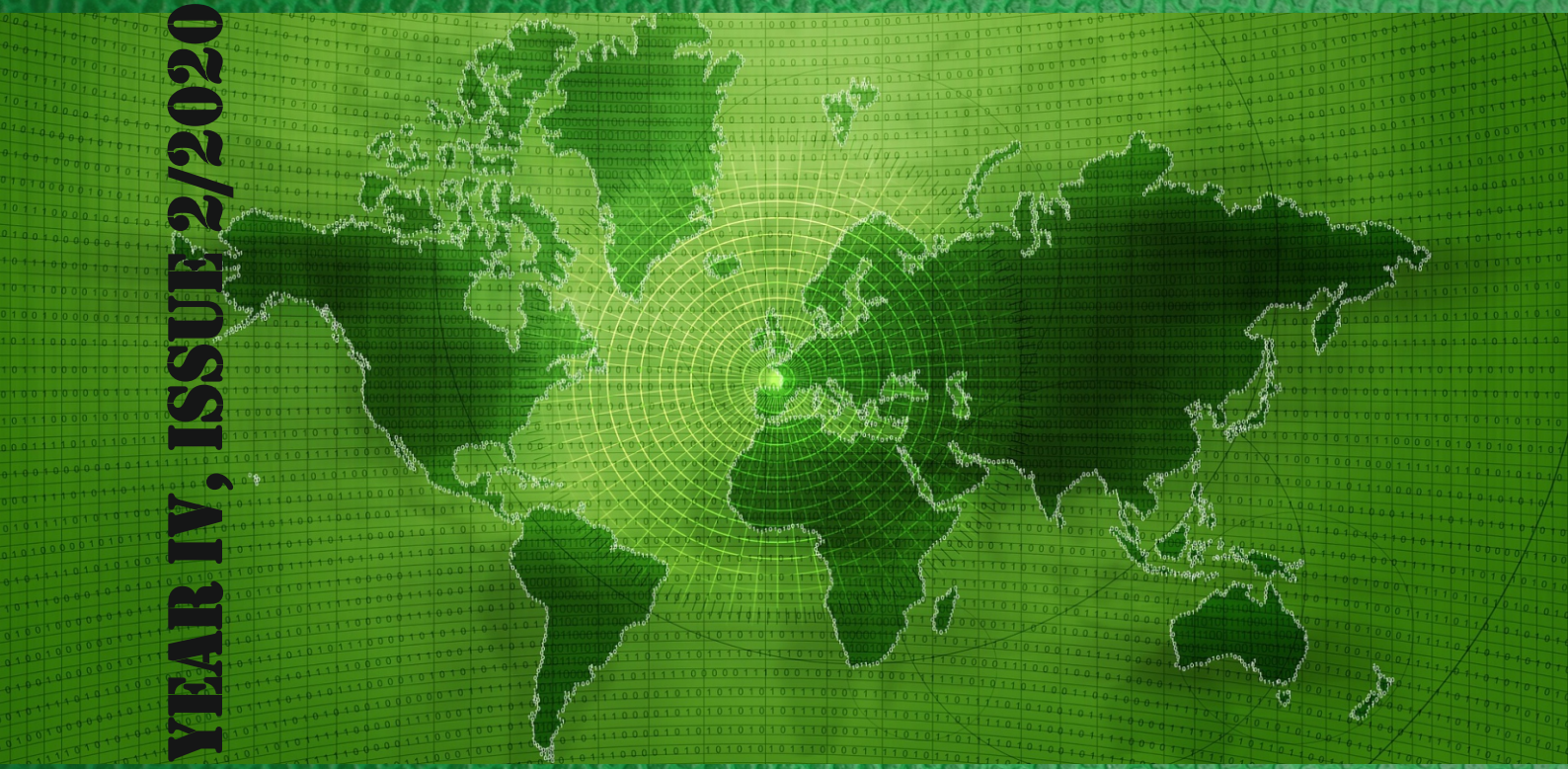
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

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



YEAR IV, ISSUE 2/2020

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 IV, ISSUE 2 / 2020

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

Possible approach for developing a model of intelligent security system applicable in its design in the quasar center of competence
Valeri Panevski 47

Machine vision - important factor for the security development in systems
Stefan Tafkov, Gencho Stoitsov, Ivan Dimitrov 51

NATIONAL AND INTERNATIONAL SECURITY

Selected aspects of the field training of the University of Defence students as a challenge for ensuring security in the future?
Luděk Rak, Pavel Zahradníček 53

INFORMATION SECURITY

Application of Digital Signatures in the Electronic System for Public Procurement in Republic of North Macedonia
Maja Georgioska 57

CMS security tips and tricks
Liliana Petkova 61

Approaching a DoS attack using change and risk management methods
Stefan Pavlov, Vesna Dimitrova, Ljupcho Antovski 64

