

INTERNATIONAL SCIENTIFIC JOURNAL

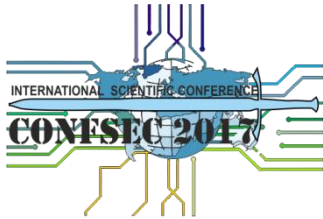
SECURITY & FUTURE

ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

**YEAR VIII,
ISSUE 3/2024**

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 VIII, ISSUE 3 / 2024

All articles are published after peer review by two independent reviewers.

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
Dimitar Dimitrov, Assoc. Prof.	Institute of Metal Science – BAS, Sofia	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
Leonid Vinogradov, Dr.sc.ing	Riga Technical University	LV
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	NM
Nurgali Zaurbekov, Prof.	Almaty Technological University	KZ
Oliver Bacanovic, Prof.	University "St. Kliment Ohridski" - Bitola	NM
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
Sasa Mijalkovic, Prof.	Academy of Criminalistic and Police Studies, Belgrade	RS
Siniša Tatalović, Prof.	University of Zagreb	HR
Stoyan Denchev, Prof.	University of Library Studies and Information Technologies	BG
Tatyana Ejevskay, Prof.	Transbaikal 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

Methods and approaches for the preparation of a comparative analysis of critical infrastructures. Analysis evaluation criteria. Criteria for evaluating the analysis.	
Dimitar Dimitrov, Nadejda . Randelova	73

NATIONAL AND INTERNATIONAL SECURITY

AI integration in airport security: a case study of sofia airport within bulgaria's critical infrastructure framework	
Antoaneta Simeonova, Angel Krumov	76
Will Ukraine remember the support given by the EU?	
Vasile Silviu	79

INFORMATION SECURITY

Analysis of internet of things security breaches	
Veselin Tselkov	82
Possibilities for using steganography methods in the quantum century	
Veselka Stoyanova	86
Artificial intelligence and data security	
Teodora Licheva	88

TECHNICAL FACILITIES FOR ENSURING SECURITY

Application of acoustic emission method for the diagnosis of underground gas pipeline without taking it out of operation	
Leonid Vinogradov, Guntis Strautmanis, Juris Gutans, Yulija Soldatova, Viktor Prokopenko, Andrei Ivlijev	91
An approach to increase the combat effectiveness of sea bottom mines	
Aleksandar Kolarov, Radostin Naydenov	94

Methods and approaches for the preparation of a comparative analysis of critical infrastructures. Analysis evaluation criteria. Criteria for evaluating the analysis.

Dimitar Dimitrov¹, Nadejda . Randelova²

Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Center "Acad. A Balevski", Sofia, Bulgari a¹

Kozloduy Nuclear Power Plant²

E-mail: ddimitrov@ims.bas.bg, NSRandelova@npp.bg

Abstract: *There are numerous methodological approaches for modelling, numerical analysis and/or simulation of the behaviour of individual systems. However, modelling the interdependencies between task-oriented or dedicated systems (the so-called system of systems) and describing their complex behaviour, necessarily through simulation, is still an unsolved issue.*

KEYWORDS: CRITICAL INFRASTRUCTURE, VULNERABILITY, RISK ASSESSMENT, RISK MANAGEMENT, MODELLING AND SIMULATION

1. Introduction

Critical infrastructure analysis may focus on different objectives (reliability, risk, vulnerability, etc.), may vary in its scope (sectoral, system-wide, or "system-of-systems"), and may follow different methodological and/or competing approaches. These facts are usually a source of confusion and require carrying out a comparative analysis with respect to the different models and analytical techniques

These methodologies have been described and relatively successfully evaluated in terms of their general suitability for assessing the vulnerability of critical infrastructures, with a focus on the role and impact of interdependencies. Thus, in view of its purposes, this paper will discuss some of the key benchmarking criteria (e.g. "Types of Interdependencies," "Types of Simulation Events," "Event Implications," "Data Needs," etc.). In this way, the paper will offer a useful basis for selecting appropriate single or combined techniques for modelling and simulation of critical infrastructure interdependencies, given a particular problem or task.

On the one hand, critical infrastructures are defined as "a network of independent, manmade systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services" [1] and are also essential for economic development and social welfare. They are subject to a multitude of potential asymmetric threats (technical, intentional or unintentional – man-made, physical, natural, cyberspace) that pose a risk to them. Critical infrastructures are highly interdependent, both physically and due to the widespread use of information and communication technologies. In other words: critical infrastructures are characteristic of highly dynamic and complex systems and are interdependent in varying degrees and with varying intensities [2].

At the same time, the vulnerability of critical infrastructure systems is often defined as the presence of gaps or weaknesses in their design, implementation, operation and/or management that make them susceptible to disruption/destruction, regardless of their recoverability.

What does the term vulnerability mean in the context of critical infrastructure protection? Some researchers [3] define the concept of vulnerability as follows: vulnerability is the manifestation of the inherent states of a system that make it susceptible to failure or loss. Various publications emphasize that vulnerability is a multidimensional concept that is best characterized by a set of state variables that describe the weaknesses of a system and how they interact to cause loss following a disruptive event.

2. Requirements regarding the methods and approaches for preparing a comparative analysis.

There are well-known "classical" methods for reliability and risk analysis that are widely applied to the so-called single complex systems: e.g. tabular techniques (FMEA, HAZOP), bow-tie techniques (Fault/Event Tree Analysis), logic representation

techniques (Petri Nets, Markov graphs), computational techniques (Binary Decision Diagrams, Monte-Carlo simulation), etc.

2.1 Need for a systematic survey

There are a number of studies that enforce and confirm the importance of understanding, modelling and simulation of interdependent critical infrastructures [4]. Although studies on available techniques do exist [5], it is clear that they lack comprehensive and clear criteria for assessing applicability. Hence, the question of how to model the complex system-of-systems behavior or of which methods are best suited for this task, is still open and provides a motivation for finding further approaches.

2.2 Objectives of the comparative assessments of techniques

The main objective is to select, describe and evaluate techniques with a view to their adequacy in preparing a vulnerability analysis of infrastructure interdependencies. To this end, it is logical to be able to distinguish between overt and covert vulnerabilities: reviewing the results of statistical data analysis helps to find obvious weaknesses if the statistics show some obvious problem areas/scenarios, such as inferences based on "blackouts." Other signs of obvious vulnerability are operational errors, emergency procedures, etc.

The need for a more precise analysis arises if the indication assessment is not "clearly defined" and the main covert vulnerabilities are still to be expected. Particular attention should be paid to interdependencies within or between systems. It is also necessary to evaluate simplified procedures developed at an earlier stage (including the "decoupling" of systems).

Therefore, the purpose of the comparative evaluations of the various techniques is to analyze the strengths and weaknesses of the different methodologies as well as to analyze, characterize, and propose appropriate techniques for modelling and simulation of interdependent critical infrastructures.

3. Basic comparative assessment criteria

3.1 Basic modelling approaches

Two main modelling and simulation approaches have been described in the current literature: *Interdependence Analysis*, which involves qualitative approaches, and *Systems Analysis*, which tends to engage with quantitative approaches.

Interdependency analysis [6] involves qualitative techniques to identify critical infrastructures and to analyze the characteristics and dimensions of their interdependencies. These techniques include extensive use of expert interviews, roundtables or workshops, appropriate questionnaires, etc. The models are relatively easy to build, but are limited to the elements explicitly focused on by the experts and are not able to systematically detect hidden critical elements and their corresponding vulnerabilities.

Systems analysis [7] uses approaches that rather represent quantitative techniques that can identify hidden dependencies, and are strongly linked to computer simulations. These techniques need sophisticated computer architectures since the approaches are extremely detailed and time consuming.

3.2 Modelling and simulation strategies

The most important assessment aspect, not only in the development of optimal modelling and simulation strategies, is the decision to choose between two basic strategies: bottom-up and top-down or a combination of both:

Bottom-up approach: the whole system is described starting from its individual parts [8]. This kind of approach usually refers to complex adaptive systems that can be built based on the results of interacting elements, such as basic entities with a defined location, capabilities and memory reflecting their identification. The bottom-up approach is generally considered more intuitive and less error-prone than the top-down approach and can usually be implemented with relative ease in software code. As long as the components are well defined, it can produce very accurate output. However, the exclusive use of the bottom-up approach can lead to significant system-level limitations being overlooked, especially when it is used in the absence of sufficient input data.

Top-down approach: the distinctive feature of the top-down approach is its focus on the general properties of the system, combined with relative ease of applicability. However, this approach is less suitable than a bottom-up approach in capturing lower-level factors, such as systems-specific issues, as well as implementation-specific details, which tend to accumulate quickly and can significantly affect the assessment. [9]

3.3 Types of interdependencies

These interdependencies describe the different types of dependencies between infrastructures. Each type has its own characteristics and effects on infrastructures, but typically, modelling and simulation approaches do not take into account every type of dependencies. Four main types of interdependencies between critical infrastructures can be distinguished. [10]

Cyber interdependencies: they connect infrastructures to each other through electronic information links. The outputs of information infrastructures are inputs to other ones;

Geographic interdependencies: they are observed when elements of an infrastructure are in close spatial proximity. For example, a faulty underground water pipeline can create interference on power lines and fibre optic communication cables in a collector; these are the so-called “causal failures;”

Physical interdependencies: they describe the material flow between different infrastructures. Such interdependencies arise in a physical connection consisting of input and output flows. For example, electrical systems and information and communication technologies (ICT) are physically interdependent. Electricity powers ICTs, while they can control and manage the operational data for the proper functioning of this power generation and its transmission and distribution;

Logical dependencies: these are dependencies that exist between infrastructures but do not belong to the above types. Often logical dependencies are caused by human decisions and actions taken in both the political and societal domains, e.g. the volume of oil and gas supplied is highly dependent on the political decisions of OPEC members.

3.4 Types of simulation events

A significant challenge associated with modelling and simulation techniques can be the creation of “what-if” scenarios to analyze critical infrastructure interdependencies. The following information about a subsequent event is possible: [11]

Incident: it describes a wide range of randomly occurring and potentially damaging events, such as natural disasters, whose origin is usually outside and independent of the system;

Attack: this is a series of potentially damaging actions taken by an intelligent adversary to achieve certain results. Cyber-attacks include intrusion into, probing and denial of service. Furthermore, the idea itself can have as serious an impact on a system as if it had actually materialized. A system that assumes an overly defensive position because of the threat of attack may significantly reduce its functionality and divert excessive resources to monitoring the surrounding environment and protecting system assets;

Damage: this is a potentially damaging event resulting from deficiencies in a system or in an external element on which the system depends. Failures may result from faulty design, manufacturing and operational (human) errors, corrupted data, etc.

3.5 Consequences of events

Interdependencies have a bearing on the consequences of single or multiple failures or interruptions within interconnected systems. Different types of interdependencies can trigger feedback loops that have accelerating or decelerating effects on the systems’ response, as observed in dynamics. The following types of events can be distinguished:

Cascading events: the occurrence of a situation in which the undesired event is in one part of the infrastructure, while the effects are in other parts of the infrastructure. An example of a cascading event in electrical systems is the overloading and disconnection of a transmission line from the power grid [12]. In such a case, its load would be shifted to a nearby transmission line, which, even without additional load, could also switch off and leave a large part of a given region without power;

Escalating events: these can be treated as a consequential outcome of cascading events, i.e. a “problem” occurring in one infrastructure can impact other infrastructures, thus causing a failure in them or an outage in another infrastructure, by increasing the severity of the failure or the recovery time. This in turn may affect the restoration of the service provided by the originally affected infrastructure;

Common cause events: these are dependent failures in which two or more fault conditions are present simultaneously or within a time interval as a direct result of the common cause. For example, fiber optic cables and power lines often share a common duct in tunnels or over bridges. If this tunnel or bridge is damaged by a fire caused by a traffic accident, this can also disrupt telecommunication and power supplies due to traffic disruption. [13]

Restrained events: failures that do not have cascading, escalating or general consequences on the infrastructures under consideration.

3.6 Need for data (information)

This criterion requires general information on the quantity and quality of inputs needed to apply the methodological approach. Inputs include information on the topology and layout of the system, its commodity flows, its functioning, as well as numerical values of the modelling parameters. The availability of input data and their quality is essential for the practical application of modelling and simulation approaches; the lack of satisfactory data is a common problem of scientific analyses and can negatively affect the application of advanced approaches. Two levels are known to exist:

High: the methodological approach is highly dependent on the high quality and quantity of input data to provide feasible modelling approaches. The presence of these factors needs to be ascertained before implementing such an approach.

Low: the methodology may be applied with inconsistencies in the quality or quantity of input data submitted to provide reliable results. In these cases, a minimum quality or quantity of information is required.

3.7 Observation scenarios

Depending on the criteria described above, the monitoring scenarios relate to modelling and simulation techniques, input data and available information. Interdependent models can be grouped into the following main categories, depending on the scenarios required:

Vulnerability assessment: the objective is to identify and quantify vulnerabilities in the system. Vulnerability is defined as the probability of an accident, successful attack or failure. Vulnerability assessments can be viewed as an extended failure analysis of elements;

Fault analysis: human errors can cause disruptions in infrastructure systems. Modelling and simulation techniques can produce system analysis and reliability theory by identifying and analysing the most common faults. Fault analysis provides identification of critical components, helps to improve the system, and to understand the relationships between critical nodes of the network as a whole.

3.8 Modelling and simulation paradigms

The modelling and simulation of dynamic processes leads to changes in the state of the system/its components. "Simulation is an 'execution' process that manages the model through discrete or continuous changes of its state over time. [14]. The combination of two paradigms is also possible.

Discrete events: state changes by "jumps." Models consist of entities (units of movement), resources (elements that provide the service), and control elements (elements that determine the states of entities and resources).

Continuous events: these describe state changes with continuous functions. If the material or information being simulated can be described as continuously changing, rather than in discrete steps or packets, it is most appropriate to use the continuous event paradigm. The simulation is based on solving differential equations that describe the evolution of the system.

5. Conclusions

Although there exist many techniques currently for analyzing individual critical infrastructures, no universal method or common interdependency tool for modelling and simulation has been universally accepted and therefore discussions on the suitability of different approaches are ongoing.

In terms of the dynamics of the systems, there is a strong argument for proposing possible improvements to the analysis, security, functional

understanding and strategic management of critical infrastructure systems. Such improvements will aid the perception of the system's operation and change over time.

With all this in mind, it is quite possible to develop adverse event scenarios that can be applied to critical infrastructure models with the aim to demonstrate the kinds of threats and vulnerabilities that would impact business operations, the management of emergencies and their consequences, information systems attacks, cyber-crime, the protection of key facilities against attack, chemical, biological and radiological hazards, water and food provision, identification and protection of land-adjacent maritime infrastructure, which can logically be applied to critical infrastructure models.

Modelling the dynamics in the systems allows observing not only normal activity, but also the functionality under adverse change and its effect on the critical infrastructure systems as a whole. Without this knowledge, the owners/operators of critical infrastructure will be severely hampered and left unprepared for likely events.

Effective modelling of critical infrastructure would enable both government and critical infrastructure owners to analyze, identify, and effectively manage and maintain the stability, security, and access to that infrastructure by developing solutions against unexpected or other challenges to its resilience.

Literature

- [1] Critical Foundations: Protecting America's Infrastructures, Paper of the President's Commission on Critical Infrastructure Protection, Washington D.C., 1997;
- [2] Panevski V. „INTEGRATED CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT“ International Scientific Journal Security & Future, 1/2018, Scientific Technical Union of Mechanical Engineering Industry 4.0, 2018, ISSN:2535-0668, p.p. 3-6;
- [3] Haimes, Y. Y. „Risk Modeling, Assessment, and Management“, 2nd Ed. Wiley, NY. ISBN:0471480487, (2004);
- [4] Department of Homeland Security. "National Infrastructure Protection Plan", DHS, (2006);
- [5] Panevski V.. „Competence centres and intelligent security systems in Bulgaria“, International Scientific Journal "Security & Future", YEAR III, ISSUE 1, HTC по машиностроене, 2019, ISBN:WEB ISSN 2535-082X, p.p 14-16;
- [6] S. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies", Proceedings of the 37th Hawaii International Conference on System Science, Hawaii, (2004).5. Juni 2008 50/50. D. Reinermann and J. Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)", Critical Infrastructure Protection Workshop. Frankfurt, (2003);
- [7] S. Panzieri, R. Setola, and G. Ulivi. "An approach to model complex in-terdependent infrastructures", Universita "Roma Tre", Roma., (2005);
- [8] S. Lee "A frame work for supporting bottom up ontology evolution for discovery and description of Grid services". Expert systems with Applications, 32(2):pp.376-385, (2007);
- [9] V. Temnenco. "Software Estimation", Enterprise-Wide. (2007);
- [10] S. Rinaldi, J. Peerenboom and S. Kelly "Critical Infrastructure Interdependencies", IEE Control Systems Magazine, (2001);
- [11] R.J. Ellison, N.R. Mead, T. A. Longstaff and R. C. Linger. „The Survivability Imperative: Protecting Critical Systems“, The Journal of Defense Software Engineering, (2000);
- [12] I. Dobson, B. Carreras, V. Lynch and D.E. Newman. „Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization“, Bulk Power System and Control, Cortina d' Ampezzo, Italy, (2004);
- [13] F.M. Marshall, D. M. Rasmuson and A. Mosleh. "Common Cause Failure Data Collection and Analysis System", 1, U.S. Nuclear Regulatory Commission, NUREG/CR-6268, (1998);
- [14] Borshchev, A., Y. Karpov, and V. Kharitonov, Distributed simulation of hybrid systems with AnyLogic and HLA. Future Generation Computer Systems, 2002. 18(6): p. 829-839 (2002).

