing Information on Violations, State Gazette No. 11 of February 2, 2023 [1]) and Directive 2019/1937 (the so-called Whistleblower Directive) [2].

The main objective of WBPS is ensure *"the protection of persons in the public and private sectors who file reports or publicly disclose information about violations of Bulgarian legislation or acts of the European Union, which became known to them during or on the occasion of the performance of their work or official duties or in another work context"*[1].

The report presents a multi-layered model of the Whistleblower Protection System as follows:

- **Layer 1:** Information on violations;
- **Layer 2:** Persons to whom protection is granted;
- **Layer 3:** Obligated entities;
- **Layer 4:** EU institutions, bodies, offices and agencies;
- **Layer 5:** European Commission.

The structural elements of the model and the types of interactions are defined.

2. MULTI-LAYER MODEL OF THE PROTECTION SYSTEM

The structural elements of the protection system model are (Fig. 1.):

- Information on violations;
- Persons who granted protection:
 - Reporting persons (reporting person);
 - Persons publicly disclosing information;
 - Supporting and related persons;
 - Legal entities in which the whistleblower has an equity interest, works for, or is otherwise associated with in a work context;
- Obligated entities, including:

- Employers in the public and private sector;
- Central Authority for External Reporting of Signals (CAERS);
- Competent authorities;
- Prosecutor's Office of the Republic of Bulgaria;
- The Commission for Combating Corruption and Confiscation of Illegally Acquired Property (CCCCIAP);
- Ombudsman of the Republic of Bulgaria;
- Institutions, bodies, services and agencies of the EU;
- European Commission.

Violation information

Breach information includes reports or public disclosure of information about:

- Violations of Bulgarian legislation or of the acts of the European Union specified in the annex to the law;
- Violations that affect the financial interests of the European Union within the meaning of Art. 325 of the Treaty on the Functioning of the European Union [3];
- Violations of the rules of the internal market within the meaning of Art. 26, paragraph 2 of the Treaty on the Functioning of the European Union, including the rules of the European Union and Bulgarian legislation on competition and state aid;
- Violations related to cross-border tax schemes, the purpose of which is to obtain a tax advantage that is contrary to the object or purpose of the applicable law in the field of corporate taxation;
- Committed crime of a general nature, for which a person under Art. 5 has learned in connection with the performance of his work or in the performance of his official duties [1].

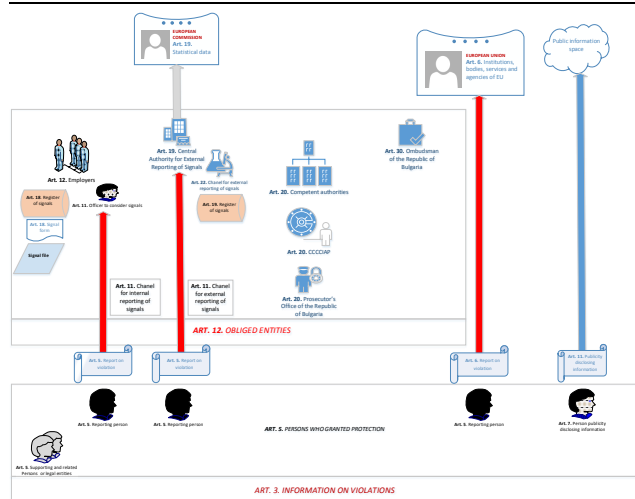


Fig. 1. Model of the System for the protection of whistleblowers or publicly disclosing information about violations

Obligated entities

Obligated entities

The main functions of all obligated entities are:

- Build a Channel for internal reporting of signals;
- Appoint an officer to consider signals;
- Communicate with whistleblowers;
- Maintain a Register of submitted signals;
- Communicate with CAERS.

Central authority for external reporting

The Central Authority for External Reporting performs:

- Builds a Channel for External Reporting of Signals (CERS);
- Checks signals and sends them according to competence;
- Maintains a Register of signals;
- Considers publicly disclosed information as a signal, if there is information about it in the Central Security Service;
- Point of contact with EU institutions, bodies, services and agencies;
- Submits aggregated statistical data to the European Commission;
- Gives methodical instructions, carries out training and control.

Authorities

The competent authorities are:

1. The Commission for the Protection of Competition;
2. The Financial Supervision Commission;
3. The chairperson of the State Agency for Metrological and Technical Supervision;
4. The Minister of Transport and Communications;
5. The Minister of Environment and Water;

6. The chairperson of the Nuclear Regulation Agency;
7. The Bulgarian Food Safety Agency;
8. The chief state health inspector within the meaning of the Health Act;
9. The Consumer Protection Commission;
10. The National Computer Security Incident Response Team;
11. The Minister of Finance;
12. The executive director of the National Revenue Agency;
13. The executive director of the Executive Agency "Main Labor Inspectorate";
14. Regional governors.

Competent authorities within their powers:

- Carry out checks on reports of violations;
- Inform CAERS about the results of the inspection;
- Comply with the instructions of the CAERS.

Ombudsman of the Republic of Bulgaria

The Ombudsman of the Republic of Bulgaria:

- Performs an external audit of the CAERS;
- Performs inspection of the CERS;
- Accepts and examines complaints against the Central Authority for External Reporting of Signals.

Reporting channels

Types of data feed channels

Data submission channels are:

- Internal reporting channel;
- Channel for external submission of signals;
- Public disclosure of information considered an External Whistleblower Channel.

Requirements for Data Submission Channels

Data feed channels provide:

- Confidentiality, integrity and availability of information;
- Permanent archiving;
- Audit and update of operating rules.

Violation report

Signal form

A form is used to register the report, which contains at least the following data:

1. The sender's three names, address and phone number, as well as an email address, if any;
2. The names of the person against whom the report is filed and his workplace, if the report is filed against specific persons and they are known;
3. Specific details of a violation or of a real danger that it will be committed, place and period of the violation, if it was committed, a description of the act or the situation and other

circumstances, as far as these are known to the reporting person;

4. Date of submission of the signal;
5. Signature, electronic signature or other identification of the sender.

Signal register

For accountability and control, a non-public register of reports of violations is created and maintained. The register contains information about:

1. The person who received the signal;
2. The date of submission of the signal;
3. The affected person, if such information is contained in the report;
4. Summary data on the alleged violation, such as place and period of commission of the violation, description of the act and other circumstances under which it was committed;
5. The connection of the transmitted signal with other signals after the establishment and in the process of processing the signal;
6. Information that was provided as feedback to the person who submitted the report and the date of provision and;
7. The follow-up actions taken;
8. The results of the check on the signal;
9. The signal storage period.

Synchronization of signal information

For the synchronization of information about the signal, the form of the signal and the way of keeping the register, the CSIRO:

- Issues a Unique Identification Number (UIN) for each received signal;
- Approves a sample of the Signal Form;
- Determines by Ordinance, the order and manner of keeping the Register of signals
- Issues instructions on the structure and content of the Signal file and the methods of performing the verification on the signal.

3. PROTECTION OF INDIVIDUALS SUBMITTING SIGNALS OR PUBLICLY DISCLOSING INFORMATION ABOUT VIOLATIONS

Privacy and personal protection measures include:

- Protection of information;
- Protection of whistleblowers' identity;
- Prohibition of retaliatory actions against whistleblowers;
- Mandatory orders to stop the damaging actions;
- Right to compensation for property and non-property damages suffered;
- Exemption from liability.

4. CONCLUSION

The proposed multi-layered model of the Whistleblower Protection System is a theoretical basis for the construction and functioning of the WBPS. It is the basis for modeling and synchronizing the interactions between the structural units of the Model.

Interactions are subject to formalization and analysis:

- Officer for consideration of the report – person submitting the report;
- Officer for consideration of the signal - supporting and related persons;
- Officer for consideration of the signal – legal entities related to the person submitting the report;
- Officer for consideration of the signal - CAERS;
- CAERS - CERS;
- CAERS – competent authorities;
- CAERS - CCCCIAP;
- CAERS – Prosecutor's Office of the Republic of Bulgaria;
- CAERS – European Commission;
- CAERS - Institutions, bodies, services and agencies of the EU;
- CAERS - Persons who are granted protection:
 - CAERS - Reporting persons (reporting person);
 - CAERS - Persons publicly disclosing information;
 - CAERS - Supporting and related persons;
 - CAERS - Legal entities in which the whistleblower has a shareholding, for which he works or with which he is otherwise connected in a work context;
- Ombudsman of the Republic of Bulgaria - CAERS.

The report summarizes the author's experience in building the personal data protection system and the whistleblower protection system. The report reflects the author's experience as a member of the Commission for the Protection of Personal Data, Central Body for External Whistleblowers. The report also contains part of the research done by the author at the University of Library Science and Information Technology.

5. REFERENCES

1. Law on the Protection of Persons Reporting or Publicly Disclosing Information on Violations, SG No. No. 11 of February 2, 2023
2. Directive 2019/1937 (the so-called Whistleblower Directive)
3. Treaty on the Functioning of the European Union of December 13, 2007

Safety and security measures during transportation of dangerous goods class 7 (radioactive materials), taking into account the requirements of ADR

Lyudmil N. Nedelchev¹, Dimitar L. Dimitrov²

Institute for Nuclear Research and Nuclear Energy, Bulgarian Academy of Sciences¹

Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria²

lnedelchev@npp.bg, ddimitrov@ims.bas.bg

Abstract: Providing a VVER-1000 type NPP with the required amount of Fresh Nuclear Fuel (FNF) for any Nuclear Reactor System (NRS) energy campaign is of primary importance and is an element of the security of supply and the reliable operation of a NPP. According to the definitions in the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), FNF is dangerous cargo because it contains substances that are permitted for road transportation only under certain conditions. The transportation of FNF on Bulgaria's roads is carried out in strict compliance with the requirements of ADR.

