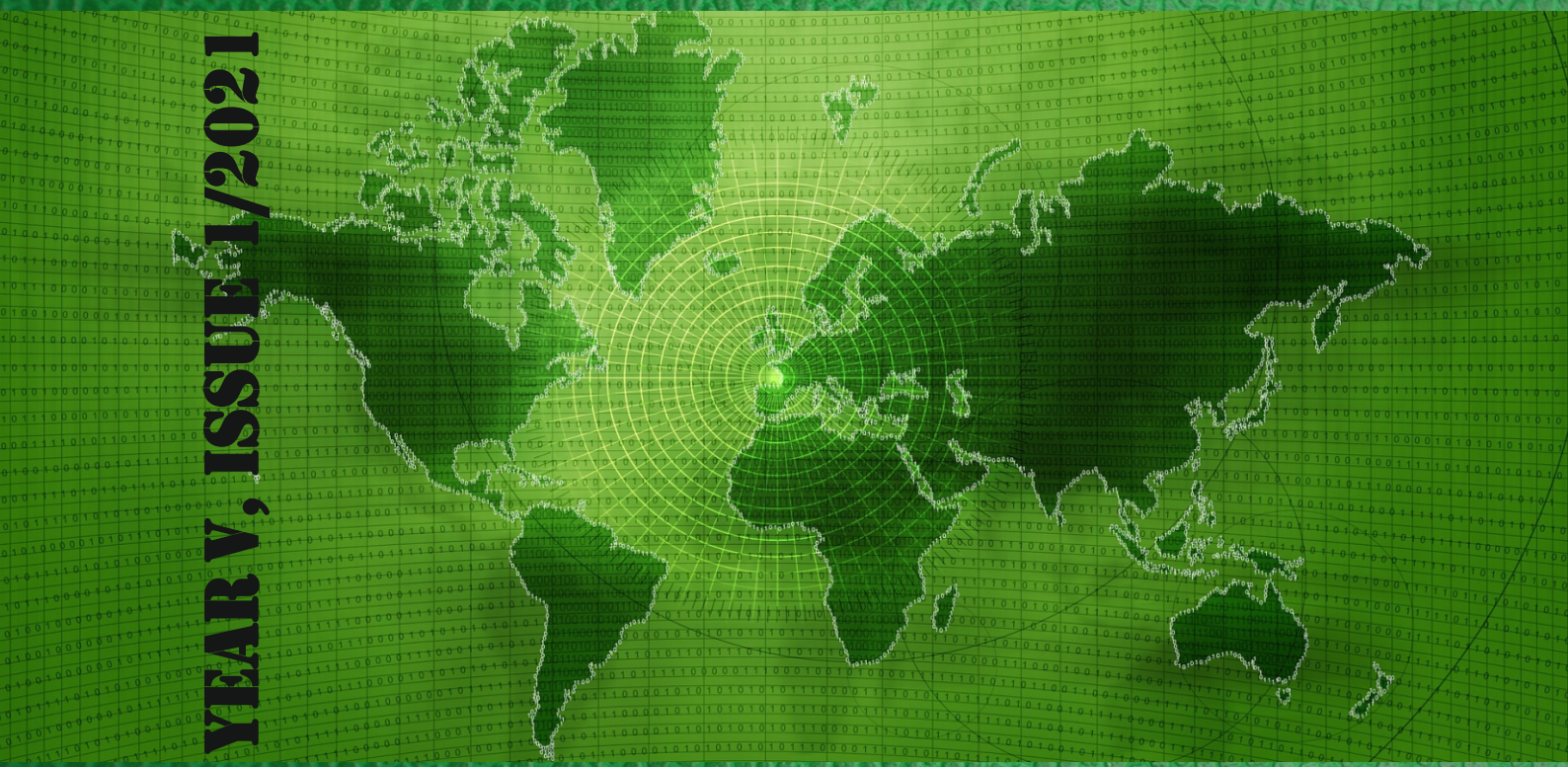
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

ISSN: (PRINT) 2535-0668
ISSN: (ONLINE) 2535-082X



YEAR V, ISSUE 1/2021

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 V, ISSUE 1 / 2021

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov
New Bulgarian University, Sofia, BG

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

C O N T E N T S

THEORETICAL FOUNDATIONS OF SECURITY

Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems develo pment - peripheral security systems
Valeri Panevski 3

Developing the opportunities for building nuclear security
Dimitar Dimitrov 7

NATIONAL AND INTERNATIONAL SECURITY

Does It Make Any Sense? – Establishing Military Bases Overseas
János Csengeri 11

Warning and reporting of biological incidents during military operations
Dimitar Nedevski, Maria Nenovska 14

Reducing the potential vulnerability of the society in case of a terrorist attack against critical infrastructure sites and facilities
Dimo Kirilov, Antoaneta Simeonova, Angel Krumov 18

The new old challenges to NATO in the Balkans
Martin Sokolov 21

INFORMATION SECURITY

Analysis of changes in the probability of an incident with information security
Petko Genchev 24

TECHNICAL FACILITIES FOR ENSURING SECURITY

Masking bottom mines by generatingimitative impulse interference
Nikolay Litchkov, Alexandar. Kolarov 28

Technical requirements and test methods of elements of equipment-specialized security remedies firefighters in incident critical infrastructure
Ivanov Ivan, Nikolova Valentina, Liliq Damyanova 32

Ensuring the safety of people, facilities and buildings from the harmful impact of the explosion
Damyanova Liliya, Nikolova Valentina, Yaneva Svetlana 36

Mobile antenna for underwater system for remote control "SOM_I"
Ivan Ivanov, Stoyan Kolev 39

Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems development - peripheral security systems

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

Abstract: *The creation of an intelligent security environment is one of the main trends in the coming years, as security technologies will be a significant part of the developed systems, incl. physical protection and system integration systems will play a key role in data collection to ensure critical infrastructure (CI) security. Organizations equipped with intelligent security systems provide increased operational efficiency by using system integration for data collection and allow systems to "communicate" and work in tandem to provide real-time information for emergency preparedness or execution.*

In addition, data collected from advanced security technologies can be analyzed by system integrators to help senior CI management better understand how their organization works and make improvements based on the information gathered. Understanding the value of connecting different physical security systems, incl. and CI peripheral security systems, as well as ways to integrate them with other systems, is a key component in developing a smarter and more secure facility. Whether applying new CI solutions or upgrading compatibility solutions, system integration offers a variety of cost options that meet the specific needs of the business environment.

Last but not least, threat information is used to determine the security regime of the CI as a basis for developing common requirements and performance targets, as well as criteria for assessing the conformity or effectiveness of physical protection systems. Modern standardized approaches have been developed, summarizing the good international practices, for determining the goals and / or requirements for physical protection, in accordance with the specifics of CI and for preventing any level of potential impact both in the sites and for the population in the neighboring territories. The development of requirements for peripheral security systems as an element of intelligent CI security systems and their integration in the CI as early as possible is the subject of this publication.

Key words: *STANDARDIZED PECULIARITY, INTELLIGENT SECURITY SYSTEMS, PERIPHERAL SECURITY SYSTEMS*

1. Introduction

System integration is the technological trend that is expected to have the greatest impact on the development of intelligent security systems (ISS) of CIs with advantages that include greater resilience and mobility of systems and accessibility for users.

An essential aspect in the development of ISS is the security regime of the organization. In order to determine the security regime of CIs, threat information is used as a basis for developing common requirements and performance targets, as well as criteria for assessing the compliance or effectiveness of physical protection systems. Contemporary standardized approaches have been developed to determine the objectives and / or requirements for physical protection, in accordance with the specifics of CI and to prevent any level of potential consequences both in the sites and for the population in the neighboring areas **[1,2,3,4,5]**.

CI management with digital vision implements large-scale innovations related to demanding solutions that help to track the technological pace in the field of security. Simplified standardized processes and an improved vision for creating a security / compatibility environment, streamlined operations and a dynamic, accurate understanding of CI status are sought. What is the goal? Proper identification of operational risks that are emerging at the moment and those that could be on the horizon, which ensures better decisions related to maintaining the functionality of CI and thus make them more secure and productive.

Operational risk management (ORM) is the new differentiator. The digital transformation and integration of ORM strategies, processes and tools provide CI management with intelligence for navigating operational risks, maintaining management and control, and continuously improving security through peripheral security systems. Moreover, ensuring the security of large areas, especially of organizations of national importance, such as military zones, nuclear sites or parliament, etc., against various possible risk events (unauthorized intrusion or terrorist acts) is difficult, complex and expensive. It is the precise determination of the input data for the development of peripheral security systems and their integration into the general system of security and management of CI that is the thematic focus of the following lines.

2. Standardized features in defining input data for development

To correct define the appropriate input data, it is useful to refer to the good international practice in the field of business continuity developments.

Also, restrictions are introduced, namely that the responsibilities of national operators for the application of the various elements of physical protection, according to the specifics of the respective CIs and the requirements of the leading international organizations, will not be considered, as they are assumed to be pre-defined, are applied and updated periodically.

2.1 Standardization base

For the purposes of publication using the following standards of the International Organization for Standardization (ISO):

- ISO 22300:2021- Security and resilience — Vocabulary;
- ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements;
- ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301;
- ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA);
- ISO 31000:2018; Risk management — Guidelines
- IEC 31010:2019; Risk management — Risk assessment techniques

The Bulgarian Institute for Standardization has introduced the standards for national application as follows: БДС EN ISO 22300:2021; БДС EN ISO 22301:2020; БДС EN ISO 22313:2020; БДС ISO 31000:2018 and БДС EN IEC 31010:2019.

2.2 Definitions

To achieve a better understanding of the proposed topic, definitions from ISO 22300: 2021 are used, namely:

- *business continuity* - "capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption";
- *business continuity management* - "process of implementing and maintaining business continuity";
- business impact analysis - "process of analysing the impact over time of a disruption on the organization;

Note 1 to entry: The outcome is a statement and justification of business continuity requirements"

- *risk analysis* - "process to comprehend the nature of risk and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Note 2 to entry: Risk analysis includes risk estimation.";

- *risk assessment* - "overall process of risk identification, risk analysis and risk evaluation

Note 1 to entry: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

Note 2 to entry: Risk assessment is described in detail in ISO 31000:2018.";

- *risk management* - "coordinated activities to direct and control an organization with regard to risk";
- *vulnerability analysis* - „process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence".

2.3 Business impact analysis (BIA)

The main source of data for building peripheral security systems is the stages "Business Impact Analysis" and "Risk Analysis" of Business continuity management systems development [ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements]

The business impact analysis is performed in accordance with ISO */TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*. Essentially, BIA is a functional assay which is carried out as part of business continuity - *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements*, in which the assessment and calculation of the qualitative and quantitative impacts on the activity of CI as a result of a probable risk event (natural disaster or man-made destruction) is performed. Qualitative impacts are related to operational aspects, such as the ability to deliver, while quantitative impacts are related to financial losses and have a digital monetary value.

Organizations (CIs) need to conduct a detailed and in-depth BIA to help their business and operational units understand the impact of a likely risk event. The BIA should list the critical and necessary business functions, the dependencies on their resources and the level of criticality to the overall organization.

The development of the Business Continuity Management Plan is based on the BIA, which helps the organization understand the impact of a devastating event on the organization. The BIA is a management-level analysis that identifies the impact of an organization's loss of resources, involving four main steps:

Step 1 - identification of critical processes and resources;

Step 2 - identification of the impact of the interruption and assessment of the outage;

Step 3 –resource requirements identification;

Step 4 - recovery priorities identification.

2.4 Risk analysis

According to item "8.2.3 Risk assessment" of ISO 22301: 2019, the risk analysis should be performed in accordance with ISO 31000. Due to the dynamic nature of the organization's security function, it is strongly recommended that the risk analysis process be reviewed regularly to identify areas for improvement. Senior management of the CI must implement and manage all security aspects of the business, including risk analysis, policies and security procedures, handling incidents training to raise awareness and emerging technologies.

The risk analysis process plays a significant role in risk management and assessment. The threats that may arise, the potential impact of the threats, the frequency of the threats and the level of confidence in the information gathered must be identified and analyzed.

As basic activities related to risk analysis can be mentioned, but not limited to:

- gathering information using automated risk assessment tools, questionnaires, interviews and reviews of policy documents;
- identification of the organization's assets and their values;
- identification of threats and vulnerabilities;
- determining the probability of threatening events and determining their impact;
- identifies risk as a combination of probability and impact (when the probability is high, the impact becomes large and the priority increases).

Good international practice and theory has identified two types of risk analysis - quantitative and qualitative:

- *Quantitative risk analysis* includes monetary and numerical values for each aspect of the risk analysis process, including asset value, threat frequency, severity of vulnerability, impact, safety costs, etc. Quantitative risk analysis has an advantage over qualitative risk analysis because it uses fewer assumptions. However, the disadvantages of quantitative risk analysis include time, data collection efforts and mathematical equations, which can be difficult and time consuming.

- Qualitative *risk analysis* includes intuition, experience, and best practices such as brainstorming, focus group, surveys, questionnaires, interviews, the Delphi method, and meetings. The advantage of qualitative risk analysis includes prioritization of risks, identified areas for immediate improvement in dealing with threats. All results of the qualitative risk analysis are subjective, reflecting the deficiency of qualitative risk analysis.

By providing the advantages and disadvantages of both risk analyzes, most organizations apply jointly - the quantitative risk analysis for tangible assets and the qualitative risk analysis for intangible assets.

2.5 Threat modeling

Organizations should apply a threat model to identify threats and potential attacks and apply appropriate mitigation measures against those attacks and threats. Threat modeling is used not only to identify threats, but also to assess threats and their impact on the organization.

This activity includes six main steps:

- identification of assets;
- identifying the sources of the threat;
- study of the currently applied countermeasures;
- identification of vulnerabilities;
- determining the priorities of the identified risks.
- identifying countermeasures to reduce risk.

2.6 Vulnerability analysis

The development of the BIA relies heavily on vulnerability analysis and risk assessment. Vulnerability assessment and penetration tests are part of the process of assessing security controls to reduce risk.

Assessing the vulnerability is often regarded as a separate step in the overall process of risk analysis. This here is about the systematic study of the CI, aiming to identify those components exposed to the highest risk of risks impact. The purpose of the vulnerability assessment is to help identify adequate security measures, as well as to analyze the correctness of these measures, after their implementation.

The vulnerability analysis includes hardware, software, or personnel to identify any weakness or lack of response. Analyzing this weakness in the absence or non-response can help reduce the risk and likelihood of an attacker or threat agent exploiting such vulnerability. The compensatory type of access control as a countermeasure to the identified vulnerabilities must be applied as it acts as risk mitigation. The organization can minimize the risk to an easier management level by applying compensatory access control.

In summary of the above, I can point out that it is the results of BIA and RA that provide information to the management of CI on:

- the assets of the CI, which must be protected;
- the probable directions for construction of peripheral security systems (PSS);
- the specifics of the area - relief, soils, vegetation, water facilities, ownership of the adjacent territory, remoteness from infrastructure, etc.
- type of MSS - stationary or portable;
- the points and the ways of integration of the PSS with the built security systems available to CI.

Based on this information, the necessary requirements of CI management for peripheral security systems can be developed.

3. Experience of practical implementation of the presented approach

Scientists and specialists from the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski" at the Bulgarian Academy of Sciences have good experience **[6,7,8,9]** in the application of international experience in the field of construction of perimeter security systems of CI (*fig. 1; fig. 2; fig. 3 and fig. 4*).

An example of this are the scientific developments in the field of security and protection of CI, which are the result of the implementation of national and international agreements, EC projects and the European Structural and Investment Funds project.



Figure 1: *Model of a mobile sensor system for perimeter security of CI.*

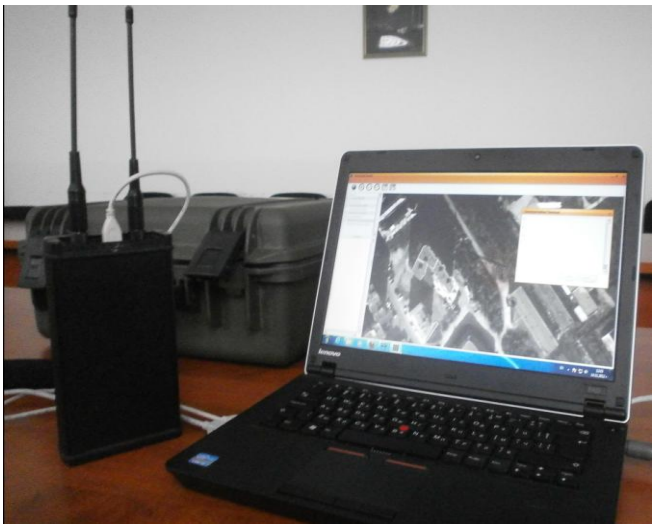


Figure 2: *Mobile local command center deployed to CI.*



Figure 3: *Mobile sensor elements from a peripheral security system.*

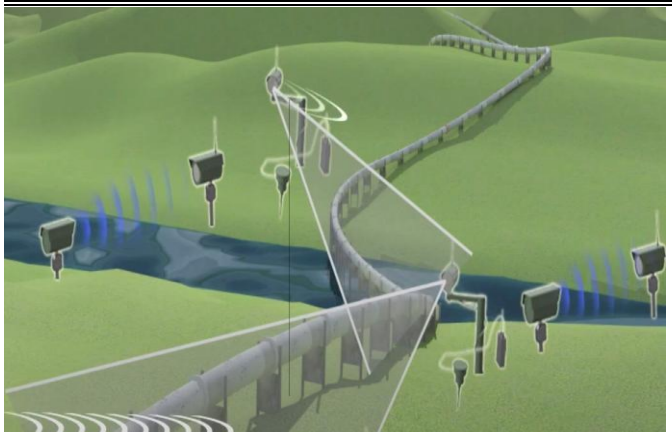


Figure 4*: Sector of Perimeter sensor system for pipeline security.* **[10]**

3. Conclusion

The applied ISO standards in the field of business continuity management, BIA and Risk management set the general framework of the process of determining the initial data for the development of peripheral security systems and their interoperability in the overall system of BCM of CI. They are only a separate step in the development of a comprehensive model, giving the main direction for determining the structure of the technical part of the model, based on the process of risk identification and assessment of the possible threat to CI and the consequences caused by the impact of a certain risk factor/ factors. The essential point is the treatment of the act of threat as a set of risk factors that may affect the assets of the organization, each of which is able to change the security and protection system of elements of the CI. The correct choice of construction and the appropriate technical level of the elements of the physical protection system also play an important role here.

This approach allows the precise distribution of functions between the management and staff of the CI, with responsibilities in the field of security and protection, related to timely planning of the necessary means for capacity building and development, with a focus on preventing and counteracting possible risk events that may to affect CI.

ACKNOWLEDGMENTS

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

Literature:

[1] Dimitar Dimitrov, "DEVELOPING, IMPLEMENTING AND MAINTAINING AN INTEGRATED PHYSICAL PROTECTION SYSTEM FOR NUCLEAR FACILITIES", Proceedings of the Scientific Conference "Current Security Issues", 5, Publishing House of Vasil Levski National University, 2020, ISSN: 2367-7465, pp. 78-86;

[2] Dimitar Dimitrov, "Comparative evaluation of techniques for modeling and simulation of interdependent critical infrastructures", Proceedings of the annual university scientific conference, 10, Publishing House of Vasil Levski, 2020, ISSN: ISSN: 1314-1937, pp. 231- 241;

[3] Pehlivanski V. "Tests in the process of designing protection systems", monograph 2020, ISBN 978-619-188-359-2;

[4] Lichkov N., Pehlivanski V., Lyaskov N., Penev N., "Method for experimental measurement of the attenuation of microwave oscillation during its propagation in a given medium", Sb. reports of the XVIII International Scientific Congress "Machines. Technologies. Materials", 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, pp. 75-78;

[5] Gueorgiev N., Boychev Y., Kosev V., "Investigation of seismic oscillations caused by one type of heavy chain technique", Sat. reports of the XVIII International Scientific Congress "Machines. Technologies. Materials", 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, 23-26;

[6] Gueorgiev N., Boychev Y., Kosev V., "Investigation of seismic oscillations caused by one type of heavy wheel equipment", Sat. reports of the XVIII International Scientific Congress "Machines. Technologies. Materials", 1, NTS in Mechanical Engineering, 2021, ISSN: 2535-0021, 27-30;

[7] Yavor Boychev, Nikolai Dyulgerov, "Preparation and properties of composites with ultrafine-grained structure", 2021, ISBN: 978-619-245-100-4, 120;

[8] Litchkov N. G., Boychev Y. D., Kosev V. I., "Analysis of the frequency characteristics of a class of seismic signals", Proceedings of the International Scientific Conference on Security "CONFSEC 2020", 4, 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 113-116;

[9] Nikolay Gueorguiev, Yavor Boichev, Konstantina Belotelova, Ivan Ivanov, "FREQUENCY CHARACTERISTICS OF SEISMIC PIEZOELECTRIC SENSORS UNDER ONE-DIMENSIONAL MECHANICAL ACTION", Journal of Theoretical and Applied Mechanics, Sofia, Vol.49 (2019), ISSN: 0861-6663 (Print), 1314-8710 (Online) pp. 130-141. Bulgarian Academy of sciences, National committee of theoretical and applied mechanics, 50, 2, 2020, ISSN: 0861-6663 (Print), 1314-8710 (Online), 130-141. SJR (Scopus):0.28;

[10] http://high-tech-ims.com/bulcip/.