AI integration in airport security: a case study of sofia airport within bulgaria's critical infrastructure framework

Antoaneta Simeonova¹, Angel Krumov¹

Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences,

67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria ¹

Abstract: This paper examines the integration of artificial intelligence (AI) in airport security, with a particular focus on Sofia Airport within Bulgaria's critical infrastructure framework. It explores the growing significance of AI in enhancing security protocols at airports, which are critical nodes in national and international transportation networks. The case study highlights a collaborative effort between Sofia Airport and VIP Security, where the "VIP Eye" system was demonstrated to airport officials for testing and feedback. VIP Eye, an AI-driven solution, is designed to detect and mitigate security threats with high precision, featuring capabilities such as weapon detection, masked face recognition, and the identification of physical altercations. The collaboration aimed to refine the system based on insights from Sofia Airport's security expertise, contributing to advancements in security technology. The study also discusses the broader implications of AI adoption for airport security in Bulgaria, considering both technical advancements and the challenges associated with integrating such technologies within the existing security infrastructure.

KEYWORDS: AI INTEGRATION, AIRPORT SECURITY, CRITICAL INFRASTRUCTURE, SOFIA AIRPORT, VIP EYE, BULGARIA, THREAT DETECTION, SECURITY TECHNOLOGY

1. Introduction

The growth of international air travel and heightened security concerns have made airport security a critical aspect of national infrastructure. Ensuring public safety in airport environments, which are vast and high-traffic, presents challenges beyond the capacity of traditional surveillance and monitoring methods. In recent years, artificial intelligence (AI) has emerged as a powerful asset in this field, enabling more efficient, precise, and proactive approaches to security that support both safety and operational flow.

In Bulgaria, the integration of AI within airport security aligns with the country's broader critical infrastructure objectives, particularly as the Bulgarian government seeks to modernize and secure essential facilities. AI technologies, such as automated threat detection and real-time video analysis, are particularly relevant to airports, where the need to swiftly identify and respond to threats is paramount. This paper examines these roles, focusing on how AI can contribute to more resilient airport security frameworks.

Through a case study of the VIP Eye system tested at Sofia Airport, we investigate AI's specific applications and explore the challenges related to accuracy, reliability, and ethical considerations. The study aims to shed light on the implications of AI adoption in Bulgarian airport security, focusing specifically on the potential to strengthen safety and operational resilience in high-risk environments.

2. AI Integration within Bulgaria's Critical Infrastructure Strategy

In December 2020, Bulgaria launched its National AI Strategy, designed to establish a sustainable foundation for AI's integration across key sectors, including critical infrastructure. Developed by the Bulgarian Academy of Sciences and finalized by the Ministry of Transport, Information Technology, and Communications, this strategy prioritizes the use of AI to improve national security and resilience within transport and security sectors, among others. [1]

2.1. AI and National Security: Key Infrastructure Considerations

A central pillar of Bulgaria's AI strategy is its application in critical security functions, including threat detection, crisis response, and cybersecurity. AI systems offer the potential for real-time monitoring and data analysis capabilities, which could help detect potential threats and system vulnerabilities more effectively. These applications are especially relevant to airport security, where AI may enhance both surveillance and rapid response capabilities,

aligning with the strategic goals for resilient and secure infrastructure. [2]

2.2. AI in Transport Infrastructure with a Focus on Air Transport

In line with Bulgaria's national goals, the AI strategy emphasizes the modernization of transport infrastructure. Within air transport, AI-driven systems have the potential to manage air traffic flow, optimize airport operations, and streamline passenger processing. At critical nodes like Sofia Airport, AI applications could enhance operational efficiency and contribute to more precise security measures, such as advanced screening and real-time threat identification. This integration aims to support seamless, secure airport operations, making air transport infrastructure a priority for AI-enabled resilience. [3]

2.3. Regulatory and Collaborative Frameworks

The strategy also advocates for a regulatory framework that adheres to international safety and ethical standards, supporting the secure implementation of AI in critical infrastructure. Collaboration among government agencies, research institutions, and industry partners is key to this initiative, promoting responsible AI use in essential sectors like airport security. Establishing these frameworks and partnerships builds public trust and ensures that AI tools can be reliable and secure, as seen in recent AI security trials at Sofia Airport, which we examine later in this paper. [4]

3. AI's Role in Airport Security

AI technology has emerged as a powerful tool in airport security, enhancing both the safety and operational efficiency of complex environments. Airports face various security challenges due to their vast layouts, high traffic, and multiple entry points, making it difficult for human operators to manage all potential security threats effectively. By leveraging AI, airports can optimize situational awareness, improve threat detection, and ensure a safer environment for passengers and staff. [5]

3.1. Enhancing Situational Awareness

One of the key applications of AI in airport security is to enhance situational awareness through intelligent video monitoring. Airports rely on extensive surveillance networks covering multiple areas, including terminals, parking zones, and entry points. AI-powered video analytics systems can monitor these areas in real time, detecting and alerting security teams to potential threats immediately. By analyzing camera footage continuously, AI helps operators stay focused on high-risk situations, which might otherwise be missed in a busy environment. [6]

3.2. Perimeter Protection and Intrusion Detection

With their extensive perimeters and numerous access points, airports are vulnerable to unauthorized entry and security breaches. AI-driven solutions are particularly effective at detecting unauthorized access and identifying suspicious behavior across vast areas. By analyzing data from multiple cameras, AI algorithms can track and flag unusual activities, such as individuals carrying weapons or acting suspiciously, and provide security teams with immediate alerts. This level of surveillance aids in preventing potential attacks, enhancing the overall security of sensitive zones within the airport. [7]

3.3. Access Control Using Biometrics

Controlling access to sensitive areas within the airport, such as the tarmac or air traffic control towers, is crucial for maintaining secure operations. AI-powered biometric systems, such as facial recognition, allow airports to implement highly secure access control mechanisms. These systems differentiate between authorized and unauthorized personnel, reducing the risks associated with lost or stolen access cards. By providing real-time alerts of any unauthorized access attempts, AI-driven biometric solutions streamline security protocols while maintaining operational efficiency. [8]

3.4. Automated Detection of Foreign Object Debris (FOD)

Foreign object debris (FOD) on airport runways poses significant risks to aircraft safety. Traditionally, FOD inspections are carried out manually, but AI solutions have introduced automated FOD detection, ensuring continuous runway monitoring and rapid response to any hazardous items on the tarmac. By reducing the need for frequent manual inspections, AI-powered FOD detection helps minimize runway downtime and prevent costly damage to aircraft, boosting both safety and operational continuity. [9]

3.5. Unattended Baggage and Lost Item Detection

Unattended baggage and lost items are frequent occurrences at airports, presenting both security risks and operational challenges. AI systems can automatically detect unattended items, such as suitcases or bags, that have been left in public areas. These systems track objects in real time and alert security personnel if any item is left unattended for a specified period. This not only aids in the timely management of security threats but also streamlines lost-and-found procedures by tracing items back to their owners. [10]

3.6. Reducing Congestion and Improving Efficiency

AI also enhances operational efficiency in airports by monitoring crowd density and predicting congestion. AI-powered systems can identify bottlenecks and optimize passenger flow, thereby reducing waiting times at security checkpoints and boarding gates. Additionally, AI assists in passenger verification, eliminating the need for repetitive ID checks, which can help prevent queues and improve the travel experience. These efficiencies not only enhance security but also contribute to a more streamlined and convenient airport environment. [11]

4. Case Study: Evaluating the VIP Eye System for Enhanced Security at Sofia Airport

As Bulgaria's primary international gateway, Sofia Airport plays a crucial role in the nation's critical infrastructure, making security innovations a top priority. The testing of the VIP Eye system at Sofia Airport illustrates an exploratory use of artificial intelligence (AI) in Bulgarian airport security, with a focus on evaluating AI's potential to address specific security threats in high-traffic areas. This industry collaboration aligns with Bulgaria's national AI strategy, which emphasizes the importance of secure, responsible AI adoption within critical sectors.

VIP Eye, developed by VIP Security, a Bulgarian company with extensive expertise in physical and technological security solutions,

is designed as an AI-driven solution capable of detecting weapons, identifying masked faces, recognizing physical altercations, and flagging unattended items or potential fire risks. The following case study examines the collaborative testing and feedback process between Sofia Airport and VIP Security, highlighting the system's capabilities and the implications for future airport security operations. [12]

4.1. Overview of VIP Eye Capabilities

VIP Eye is built to automate threat-detection processes that are essential in airport security environments. Its primary features include:

- **Weapon Detection:** Through AI algorithms, VIP Eye can detect firearms and other weapons, potentially reducing response times during critical incidents.
- **Masked Face Recognition:** This function enables VIP Eye to identify individuals wearing masks or obscuring their faces, a capability that could support efforts to control unauthorized access or manage identity verification challenges.
- **Physical Altercation Recognition:** VIP Eye is designed to recognize physical confrontations or group clashes, providing real-time alerts to security personnel for swift intervention.
- **Additional Safety Features:** The system also identifies forgotten items and smoke or fire risks in terminal areas, addressing two significant security concerns in airport environments.

These functionalities enable VIP Eye to address multiple threat scenarios simultaneously, offering an enhanced level of vigilance that could alleviate some of the pressures faced by human operators in busy airport settings. [13]

4.2. Collaborative Testing and Feedback Process

The testing of VIP Eye at Sofia Airport was conducted as a collaborative effort between VIP Security and the airport's security team, with Sofia Airport providing situational feedback based on their security operations. During this trial phase, VIP Eye's effectiveness in detecting unattended items and fire risks was assessed, contributing to the airport's operational efficiency. The system's performance in these specific areas highlighted its potential usefulness in addressing key airport security concerns.

While this trial did not involve official integration, it provided VIP Security with valuable insights into VIP Eye's performance in a real-world, high-traffic environment. This collaborative process enabled refinement of the system's adaptability for potential future applications in airport security, underscoring the reciprocal benefits of the testing. [14]

4.3. Potential Operational Impact

Although VIP Eye has not been formally adopted by Sofia Airport, the system demonstrates the potential of AI to support airport security operations by automating threat detection tasks. This automation could help reduce the cognitive load on security personnel, allowing them to focus more on response rather than continuous monitoring. The airport's security director noted that, during testing, VIP Eye served as a consistent and reliable asset in the security workflow, enhancing operational efficiency without the limitations of human fatigue or stress.

In conclusion, the VIP Eye system's trial at Sofia Airport provides an example of how AI-driven technology might eventually integrate into airport security strategies. While further evaluations are needed to determine the feasibility of full implementation, the collaborative testing process highlights AI's promise in enhancing security accuracy and operational efficiency in critical infrastructure environments. [15]

5. Challenges and Considerations in AI-Driven Airport Security

While previous sections have discussed AI's potential to enhance airport security through advanced threat detection and operational efficiency, implementing these systems within critical infrastructure such as airports presents several unique challenges. These challenges are particularly relevant to Bulgaria's ongoing efforts to modernize its national security framework and enhance protections at high-traffic points like Sofia Airport. Key considerations include ensuring high accuracy and reliability of AI systems, addressing ethical implications, and safeguarding passenger privacy. [16]

5.1. Accuracy and Reliability in Threat Detection

In airport security, the accuracy and reliability of AI systems are paramount to ensuring effective threat detection. AI technologies in this context rely on precise identification capabilities to distinguish between genuine threats and benign objects or behaviors. However, without regular updates, rigorous testing, and careful monitoring, these systems can yield false positives or overlook actual risks, undermining both security and operational flow. Improving reliability in such high-stakes environments requires adaptive risk assessment techniques, which can enhance the robustness of AI solutions across varying airport conditions. For Bulgaria's critical infrastructure, these factors are vital, as any inconsistency in detection could compromise not only airport operations but also public safety and national security.

Additionally, while certain experimental AI applications, such as systems analyzing micro-expressions to detect deception, may seem promising, they remain largely unvalidated and could introduce errors in threat assessment. Relying on such technology prematurely could lead to both operational inefficiencies and potential misinterpretations of passenger behaviors, underscoring the need for rigorous validation in high-traffic environments like airports. [17]

5.2. Ethical and Privacy Considerations

Implementing AI in airport security brings critical ethical and privacy concerns, particularly in terms of data transparency and passenger rights. Ensuring AI algorithms avoid biases is essential, as any unintended biases could disproportionately affect certain groups of travelers. An ethical framework that focuses on responsible autonomy and proactive engagement with social values is necessary to support AI's integration in airport security, providing assurances that technology aligns with both legal standards and public expectations.

Passenger privacy is also a central concern. AI systems used in security screenings often process sensitive personal data, such as biometric information and travel history, to enhance operational efficiency. However, this data must be handled in compliance with privacy regulations to protect against unauthorized access or misuse. For Bulgarian airports, maintaining passenger trust through transparent data practices is essential. Clear policies should inform travelers about how their data is collected, processed, and safeguarded, balancing the security benefits of AI with respect for individual privacy rights.

In summary, while AI holds significant potential to transform airport security, addressing these challenges is critical to align the technology with the unique demands of Bulgaria's national infrastructure and broader European security frameworks. By ensuring that AI applications remain accurate, ethically sound, and privacy-conscious, Bulgaria can better integrate AI into its critical infrastructure while maintaining public trust and enhancing national security. [18]

6. Conclusion

The integration of artificial intelligence in airport security marks a pivotal advancement for safeguarding critical infrastructure, particularly in high-stakes environments like airports. Through the use of AI-powered solutions, such as the VIP Eye system tested at Sofia Airport, this paper has illustrated how AI can enhance situational awareness, automate threat detection, and improve response times. These capabilities not only streamline security processes but also allow airport security personnel to allocate resources more effectively, ultimately elevating both safety and operational efficiency.

Despite the clear advantages, the deployment of AI in airport security also presents challenges that warrant careful consideration. Issues of accuracy, ethical concerns regarding privacy, and the need for rigorous reliability testing are essential factors for responsible AI implementation. Addressing these challenges will require ongoing refinement of AI models and close alignment with regulatory standards, ensuring that AI remains a trusted and effective tool for airport security.

As the role of AI in security technology continues to grow, its potential to transform airport operations and passenger experiences becomes increasingly apparent. By embracing AI thoughtfully, Bulgarian airport authorities have an opportunity to set a standard for innovation in security while maintaining public trust and upholding high ethical standards.

References

1. European Commission. "Bulgaria AI Strategy Report." AI Watch, 2020. Available at: https://ai-watch.ec.europa.eu/countries/bulgaria/bulgaria-ai-strategy-report_en. Accessed 10 November 2024.
- 2-3. Ministry of Transport, Information Technology and Communications. Concept for the Development of Artificial Intelligence in Bulgaria until 2030. Sofia, Bulgaria, 2020, pp. 13-15. Available at: <https://www.mtc.government.bg/sites/default/files/conceptforthedevelopmentofaiinbulgariauntil2030.pdf>. Accessed 10 November 2024.
4. European Commission. "Bulgaria AI Strategy Report." AI Watch, 2020. Available at: https://ai-watch.ec.europa.eu/countries/bulgaria/bulgaria-ai-strategy-report_en. Accessed 10 November 2024.
- 5-11. Scylla. "How Leveraging AI Helps Optimize Safety and Security for Airports." Available at: <https://www.scylla.ai/how-leveraging-ai-helps-optimize-safety-and-security-for-airports/>. Accessed 10 November 2024.
- 12-13. VIP Security. "VIP Eye." Available at: <https://vipsecurity.bg/vip-eye/>. Accessed 10 November 2024.
- 14-15. Летище София. "VIP Eye Interview @Sofia-Airport." YouTube, 7 October 2024, https://www.youtube.com/watch?v=kPqlkNK_q2c. Accessed 10 November 2024.
- 16-18. Pik, E. "Airport Security: The Impact of AI on Safety, Efficiency, and the Passenger Experience." *Journal of Transportation Security*, vol. 17, no. 9, 2024, pp. 7-9. Available at: <https://doi.org/10.1007/s12198-024-00276-6>. Accessed 10 November 2024.