KEYWORDS: NUCLEAR FACILITIES, PROTECTION OF NUCLEAR INSTALLATIONS, FRESH NUCLEAR FUEL (FNF), INTERNATIONAL CARRIAGE OF DANGEROUS GOODS BY ROAD (ADR)

1. Introduction

The fundamental goal of capacity building is to enhance the abilities of relevant stakeholders to assess, establish and implement elements of a nuclear security regime.

The infrastructure needed for capacity building includes, among many other things, educational and training institutes with personnel competent in nuclear security, technical support centres, nuclear security laboratories and equipment, and the means to produce appropriate course materials.

In addressing how to build the capacity to establish, implement and sustain a nuclear security regime, it is necessary to look at the essential elements that should be in place and the underlying functions that make a security programme effective. The Nuclear Security Fundamentals [1] set out different essential elements of a nuclear security regime.

Capacity building programmes need to be tailored to the national infrastructure and resources that are available, but also to address these important and essential elements.

Taking into account importance of the problem, the European Agreement on the international transportation of dangerous goods by road ADR [2, 3] was adopted in Geneva on 30 September 1957 under the auspices of the United Nations Economic Commission for Europe and came into effect on 29 January 1968.

It was subsequently and repeatedly amended and supplemented. Currently, the ADR structure is aligned with the UN Recommendations on the Transport of Dangerous Goods, the International Maritime Dangerous Goods Code (IMDG Code) and the Regulation concerning the International Carriage of Dangerous Goods by Rail (RID).

2. Organizational and technical safety measures when transporting radioactive materials.

2.1. Purpose

The purpose of the ADR agreement is to ensure the protection of people, property and the environment from the effects of radiation when transporting dangerous goods of Class 7 (containing radioactive substances).

This protection is achieved by:

- sealing the radioactive contents;
- control of external radiation levels;
- prevention of a state of criticality;
- prevention of damage caused by thermal effects.

The transportation of radioactive material must be carried out in accordance with a radiation protection program, which consists of systematic prescriptions aimed at due compliance with radiation protection measures.

The nature and extent of the measures provided for in the program must be related to the degree and likelihood of radiation exposure. The following requirements form an integral part of the program:

- radiation doses must be below the permissible limit;
- when monitoring people or workplaces, appropriate documentation must be kept;
- workers must undergo appropriate radiation protection training.

2.2. Transportation of dangerous goods

Any enterprise whose activities involve the transportation of dangerous goods by road or related activities of packing, loading, filling or unloading of dangerous goods, must appoint one or more dangerous goods transportation safety consultant whose task is to help prevent the risks, inherent in these activities, to the public, to the various types of property or to the environment.

The safety consultant's duties more specifically are as follows:

- to monitor the compliance with the requirements governing the transportation of dangerous goods;
- to consult the enterprise on the transportation of dangerous goods;
- to submit to the management of the enterprise or to the local public authority an annual report on the enterprise's activities involving the transportation of dangerous goods;
- to monitor the procedures for compliance with the requirements concerning the identification of the transported dangerous goods;
- to monitor the enterprise's practice, when purchasing new vehicles, of taking into account the special requirements for transporting dangerous goods;
- to monitor the procedures for the inspection of equipment used for the transportation, loading and unloading of dangerous goods;
- to monitor the availability of appropriate and responsible training of the employees and the workers in the enterprise and the keeping of records of this training;
- to implement emergency procedures in the event of an accident and/or incident;
- to investigate and, if necessary, to report any serious accident, incident or serious violation documented during the transportation, loading or unloading of dangerous goods;

- to take appropriate measures to prevent the recurrence of accidents, incidents or serious infringements;
- to comply with the regulatory provisions and special requirements for the transportation of dangerous goods when selecting and using subcontractors or third parties;
- to check that all employees and workers involved in the transportation, loading and unloading of dangerous goods have detailed working instructions;
- to introduce measures to increase the knowledge on the risks inherent in the transportation, loading and unloading of dangerous goods;
- to introduce procedures for checking that vehicles carry the safety documentation and equipment which must accompany transport shipments and that these documents comply with the regulatory requirements;
- to monitor the availability of a security program (plan).

2.3. Technical measures for transportation of Fresh Nuclear Fuel (FNF).

The delivery of fresh nuclear fuel (FNF) for the VVER- 1000 type Nuclear Reactor System (NRS) is usually carried out using transport packaging containers (TPK) of the TK-C5-B type.

According to the TPK certificate, the package identification is RUS/3014/IF-96 and the UN classification cargo designation is UN number UN 3324 Low Specific Activity Radioactive Material Group 2 (LSA-II), fissile.

The materials that are defined as Low Specific Activity ones (LSA-II) must meet the following condition:

- when the activity is distributed throughout the substance, the calculated average specific activity must not exceed $10^{-4} \text{ A}_2/\text{g}$ according to item 2.2.7.2.3.1.2. of ADR, where the permissible value of A_2 for neutron emitting nuclides is up to $9 \times 10^{-5} \text{ TBq}$, according to table. 2.2.7.2.2.2. of ADR - Basic radionuclide values for unknown radionuclides or mixtures.

- according to [4, 5], the approximately determined activity A of a fresh heat releasing cartridge with 4.4% enriched U^{235} is 0.5 Ki , which means that the specific activity $a[\text{Bq/g}]$ is $a = A/m = 18.5 \text{ GBq} / 500 \text{ kg} = 0.037 \text{ GBq/kg} = 37 \text{ Bq/g}$, where the mass of the radioactive substance (here nuclear fuel) m is approximately 500kg.

On the other hand, the permissible value of the specific activity is $a_{\text{perm}} = 9 \times 10^{-5} \text{ TBq} \times 10^{-4} = 9 \times 10^{-9} \text{ TBq} = 9 \text{ KBq/g}$.

Therefore, $a_{\text{perm}} > a$ ($9 \text{ KBq/g} > 37 \text{ Bq/g}$).

This means that the considered radioactive material Fresh Nuclear Fuel (FNF) can be transported safely using the proposed transport packaging in accordance with the requirements of ADR.

3. Measures to ensure transportation security

3.1. Security program (plan).

Carriers, freight forwarders and other participants in the transportation of high-risk dangerous goods (including radioactive material) are required to adopt and effectively implement security-related plans that cover at least the following elements:

- specific assignment of security-related responsibilities to persons equipped with knowledge and qualifications and having the necessary powers;
- recording and reporting of the relevant dangerous goods;
- assessment of the current operations and the resulting security risks, including stoppages and instances of the dangerous goods remaining in the transport vehicles due to the conditions of the transportation and/or the specific road conditions;

- a clear presentation of the measures to be taken to reduce security risks;
- effective and up-to-date procedures for reporting and countering threats, security breaches and other incidents;
- procedures for evaluating and verifying security plan, as well as the procedures for periodical reviews and updating of the programs;
- measures to ensure the physical protection of the transportation information contained in the security plan;
- measures to guarantee that access to the shipping information contained in the security plan is allowed only to persons who need that information.

For the purpose of exchanging information on possible threats, the carriers, consignors and consignees should cooperate with each other and be prepared to implement appropriate security measures and to respond to security threats.

3.2. Road transportation safety measures.

Prior to the road transportation of the radioactive material, it is necessary to carry out the following:

- all critical points must be determined ;
- the local traffic police must be notified about the transport transit time;
- the vehicles must move in a column signaled in accordance with the Road Traffic Regulations and observing the maximum speed set by the Nuclear Regulation Agency (NRA) for the specific transport and route;
- traffic police posts must be placed at all intersections to block the movement of vehicles, people and animals along the column route;
- the column must be headed by a traffic police vehicle;
- at a distance of 1 km in front of the column, a pilot car must move ahead to explore the road and notify the column in good time of any obstacle;
- the transport vehicles must be escorted by NPP Departmental Security vehicles and a specialized vehicle equipped as necessary to measure and control the radiation situation;
- the drivers of the column vehicles must receive instructions on the specific features of the route and the critical points and must know the regulations for communication with each other, with the NPP Departmental Security and with the traffic police authorities.

4. Interfaces with nuclear safety

Nuclear security and safety have the common aim of protecting persons, property, society and the environment. Security and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that security measures do not compromise safety and safety measures do not compromise security [1].

When building the capacity for nuclear security, there will be direct interfaces with nuclear safety. In addition, there may be interfaces with nuclear safeguards such as in nuclear material accounting and control.

In practical terms, this means that there are likely to be many areas where building the capacity of regulators or operators can follow a common approach. In some cases, basic competences may be the same (e.g. using equipment for detection, and identification of radioactive material). In other cases, the individuals may be the same (e.g. inspectors having responsibilities in both safety and security).

Furthermore, a person with an education and experience in nuclear safety may work in nuclear security or safeguards for some portion of their career.

A major interface where capacity building may overlap is in emergency management. Safety and security will both be major considerations in addressing nuclear or radiological emergencies arising from nuclear security events.

Although preparedness and response for a nuclear security event is different from that for a nuclear or radiological emergency, the response arrangements need to have the capacity to work together seamlessly for the protection of the public and the environment [6].

The capacity to implement a nuclear security regime rests largely in countries laws and regulations, its organizations and the people in those organizations.