Developing the opportunities for building nuclear security

Dimitar Dimitrov
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *The potential for criminal or intentional unauthorized acts involving or directed at nuclear or other radioactive material or their associated facilities and associated activities is an ongoing global concern. Because of their widespread use, nuclear and other radioactive materials are vulnerable to sabotage, or to being stolen, lost or acquired illegally by individuals or groups that may use them for malicious purposes. The objective of a nuclear security regime is to prevent, detect and respond to nuclear security events, and to protect persons, property, society and the environment from harmful consequences associated with nuclear and other radioactive materials.*

KEYWORDS: NUCLEAR AND RADIOACTIVE MATERIAL, NUCLEAR SECURITY REGIME, NUCLEAR SECURITY EVENTS, MALICIOUS PURPOSES, MALICIOUS ACTS.

1. Introduction

The fundamental goal of capacity building is to enhance the abilities of relevant stakeholders to assess, establish and implement elements of a nuclear security regime. The infrastructure needed for capacity building includes, among many other things, educational and training institutes with personnel competent in nuclear security, technical support centres, nuclear security laboratories and equipment, and the means to produce appropriate course materials.

In addressing how to build the capacity to establish, implement and sustain a nuclear security regime, it is necessary to look at the essential elements that should be in place and the underlying functions that make a security programme effective. The Nuclear Security Fundamentals [1] set out 12 essential elements of a nuclear security regime. Capacity building programmes need to be tailored to the national infrastructure and resources that are available, but also to address these 12 essential elements.

2. Objective and scope

The main objective - development of a national strategy for building the capacity of organizations and individuals to establish, implement and sustain an effective nuclear security regime [2]. The roles of governments, organizations and individuals in capacity building are defined and key elements of capacity building programmes are described. Methodologies are provided for using a systematic approach to develop capacity building programmes.

The term 'capacity' here refers to an organization or individual that has both the competence (knowledge, skills, and attitude) and capability (resources, authority, processes, equipment, means of deployment) needed to achieve their desired goal.

Capacity building for nuclear security refers to a systematic approach to the use of education, training, exercises, awareness raising, workforce management, knowledge management and knowledge networks to develop and continuously improve the governmental, organizational and individual competences and capabilities necessary for establishing, implementing and sustaining an effective nuclear security regime.

Human, technical and financial resources are necessary to ensure effective nuclear security. Infrastructure, equipment and other physical elements support a State's nuclear security regime.

3. Roles for capacity building

Capacity building programmes are typically developed with roles at the following three levels:

Governmental: Policy makers at the national level should enable capacity building by establishing the policies and frameworks within which organizations and individuals can operate effectively. Every country should clearly assign responsibilities and facilitate effective coordination mechanisms for national competent authorities and other organizations that are responsible for implementing elements of the nuclear security regime, should also allocate sufficient resources for effective implementation of these elements.

Organizational: Competent authorities and organizations involved in nuclear security should develop nuclear security capacity building programmes for management, personnel and any other relevant stakeholders that address nuclear security systems and measures relevant to their respective responsibilities. This includes fostering coordination and cooperation between relevant organizations both within and outside of the nuclear security regime.

Organizations should communicate with the government about the resources and infrastructure that they need to develop the capacity to implement nuclear security measures while continuously fostering nuclear security culture.

Individual: Individuals with responsibilities for nuclear security should develop their knowledge, skills and capabilities for nuclear security through educational, training and awareness raising activities, and through exercises. Individuals may also benefit from participating in workforce management and knowledge management activities and from knowledge networks for nuclear security.

3.1 Roles of government [1]. The distribution of governmental responsibilities for capacity building will depend upon the existing legal, governmental and organizational arrangements. Every state may take into account international guidance and best practices in selecting the most effective distribution of responsibilities.

The government should ensure that sufficient human, financial and technical resources are available to the government and to organizations with nuclear security related responsibilities, and that an appropriate number of capable individuals within the country are available to successfully establish, implement and sustain a nuclear security regime.

In this context, the government should ensure the provision of resources for building and maintaining the competence of suitably qualified and experienced staff, and promote participation in national and international sharing of knowledge.

3.2 Roles of organizations. Organizations with nuclear security responsibilities include competent authorities and other organizations that deal directly with the security of nuclear and other radioactive materials, and organizations such as law enforcement or national security organizations with broader functions that include specific roles and functions related to nuclear security.

Specific nuclear security responsibilities need specialized knowledge, skills and experience that may necessitate (in addition to appropriate personnel selection procedures) education, training

and knowledge management to ensure that adequate capacities are developed within individual organizations or at the national level.

Organizations may develop their own nuclear security capacity building programmes and/or make use of capacity building programmes implemented at the national level.

3.3 Roles of individuals. Individuals with responsibilities for nuclear security are expected to cooperate in and contribute to building their own individual competences as well as the collective competences of their organizations.

Individuals need to understand the overall objective and strategy of nuclear security within their organizations and be able to communicate effectively and appropriately their observations and experiences to help identify and resolve issues and promote continuous improvement.

As well as developing their own knowledge, skills and experience, individuals involved in national nuclear security programmes should contribute to the development and continuous availability of the necessary collective knowledge to support the nuclear security regime in the country.

Such individuals may contribute to building their and others' competences by participating in programmes of continuing education and training, including planned and on-the-job training programmes. Individuals should also strive to contribute to the body of knowledge for nuclear security in their organization and pass on this knowledge through the mentoring and training of others.

4. Capacity building elements

Capacity building includes several key elements, in particular education, training, exercises, awareness raising, workforce management, knowledge management and knowledge networks.

Education, training and exercise activities build capacity by facilitating the development of knowledge and skills, helping new and existing professionals to master the principles and technologies associated with nuclear security. In building capacity for nuclear security, awareness raising, targeting multiple audiences, can promote understanding of the importance of protecting nuclear and other radioactive materials.

4.1 Education. Nuclear security education includes individual courses and other formalized instructional activities conducted through educational institutions. Education programmes in nuclear security should aim to establish in-depth knowledge and thereby help foster a nuclear security culture [3] in a country or region. Ideally, persons interested in pursuing a career in nuclear security should be able to receive specialized education on nuclear security, as these educated individuals are expected in the future to design, implement and evaluate the State's nuclear security infrastructure.

A regional education programme could also be useful to establish a common understanding of nuclear security culture and enhance further collaboration on nuclear security with neighboring countries. Curricula for nuclear security education programmes should be developed through collaboration between the relevant stakeholders, which may include, for example, law enforcement and military academies and other designated nuclear security related organizations as well as universities and research institutions.

Education programmes may be tailored to suit the needs of the different organizations with responsibilities for nuclear security, including regulatory bodies and other competent authorities, law enforcement agencies and operators. The country may cooperate with other countries and international organizations to provide insights into the competences and resources necessary for implementing a national nuclear security education programme.

Prior to the development of curricula for such education, it may be useful to obtain experience of education in institutions in other States, either by sending students or by employing nuclear security specialists from other States to provide academic and practical education.

4.2 Training and exercises. A well-trained workforce is needed for an organization to meet its nuclear security responsibilities and to contribute to an effective nuclear security regime. Selected members of this workforce may act as subject matter experts in developing more extensive training and educational materials and may serve as resources for building the national capacity for nuclear security.

Training, whether knowledge based or skill based, should be carefully designed to ensure its quality and effectiveness for the personnel being trained. Determining what is to be taught is critical to this process. This is accomplished through a systematic approach to training (SAT), which comprises five basic phases: analysis, design, development, implementation and evaluation. Evaluation occurs at each step of the process and also at the completion of the training cycle.

The evaluation results are then acted upon to ensure continuous improvement of the training activity and, where appropriate, as input to other performance improvements, if such results indicate organizational issues.

Training is generally focused on learning a new skill for a specific job or on improving performance. Fundamentally, an SAT should help to provide all of the training needed to address performance needs within the established competence framework. The first phase of the SAT is to determine the training needs of personnel at all levels and with all types of responsibility for nuclear security.

The use of exercises will enhance organizational readiness and help develop the processes and procedures to evaluate and monitor the effectiveness of detection and response systems. Nuclear security exercises provide a means to assess capacity building needs, build capacity and evaluate the effectiveness of capacity building efforts.

4.3 Awareness rising. Awareness rising differs from education or training in that its objective is limited to making the target audience aware of a particular condition, event or issue rather than providing broad knowledge or skills to accomplish a specific task.

Awareness is achieved when an individual, at whatever level (e.g. with national or organizational responsibilities, or a member of the public) internalizes information regarding nuclear security, threats, nuclear security systems and measures, and organizational roles and responsibilities relevant to his/her own responsibilities, and develops the desired behaviors and beliefs appropriate for his/her situation.

Awareness raising programmes are less formal than education or training in the method of development, delivery or measurement of effectiveness. Awareness programmes need to be implemented carefully in order to take into account the requirements for protection of sensitive information related to nuclear security and the 'need to know' rule, depending on the target audiences.

In order to establish a strategy for developing an awareness programme, goals should be established to focus awareness raising efforts, including the following:

Providing individuals with foundational knowledge and guidance relevant to their roles and responsibilities for nuclear security (e.g. information on nuclear security threats, detection options and operations) for building an effective nuclear security culture. This knowledge can provide a basis for advanced training and a broader understanding of one's responsibilities.

Fostering the development of political will of government entities and organizations to build and sustain nuclear security capabilities and programmes. It is believed that institutionalizing nuclear security within the responsible organization will enhance the effectiveness of national nuclear security capabilities. Promoting a common terminology and basis for raising awareness with the general public and non-governmental organizations.

4.4 Workforce management. The following elements should be incorporated into workforce management strategies: Workforce planning; Career management; Performance management [4].

4.4.1 Workforce planning

Workforce planning involves addressing both short term and long term needs to continuously fulfil nuclear security responsibilities. It involves planning for the whole employment cycle, from recruitment to retirement, including short and long absences, special situations requiring extra resources and succession planning.

A recruiting strategy is needed to attract a high quality workforce to meet current and future staffing needs for nuclear programmes, including regulatory bodies and other competent authorities. Merit based promotion systems may help attract highly motivated candidates to the security field and encourage them to gain competences and achieve a higher performance level.

4.4.2 Career management

Career management includes continuously motivating personnel with nuclear security responsibilities to continuously improve their performance. Providing appropriate remuneration commensurate with an employee's contribution is a good practice. Rewarding individual employees for outstanding performance may also serve to encourage the workforce in general to improve their performance and to contribute to achieving nuclear security objectives.

Another important consideration for career management is the planning of personal career paths. Providing a clear career path towards higher positions helps personnel set their own professional goals, thereby encouraging them to strive for promotion. This starts with assigning personnel to positions that fit their own competences and then allowing them to develop and continuously improve their overall nuclear security performance.

4.4.3 Performance management

Performance management is a key part of workforce management, and includes periodic performance evaluation. In these periodic evaluations, particular emphasis should be placed on identifying possible gaps between expected and actual performance and the reasons for them.

Different skills are involved in fulfilling different nuclear security responsibilities. Some skills can be attained relatively quickly, but others take more time, and different individuals may also attain skills at different rates. Uneven development of individual skills needs to be evaluated from a long term perspective, and periodically reviewed to determine whether the situation is improving within expected timescales.

If weaknesses in performance are found to result from functional deficiencies in the workforce management programme (rather than weaknesses at the individual level), a thorough analysis should be carried out to identify the underlying causes of these deficiencies and correct them. These causes could include misinterpretation of needs, inadequate workforce planning, incomplete or ambiguous procedures, mismatches in personnel assignments, a lack of incentives to encourage better performance, or many others.

4.5 Knowledge management

Nuclear security related knowledge needs to be appropriately managed in order for it to be used to effectively build capacity. The knowledge acquired in operating a nuclear security system should be shared among those with roles and responsibilities relating to the system, to achieve better performance. It should also be preserved in a manner allowing it to be efficiently transferred to individuals assigned such roles and responsibilities in the future. Therefore, knowledge management should be an integral part of capacity building programmes and needs to be aligned with workforce management strategies.

Knowledge management is an integrated, systematic approach to identifying, acquiring, transforming, developing, disseminating, using and preserving knowledge, relevant to achieving specified objectives. States should aim at establishing a knowledge management system and coordinating related activities to build a structure in which to share and effectively transfer the necessary knowledge to support capacity building efforts.

Identifying the knowledge that needs to be managed for capacity building purposes should be the first step in a knowledge management process. The knowledge identified to meet these needs may be explicit, such as technical information on paper or in electronic form, or may be tacit, such as experience based insights and skills in the people implementing nuclear security measures. The identified knowledge, either explicit or tacit, needs to be recorded and stored in an organizational knowledge database.

4.6 Knowledge networks

Knowledge management can be supported through the development and utilization of knowledge networks. Knowledge networks include people with nuclear security knowledge and serve as a platform to enable the analysis and sharing of such knowledge to supplement efforts to build national nuclear security capacity. Knowledge networks can be established at both the national and international levels.

Knowledge networks for nuclear security at the national level could serve as a pool of people considered as human resources to build national nuclear security capacity. For example, the graduates of Master of Science programmes in nuclear security might represent the list of people considered competent to serve as nuclear security officers in competent authorities and other nuclear related organizations. Establishing such a network helps to be equipped with competent human resources to continuously meet national nuclear security requirements. This network could include groups with different specializations, including, for example, analysis of national nuclear security policies, nuclear security risk assessment or design and evaluation of physical protection systems.

Knowledge networks for nuclear security at the national level could also support effective knowledge management. Knowledge networks based on specified types of responsibility in a national nuclear security regime are ideal units for effective knowledge sharing, among people with common roles, on good practices in those roles, thus encouraging continuous improvement of their performance.

5. Interfaces with nuclear safety

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

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

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

A major interface where capacity building may overlap is in emergency management. Safety and security will both be major considerations in addressing nuclear or radiological emergencies arising from nuclear security events. Although preparedness and response for a nuclear security event is different from that for a

nuclear or radiological emergency, the response arrangements need to have the capacity to work together seamlessly for the protection of the public and the environment [5].

The capacity to implement a nuclear security regime rests largely in countries laws and regulations, its organizations and the people in those organizations. Consequently, these also affect, either directly or indirectly, the implementation of safety and material accounting and control, especially at nuclear facilities.

Therefore, the capacity that is developed at the regulatory and facility level should take into consideration how security will be applied and how this interfaces with other programmes such as safety. For example, if there is a single regulatory body for safety and security, then that regulator might share resources for its rulemaking, inspection and enforcement. These resources represent the capacity of the regulator to perform its duties.

As another example [6], a nuclear facility operator needs to implement all requirements for safety, security and nuclear material accounting. Therefore, it is most effective and efficient if the management systems, procedures and personnel at the facility are designed to take maximum advantage of shared facilities, equipment and resources and to work together to achieve their respective goals (to the extent possible, taking into consideration the differences between these areas).

5. Conclusion

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

This approach should be developed as part of a national security policy and implementation strategy. Before initiating the approach, the government should decide which organizations should coordinate the approach at the national level. Furthermore, each organization with responsibilities should assign a unit to perform the necessary work.

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

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

6. Acknowledgement

The issues discussed in this report are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum communication, intelligent security systems and risk management (Quasar) " , which has received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

Bibliography

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

[2]. Panevski V.S., "Possible approach for developing a model of intelligent security system applicable in its design in the quasar center of competence", SECURITY & FUTURE, 4, 2, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2020, ISSN:2535-082X, стр. 47-50.

[3]. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[4]. INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

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

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

Does It Make Any Sense? – Establishing Military Bases Overseas

János Csengeri
National University of Public Service – Budapest, Hungary
E-mail: csengeri.janos@uni-nke.hu

Abstract: *In the paper the author examines the dilemma of establishing military bases abroad in order to wage war, maintain presence or secure the interests of a state. The study concerns the Loss-of-Strength Gradient, advantages and disadvantages of overseas presence of armed forces and the characteristic of an overseas military base.*
KEYWORDS: LOSS-OF-STRENGHT GRADIENT, OVERSEAS BASE, MILITARY BASE, SECURING INTERESTS

1. Introduction

It takes a huge effort. It is really expensive. Stationing our troops outside of our own country at a host base or especially at an overseas base is challenging. Then why would we do that? We have satellites to perform surveillance, aircraft to carry out reconnaissance missions, a wide variety of missiles, rockets and bombs to hit the adversary, cyber tools to gain advantages in this relatively new domain, information operations to influence the fifth domain, the human hearts and minds.

Yet as everything, these high efficient assets have limitations as well. Also overseas bases hold diplomatic relevance, so these facilities are not merely used for waging war, but keeping and ensuring friendships between states and within alliances. The aim of this paper is to outline the importance of overseas bases from two approaches.

2. Loss-of-Strength Gradient

Military operations whether it is waging war, peacekeeping or humanitarian aid are about logistics, which is about distance, transporting and sustaining materiel and human resources. The further we go the more human resources are needed in order to maintain an efficient chain of supply. The longer the distance, the more manpower is "lost" within the supply chain and less remain to carry out the mission itself, so our strength is continuously degrading by the increase of the distance of conflict from our homeland or home base.

This theory is not completely fresh, but it is originated from Kenneth E. Boulding back in 1962. In his book [1] Boulding called this formula as the 'loss-of-strength' gradient. Throughout his book he was studying the nature of conflicts and the relations within it. He says, that the further we go and the longer the chain of supply is, the more strength we lose compared to that strength we could utilize from our home bases during a conflict near us. He is explaining this theory through complex mathematic formulas, as Figure no. 1 shows. The formula and the calculation express how many men we lose in relation of the distance of conflict.

s (miles)	1	2	3	4	5
Primary suppliers	qh	qh	qh	qh	qh
Secondary suppliers	$4q^2h$	$3q^2h$	$2q^2h$	q^2h	
Tertiary suppliers	$6q^3h$	$3q^3h$	q^3h		
Quaternary suppliers	$4q^4h$	q^4h			
Quintary suppliers	q^5h				
Sum	$qh(1+q)^4$	$qh(1+q)^3$	$qh(1+q)^2$	$qh(1+q)$	qh

s	0	1	2	3	4	5	6	7	8	9	10	20
$1+sq$	0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	2.0	3.0
$h_1 = \frac{a}{1+sq}$	1000	909	833	769	714	667	625	588	556	526	500	333
$h_2 = \frac{a}{(1+q)^s}$	1000	909	826	752	685	621	535	488	443	401	365	148

Figure 1.: *Loss-of-Strength Gradient [1]*

The critics (even Boulding in his next book [2]) of this theory say that by the utilization of modern weapon systems like missiles, strategic bombing aircraft and solutions like rapid global airlift eliminate the significance of this idea. However, the former facts exist, these assets cannot be applied in every case. Conflicts of our days proved that centres of gravity are either not easy to be determined or almost impossible. Fighting against a hiding, irregular or harassing adversary necessitate much time on target and constant air (military) presence. In order to realize a constant presence, we need to project our military power, even air power to overseas or forward deployed military bases.

3. Forward Based Military Presence During Conflicts

Forward basing is not merely connected to conflicts, as illustrated by the United States of America's overseas military presence nowadays. [3] However, forward military presence is not confined only to the air force, but the author being an airman is partial to air force related instances. Therefore, even if the model is insular or simplistic, the basic idea is valid. It is further underlined, if one takes a look at the conflicts of the 20th century.

3.1. Vietnam 1965-'73.

Forward military presence is usually dangerous in conflicts, as it was during the Second Indochina War for the American troops in Vietnam. Employing air power from a distance in a conflict is usually a safer way of intervention rather than engaging by land forces, however sometimes it is not possible to stay away from the operational area. In 1968, 2000 tactical planes and 3300 helicopters were stationed in the area of operation in Vietnam, but the large strategic B-52 bombers were based further away in Thailand or on Guam. [4]

3.2. Iraq, 1991.

During the USA-led coalitional forces' campaign against Iraq in 1991, several Middle-Eastern states provided host bases for the aircraft. The risk that the coalitional forces at air bases had to face with was much less than during the instance above. It is because, during this time, the host bases were outside of the operational area. Most of the bases were provided by Saudi Arabia, but there were some other contributors like Qatar, Bahrein, The United Arab Emirates, Turkey, Egypt, Oman, and RAF Akrotiri Air Base was also occupied by American aircraft. On aircraft carriers even more air assets were deployed into the region on the Red Sea and in the Persian Gulf. [5]



Figure 2.: *Host nation providers from neighbouring countries of Iraq during Operation Desert Storm [5]*

As it can be seen on Figure 2. Iraq was surrounded by Coalition air component and therefore aircraft. The conduct of air operations could be realised from many angles which also contributed to the rapid military success achieved.

3.3. Kosovo, 1999.

Against the former Yugoslavia, many surrounding NATO members or partners provided host nation support for the involved forces, mainly air force troops.

Table 1.: *Distribution of air force aircraft during Operation Allied Forces [6]*

Aircraft at different nations' bases	Helicopters (pcs.)	Palnes (pcs.)
Albania	87	-
Bosnia and Herzigovina	117	-
France	-	47
Germany	-	120
Greece	-	10
Hungary	12	46
Iltaly	5	478
Macedonia	34	-
Spain	-	37
Turkey	-	38
United Kingdom	-	88
United States of America	-	6
Aircraft carriers (on 3 pcs.)	36	79

In Table 1. we can see the numbers of aircraft on different air bases, but again it is better to visualize the dislocation on the map. Due to the difficulties of display, air bases in the United States are not presented on Figure 3. but there were 6 pieces of B-2 Spirit subsonic strategic aircraft of which this was their first operational employment.