Will Ukraine remember the support given by the EU?

Vasile Silviu

Armed Forces Academy „Alexandru Cel Bun”

Security And Defence Department, Doctoral School, Chisinau, Republic Of Moldova

Abstract: *The EU integrates new members through the enlargement process once they meet a number of political and economic conditions. The process encourages democratic and economic reforms in countries that want to become EU members and promotes greater stability and prosperity in Europe.*

Enlargement is the process whereby states join the European Union, after they have fulfilled a set of political and economic conditions.

Any European state which respects EU democratic values and is committed to promoting them may apply for EU membership.

The accession criteria, or Copenhagen criteria (named after the 1993 Copenhagen European Council meeting which defined them), are the essential conditions all candidate countries must satisfy to become an EU member state. These are: political criteria: stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities; economic criteria: a functioning market economy and the capacity to cope with competition and market forces; administrative and institutional capacity to effectively implement the EU acquis (body of common rights) and ability to take on the obligations of EU membership. The EU's capacity to take in new members, while maintaining the momentum of European integration, is also an important consideration.

Introduction:

Ukraine applied for EU membership in February 2022 and was granted EU candidate status in June 2022. The EU held its first intergovernmental conference with Ukraine in June 2024 and issued its opinion on the application for EU membership.

On 23 June 2022, the European Council granted candidate status to Ukraine. It invited the European Commission to report to the Council on the fulfilment of the conditions specified in the Commission's opinion on the membership application. Parallel to the enlargement process, the EU and Ukraine also cooperate to strengthen political and economic relations, including through the Eastern Partnership. Since 2017, an association agreement between the EU and Ukraine is in force and the partners have been continuously working on its implementation, aimed at further deepening Ukraine's political association and economic integration with the EU. The EU and its member states firmly condemn Russia's unprovoked and unjustified military aggression against Ukraine and will continue to provide political, financial, economic, humanitarian, military and diplomatic support to Ukraine and its people for as long as it takes and as intensely as needed. EU measures in support of Ukraine include: economic assistance, military support, humanitarian aid and civil protection, welcoming refugees, investigation and prosecution of war crimes, protection of children. The EU has adopted an unprecedented number of sanctions in response to Russia's war of aggression against Ukraine and the illegal annexation of Ukraine's Donetsk, Luhansk, Zaporizhzhia and Kherson regions, all those measures are designed to weaken Russia's economic base, depriving it of critical technologies and markets and significantly curtailing its ability to wage war.

The association agreement under the Eastern Partnership is the main tool to bring Ukraine and the EU closer together and it promotes deeper political ties, stronger economic links, respect for common values.

The Association Council is the main body established under the EU-Ukraine association agreement to monitor and supervise the implementation of the agreement.

In March 2024 took place the meeting of the EU-Ukraine Association Council and they exchanged views on the situation following Russia's war of aggression and touched on wider global and regional issues. They also discussed the implementation of the association agreement since the start of the Russian war of aggression. The enlargement process entered a new phase with fresh momentum in 2024. Following the December 2023 European Council decision to open negotiations with Ukraine, the first intergovernmental conferences opening the negotiations was held on 25 June 2024.

In spite of Russia's ongoing war of aggression, Ukraine maintained its strong commitment to reform across many sectors. The Ukraine Plan, endorsed in April 2024 and serving as a comprehensive reform strategy, contributed to strengthening broader policy commitments within the enlargement process. With the Ukraine

Facility, the EU continues to tie its financial support for the recovery with the reforms needed to lift Ukraine's economy and to help it on the path towards accession. The EU-Ukraine joint security commitments signed in June 2024 stated that security, resilience and defense support, as well as Ukraine's EU accession process, support to reforms, macro-financial, humanitarian and reconstruction assistance reinforce each other. For its part, Ukraine committed to continue undertaking reforms in line with its EU path, including in the security, defense and intelligence sectors. Russia's war of aggression against Ukraine continues to cause a massive displacement of the population within Ukraine and the wider region. Countries in the wider region have continued to host Ukrainian refugees, contributing to protection and integration efforts. The EU and its partners are doing their utmost to help Ukraine and we have seen high levels of support and unprecedented political decisions. The EU has reacted swiftly, adopting unprecedented sanctions against Putin's regime, and its collaborator, the Lukashenko regime. As part of the EU solidarity response with Ukraine, the European Commission suspended all import duties on Ukrainian exports to the EU until June 2025. The Commission also established 'Solidarity Lanes' to help Ukrainian grain and other agricultural goods to reach their destinations through alternative routes to the Black Sea ports blocked by the Russian navy, using all relevant transport modes through EU Member States. It should also ensure that Ukraine could import goods of first necessity (such as humanitarian aid, food, animal feed, fertilizers, fuel). The EU's Solidarity Lanes have helped Ukraine export 136 million tonnes of cereals, oilseeds and other related products until now. EU Member States and their citizens are showing impressive solidarity with the Ukrainian people. Each of us can contribute to support Ukraine and its citizens to face the destructions of war and displacement.

On February 24, 2022, Russian armed forces launched a full-scale invasion of Ukraine. The EU and Parliament supported this country by condemning Russia's aggression, sanctioning those responsible and providing financial and material aid.

The EU reacted quickly and decisively to Russia's aggression, adopting restrictive measures that have massive and serious consequences for Russia and has stepped up its political, humanitarian, military and financial support of the Ukrainian economy and society and its contribution to the country's reconstruction. The Parliament also supported Ukraine's efforts to become an EU candidate country and called on EU countries to launch accession negotiations. Information is ordered in reverse chronological order, meaning the most recent event will appear at the top and the oldest at the bottom.

MEPs call on NATO allies to honour their commitment to Ukraine and pave the way for Kyiv to be invited to join the defence alliance. In the resolution, adopted MEPs stress that they expect that the accession process will start after the war is over and be finalised as soon as possible.

Until full membership is achieved, the EU and its member states, together with NATO allies and like-minded partners, must work closely with Ukraine to develop a temporary framework for security guarantees, MEPs say, which is to be implemented immediately after the war. Parliament emphasises that Ukraine's integration in both NATO and the EU would enhance regional and global security and strengthen the bonds between Ukraine and the Euro-Atlantic community. Even before Ukraine came under attack from Russia in February 2022, the EU was keen to support Kyiv and forge closer links. Since withdrawing from the Soviet Union in 1991, Ukraine has been keen to pursue its own path, including forging closer links with the rest of Europe.

Russia's Aggression Against Ukraine

Ukraine's relations with Russia have been tense due to the latter's determination to keep the country within its sphere of influence. In 2014, Russia annexed Crimea in violation of international law, a move strongly condemned by the EU. It has also been waging a hybrid war against Ukraine, including economic pressure and disinformation attacks. Two years ago, Putin launched a war of aggression against Ukraine, challenging Ukrainian aspirations for a better future and closer proximity to the EU. It is an attack not only on Ukraine, but also on freedom, self-determination and democracy. Ukraine has shown remarkable resilience in the face of this brutal attack. It showed how much force a nation fighting for its rights and aspirations is capable of. Ukraine's resilience is a source of hope for all freedom-loving people on the planet. We remain firmly convinced that Ukraine will win, with Europe standing by its side as long as necessary.

In the months prior to Russia's full-scale invasion in February 2022, MEPs expressed increasing concern about the country's military threat and called for a coordinated EU response. On 24 February 2022, Russia launched a wide-ranging attack on Ukraine. The EU responded with a series of sanctions against Russia as well as initiatives to support Ukraine. Why the EU and the European Parliament stand with Ukraine. Russia's illegal and unprovoked invasion of Ukraine is not only an attack on the country's territorial integrity, but also poses a grave risk to the security and stability of all of Europe. It's also an attack on the fundamental values the EU stands for such as freedom and democracy.

Ukraine's EU membership prospectives

In 2014, the EU-Ukraine Association agreement was adopted. The deal established political association and economic integration between the EU and Ukraine and provided for mutual free market access.

Ukraine applied for EU membership in February 2022. Parliament supported its application and called on EU countries to grant it candidate status, which happened in June 2022, and later to open accession talks, which were formally launched in December 2023.

In order to join the EU, Ukraine, like other prospective members, needs to have stable institutions guaranteeing democracy and the rule of law; a functioning market economy; and the ability to take on and carry out the obligations of EU membership. The EU is Ukraine's main trading partner.

In April 2017, the European Parliament supported an agreement to exempt Ukrainian citizens from EU short-stay visa requirements. Ukrainians who hold a biometric passport can enter the EU without a visa for 90 days in any 180-day period, for tourism, to visit relatives or friends, or for business purposes, but not to work.

There are various EU initiatives to support Ukraine's economy, aid its green transition and help the country to reform. Since Russia launched its full-scale invasion in February 2022, the EU supported Ukraine by condemning Russian aggression, sanctioning those responsible and providing financial and material aid. In 2022 Parliament approved several loans to Ukraine and supported measures to help countries taking in Ukrainian refugees. In October 2022 MEPs called for a massive increase in military assistance to Ukraine.

2023 saw Parliament call on Nato to invite Ukraine to join the alliance, fast-track proposals to speed up the production of ammunition, push for a special tribunal to punish Russian crimes, as well as many other measures to support the country. In addition, military assistance measures and with the resources made available to help Member States meet the needs of Ukrainians fleeing the war in the EU, total support to Ukraine and Ukrainians amounts to approx. €100 billion. These agreed measures will finance both the provision of equipment and supplies to the Ukrainian Armed Forces by EU Member States, including personal protective equipment, first aid kits and fuel, as well as military equipment designed to deliver lethal force for defensive purposes.

In addition, on 17 October 2022, the EU agreed to establish a two-year Military Assistance Mission in support of Ukraine (EUMAM Ukraine). This provides for training for the Ukrainian Armed Forces as well as the coordination and synchronization of Member States' own training support for Ukraine.

At the same time, the EU introduced an unprecedented package of sanctions against the Kremlin as well as the Lukashenko regime in Belarus.

In February 2024 MEPs reached an agreement with EU countries on the revision of EU's long-term budget to ensure a stable financing solution for Ukraine. The EU will provide Ukraine with €50 billion in loans and grants until the end of 2027. Over the past two and a half years, the EU has provided Ukraine with extensive support, amounting to almost EUR 122 billion, in the form of economic, military, financial and humanitarian aid, as well as assistance in various sectors. Of this amount, EUR 1.5 billion comes from frozen Russian assets. The EU continues to work tirelessly with international partners to ensure that Ukraine receives support and to hold Russia accountable for its actions.

Ukraine's path to EU membership has made significant progress, reflecting the will of its people to achieve democratic reforms. In December 2023, EU leaders decided to start accession negotiations with Ukraine in response to the country's commitment to continue reforms. Even in times of war, she continued to make progress and introduce reforms – from new legislation to expand the rights of national minorities to improving the judiciary and ensuring a system of checks and balances on power.

The EU has had increasingly difficult relations with Russia in recent years due to its attacks on Ukraine and democracy and its disinformation campaigns.

Until Russia's annexation of Crimea in 2014, the EU had been working on building a strategic relationship with the country in areas such as the economy, energy, climate change, education and conflict resolution in the Middle East. The EU also strongly supported Russia joining the World Trade Organization.

However, EU-Russia relations have become increasingly strained over the years, not least because of the Kremlin's consistent attacks on Ukraine's sovereignty, including its 2014 annexation of Crimea and the full-scale invasion launched in February 2022.

Russia's illegal and unprovoked invasion of Ukraine is not only an attack on the country's territorial integrity, but also poses a grave risk to the security and stability of all of Europe. It's also an attack on the fundamental values the EU stands for such as freedom and democracy.

In March 2022, the EU adopted its Strategic compass for security and defence, stating that Russia represented a long-term and direct threat for European security. Another source of tension is Russia's disinformation campaigns and cyber-attacks, as well as attempts to interfere in Western democratic processes.

After the annexation of Crimea in 2014, EU economic sanctions targeted Russia's financial, defence and energy sectors. Russia responded with counter-sanctions, banning around half of its agri-food imports from the bloc.

As a direct result of Russia's full-scale invasion of Ukraine, the EU has adopted a series of sanctions against the country. These include individual sanctions, economic sanctions and diplomatic measures. Ever since the start of Russia's full-scale invasion of Ukraine in February 2022, the EU and the Parliament have supported the

country by condemning Russia's aggression, sanctioning those responsible and providing financial and material aid.

Parliament has also been supportive of Ukraine's efforts to become an EU candidate country and has been calling on EU countries to launch accession talks.

Another aspect of EU-Russia relations is energy. Controversy over the new Nord Stream 2 pipeline highlighted the country's leverage as the EU's main energy supplier. In a resolution adopted in January 2021, MEPs called on the EU to immediately stop work on the controversial pipeline, which would link Germany directly to Russia. Following the Kremlin's full-scale invasion of Ukraine in February 2022, MEPs called for the EU to boost its energy independence by diversifying energy purchases and investing in renewables. They also demanded a full embargo on Russian imports of oil, coal, nuclear fuel and gas. Subsequent sanctions adopted by the EU included measures such as a ban on imports from Russia of oil and coal and introducing a price cap related to the maritime transport of Russian oil.

According to the UN Refugee Agency UNHCR, almost six million refugees from Ukraine have been registered across Europe since the war began.

On March 4, the Council of the European Union unanimously decided to activate the Temporary Protection Directive to provide quick and effective assistance to people fleeing the war in Ukraine.

This means that those fleeing war will be granted temporary protection in the territory of the European Union: rights of residence, right of access to the labor market, access to housing, social assistance, medical or other assistance and means of subsistence.

Once adopted, the temporary protection went into effect immediately and will be valid for one year. This could last up to

three years – unless the situation in Ukraine improves enough for people to return home.

Citizens outside Ukraine and stateless persons with legal residence in Ukraine who cannot return to their country or region of origin, such as asylum seekers or beneficiaries of international protection and their family members, will also benefit from protection in the EU. Others who are legally in Ukraine for a short period of time and who are able to return safely to their country of origin will be granted access to the EU to transit before returning to their country of origin.

On 23 June 2022, the EU Leaders' Summit unanimously agreed to grant Ukraine candidate status, following a recommendation by the European Commission on 17 June. On 14 December 2023, EU leaders agreed to open accession negotiations with Ukraine, which officially began on 25 June 2024 with an intergovernmental conference in Luxembourg.

Ukraine formally submitted its application to join the European Union on 28 February 2022.

Bibliography

Giles, K. (2016). Handbook of Russian information warfare. NATO Defence College Research Division.

Khaldarova, I., & Pantti, M. (2020). Fake news: The narrative battle over the Ukrainian conflict. In *The Future of Journalism: Risks, Threats and Opportunities* (pp. 228- 238). Routledge.

Khaldarova, I. (2016). Strategic Narratives of the Ukraine Conflict Projected for Domestic and International Audiences by Russian TV Channels. *Media and the Ukraine Crisis: Hybrid Media Practices and Narratives of Conflict*, Peter Lang.

Analysis of internet of things security breaches

Veselin Tselkov

University for Library Studies and Information Technologies
Sofia, Bulgaria

Abstract: The report analyzes the nature of the Internet of Things (IoT), presents a basic architectural model of IoT, and categorizes IoT according to various criteria. The most famous IoT security breaches are presented. The vulnerabilities that led to the security breaches and the scale and consequences of the impact of the breach are analyzed. Overview and analysis of IoT security breaches are the subject of this research. The main threats and vulnerabilities are systematized and the response of the world community is tracked

Keywords: IOT, INTERNET OF THINGS, SECURITY, THREATS, VULNERABILITIES, BREACHES, HACKERS

1. Introduction

Internet of Things (IoT) are devices connected to the Internet with built-in sensors for various parameters that collect and exchange data using the capabilities (network services) of the Internet. We can define IoT as a network of uniquely identifiable physical objects (a very commonly used "Internet of Things") that have the ability to collect information, and interact with various objects on the Internet. The IoT has seen significant growth in recent years, with an estimated 31 billion connected devices worldwide in 2020, and this number is expected to reach 75 billion by 2025. While IoT provides numerous benefits and conveniences, serious concerns are also present for data security and privacy. Overview and analysis of IoT security breaches are the subject of this research. The main threats and vulnerabilities are systematized and the response of the world community is tracked [1, 2].

2. The essence of the Internet of Things

The essence of IoT we can define in the following directions [6, 7]:

- Characteristics of the Internet of Things;
- Basic architectural model of the Internet of Things;
- Internet of Things categories.