Consequently, these also affect, either directly or indirectly, the implementation of safety and material accounting and control, especially at nuclear facilities.

Therefore, the capacity that is developed at the regulatory and facility level should take into consideration how security will be applied and how this interfaces with other programmes such as safety.

For example, if there is a single regulatory body for safety and security, then that regulator might share resources for its rulemaking, inspection and enforcement. These resources represent the capacity of the regulator to perform its duties.

As another example [7], a nuclear facility operator needs to implement all requirements for safety, security and nuclear material accounting.

Therefore, it is most effective and efficient if the management systems, procedures and personnel at the facility are designed to take maximum advantage of shared facilities, equipment and resources and to work together to achieve their respective goals (to the extent possible, taking into consideration the differences between these areas).

4. Conclusions

The transportation of Class 7 dangerous goods on the roads of Europe is a highly responsible activity where compliance with the regulatory requirements of ADR is mandatory.

First and foremost come the technical safety measures, such as the availability of properly selected packaging for the transportation of the specific material, availability of a certificate of intended use and shelf life of the packaging and details of the design algorithm and tests carried out on the packaging during manufacture

Secondly, but no less important, is the existence and the implementation of a program (plan) for security during transportation.

The development of such a program is a specific activity requiring competences in the fields of security management, public order protection, traffic control, and operational combat training and police systems organization.

A professionally prepared security program is a good prerequisite for securing the road transportation of Class 7 materials (according to the requirements of ADR) in normal and emergency situations related to natural disasters, malicious acts or the threat of radioactive (nuclear) terrorism.

Building capacity for nuclear security should be undertaken via a systematic approach that includes provisions for assessment, planning, implementation, documentation, evaluation and feedback.

This approach should be developed as part of a national security policy and implementation strategy. Before initiating the approach, the government should decide which organizations should coordinate the approach at the national level.

Furthermore, each organization with responsibilities should assign a unit to perform the necessary work.

Building the capacity of organizations and people to establish, implement and sustain a nuclear security regime is an essential responsibility of an each country.

Analysis of national nuclear security needs and existing infrastructure should drive the development of capacity building programmes to combat the threat of sabotage or the use of nuclear or other radioactive material for malicious acts, and to prepare effective response measures to nuclear security events.

Bibliography

[1]. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2]. United Nations, European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), Volume 1, 2017, New York and Geneva, 2016.

[3]. United Nations, European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), Volume 2, 2017, New York and Geneva, 2016.

[4]. В.Д.Шмелев, Ю.Г.Драгунов, В.П.Денисов, Активные зоны ВВЭР для атомных электростанций, ИКЦ "Академкнига", 2004г., Москва,

[5]. В.К.Резепов, Н.А.Кирилук, В.П.Денисов, Активные зоны ВВЭР для атомных электростанций, ИКЦ "Академкнига", 2004г., Москва

[6]. Пъневски В. С., "Възможни специфични изисквания към проектирането на мехатронни системи за сигурност и защита на критична инфраструктура", Сборник доклади от Научна конференция „Актуални проблеми на сигурността“, 22-23 октомври 2020 г., 6, Издателски комплекс на НВУ „Васил Левски“, 2020, ISSN:2367-7465, стр. 84-90;

[7]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Culture in Nuclear Installations: Guidance for Use in the Enhancement of Safety Culture, IAEA-TECDOC-1329, IAEA, Vienna (2002).

Safety and security measures during transportation of dangerous goods class 7 (radioactive materials), taking into account the requirements of ADN

Lyudmil N. Nedelchev¹, Dimitar L. Dimitrov²

Institute for Nuclear Research and Nuclear Energy, Bulgarian Academy of Sciences¹

Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria²

lnedelchev@npp.bg, ddimitrov@ims.bas.bg

Abstract: One of the main continuous processes occurring in the operation of a nuclear power plant (NPP) is the normal provision of the Nuclear Fuel Cycle (NFC). The NFC includes all activities performed with Nuclear Fuel (NF) from the time of uranium mining and includes enrichment, fabrication of fuel assemblies, transportation, operation in a reactor plant as well as processing, disposal, storage or disposal of Spent Nuclear Fuel (SNF). The storage and reprocessing or disposal of SNF is the subject of a national strategy for the use of nuclear fuel. In most versions of the nuclear fuel strategies, transport of certain quantities of SNF from the reactor to the designated storage, processing or disposal site is envisaged. This transport may range from a few hundred meters to thousands of kilometers. In practice, land and water transport are mainly used. In both cases, the transport must be carried out in strict compliance with all safety and security requirements

KEYWORDS: NUCLEAR FACILITIES, PROTECTION OF NUCLEAR INSTALLATIONS, SPENT NUCLEAR FUEL (SNF), INTERNATIONAL CARRIAGE OF DANGEROUS GOODS BY INLAND WATERWAYS (ADN)

1. Introduction

According to the definitions in the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN), SNF is dangerous goods (radioactive material class 7), as it contains substances which are only permitted for carriage by inland waterways under certain safety conditions. Inland waterways in this case means all stretches of navigable rivers in the European Community that are used for navigation. The ADN Agreement does not apply to sea and ocean waterways used for navigation.

The European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN) [1,2] was done at Geneva on 26 May 2000 under the auspices of the United Nations Economic Commission for Europe and the Central Commission for Navigation on the Rhine. It entered into force on 29 February 2008.

The Regulations applied to the ADN contain provisions relating to dangerous substances and articles, their carriage in packages and in bulk on board inland waterway vessels or tankers, and also provisions relating to the construction and operation of these vessels.

Member States of the United Nations Economic Commission for Europe (UNECE) in whose territories inland waterways are situated (excluding coastal routes) may also become Contracting Parties to the Agreement by joining it, provided that these inland waterways form part of the network of waterways of international importance as defined by the European Agreement on Main Inland Waterways of International Importance (AGN).

2. Organizational and technical safety measures when transporting radioactive materials.

2.1. Purpose of the ADN

The purpose of the ADN agreement is to ensure the protection of people, property and the environment from the effects of radiation when transporting dangerous goods of Class 7 (containing radioactive substances). This protection is achieved by:

- sealing the radioactive contents;
- control of external radiation levels;
- prevention of a state of criticality;
- prevention of damage caused by thermal effects.

The transportation of radioactive material must be carried out in accordance with a radiation protection program, which consists of

systematic prescriptions aimed at due compliance with radiation protection measures.

The nature and extent of the measures provided for in the program must be related to the degree and likelihood of radiation exposure. The following requirements form an integral part of the program:

- the individual radiation doses must be below the permissible limit;
- the individual dosimetry monitoring of workplaces and/or personnel must be appropriately documented;

The workers must undergo appropriate radiation protection training, including the precautions they need to take to limit occupational exposure of personnel and others who may be affected by their actions.

2.2. Carriage of dangerous goods

Any enterprise whose activities involve the carriage of dangerous goods by inland waterways or related activities of packing, loading, filling or unloading of dangerous goods, must appoint one or more dangerous goods transportation safety consultants whose task is to help prevent the risks, inherent in these activities, to the public, to the various types of property or to the environment. The safety consultant's duties more specifically are as follows:

- to monitor the compliance with the requirements governing the transportation of dangerous goods;
- to monitor the existence of a Security Program (Plan);
- to consult its enterprise on the transportation of dangerous goods;
- to submit to the management of the enterprise or to the local public authority an annual report on the enterprise's activities involving the transportation of dangerous goods.

This report shall be kept for five years and made available to the national authorities upon request;

- to monitor the procedures for compliance with the requirements concerning the identification of the transported dangerous goods;
- to provide appropriate training of the employees and the workers in the enterprise and the keeping of records of this training;
- to monitor the enterprise's practice, when purchasing new vehicles, of taking in to account the special requirements for transporting dangerous goods;
- to monitor the procedures for the inspection of equipment used for the transportation, loading and unloading of dangerous goods;
- to implement emergency procedures in the event of an accident and/or incident;

- to investigate and, if necessary, to report any serious accident, incident or serious violation documented during the transportation, loading or unloading of dangerous goods;
- to take appropriate measures to prevent the recurrence of accidents, incidents or serious infringements;
- to comply with the regulatory provisions and special requirements for the transportation of dangerous goods when selecting and using subcontractors or third parties;
- to check that all employees and workers involved in the transportation, loading and unloading of dangerous goods have detailed working instructions;
- to introduce measures to increase the knowledge on the risks inherent in the transportation, loading and unloading of dangerous goods;
- to introduce procedures for checking that vehicles carry the safety documentation and equipment which must accompany transport shipments and that these documents comply with the regulatory requirements;
- to monitor the availability of a security Program (Plan).

2.3. Technical measures for transportation of Spent Nuclear Fuel (SNF).

The transportation of the SNF for the VVER- 1000 type Nuclear Reactor System (NRS) is usually carried out using transport packaging containers (TPK) of the TUK-13/1B type.

According to the TPK certificate, the package identification is RUS/3014/IF-96 and the UN classification cargo designation is UN 3328 Radioactive Material, type B (U) package, fissile.

According to paragraph 2.2.7.2.4.6.2. of ADR, the content of a type B (U) package shall be as specified in the certificate of approval.

The package must not contain:

- materials with activities greater than those authorized for the package design and specified in the certificate of approval;
- radionuclides other than those authorized for the package design and specified in the certificate of approval;
- ingredients in a form or in a physical and chemical state other than those authorized for the package design and specified in the certificate of approval.