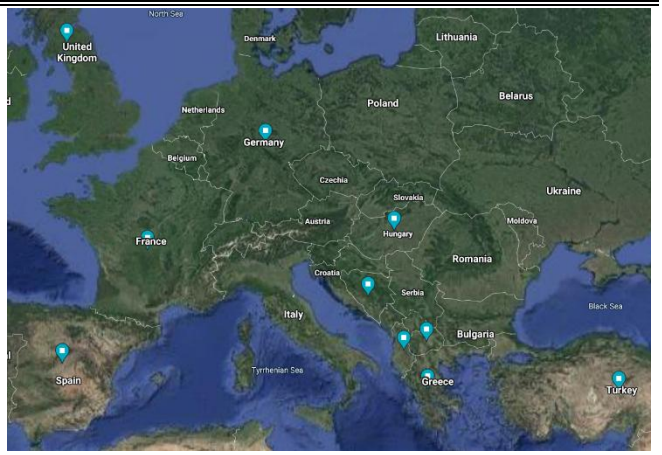


Figure 3.: *Host nation providers from neighbouring countries of Yugoslavia during Operation Allied Forces*

Once again the target was surroundedby tactical aircraft on surrounding air bases, but air assets with greater range like B-52s, B-1s and F-117s were also employed from distant locations in Germany and the United Kingdom.

3.4. Libya, 2011.

In 2011, from 19 March to 31 October, a NATO led operation, the so-called Operation Unified Protector was carried out against Libya to stop the violence against civilians. The intervention focused on air efforts and the warfighters followed the old recipe, however the investing could not be realised as purely as above, but they still utilised many air bases to the North.



Figure 4.: *Host nation provider nations during Operation Unified Protector [7]*

In this conflict, the global precision air-to-surface bombing was practiced from US air bases, from more than 9.000 km distance away by B-2 Spirits and B-1B Lancers. Tactical aircraft were deployed into and operated from European countries as it is shown on Figure 4.

4. Conclusion

Distance is still a vital factor at times of conflict, even during the employment of air forces. Yet time is also at least as important as the distance between our forces and the targets or area of operations.

Distance comes to the front when military presence has to be maintained like a no-fly-zone over a given area. To maximise the time on target of military aircraft, the launching bases should be around the area of operation. These bases can be also inside of the mission area, but this usually is a dangerous situation, however the employment of forces other than air force necessitates this solution.

Time is in the forefront when there is a clear, well defined target and we need to gain effect by hitting or eliminating that given target or set of targets.

Responsiveness, so both time and distance are vital factors when there are time sensitive targets that we need to react to quickly. In this case, close forward bases are required to provide the proper responsiveness and flexibility to the joint commander.

Most of the above mentioned instances prove that even air heavy operations necessitate forward deployed or overseas bases. It could be seen both contra- and pro loss-of-strength gradient advocates are right to a certain degree. Distant bases can be utilised when we have stationary, well defined set of targets, but close bases need to be utilised to react on pop-up, time sensitive targets.

References

[1] K.E. Boulding: Conflict and Defense – A General Theory. Valmy Publishing (2018)

[2] K.E. Boulding: The Meaning of the Twentieth Century: The Great Transition. London, George Allen & Unwin (1964)

[3] United States of America, Department of Defence: Base Structure Report Fiscal Year 2017 Baseline – A Summary of Real Property Inventory. (https://www.acq.osd.mil/eie/Downloads/BSI/Base%20Structure%20Report%20FY17.pdf; downloaded: 2021.04.13.)

[4] D.J. Mrozek: Air Power and the Ground War in Vietnam. Washington D.C., Pergamon-Brassey's, (1989)

[5] J. Corrigan: Desert Storm Air War: The Aerial Campaign against Saddam's Iraq in the 1991 Gulf War. Guilford, Stackpole Books (2017)

[6] I.H. Daalder; M.E. O'HANLON: Winning Ugly – NATO's War to Save Kosovo. Washington D.C., Brookings Inst. Press (2001)

[7] P.K. Mueller (edt.): Precision and Purpose: Airpower in the Libyan Civil War. Santa Monica, RAND (2015)

Warning and reporting of biological incidents during military operations

Dimitar Nedevski, Maria Nenovska

"G. S. Rakovski" National Defence College, Sofia, Bulgaria

d.nedevski@rndc.bg, m.nenovska@rndc.bg

Abstract: *In the past years, NATO member countries have faced the threat of bioterrorism, which requires the development of capabilities to deal with this threat. Timely detection and accurate identification of the type of bioagent used is essential for early warning of threatened military units, as part of the process of prevention and reduction of human casualties, as well as for the spread of the disease. The possible use of biological agents as weapons of mass destruction (WMD) is presented in the report. The military reconnaissance role in the process of investigation of disease outbreak is considered. For the implementation of the process for early warning and alert of biological threat, a scheme of a model of a platform for biological reconnaissance and monitoring is presented. In the model a configuration of hardware and software is used. Due to the increasing risk of use of biological weapons by terrorist organizations, the acquisition and integration of an advanced platform for monitoring and outbreak reconnaissance from the units of the Armed Forces of the Republic of Bulgaria is of key importance.*

Keywords *BIOLOGICAL CONTAMINATION, BIOLOGICAL AGENTS, RECONNAISSANCE, MONITORING, EARLY WARNING, MODEL*

1. Introduction

An analysis of the detectors used by the military units shows that with the available instruments they cannot meet the requirements related to the biological reconnaissance capabilities laid down in the accepted for implementation Allied Tactical Publication *ATP-45(F) Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents* [1]. The reason for this is the fact that the means used for detection, identification and monitoring of biological agents do not meet the modern requirements for detectors for registration of biological contamination. This is also the reason why the Republic of Bulgaria does not ratify the specified document.

2. Essence of the researched problem

In order to achieve interoperability with their allied and coalition partners, the Chemical, Biological, Radiological and Nuclear (CBRN) Defence units of the Bulgarian Armed Forces need to build capabilities for detection, identification and monitoring of biological materials from a safe distance. This can be accomplished through the use of detectors capable of transmitting data in a network environment. Our efforts have focused on the development of a schematic model of a platform for biological reconnaissance and monitoring.

3. Preparation of protection

Preparation for protection in the event of an attack with biological weapons includes a wide variety of activities. They include the following steps: raising awareness of the problem, establishing a preliminary organization for action and providing forces and resources, utilization of procedures for reducing the effect or for protection of biological agents and prevention of diseases from them, upskilling and updating the regulatory documentation. This preparation is specific to each structure and depends on the purpose and the main functions assigned to it. It includes main activities as follows:

1. Collection of up-to-date information on the problem and maintenance of a database on the natural infectious morbidity of the nosological units that appear on the list of biological weapons.

2. Development of plans and programs with detailed measures for maintaining the readiness for protection and increasing security level.

3. Preparation of estimates and provision of the necessary material resources regarding the readiness for work for the liquidation of emerging crisis situations related to the biological agents use.

4. Keeping the resources of warning on standby and availability of individual and collective means of protection.

5. Organization of the interaction and coordination for the work of military and civilian structures.

4. NATO standardization documents

The activities for detection, analysis and prediction of events related to biological hazards for the military units are regulated in two main NATO standardization documents.

The first, *ATP-45 (F) Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents* [1], describes the processes for detecting, warning and reporting biological hazards. ATP-45 is designed to warn military populations of CBRN hazards by providing area warning templates based on CBRN messages.

The second document *(AEP-66 NATO handbook for sampling and identification of biological, chemical and radiological agents (SIBCRA))* [2] regulates the sampling, transport and analysis of samples in such a way to ensure the subsequent legal burden of this process. Sampling is the first step of the process. The next step is the transport of the samples to the laboratories for analysis. The process ends with a sample analysis performed in a certified or accredited laboratory. If one of the steps is not realized, it is impossible to carry out the mission of sampling, transport and analysis of samples contaminated with bioagents. The adenosine triphosphate method of operation of HY-LITE-2 is one of the best ways to detect organic contamination, but this does not mean that the rapid hygiene control system can be classified as a kit for the identification of biological agents [3].

Requirement specified in *AEP-66 NATO handbook for sampling and identification of biological, chemical and radiological agents (SIBCRA))* is that mobile systems (laboratories) for biological detection and identification should be located near the area of use to provide commanders with timely information. With the appropriate equipment and trained staff, they will be able to detect the presence of biological agents on site. Such a preliminary analysis reduces the work in the main laboratories, where it is possible to identify the agents accurately. Mobile systems (laboratories) may be able to perform a qualitative analysis but not be able to perform a quantitative analysis of the sample contaminated with bioagent. Quantitative determination of the biological agent is of paramount importance to assess whether it is an endemic or epidemic case. If the laboratory does not have the possibility for quantitative analysis, it is necessary to send the samples to those who can perform the test.

It is necessary to predict the biological situation in order to provide commanders with the information needed for warning units that may fall into a biologically dangerous area. The application of modern technologies enables efficient monitoring and development of digital maps for risks and hazards, and create informational manageable process chain: "predicting disasters and accidents -

predict the consequences - defining scenarios response" united in a unified state information system. [4]

Biohazard warning and reporting is a process in which reports of the results of the use of bioagents or accidents that have occurred are sent down the chain of command. Thus the military units are warned of the emerging hazards. The purpose of warning and reporting is the timely collection, evaluation and dissemination of data related to attacks with biological agents or suspected hazardous areas.

The process is coordinated by a hierarchical structure made up of centers for collection of information on chemical, biological, radiological and nuclear (CBRN) environment. In the basis of this structure are the CBRN reconnaissance units. The elements of this hierarchical system collect, process and analyze data related to the biological environment. They calculate the zones of contamination and recalculate them when the situation changes. They organize and carry out warnings about the use of bioagents or the occurrence of accidents by assessing their impact on the troops. Also they offer appropriate options for their action in the current situation. The system analyzes the data from the conducted biological reconnaissance and sends information about the actually infected areas of the units that may be affected. In this way the warning process is realized.

Warning and reporting are done according to the Allied Tactical Publication *ATP-45 (F) – Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents*. [1]

Intelligence and biological hazard warning data of endangered units are exchanged through standard forms of communication. They are denoted by the Latin abbreviation – CBRN (Chemical, Biological , Radiological, Nuclear). The messages are numbered from 1 to 6.

CBRN 4 BIO message (see Table 1) is used to transmit the results of the monitoring, sampling of biological agents and monitoring of the created environment. Once the results (from surveillance and reconnaissance) have been collected, they are summarized by the centers for collecting and processing information on the CBRN situation at the tactical and operational level. Endangered units in the area of operations are disclosed through a CBRN 3 message.

All information exchanged using the CBRN 4 BIO message is collected for summarization in the CBRN Collection Centers and CBRN Control Centers (Zone (ZCC) and Area Control Center (ACC). Based on this data, the authorities at all levels of the system map the actual areas of infection and provide them to the relevant headquarters.

Table 1: *CBRN 4 BIO – Example.* [1]

BIO 4			
Common Message Heading followed by the following "M" mandatory and "O" operationally determined sets:			
Set	**Description**	**Cond.**	**Example**
ALFA	Incident Serial Number	O	ALFA/BEL/001/001/B//
INDIA	Release Information on CBRN Incidents	M	INDIA/TS:BAC/NP/OTH/-//
INDIAB	Release and Sampling Information on Biological Incidents	O	
QUEBEC*	Location of Reading, Sample, Detection and Type of Sample/Detection		FS/-/-/-/-/-/-/31UDS8740049600/-10M//
ROMEO*	Level of Contamination, Dose Rate Trend and Decay Rate Trend	O	ROMEO/CON:15PPM/INIT/-/-/-//
SIERRA*	Date time Group of Contamination Measurement	M	SIERRA/031040ZAPR2010//
TANGO*	Terrain/Topography and Vegetation Description	O	TANGO/FLAT/BARE//
WHISKEY*	Sensor information	O	WHISKEY/ABV/MAN/PCD/-/-/-/-//
YANKEE*	Downwind direction and Downwind Speed	O	YANKEE/180DGG/17KPH//
ZULU*	Measured Weather Conditions	O	ZULU/4/20C/0/0/0//
XRAYZ*	Cloud Plot Contour Information	O	XRAYZ/CON:15PPM/MGRS:32VNJ5750020300/MGRS:32VNJ5720021100/MGRS:32VNJ5600021900/MGRS:32VNJ5340021800/MGRS:32VNJ5750020300//
OSCARZ*	Date Time Group for Cloud Plot Contour	O	OSCARZ/030830ZAPR2010/030930ZAPR2010/SRL1/SRL2/SRL3//
GENTEXT	CBRN info	O	GENTEXT/CBRNINFO/HHA HANDHELD ASSEY//

* Sets QUEBEC, ROMEO, SIERRA, TANGO, WHISKEY, YANKEE and ZULU are a Segment. Sets XRAYZ and OSCARZ are a different segment. The report can either contain the QUEBEC segment or the XRAYZ segment but not both. The QUEBEC segment can be repeated, if there is a repetition, the whole segment has to be repeated. Set QUEBEC is not allowed to be repeated before set SIERRA has appeared. Sets/segments are repeatable up to 20 times in order to describe multiple detection, monitoring or survey points.

In the column "Cond." (Input conditions) with M the required groups for each message are indicated. Reports begin with a "title" containing the CBRN report number (1-6) and the event (NUC, BIO, CHEM, ROTA or unknown - UNKNOWN).

The likelihood of a biological situation and its consequences are factors that can affect the course of a particular operation. For this purpose, information must be provided, the analysis of which determines the presence or possibilities for production of biological agents by the opposing party, the probability of its use, the perceptions and the ways of its use. The algorithm for assessing the risk of biological weapon use is shown in Figure 1. [5]

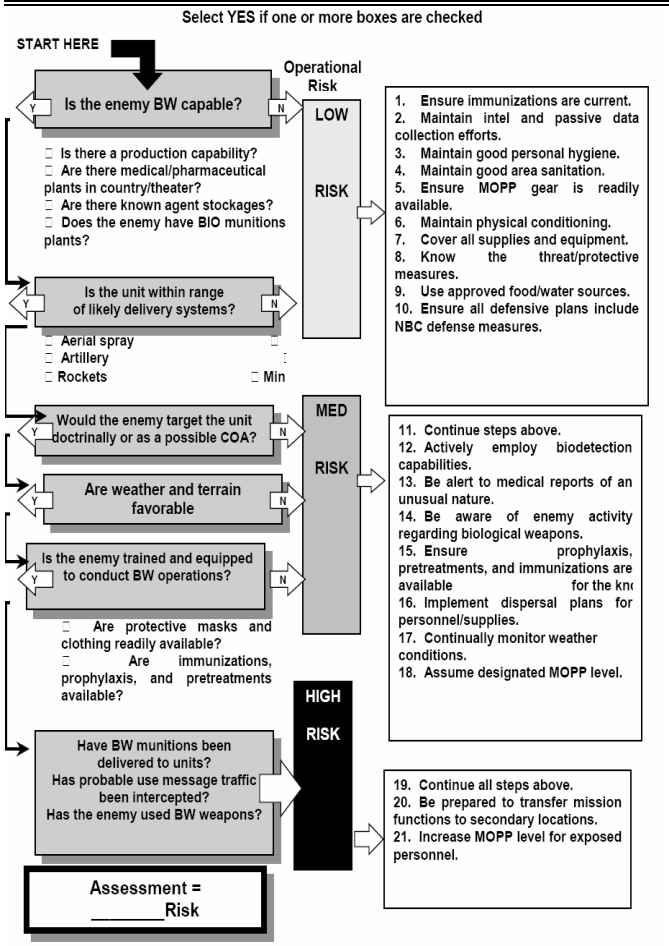


Fig. 1 *Algorithm for assessing the risk of biological weapon use. [5]*

5. Detection of biological agents

Interoperability with allied and coalition partners in terms of CBRN protection from the armed forces goes through the need to build capabilities for remote detection, identification and monitoring of biological materials through the use of detectors that can transmit information in a network environment.

The identification is a fundamentally different process from the detection. While for the detection the main goal is to register the presence or absence of CBRN contamination, the identification aims to qualitatively and quantitatively determine this contamination. The process of identification of CBRN agents aims to determine their characteristics, to confirm their presence, to establish a new level of protection of the units and to determine appropriate countermeasures. In cases of biological detection and identification, it is likely difficult to confirm the existence of an event. Biological agents exist in the nature very often, so the assessment of a particular agent must be compared with the actual biological environment. Only in this way an assessment of the occurrence of a biological accident can be performed.

Implementation of interoperability in the field of biological protection can be accomplished by the acquisition of the following means for the detection of biological agents:

- portable point detectors for biological agents that are capable of detecting the presence of biological agents;
- portable biological point detectors with the ability to transmit data in a network (mounted on machines or separately) and monitor the presence of biological warfare agents, their temporary (conditional) identification and warning of units with minimum false alarms.
-

6. Platform for biological reconnaissance and monitoring

These activities can be realized by building a platform for biological reconnaissance and monitoring. It is a configuration of hardware and software that are the basis for primary sources of information. Depending on the intended use (e.g. stationary monitoring post, air reconnaissance), the platforms can be completed to perform tasks in specific conditions.

The platform is built on a modular principle with a module of sensors and a module for "warning and reporting". It has a set of sensors by which automatically detects and identifies biological substances. There is an option for collecting and storing samples for later laboratory evaluation and warning of endangered objects by preparing and transmitting messages.

Optimally, the task of the system for determining Bio-contamination can be realized through the biological collector of air samples SASS 2000 PLUS [6]. It ensures the collection of pathogens from the air samples taken, and the sample is automatically transferred at certain intervals for analysis in a biological identifier (portable 4-channel fluorometric system for highly sensitive monitoring of biological agents, toxins and chemical contaminants). This is a significant advantage because it ensures the reuse of reagents, which reduces the consumption of expensive immunochemicals. The data from the analyzes with the time of registration are automatically saved for storage in the memory of the device and can be transferred to a personal computer.

The operation of external devices (biological contamination sensor, meteorological data, GPS) is controlled by a network hub consisting of input RS-232 interfaces and an output Ethernet interface for PC connection. The control of the sensors, the graphical visualization of the data for the background map and the visualization of the location are controlled by the software module of the hub. It is based on the SensAware^{TM} software product [7] or the Sensor Connectivity Management Software® (SCIM) [8]. It controls the sensor unit and any error or detection can be recorded. When an infection is detected, the information is automatically, semi-automatically or manually sent as CBRN 1 or CBRN 4 message to the CBRN Analysis program, which clarifies the biological situation and warns the infected objects.

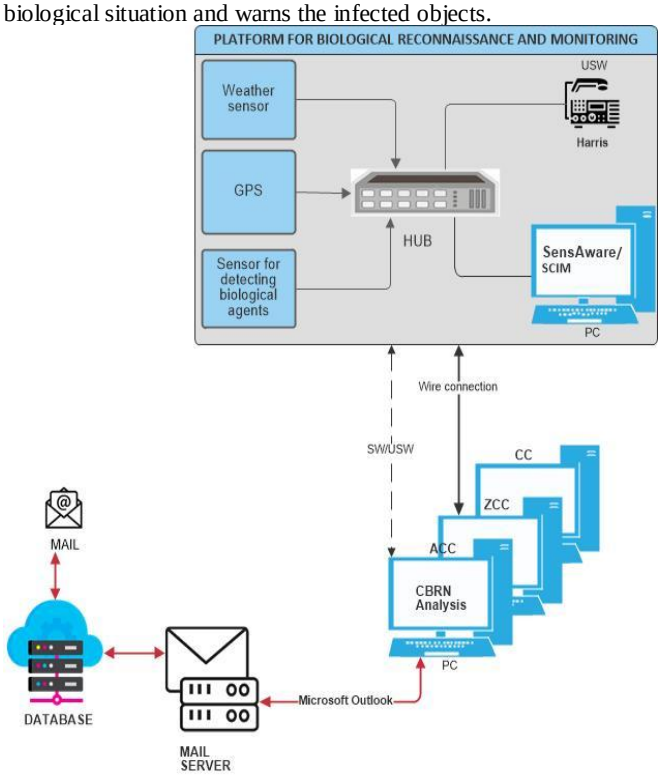


Fig. 2 *Working principle of a platform for biological reconnaissance and monitoring.*

The communication with other units and sites, as well as the transmission of all messages and reports related to the warning about the biological situation, is carried out through a digital ultrasound waves (USW) radio with an integrated message terminal. It provides the possibility of packet switching when transmitting data integrated into the platform via RS-232 interface.

All units have such equipment (including those for BIO reconnaissance), which is a very good basis for building the system, in accordance with the principle of rational transition from the current technical and technological state.

7. Conclusion

Considering the new risks related to the creation of a biological environment and the requirements imposed by the membership of the Republic of Bulgaria in NATO, the construction of a platform for biological reconnaissance and monitoring based on modern software will provide reliable and timely information to the authorities. This allows for accurate decisions about the behavior of the elements controlled by them, providing anticipatory action against the devastating effect of the created biological environment.

8. References

1. ATP-45, *Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (operators manual)*, Ed. F, Ver. 1 (2019)
2. AEP-66, *NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA)*, Ed. 1, Ver. 1, (2015)
3. D. Nedevski. I. Markov. Inteligentnata otbrana i neobhodimite sposobnosti za otkrivane i identificirane na YAHB opasnosti *[Smart Defence and the Necessary Abilities to Detect and Identify CBRN Hazards]*, Yearbook of Rakovski National Defence College, Faculty of Command and Staff, **2** (2013), p. 277-285
4. S. Velev, *Riskat ot bedstvia – razbirane, ocenka i upravlenie [Disaster Risk – Understanding, Assessment and Management]*, Long-term security environment challenges and armed forces capabilities development, Proceeding of the International Scientific Conference, Rakovski National Defence College, Sofia, **2**, (2019), p. 173-179, ISBN978-619-7478-35-8
5. ATP 3.8.1., *CBRN Defence on Operations*, vol.1 (2010)
6. J. Kesavan, K. Aubrey Hottel, D. Shepers, *Characteristics and Sampling Efficiencies of the Smart Air Sampler System (SASS) 2000$^{plus®}$*, (2004), Aberdeen Proving Ground MD 21010-5424
7. http://elta.bg/sigurnost-i-otbrana/produkti-i-sistemi/yadreno-khimichesko-i-biologichno-razuznavane-i-zashchita
8. https://bruhn-newtech.com/cbrn-defence/sensor-connectivity-management-software/#scim

Reducing the potential vulnerability of the society in case of a terrorist attack against critical infrastructure sites and facilities

Dimo Kirilov, Antoaneta Simeonova, Angel Krumov
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 article discusses the issues related to the planning of activities for ensuring the physical security of critical infrastructure sites. The critical infrastructure is considered as an important element of the national security of the country, and the criticality is determined by the interdependence between the individual elements and the dependence of the society on its normal functioning.*

***Keywords**: risk, national security, protection, critical infrastructure, terrorism.*

1. Introduction

The problem of critical infrastructure protection gained great international popularity in 2001 after the September 11 terrorist attacks in the United States. This made almost all countries that are at potential risk of terrorist threats to initiate and implement serious changes in their legislation both in the field of protection of critical infrastructure and in the direction of terrorism. Special programs for the protection of critical infrastructure are being created, which are growing into strategic plans and even national strategies. Special attention is paid to cross-border cooperation in order to reduce the risk of terrorist attacks on critical infrastructure.