Characteristic of the Internet of Things

The main characteristics of IoT we can define:

- Intelligent devices (systems) with built-in sensors, with or without an operating system;
- Collection and processing of data mainly in real time
- Use of all types of networks - local network, corporate networks and the global Internet with all kinds of connection solutions (wired and wireless);
- Permanent or periodic connections to the Internet with the possibility of using cloud technologies;
- Measurement of a large number of (different) physical parameters;
- Ability to analyze and make decisions based on the data collected by these devices;
- Ability to manage end devices (for certain type of IoT).

Basic IoT architecture model

We can define the basic architectural model of IoT at four levels:

- IoT device (system of devices) – devices with built-in sensors and a data processing and management system, including hardware and software components;
- IoT communication – technical means and communication protocols for connecting to the Internet;
- IoT processing – data and technological solutions for data collection, storage and processing;
- IoT remote access - technology solutions for remote access to IoT (system configuration, data and management).

IoT Categories

We can categorize IoT in different criteria:

- Reaction;
- Scope;
- Number of IoT.

Reaction

Depending on possible responses and feedback capabilities, IoT can be:

- Passive;
- Active.

Scope

The application of IoT is extremely diverse. One possible overview of the scope is as follows:

- Infrastructure objects and systems:
 - Infrastructure systems related to production;
 - Infrastructural objects related to public services;
 - Infrastructural facilities related to national security;
- Personal, including:
 - health care related;
 - smart devices connected to the person - smart bracelets, watches, phones, etc.;
 - smart appliances connected to consumer devices (systems) - cars, TVs, heating, lighting, etc. household appliances;
 - IoT related to security - access control systems, video surveillance, fire protection systems, etc.

Number of IoT

- Single device;
- Many devices.

3. Identification of IoT vulnerabilities and threats

The identification of vulnerabilities and threats is based on the clear construction of the basic architectural model and the precise categorization of the specific IoT system. The main vulnerabilities and related threats can be found in the following areas:

- Vulnerabilities and threats related to the security of information and information systems;
- Vulnerabilities and threats related to privacy and privacy of individuals.

Security vulnerabilities and threats

At the different levels of the underlying IoT architectural model, vulnerabilities and threats are:

- IoT device (system of devices) level;
 - Security mechanisms are not included in the design and creation;
 - Low computing power;

- Minimum capabilities of the operating system;
- Weaknesses in configuration and updates;
- Weak (missing) access control mechanisms = to the device and data;
- Lack of physical security measures;
- Training and awareness;
- IoT communication:
 - The variety of communication protocols;
 - Lack of protection (encryption and access control) during data transmission;
- IoT Processing:
 - Not clear data processing technology;
 - Lack of data protection measures;
 - Unknown access control mechanisms;
 - How third party data is protected;
 - Lack of accountability for data processing;
 - The lack of an incident response system
- IoT remote access (mostly for mobile applications):
 - Weak access control mechanisms (passwords, digital certificates, etc.);
 - Unsecured communication;
 - Ability to install malicious software;
 - Weaknesses and gaps in training and awareness;
 - Lack of accountability for actions.

Summary of IoT Security Threats

Despite the many opportunities IoT opens up for businesses, there are many factors that create security threats. For example, for many open source sources, hackers are well versed in the specifics of the code. Here are some other threatening factors:

- **Use default passwords.** Most companies ship devices with default passwords and don't even advise you to change them. This is often the case with security cameras, home routers and lighting control systems, for example. One of the most significant IoT security risks is that default passwords are widely known, making it easy for thieves to compromise them.
- **Insecure communication.** Messages sent over the network by IoT devices are often not encrypted, creating IoT security issues. Using standards such as Transport Layer Security (TLS) and transport encryption is the best way to ensure a secure connection. Using multiple networks to isolate devices also ensures secure and private communication, preserving the privacy of the data sent.
- **Leakage of personal information.** Savvy data thieves can cause significant harm even by simply learning Internet Protocol (IP) addresses from IoT devices without patching. These addresses can be used to determine the user's exact location and residential address. Many Internet security professionals advise using a Virtual Private Network (VPN) to hide your Internet Protocol address and secure your IoT connection.
- **Automation and AI.** AI technologies are already being used on a global scale. But automation has a downside: it only takes one programming error or faulty algorithm to bring down the entire AI network and the infrastructure it was responsible for. Automation and artificial intelligence are just pieces of code. So if cybercriminals gain access, they can take control of the automation and do whatever they decide. Therefore, ensuring that tools are protected against such hazards and attacks is critical.

The main reason for the existence of vulnerabilities and threats related to the confidentiality and integrity of data is the lack of (or inadequate) policy and a multitude of rules and procedures for the implementation of this policy [3, 4].

4. Overview of IoT security breaches

Hackers have the power to launch attacks and access thousands or millions of unprotected connected devices, destroying infrastructure, bringing down networks or accessing sensitive data. Here are some of the most illustrative cyberattacks demonstrating IoT vulnerabilities.

IoT security breaches in infrastructure objects and systems

A brief overview and analysis of the security breaches is as follows:

Stuxnet (Stuxnet, 2010). Stuxnet is perhaps the most famous IoT attack. Its target is a uranium enrichment plant in Iran. During the attack, the Siemens Step7 software running under Windows was compromised, giving the worm access to the industrial programmable logic controllers. This allowed the worm's developers to control various machines at industrial sites and gain access to vital industrial information. Stuxnet is a highly sophisticated computer worm that became widely known in 2010. It used previously unknown Windows zero-day vulnerabilities to infect target systems and spread to other systems. Stuxnet primarily targeted the centrifuges at Iran's uranium enrichment facilities with the intention of covertly derailing Iran's then-nascent nuclear program. However, Stuxnet was modified over time to be able to target other infrastructure such as gas pipelines, power plants and sewage treatment plants. The first indications of a problem with the nuclear facility's computer system emerged in 2010. When IAEA inspectors visited the Natanz plant, they saw an unusually high rate of uranium enrichment centrifuges breaking down. Multiple malicious files were later found on Iranian computer systems in 2010. The Stuxnet worm was found to be included in these malicious files. Although Stuxnet was publicized in 2010, its development is believed to have begun in 2005. It is considered to be the world's first cyberweapon and therefore generated significant media attention. The worm reportedly destroyed nearly a fifth of Iran's nuclear centrifuges, infected more than 200,000 computers, and caused physical degradation to 1,000 machines. Iran has not provided detailed information on the results of the attack, but the Stuxnet virus is believed to have damaged 984 uranium enrichment centrifuges. This is estimated to have resulted in a 30% reduction in enrichment efficiency.

Although no one has officially claimed responsibility for Stuxnet, it is widely believed to be a joint creation of the US and Israeli intelligence agencies. The secret program to develop the worm was reportedly codenamed "Olympics," which began under President George W. Bush and then continued under President Obama. The goal of the program was to thwart, or at least slow down, Iran's emerging nuclear program.

The Stuxnet malware was initially installed at four engineering firms linked to Natanz - a key site in Iran for its nuclear program - relying on the sloppy use of USB sticks to carry the attack into the facility. To this day, it remains one of the most advanced malware attacks in history. Stuxnet is important for a number of reasons:

1. It was the world's first digital weapon. Rather than simply hijacking targeted computers or stealing information from them, Stuxnet escaped the digital realm to cause physical destruction to the equipment controlled by the computers. This set a precedent that attacking another country's infrastructure via malware was possible.
2. It was created at the level of a nation state, and although Stuxnet was not the first attack in the history of cyberwarfare, it was considered the most sophisticated at the time.
3. It was very effective: Stuxnet reportedly destroyed nearly a fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000

computers and caused the physical degradation of 1,000 machines.

4. It used four different zero-day vulnerabilities to spread, which was very uncommon in 2010 and is still uncommon today. Among these exploits was one so dangerous that it simply required an icon visible on the screen – no interaction required.
5. Stuxnet highlighted the fact that air-gapped networks could be breached – in this case, via infected USB drives. Once Stuxnet was on a system, it spread rapidly, seeking out computers with control over Siemens software and PLCs

Duqu (Duqu, 2011). Duqu was designed to log keystrokes and extract data from industrial facilities, possibly to launch a later attack.

Flame (Flame, 2012). Flame is an advanced spyware that recorded Skype calls, recorded keystrokes, and collected screenshots, among other activities. Like Stuxnet, Flame spreads via a USB memory stick. It targets government and educational organizations and some private individuals primarily in Iran and other Middle Eastern countries.

Havex (Havex 2013). Havex aims to gather information from energy, aerospace, defense and pharmaceutical companies, among others. Havex malware mainly targets US, European and Canadian organizations.

The Jeep Hack (2015). In July 2015, a group of researchers tested the security of the Jeep SUV. They were able to take control of the vehicle through Sprint's cellular network by exploiting a firmware update vulnerability. They could then control the vehicle's speed and even steer it off the road.

Industroyer (Industroyer, 2016). It is aimed at targeted energy facilities. This reportedly caused a blackout in Ukraine in December 2016.

Cold in Finland (Cold in Finland). In November 2016, cybercriminals turned off the heating in two buildings in the Finnish city of Lappeenranta. Another DDoS attack was then carried out, forcing the heating controllers to reboot the system multiple times, preventing the heating from turning on. It was a serious attack as Finland experiences extremely cold temperatures at this time of the year.

The Mirai Botnet (2016). An IoT botnet (a network of computers each running bots) was used to carry out the worst DDoS attack against internet performance management service provider Dyn in October 2016. As a result, several websites were offline, including major ones like CNN, Netflix and Twitter. Once infected with the Mirai malware, computers continuously scan the network for susceptible IoT devices before infecting them with malware by logging in with well-known default usernames and passwords. These gadgets include, for example, digital cameras and DVR players.

Torii (Torii, 2017). Torii is a botnet that surpasses Mirai in complexity. Unlike Mirai, QBot and their derivatives, this botnet tries to operate more stealthily and remain on the device once installed on it. So far, it doesn't do the things that a botnet usually does, such as carrying out DDoS attacks and mining cryptocurrencies. Instead, it has a rich arsenal of features for extracting sensitive information and an architecture capable of executing various commands and codes. And all of this happens through encrypted communication," Avast says. According to the study, Torii can affect a large number of devices and runs on devices with different processor architectures, including MIPS, ARM, x86, x64, PowerPC, SuperH and others. The malware is believed to have been operational since at least December 2017.

Triton (Triton, 2017). It targeted the safety systems of a petrochemical plant in the Middle East, raising concerns about the malware creator's intent to cause physical harm to workers.

The latest (Most recent, 2018). An unnamed virus with characteristics of Stuxnet reportedly struck unspecified network infrastructure in Iran in October 2018.

The Verkada hack (2021). Verkada, a cloud-based video surveillance service, was hacked in March 2021. The attackers had access to personal information belonging to Verkada software clients and access to live feeds of over 150,000 cameras installed in factories, hospitals, schools, also shut down other sites using legitimate administrator account credentials found on the Internet. More than 100 employees were later found to have "super admin" privileges, allowing them access to thousands of customer cameras, exposing the risks associated with over-privileged users.

RaptorTrain (19.09.2024). China-Linked IoT Botnet 'Raptor Train' Revealed (2024-09-19) A massive IoT botnet involving over 200,000 compromised devices dubbed the "Raptor Train" was uncovered by Black Lotus Labs, the threat intelligence division of Lumen Technologies. The botnet is believed to be run by Chinese state-sponsored threats known as Flax Typhoon.

The investigation – which began in mid-2023 – revealed a complex network of small office/home office (SOHO) and IoT devices, including routers, NVR/DVR devices, network attached storage...

IoT security breaches in the smart home

The smart home is vulnerable. There have been cases of their smart home being hijacked by compromising Internet-connected devices. Possible consequences are changing the setting of appliances, disturbing the peace, stopping work and illegal actions. The possible locations for the breach are as follows:

Smart security cameras. It is possible to use the security cameras to access the internal network, use and modify the image from the cameras. Security gaps and break-in opportunities have been identified with a number of manufacturers.

Internet-connected fax machines. Security researchers at Check Point have discovered that fax machines have security vulnerabilities that could allow a hacker to steal data across a company's network using just a phone line and fax number. Vulnerabilities in the fax machine allow malicious software to decode the files and upload them to its memory, which could compromise confidential information or cause disruption to connected networks.

Smart TVs. According to the FBI, smart TVs have several overlooked and overlooked security issues. Security is the last thought for several smart TV manufacturers, making them vulnerable to various types of threats. Hackers can not only control your unsecured TV to change channels or volume controls, but also stalk your daily movements and conversations using the built-in camera and microphone.

Smart bulbs can be hacked. Multiple reports have revealed security vulnerabilities in smart bulbs. Hackers can compromise infrared smart bulbs by sending commands through infrared invisible light emitted by the bulbs to exploit other connected IoT devices existing in the home network.

Smartphone microphone. The smartphone microphone can be used to launch a side channel acoustic attack. Academic researchers in England and Sweden have created malware that can use a smartphone's microphone to steal device passwords and passcodes. In their report, "Hearing Your Touch: A New Acoustic Side-Channel on Smartphones," researchers claim to have discovered the first acoustic side-channel attack that represents what users type on their touch devices.

Smart coffee machine. Smart coffee machines that are connected to the Internet using special applications can be attacked by hackers to steal their owner's bank or card details. Smart coffee machines allow owners to control them remotely using their phones. Users can even give voice commands to the machines if they are connected to virtual assistant software. Coffee machines are not designed for security. They are additional gateways to your network.

Connected printers. According to the security research firm, printers that are connected to an organization's network are the potential vector for cyberattacks. In its Global Print Security Landscape, 2019 report, Quocirca addressed the potential security vulnerabilities posed by connected printers. The report highlights that 60 percent of businesses in the UK, US, France and Germany experienced a print-related data breach in 2019, resulting in data loss that cost companies over \$400,000 on average.

SUMMARY: Today, cyber means are widely used for intelligence gathering, sabotage, and information operations by many states and non-state actors, for criminal activities, strategic purposes, or both. However, ordinary computer users do not have much reason to worry about Stuxnet-based malicious attacks, as they mainly target large industries or infrastructure such as power plants or defense.

5. Responses to security threats and breaches

Global agencies warn of increased cyberattacks against IoT devices (05/02/2024). Global federal agencies are sounding the alarm about an increase in cyberattacks by pro-Russian groups targeting operational technology (OT) devices in critical infrastructure in North America and Europe. The Cybersecurity and Infrastructure Security Agency (CISA), FBI, NSA, EPA, DOE, USDA, FDA, Multi-State ISAC, Canadian Cyber Security Center and UK National Cyber Security Center have monitored these threats that can compromise the IoT for industrial control.

The US FCC (US Federal Communications Commission) is introducing IoT cybersecurity labeling. The US Federal Communications Commission has voted to create a voluntary cybersecurity labeling program for wireless consumer Internet of Things (IoT) products. Under the program, qualified consumer smart products that meet robust cybersecurity standards will carry a label — including a new "US Cyber Trust Mark" — that will help consumers make informed purchasing decisions, differentiate trusted products in the market, and create incentives for producers to meet the requirements.

Global Platform Releases Protocol Enhancing IoT Security. Global Platform has released a new secure channel protocol aimed at improving security and enabling remote control for IoT devices operating in low-power, constrained networks. The Secure Channel Protocol promises to accelerate robust adoption of end-to-end security in the IoT ecosystem while simplifying device management, maintaining regulatory compliance, and promoting sustainability through reduced power consumption.

UK Introduces First IoT Security Laws (04/03/2024). The UK has become the first country to legislate cybersecurity standards for IoT devices. The new laws that went into effect today aim to protect consumers from cyber threats and increase the nation's resilience against rising cybercrime. Under the Product Security and Telecommunications Infrastructure (PSTI) regime, manufacturers will be required by law to build security protections into every Internet-connected product. Easy-to-guess default passwords like "admin" and more, are not recommended.

6. Conclusion

The application of IoT technology provides both exceptional functional opportunities and conveniences, but also generates a large number of security, privacy and privacy risks, so the challenges of using IoT devices in terms of security are enormous.

A careful security threat assessment should precede any IoT deployment to ensure that all relevant, underlying issues are identified. Without sufficient security and data protection, IoT will not be successful in the long term.

Acknowledgments and funding

The report was prepared with the financial support of the National Science Program "Security and Defense", financed by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No. 731 of 21.10.2021.