In this particular case, the TUK-13/1B package was designed for maximum activity values of $2.44 \cdot 10^{17}$ Bq[5], when filled with 12 spent fuel cassettes. The radioactive contents could be heat-separating spent fuel cassettes (HSSFC) from VVER-1000 reactors. The HSSFC must meet the technical conditions "Heat-separating spent fuel cassettes from nuclear power reactors VVER-1000 of Kozloduy NPP."

In the table below is given the average activity by isotopes and the total activity of 12 pcs. HSSFCs from VVER-1000 containing U^{235} over isotope enriched on average to 3.3%, after having worked over four operating campaigns and then aged about ten years in a wet storage facility [6].

The weight of the metal in an HSSFC is approximately 420 kg and its average activity is about $5.02 \cdot 10^{15}$ Bq [3,4].

Therefore, the total activity is less than the maximum allowable activity value for which the package is designed ($0.602 \cdot 10^{17} < 2.44 \cdot 10^{17}$) and the radioactive material under consideration (Spent Nuclear Fuel) can be transported safely in the proposed transport package TUK-13/1B according to the requirements of ADR.

Isotope	Ratio of activity relative to the total one	Relative activity. [Bq]
Am241	$1.04 \cdot 10^{-02}$	$6.24 \cdot 10^{14}$
Ba137	$2.18 \cdot 10^{-01}$	$1.31 \cdot 10^{16}$
Ce144	$1.22 \cdot 10^{-07}$	$7.35 \cdot 10^{09}$
Cm244	$5.03 \cdot 10^{-03}$	$3.03 \cdot 10^{14}$
Cs134	$8.46 \cdot 10^{-04}$	$5.09 \cdot 10^{13}$
Cs137	$2.31 \cdot 10^{-01}$	$1.39 \cdot 10^{16}$
Eu154	$4.93 \cdot 10^{-03}$	$2.97 \cdot 10^{14}$
Eu155	$8.26 \cdot 10^{-04}$	$4.97 \cdot 10^{13}$
H3	$2.61 \cdot 10^{-07}$	$1.57 \cdot 10^{10}$
Kr85	$1.12 \cdot 10^{-02}$	$6.77 \cdot 10^{14}$
Pm147	$3.36 \cdot 10^{-03}$	$2.02 \cdot 10^{14}$
Pr144	$1.22 \cdot 10^{-07}$	$7.35 \cdot 10^9$
Pu238	$8.99 \cdot 10^{-03}$	$5.41 \cdot 10^{14}$
Pu239	$1.16 \cdot 10^{-03}$	$7.00 \cdot 10^{13}$
Pu240	$1.74 \cdot 10^{-03}$	$1.05 \cdot 10^{14}$
Pu241	$1.94 \cdot 10^{-01}$	$1.17 \cdot 10^{+16}$
Rh106	$3.77 \cdot 10^{-06}$	$2.27 \cdot 10^{11}$
Ru106	$3.77 \cdot 10^{-06}$	$2.27 \cdot 10^{11}$
Sb125	$2.33 \cdot 10^{-04}$	$1.40 \cdot 10^{13}$
Sm151	$8.77 \cdot 10^{-04}$	$5.28 \cdot 10^{13}$
Sr90	$1.54 \cdot 10^{-01}$	$9.30 \cdot 10^{15}$
Te125	$5.70 \cdot 10^{-05}$	$3.43 \cdot 10^{12}$
Y90	$1.54 \cdot 10^{-01}$	$9.30 \cdot 10^{15}$
Total activity: $6.02 \cdot 10^{16}$ Bq		

3. Measures to ensure transportation security

3.1. Security program (plan).

Carriers, freight forwarders and other participants in the transportation of high-risk dangerous goods (including radioactive material) are required to adopt and effectively implement security-related plans that cover at least the following elements:

- specific assignment of security-related responsibilities to persons equipped with knowledge and qualifications and having the necessary powers;
- recording and reporting of the relevant dangerous goods;
- assessment of the current operations and the resulting security risks, including stoppages and instances of the dangerous goods remaining in the transport vehicles due to the conditions of the transportation and/or the specific road conditions;
- a clear presentation of the measures to be taken to reduce security risks;
- effective and up-to-date procedures for reporting and countering threats, security breaches and other incidents;
- procedures for evaluating and verifying security plan, as well as the procedures for periodical reviews and updating of the programs;

- measures to ensure the physical protection of the transportation information contained in the security plan;

- measures to guarantee that access to the shipping information contained in the security plan is allowed only to persons who need that information.

For the purpose of exchanging information on possible threats, the carriers, consignors and consignees should cooperate with each other and be prepared to implement appropriate security measures and to respond to security threats.

Carriers, freight forwarders and other participants in the transportation of high-risk dangerous goods (including radioactive material) are required to adopt and effectively implement security-related plans that cover at least the following elements:

- specific assignment of security-related responsibilities to persons equipped with knowledge and qualifications and having the necessary powers;

- recording and reporting of the relevant dangerous goods;

- assessment of the current operations and the resulting security risks, including stoppages and instances of the dangerous goods remaining in the transport vehicles due to the conditions of the transportation and/or the specific road conditions;

- a clear presentation of the measures to be taken to reduce security risks;

- effective and up-to-date procedures for reporting and countering threats, security breaches and other incidents;

- procedures for evaluating and verifying security plan, as well as the procedures for periodical reviews and updating of the programs;

- measures to ensure the physical protection of the transportation information contained in the security plan;

- measures to guarantee that access to the shipping information contained in the security plan is allowed only to persons who need that information.

For the purpose of exchanging information on possible threats, the carriers, consignors and consignees should cooperate with each other and be prepared to implement appropriate security measures and to respond to security threats.

3.2. Safety measures for water transportation of SNF

Prior to the water transportation of the spent radioactive material, it is necessary to ensure:

- Documents proving the serviceability and seaworthiness of the vessel as well as of the cargo facilities of the ports involved in the transport;

- Documents indicating that the vessel is authorized to carry Class 7 cargo (radioactive materials);

- Documents indicating the capability of specific ports to handle Class 7 cargo;

- Existence of an emergency plan to deal with emergencies on board the vessel carrying class 7 radioactive materials;

- Document certifying that all crew members are familiar with the emergency plan in force;

4. Risk associated with the use of nuclear material and nuclear facilities

There are well known risks associated with the use of nuclear material and nuclear facilities. From a nuclear security perspective the two primary risks are those associated with unauthorized removal of nuclear material, for potential use in a nuclear explosive device, and with sabotage of the material and/or facility resulting in Unacceptable Radiological Consequences (URC).

The management of these risks is the primary basis for nuclear security in relation to nuclear material and nuclear facilities.

If a country has made the decision to accept nuclear material and nuclear facilities within its borders, it is also accepting the responsibility to protect those materials from unauthorized removal and the facilities and materials from sabotage resulting in a release of radionuclides.

The country's physical protection regime should be reviewed and updated regularly to reflect changes in the threat and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of nuclear material and nuclear facilities.

Nuclear facilities have often been designed without giving sufficient consideration to nuclear security until late in the design stage or after operational and safety features had already been determined.

Nuclear security measures were added later, often resulting in the application of measures that were not integrated or fully compatible with measures relating to safety, safeguards, and operations.

Moreover, implementing new or additional security measures after a nuclear facility is in operation may be difficult and costly. Considering security requirements early in new designs, partial redesigns and modifications can result in nuclear security that is more efficient and effective as well as better integrated with other measures in the facility.

4. Conclusions

The carriage of Class 7 dangerous goods according to the requirements of ADN on the inland waterways of Europe is a highly responsible activity where compliance with the regulatory requirements of ADN is mandatory.

First and foremost come the technical safety measures, such as the availability of properly selected package for the transportation of the specific material, availability of a certificate of intended use and shelf life of the package and details of the design algorithm and tests carried out on the package during manufacture.

Secondly, but no less important, is the existence and the implementation of a program (plan) for security during transportation.

The development of such a program is a specific activity requiring competences in the fields of security management, public order protection, traffic control, and operational combat training and police systems organization.

A professionally prepared security program is a good prerequisite for securing the transportation on the inland waterways of Europe of Class 7 materials (according to the requirements of ADN) in normal and emergency situations related to natural disasters, malicious acts or the threat of radioactive (nuclear) terrorism.

Bibliography

- [1]. United Nations. European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways – AND, Vol. 1, Geneva, 2008.
- [2]. United Nations. European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways – ADN, Vol. 2, Geneva, 2008.
- [3]. В.Д. Шмелев, Ю.Г. Драгунов, В.П. Денисов, Активные зоны ВВЭР для атомных электростанций, ИКЦ “Академкнига”, 2004г., Москва
- [4].] В.К. Резепов, Н.А. Кирилук, В.П. Денисов, Активные зоны ВВЭР для атомных электростанций, ИКЦ “Академкнига”, 2004г., Москва
- [5]. Certificate-approval for packag's construction and for transportation. Transport equipment TUK-13/1B for spent nuclear fuel from VVER-1000 reactors.
- [6]. Съхраняване на ядрено гориво-технология и опит. Е. Вапирев, И. Христосков

Maritime piracy and armed robbery evolution in 2008-2022

Adelina Tumbarska

Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski",
Bulgarian Academy of Sciences (IMSETHAC – BAS), Sofia, Bulgaria
E-mail: y.toumbarski@ims.bas.bg

Abstract: Maritime crime (piracy and armed robberies against vessels) are challenges to the shipping that have global impact on maritime trade and security. The evolution of this phenomenon is a dynamic process which is characterized by rapid changes both in terms of the number and severity of incidents and in their geographical concentration. This study traces the development of maritime crime over the past 15 years, divided into three 5-year periods. It is performed by analyzing the data collected and published by the International Maritime Bureau, concerning the number, character and location of incidents for the 2008-2022, in order to outline the trends in the contemporary sea piracy and armed robbery.