The process of critical infrastructure protection is defined by the Bulgarian legislation (Disaster and emergency situations Protection Act), as: "A set of activities aimed at ensuring the normal functioning, continuity and integrity of critical infrastructures in order to prevent, reduce, mitigate or neutralize threats, their risks or vulnerability "[1].

The tasks and responsibilities of the competent institutions for counteracting terrorism and controlling the consequences of terrorist acts derive from the Counter-Terrorism Act, updated in State Newspaper. no. 103 of 27 December 2016, the National Counter-Terrorism Plan, accepted by Decision № 669 of the Council of Ministers of 02.11.2017 and the regulations governing their activities and their interaction with other state and non-state entities [2, 3] .

When it comes to the possible threat of a terrorist act against potentially dangerous critical infrastructure, it must be taken into account that terrorist actions are premeditated and planned in detail and bear the scars of an operation that reflects the specific objectives and motives of the executors and meets their capabilities.

In order to ensure permanent and adequate protection against the terrorist threat, it is necessary to build sustainable communication channels between state institutions, local authorities, non-governmental organizations, religious and ethnic organizations. Ministries, departments and local authorities perform their tasks in accordance with their action plans and the orders and directives of the respective managers.

2. Vulnerability of society in case of a terrorist attack

In today's security environment, the threat of terrorist acts is growing and the lives and health of the personnel living in the infrastructure of a critical site or facility, as well as of all citizens located in conventional civilian sites, are directly endangered.

As each object of the infrastructure performs different tasks and functions, a huge expert resource is needed for the collection and analysis of data on the real technical condition of all objects as a whole. This requires decision-making on a case-by-case basis and prioritization of sites. The next and most important step is to take adequate action to implement physical security measures against terrorism for critical infrastructure sites and facilities.

Analyzes of terrorist attacks in recent years have led to the derivation of some basic scenarios for terrorist activity. Here we will focus on terrorist acts by placing explosives that pose a serious threat and pose a risk to potentially dangerous critical infrastructure facilities, such as hydrotechnical facilities (HTF) and, more specifically, tailings ponds, which we will consider as a "priority object".

3. Analysis of the risk of a terrorist attack against hydrotechnical facilities (tailing ponds)

As we have already noticed, in recent years the protection of critical infrastructure has begun to become part of the national security policy of any modern and rapidly evolving society. At the same time, some accidents and incidents that occur at its sites give the impression that the measures taken to protect it are not effective enough.

The analysis of the risk of a terrorist attack against hydrotechnical facilities (tailings) requires the collection of a complete set of data on the investment project, the functions of the facilities, location, orientation, surrounding areas and areas adjacent to the regulated property.

The information generated as a result of this survey serves the experts and those responsible for the planning and design of such facilities to draw up a general plan of infrastructure and functions, assessment and prioritization of the most valuable assets and vulnerable areas.

Risk analysis is a necessary tool to help determine the level of protection as well as the design of protection measures. As it is practically impossible to design safeguards to achieve zero risk, the concept of "accepted risk" is accepted or more precisely defined and how this risk supports the risk analysis when deciding on the integration of physical security measures against terrorist attack in the facilities and adjacent infrastructure.

The developed methods aim to provide minimum measures for protection of the facilities by:

- increase of safe distances;
- design of constructions so as to avoid the phenomenon of progressive collapse;
- design of non-structural parts to reduce the risk of flying debris in case of an explosion or impact;
- development of computer-simulated incidents to support the security of the facilities;
- continuous video surveillance and notification.

The contribution of the Republic of Bulgaria in this area is expressed through the Order of the Ministry of Regional Development and Public Works № RD-02-20-6 of 19 December 2016 on the technical requirements for physical security of construction, which generally recommends methods of physical security against intrusion, published in State Newspaper, issue 1 of 2017 [4].

4. Ensuring a certain level of protection and reducing the potential vulnerability of society in case of a terrorist attack

In today's security environment, there are asymmetric threats and increased terrorist activity on civilian and critical infrastructure sites outside the conflict areas and often in NATO and European Union member states, which requires a new approach to security management for buildings and facilities.

For this purpose, it is necessary to develop documents and practical methodologies giving guidelines for defining an emergency project situation (specifically for each prioritized site), by predicting scenarios, preventing the causes, limiting the damage and dealing with the consequences of the incident in order to be achieved low levels of risk of loss of assets or human health and life.

The process of critical infrastructure protection consists of the following stages:

- Strategic planning – strategic planning for the protection of critical infrastructure is related to the development and implementation of strategies that reflect the state policy of the country in the study area and contain guidelines for future action. Each strategy, whether in the field of security, an element of which is the critical infrastructure or other problem area, indicates the ways to achieve the set strategic goals. Many of the strategies are implemented in addition to an action plan, which contains a set of key tasks that must be completed in advance by the relevant contractors through the necessary resources;

- Criticality identification – starts with defining a list of critical sectors. The criticality of a sector is determined by its place and importance in the supply chain of vital products and services, and by the potential, adverse, destructive impact that its disruption would have on it. As a general rule, when defining vital sectors in all countries, "the potential loss of human life, the economic, political and social consequences" are taken into account. The process of identifying critical infrastructure is directly linked to vulnerability assessment, interdependence assessment and threat assessment activities [5];

- Threat assessment – from the point of view of their nature, the threats for the objects of the critical infrastructure can be divided into the following main groups: natural disasters – earthquakes, floods, droughts, landslides, strong winds, dust storms, hail, etc .; fires – from intentional and unintentional actions of the human factor; accidents – in sites operating with nuclear, radiation, explosive and flammable materials, industrial toxic substances and toxic gases, and are the result of intentional and unintentional actions by human factors; epidemics and pandemics – by humans, animals and plants; catastrophes – space, aviation, railway, road, with vessels, as a result of intentional and unintentional actions, as well as the result of targeted human actions – terrorism. The detailed analysis of the threats for the objects of the critical infrastructure allows their timely neutralization and increase of the resilience of the system [6];

- Vulnerability assessment – is the degree of susceptibility of an object from the critical infrastructure to certain threats. Indicates a place (object, connection) in the system, which is characterized by a greater degree of susceptibility to the impact of threats. Vulnerability, in itself, does not generate adverse consequences, it is realized only when it is exposed to a threat;

- Assessment of interdependencies – in the context of critical infrastructure protection, interdependence is "a two-way relationship between the elements of critical infrastructure, and the degree of dependence is not necessarily the same in both directions." [7]. "There are four main types of interdependencies: physical, informational, geographical and logical (two infrastructure sites are logically interdependent if the state of one depends on the state of the other through some mechanism that is neither a physical nor an information or geographical connection). Different political, legal or regulatory mechanisms can lead to a logical relationship between the elements of critical infrastructure "[8];

- Risk assessment – the process of analysis and risk assessment is reduced to determining the nature and extent of risk as a function of danger, vulnerability and probability. "The risk of a certain object from the composition of the critical infrastructure is defined as a function of three parameters: threat to the object – it is expressed in its intensity and the probability of disaster, its intensity and nature; consequences – in the site of the direct impact of the disaster (direct losses); loss assessment – as a result of the mutual influence between the objects of the critical infrastructure (indirect losses).

  Direct losses are assessed on the basis of the following negative consequences: human losses – human victims; people with permanent disability; people affected by the disaster; material losses – includes all types of possible material losses, calculated in material terms; environmental consequences – pollution of terrains that require the intervention of specialized teams or hinder the operation of the terrain for a longer period of time. Indirect losses are the result of reduced production and supply of goods and services, due to disruption in the functioning and mutual influence of objects and systems (sectors) that ensure people's daily lives [9];

- Strategic decision-making – strategic decisions set the direction for the future development of critical infrastructure protection, have a lasting impact, require reforms, require rational restructuring, commit significant resources and create competitive advantages. The goals and strategies for protection of the infrastructure affect the advantages and disadvantages, the opportunities and threats, the spheres of action, etc. They are taken in the formation, selection, implementation, control and evaluation of a selected strategy.

5. Conclusion

The modern interpretation of the term "critical infrastructure" defines it as a system of facilities, services, information systems, the shutdown and malfunction or destruction of which would have a serious negative impact on the health and safety of the population, environment, national economy or the effective functioning of the State Management.

Due to previous perceptions of the safety of the operation of buildings and facilities, according to which they need to be protected only from natural forces and human error, there was a lack of legislation concerning safety in case of intentional human-caused accidents. Terrorist activity on the territory of NATO and European Union countries in recent years has sparked a wave of proposals to improve the security environment by improving urban, defense and critical infrastructure.

The analysis of the risk of a potential terrorist attack against hydrotechnical facilities (tailings) and the information generated as a result of collecting a complete set of data on the investment project, the functions of the facilities, location, orientation, surrounding areas and areas adjacent to the regulated property is a necessary tool to help determine the level of protection as well as the design of protection measures.

The results of this report are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence "Quantum communication, intelligent security systems and risk management (Quasar)"", which has received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

Literature:

1. Disaster and emergency situations Protection Act, updated State Newspaper no. 102 of 19 December 2006, as changed State Newspaper no. 41 of 22 May 2007, as changed State Newspaper no. 113 of 28 December 2007, as changed State Newspaper no. 69 of 5 August 2008, as changed State Newspaper no. 102 of 28 November 2008, as changed State Newspaper no. 35 of 12 May 2009, as changed State Newspaper no. 74 of 15 September 2009, as changed State Newspaper no. 93 of 24 November 2009, as changed State Newspaper no. 61 of 6 August 2010, as changed State Newspaper no. 88 of November 9, 2010, as changed State Newspaper no. 98 of 14 December 2010, as changed State Newspaper no. 8 of January 25, 2011, as changed State Newspaper no. 39 of 20 May 2011, as changed State Newspaper no. 80 of 14 October 2011
2. Counter-Terrorism Act, prom. DV. no. 103 of 27 December 2016, available at https://www.strategy.bg/
3. National Counter-Terrorism Plan, accepted by Decision № 669 of the Council of Ministers of 02.11.2017, available at https://www.strategy.bg/
4. Order of the Ministry of Regional Development and Public Works № RD-02-20-6 of 19 December 2016 on the technical requirements for physical security of construction works, published in State Newspaper no. 1 of 2017
5. Drakalieva, P., Ivanov, I., Problem analysis of critical infrastructure, project "Protection of critical infrastructure in the EU and Bulgaria – economic and organizational aspects", Department of National and Regional Security, UNWE, Sofia, 2008, pp. 19-20
6. Methodology for modeling, analysis of critical infrastructure, identification of interdependencies, assessment of vulnerabilities and risk and planning of protection capabilities, Research report, BAS, Sofia, 2005, article
7. Homeland Security – National Infrastructure Protection Plan, USA, p.118
8. Kirov G., Stoyanov V., Simulation approach for analysis and assessment of the interdependencies between the elements of the critical infrastructure, in "Second National Scientific and Practical Conference on Emergency Management and Protection of the Population", BAS, Sofia, 2007, article
9. Hadjitodorov S. and team, Methodology for assessment of critical infrastructure at the municipality level, in the Second National Scientific and Practical Conference on Emergency Management and Protection of the Population, BAS, Sofia, 2007, article

The new old challenges to NATO in the Balkans

Martin Sokolov
Youth Research Centre 'Knowledge and Progress', Sofia, Bulgaria.
martinsokolov@abv.bg

Abstract: *NATO is facing an array of challenges in the Balkans – both 'old' and conventional, and 'new' and asymmetric. This paper seeks to offer an overview and provide an analysis of the risks emanating from Russia's strategic interests in the peninsula and possible complications as an example of 'traditional' threat. Additionally, the author will strive to analyze them in the context of 'modern' security challenges in the region, such as the risks stemming from the migration from the Middle East and North Africa, and the challenges, particularly in the Western Balkans, of radicalization and returning foreign fighters. NATO's role in the region is particularly important as no single country in the region has the capabilities to address such transnational threats and challenges unilaterally. The hypothesis is that the Alliance needs to significantly enhance its soft power capabilities, intensify cooperation between stakeholders in the region, and adapt to more contemporary and asymmetric threats.*
Keywords*: NATO, RUSSIA, BALKANS, HYBRID, THREATS, RADICALIZATION, TERRORISM*

1. Introduction

The Balkans are one of the most heterogenic regions in the world and also of significant strategic importance for the different stakeholders. Following the collapse of the Soviet Union the countries in the region have gradually aligned and integrated themselves within the structures of the European Union (EU) and the North Atlantic Treaty Association (NATO) with the aim of improving national and regional security, and insuring economic growth.

While several countries have achieved their objective of joining both organizations, the Western Balkans are yet to successfully join the EU. This has created a certain 'vacuum' which has accommodated the growth of threats and created opportunities for influence by third parties that are in contrast with the stated objectives by the governments in the region [6]. First, currently, as in the EU and most of the world, one of the most pressing threats is that of radicalization and the additional challenges emanating from it: terrorism and returning foreign fighters. According to data the Balkans have the highest number *per capita* of individuals that traveled to the Middle East to join the terrorist organization ISIS [1, 3, 8]. This necessitates the study of the underlying causes for this trend and also the adoption and implementation of specific approaches to deradicalization, as there will certainly be return of foreign fighters in the region.

The second challenge that needs to be taken into consideration is the clashing interests in the region between the West and Russia. As stated, all the countries in the region are striving to become EU and/or NATO members, while Moscow regards the enlargements of these organizations as a threat to its national security. This has resulted in the Kremlin undertaking actions to both potentially postpone or dissuade states to join particularly NATO, and to also challenge the Alliance's unity itself via actions in current members [6, 7]. This has resulted in the fact that NATO has had to enhance its existing capabilities for conventional deterrence against an 'old' threat and to adapt to the 'new' one of radicalization and terrorism. However, because of factors such as globalization and interconnection it is evident that certain complexities have emerged that require the Alliance to both adapt, as well as increase cooperation with the EU in order to successfully tackles such issues.

2. Russian interests in the Balkans

Following the dissolution of the Soviet Union Moscow's influence and interests objectively diminished in the Balkans; however, there has been a clear resurgence since the beginning of the new energy. This should be understood through the prism that the Kremlin: one, wants to reestablish its role as a regional and global power, as illustrated in its approaches to the Middle East and the wider Black Sea region; and, two, its view of NATO enlargement as a clear threat to its national security. Therefore, as all countries from the Balkans are either current or aspiring members of the EU and/or NATO, Russia's approach should be considered as damaging [6].

Moscow predominantly exercises its influence through hybrid means, strategic communications, investments in media outlets, utilizing its dominant role in the energy market, support for individuals and groups characterized by corruption, and subversive actions [7, 9]. In non-member states the Kremlin can directly challenge EU and NATO influence, while in member states it is applying the same means to challenge the unity of these organizations [7]. Furthermore, a worrying trend in the last decade is the formation of pro-Russian paramilitary organizations in the region. While such groups are not necessarily directly organized or supported by the Kremlin, they are at the very least influenced by anti-Western and pro-Russian propaganda, promoted by pro-Russian media outlets. Such supposedly self-organized paramilitary organizations have acquired firepower and gained prominence in 2015/16 at the peak of the migration wave for the Middle East and North Africa, claiming to seek to protect people, religion in traditions from both migrants and Western influence. Such organizations have formed and are active in Serbia, Bulgaria, and Montenegro [6].

Table 1: *Russia's view of contemporary warfare.*

Russia's approach to warfare [4]	
Direct destruction	Direct influence
Direct annihilation	Opponent's inner decay
War with weapons and technology	Culture war
War with conventional forces	War with specially prepared forces and commercial irregular groups
Traditional battleground	Information/psychological warfare and war of perceptions
Direct contact	Contactless warfare
Clashes in the physical environment	War in human consciousness and cyberspace
Symmetric warfare	Asymmetric warfare of political, economic, information, technological, and ecological campaigns
War in a defined period of time	State if permanent engagement as the natural condition of life

Russia evidently understands the primary battlespace of the 21st century, which elaborates why it place significant importance on information and psychological warfare, with the idea to gain advantage prior to any direct contact, or if possible, avoid any contact [4]. Furthermore, this is not limited to enemy troops but to an adversary's entire population. Ideally this not only reduces the need to deploy hard military power but would also manifest itself in the support of local population for the aggressor. Additionally, this allows such operations to be both simultaneously evident and hidden; by blurring lines between state relations and subversion,

falsehood and reality, and war and peace itself, military campaigns can be conducted over extended periods of time at a relatively inexpensive cost [7].

Nevertheless, it must be emphasized that the Russian Federation is neither the 'creator' of hybrid warfare, nor the only country employing it. Prior to the illegal annexation of Crimea in 2014, the most cited example of hybrid warfare was the Israel – Hezbollah in 2006. Additionally, China has its own concept of 'unrestricted warfare', according to which as a result of globalization, the nature of war itself has changed, moving beyond the military realm. [5] Regardless of the name such concepts stem from the same practical necessity, i.e., to challenge the West economic and technological superiority via asymmetrical measures.

3. Radicalization and early signs

The conflict in Syria and the rise of ISIS was characterized by an unprecedented outflow of foreign fighters from the Western Balkans, particularly Kosovo and Bosnia and Herzegovina, who provide approximately 1/3 of the fighters [1]. What is more, while there are various reasons why these individuals decided to travel to Syria and Iraq, the majority of them did join terrorist organizations such as ISIS or Jabhat al-Nusra.

Table 2: *Number of foreign terrorist fighters from the Balkans 2014-2015* [10].

Country	Number of Foreign Fighters	Per capita basis/per million people
Kosovo	316	172
Bosnia and Herzegovina	330	85
Albania	90	30
Serbia	70	10
N. Macedonia	12	6

One of the key driving factors for the process of radicalization is the feeling of vulnerability or even marginalization by the state: feeling that their respective governments either do not have the capacity or will to protect and ensure their civil rights and legitimate interests. Nevertheless, radicalization is a complex process based on complex factors, that takes time. They can be divided into macro-, micro-, and the individual-personal-level [2].

Table 3: *Radicalization factor levels.*

Radicalization factors	
Macro-social	*Globalization, flow of goods and services, connectivity.*
Micro-social	*Social identification, collective emotions, group-group interactions, group- state interactions*
Individual-personal	*Emotions, experience, gender, age, etc.*

The **macro-social level** referrers particularly to globalization, which allows the unimpeded spread of ideologies, and both the horizontal and vertical movement of people and resources. Of this order are the problems with the integration of minority groups, poverty and social bleakness. The **micro-social level**, incorporates categories such as social identification, collective emotions, interaction between groups, alienation from the state and society. At the **individual level** are factors such as personal characteristics, personal experience, emotions, gender, age, etc. The role of the Internet as an important factor through which radical ideas and currents are easily spread and followers should also not be overlooked. For example, 90% of French citizens who joined and likely fought for ISIS were recruited online [2, 6]. The complex combination of many of these factors leads to radicalization and terrorism, but the processes themselves have not yet been sufficiently analyzed.

Nevertheless, it is certain that education and upbringing are particularly important in the fight against radicalism and terrorism, and also identifying their early signs. The psychological processes behind radicalization are often associated with external manifestations. In many cases, this is the change of names or the adoption of pseudonyms taken from religious texts, thus aiming to demonstrate empathy. A change is made in the appearance - change of clothing and shaving - hair and/or beard [8].

Behavioral changes often begin with the desire for regular contact with leaders of radical religious groups, accepted as undisputed authorities, whose opinions are accepted with no question. Suspiciously large amounts of propaganda material can be found in the homes of radicalized individuals. This process is often accompanied by a change in religious practices themselves. The individual becomes significantly stricter in the observance of religious practices, which are performed in full accordance with the canon, and also as often as possible. In order to strictly observe these rituals, the individual often begins to neglect daily activities, such as going to school or work. Another typical sign is visiting websites and forums with radical content. In this space, the individual satisfies his need to share his more extreme ideas. In these circles, he finds like-minded people and other people he could potentially radicalize. In the process of radicalization, there is a change in the pattern of travel and stay in specific places where residents share the ultimate views. In most cases, these are countries, regions of the country or neighborhoods in which a given ideology is widely accepted and practiced freely. In this way, the person can without hesitation demonstrate their empathy for the community or group [2].

The glorification of martyrdom is also a sign of radicalization [3]. The individual no longer seeks only an excuse for his possible actions, but also perceives the processes as a personal path and vocation. Socially, there is isolation, such as avoiding work, school, concerts and other events where many people gather. There is a change in the attitude, as well as in the interaction with others, the use of radical or specific terminology, which is not generally available and cannot be perceived as a random means of expression. The bearers of Islamist radicalism skillfully blame ordinary Muslims for not being good enough Muslims and succumbing to the new age. Breaking their ties with Islamic traditions and in an environment of informal segregation, some Muslims in European countries are seeking a new identity in jihad. The individual begins to feel strong when he identifies with the ideal religious community as the antithesis of the modern secular state. Sometimes the process of radicalization is characterized by the commission of minor crimes. They are not for material gain, but to demonstrate disrespect for established rules in societies. This often grows into disrespect for secular power and the norms of regulating public relations through demonstrative disrespect for it [2].