7. References

1. Tselkov, V., Sensor devices connected to the Internet - a big challenge for privacy and data protection, Information Bulletin of the Commission for Personal Data Protection, ISSN 2367-7759, issue 5 (56), September 2015
2. Tselkov, V., Internet-based sensor systems and data protection, XIII National Scientific Conference with International Participation "Knowledge Society and Humanism of the XXI Century", October 31 - November 1, 2015, UniBIT, BAS
3. Tselkov, V., Risk management for the security of communication and information systems, Academic publishing house "About letters - About letters", 2020, p. 128, ISBN 978-619-185-445-5- pdf
4. Tselkov, V, IoT, Security and Privacy, XII International Scientific Conference "TECH. TECHNOLOGIES. EDUCATION. SECURITY 2024", SECURITY & FUTURE ISSUE 1/2024, ISSN: (PRINT) 2535-0668 ISSN: (ONLINE) 2535-082X, pp. 29-30
5. Tselkov, V, Evaluation of the security of the Internet of Things, VVMU "N. I. Vaptsarov", Scientific Conference "NATIONAL SCIENTIFIC PROGRAM "SECURITY AND DEFENSE" - STATUS AND ACHIEVED RESULTS", November 5 and 6, 2024.
6. Tselkov, V, Risk assessment model for the Internet of Things, , Collection of reports from the Annual University Scientific Conference - 2024, October 3 and 4, 2024, Volume 2, IC National Military University "Vasil Levski", ISSN 1314-1937, pp. 161=170
7. Tselkov, V., S. Denchev and Ir. Peteva, Security of information resources, Academic publishing house "About letters - About letters", 2020, 268 pages, ISBN 978-619-185-432-5
8. Scott R. Peppe, REGULATING THE INTERNET OF THINGS: FIRST STEPS TOWARDS MANAGING DISCRIMINATION, PRIVACY, SECURITY & CONSENT RICK SMOLAN & JENNIFER ERWITT, THE HUMAN FACE OF BIG DATA 3 (2012).
9. <https://www.hostduplex.com/blog/top-iot-device-vulnerabilities/#:~:text=IoT%20devices%20are%20vulnerable%20to,both%20organizations%20and%20individual%20users.>

Possibilities for using steganography methods in the quantum century

Veselka Stoyanova

National Military University, Faculty of Artillery, AAD and KIS,
1 Karel Shkorpil Str., 9700 Shumen, Bulgaria,
veselka_tr@abv.bg

Abstract: Security of confidential information has always been an important issue. The aim of this work is to present and discuss the main themes at a new level in steganography methods nowadays. This review paper introduces a comprehensive survey related to nowadays embedding techniques. Steganography is often used with cryptography so that the information is doubly protected, but the combination of these techniques ensures that even if the steganographic method is discovered, the encrypted data remains secure and unreadable without the proper decryption key. This dual-layered approach significantly enhances the overall security of the hidden information.

Keywords: STEGANOGRAPHY, DEEP LEARNING IN STEGONAGRAPY, SOCIAL MEDIA

1. Introduction

The steganography is a part of a new security reality and will help us to do really confident communication. With the approach of computerized innovations, steganography has tracked down new applications and has turned into a vital part of the domain of data forensics and cybersecurity [1-2].

There are many definitions of steganography [5-7] and the common thing in them is that it is a science in which information is hidden in digital media with the help of various technical means, and its transmission between two communicating parties is realized.

2. Steganography possibilities in the new era.

Steganography has a significantly place in area of the security in the new era, leveraging advancements in technology to enhance its capabilities and applications. Here are (see fig. 1) some of the exciting possibilities. The steganography is mainly used in secure communication, digital watermarking, data protection, blockchain technology, social media and e.g.

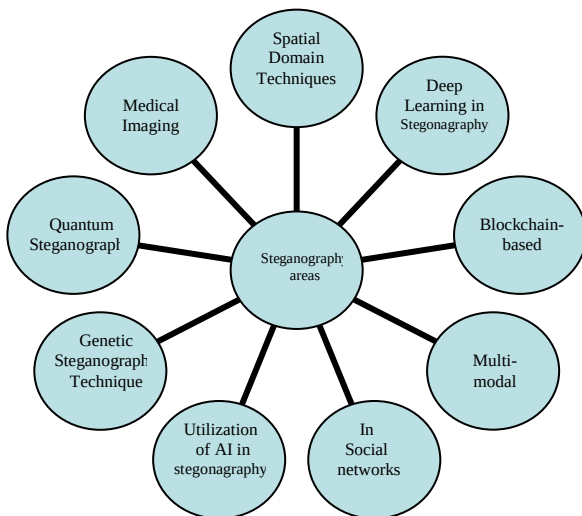


Fig. 1. New areas in Steganography techniques

Steganography in Blockchain refers to the practice of embedding hidden data (such as messages or files) within the transactions or other data structures of a blockchain, making the data invisible or undetectable to casual observers while still being accessible to those who know how to extract it.

Multi-modal steganography is an advanced technique for hiding secret information by using multiple types of media, such as text, images, audio, and video, rather than relying on a single type of cover medium. This approach enhances the security and imperceptibility of the hidden information by leveraging the strengths of different media types. This approach provides a higher level of security and flexibility compared to traditional single-modal

steganography methods, making it a promising area of research and application in the field of secure communications [3-4].

Genetic Steganography Technique represents a cutting-edge intersection of the biology and information security, offering new possibilities for data protection and secure communication in the digital age. [8] embed the QR codes into the most appropriate location by applying the Haar Wavelet technique on the resulting DNA signals and LSB (Least Significant Bit) with assist of the GA (Genetic algorithm) in order to reduce the error between the cover image and the stego-image. Experimental results have presented a high PSNR which indicate a high level of quality in stego-image with high capacity.

In [9] steganography in image segments using **Genetic Algorithm** is based on the before embedding hiding techniques it helps to find accurate places in carrier image to store the data with the less changes of bits.

The spatial-domain embedding techniques are more common in comparison with the transform domain due to its simplicity in the embedding and extraction procedures, but with less strength [10].

In the last years, the introducing of **deep learning in steganography** has presented a great improvement in the effectiveness of steganography methods. Steganography methods showed in [11–13] have been developed to improve the imperceptibility and security of steganography and they used deep learning.

Steganography in **social networks** involves hiding secret information within the content shared on social media platforms, such as images, videos, or text posts. Subject of the research was hidden information and this is showed in a great way in [16].

A book [19] on **using AI for image steganography** demonstrated how deep learning models can be trained to embed and extract hidden messages within images, achieving high levels of security and imperceptibility. They discussed different artificial intelligence techniques used to achieve maximum hidden information and high quality of image. The low quality is a sign of distortion which means that there is something hidden.

Quantum steganography is an advanced technique that leverages the principles of quantum mechanics to hide secret information within quantum states. The tools which we can use for **Quantum Steganography** is shown in fig.2.

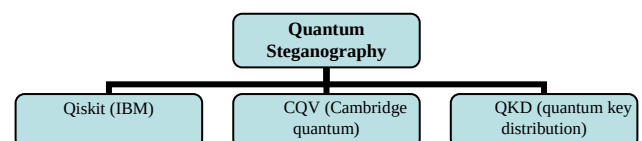


Fig.2 The most popular tools for quantum steganography

A basic knowledge of quantum information science can be read at [14]. In [15] has excellent a quantum image steganography scheme (see fig.3). In that paper [15], the authors provide us with the necessary information and components found in the quantum

image steganography field, including the quantum image representations commonly used for data hiding.

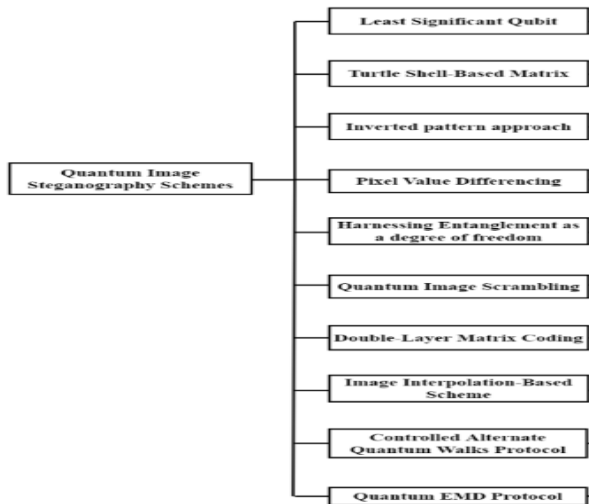


Fig.3. Implemented quantum image steganography schemes [15]

Medical imaging steganography can be used to embed patient information within medical images, ensuring that the data is securely stored and transmitted along with the image. In [17] we can see efficient authentication scheme for digital image steganography on medical images benefiting from the combination of both techniques: Support Vector Machine (SVM) and Integer Wavelet Transform (IWT). This study presents us with the various experimental analyses to establish the acceptability of the existing scheme. The simulation is performed to measure the imperceptibility using Peak Signal to Noise Ratio (PSNR) and to test the robustness using the Structural Similarity Index Measure (SSIM). The experimental result shows good imperceptibility with a PSNR of 64 dB and better robustness with a SSIM of 0.96 for the proposed steganographic scheme. The degree of similarity of the images before and after the embedding of the data, measured by the MSE and the PSNR, determines the quality of the stego-image [18].

Conclusion

In this paper was introduced a review of a comprehensive survey related to recent embedding techniques of information. The difference between the various of methods for information hiding is provided together with the information for most popular tools that can be used. Quantum steganography represents a significant advancement in the field of secure communication, offering unparalleled levels of security and privacy.

Acknowledgement

The author would like to thanks that the paper was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

3. References

1. Rabiner, L., Juang, B., An introduction to hidden Markov models., IEEE ASSp magazine, 1986;3(1):4-16.
2. Johri, P., Mishra, A., Kumar, A., Survey on steganography methods (text, image, audio, video, protocol and network steganography, International Conference on Computing for Sustainable Global Development, (2016).
3. Hu, Y., Li, H., Song, J., Huang, Y. (2020). MM-Stega: Multi-modal Steganography Based on Text-Image Matching. In: Sun, X., Wang, J., Bertino, E. (eds) Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science, vol 1254. Springer, Singapore. https://doi.org/10.1007/978-981-15-8101-4_29.

4. Hu, Y., Yang, Z., Cao, H., Huang, Y. (2021). Multi-modal Steganography Based on Semantic Relevancy. In: Zhao, X., Shi, YQ., Piva, A., Kim, H.J. (eds) Digital Forensics and Watermarking. IWDW 2020. Lecture Notes in Computer Science(), vol 12617. Springer, Cham. https://doi.org/10.1007/978-3-030-69449-4_.
5. Tasheva, A., Tasheva, Zh. & Nakov, P. Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching. In Proceedings of the 18th International Conference on Computer Systems and Technologies (CompSysTech'17), Boris Rachev and Angel Smrikarov (Eds.). ACM, New York, NY, USA, 233-240. DOI: <https://doi.org/10.1145/3134302.3134325>.
6. Kumar, P.M. & Shanmuganathan, K. L., Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate", Journal of Telecommunications and Information Technology, 2/2011.
7. Stoyanova, V. Research of the characteristics of a steganography algorithm in images when using different alphabet. In: ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference. 2024. p. 255-259.
8. Wazirali, R., Chaczko, Z., Carrion, L. (2015). Bio-informatics with Genetic Steganography Technique. In: Borowik, G., Chaczko, Z., Jacak, W., Luba, T. (eds) Computational Intelligence and Efficiency in Engineering Systems. Studies in Computational Intelligence, vol 595. Springer, Cham. https://doi.org/10.1007/978-3-319-15720-7_24.
9. Nosrati Masoud, Ali Hanani, Karimi Ronak "Steganography in Image Segments using Genetic Algorithm" IEEE Fifth International Conference on Advanced Computing & Communication Technologies pages 102-107, Feb 2015.
10. Hussain, M., A. W. A. Wahab, Y. I. B. Idris, A. T. Ho and K. H. Jung. "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46–66, 2018, <https://doi.org/10.1016/j.image.2018.03.012>.
11. Baluja, Sh., Hiding images in plain sight: Deep steganography. Advances in neural information processing systems, 2017, 30.
12. Zhu, J., Kaplan, R. Johnson, J., and Fei-Fei, L., Hidden: Hiding data with deep networks," in Proc. of the European Conf. on Computer Vision ECCV Munich, Germany, 2018, pp. 657–672.
13. Shang, Y., Jiang, S., Ye, D., and Huang, J., Enhancing the security of deep learning steganography via adversarial examples, Mathematics, 2020, vol. 8, no. 9, pp. 1–10.
14. Chuang, I., Nielsen, M., Quantum Computation and Quantum Information, Cambridge University Press, ed. 1, 2000.
15. Min-Allah N, Nagy N, Aljabri M, Alkharraa M, Alqahtani M, Alghamdi D, Sabri R, Alshaikh R. Quantum Image Steganography Schemes for Data Hiding: A Survey. *Applied Sciences*. 2022; 12(20):10294. <https://doi.org/10.3390/app122010294>
16. Dimitrov, D., Kirov, M., Методи за повишаване на достоверността на информацията при опознаване в системите за идентификация, Научна сесия НВУ "В. Левски", факултет "А, ПВО и КИС, Шумен, Сборник научни трудове, стр. 153-158, Шумен, 2010г ISSN: 1313-7433
17. Chowdhuri, P., Pal, P. & Si, T. A novel steganographic technique for medical image using SVM and IWT. *Multimed Tools Appl* **82**, 20497–20516 (2023). <https://doi.org/10.1007/s11042-022-14301-0>.
18. Rao K. R., and P. C. Yip. „The Transform and Data Compression Handbook“, 1st ed.: CRC Press, 2001.
19. Georges, J., Magdi, D.A. (2020). Using Artificial Intelligence Approaches for Image Steganography: A Review. In: Ghalwash, A., El Khameesy, N., Magdi, D., Joshi, A. (eds) Internet of Things—Applications and Future. Lecture Notes in Networks and Systems, vol 114. Springer, Singapore. https://doi.org/10.1007/978-981-15-3075-3_16

Artificial intelligence and data security

Teodora Licheva
New Bulgarian University, Sofia, Bulgaria
teodora_licheffa@abv.bg

Abstract: New technological capabilities are becoming an increasingly important part of our daily lives. If we want to be sustainable and competitive, we as a society must take advantage of them. The huge volume of data cannot be used effectively without the implementation of artificial intelligence algorithms. And to be effective and useful, data must be protected and secure.

Keywords: ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, DATA, SECURITY, TECHNOLOGIES

1. Introduction

More and more organizations are focusing on artificial intelligence, and this is due to its capabilities not only to increase productivity, but also to discover options and solutions in real time. However, everything depends on the ability of structures to use the potential of their data and thus effectively manage artificial intelligence. The presence of “dirty” data - incomplete, old or insecure, can compromise the results of even the most precise machine learning algorithms. It is a priority for citizens to have their data protected so that they do not become victims of cyberattacks, malicious actions and encroachments.



Dirty data

AI algorithms require accurate and organized data that is unmanipulated, trustworthy and secure.

2. Preparing data for artificial intelligence

For artificial intelligence to be successful, steps need to be taken to clean and update data, so that every intelligent solution will be powered by high-quality data extracted automatically from the ecosystem. It is recommended to take the following actions:

- Data management strategy

To use the potential of AI in a qualitative way, a guaranteeing framework is needed that defines secure and reliable data. Origin, storage and significance of data are key factors on which the strategy for their management should be created.

- Simplified data management methods

Creating a data structure classified in a single system will improve its visibility and accessibility. In addition, it will improve the time for performing processes and minimize the excess of resources.

- Implementation of an open data platform

Data is different in importance, focus, format, etc. and in order for it to be used in the best way, a single, flexible platform must be created that supports all data formats.

- Creating a data infrastructure

The growth of data requires the creation of a scalable infrastructure that is necessary for training with artificial intelligence algorithms.

- Automation of transfer processes

Data must be processed in real time, so it is necessary to automate the processes of its transfer. Time is of crucial importance and a main factor for timely advice and decisions.

In the current decade, generative AI is being created that can produce new content. It starts with an invitation, which can be in the form of text, image, video, design, musical notes or any input that the system can process. Then, various AI algorithms return new content in response. The content can include various formats such as essays, problem solutions, created from photos, or human audio.

With the capabilities of language models, such as ChatGPT, Google's Bard, generative AI allows the creation of economical content and can prevent many business ideas from being realized and obtaining proof of ownership. Blockchain system is used to prove ownership of content and origin. It can be used to verify the authenticity of the video - when it was created and what was edited. The potential of AI is huge for the industry and is used in a variety of processes - data processing and systematization, analysis, inventory management and supply chains. Every algorithm has limitations, and therefore hybrid solutions are being sought for the intelligent system to cope with and overcome future challenges - both technological and the ever-increasing flow of data.