Keywords: MARITIME PIRACY, MARITIME ARMED ROBBERY

1. Introduction

The boom in pirate attacks in the late first and early second decade of the 21st century attracted considerable attention. Due to the significant economic impact and the human cost of pirate attacks, this phenomenon has become one of the serious challenges facing global maritime trade and security. Currently, as a result of international efforts, pirate attacks in the hottest spots such as the Gulf of Aden and off the coasts of Somalia, and later in the Gulf of Guinea, have been reduced to almost zero level. At the same time, in other regions the number of incidents (mostly armed robberies) has increased rapidly. Since the dynamics of maritime crimes is quite erratic and dependent on a number of factors, it can be said that the development of piracy in the long run is very difficult to predict.

The present study is based on statistical data taken from the annual piracy and armed robbery reports of the International Maritime Bureau (IMB) for a period of 15 years [1] - from 2008 to 2022 included. Data are grouped and analyzed for three 5-year periods: 1) 2008-2012 – the peak of piracy activity (with the boom of Somali piracy); 2) 2013-2017 – a period of significant decline in piracy attacks (after the almost complete eradication of Somali piracy); 3) 2018-2022 - a period with the lowest levels of incidents in the last few decades. This study is a continuation of the author's previous research [2, 3] for 2008-2017, to which the data for the next 5 years are added. The number, character and location of incidents for the three periods are analyzed within the individual periods, and then compared by periods, in order to outline the trends in the evolution of sea piracy and armed robbery over the past 15 years.

2. Definitions and types of pirate attacks

Maritime crime is generally divided into two categories - armed robbery and piracy, which are often confused, so it is necessary to clarify the differences between the two types of crime. Various definitions are found in the literature, which will not be cited here due to the limited volume of this publication.

Generally, the similarity between the two types of crime is that criminals board a vessel with the intent of committing a robbery or other crime by using threats and weapons.

An essential difference between these categories is that armed robbery takes place within a State's internal waters, archipelagic waters and territorial sea, while piracy is committed on the high seas, outside the jurisdiction of any State.

Another difference is the ultimate goal of the attack, as well as the way it is prepared and executed. Maritime armed robbery is quite similar to the armed robbery on shore. These attack, as a rule, are opportunistic, occurring when the vessel is anchored. Criminals are most often armed with knives and can easily convince unarmed people on board to part with their money and belongings. Kidnapping is rare and is for the purpose of an easier retreat from the scene of a crime, not a ransom demand. Unlike these low-cost

and low-risk crimes, piracy attacks are usually preceded by detailed intelligence for the targeted vessel (route, crew, presence of armed guards, security measures on board, etc.) and are carried out mostly underway. Pirates are equipped with modern means of communication to locate vessels far in the sea, high-speed boards (often with logistics provided by "mother-ships"), and heavy armament. Additionally, pirates use organized shore support to unload and sell cargo, repaint and sell stolen vessels, negotiate ransoms, receive and "launder" ransom money, etc.

The term "piracy" covers two different types of crime: the first is robbery or *hijacking*, where the purpose of the attack is to steal the ship or its cargo; the second is *kidnapping*, where the ship and crew are held captive until a ransom is paid.

Because of the high "stakes" and the difficulty of capturing a ship while underway, especially if the crew resists, such operations can be accompanied by a high level of violence both during the attack itself and after the successful capture of the ship.

The incidents categorization in accordance to their effect on crew, vessel and cargo, proposed by the (IMB) [1], includes 3 levels: *Level I*: accidents which have direct impact on crew: crew being taken hostage, injured, kidnapped, killed, missing, threatened; *hijacking* where the command of the ship is taken over by those boarding; accidents where the crew retreats into the citadel; *Level II*: includes a vessel being fired upon, security team firing against approaching threat, robbers/pirates identified with weapons (violence is offered) whether boarding or otherwise; *Level III*: incidents which does not fall into either Level I or Level II.

3. Discussion of statistical data

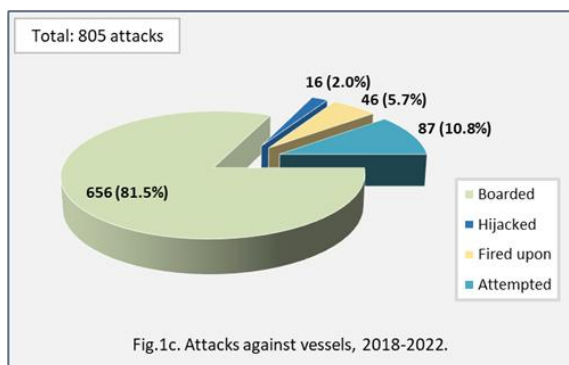
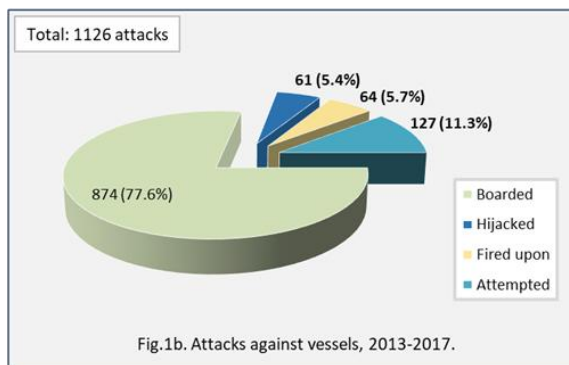
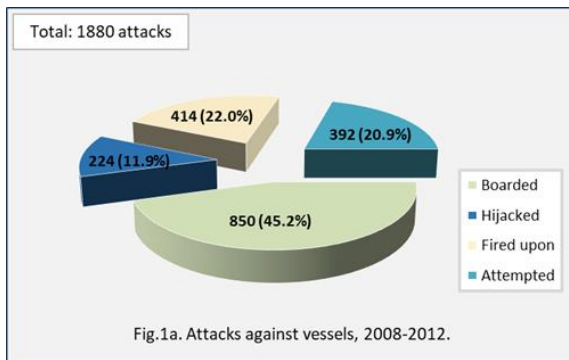
3.1. Attacks against vessels and crew members

The number and types of attacks against vessels are presented in Table 1 and Fig.1; the number and types of violence to crew are presented in Table 2 and Fig.2.

The first period (2008-2012), is characterized by a significant share of hijacking ships and keeping crew as hostages. This is mostly due to the boom of piracy in the Gulf of Aden and off Somalia coast which almost always involved hostage situations, often long lasting (an average 6 months to get large ransoms). These attacks have been carried out with patience and strategy and have been largely free of violence because it was in the pirates' interest to keep their hostages alive. [4] In the Gulf of Guinea, pirates usually hijacked ships (mostly oil tankers) for several days and after stealing the cargo, sailors were released. In Southeast Asia, piracy was focused on the ransacking cargo and fishing products from vessels like tugs, trawlers and passenger boats. Hijacking occurred mostly in Malaysia, Indonesia and Strait of Malacca, where attacks was aimed mostly in hijacking slow-moving tankers to steal the oil from but rarely seek to ransom the crew. In some of these cases crew members have been injured and the ship equipment - heavily damaged.

Table 1. Number and types of attacks against vessels

Type of attacks	Number of attacked vessels by years					
	2008	2009	2010	2011	2012	Total
Boarded	151	153	196	176	174	850
Hijacked	49	49	53	45	28	224
Fired upon	46	120	107	113	28	414
Attempted	47	84	89	105	67	392
Total	293	406	445	439	297	1880
	2013	2014	2015	2016	2017	Total
	2018	2019	2020	2021	2022	Total
Boarded	202	183	203	150	136	874
Hijacked	12	21	15	7	6	61
Fired upon	22	13	1	12	16	64
Attempted	28	28	27	22	22	127
Total	264	245	246	191	180	1126
Boarded	143	130	161	115	107	656
Hijacked	6	4	3	1	2	16
Fired upon	18	11	11	5	1	46
Attempted	34	17	20	11	5	87
Total	201	162	195	132	115	805



Since 2013 the majority of incidents were low level attacks (robberies). Only a few incidents in the Somali pirates' area of activity were registered till 2016, but 3 vessels have been hijacked in 2017, demonstrating that Somali pirates still had capabilities to act. In the Gulf of Guinea, after the downturn in oil prices, pirates expanded the hostage-taking to include off shore supply vessels and general cargo ships. Pirates of the West coast of Africa were often well armed and violent and hijacked and robbed vessels, kidnapped and injured crews along the coast, rivers, anchorages, ports and surrounding waters. As a whole, in 2013-2017 the number of crew held hostages is less than during the previous period. On the other hand, in 2016-2017 the share of kidnapping has risen, mostly off Nigeria, as well as in the region of Malaysia and the Philippines.

In 2018-2022, the trend of decreasing number of incidents continued. The number of vessels hijacked was nearly 4 times lower than in the previous period and about 14 times lower than this in 2008-2012. However, the number of kidnapped crew members marked considerable growth (except for 2022), with peak values in 2019 and 2020, reaching for the overall period 2 times more persons compared to the previous two periods. Most of vessels hijackings and crew taken hostages occurred in the Gulf of Guinea. Vessels have been boarded outside territorial waters, the crew kidnapped and taken into Nigeria where they are held for ransom. According to [5], while recently piracy in the region is on the decline, illegal oil bunkering and pipeline vandalism is at an all-time high because it is less risky and much profitable. Worldwide, since 2021 incidents decreased considerably in number and severity, and in 2022 they hit their lowest levels in decades - only 2 vessels hijacked and 1 fired upon.