If the processes of radicalization continue unchecked it is also possible to manifest into acts of terrorism either on home soil or in other parts of Europe because of the relatively easy movement of people even for European countries outside the EU. This risk is further exacerbated by the return of foreign fighters. Some of them will likely be traumatized and perhaps sincerely disheartened by what they witnessed in ISIS [2, 6]. Nevertheless, it is also possible that some will also return with the idea to continue ISIS' war on European soil, seeking to either carry out acts of terrorism, radicalize other individuals, and/or create terrorist networks and cells. This necessitates the establishment of platforms and mechanisms not only for preventing radicalization but deradicalizations as well. This in itself requires both regional and multinational cooperation and support from the EU and NATO.

4. Adapting NATO to the new challenges

Despite these challenges and the continuing need for improvement and adaptation, NATO has an indispensable contribution to security in Europe and an indisputable deterrent to potential aggressors. Additionally, it should be emphasized that the Alliance and the EU have 21 common member states, which largely have a shared vision and a synchronized assessment of the risks facing Europe. The Lisbon Summit in 2010 emphasized the need to improve the NATO-EU strategic partnership. The 2010 Strategic Concept commits the Alliance to work more closely with other international organizations to prevent crises, manage conflicts and stabilize post-conflict situations. Subsequently, in Warsaw in July 2016, the two organizations outlined areas for enhanced cooperation on common East and South challenges, including countering hybrid threats, increasing resilience, defense capacity building, cyber defense, maritime security and exercises. In December of that year, NATO foreign ministers approved a statement to which 42 common measures to advance NATO-EU co-operation were attached. In December 2017, another 32 measures were agreed. On 10 July 2018, in a joint declaration, the two organizations agreed to focus on military mobility, the fight against terrorism and strengthening the resilience of chemical, biological, radiological and nuclear risks. This joint declaration was welcomed at the Brussels summit in July 2018 and noted that the development of European defense capabilities, which will also contribute to the security of the Alliance [6, 7]. Close cooperation between NATO and the EU is undoubtedly an important element in developing an international "comprehensive approach" to crisis management and operations that requires the effective deployment of both military and civilian assets.

In the Balkans specifically NATO continues to provide stability based on membership or partnership. At the same time, it has been demonstrated that the two organizations can support each other with ever-increasing levels of cooperation, as evidenced by the provided support to the EU's operation Sophia in 2016 to secure European borders [6]. Furthermore, NATO has the capacity to intensify the exchange of good practices in the region and promote expertise. To counter specifically the process of radicalization, the establishment of a shared database between the EU and the alliance would significantly ease the flow of important information. Additionally, while EU enlargement has stalled, Brussels can still intensify efforts for adequate reforms in non-member states that a striving for accession. The focus of EU-led social reforms can play a significant contributory role to NATO's security, by decreasing internal tensions in countries, where they are rooted in the lack of rule of law, high levels of corruption, slow economic growth, and threats of radicalization stemming from general social and economic factors.

5. Conclusion

NATO faces increasing and overarching challenges, both external and internal, that require innovation and adaptability. Addressing and overcoming them requires optimal levels of cooperation, both within the Union and with the EU. This report presents and analyzes only them of these threats. For a more in-depth study of the topic, it will be appropriate to take into account: Russia's subversive activities in Europe through energy projects; the activities of Russian private military companies such as Wagner in the Middle East and Africa; the country's policies and actions in countries such as Syria and Libya; bilateral relations between Moscow and Beijing; China's investments in NATO and EU member states; Chinese state-owned companies that use Western funds to finance military technology; return of foreign terrorist fighters to Europe; radicalization; and terrorism.

A significant part of these proposed topics' themes and challenges does not *prima vista* necessitate the competence and expertise of NATO. However, each of them has the potential, indirectly or directly, to become a destabilizing factor for NATO, particularly in the Balkans. This, in turn, requires an increase in the Alliance's expertise, but also the need for coordination, cooperation and even possible harmonization on a number of policies with the EU. But only by continuing to maintain its deterrence capacity, technological superiority, innovative approach, levels of cooperation and exchange of good practices and experience, timely and coherent action and operations, and to remain an attraction for democracies around the world, will NATO succeed to legitimize not only its power but also its very existence.

6. References

1. A. Shtuni, *Returning Western Balkans Foreign Fighters: A Long-Term Challenge* (ISPII, 2020) https://www.ispionline.it/en/pubblicazione/returning-western-balkans-foreign-fighters-long-term-challenge-24762#N1

2. St. Hadjitodorov, M. Sokolov, *The threat of radicalization: early signs and prevention* (Debati.bg, 2017) https://debati.bg/opasnostta-ot-radikalizatsia-razpoznavane-i-preventsia-2/

3. T. Tsvetkov, *Religious radicalization – reasons, motivations, confessions, prevention* (SSF, 2016) (2016), http://www.sofiaforum.bg/imgpool/file1465240594.pdf

4. J. Bērziņš, *A New Generation of Warfare* (Per Concordiam, 2015) http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V6N3_en.pdf

5. Q. Liang, W. Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999) https://www.oodaloop.com/documents/unrestricted.pdf

6. M. Sokolov, M. *The role of international actors in the Balkans*, (Diplomacy Journal, 18 (4), 2016)

7. S. Hadjitodorov, M. Sokolov, M. *Blending new-generation warfare and soft power: hybrid dimensions of Russia-Bulgaria relations* (Connections, 17: 1, 2018)

8. M. Sokolov, (2019) *Black Swan Scenario on Counter-Terrorism in Bulgaria*. (NATO Science for Peace and Security Series - E: Human and Societal Dynamics, 143:1, 2019)

9. T. Tagarev, *Lessons from the Procedure of Acquiring a New Type of Combat Aircraft, 1999-2017* (Sofia: Institute of ICT, May 2018)

10. A. Speckhard. *The Roles of Women in Supporting, Joining, Intervening in and Preventing Violent Extremism in Sandjak* (ICSVE, 2016) https://www.icsve.org/the-roles-of-women-in-supporting-joining-intervening-in-and-preventing-violent-extremism-in-sandjak/

Analysis of changes in the probability of an incident with information security

Petko Genchev
Computer Science and Engineering Department, Technical University of Varna
Varna, Bulgaria
P.Genchev@tu-varna.bg

Abstract: *Risk assessments are not a one-off action, but there are no formal guidelines on when and how often a risk assessment should be performed. Changing factors affect the risk assessment parameters. The strongest influence of these changes is the probability of an accident. Examining changes in the likelihood of an accident will allow for more accurate planning of periods for checking risk factors and assessing risk. In this way, the assessed risk will reflect the changes that have taken place and will lead to more adequate risk management. The analysis of the influence of the changing risk factors is made with the help of a model, which is built on the basis of one asset and the accident scenarios determined for it. The model examines the characteristics of changes in the risk factors for the asset. The probability distribution for the random number of changes is determined. The results of the amended conditions are also random. They are expressed in a change in the level of probability of an accident. For these random variables, the main probabilistic characteristics are determined and dependencies are derived that can be used for analysis.*
Keywords*: INFORMATION SECURITY, RISK ASSESSMENT, DYNAMIC SYSTEMS AND CONTROL*

1. Introduction

According to ISO/IEC 27005 standart[1], in the process of information security risk assessment for each asset, all threats and vulnerabilities to the asset are identified. Vulnerability is mapped to each threat and thus incident scenarios are identified. In this sense, an incident means a threat that has attacked a vulnerability and led to a negative impact on the asset. After determining the incident scenarios, using qualitative and quantitative methods, the levels of probability of realization of the identified scenarios are determined, as well as the levels of impact that each incident may have on the asset. The level of risk is determined by the probability of each scenario and the impact of the incidents. It is a snapshot of the risk to the asset because the assessment was made under certain conditions for the asset. Over time, the conditions for the asset change and it is therefore possible that the probability of an accident and the impact of the incident may also change. Changes in conditions affecting the level of impact are largely deterministic and can be reflected in the level of risk. But the change in the conditions for the realization of accident scenarios is a random variable. This should lead to a change in the level of risk. Of course, in the event of a change in the impact, there are accidental impacts, but the process of change is slower and more determined than that of changing the conditions for an accident.

It is therefore very important to periodically check the risk factors and, if necessary, to re-determine the level of risk. There are no officially defined guidelines on when and how often a risk assessment should be performed. There are recommendations for more frequent reviews of the level of risk in case of significant changes in the subject of activity of the organization, improvements that have been made in the organization, problems arising from the task, incidents or omissions. It can be summarized that the security risk assessment should be a continuous activity. For critical information systems, it is highly recommended that a more frequent security risk assessment be performed.

The ISO/IEC 27004 standard [2] provides recommendations for periods of verification of the effectiveness of applied controls. This can serve as a basis for determining the periods for checking the risk factors for a group of assets. In most cases, verification periods are recommended by experts based on statistics from insurance companies and government statistical organizations.

The frequency of inspections depends on the type of asset and other factors and a simplified approach is needed to easily determine the frequency of inspections.

The purpose of the material is to make an analytical model of the process of changing risk factors to determine their influence on the value of the probability of an accident.

The article is structured in 4 parts: introduction, analysis of the influences of the changed risk factors on the probability of realization of an incident, the analysis of the changes of the probability of an incident and conclusion.

2. Analysis of the influences of the changed risk factors on the probability of an accident

2.1 What are the risk factors?

The ISO / IEC 27005 standard [1] defines some of the risk factors such as asset value, impacts, threats, vulnerabilities, probability of occurrence. It is determined that they should be monitored and reviewed in order to identify any changes in the context of the organization at an early stage and to have an up-to-date view of the overall risk picture.

It is necessary to monitor the new assets included in the scope of risk management, the necessary modifications of asset values, the emergence of new threats inside and outside the organization, the emergence of new or increased vulnerabilities, the emergence of new opportunities to exploit vulnerabilities, increased impact, as well as information security incidents.

2.2 Objectives and statement of the task

In the process of changing the level of risk, the greatest influence is exerted by the probability of an accident. In addition, this element of the level of risk changes most dynamically. From this point of view, it is important to study the rate of change and the levels of change in the level of probability of an accident.

The possibility of realizing accident scenarios represents probability I0 at a certain moment and the change of conditions over time. It is important to determine the period for checking the conditions. Changing conditions will lead to a change in the probability of an accident at the end of the period. An acceptable level of probability level is defined in the risk assessment methodology approved by the

organization. This value can be used for a limit value Ilimit, up to which the level of probability may increase with changes in conditions. The difference Ilimit - I0 will determine the amount of allowable change in the probability depending on the changes in conditions during the time between two inspections.

It is important to determine the parameters influencing the determination of the period for inspections of risk factors. The size of the period must ensure that the probability of an accident changes within the allowable probability value.

We will consider the following statement. For a period of approximately one year, it is assumed that there are n incident scenarios defined for an asset. It is also assumed that the dynamics of the emergence of new scenarios is less than the dynamics of changes in the described scenarios and will not affect the objectives of the analysis.

2.3 Mathematical model

Within one year, changes in probability characteristics may occur in none, one or more of the scenarios. Depending on the case, this number may be different and should therefore be considered as a random variable K with some probability distribution:

(1) $P_k = P\{K = k\}$, за к=0, 1, 2, ...n

There are various hypotheses about the probability distribution of such a random variable. One of them can be synthesized as follows. Let q denote the probability of a change in the conditions for the individual scenarios and assume that it is the same for all scenarios. Independence of changes in the conditions for all scenarios is assumed. In this situation, the number K of changes during the year represents a random variable with binomial distribution:

(2) $P\{K = k\} = \binom{n}{k} q^k (1-q)^{n-k}$

With such a distribution, the average number of changes in conditions per year will be equal to nq, with a variance of nq (1-q) [3].

It is known that the binomial distribution with a small probability q is quite close to the Poisson distribution with parameter $\lambda = nq$ [3]. So another possibility for the distribution of the number K of changes during the year is that of Poisson:

(3) $P\{K = k\} = \frac{\lambda^k}{k!} e^{-\lambda}$, за к = 0,1,2, ... ,

with mathematical expectation λ and variance also λ [3].

The use of the Poisson distribution allows overcoming some technical difficulties and therefore in further consideration we will use it as an example for the distribution of the random variable K.

As a result of the changes in the conditions for realization of the scenarios, an addition to the probability of an accident in a given scenario is formed. The size of the additive, and hence the risk to the asset, varies from case to case and it is logical to consider it as a continuous random variable X. It is often hypothesized that this random variable has an exponential distribution with intensity ξ [4].

(4) $P\{X \geq x\} = e^{-\xi x}$

In this situation, the average size of the additions to the probability of an accident in the individual scenarios is 1/ξ , and the variance is 1/ξ^2 .

An important hypothesis for the further construction is that for the different incident scenarios the changes are independent random variables and do not depend on which other scenarios an additive has occurred, nor on the number of scenarios.

The sum of the additives during the year is random variable and the asset may be at risk if these values exceed a certain critical level.

Therefore, studying the distribution of the annual additives to the probability of an accident could contribute to clarifying the risk management policy for the asset.

What is special about considering the annual amount of additives is not only that additives are random, but also that their number is also random:

(5) $Z = X_1 + X_2 + \cdots + X_k$, for K>0 and $Z = 0$, for K=0

The mathematical expectation of the sum is relatively easy to find. The notional average value, provided that K has a certain value, is the sum of the average values of the individual collectibles:

(6) $E(Z) = \frac{E(K)}{\xi} = \frac{\lambda}{\xi}$

The variance is obtained analogously as a sum of independent random variables .:

(7) $D(Z) = \frac{D(K)}{\xi^2} = \frac{\lambda}{\xi^2}$

3. Analysis of changes in the probability of an accident

The development of the probability of an accident for an asset is determined directly by two factors. First, from the initial level of probability, the size of which determines one or another starting position of the risk for the asset. And second, from accidental additions to the probability of an accident over a period of time.

The initial level of probability of accidents is defined in the risk assessment of the asset and represents the initial value of the probability, which can be changed until the next check. The change in the probability of an accident until the next inspection is due to accidental changes in the risk factors for this asset in the period between inspections. This element of the total probability of an accident has the possibility to add or subtract from the value of the probability of an accident. We will be interested only in the added value, because only it leads to an increase in the risk for the asset.

Let us consider a situation in which checks of risk factors are made during period ***t***. If there are no changes in the risk factors for the asset, there will be no formed addition to the probability of incidents with the asset. Then at the end of the period between inspections we will have a probability I_t with the same value as at the beginning of the period I_0 .

The appearance of changes in risk factors will lead to the formation of an addition to the probability of an accident at the end of the period. As it has already become clear, this quantity is the sum of a random number ***K(t)*** of random variables $X_1, X_2, \ldots X_{K(t)}$:

Then, at the end of the period between inspections, we will have the possibility of an accident

$$(8)\quad I_t = I_0 + \sum_k^{K(t)} X_k$$

The random variables $X_1, X_2, \ldots X_{K(t)}$ are assumed to be independent and with the same distribution with mathematical expectation μ and variance σ^2.

Suppose that the number of additives for a period from ***0*** to ***t*** as an average value accumulates at a constant rate $E(K(t)) = \lambda t$. . In this case, the mathematical expectation of the annual size of the additions to the probability of an accident would be $\lambda\mu$,, and for the total value of the probability of an accident as a mathematical expectation will apply:

$$(9)\quad E(I_t) = I_0 + \lambda\mu t$$

Where: $E(I_t)$ is the total level of probability of an incident with the asset, which is accumulated for time ***t;*** I_0 is the initial level of probability of an asset incident; λt is the number of changes for time ***t*** , which represents average rate of accumulation; μ is a mathematical expectation of the size of the additions to the probability of an accident. This shows how much the probability of an accident changes on average

Then the average increase of the additives to the probability of an accident for time ***t*** is $\lambda\mu t$. If the value of $\lambda\mu$ is positive, the value of the additive will increase, albeit only as an average value, as a general trend, where fluctuations up and down are possible. Otherwise, if $\lambda\mu$ is negative - the addition to the probability of an accident will decrease, although again only as a trend in the average value.

At $\lambda\mu t. < 0$ we have a situation in which over time the probability of an incident with a scenario decreases. This is a positive trend to reduce the risk to the asset. This trend should have little impact on the risk monitoring process, as it does not reduce the inspection period. However, reducing the likelihood of risk should not automatically lead to an increase in the time between inspections. It is necessary to conduct an expert analysis of the causes of this phenomenon and to take steps to increase the time between inspections only after establishing a lasting trend to reduce the likelihood of an accident. The value of the variable $\lambda\mu t$ is a function of the changes in the conditions of several events that have different trends and they must be tracked. Even if an event reaches probability ***0***, the threats and vulnerabilities that determine it must be monitored for new trends to emerge. In addition, the current analysis of the required verification period is made on the assumption that the dynamics of new scenarios is low, but this does not exclude the possibility of new events (threat-vulnerability). Therefore, the decision to extend the period for checking the risk factors for the asset in question must also take these factors into account.

If $\lambda\mu t. > 0$ we have a case of increasing probability of accidents. This is the situation that should have a major impact in determining the inspection period. The following cases need to be considered:

• For $I_0 \geq I_{limit}$ we have a calculated probability of an accident that is equal to or greater than the acceptable level of probability for this asset. This assumption is unlikely because in such a situation risk mitigation measures are taken to reduce the risk below the acceptable level. It is possible to reach this situation at a very high cost of reducing the level of risk and deciding to accept the high level of risk. In this case, the periods for checking the risk factors should be determined by the management of the organization with the assistance of risk management experts.

• When $(I_0 + \lambda\mu t) \geq I_{limit}$ there is a very high rate of increase in the probability of an accident, which for time ***t*** leads to an increase in the probability of an accident above the specified acceptable value of the probability level. In this case, the period for checking the risk factors must be reduced to values where the acceptable level of probability is not reached. Simultaneously with the reduction of the inspection period, it is necessary to conduct an analysis to take measures to reduce the rate of increase in the probability of an accident. In Fig. 1 this situation is illustrated with values above the ***Ilimit*** value.

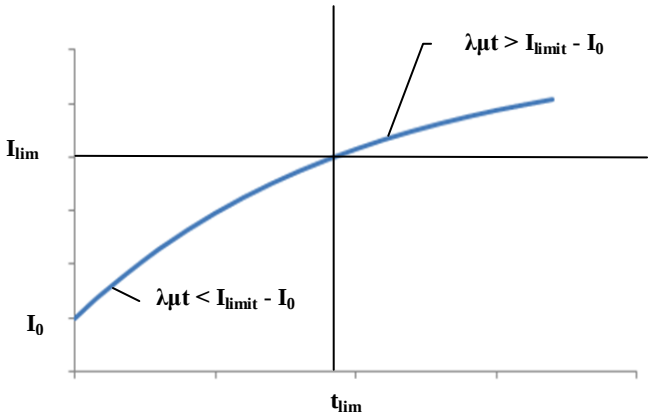


Fig. 1 *Change in the probability of an accident*

• At $(I_0 + \lambda\mu t) < I_{limit}$ we have a situation of a normal rate of increase in the level of probability of an accident due to changes in risk factors. In this case, it can be assumed that an acceptable period of inspections has been set. . В илюстрацията на фиг.1, това е периода в границите от ***0*** до t_{limit}.

In the defined period, the risk factors are checked and the level of risk is determined. The performed inspection serves as a starting point for determining a new period for performing the next examination of the risk factors.

4. Conclusion

The material is a model of the influences and dynamics of changes in risk factors in determining the risk to information security of an asset. The probabilistic characteristics of the changes are determined and the main dependences that can be used for analysis are derived. Based on the identified dependencies, the change in the probability of an accident is modeled and analyzed. Conclusions are made about the relations between the probabilistic quantities and the intensity of the changes.

The analysis used the statement and characteristics of the risk assessment process for information security, but the conclusions can be used for the needs of risk assessment in other risk management systems.

The models made and the derived dependencies can be used to analyze and define an approach for determination of the periods for checking the risk factors.

5. References

[1] INTERNATIONAL STANDARD ISO/IEC 27005:2018, “Information Technology-Security Techniques-Information Security Risk management”, Reference number ISO/IEC 27005:2018(E).

[2] INTERNATIONAL STANDARD ISO/IEC 27004:2016, „Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation”, Reference number ISO/IEC 27004:2016..

[3] Людмил Цанков, “Вероятности и физическа статистика - записки на лекции”, “Probabilities and physical statistics - lecture notes”, Sofia, 2011г., look at http://ntne.phys.uni-sofia.bg/BG/Manuals/PS.pdf

[4] “Събития, инциденти, случайности, опасност и риск”, "Events, incidents, accidents, hazards and risks", look at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj81vTSk5TuAhUHfMAKHVJmB7E4ChAWMAN6BAgEEAI&url=http%3A%2F%2Fspaska.lirex.net%2Fins-educ%2Fbook-1%2F04.pdf&usg=AOvVaw2_uboSA0ac8YsvR7RYdABh

Masking bottom mines by generatingimitative impulse interference

Nikolay Litchkov, Alexandar. Kolarov
[1] Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences,
67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria
e -mails: niki0611@abv.bg, aleksandar_kolarov@abv.bg

Abstract: *Dethedetection of hulls requires the implementation of a built-in or autonomous provides a full range of functionalities for the detection and classification of transmitted sonar signals, generation of imitative signal with spatial parameters, analogous to those reflected by the seabed, and its radiation. This helps to model the shape, the sonar shadow and the reflective surface of the bottom mine in order to mask it by generating a packet simulating chaotic impulse disturbances with parameters corresponding to those of possible reflections from fictitious bottom objects and by re-emitting the received and additionally modeled hydro acoustic pulses with a calculated time lag to achieve the desired result.*
Keywords*: DETECTION, CLASSIFICATION, SONAR SIGNALS, BOTTOM MINE, SIMULATING CHAOTIC IMPULSE*

1. Introduction

When analyzing the processes for improving the methods and means for increasing the effectiveness of actions for detection and destruction of sea mines, should not ignore the fact that except as a threat to shipping, naval mining weapons are an important tool for protecting activities in the adjacent sea areas against enemy forces in cases of war or armed conflict and have a real deterrent effect.