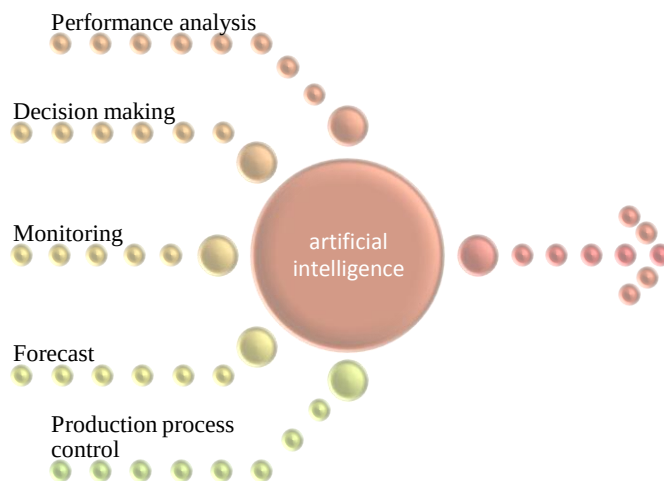


Fig. 1. Possibilities of artificial intelligence in production processes

Researchers use neural network algorithms as a tool for life cycle prediction, monitoring and system surveillance¹.

3. Regulated use of artificial intelligence

The European Union sets the first global legal framework for artificial intelligence.

A European Artificial Intelligence Office is being created in 2024², as part of the European Commission. Its aim is to create a legislative framework for the implementation of AI applications that ensures that citizens' rights are protected, data security is

¹ Zhao, R., Wang, D., Yan, R., Mao, K., Shen, F., Wang, J.: Machine health monitoring using local feature-based gate recurrent neural networks. IEEE Trans Ind Electron. 65 (2), 1539–1548 (2018). Doi: <https://doi.org/10.1109/TIE.2017.2733438>

² <https://digital-strategy.ec.europa.eu/en/policies/ai-office>

guaranteed, and a common understanding is created between them. It is necessary to encourage cooperation between researchers and stakeholders in order to achieve sustainable development of artificial intelligence technologies.

The aim of the legislative act is to create clear rules and requirements for developers and users regarding the application of AI.

A broad package of policy measures for trustworthy artificial intelligence is being adopted to prepare and establish the legislative framework. The measures are necessary to ensure the safety of the rights of people and organizations when artificial intelligence is available.

The aim of the new rules is to promote trustworthy artificial intelligence, both in Europe and beyond. To ensure that artificial intelligence systems respect fundamental rights, safety and ethical principles and to address the risks of very powerful and impactful AI models and algorithms.

Citizens need to be convinced that the innovations they are offered are safe and can be trusted. They also need to realize that they will be useful to them, will solve many of the challenges and will help society develop.

The existing legislative framework cannot guarantee that it will be able to cope with the specific challenges that AI algorithms may create. Therefore, it is necessary to analyze and pay attention to the following activities³:

- Identify the specific risks that AI applications would pose.
- Create a list of risky AI practices and a ban on the use of high-risk applications.
- Define specific obligations and parameters for employees implementing and providers of high-risk AI applications.
- Conduct a pre-compliance assessment and introduce enforcement before an AI application is put on the market.
- Create responsible structural units, both at European and national level.

4. Risk levels for AI applications

The regulatory framework defines 4 levels of risk

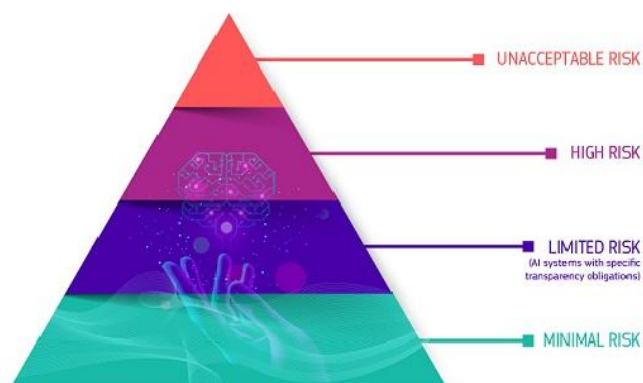


Fig. 2. Risks facing applications with artificial intelligence algorithms ⁴

Applications that incorporate artificial intelligence can be risky to people's safety, rights, and livelihoods and therefore should be banned, and if they need to be used, it should be strictly regulated, without unnecessary risks to data security.

4.1. Minimal risk

³ <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>

⁴ <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>

The legislative framework will allow AI to be used for free when the risk is negligible. This includes video games with artificial intelligence or spam filters. The majority of AI algorithms used in the EU fall into this category.

4.2. Organic risk

The limited risk is associated with a lack of transparency and clear rules when using AI applications. The legal framework provides for the establishment of mandatory transparent procedures to ensure that citizens are informed, and their trust is justified. It is important to note that if information text is published, it must be marked as artificially generated.

4.3. High risk

Remote biometric identification systems are high-risk and their use in publicly accessible places is strictly prohibited. In case an exception is required⁵, then special permissions from a judicial or other independent authority are required.

High-risk artificial intelligence algorithms have been used in the following areas:

- Infrastructure that may endanger the lives and health of citizens.
- Training to determine access to a course or educational system⁶;
- Mandatory product safety elements⁷;
- Personnel selection⁸;
- The sphere of public and private services⁹;
- Law enforcement that may violate fundamental human rights.
- Customs service management¹⁰;
- Administration of justice and legal processes¹¹.

High-risk systems using artificial intelligence need to have preliminary steps and actions before they are implemented and released to the market. The processes can be combined into the following activities:

- Ensuring the highest level of security and stability.
- Working risk assessment system and mechanisms for its reduction.
- High-quality and clean data to protect citizens from discrimination.
- Ensuring traceability of results.
- Detailed documentation for the system to assess its compliance.
- Appropriate employees to prevent risky and unregulated use of information.

5. Implementing artificial intelligence in high-risk systems

Once an AI application is launched, there are distributed responsibilities for ensuring the security of the system and the data within it.

⁵ These exceptions are very rare and often are isolated cases – searching for a missing person, preventing a terrorist threat, activities related to a perpetrator or suspect of a serious crime, etc. (author's note)

⁶ For example, grading exams (author's note)

⁷ AI algorithms used in robot operations (author's note)

⁸ AI applications for personnel selection and CV distribution (author's note)

⁹ AI credit scoring system with the potential to deny citizens the opportunity to borrow (author's note)

¹⁰ Automatic processing of applications, visa documents, vaccination certificates, etc. (author's note)

¹¹ AI algorithms for searching court decisions (author's note)

Authorities are responsible for market surveillance, implementing entities provide supervision and monitoring, and providers for the surveillance system.



Fig. 3. Steps for implementing high-risk applications based on artificial intelligence¹²

Artificial intelligence is a rapidly evolving technology, and this is understandable, because it is based on data which is collected and analyzed by big data. AI systems must be secure and reliable, not only when they are commercially available, but also when they are used. This requires quality monitoring and constant risk analysis by suppliers.

With the help of artificial intelligence, a new productivity of human labor is created, blockchain¹³ will help those who are not covered by banking, robotics will help people maintain return on investment in a targeted and very profitable way¹⁴.

6. Conclusion

Artificial intelligence has the potential to change the way people live. Its advancements and developments are being used in the workflow of organizations to automate processes that are routine and repetitive, but also for customer service and prospecting, fraud detection and quality control. For repetitive tasks that are detail-oriented, AI performs tasks better than humans because it eliminates the possibility of human error. Another role is that more and more data requires fast and relatively small errors to analyze and extract the information sought and even to predict future operations of enterprises.

The rapidly growing popularity and use of artificial intelligence is in various fields - education, marketing and advertising and even design.

In today's digital and hyper-connected world, data is the key resource of prosperity, success and competitiveness in both the public and private sectors. *"The most valuable resource in the world is no longer oil, but data."*¹⁵.

Literature:

1. Licheva, T. Modern Security in Management, Publishing House of the National Technical College of Mechanical Engineering "Industry-4.0" Sofia, 2023, ISBN 978-619-7383-30-0
2. Economist, 2017
3. Zhao, R., Wang, D., Yan, R., Mao, K., Shen, F., Wang, J.: Machine health monitoring using local feature-based gate recurrent unit networks. IEEE Trans Ind Electron. 65 (2), 1539–1548 (2018). Doi: <https://doi.org/10.1109/TIE.2017.2733438>
4. <https://aryunetworks.com/what-will-the-5th-industrial-revolution-look-like/>
5. <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>
6. <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>
7. <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>
8. <https://digital-strategy.ec.europa.eu/en/policies/ai-office>
9. <https://xn--80aahddubcb0awc4bnhip4t.bg/tema/sklad-badeshteto/etikata-chetvartata-industrialna-revolutsiya>

¹² <https://digital-strategy.ec.europa.eu/bg/policies/regulatory-framework-ai>

¹³ Licheva, T. "Modern Security in Management", Publishing House of the National Technical School of Mechanical Engineering "Industry-4.0" Sofia, 2023, p. 208

¹⁴ <https://aryunetworks.com/what-will-the-5th-industrial-revolution-look-like/>

¹⁵ Economist, 2017

Application of acoustic emission method for the diagnosis of underground gas pipeline without taking it out of operation

Leonid Vinogradov¹, Guntis Strautmanis¹, Juris Gutans¹, Yulija Soldatova¹, Viktor Prokopenko¹, Andrei Ivlijev²
 Institute of Aeronautics, Space Engineering and Transport of Riga Technical University, Riga, Latvia¹.
 Testing laboratory Tallinn, Estonia²

E-mail: leonids.vinogradovs@rtu.lv, Guntis.Strautmanis@rtu.lv, Juris.Gutans@rtu.lv, Julija.Soldatova@rtu.lv, prokopenkovik@gmail.com, aivlijevi@gmail.com

ABSTRACT: The study of the acoustic properties of a pipeline section was conducted in accordance with standards regulating acoustic emission testing of pressure vessels and related activities. To achieve this objective, an experiment was performed to emit acoustic signals on the surface of the pipeline section. Based on the test results and assessment, corrective measures were prescribed to restore the pipeline to optimal operational condition. A multi-channel acoustic system was utilized to carry out the tests on the pipeline section.

KEYWORDS: ACOUSTIC SYSTEM, PIPELINE INSPECTION, LEAK TESTING, PIPELINE INTEGRITY

1. Introduction

The Acoustic Emission (AE) method is based on the occurrence and propagation of elastic oscillations (AE waves) during the formation and development of defects in the material of monitored objects. These elastic oscillations are recorded and converted into electrical signals by piezoelectric sensors, which are placed on the surface of the objects according to a specific sensor placement scheme (sensor layout plan). Based on the parameters of the recorded AE signals (amplitude, duration, energy, etc.), conclusions are drawn about the hazard level of the signal sources. The location of AE sources is determined by calculating the time difference of signal arrival at various sensors.

Pipelines are a vital part of industrial infrastructure, as they play a crucial role in the transportation of liquids and gases in various industries. They are also one of the most popular modes of transport globally due to their accessibility, safety, and economic benefits. However, pipeline leaks can occur due to factors such as fatigue cracks, material corrosion, material defects, and environmental influences. A leak can result in economic losses and pose potential environmental contamination risks. Therefore, early detection of leak conditions is extremely important for ensuring the stability and reliability of pipeline systems. It should be emphasized that detection of a leak condition refers to the task of identifying the presence of a leak in the pipeline, without considering its location. Thus, detecting leak condition does not involve localization, which is inherently complex and labour-intensive to perform [1].

Acoustic Emission (AE) is an excellent tool for detecting and localizing developing defects in buried pipelines. Access to the pipeline is required only locally for the installation of AE sensors. The pipeline remains pressurized, and AE testing can be conducted on sections up to 1000 meters in length at a time. AE sensors detect turbulent flow at the leak site, and with the use of digital AE systems and specialized software, the leak location is determined. This paper provides a technical description of the AE method, outlines the necessary features of AE equipment for performing such tasks, and reports examples of successful applications of the method on an operational underground gas pipeline [2,3].

2. General provisions and brief description of acoustic emission testing (AET) and its application methodology

The study of the acoustic properties of a pipeline section was conducted in accordance with the requirements of European Standard EN 14584:2013, which regulates acoustic emission testing (AET) of pressure vessels and other related activities.

To address the task, an experiment was conducted to emit acoustic signals on the surface of an 800-metre pipeline section with a diameter of $\phi 150$ mm, wall thickness of 10 mm, and burial depth of 800 mm. Based on the test results and assessment, corrective measures (if necessary) are to be prescribed to restore the pipeline to optimal operational condition.

For conducting tests on the pipeline section, a Vallen Systeme GmbH (Germany) 8-channel acoustic emission (AE) system was used.

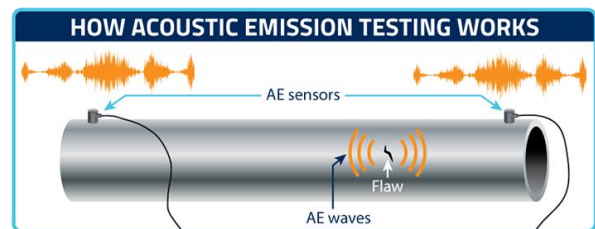


Fig. 2.1. Principle of AET

AE, or Acoustic Emission, is the emission of acoustic waves by the monitored object.

AET, or Acoustic Emission Testing (method), is a testing method based on the analysis of elastic waves of acoustic emission.

An AE source is an acoustic emission source, which is the area of the monitored object where a particular type of energy is converted into the mechanical energy of acoustic emission.

An AE signal is an acoustic emission signal, which is a changing stochastic value that reflects information about acoustic emission.

Continuous AE is acoustic emission whose mechanical signals represent a continuous wave field or are recorded as a continuous signal.[4]

AET is an acoustic emission transducer, which is a device that converts the mechanical AE signal into an electrical signal.

3. Equipment (devices)

AE registration system made by Vallen Systeme GmbH, Germany, is an 8-channel AE signal registration and record system AMSY-6 model MB6 by Vallen Systeme GmbH. It conforms to the EN13477-1 "Non-destructive testing - Acoustic emission.

This is a multi-channel modular system for collecting and processing AE information, featuring a high-speed digital data transmission channel.

It ensures continuous real-time acquisition of all test data, explosion-proof design, and the ability to automatically control the testing process.

All processing of the obtained information and calculation of AE parameters occurs directly in the module located on the monitored object, with the transmission of processed data carried out in digital form, ensuring galvanic isolation of each module.

The design principle of the system and its capabilities allow the Vallen System to be used for both mobile periodic monitoring and stationary continuous monitoring, with the ability to control the monitored object.

The cable segments connecting the modules can vary in length depending on the characteristics of the monitored objects, and the use of standard adapters allows for the extension of segment length if necessary. Furthermore, it becomes possible to position the

system and maintenance personnel at the maximum possible distance from the monitored object.

The Vallen System offers the following features: adjustable gain, software-switchable filters, pulse emission mode, a digital oscilloscope with the ability to set an independent threshold and adjustable sweep, three parametric channels with the option to reconfigure as control outputs, a temperature sensor, and a bi-colour status indicator for the AE module, all of which are available for each channel.



Fig.3.1. Vallen System AE processor unit (below) with the recording PC (on top) AE sensor VS-150-RSC

4. The object of testing

The object of testing is a section of a natural gas pipeline system (gas-methane-CH₄) consisting of 800 metres of steel pipe with dimensions $\varnothing 150 \times 10$ mm, located as part of a gas distribution installation at a burial depth of 800 mm.

A section of 800 metres of steel pipeline is between the line valves and the gas distribution station.



Fig.4.1. The object of AE testing

Conditions for AE testing

Sensors were installed in the pits on the pipe, with the working medium being compressed methane gas (CH₄);
the level of acoustic noise is no more than 57 dBA;
vibration level - there was no vibration detected during the registration of AE signals;
electromagnetic interference - no interference present;
frequency of pulsed electromagnetic interference - less than 0.01 Hz;
ambient temperature - plus 19°C;
No abnormal phenomena affecting the results of AE testing were recorded.

5. Preparation for AE testing

During the preparation for AE testing, safety measures were taken in accordance with the requirements of the current regulations (Operator of the monitored object - a 800-meter pipeline section).

Excavation work was carried out to enable the technical inspection and access to the pipe.

The insulation coating of the pipe and the condition of the shut-off valves were inspected and found to be satisfactory.

The main pressure gauge indicating the operating pressure was also checked.

The insulation layer on the pipe at the sensor attachment points was removed, and the surface (40x40 mm) was cleaned to a shiny metal finish using a grinding disc.

To reduce the level of interference, the following measures were implemented:

- a reliable alternating current source with a voltage of 220 V (50 Hz) was provided, along with secure grounding;
- all activities unrelated to the AET were halted during the AET (silent mode at the site).



4.1



4.2

Fig.5.1. Standard processing

Fig.5.2. Sensor installation locations

AE transducers of type VC-150RSC were installed to ensure reliable ultrasonic contact with the bare metal of the pipe using CIATIM-221 lubricant, and secured at the top of the pipe with rubber bands and powerful permanent magnets as holders.