Table 2. Number and types of violence against crew

Type of violence	Number of crew members					
	2008	2009	2010	2011	2012	Total
Assaulted	7	4	6	6	4	27
Hostage	889	1050	1174	802	585	4500
Injured	32	69	37	42	28	208
Kidnap/Ransom	42	12	27	10	26	117
Killed	11	10	8	8	6	43
Missing	21	8	0	0	0	29
Threatened	9	14	18	27	13	81
Total	1011	1167	1270	895	662	5005
	2013	2014	2015	2016	2017	Total
	2018	2019	2020	2021	2022	Total
Assaulted	0	1	14	5	6	26
Hostage	304	442	271	151	91	1259
Injured	21	13	14	8	6	62
Kidnap/Ransom	36	9	19	62	75	201
Killed	1	4	1	0	3	9
Missing	1	1	0	0	0	2
Threatened	10	9	14	10	10	53
Total	373	479	333	236	191	1612
Assaulted	0	0	5	3	6	14
Hostage	141	59	34	8	41	283
Injured	8	7	9	4	0	28
Kidnap/Ransom	83	134	135	57	2	411
Killed	0	1	0	1	0	2
Missing	0	0	0	0	0	0
Threatened	9	6	8	9	6	38
Total	241	207	191	82	55	776

For the entire 15-year period, in general, the number of

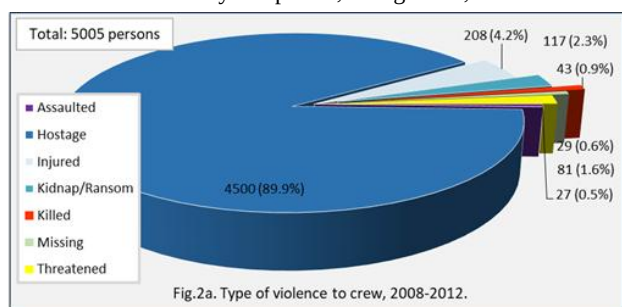


Fig.2a. Type of violence to crew, 2008-2012.

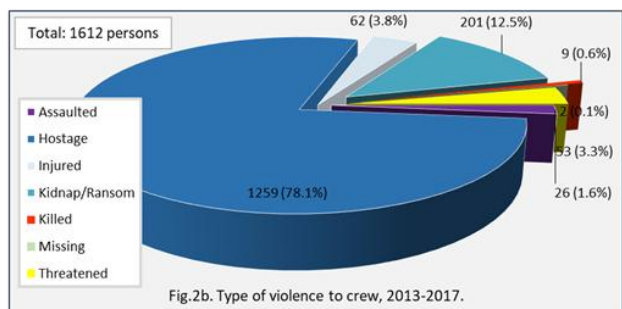


Fig.2b. Type of violence to crew, 2013-2017.

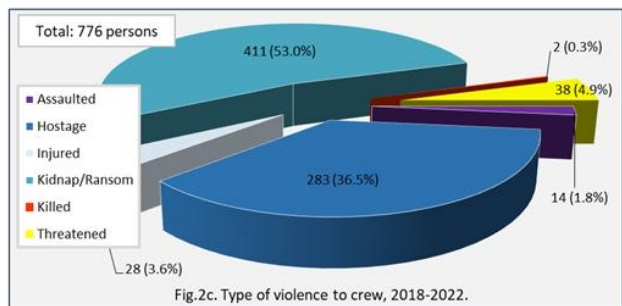


Fig.2c. Type of violence to crew, 2018-2022.

incidents shows a gradual decreasing trend after the peak of Somali piracy in 2009-2011. The number of boarded vessels vary in relatively narrow boundaries within the whole period. The number of hijacked vessels drastically decreases. While the number of hostages is gradually lowered, crew kidnapped for ransom shows the opposite trend with a peak towards the end of the period, excluding 2022.

Statistics concerning the state of vessels during the incidents show that the target of attack were mostly anchored and steaming vessels. During the heyday of Somali piracy the number of anchored and steaming vessels is nearly equal. Since 2012, as a result of powerful international naval presence in the affected regions, the share of attacked vessels underway has gradually begun to decline (except in 2015). In the third period under review, the ratio anchored/steaming vessels was again levelling off. In all 15 years under survey, vessels at berth have been very rarely attacked.

Another interesting observation concerns the ratio of successful attacks (boarded and hijacked vessels) and unsuccessful attacks (attempted attacks and firing upon vessels). In 2008-2012 the ratio is about 57:43 %, while in the next two periods over 83 % of the attacks have succeed (reaching 95 % in 2022). This fact can be attributed to the difficulties in carrying out the attacks in the first period due to the type of attacks, powerful naval presence in the region and increased security measures on the ships, while in the following years the overwhelming majority are low level incidents.

3.2. Attacks by location

The number of attacks against vessels by location is presented in Table 3 and Fig.3.

In 2008-2012 pirate attacks were largely confined to four major regions: the Gulf of Aden, the Gulf of Guinea, Malacca Strait and off the Indian subcontinent. Unprecedented number of attacks was registered off Somalia coast and the Gulf of Aden in 2009-2012, most often aimed hijacking ships, with crew kept hostages for

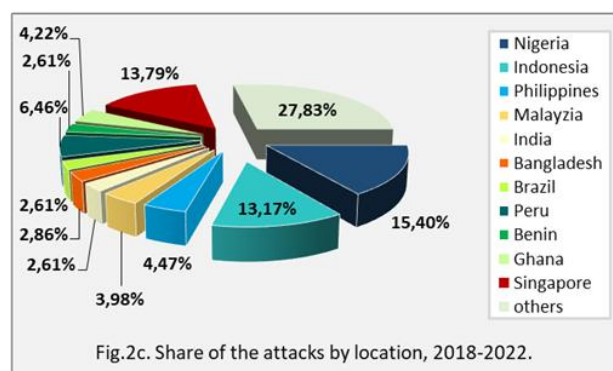
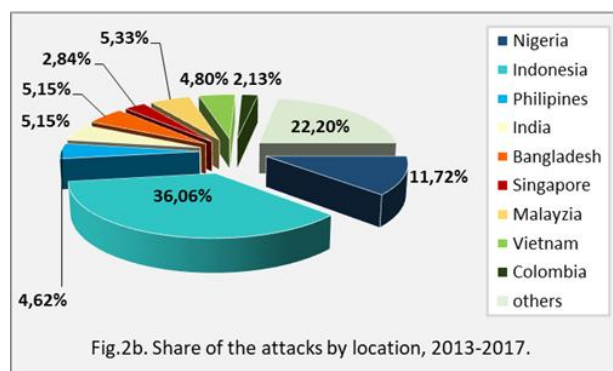
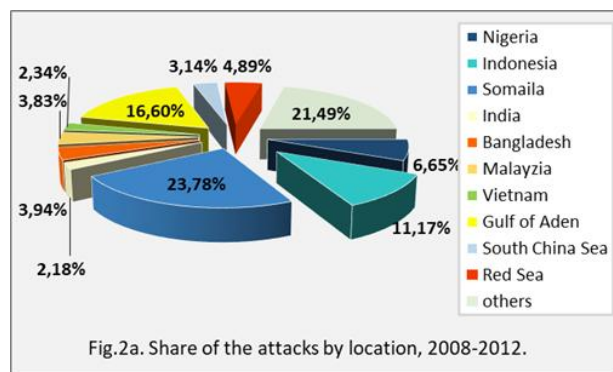
several months. This caused international concern and multinational naval forces were formed to patrol in the region, which led to a steady drop in the number of incidents since 2012. Growing number of attacks was observed in Southeast Asia, especially in Indonesia. Most attacks over the world in this period, except the area of Somali pirates operations, were low-level incidents (robberies). Hijackings were targeted mostly at tankers and cargo ships with the intent to steal and sell the cargo, often with significant violence against crews.

Table 1. Number of pirate and armed robbery attacks by location

Location	Number of attacks					
	2008	2009	2010	2011	2012	Total
Somalia	19	80	139	160	49	447
Gulf of Aden	92	117	53	37	13	312
Indonesia	28	15	40	46	81	210
Nigeria	40	29	19	10	27	125
Red Sea	-	15	25	39	13	92
Bangladesh	12	18	23	19	11	74
Malaysia	10	16	18	16	12	72
South China Sea	-	13	31	13	2	59
Vietnam	11	9	12	8	4	44
India	10	12	5	6	8	41
Others	71	82	80	94	77	404
Total	293	406	445	439	297	1880
	2013	2014	2015	2016	2017	Total
Indonesia	106	100	108	49	43	406
Nigeria	31	18	14	36	33	132
Malaysia	9	24	13	7	7	60
India	14	13	13	14	4	58
Bangladesh	12	21	11	2	11	58
Vietnam	9	7	27	9	2	54
Philippines	3	6	11	10	22	52
Singapore Str.	9	8	9	2	4	32
Colombia	7	2	5	4	6	24
Others	64	46	35	57	48	250
Total	264	245	247	191	180	1126
	2018	2019	2020	2021	2022	Total
Nigeria	48	35	35	6	-	124
Singapore Str.	3	12	23	35	38	111
Indonesia	36	25	26	9	10	106
Peru	4	10	8	18	12	52
Philippines	10	5	6	9	6	36
Ghana	10	3	9	5	7	34
Malaysia	11	11	4	2	4	32
Bangladesh	12	-	4	-	7	23
India	6	4	6	2	3	21
Brazil	4	2	7	3	5	21
Benin	5	3	11	2	-	21
Others	52	52	56	41	23	224
Total	201	162	195	132	115	805

In the second period (2013-2017), regardless the significant reduction of overall number of attacks after eliminating Somali piracy, the number of attacks in most of the other hot spots remained almost constant, with predominant low-level incidents. Indonesia had the largest share of global attacks - more than 36 %,

however the number of incidents began to decline by the end of the period. Since 2014 the Philippines also appeared in the ranking. At the same time, attacks near Nigeria increased more than twice, including kidnapping crew for ransom, making the Gulf of Guinea the new piracy hotspot. The escalation of kidnapping and hijacking in West Africa since 2016 became a cause for serious concern and



gave reason to conclude that piracy is becoming more violent.