In the implementation of modern systems for counteracting sea mines, which represent an information complex deployed on many levels, here is a reversal in hydroacoustic technology, used in the fight against sea mines, which is characterized by a transition from the simple discovery of a sea mine as a local hydroacoustic target to detailed monitoring of the underwater environment through the combination of the two technologies – the traditional sonar with determination of the coordinates of the contrast energy point from the reflected hydroacoustic signal and side-scan sonars, which initially used as profilografi seabed registering mainly the hydroacoustic shadow of an object protruding above the seabed. The localization of mine as a local hydro-location target against the background of the environment is increasingly transformed into the creation of a detailed sonar map of sections of the seabed with detailed inspection of any suspicious object and fixing all local changes, which guarantees the safety of navigation in coastal areas.

As a basic anti-mine weapon of surface ships (mine hunters) against mining threat self-propelled autonomous or remote-controlled underwater vehicles are used, which are usually equipped with side-scan sonar equipped with a sonar antenna type array antenna with synthesized apritura (Fig.1).

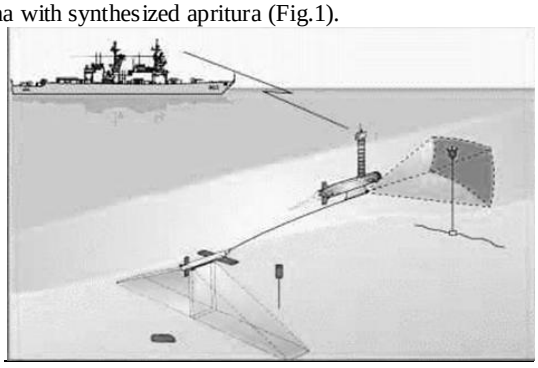


Fig. 1 *Principle of operation of a modern self-propelled autonomous anti-mine system*

The sonar provides detection and classification of mine-like objects with simultaneous processing according to the level of the reflected hydroacoustic signal (echo signal) and the shape and characteristics of the hydroacoustic shadow against the background of reflections mainly from the bottom and from the noise - own and at sea. For this purpose, they are usually multifrequency, and each frequency is optimized for a specific task, as follows:

- Low Frequency – 75 ÷ 150 kHz - for operation detection anchor and bottom mines a large distance in a horizontal sector 15 ° ÷ 90 ° in the course of the ship and vertical sector of 3° ÷ 30°. The sonar provides 3D imaging of the underwater environment and detection of bottom mines on muddy, sandy and stony bottoms;
- High Frequency - 200 ÷ 300 kHz - to work in all types of bottom detection and classification of bottom mines echo signal and sonar shadow;
- Very High Frequency - 400 ÷ 600 kHz - working mode classification with high resolution on a rocky bottom with a strong bottom reverberation.

The width of the horizontal and vertical sector of inspection (scanning) in HF and VHF are usually in the range of respectively 10 ° ÷ 30 ° and 10 ° ÷ 20 °.

The emitted hydroacoustic pulse has a duration in the range of 0.1 ÷ 0.5 ms with frequency modulation type HFM / LFM / CW.

The technical characteristics of anti-mining sonar showed that rely on detecting bottom mines the energy of the reflected signal over a distance up to 800 meters. Taking into account the speed of sound in sea water (~ 1450 m/s) може to expect a maximum repetition rate $T_{п\,max}$~3s and minimal – $T_{п\,min}$ ~ 0.5÷1 s.

The use of the bottom mine classification method and the ability to improve the mine visibility at small sliding angles of the directional diagram stimulated the emergence of side-scan sonar with variable depth antennas. The realized idea of compiling hydroacoustic maps by grouping the data from the side view was justified only in cases where the surface of the seabed is relatively flat and homogeneous. Studies have shown that acoustic inhomogeneities and especially the unevenness of the seabed dramatically reduce the quality of the hydroacoustic picture, which varies depending on the angle and distance to the bottom. Therefore, without special procedures it is impossible to compare the images of the same section of uneven seabed from the screens of different sonar, as well as from the screen of the same sonar, when the geometry of the survey has changed.

2. Assumptions and ways to solve the problem

Current trends in the processing of mine detection signals by their sonar shadow and reflected signal level, as well as the signs and algorithms used for this in the anti-mine sonar, determine the following requirements for the newly developed bottom mines to ensure their camouflage [1- 4]:

- low vertical profile - to make smaller sonar shadow;
- low reflectivity - is assessed by the center of gravity and if a mass has a larger area it is lower contrast;
- large area - the shadow is masked, and in addition the filters for the size of the target (regarding the dimensions of known mines) do not classify it as a mine-like target [1,2];
- symmetry of the form - usually a double search of perpendicular courses is performed and the signals from the targets are evaluated (subtracted).

The analysis of these conditions shows that the first and partially the second can be achieved with the help of design solutions and the use of camouflage and low reflectivity materials. Other conditions must be modeled by means of active agents for enhancing anti-mining resistance of bottom mines.

For this purpose by a team of Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences /IMS-BAS/ is a designed and developed device "Jammer for Sonars of Mine Warfare Vessels", which provides when it is irradiated by ship sonar and after exceeding the level of signals received from the acoustic antennas above the pre-set thresholds, generating a series of electrical pulses according to a predetermined algorithm in the corresponding frequency range, which then transforming them into acoustic signals emitted by the jammer in the water surrounding space.

Figure 2 shows:

1. Sonar indicator MG-79 without jammer;
2. MG-79 sonar indicator with jammer;
3. DUBM21B sonar indicator without jammer;
4. DUBM21B sonar indicator with jammer.

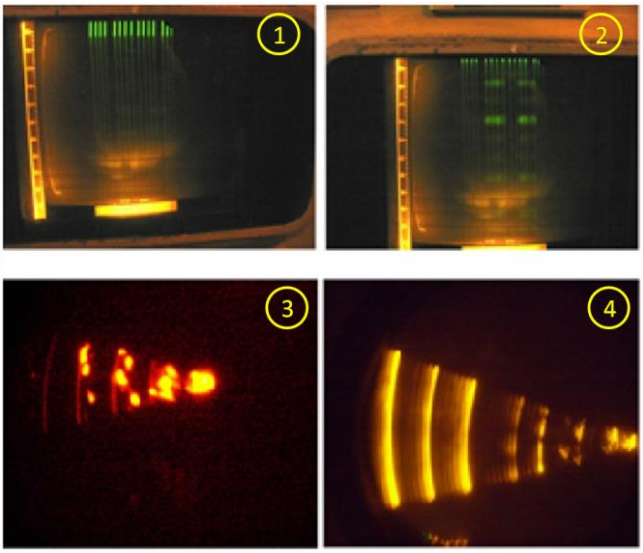


***Fig.2** Picture of mine sonar indicators*

The analysis of the image shows that after its activation, the jammer unmasks its place, respectively that of the bottom mine, if it is installed in its body. From a tactical point of view, its use is appropriate within the minefields to increase the efforts of anti-mine forces, as well as to mislead them about the existence of mine barriers.

In the specialized anti-mine sonar for optimization of the sonar image analysis process - echo signal + hydroacoustic shadow, an analysis is performed by placing on the image of a suspicious object a suitable delta mask, described by deterministic statistical laws. For specific sonar characteristics (frequency range, resolution, acoustic beam angle, noise, reverberation and echo), the statistical variable representing the image of the mine and the statistical variable representing the image of the bottom are considered to be statistical mixtures, which are presented using a set of delta masks.

The significant characteristics of the hydroacoustic shadow from underwater objects are:

- the average brightness of the shadow, which is a measure of the darkness of the shadow of the object;
- the average brightness of the illumination, which is a measure of the brightness of the illumination of the object;
- the scattering of the shadow;
- dissipation from the seabed;
- the contrast between shadow and illumination, which is the absolute difference between the average brightness of the shadow and the average intensity of illumination;
- the contrast between shadow and background, which is the absolute difference between the average brightness of the shadow and the average strength of the background.

To reduce the effectiveness of this type of anti-mine sonar, it is necessary to make such changes in the sonar image, both in the background and in the shadow of the bottom mine, че that the detection system implemented on anti-mining sonar to be "deluded", that the discovered target is not mine-like, but is, for example, rock bottom rock, alluvial or sand formation, etc.

Realized by a team of IMS-BAS device for forming in response to irradiation imitating pulse disturbances,, which is protected by Patent for Invention Reg.№ 67138 B1, provides an opportunity to change the delta mask used by the sonar algorithms in the process of plausibility with a mine-like object and to create additional elements in the delta mask of the soil at the bottom, which would complicate the analysis of the mixture of pre-embedded in the system masks of bottom mines and soil types of the seabed.

The device for forming corresponding imitation pulse disturbances is effective for counteracting sonar with a built-in algorithm for analysis of the hydroacoustic shadow of an underwater object, but the protected object is energetically contrasting with the seabed and creates preconditions for inspection by other means.

3. Solution to the studied

The task of masking a bottom mine against the background of the seabed in the area where it is placed in position is to create a device for the formation of a response masking impulse disturbances, which provides an impact on the algorithms for analyzing the sonar image, used in modern anti-mine sonar, by masking the shape, shadow and reflective surface of the bottom mine, by simulating the reflection of ultrasonic energy in the field of view of anti-mine sonar with an intensity close to that characteristic of the seabed [3].

A device is available for this purpose, source of responding masking chaotic impulse interference with parameters:

- pulse repetition frequency T;
- pulse duration τ;
- frequency of oscillations filling the pulse f, and
- intensity I,

corresponding to those of possible reflections from fictitious bottom formations with effective reflective surface σд, or the re-emission of received hydroacoustic pulses over time, calculated to achieve the desired result.

Depending on the type of soil on the seabed and tactical characteristics of the area of anti-mining activities, the source of those responsible masking interference can be placed in the body of the mine itself or around it [4].

Activating this/these elements should be carried out automatically after exposure to sonar signal, which is classified as such by the mine-sonar.

Figure 3 shows a block diagram of a device for masking a bottom mine against the background of the seabed, which is performed by forming and emitting corresponding masking pulse interference.

The following blocks and elements are included in the composition of the device for emitting corresponding masking interference [5,6]:

- multi frequency sonar antenna (1), which is composed of n number of piezoceramic transducers, providing the process of reception / transmission of hydroacoustic signals in the whole selected frequency range (50 ÷ 600 kHz);
- frequency signal switch (2), providing switching of the sonar antenna from "receive" mode to "transmit" and vice versa;
- corresponding to the number of piezoceramic transducers hydroacoustic receivers of hydroacoustic signals (3);
- demodulator (demodulators) (6), which separates the envelope of the mine sonar radiation pulse;
- CPU (4), providing the connection and control of the operation of the memory unit, demodulator, synthesizers and modulator of the emitted simulated hydroacoustic signal. It includes a Fourier spectrum analyzer, which allows in addition to spectral characteristics, to determine statistical and other characteristics of the input signals in real time, to analyze random signals in the presence of significant noise, as well as the general parameters and interrelationships between two or more signals in a wide frequency range. The processor unit (CPU) performs the following functions:

– provides preliminary introduction of the attenuation coefficients of the ultrasonic waves reflected from the bottom mine and from the ground in the place of positioning for the respective frequency range, which serve to determine the intensity of the emitted simulated signal;
– registers and classifies the occurrence of sounding sonar pulses from anti-mine sonar and determines its parameters –T, τ, f и I;
– provides memorization of the received hydroacoustic signal emitted by the anti-mine sonar in a memory block (5) ;
– ensures that the synthesizers produce a pseudo-random continuous series of rectangular pulses to mimic reflections from fictitious bottom formations;

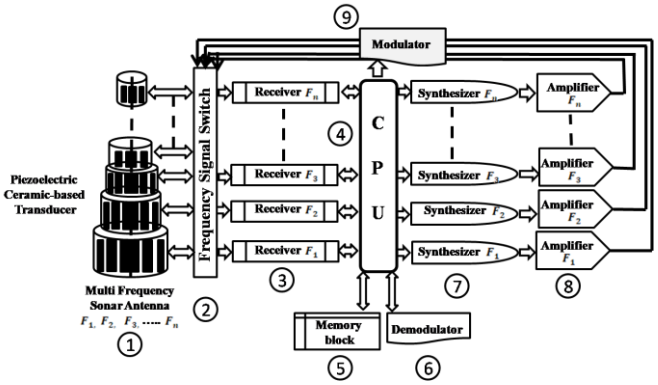


Fig.3 *Block diagram of a device for masking a bottom mine*

- synthesizers (7) and amplifiers (8);
- modulator (modulators) (9), which fills the produced simulation signal, similar to that of reflections from the seabed in the setting area, with the carrier frequency (Fig. 4).

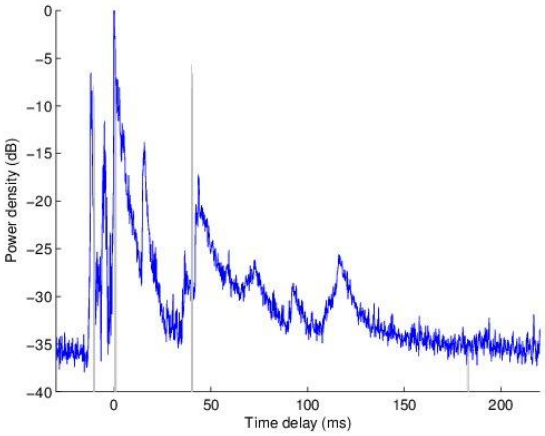


Fig.4 *Oscillogram of reflections from a real seabed*

The principle of operation of the device is based on the analysis of the pulses emitted by the anti-mine sonar and re-emission of masking ones, which are shifted in time, and a series of additional signals are added to the signal reflected by the bottom mine, with intensity of fictitious bottom formations and soil reflected with real parameters imitating pulses throughout the field of view realized by the directional diagram of the hydroacoustic antenna of the anti-mine sonar.

The operation of the device for creating corresponding masking impulse interference proceeds as follows:

- the pulses emitted by the anti-mine sonar in the direction of the mine fall on the multi-frequency hydroacoustic antenna (1);
- the piezoceramic transducer, which has the corresponding frequency band, converts it into an electrical signal (pulse), and the switch (2) directs it to the corresponding receiver for processing and amplification;
- the signal from the corresponding sonar receiver (3) is fed to the input of CPU (4). Unnecessary frequency components are removed in the low-pass filter;
- in the demodulator (6) the envelope of the carrier frequency is separated;
- in the analog-to-digital converter, the input signal is converted into digital form, which is recorded in the memory block (5) and the classification of the plausibility signal is performed with pulse signals from anti-mine sonar. With a positive result, in the processor unit its parameters necessary for the production of imitation pulse interference are obtained, as well as the pulse repetition frequency, whose value determines the time for emission of a complex imitation signal (during this time the receivers are "clogged"). In addition, the intensity (power) of the expected reflected signal is calculated, proportional to the intensity of the incident sonar wave, the reflection coefficient of the bottom mine to be masked, as well as the previously introduced type of soil and bottom formations - rocks, stones, sediments, etc .;
- CPU controls the operation of the corresponding pair of synthesizer (7) - adjustable amplifier (8);
- the signals filled with pulses from the respective synthesizer with a duration equal to the repetition time are fed to the input of the respective adjustable amplifier (8), which gives the pulses the required amplitude;
- in the modulator (9) the envelope of the pulse series is filled with the original carrier frequency of the pulse emitted by the anti-mine sonar;
- through the switch the pulse is fed to the hydroacoustic antenna for emission in the sea space in the direction of the directional diagram of the anti-mine sonar.

4. Results and discussion

Experimental model of the device for formation of corresponding masking impulse interferences is realized on the basis of a product of IMS-BAS – «Bottom mine GM-750», in the housing (on the wings) on which on each side are built 2 lines of piezoceramic transducers, creating a multi-element multifrequency hydroacoustic antenna, which covers the entire range of operation of anti-mine sonar - Fig.5. Electronic unit composed of those in the block diagram (Fig. 3) elements, is placed in an airtight unit within the housing of the mine.

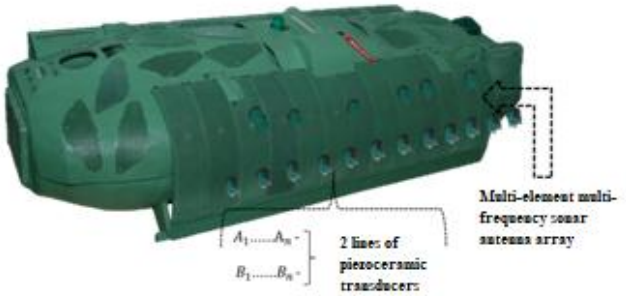


Fig.5 *Bottom mine GM-750 with device for formation of corresponding masking impulse*

The use of the device for formation of corresponding masking impulse interferences significantly reduces the efficiency of modern anti-mine sonar for detection and classification of bottom mines, which function on the basis of two complementary factors - the reflected energy from the mine against the background of the reflections from the seabed formations and the presence of a hydroacoustic shadow after the location of the bottom mine, which reveals not only the fact of the presence of a bottom mine or a mine-like object, but also its approximate shape[7].

The efficiency of the offered device is confirmed by the conducted field tests in the water area of Varna Bay with the use of towed side scan sonar with operating frequency 105 kHz and 500 kHz - Fig.6.

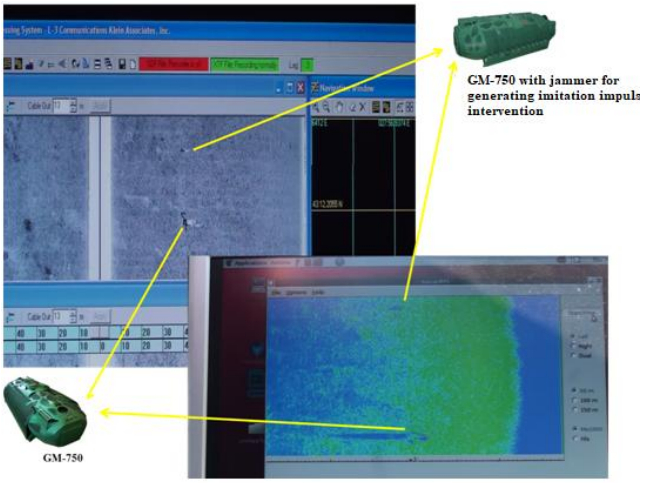


Fig.6 *Images of bottom mines on indicators of towed side scan sonars*

The analysis of the obtained image of the sonar indicator devices shows, that the scattering of the hydroacoustic shadow, the contrast and the brightness of the illumination of the bottom mine and the rock formations of the ground, respectively for the bottom mine GM-750 with and without a built-in device for forming corresponding masking impulse interferences are many times less in favor of the former, which significantly reduces the effectiveness of mine detection by specialized anti-mine sonar [8,9].

5. Conclusion

The device for the formation of corresponding masking pulse interference affects the performance of the algorithms for analyzing the sonar image, which are used in modern anti-mine sonar and provides masking of the bottom mine by generating a complex simulation signal, in which to the envelope of the received signal are added elements characteristic of the pre-entered type of soil and bottom formations – rocks, stones, sediments, etc., and subsequent filling with the original carrier frequency of the received irradiation pulse, with calculated intensity (power) of the expected reflected signal, proportional to the intensity of the hydroacoustic wave hitting the mine body, and with the reflection coefficient of the bottom mine (depending on the height and material of the hull, the technology of profiling the body of the mine, etc.), which is subject to masking, and controlling the repetition rate of the pulses, the value of which determines the time to emit a complex simulation signal (during which time the receivers are "clogged").

The emitted corresponding imitation pulse interference provide a change in the actual characteristics of the sonar image to a degree, when the device for classification of the echo signal in the sonar от does not register the presence of the active pulse interference, nor does it detect a sea mine or decide that the reflections are from more contrasting bottom objects.

The developed device is intended for use in complex port security systems, maritime infrastructure facilities, areas of maritime national waters and other systems for protection of critical infrastructure sites and in conducting operations related to national security [5-9].

6. Acknowledgements:

The results can be used in the implementation of Work Package 2 “Intelligent Security Systems” of Project BG05M2OP001-1.002-0006 – Creation and Development of a Centre of Competence “Quantum Communication, Intelligent Security Systems and Risk Management” (Quasar), funded by the European Regional Development Fund through the Operational Programme “Science and education for smart growth 2014-2020”.