The AE system was located near the midpoint of the pipe to ensure the safety of the AE testing specialists and maintain operational contact with the pipeline personnel for monitoring the stages of work. The registration of AE signal parameters was carried out by connecting the AE measurement channels in a parallel configuration on the pipe.[5]

To ensure the reliability of the AE measurements, a trial measurement of the AE signal was conducted by the AE device in the first pit, 40 meters from the gas pumping station.

The AE testing of the steel gas pipe was conducted in seven stages: first, the pressure was reduced to the accessible minimum of 20 bar, followed by an increase back to 27 bar and holding, as well as an increase to the maximum accessible pressure of 34 bar and holding, during which the gas (methane) was retained in the internal cavity for approximately 10 minutes at each holding stage.

- 1st stage - pressure - 34 bar (with subsequent reduction);
- 2nd stage - pressure - 20 bar (with subsequent increase);
- 3rd stage - pressure - 27 bar (with subsequent increase);
- 4th stage - pressure - 34 bar.

During the AE testing, preparatory measures were carried out. No electromagnetic interference or abnormal phenomena affecting the results of the inspection were observed during the AE testing.[6]

The pressure loading programme for the object of testing was coordinated based on the technological capabilities of the customer

to prevent any interruption in gas supply to consumers, without taking the tested object out of operation.

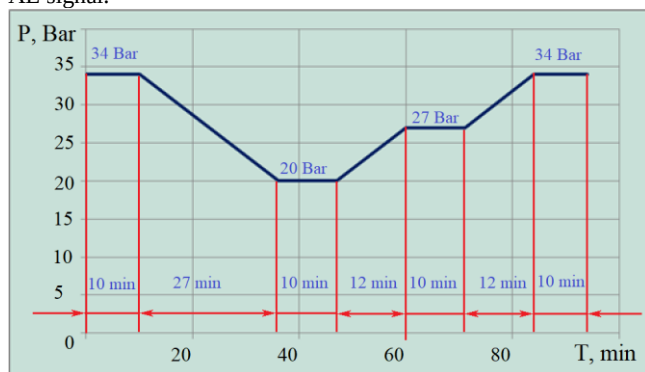
Table 1 presents the operating gas pressure at the time of testing.

Testing stage	Time, min	Operating gas pressure, bar	
		Initial	Final
1	10	34	34
2	27	34	20
3	10	20	20
4	12	20	27
5	10	27	27
6	12	27	34
7	10	34	34

Table.1 Operating gas pressure at the time of testing

Operating gas pressure at the time of the experiment - 34 bar.

T/minute - the time required to reduce the pressure by 14 bar, to increase the pressure by 7 bar, and the time required to register the AE signal.



AE diagnostics (10 min)

Fig. 5.3. Load chart of the AE testing object, with pressure holding time of 10 minutes (600 seconds).

6. Processing and presentation of AE testing results

AE signal registration was carried out during the pressure holding stage, with AE signals during pressure release and increase being filtered out.

Id	DAY	HHMMSS	MSEC	CHAN	THR	A	D	R	CNTS	E	SS
		[hhmmss]	[ms_μs]		[dB]	[dB]	[μs]	[μs]		[eu]	[nVs]
La Label 1:		16:02	Resume								
Dt	Tuesday, May 21, 2024,	Host Time:	4:02:05 PM								
La Label 2:		TimeZone:	+03:00 (FLE Standard Time)								
Ht	21 16:06:12	605.8159		3	36.1	38.1	8.2	0.3	2	755E-2	352E-2
La Label 3:		16:12	Suspend								
La Label 4:		16:39	Resume								
Dt	Tuesday, May 21, 2024,	Host Time:	4:39:03 PM								
La Label 5:		TimeZone:	+03:00 (FLE Standard Time)								
Ht	21 16:43:11	542.0959		1	36.1	44.6	1573.1	32.1	53	244E00	521E-1
Ht	21 16:46:49	952.9406		1	36.1	37.8	204.7	204.2	1	365E-1	121E-1
La Label 6:		16:50	Suspend								
La Label 7:		17:02	Resume								
Dt	Tuesday, May 21, 2024,	Host Time:	5:02:14 PM								
La Label 8:		TimeZone:	+03:00 (FLE Standard Time)								
Ht	21 17:03:05	207.9426		1	36.1	41.3	613.7	204.5	21	105E00	263E-1
Ht	21 17:13:14	816.7661		4	36.1	37.5	49.0	0.4	0	967E-2	474E-2
La Label 9:		17:14	Suspend								
La Label 10:		17:26	Resume								
Dt	Tuesday, May 21, 2024,	Host Time:	5:26:03 PM								
La Label 11:		TimeZone:	+03:00 (FLE Standard Time)								
Ht	21 17:27:50	935.6118		3	36.1	42.2	1236.7	339.6	40	199E00	445E-1
La Label 12:		17:36	Suspend								

Fig. 6.1. Table of AE test data by channels: channels No. 1 - 8

During the first holding period, two instantaneous signals were recorded on AE sensor No. 3 (at 2338.025117 seconds) and No. 4 (at 2355.18251 seconds).

AE signals did not recur during the subsequent holding stage.

All other AE signals were obtained during transitional phases and can be disregarded. The acceptable source is corrosion delamination on the inner wall of the pipe.

During the testing, the detected AE activity indicated a minor signal and is classified as "non-critical". At the time of the AE testing, the pipe showed no risk of significant defects, despite a sufficiently long period (35 years) of regular operation.[7]

It is recommended to conduct monitoring and testing at established regular intervals in accordance with the quality documentation approved by the operator.

At the time of the AE testing, the detected AE activity indicates the possible presence of minor corrosion on the inner walls of the pipe.

7. Conclusion

Based on the results of the pipeline section testing, it should be noted that the most optimal non-destructive testing method, which allows for the establishment of monitoring systems, is the integral acoustic emission method. Its application is possible for monitoring a wide range of technical devices, and its existing advantages enable the determination not only of the location but also of the hazard class of AE sources (fatigue and corrosion damage). The AE method does not require scanning the surface of the object (to assess the condition of the object, it is only necessary to install several sensors stationary on its surface), allowing for real-time monitoring of the object (On-Line). The detection of AE sources will play an even more critical role in the future, achieving its objectives while conserving valuable resources and protecting the environment. The use of scanning non-destructive testing methods is necessary as a tool to confirm registered damages.

Monitoring is effective if it is strategic in nature, aimed at achieving specific results, timely, responsive, accurate, and cost-efficient.

References

- ASTM E1002-11(2018), Standard Practice for Leaks Using Ultrasonics
- A.A. Pollock, S.-Y.S. Hsu Leak detection using acoustic emission, J. Acoust. Emiss., Vol. 1 (No. 4) (1982), pp. 237-243
- Alan S. Bandes, Detect Leaks with Ultrasound", Chemical Engineering, [online] Available: Dec. 2002, <http://www.che.com>.
- <https://doi.org/10.3390/s23239296>
- Submission received: 14 October 2023 / Revised: 17 November 2023 / Accepted: 19 November 2023 / Published: 21 November 2023
- Acoustic emission leak detection of liquid filled buried pipeline Athanasios Anastasopoulos, Bimirtios Kourousis And Konstantinos Bollas Envirocoustics ABEE, El. Venizelou 7 & Delfon, 14452 Metamorphosis, Athens, Greece
- Carjova, K., Banov, M., Vinogradovs, L., Kravchenko, S., Strautmanis, G. Acoustic Emission Method as a Means of Quality Control in Multilayer Welding of Thick-Walled Welded Joints. Latvian Journal of Physics and Technical Sciences, 2023, Vol. 60, No. 4, 40.-51.lpp. ISSN 0868-8257. Pieejams: doi:10.2478/lpts-2023-0023
- Carjova, K., Banovs, M., Unbedahts, A., Strautmanis, G., Vinogradovs L., Kurjanovics, I. Characteristics of mathematical modeling of acoustic emission method for diagnosis of fatigue cracks in the elements of marine power plants. Latvian Journal of Physics and Technical Sciences, 2023, Vol. 60, No. 5, 3.-14.lpp. ISSN 0868-8257. Pieejams: doi:10.2478/lpts-2023-0026
- Vinogradovs, L., Nasibullins, A., Banov, M., Soldatova, J., Gutāns, J. Experience of applying the acoustic emission method for monitoring systems. No: Trans Motauto World, Bulgārija, Varna, 24.-27. jūnijs, 2024. Sofija: 108, Rakovski Str., 1000 Sofia, Bulgaria, 2024, 43.-45.lpp. ISSN 2534-8493.

An approach to increase the combat effectiveness of sea bottom mines

Aleksandar Kolarov, Radostin Naydenov

Bulgarian Academy of Sciences –

Institute of metal science, equipment and technologies with Hidroaerodynamics centre “Acad. Angel Balevski”,

e-mail:aleksandar_kolarov@abv.bg; radonaydenov@yahoo.de

Abstract: *In constructing the modern sea bottom mines usually seek a compromise between tactical requirements for this type of weapon and requirements for high resistance against possible mine countermeasure-action e.g. make it a cylindrical shape when you need to put an item on the torpedo apparatus submarines, their shell is constructed in the so-called "stealth" technology and is made of non-metallic materials, increasing the quantity of the explosive when the depth of the region is greater, etc. The article proposes an approach that provides a common solution to all these requirements and allows the construction of a highly functional, versatile, high anti-mining resistance sea bottom mine that has no analogue in the naval practice.*

Keywords: BOTTOM FRAGMENTED RESURFACED MINE, LOW VERTICAL PROFILE, GROUPING NON-CONTACT FUZE

1. Introduction

Naval mines are a universal weapons and are capable of striking not only military targets, but also effectively disrupting the country's economy and military production. The mass use of mine weapons could significantly disrupt or completely sever sea and ocean transport. A mine can be a precise weapon for calculated military pressure (in a certain situation it is possible to block a naval base or a port for a certain period of time in order to demonstrate to the enemy the effect of a possible blockade). The high potential of naval mines is ensured not only due to their high tactical-technical characteristics, but also due to the high flexibility and variety of tactics for their use. According to naval experts, naval mines are "the quintessence of modern asymmetric warfare" [1].

The analysis and assessment of existing approaches to the formation of maritime security, after projecting the threats and the capabilities of the existing forces and means of the state for impact in the conditions of budget cuts, shows that an acceptable option is the realization of an impact of a synergistic nature between different types of impacts – with various forces and means, including the use of naval mine weapons. Do to this trend a significant argument is made for investing funds in scientific research and efforts to develop and improve sea mines that enable the fulfillment of the tasks set.

At the same time, it should be noted that modern mine countermeasure systems for the detection and destruction of bottom mines use the latest achievements in the field of hydro acoustics in combination with optical means, magnetometers and information technologies, which turns them into an information complex organized on many levels, and the simple detection of the bottom mine as a local sonar target against the background of the surrounding environment is increasingly transformed into monitoring the underwater situation and creating a detailed sonar map of sections of the seabed with a detailed survey for each suspicious target and fixing all local changes. Also, the development of technology for the implementation of marine robotics with the creation of autonomous underwater vehicles (AUVs), with on-board sonars providing high-resolution images of the marine environment, which are particularly effective for detecting objects on the seabed, with the embedding of "intelligence" and algorithms to detect and classify the objects in near real time and algorithms to optimally adapt the route of the AUV according to the received information in the AUVs so that it can react immediately according to the received information, in many greatly increase the effectiveness of mine countermeasure forces and means [2].

2. Prerequisites and means for solving the problem

The methods for detecting and classifying sea mines implemented in specialized mine countermeasure sonars can be broadly divided into classical image processing techniques, machine learning (ML) - the use and development of computer systems that can learn and adapt without following explicit instructions, using algorithms and statistical models to analyze and infer patterns in the data, and deep learning (DL), a type of machine learning based on

artificial neural networks, in which use processing layers to extract progressive, higher-level features from data.

Traditional seabed image processing requires expert evaluation and selection of specific features that unambiguously allow discrimination of a mine-like target, and is mostly based on combinations of back bottom (reflections from the seabed), contrast (highlight) point, background (background) and hydroacoustic shadow. The detection and classification of sea mines is a challenge due to the low quality of sonar images, which are complicated to analyze due to environmental noise causing false shadows, interference on the side sheets of antenna directivity patterns, and multipath reflection. This leads to significant variability in targets, clutter and background noise. Numerous image processing techniques have been developed to address these obstacles.

The most conventional approach for the detection and classification of bottom mines is the classical image processing approach, the performance of which depends on the image quality and the training of the operators [3].

The reliability in classification of objects largely depends on the details of their sonar image, which in turn is determined by the resolution. At low resolution - objects will appear as point targets and their image classification will be difficult or impossible. Therefore, the first direction is to increase the resolution of the sonar image in distance and angular coordinates. The necessary resolution in distance is achieved by the use of broadband sounding signals. The main difficulty lies in obtaining high linear resolution in the angular coordinate. It can be improved by increasing the frequency or the physical size of the sonar antenna.

The most promising method for obtaining high resolution in the range of side-scan sonar is synthetic aperture (SA) antenna (SAS - Synthetic Aperture Sonar). This method is based on the in-phase summation of several reflected sonar signals.

According to foreign experts, the second direction to improve the reliability of the classification is by using a set of independent images obtained during the examination from different observation points in the classification process. It is noted that in most cases three images obtained during a survey with an interval of 30-45 ° along the angle of the course with rectilinear movement of the carrier are sufficient for successful classification. To collect additional information about an object and its classification, the mine countermeasure vessels must approach the object at a distance corresponding to the range of the classification sonar and circle around it, i.e. to implement a multi-aspect survey mode that improves the reliability of classification and efficiency in searching for bottom mines [4].

The third direction is the use of interferometric processing in SSS. These stations make it possible to obtain information about the eyes in a depth strip and at the same time an acoustic image of the bottom surface, in particular to determine the distance from the bottom for the object held by the anchor. The resulting bathymetric data is very accurate, which provides a more reliable classification of objects in conditions where the bottom surface is not flat [5].

Manufactured mine warfare systems, embodying the latest scientific and technological achievements, have not exhausted their potential for further improvement and expansion of the scope of

existing weapon systems, as well as for the development of fundamentally new systems capable of performing non-standard missions. According to military experts, the new sea mines are envisioned to be modular, with sensors and effectors able to be part of a distributed network on the seabed capable of multi-phase combat operations, offering flexible, scalable, distributed, relaying, persistent and autonomous lethal and non-lethal effects of the seabed. The general concept of seabed warfare, especially in the sea mine community, is not new. What is new is the unification of diverse technologies, modular systems and platforms that can generate a variety of kinetic (in addition to the traditional high-explosive mine) and non-kinetic effects for military missions on the seabed throughout the underwater domain [6].

The basic criteria in the development of sea mines are the same for all navies in the world. They are:

- greater detection range of targets with low levels of physical fields;
- ability to strike fast-moving targets, including submarines, hovercraft and hydrofoils;
- modernization of existing explosives and development of new unified multifunctional ones;
- reducing the visibility of bottom and anchor mines;
- increasing the selective ability and impact resistance of mines;
- the state of remote control mines "active - deactivated - self-destruction";
- improving the capacity and characteristics of the power supply units;
- development of multifunctional transportable mines;
- reducing the time to attack the target and simultaneously increasing the reliability and noise resistance of the mines;
- optimization of the selection of targets from a group of targets;
- optimization of the attack trajectory;
- improvement of weight and size characteristics;
- developing systems adapted in terms of their specifications to aircraft and submarines of all navies in the world.

Regarding the implementation of new camouflage and camouflage elements in the construction of bottom mines to counter the means of detecting weapons in mine countermeasures forces and means, the main directions are [7]:

- transformational acoustics, as an unconventional theory, providing a powerful tool for the design of various types of transformational-acoustic designs, including 3D hulls of bottom mines;
- the application of new materials that absorb and/or have a low reflectivity when irradiated with hydroacoustic waves in the operating ranges of modern minesweepers;
- optimization of the profile of the mines body to meet the requirements of the "stealth" technology for dispersing sound energy in a direction other than the angle of incidence;
- use of electronic means for hydroacoustic countermeasures, integrated in bottom mines;

3. Results and discussion

In order to reduce the effectiveness of anti-mine sonars in detecting bottom mines by the size and shape of their hydroacoustic shadow and by the level of the reflected signal, a modern bottom mine must meet the following requirements:

- have a low vertical profile to form a smaller hydro acoustic shadow on the seabed;
- to be constructed of material that absorbs and/or has a low reflectivity when irradiated with hydro acoustic waves in the operating ranges of modern minesweeper sonars – 30 ÷ 600 kHz;
- the profile of the mine body must meet the requirements of the "stealth" technology for dispersing sound energy in a direction other than the angle of incidence;
- have a large reflective surface to result in shadow masking where target size filters (relative to the dimensions of known mines) will not classify it as a mine-like target;
- to have symmetry of shape due to the fact that a double search of perpendicular bearings is usually carried out and the signals from the targets are evaluated (subtracted);

- to have a low reflective energy capacity, because an assessment of the center of gravity is carried out, i.e. if a mass has a larger area it is less contrasty.