During the period 2018-2022 Nigeria topped the list in both the number and severity of pirate attacks. However, the heavy presence of international and regional navies in the Gulf of Guinea has made piracy a risky business. Since 2021, there has been a pattern of failed attacks, it has become increasingly difficult for pirate groups to kidnap seafarers from vessels deep offshore and the incidents fell to 19 in 2022. [6] The waters of Southeast Asia and in particular the Singapore Straits are both the most dangerous and the area where the number of incidents was still on the rise. During the period, the number of incidents in the Singapore Straits jumped by about 13 times, however they were opportunistic, low-level crimes. Attacks off Indonesia have seen a nearly 3 times reduction.

4. Conclusion

The period 2008-2022 is characterized by significant dynamics both in terms of the intensity and nature of the incidents and their location. Within just 15 years, there have been considerable changes in the number and severity of incidents at regional and global level. Thanks to measures taken, especially international efforts, over the past year a record low number of incidents were registered, with the

majority of them low-level attacks. This, however, does not preclude the possibility for criminals in some regions to re-orientate quickly from robberies to the more profitable hijacking and kidnapping. In order to keep the progress made in combating piracy, maritime security organizations and experts stress the need for adequate awareness of the risk of attacks, crews high vigilance for potential threats and maintaining the vessels protection measures.

References

- [1] IMB. Piracy and Armed Robbery against Ships. Annual reports for 2008–2022, taken from:
http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2008.pdf
http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2009.pdf
http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2010.pdf
http://psm.du.edu/media/documents/industry_initiatives/industry_reports/maritime_imb_annual-report-2011.pdf
<https://www.kvnr.nl/stream/2012-annual-imb-piracy-report>
http://www.ship.sh/attachment/files/2013_Annual_IMB_Piracy_Report.pdf
<https://www.hellenicshippingnews.com/wp-content/uploads/2015/01/2014-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
<https://www.hellenicshippingnews.com/wp-content/uploads/2016/02/2015-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
<http://www.allaboutshipping.co.uk/wp-content/uploads/2017/01/2016-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
<https://www.hellenicshippingnews.com/wp-content/uploads/2018/01/2017-Annual-IMB-Piracy-Report-Abridged.pdf>
<https://maritimecyprus.com/2019/01/17/icc-imb-annual-report-2018-world-wide-incidents-of-piracy-and-armed-robbery-against-ships/>
<https://maritimecyprus.com/2020/02/04/icc-imb-annual-report-2019-world-wide-incidents-of-piracy-and-armed-robbery-against-ships/>
<https://maritimecyprus.com/2021/01/17/icc-imb-annual-report-2020-world-wide-incidents-of-piracy-and-armed-robbery-against-ships/>
<https://maritimecyprus.com/wp-content/uploads/2022/01/2021-Annual-IMB-Piracy-Report.pdf>
<https://maritimecyprus.com/wp-content/uploads/2023/01/2022-Annual-IMB-Piracy-and-Armed-Robbery-Report.pdf>
- [2] Tumbarska A. Maritime Piracy and Armed Robbery Evolution in 2008-2017. International Scientific Journal "Security and Future", 2, 1, STUME, 2018, ISSN: 2535-0668, 18-21. <https://stumejournals.com/journals/confsec/2018/1/18>
- [3] Tumbarska A. Current Maritime Piracy Practices and Anti-piracy Protection. International Scientific Journal "Science, Business, Society", 3, 3, STUME, 2018, ISSN: 2367-8380, 141-144. <https://stumejournals.com/journals/sbs/2018/3/141>
- [4] Christopher A., S. Christopher. Combating Maritime Piracy. Council on Foreign Relations, March 2012. <https://www.cfr.org/background/combating-maritime-piracy>
- [5] The Maritime Executive. Why Are Gulf of Guinea Pirates Shifting to Illegal Oil Bunkering? 4 December 2022. <https://www.maritime-executive.com/article/why-are-gulf-of-guinea-pirates-shifting-to-illegal-oil-bunkering>
- [6] The Maritime Executive. IMB Calls for Vigilance While Highlighting Drop in Piracy in 2022. 12 January 2023. <https://www.maritime-executive.com/article/imb-calls-for-vigilance-while-highlighting-drop-in-piracy-in-2022>

Flood risk assessment and management through a water management information system

Sabina Nedkova^{1,*}, Galina Baycheva², Plamena Atanasova¹, Hristo Bozov¹

University "Prof. d-r Asen Zlatarov", Bulgaria¹

Head of Department, Crisis Management, Public Order and Security Directorate, Burgas Municipality, Burgas²
sabina_nedkova@abv.bg

Abstract: Floods are the most common natural disasters on the territory of Bulgaria. As a temporary flooding of a significant part of the land as a result of the action of natural forces, destruction of hydro technical facilities (dam walls, dams) or other critical situations (accidents), these are events with a great possibility of prevention and mitigation of negative effects, since unlike other natural disasters, they are highly predictable. In many cases, the timing, nature and expected sizes can be determined in advance, which, together with the preparation of the population for response and crisis management measures, are part of the complex activity of Flood Protection. The researched information system for water management is part of the measures for the effective management of the risk of floods in the territory of the Municipality of Burgas, as the most frequently occurring disaster in the territory of the Municipality, related to large material damages, destruction and casualties. Photos of the operation of the system in real conditions of rising waters of the monitored water bodies are presented, as well as the actions aimed at controlling the negative effects of the disaster.

Key words: INFORMATION SYSTEM FOR WATER MANAGEMENT, FLOODING, PROTECTION, FLOOD RISK MANAGEMENT

1. Introduction

The location Floods are a potential cause of accidents, cause damage to the environment and affect economic activity. Flooding is a natural phenomenon that cannot be prevented, but some human activities (such as the growth of settlements and economic assets in floodplains, as well as the reduction of the natural ability of the soil to retain water caused by improper land use) and the climate change, contribute to an increase in the likelihood of floods and their adverse consequences for human health and life, the environment, economic of the municipality of Burgas - among three lakes (Atananovsko, Mandrensko and Burgasko (Vaya)) and the peculiarities of the circulation processes above it determine the great variety of climatic conditions. The territory of Burgas municipality falls in an area with maximum precipitation in late autumn and early winter and minimum in summer. Due to the change in the climate characteristics and as a result of the global warming, intense rainfall is not an exception in summer [2]. This creates a need for constant monitoring of the level of water bodies in the region, due to the possibility of exceeding the critical level and the provision of preventive actions for continuous manual and mechanized maintenance of their condition, passable and accessible, through regular planned cleaning of riverbeds and ravines in the urbanized territories of settlements.

Flood risk management system in Burgas Municipality

Since 2015, the Municipality of Burgas, within the framework of the "Flood Risk Management" project, has been building a "Water Management Information System" (WAMS) in the most critical sections of riverbeds, ravines and dams in populated areas on the territory of the Municipality of Burgas. The system also includes an information platform for notification, by phone message, when certain values of the water level are reached, a website for visualization of the measurement data and a mobile application for its visualization as well as a notification for iOS and

Android.

The information system consists of 22 automatic telemetric hydrometric stations for measuring the water level. They are located on rivers, ravines, dams, Lake Vaya, etc. Three of them are combined stations for measuring the water level and the amount of precipitation, located on the roof of the administrative building of the Municipality of Burgas, in the village of Izvor and the Lozovo district, as well as two for measuring the water level and wave height are located on Sveta Island Anastasia and at the marina in Sarafovo quarter (Fig. 1).

The information system for water management is an important tool for prevention and crisis management, since from the moment of its introduction, the information obtained from it prevents damage and incidents from floods in the territory of the Municipality of Burgas. It is composed of the following basic software components:

- information platform for water management, incl. notification by sms when certain values are reached, composed of the following modules with the corresponding user interfaces: administrative, communication, for processing and visualization, for inquiries;
 - dynamic web page for visualization of measurement data;
 - mobile application for visualization of measurement data and notification when certain values are reached for iOS and Android.
- The system consists of 4 different hardware configurations providing:
- Database storage;
 - Visualization of web applications and support of mobile applications;
 - Collection of input data from exported measurement points in raw format
 - Connectivity between the systems in the platform and their connectivity to the Internet space.

The system is installed on a server of the Municipality of Burgas and the basic applications and database management system (DBMS) used by it are: Apache HTTP server, J2EE server - Apache Tomcat, GeoServer, Drupal CMS, GIS desktop Quantum GIS, PostgreSQL. Supports desktop and web based clients.

The copyright, software, including source code and other intellectual or industrial property rights are the exclusive property of the Municipality of Burgas.