7. References:

1. Samuel Shephard, Simon P. R. Greenstreet, GerJan J. Piet, Anna Rindorf, and Mark Dickey-Collas. Surveillance indicators and their use in implementation of the Marine Strategy Framework Directive. ICES Journal of Marine Science 2015, doi:10.1093/icesjms/fsv131;
2. J. A. Fawcett (2001) Image-based classification of sidescan sonar detections, Proceedings of CAD/CAC 2001, Halifax, Nov. 12-14;
3. S.Reed, Y.Petillot, J.Bell (2004) A model based approach to the detection and classification of mines in sidescan sonar, Applied Optics, Vol. 43, Issue 2, p237-246;
4. G.J.Dobeck (2001) Algorithm fusion for automated sea mine detection and classification, Proc. MTS/IEEE Oceans Conf. and Exhibition, pp.130-134;
5. Kiril Stoichev**,** Dimitar Dimitrov**,** Valeri Panevski. Critical infrasturture integrated security and protection. IMSETHAC-BAS, 2018, ISBN:978-619-90310-8-7, 258
6. Borislav GENOV, Delyan NEDELCHEV, Mitko MIHOVSKI, Yordan MIRCHEV, Comprehensive approach for service life assessment of solid-propellant rocket motors, NDT Days, Volume II / Issue 4 (2019), ISSN: 2603-4018 (print), 2603-4646, pages 467-475
7. Antoaneta Simeonova**,** Dimo Kirilov**,** Angel Krumov. Good Practices and Increasing the Protection of Big Industrial Sites in Risk Situations. Year 3, Issue 1 (5), NTS for MECHANICAL ENGINEERING, 2019, ISSN:(print) 2603-2945, (online) 2603-2953, 76-78
8. Tumbarska A.**.** Criteria for Evaluating the Capabilities of Groups of Similar Non-lethal Weapons. Security & Future, Брой 1, Scientific Technical Union of Mechanical Engineering, 2017, ISSN:2535-0668, 30-33
9. Tumbarska A.**.** Maritime Piracy and Armed Robbery Evolution in 2008-2017. International Scientific Journal "Security and Future", 2, 1, Scientific Technical Union of Mechanical Engineering, 2018, ISSN:2535-0668, 18-21
10. Panevski V.S**.**. Systemic approach to the development of security systems for critical infrastructure protection as a research methodology applied at the center of competence QUASAR. SECURITY & FUTURE, 4/2019, Scientific Technical Union of Mechanical Engineering "Industry 4.0", 2019, ISSN:2535-0668, 144-147

Technical requirements and test methods of elements of equipment-specialized security remedies firefighters in incident critical infrastructure

Ivanov Ivan [1], Nikolova Valentina [2], Liliq Damyanova [3]
Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria[1,2,3]
Email: itoivanov@abv.bg[1],valya_g@abv.bg[2], lilydamianova@gmail.com[3]

Abstract: *A report and examined the technical requirements and test methods for components of the equipment -specialized protective equipment to protect personnel - firefighters , for neutralization and elimination of threats and consequence of these incidents at sites of critical infrastructure*
Keywords: *SITES OF CRITICAL INFRASTRUCTURE, MEANS FOR PROTECTION OF FIREFIGHTERS*

1. Introduction

The modern development of technologies predetermines the use of various substances and materials. Defiles small part of them according to their physico-chemical properties are flammable, explosive and toxic. These properties, in turn, determines the item requirements to specialized protective means (SPM) for the protection of firefighters involved in accidents and neutralizing the effects of them.

2. Technical requirements for protective equipment

Protective clothing, for firefighters is specialized personal protective means (SPPM) providing protect the torso, neck, arms and legs fireman. [1]

An additionalspecialized personal protective equipment (ASPPE) is for protect the head, face, wrists and feet.

Although the role of the firefighter is to put out fires, he has many other activities where thermal protection is not required.

Therefore, finding a balance between thermal protection, comfort and other requirements is crucial. Determining the danger s gives an opportunity for the fire department, after a risk assessment to make choices consistent of risks assessment.

Specialized protective means (SPM) is the sum of SPPM and ASPPE with suitable protection of the respiratory tract , where necessary degree.

The use of inappropriate SPM may affect h and reduced productivity and perception and has a paradoxical effect in the daily activities of firefighters.

It is essential that the fire and rescue service at critical infrastructure sites carry out a risk assessment. To verify compatibility th and ergonomics so all parts of ASPPE (respirators, gloves, boots, etc.) And meet at Ziska Regulation (EU) 2016/425 on personal protective equipment. To ensure protection from nuisance is necessary firefighters and staff in maintenance to is familiar with the selection, use, care and maintenance of all personal protective equipment. [2] There is an increased focus on the contamination of firefighters and / or their SPM by smoke, particles and gases, as well as all decontamination processes.

In order to achieve a certain level of protection and comfort of SPPM with assessment of the probable risks, the requirements to SPM and ASPPE are determined.

The requirements for protective clothing, cover design and comfort and, visibility so,of heat a and flame of m echanical and and chemical and materials.

In er h on an assessment of risk, and the specificity of the medium in which they are used SPM levels of protection are divided into two levels of performance:

- **Level 1**: defines the minimum requirements for firefighting clothing when working with fire outdoors and their ancillary activities taking into account the environmental conditions of expected operational scenarios such fire protection activities.

Level it is not applicable for protection against risks arising from firefighting or rescue from firefighting activities in buildings, unless they are combined with level 2 or another and specialized and PPE.

- **Level 2:** defines the minimum requirements for fire fighting clothing risks encountered etc. and firefighting and rescue of fire in structures (buildings).

The distinction between Level 1 and Level 2 clothing is limited to the requirements for protection against heat (X1) and flame (X2). These levels of protection can be achieved through a single garment or a combination of individual clothing.

A security enes are pairs is degrees of protection against ingress of water with identification marks (Y) and resistance to water vapor with (Z).

At the high level of efficiency - Level 2 of SZS is aimed at specialized firefighting with a large amount of radiant heat, operations dealing with hazardous chemicals and others. dangers.

2.1 Requirement to SPM - comfort and design

2.1.1 Black

The levels of protection of the SPM are achieved by clothing, which may contain multilayer materials or combinations of materials. The elements of which composition eno clothing must meet the specified requirement, and should be tested together. To ensure a certain level of protection, they must be worn together. [3,4,5].

In protections ene and from two-piece suit must have overlapping jacket and pants while. The overlap must be maintained when both hands move over the head and when not bending from a vertical position until the fingertips reach the ground. The wrists and ankles should remain covered in an upright position.

Verification of the fulfillment of this requirement shall be visually. [1]

In anshniya t material from which made clothing to misses harmful substances to the inner layer and from there to the skin of the person wearing it. [6,7,8,9,10,11,12]

Protective clothing should be designed so that the design there are no sharp edges, bumps or protrusions, the reason yavashti injury to the user.

The end of the sleeves, the lower part of the jacket and the end of the trouser legs (overalls) should be made of material that does not allow loosening. Also can stand stably and tightly to the body, in order not to miss the entry of water and harmful substances.

On the clothing are stitched claimed reflective, fluorescent signs, tapes or Combin ation for them to provide no visibility unto them from afar.

D pockets

All pockets of the garment must be designed in such a way as to prevent the entry of heat, flames or hot and gases and material.

The pockets are external and internal made under the following requirements:

(a) an outer pocket made of a separate piece of material such as the outer main sewn on the outside without piercing the outermost layer of the garment.

b) outer - built-in pocket sewn for the inner material of the garment without piercing the outer layer of the garment.

Increasing the number of pockets can lead to additional weight and insulation of the garment, which can increase the physiological impact on the user.

Hood

It is very important to determine in what operations to use a garment with a hood. When the garment is designed with a hood, it can have a negative effect on the accumulation of heat or the perception of the user (reduction of hearing and perception).

Breathable material

In order to allow passage of moisture from the garment from the inside out the material from which is made the garment should be "breathable". This fabric is suitable for slaves because it does not allow the body to be steamed.

And inspection

The clothing is made with holes and nspektsi her in order to provide not possible to verify the protective layers or coatings and different seams.

Closing system

The area of the closing systems must provide the same level of protection as the rest of the garment.

The distance between the broken closing system (eg holes or fasteners) must not lead to unprotected openings in the garment. When using zippers, the sliding clasp shall be designed to lock until fully closed, including when using a zipper with a quick release mechanism. The closing system must not be opened accidentally. The verification of the fulfillment of this requirement is performed visually and with a manual test. [13]

3. Test methods

3.1 Heat and flame

3.1.1 Flame propagation test

All materials and structural seams are tested before and after pre-treatment. Results are evaluated when samples are included in the test framework.

The prefabricated component of the outer garment shall be tested by applying the test flame to the surface of the outer material and to the surface of the innermost lining of individual specimens. [14,15,16]

Clothing type "bulb ", the outer garment and the innermost lining should be tested in addition to separately and together . The sutures are tested with three samples and they must not be opened. In the test Obrazetsa item must be oriented so that the seam to walk the middle line of the test specimen so that the flame of the burner to hit directly on the seam.

The material used for the cuffs of the sleeves and legs and the end of the jacket shall be tested separately, with the flame directed at the outer surface of the material.

Tags, badges, reflective materials, and the like., K oito is applied on the outermost surface of the garment is tested so only after pretreatment in combination with the outer layer to make possible the taking of samples. [17].

3.2. Contact heat test on garments marked X2

For level 2, three samples of component a or clothing must be tested before and after pre-treatment . The tests are performed at a temperature of 250 ° C [18] . In the net test, each sample must have a minimum residence time of 10 s.

K lasifi cation is based on the lowest single result of three they separate values and rounded to the nearest whole second count for the result obtained.

3.3. Heat transfer test of garments marked X1/X2 at:

- Flame - The test is performed with at least three specimens from the set of samples before and after preliminary preparation - cleaning of the garment according to the manufacturer's instructions [19,20]. The classification is according to the lowest single result of the three separate values and rounded to the nearest whole second is considered for the obtained result (Table 1) ;

Tabl. №1

Heat transfer index	Level of implementation 1	Level of implementation 2
HTI_{24}	≥ 9,0	≥ 13,0
$HTI_{24} – RHTI_{12}$	≥ 3,0	≥ 4,0

HTI_{12} – time in seconds, expressed to one decimal place to achieve an increase in the temperature of the caliper of (12 ± 0,1)) ^{0} C.

HTI_{24} - times per second, expressed to one decimal place, to achieve a temperature increase in the calorimeter of (24 ± 0,1) ° C

Transmission - The test shall be performed with at least three copies of the sample set before and after preliminary preparation. [21,22] The tests are performed at a heat flux density of 40 kW / m^2. (Table 2)

Tabl. №2

Heat transfer index (radiation)	Level of implementation 1	Level of implementation 2
$RHTI_{24}$	≥ 10,0	≥ 18,0
$RHTI_{24} – RHTI_{12}$	≥ 3,0	≥ 4,0

3.4. Residual tensile strength of the material upon exposure to:

- Radiation- The test is carried out at least in triplicate on sample sets of a base and in the weft of the outermost material after pre-treatment at a density of heat flux of 10 kW /m^2. Each specimen must have a tensile strength ≥ 450 N. [23,24]

- Heat resistance - and zpitvane it is carried out at a temperature of (180±5)°C for a time of 5 minutes. All the material and the used and clothing should not ignite m or top th and does not shrink so more than 5 %. Each layer of material is tested separately. [25]

Closing system devices were tested at a temperature of (180 ± 5) ° C for a time of 5 min., They should retain the function after the test.

- Heat resistance of seam s clothing - test shall be carried at a temperature of (260 ± 5) °C, the seams must not melt.

3.5. Test for resistance to penetration by liquid chemicals - The test is performed with at least three specimens from the set of samples after pretreatment. Proveryavat filaments warp and weft , using the time for -application of 10 s, with liquid chemicals described in Table. 3. [26]

For each sample there must be no penetration to the inner surface and the index of the repulsion to be ≥ 80% classes cation based on average result of test .

Tabl. №3

Chemikal	Mass (%)	Temperature of chemical ± 2 °C
H_2SO_4	30	20
C_8H_{10} (o-xylene)	100	20

3.6. Mechanical examination of the material from which the garment is made

- Tensile strength

P ri testing of in anshniya material after the pretreatment, the threads on the base and weft of fabric with a coating must withstand a tensile strength ≥ 450 N. [27]

The seams of the outer material during the test must have a maximum seam tear strength ≥ 300 N. [20]

Tear strength

When testing the outer material after pre-treatment, its warp and weft threads shall be able to withstand a tear force ≥ 30 N. [27]

3.7. Water penetration of clothing marked with Y1 / Y2

The finished product is tested for resistance to water ingress at a pressure of 0,98 ± 0,05 kPa / min and must achieve one of the following efficiency levels:

- Y1 <20 kPa, for clothing without moisture barrier;
- Y2 ≥ 20 kPa, for clothes with a moisture barrier. [28].

3.8 Resize

Changes and size after cleaning material and n and protective clothing should not exceed ± 3% for woven and ± 5% for trikot Agen material and non-woven fabric

The performance test of the kit is not performed. Each layer of the set must meet the requirements for resizing.

3.9. Area of visibility of the material

The minimum size of reflective material should be no less than 0,13 m ^{2}, and the minimum size of the fluorescent material must not be less than 0,2 m^2.

The minimum area for compound material for execution must be not less than 0.2 m^2.

3.10. Comfort requirement

- Resistance to water vapor with marked Z1 / Z2

The requirements for water vapor resistance (Ret) must be in accordance with one of the following efficiency levels for the following indicators:

- Z1> 30 m 2 Pa / W, but not more than 45 m^2 Pa / W;
- Z2 ≤ 30 m 2 Pa / W.

- Clothing testing

the finished product is tested on a manikin at an exposure: 8 s at 84 kW / m ^{2}.

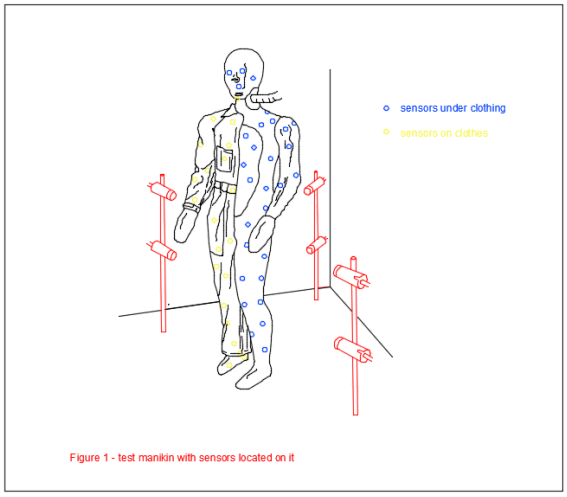
In addition, additional integrated devices must be included to be used with protective clothing testing.

In addition to tests on and clothing Level 2 or prefabricated clothing can be tested and instrumental mannequin with a precondition that the clothes are made from materials tested and have the appropriate size [29].

The test is performed with a single cycle of pretreatment e Reha or said fitted kit, which with is combined to obtain a level of protection X 1 or X 2. T substantially the in heat flux of 84 kW / m ^{2} for a duration of 8s. The test must be performed with or without underwear. The average value for the three tested garments is reported.

Any additional integrated devices that will be used with the clothing may be included in this test.

Thermocouples are placed on the manikin, forming separate sections on it, as the optimal number is 130. (Fig. 1 and Fig. 2)



Fi. 1 *Mannequin with sensors*

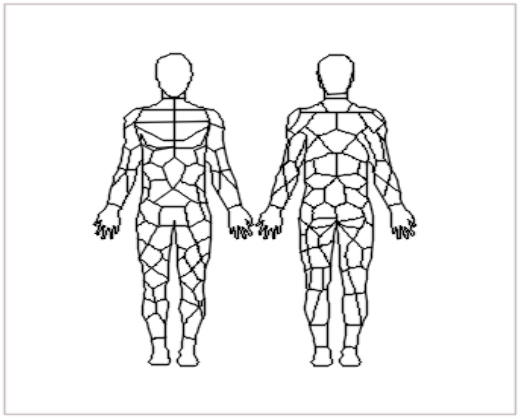


Fig.2 *Zoning*

real test of fire-retardant clothing and the impact on the manikin and the degrees of burns are shown in fig. 3 and fig 4

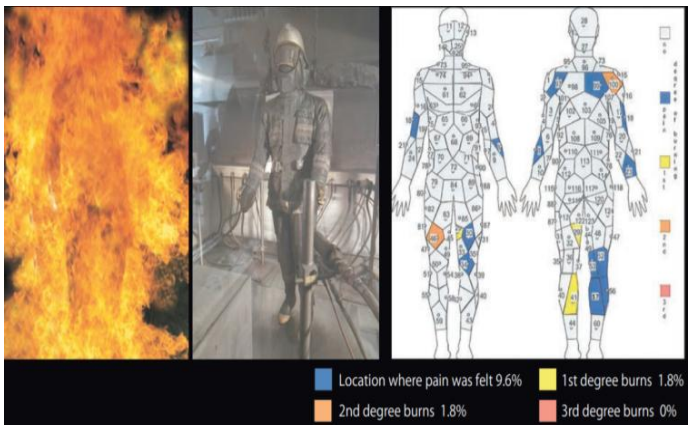


Fig. 3

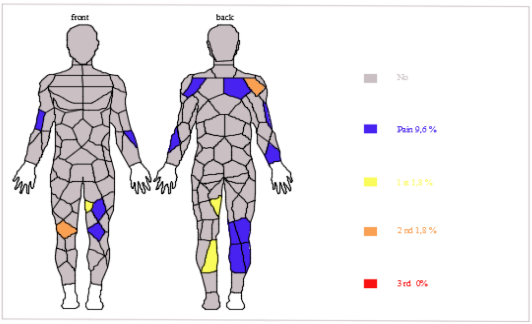


Fig. 4

3. Conclusions

In er n streams passing to the clothes in separate tests in the light of the findings of the risk assessment in real and situations and in case of accidents hazards they have a large effect on the body. for this it is necessary to continue the tests in order to improve the protective qualities of the specialized protective clothing.

According to the risk assessment for the critical infrastructure site with the most likely severe scenarios, we propose to develop a chamber with an integrated version of the test methods in which the amount of oxygen in the chamber, temperature, pressure and flow rate of different gases can be regulated and the combination thereof. The test manikin is wearing a full set of protective clothing and personal protective equipment, with standard equipment - for respiratory protection. The sensors are arranged both on the outer

side of the garment and on the inside by measuring quantities such as temperature, moisture permeable OCT of toxic products, static but electricity, Tamb h Oliri ability.

In conclusion, it can be said that the proposed test model, including the synergy of hazards, will simulate situations as close as possible to the real ones. The conclusions will be drawn for the Grand pm Nittel value of default parameters to which protective agents will be effective, is enabled evaluation of specific protection and against other hazards, for example chemical, biological, radiological and electrical hazards.

The results are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum Communication, Intelligent Security Systems and Risk Management (Quasar) ", which received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

4. References

1. BDS EN 469: 2021 Protective clothing for firefighters - fulfillment of requirements for protective clothing for firefighting.

2. CEN / TR 14560: 2018, *Guide for selection, use, care and maintenance of protective clothing against heat and flame*

3. Yaneva S., Petrov V., Requirements for ballistic resistance of bulletproof vests arising from various international standardization documents, Sixth National Conference with international participation "Metallurgy, Hydro- and Aerodynamics, National Security '2017" 29-30.05.2017, Proceedings, ISSN 1313-8308, pp. 374-378

4. S. Yaneva, STAB RESISTANCE OF BULLETPROOF VESTS. A CONCEPTUAL MODEL OF TEST BENCH, Proceedings of VII International BAPT Conference "Power Transmissions 2020", 10–13.06.2020 Borovets, Bulgaria, Publisher: Scientific-Technical Union Of Mechanical Engineering - Industry 4.0, ISBN 978-619-7383-18- 8, pp.122-126

5. S. Yaneva, BALLISTIC RESISTANCE OF BULLETPROOF VESTS LEVEL IIIA. DEVELOPMENT OF TESTING METHODOLOGY, Proceedings of VII International BAPT Conference "Power Transmissions 2020", 10–13.06.2020 Borovets, Bulgaria, Publisher: Scientific-Technical Union Of Mechanical Engineering - Industry 4.0, ISBN 978-619-7383-18-8, p.127-131

6. EN ISO 139, *Textiles - Standard atmospheres for conditioning and testing (ISO 139: 2005)*

7. EN ISO 3175 (all parts), *Textiles - Professional care, dry cleaning and wet cleaning of fabrics and clothing (ISO 3175)*

8. EN ISO 6330, *Textiles - Home washing and drying procedures for textile testing (ISO 6330)*

9. EN ISO 9092: 2011, *Textiles - Nonwovens - Definition (ISO 9092: 2011)*

10. EN ISO 12947-1, *Textiles - Determination of abrasion resistance of fabrics by the Martindale method - Part 1: Martindale abrasion tester (ISO 12947-1)*

11. EN ISO 15487: 2010, *Textiles - Method for assessing the appearance of garments and other textile- finished products after home washing and drying (ISO 15487: 2009)*

12. EN ISO 15797, *Textiles - Industrial washing and finishing procedures for testing workwear (ISO 15797)*

13. EN 16732, *Sliding zippers - Specification*

14. EN ISO 18640-1: 2018, *Protective clothing for firefighters - Physiological effects - Part 1:*

Measurement of associated heat and moisture exchange with the sweating torso (ISO 18640-1: 2018)

15. EN ISO 18640-2: 2018, *Protective clothing for firefighters - Physiological effects - Part 2: Determination of physiological heat load caused by protective clothing worn by firefighters (ISO 18640-2: 2018)*

16. ISO 9886, *Ergonomics - Estimation of thermal load by physiological measurements*

17. EN ISO 15025: 2016, *Protective clothing - Flame protection - Test method for limited flame spread (ISO 15025: 2016)*

18. EN ISO 12127-1: 2015, *Clothing for protection against heat and flame - Determination of contact heat transfer by protective clothing or composite materials - Part 1: Contact heat produced by a heating cylinder (ISO 12127-1: 2015)*

19. EN ISO 13506-1: 2017, *Protective clothing against heat and flame - Part 1: Test method for completeness of clothing - Measurement of energy transferred using a manikin (ISO 13506-1: 2017)*

20. EN ISO 13935-2: 2014, *Textiles. Tensile properties of fabric and finished textiles. Part 2: Determination of the maximum tensile strength of the seam using the gripping method (ISO 13935-2: 2014)*

21. EN ISO 6942: 2002, *Protective clothing - Protection against heat and fire - Test method: Evaluation of materials and joints of materials when exposed to a radiant heat source (ISO 6942: 2002)*

22. EN ISO 9151: 2016, *Protective clothing against heat and flame - Determination of heat transfer on flame exposure (ISO 9151: 2016, corrected version 2017-03)*

23. EN ISO 13688: 2013, *Protective clothing - General requirements (ISO 13688: 2013)*

24.. EN ISO 14116: 2015, *Protective clothing - Flame protection - Flame retardant materials, joints of materials and clothing (ISO 14116: 2015)*

25. ISO 17493: 2016, *Clothing and heat protection equipment - Test method for convective heat resistance using a hot air circulation oven*

26. EN ISO 6530: 2005, *Protective clothing. Protection against liquid chemicals. Test method for resistance of materials to penetration by liquids (ISO 6530: 2005)*

27. EN ISO 1421: 2016, *Rubber- or plastics-coated fabrics - Determination of tensile strength and elongation at break (ISO 1421: 2016)*

28. EN ISO 811: 2018, *Textiles - Determination of resistance to water penetration - Hydrostatic pressure test (ISO 811: 2018)*

29. EN ISO 11092: 2014, *Textiles - Physiological effects - Measurement of heat and water resistance to steady state (sweat protection stove test) (ISO 11092: 2014)*

Ensuring the safety of people, facilities and buildings from the harmful impact of the explosion

Damyanova Liliya [1], Nikolova Valentina [2], Yaneva Svetlana [3]
Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria[1,2], Technical University of Sofia [3]
lilydamyanova@gmail.com[1],valya_g@abv.bg[2], svetlana_ianeva@tu-sofia.bg[3]

Abstract: *The report discusses the basic requirements for ensuring the safety of people, facilities and buildings from the harmful effects of the explosion. It considers the requirements of the necessary distances, ensuring the safety of people, facilities and buildings from the harmful effects of the explosion.*
Keywords*:SAFE DISTANCES, EXPLOSIVES, HUMAN SAFETY*

1. Introduction

One of the main issues in ensuring the safety of people, facilities and buildings from the harmful effects of the explosion is to ensure safe distances to sites for the production, storage and trade of weapons, ammunition, explosives and pyrotechnic articles .