The influence of the vertical profile of the mine body on the magnitude of the hydroacoustic shadow is shown in Fig.1, where:

- H [m] – distance of the towed sonar with side view (AUV); from the bottom;
- h [m] – height of the bottom from the bottom;
- D [m] – distance between the sonar and the mine;
- S [m] – length of the hydro acoustic shadow.

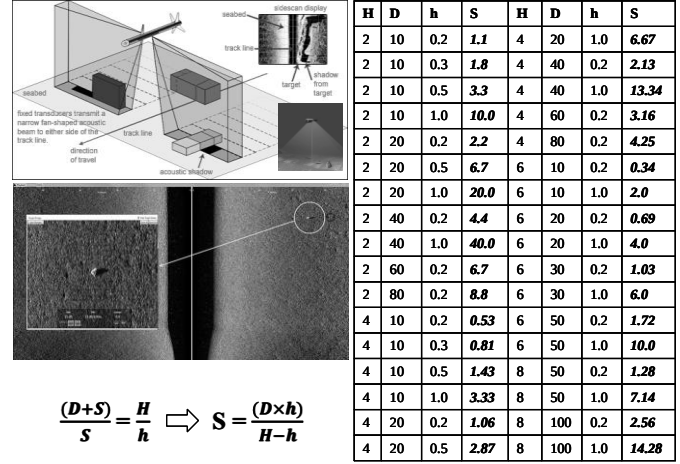


Fig. 1 Hydroacoustic shadow of a target positioned on the bottom

It can be seen that the size of the shadow of a 0.1 m high mine is 10-15% of that of the most common bottom mines with a height of about 1 m.

To satisfy the requirement of symmetry, it is expedient for the mine to have a star-shaped shape in the fragmented state (when it is in position on the bottom), and in order to reflect the sound waves in lateral directions, it is necessary that the surface of the fragments make a right angle with the plane of the bottom. The casings of the individual fragments must be made of material with reduced reflectivity. When grouping the fragments (defragmentation), the mine must acquire a cylindrical shape with a diameter allowing it to be fired from a torpedo apparatus.

From the point of view of the combat effectiveness of a bottom mine, it can be assumed that its striking ability is inversely proportional to the distance to the underwater part of the ship and directly proportional to the size of the charge. In accordance with the method of calculating the pressure of the shock wave, related to the shape and dimensions of the gas bubble, it is proved that the charge must be compact with a shape close to spherical (cylindrical) and with a minimum radius. It is known that the striking effect of a TNT charge can be calculated by the formula [8]:

$$(1) \quad P_{max} = 23800 \left(\frac{\sqrt[3]{W}}{R} \right)^{1.16}$$

where: P_{max} [dB] – acoustic pressure at the front of the shock wave; W [lb] – weight of the TNT charge; R [ft] – distance to the ship's hull.

Some dependences between P_{max} , W and R are presented in Table 1, in which k denotes the spatial coefficient of energy distribution of the gas bubble in space.

From the analysis of the results calculated by the formula, it can be concluded that the damage that can be expected from a bottom mine with a charge weight of 500 kg at a distance of 30 meters from the ship's keel is approximately equal to the damage from an underwater charge with a weight of 10 kg at a distance of 5 m from the ship's hull. Therefore, the modern bottom mine must be compact and detonate at an optimal (minimum) distance to the bottom of the target ship, which will allow it to be positioned at depths corresponding to the area of action of non-contact sensors - 100 ÷

200 m, and not of the zone of action of the striking action of a concentrated charge - 30 - 40 m for a charge of 1000 kg.

Table 1: Dependences between P_{max} , W and R

P_{max} (Pa)	R (ft)	R (m)	W (lb)	W (kg)	K	Note
1455.6	131.23	40	1653.47	750	1	
2620	131.23	40	1653.47	750	1.8	bottom
1243.2	131.23	40	1102.31	500	1	
2237.8	131.23	40	1102.31	500	1.8	bottom
954.3	131.23	40	551.16	250	1	
1717.7	131.23	40	551.16	250	1.8	bottom
2032	98.43	30	1653.47	750	1	
3657.7	98.43	30	1653.47	750	1.8	bottom
1775.6	98.43	30	1102.31	500	1	
3124	98.43	30	1102.31	500	1.8	bottom
446.3	98.43	30	551.16	250	1	
803.4	98.43	30	551.16	250	1.8	bottom
7777.8	65.62	20	1102.31	500	1	
5000	65.62	20	1102.31	500	1.8	bottom
2132.2	65.62	20	551.16	250	1	
3838	65.62	20	551.16	250	1.8	bottom
4764.7	32.81	10	551.16	250	1	
5316.4	32.81	10	220.46	100	1	
2560	32.81	10	110.23	50	1	
5772.7	16.4	5	110.23	50	1	
3967	16.4	5	44.09	20	1	
3662.4	16.4	5	22.05	10	1	
25661	3.28	1	44.09	20	1	
19809.2	3.28	1	22.05	10	1	

From the point of view of the tactics of laying mine fences, it is expedient that bottom mines, in addition to the traditional way of laying mines - on rails from the deck or with lifting and launching devices, can also be placed through the torpedo tubes of warships and submarines, i.e. is. to have a cylindrical shape with the corresponding radius.

To satisfy all these sometimes conflicting requirements with the aim of increasing the combat effectiveness of sea bottom mines, a new engineering design of Bottom Fragmented Resurfaced Mine /BFRM/ is proposed, which consists of N number of warheads that are connected by means of movable links with a central cylindrical body - grouping non-contact detonator, which contains the sensors, the power unit of the mine and a jet engine and/or an airbag, which serves to detach the body from the bottom and drive it in a vertical direction and group the warheads – Fig. 2.



Fig. 2 Bottom Fragmented Resurfaced Mine

Advantage of the mine is that provides detonation of charges grouped optimal distance from the hull of the target. Rated mine power is depending on the number of the combat bodies and the power of the charges therein. Distinctive characteristic of the mine is that it can be placed from a moving ship or submarine torpedo tube. After placing the mine fragmented and sank smoothly. The mine has a low vertical profile and makes small sonar shadow. Relatively large surface and symmetry of form make difficult mine detection and classified as a bottom mine. Protection of the mine is realized through installation of camouflage frequency broad band absorbing shell which covers the entire body. The construction of the mine allows it to stand firmly on the position of the bottom with a slope greater than that required for standard bottom mines (15°). Standard on bottom fragmented resurfaced mine has four combat units, each loaded with 10 kg of explosives. The actual impact on the target is approximately equal to that of a standard bottom mine, charged 750 kg positioned at a depth of 30 m.

Option: Instead of the standard combat body mine can be equipped with self-surfacing in command combat units and/or launch tubes for torpedoes.

BFRM is intended for destruction of underwater hull and applying martial damaged ships with medium and large displacement, submarines and amphibious ships, including hovercraft, placing position with free skiing on water deck of a ship or a torpedo apparatus of warships and submarines. Defragmentation process (grouping of elements) of the mine after

the signal from the sensor system and its swims up in optimum depth for the effective use of the striking force of the underwater blast in the realization and mining option or appropriate position (orientation) of the elements when using a cassette launch design.

The BFRM consists of:

- Grouping non-contact fuze /GNF/- cylindrical box of non-metallic material with a minimum height and a radius equal to the diameter of the torpedo apparatus. An underwater jet engine (s) is mounted (secured) at the bottom of the box. At the top is placed airbag and a bottle of compressed air for filling it. In the remaining volume is unresponsive have elements fuse and power supply unit. Jet engine design provides detachment from the bottom and adding vertical speed paid off. Airbag provides vertical sail of the mine;
- Combat bodies- corresponding to the given weight charge of mine and diameter of GNF number of combat units that have the shape of a cylindrical segment or a cylinder with a radius of 200 mm and read length - up to 3000 mm. Combat units are attached properly to the body of the cylindrical box GNF so as to provide them with free movement in the sector 180° in the vertical plane at the same time fixing their position in the horizontal plane.

Multifunctionality of the product to be characterized besides possibilities of mining staging (from a ship or submarine), and the choice of the type of combat bodies, the volume of aerbeg and power underwater jet engine. They can be realized following options as required for military use BFRM in a specific operation:

- BFRM-1 - without airbag and underwater jet engine - for anti-amphibious marine mining enclosures at a depth of 10 meters. There is no grouping of combat bodies before detonation;
- BFRM-2 - with underwater jet engine with low power and/or airbag small volume. In this variant it is ensured the compacting of the combat bodies in a compact condition after lifting the GNF at a height from the bottom equal to their length - standard version of a bottom mine, positioned at depths of $10\div40$ m;
- BFRM-3 - provides mine movement to the surface of the sea and approaching the target when the mine is placed at depths of more than 40 m, but not greater than the distance of the sensors;
- BFRM-4 - with cassette launcher structure. Each combat body has its own airbag with or without underwater jet engine, which realize the area of lesion with programmable characteristics. For small targets is possible programmed release of one or more combat bodies;
- BFRM-5 - with cassette launcher for small-scale high-speed torpedoes, equipped with autonomous guidance system. In volumes of combat bodies instead of explosive are featured compact high-speed torpedoes.

It is proposed that the mine is equipped with the following sensors:

- Acoustic /passive/ sensor
- Acoustic /active/ sensor directed by action
- Hydrodynamic sensor.

When it is necessary to increase the combat effectiveness of the mine additional sensors can be added - magnetic, potentiometric, light, etc.

4. Conclusion

The experiments carried out to evaluate the new technical solutions in the construction and operation of BFRM show that they help to a significant extent to increase the effectiveness and anti-mine resistance of sea bottom mines in the following areas:

- Versatility – can be positioned at the entire operational depth range of the emplacement area by surface ships and submarines for impact against virtually all types of surface ships and submarines;
- Multi-functionality – it is possible to use them in an optimal version according to the requirements for combat use in a specific operation or combined;
- There is a significant reduction in the effectiveness of anti-mine sonars in detecting bottom mines by the size and shape of their hydroacoustic shadow and reflected signal level. In Fig. 3 it can be seen that the hydroacoustic shadow of the BFRM is smaller

than that of a 50 liter metal barrel and significantly smaller than that of a standard bottom mine with a charge of the same TNT equivalent;

- The process of clustering the charge and moving the mine to the surface, respectively to the target, which is shown in Fig. 4, significantly increases its combat effectiveness

The new technical solutions implemented in BFRM make it unique in the military production of this type of weapons.

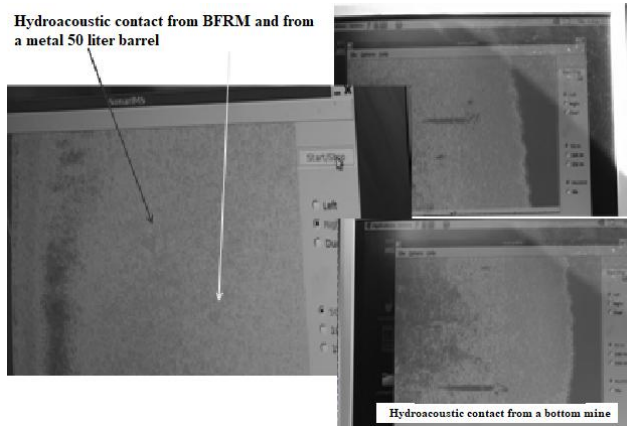


Fig. 3 Hydroacoustic shadow and reflected signal level from various objects

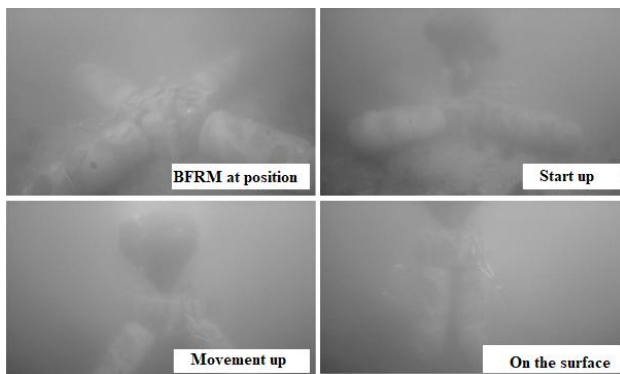


Fig. 4 Stages of mine operation

The conducted experiments show that for depths in the mine staging areas up to 70 - 80 m, it is appropriate to use an BFRM variant with a GNV with a low-power jet engine to ensure overcoming the suction force of a muddy bottom, and an airbag to ensure grouping and floating to the surface. In this case, it is important that the vertical speed of movement is sufficient to realize a detonation under the keel of the target ship at an optimal distance, or generally speaking, for the time that the target travels the distance of detection by the sensors, the mine should float under it at optimal distance to defeat the underwater part.

The proposed approach to increase the combat effectiveness of sea bottom mines is the realization of a bottom mine designed to destroy an underwater hull and to combat damage to ships of medium and large displacement, submarines and landing ships, including an air cushion, with the following innovations and design features :

- Low vertical profile of all elements of the fragmented mine body located on the bottom to minimize the hydroacoustic shadow;
- The casings of the components are made of non-metallic materials - fiberglass, which absorb and/or have a low reflectivity when irradiated with hydroacoustic waves in the working ranges of modern mining sonars - 30 kHz ÷ 600 kHz;
- The casing profiles of the mine components meet the requirements of the "stealth" technology for dispersing sound energy in a direction other than the angle of incidence;
- The supporting structure and product variants will allow the components to be profiled with maximum useful volume in a "bottom mine" variant and with appropriate launch containers for "underwater jet" and "small high-torpedo";

- A large area of the fragmented mine that filters into sonar receivers for the size of the target (by the size of known mines) does not classify it as a mine-like target;
- The symmetry of the shape reduces the efficiency of the procedure for searching for perpendicular gales by subtracting signals from the target in the receiver;
- Low reflective energy capacity - estimated at the center of gravity and if the mass is greater, it is a lower contrast;
- Mining will be carried out by free-falling the defragmented mine from the deck of the ship or on the torpedo launchers of battleships and submarines. The diameter of the defragmented mine will be tailored to the size of the selected torpedo type;
- The selected geometric shape of the fragmented body and mass-dimensional features ensure gradual deepening and positioning of the bottom;
- The process of defragmentation (grouping of the elements) of the mine after a signal from the sensor system and taking it to an optimal depth (in the mine variant) or a suitable position of the elements in the torpedo tube variant.

5. References:

1. Panevski V. S.. *Possible specific requirements for the design of mechatronic systems for security and protection of critical infrastructure*. Proceedings of the Scientific Conference "Current Security Issues", October 22-23, 2020, 6, Vasil Levski University Publishing Complex, 2020, ISSN:2367-7465 (print), 2367-7473 (online), 84 -90;
2. Tumbarska A.. *Trends in the development of non-lethal technologies and protection systems*. IMSTCHA-BAN, 2020, ISBN:978-619-7466-07-2, 402 ;
3. Dimitar Dimitrov. *Developing, implementing and maintaining an integrated physical protection system for nuclear facilities*. Collection of reports from the scientific conference "Current problems of security", 5, Publishing complex of NSU "Vasil Levski", 2020, ISSN:2367-7465, 78-86;
4. Kolev S, Nenova B, Ivanov I. *Influence of seawater depth in hydroacoustic transmission of binary numbers*. International Scientific Journal "Security&Future", 4, 3, Scientific Technical Union of Mechanical Engineering – Bulgaria, 2020, ISSN:2535-082X, 119-120;
5. Panevski V.S.. *Compatibility between design of mechatronic systems for critical infrastructure security and technological readiness levels*. International Scientific Journal "Security & Future", 4, 3, Scientific Technical Union of Mechanical Engineering "Industry-4.0", 2020, ISSN:2535-0668, 111-114;
7. Ivan Ivanov, Stoyan Kolev, Martin Lolov, Bistra Nenova. *Characteristics and features of the hydroacoustic system for management and control of underwater objects "SOM"*. Magazine "Acoustics", Year XXII, 22, Technical University - Sofia, 2021, ISSN:1312-4897, 59-63
8. Valery Panevski. *Applicable International Standardized Basis In Defining Data For Security Systems Development*. Comptes rendus de l'Acad'emie bulgare des Sciences, 77, 8, 2024, ISSN:1310-1331 (Print), 2367-5535 (Online), 1193-1200. SJR (Scopus):0.16 Q3 (Scopus).