Case studies

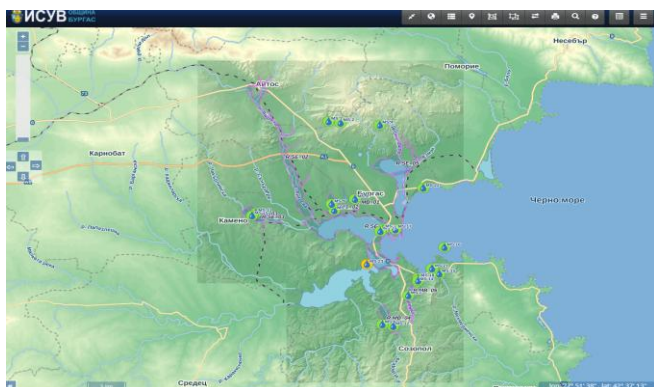


Fig.1 Monitoring stations' map on the territory of Burgas Municipality

Overflow of Chakarliyska River and Malkata Reka River 25.10.2017

The Chakarliyska River is 37 km long and flows through the southeastern part of the Burgas lowland, flowing into Vaya Lake (Burgas Lake) with a catchment area of 129 km². Along the course of the river there are three villages in Aytos Municipality - the village of Chukarka, Kameno Municipality - the village of Vratitsa and Burgas Municipality - the village of Ravnets.



Fig. 2-3 Before and after the waters of the Chakarliyska River

On 25.10.2017 due to the extremely intense rains (in total for the southern and western regions of the municipality - 186.4 l.sq.m.) and the strong hurricane wind, a partial state of emergency was declared in the village of Ravnets after the Chakarliyska River and the Malkata Reka River (which in the previous day look dried up), came out of their beds.



Fig. 4 Water level of the Chakarliyska River 0.00-2.30 o'clock

The attached Fig. 2-3-4-5-6-7 show the spontaneous nature of these small rivers, which caused the disaster situation not visible in any way from their condition in the photos from the previous day, 10/24/2017. From Fig. 4 it can be seen that on 25th of October 2017 from 0.00 to 2.30 as a result of the heavy rains, the Chakarliyska river rose its level from 8 cm to 250 cm, having crossed almost double the dangerous level of 120 cm and the river Malkata Reka has in almost the same time raised its level from 0 to 200 cm (Fig.7). The rivers are out of their beds and as a result of the organized early warning and informing the population, no human lives were taken from the threatened village of Ravnets.



Fig. 5-6 Malkata Reka river before /dried up and after during rain



Fig. 7 Water level of Malkata reka river 0.00-2.45 o'clock

Lozovska river - 22.01.2018

As a result of an intense rain on 22nd Jan.2018. the monitoring station in the Lozovo district reports increased levels of the Lozovska River (Fig. 8-9) The attached graph (Fig. 9) is for the time range 0.00 - 14.15 o'clock, during which time the Lozovska River passed the line marking an increased level and at 6.15 o'clock it reached a water level of 42.74 cm.

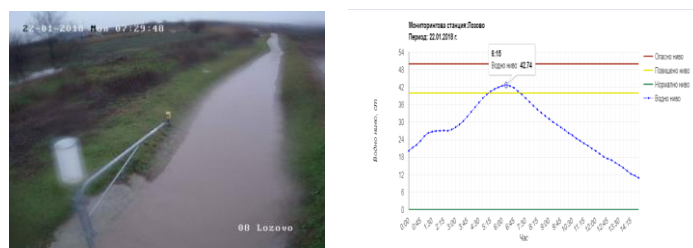


Fig. 9-10 Lozovska river on 22.01.2018

Increased levels of Lake Vaya (Lake Burgas) and prevention activities - 06.03.2018

As a result of an intense rain on 6th March 2018 the water level of Vaya Lake rises significantly to the critical 167.45 cm. The data on the rise in the water level for such a short time showed the disaster potential of the situation and within only half an hour activities were carried out to prevent and minimize the risk of flooding by building dikes along the roadway which allowed no flooding of the road infrastructure. (Fig.11-12)



Fig. 11-12 Vaia Lake on 12.29 and 12.59 o'clock

Landslide as a result of heavy rainfall in Sarafovo district - 01.18.2018

The extremely intense rain on 1st of Oct. 2018 was the reason, the monitoring station in the district of Sarafovo to report an increased water level of 282.17 cm. Due to the intense rain, earth masses from the slope of a road facility on the main road I-9 slid onto a car, covering the road connection to Sarafovo district and Burgas Airport. More than 200 properties at the area were flooded, as well as the road surface. It was necessary to close the national road I-9 until restoration works had been carried out (Fig. 13 - 14).

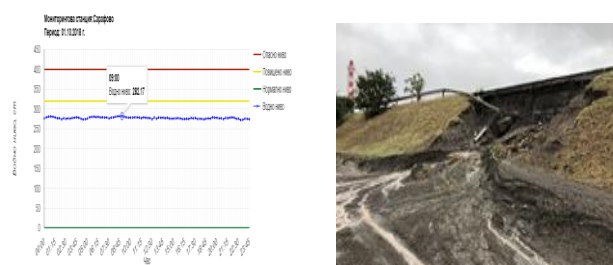


Fig. 13-14 Sarafovo monitoring station data (left graph) and landslide alongside the Sarafovo road

Increase in the levels of the Marinka River and the Otmanliyska River 26.11.2019



Fig. 15 Marinka river



Fig. 16 Otmanliyska river

The intense rainfall of 137 l/sq.m. lead to an increase in the level of the Marinka River in the Chernitsite villa area (Fig. 15) and of the Otmanliyska River (Fig. 16) on 26th of November 2019. The timely evacuation, provoked by the received information about the risk of flooding, did not allow deaths of the population living in the overflow area.

Rising sea water level in the monitoring station "Ribarsko Selishte"

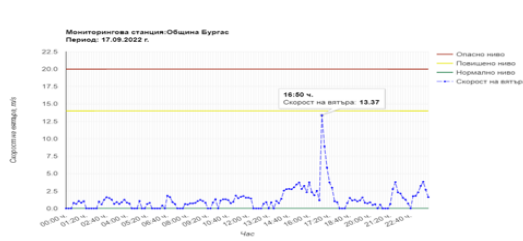
For the period, 08-12 of January 2021, as a result of intense amounts of rain, which in total in the city of Burgas was 150.8 l/sq.m, and in the villages in the south-eastern region of Marinka, Izvor, Dimchevo, Fisherman's village and villa zone "Chernitsite" was 220.20 l/sq.m, had been developed a critical situation. The large amount of rain and the increase in the water level create a risk and danger to the life and health of the population of the territory of the Municipality of Burgas. The measured amounts of intense rainfall in the municipality for this period in January 2021 are five times higher than the monthly norm of 40 l/sq.m for the area (Fig. 17). The graph shows an increase in the water level to values of 200 cm at 17.30 o'clock on the 12th of January 2021



Fig. 17 Increase in the water level of the "Ribarsko selishte Village"

Squall – 17.09.2022

On the 17th of September 2022, in the city of Burgas, were measured wind speed values from the monitoring station located on the Burgas Municipality building, which show a critical situation that developed within a few minutes with a peak at 16.50 o'clock with a wind speed that raised sharply from about 1.5 m/s at 16.00 (direction 120° - southeast) to 13.37 m/s at 16.50 (direction 310° - northwest [3]). This meteorological phenomenon, in which there is a sudden change in wind speed and direction, accompanied by cumulus clouds is known as a squall and due to its nature and power, it creates a risk of property damage and flying objects and branches that can create a danger to the life and health of the people

Fig. 18 Sharp increase in wind speed and change in its direction on the 17th of September 2022

In the city of Burgas, this phenomenon caused a lot of material damage, but it passed quickly and without human casualties (Fig. 18-19).



Fig. 19 Damages after the meteorological phenomenon - squall 17.09.2023 on the territory of the University "Prof. Dr. Asen Zlatarov", Burgas

Conclusion

The development of the strategy for action in case of crises is an extremely important stage of their mastery, because it is the process of establishing possible solutions to situations of a risky nature that have not yet arisen. At this stage, the realistic data and the ability to make timely information available to the control authorities about the real values of key parameters are the two most important factors for building a reasonable and workable strategy to deal with the crisis, which brings with it many unknowns and high potential for causing damage and loss, including loss of human life.

The presented Information System for Water Management, implemented in the activities of the Municipality of Burgas for several years, is a very important part in the creation of the strategy for actions in case of crises, because it ensures effective management of water and the risk of floods in the territory of the Municipality of Burgas and supports the process of decision-making, through the timely information of the responsible institutions and the population.

The system proved its effectiveness during large-scale floods in 2017 and 2021 as an intelligent system of early warning in case of risk of flooding.

The information system cannot prevent floods, but through the early warning, it enables a timely response to evacuation and redirection of resources where they are most needed. In addition to this specialized information, through the system and the free mobile application, citizens have a possibility to access at any time and automatically receive notifications of potential risk or current danger. Development of subsystems for monitoring and notification of other disasters and threats - fires, icing, etc. is expected. In the future, it is expected also that the means for mobile notification of the population will be improved, as well as specialized functions will be built for improved response and rescue of people at risk and with increased vulnerability.

References

1. 2000/60/EC of the European Parliament and of the Council of October 23, 2007.
2. Flood Action Plan, Burgas Municipality (2021)
3. <https://freemeteo.bg/weather/burgas/history/daily-history/?gid=732770&station=4911&date=2022-09-17&language=bulgarian&country=bulgaria>