Basic requirements for planning and design of buildings for production, storage and trade of weapons, ammunition, explosives and pyrotechnics are represented in this report (WAEP). The requirements for risk assessment and management in the planning and design of constructions for (WAEP) are indicated, as well as the necessary minimum distances for ensuring the safety of people, buildings and facilities.

2 . Basic requirements for the planning and design of construction works for the production, storage and trade of weapons, ammunition, explosives and pyrotechnic articles, abbreviated as "construction for WAEPA"

A major issue in planning and design of construction for WEAPA is making a qualitative and quantitative analyzes in order to identify the type of explosion risk depending on the type and estimated quantity of produced and/or stored WEAPA and therefore assessment and risk management.

The basis of proper evaluation and in risk management is identifying the dangers including ensuring the safety clearances for people and property and outside the building for WEAPA. Risk management also includes the identification of environmental hazards, the quantification of the consequences, the calculation of risks and the identification of measures to eliminate and/or reduce the identified risks.

The minimum range of quantitative analysis and risk management includes: dangers and minimum distances from existing sites; type and quantity of WEAPA; location of the buildings and facilities on the construction site for WEAPA; type of building structures; number of potential victims and property affected; way to evacuate.

During the development of the terms of reference for the design of construction for WEAPA a risk assessment needs to be prepared [1] .

3. Risk assessment and management in the planning and design of constructions for WEAPA

When planning and designing the constructions for WEAPA it is necessary to make an assessment of the type of explosion hazard depending on the type and estimated quantity of the produced and / or stored WEAPA. Table №1 shows four types of explosion hazards according to the expected damage from the produced and / or stored WEAPA [1 , 2].

Table № 1

Type of hazard 1	Production and / or storage of WEAPA in which there is a risk of mass explosion (mass explosion is an explosion in which the whole body of explosives explodes as one)
Type of hazard 2	Production and / or storage of WEAPA, where there is a serious projectile danger, but there is no danger of a mass explosion
Type of hazard 3	Production and / or storage of GDPI, in which there is a danger of ignition and insignificant explosion or danger of disposal, or in combination of them, but there is no danger of mass explosion, ie. in the case of explosives which cause significant radiant heat or which are in danger of being discharged
Type of hazard 4	Production and / or storage of WEAPA, where there is a danger of fire and / or light explosion only with local effect, ie. in the case of explosives with a low degree of danger in the event of ignition or activation and there is no danger of discarding fragments of significant size or in a large range

3.1. Explosive pressure and blast wave propagation

The explosive load is a wave pressure caused by the rapid release of energy during a chemical reaction. The propagation of the wave is spherical in nature and is scattered in the direction from the place of the explosion. A scheme of blast wave propagation in open and closed rooms is shown in fig. 1.

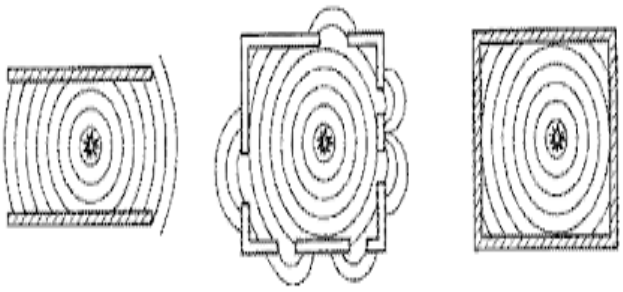


Fig. 1

The first step of the risk assessment process in the event of an explosion requires determining the load from the explosive event . A scheme of blast wave propagation in open and closed rooms is shown in fig. 1 . The first two diagrams show the propagation of the blast wave in open spaces, and the last diagram - indoors. Regardless of the spherical propagation of the blast wave, it will bring differential pressures along the length of some building elements, such as columns. [1 , 2].

Providing protective equipment to buildings, facilities and sites with a potential risk of explosion can significantly reduce the likelihood that people or property located on the other side of the protective equipment will be affected by the blast wave and quickly leave the site of the explosion.

In fig. 2 is a diagram of the propagation of an explosive wave.

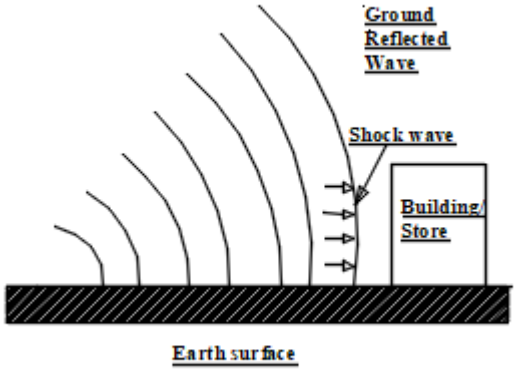


Fig. 2

3.2. Minimum safe distances to urban areas and existing sites of buildings, facilities and sites with a potential risk of explosion, which are part of the construction for WEAPA

In order to reduce the damages and losses from the occurrence of an explosion in sites for WEAPA, it is necessary to locate the constructions at safe distances to neighboring buildings and facilities.

The minimum safety distances shall be measured in a horizontal plane and without regard to the intersection of the terrain from the outer edge of the building and / or the site with potential risk of explosion to the nearest point of urbanized area and / or existing site to which the safe distance applies. [3,4,5,6,7].

Based on the calculations for planning and design of constructions intended for production, storage and trade of weapons, ammunition, explosives and pyrotechnic articles, the normative minimum distances to urban areas and existing sites of buildings, facilities and sites with potential risk of explosion. [8 , 9,10,11].

These distances apply only on medium terrain (dense forest, hill, earth embankment, etc.).

In the table. №2 are specified distances mentioned is that most - important in determining the safety distances there so the number of people who reside in close proximity , the presence of activities open fire ; the presence of gas supply transmission (highway) lines and facilities to them, as well as the presence of railways, highways and roads of I and II class, waterways, stations and ports, which would have a negative impact on the economic plan for the country.

Table №2

№	Name and characteristics of the objects	Minimum distances, m				
		Warehouses, manufacturing facilities and subversive territory with maximum explosives				
		From 10 to 20t	Up to 30t	Up to 50t	Up to 100t	Up to 150t
1	Urban areas, industrial buildings, with farmyards, workshops and other working playgrounds for over 50 people	600	900	1100	1600	2000
2	Barracks areas (barracks, garages, workshops and other farm, residential and administrative buildings in them)	400	500	700	1000	1100
3	Main railways, highways and roads of I and II class, waterways, stations and ports	400	700	900	1200	1500
4	Secondary railways, class III roads and local roads	300	500	700	1000	1100
5	Airports, gas supply transmission (main) lines and facilities to them	600	900	1100	1600	2000
6	Warehouses for flammable and combustible materials	300	300	400	600	800
7	Quarries, open-cast mines and open-air shooting ranges	600	1000	1000	1000	1000
8	High voltage overhead power lines, substations and substations	200	350	450	600	800
9	Separate outbuildings and villas outside urban areas	300	500	700	1000	1100

4. Conclusions

In conclusion, it should be noted that in order to ensure safety so people, equipment and buildings from the harmful effects of the explosion needed to be followed and analyzed these steps:

-Determining the type and quantity of WEAPA produced / stored in one site

- Providing safe distances for people and property on site.

- Providing safe distances for people and property outside the site

The basis of good site management for WEAPA is the planning and design in the initial phase of construction, making an analysis and identification of hazards, risk analysis and taking measures to eliminate and reduce the impact of identified risks Fig.3.

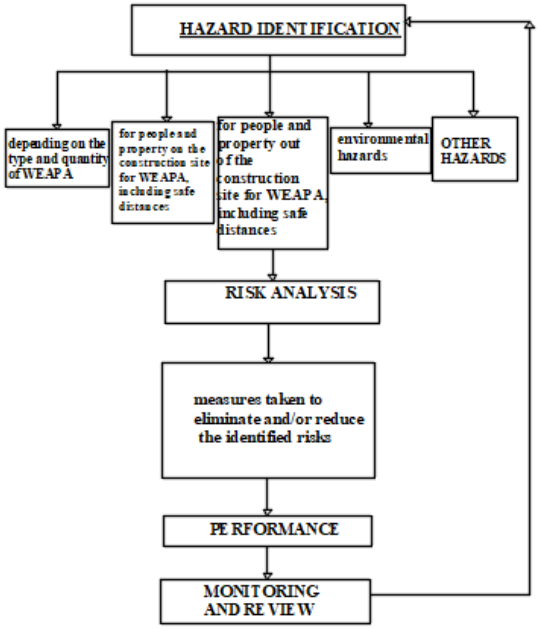


Fig. 3

The results are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum Communication, Intelligent Security Systems and Risk Management (Quasar) ", which received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

5 . References

1. Panevski C. C .. Neccessity to manage business continuity of critical infrastructure. 2019, ISBN: 978-619-188-284-7, 156

2. Panevski VS. Improving the management of business continuity of critical infrastructure by optimizing the functionality of physical protection systems. Publishing House of BAS "Prof. Marin Drinov", 2020, ISBN: 978-619-245-026-7, 192 4, 3, NTS in Mechanical Engineering, 2020, ISSN: 2535-0315, 194-197.

3. Petkov S., Petkov P., Tumbarska A .. Dynamic deformation of the cladding and the body of cumulative charges. Journal of Engineering Sciences, LVI, 3, IMSTCA-BAS, 2019, ISSN: 1312-5702, DOI: 10.7546 / EngSci.LVI.19.03.03, 24-32 National Academic Publishing House

4. Marinov G., Yaneva S .. Requirements for ballistic stability of armored vehicles, arising from GOST R 50963-96 and STANAG 4569. Comparison and analysis. Proceedings of the International Scientific Conference "Technology. Technologies. Education. Security ", 3, 4, NTS in Mechanical Engineering, 2019, 310-313

5. Lichkov N. G, Dimitrov DL, Mihail Hristov, Stoyanov I .. K lasifikatsiya chain equipment as a source of distribution of surface seismic oscillations in different soil types .. Proceedings of the International Conference on Security "CONFSEC 2020", 4 , 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 21-24 National Non-Academic Publishing House

6. Lichkov N. G, Dimitrov DL, Mihail Hristov, Stoyanov I .. Classification of wheeled vehicles as a source of propagation of surface seismic oscillations in different types of soils .. Proceedings of the International Scientific Conference on Safety "CONFSEC 2020", 4 , 1, NTS in Mechanical Engineering, 2020, ISSN: 2603-2945, 17-20 National Non-Academic Publishing House .

7. Tumbarska A. Trends in the development of non-lethal weapons with kinetic (impact) action. Proceedings of the International Scientific Conference "Technology. Technologies. Education. Security

8. Ordinance № RD-02-20-1 of 19.1.2017 on planning and design of constructions intended for production, storage and trade of weapons, ammunition, explosives and pyrotechnic articles (Promulgated, SG No. 11) from 31 January 2017, effective from 01.03.2017).

9. Ivanov I , Marinov G , Current requirements to the safety means for the participants in fire extinguishing for critical nfrastructure sites , 2019, III INTERNATIONAL SCIENTIFIC CONFERENCE Borovets, Bulgaria. ISSN (PRINT) 2603-2945 ISSN (ONLINE) 2603-2953, YEAR 3, ISSUE 1 (5), DECEMBER 2019 , 155

10. Petkov, PS Tumbarska, A. Optimization of the design of fragmentation warheads forming an axial flow of preformed fragments , 2019, iii international scientific conference borovets, bulgaria. issn (print) 2603-2945 issn (online) 2603-2953, year 3, issue 1 (5), december 2019 , 139

11. Ivanov I., Prospects for the use of new solutions in equipment for fire extinguishing in critical infrastructure sites 2020, IV INTERNATIONAL SCIENTIFIC CONFERENCE BOROVETS, BULGARIA. ISSN (PRINT) 2603-2945 ISSN (online) 2603-2953, year 4, issue 1 (6), december 2020, 107

Mobile antenna for underwater system for remote control "SOM_l"

Ivan Ivanov, Stoyan Kolev
Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences

Abstract: *Mobile hydroacoustic antennas have been developed after theoretical optimization of their directivity characteristics. The directivity characteristics in the plane passing through their axis in radiation mode have been determined experimentally. A comparison is made between the calculated and experimentally obtained results for the orientation characteristics.*
Key words *: underwater acoustic system, management, control*

Introduction

The underwater site management system is designed to control the status of underwater objects (on / off) over a underwater acoustic channel by transmitting and receiving coded commands [1]. The control is performed by means of hydroacoustic signals, coded in a way that ensures a minimum probability of false positives. Up to 19683 code combinations can be transmitted.

Exhibition

The one-way management and control system "SOM - 1" consists of:

- control and monitoring device with radiating underwater acoustic antenna with connecting cable up to 25 meters long (Fig. 1);

- underwater actuators, including a underwater acoustic receiver and a receiving underwater acoustic antenna, installed in the underwater sites.

The system for management and control of underwater objects has been adopted by the Bulgarian Army. in 2002. It is an integral part of the system for integrated port security, developed under the NATO program "Port Protection". There is not a single "false" operation during this period of operation.

The system is developed in three variants:

- "SOM - H" for distances up to 500m with a frequency range of transmitted signals from (40 to 70kHz) and a level of not less than 1500Pa per meter of the transmitting antenna;

- "SOM - M" for distances up to 1000m with a frequency range of transmitted signals from (20 to 30)kHz with a level of not less than 2500Pa per meter of the transmitting antenna;

- "SOM - L" for distances up to 3000m with a frequency range of transmitte signals from (10 to 20)kHz with a level of not less than 4000Pa per meter of the transmitting antenna.



Fig. 1. *The system for management and control of underwater objects: on the left - the radiating antenna, in the center - the electronic unit and on the right - the receiving executive device*

The operation of the low-frequency version of the system "SOM - L" showed the need to increase the distance at which it is possible to control the condition of underwater objects. This can be achieved by increasing the level of the transmitted underwater acoustic signals and by increasing the sensitivity of the receiving devices.

The directional characteristic of a cylindrical underwater acoustic antenna in the vertical plane passing through its axis is determined by the same equation as for a linear antenna array [2,3]:

$$R_\theta = \left| \frac{\sin\left(\frac{n\pi d}{\lambda}.\sin\theta\right)}{n.\sin\left(\frac{\pi d}{\lambda}.\sin\theta\right)} . \frac{\sin\left(\frac{\pi a}{\lambda}.\sin\theta\right)}{\frac{\pi a}{\lambda}.\sin\theta} \right| \quad (1),$$

where: n - number of elements that make up the antenna;

d - distance between the centers of the elements;

a - size of the individual element;

λ - wavelength;

θ - angle of deviation from the normal in degrees.

Characteristics in the vertical plane of 15kHz of a cylindrical piezo ceramic antenna based on a cylinder with an outer diameter of 96mm and a height of 60mm at a level minus3dB depending on the number of elements and the distance between their centers are given in Table 1.

Table 1

d / n	62	70	80	90
2	40˚	38˚	34˚	30˚
3	26˚	24˚	22˚	20˚
4	20˚	18˚	16˚	15˚
5	16˚	14˚	13˚	11˚
6	13˚	12˚a	10˚	9˚

Increasing the level of the transmitted underwater acoustic signals is achieved by narrowing the pattern of the radiating antenna of the system in the vertical plane. After analyzing the results of Table 1, a cylindrical underwater acoustic antenna is constructed Fig.2. The antenna includes four piezo ceramic cylinders with an outer diameter of 96mm and a height of 60mm and three passive polyamide cylinders with a diameter 96mm and height 30mm. The dimensions of the sealed antenna of Fig. 2 without the handle are 120 mm in diameter and 380 mm in length.



Fig. 2. *General type of antenna based on four piezo ceramic and three passive cylinders*

Figure 3 shows the patterns of directivity in the plane passing through the axis of the antenna from: blue – theoretically calculated and red – experimentally determined.

With the underwater acoustic antenna realized in this way and by increasing the supply voltage of the final stage of the control and monitoring device from 12V to 36V in laboratory conditions, we registered 18000Pa per meter of the antenna.

After taking into account the signal absorption in the range of about 15kHz of about 1.4dB / km [4] and the attenuation due to the expansion of the wave front - 1 / R [4] at a point at a distance of 3000m we would register a sound pressure of about 0.8Pa. At this value at the level of the encoded sonar signal, the system actuator will receive the command with a probability of false alarms of 0.1.

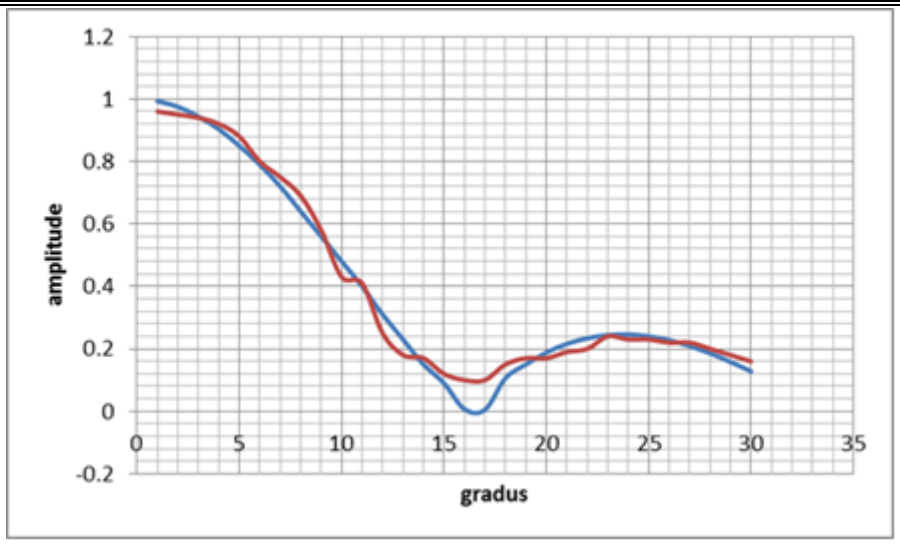


Fig.3. *Directional diagrams in the plane passing through the axis of the antenna of Fig.2: blue - theory, red – experimental*

This work was supported by the European Regional Development Fund within the OP "Science and Education for Smart Growth 2014 - 2020", Project CoE "National center of mechatronics and clean technologies", № BG05M2OP001-1.001-0008-C08.

Conclusion

The developed four-element cylindrical underwater acoustic antenna with 15˚ solution of the pattern in the vertical plane at minus 3dB provides an increase in distances up to 6000m, which with the low frequency system "SOM - L" it is possible to control the state of underwater objects.

Literature:

1. Ivanov I.K., Vodenicharov S.B., Kolev St.G. and others. "Marine Mine Management System", patent 99649 / 15.01.1997, Patent Office of the Republic of Bulgaria.

2. Evtyutov AP, "Engineering calculations in underwater acoustics", ed. Shipbuilding, Leningrad, 1988

3. Orlov LV, Shabrov AA, "Calculation and design of antennas for underwater acoustic fish search stations" Moscow, 1974.

4. Urik R.J. "Fundamentals of underwater oacoustics", translation, ed. Shipbuilding, Leningrad, 1978

MOBILE ANTENNA FOR UNDERWATER SYSTEM FOR REMOTE CONTROL "SOM_L"

Ivanov I.K.[1] eng., PhD Kolev St.G[2] eng, Assoc.Prof., PhD

1,2 - Institute of Metal Science, Equipment and Technology with Hydroaerodynamic Center at Bulgarian Academy of Sciences, 67 Shipchenski Prohod Street, 1574 Sofia, Bulgaria .

e-mail: ivo1942@abv.bg, s_kolev@abv.bg