TECHNICAL FACILITIES FOR ENSURING SECURITY

Audio recording system for underwater monitoring with fast notification for detected sound anomaly
Nikolai Georgiev, Aleksandar Kolarov, Ilian Iliev 68

World radiocommunication conference wrc,19 - impact over security of the modern human society
Veselin Demirev 72

Investigation of characteristics of cylindrical piezoceramic transducers used in systems for underwater monitoring and management
Ivan Ivanov, Stojan Kolev, Bistra Nenova, Vassil Kossev 75

Influence of the clock of the encoding pulses in hydroacoustic transmission of binary numbers
Stoyan Kolev, Bistra Nenova, Ivan Ivanov 78

Safety of the technological process in the production and storage of explosives and ammunition
Damyanova Liliya, Nikolova Valentina, Yaneva Svetlana 80

Possible approach for developing a model of intelligent security system applicable in its design in the quasar center of competence

Valeri Panevski
Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *Through the development and operation of intelligent security systems, with a focus on critical infrastructure, it is expected to improve the security of the population in our country. This process finds real dimensions in the goals and tasks of the centers of competence, which are in the process of construction during the current period. A key element contributing to the proper functioning of intelligent security systems is its design, in accordance with the specifics of the security environment.*
Precisely the synergy of the efforts of the scientific, educational and industrial communities for the development of contemporary models of security systems, structured within the functional scope of the QUASAR competence center, is the basis of this article.
Keywords*: INTELLIGENT SECURITY SYSTEMS, DESIGN*

1. Introduction

Business Continuity Management (BCM) is the way which can solve the challenges facing critical infrastructure (CI), related to the diversity of critical risks to the security environment. The essential part of the BCM is the correct identification of CI-critical risks, the related management strategies to be planned and how to respond to probable risk events.

At the same time, physical security is one of the most basic security aspects of the organization providing BCM. The application of physical security is the process of using layers of physical security measures to prevent unauthorized access or damage.The crucial element that contributes to the smooth improvement of the organization's security is technology.

An intelligent solution is the basis of the operation of the entire technology of the security system, in which the common security is built and managed by the security policy. As the security situation changes, the security policy must be dynamically defined and adjusted in order to achieve the necessary adequate levels of compliance with the type and extent of the likely risks.

In earlier security systems, decision-making and the adjustment of security and protection policies relied mainly on people, leading to an ineffective security response. For highly dynamic and complex network systems, this traditional way of making security decisions and policy adjustments does not meet security requirements **[1,2,3]**.

With the development of technology, it has become possible to automate decision-making with the help of intelligent systems (mechatronic and those with artificial intelligence). In this way the awareness of the situation is improved and through the automated response technology the adaptive protection against the threats to the security of the CI is realized and the speed of reaction is significantly increased.

All this requires a rethinking of the approach to the development of modern CI security systems that meet both the dynamics of the risks of the security environment and be in line with the innovations and innovative processes of applied science and industrial technologies globally.

Therefore, the emphasis of this publication is aimed at presenting the current results of the activities and stages developed by the Institute of Metallurgy, Equipment and Technologies with a Center for Hydro- and Aerodynamics „Academician Angel Balevski" at BAS in the implementation of the Working Package 2 „Intelligent Security Systems" from Project BG05M2OP001-1.002-0006 „Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar), funded by the Operational Program „Science and Education for Smart Growth", co-financed by the European Union through European Structural and Investment Funds.

2. Possible model of the Intelligent Security System

The organization's Intelligent Security System Model (ISSM) schematically describes the purpose and activities of security (and, if necessary, protection), the personnel who perform them, and the interrelationships and consequences of these activities.

Functions of the organization's ISSM:

- Detection of probable risk impact, identification and response;
- Maintaining a constant readiness for reaction;
- Ensuring continuous and normal operation of CI.

The purpose of the ISSM is through technical, organizational and other measures and actions to: identify threats; propose response and reaction to prevent unauthorized access to / unauthorized impact on the protected area / protected areas of the organization / facility of the organization.

The model consists of two parts:

- Organizational part – analyzes and evaluations, policies, strategies, plans and procedures.
- Technical part.

An important moment in the implementation of the ISSM model is the risk analysis and risk assessment, which in the most general framework includes the following elements:

- Risk factors assessment;

- Vulnerability assessment of CI components;

- Staff's resilience assessment against the impact of risk factors.

Based on proper risk assessment, the implementation of preventive protection activities is determined, including works such as:

- Analysis and identification of the risks against which the critical processes are determined, the interdependence between them and the resources necessary for the functioning of the organization. Based on the results, a vulnerability analysis is prepared for all components;

- Analysis of these risks, in terms of their potential to induce long-term cessation of the manufacturing process as well as the probability of their realization and determine their impact level;

- Comparative assessment of the risks level. The aim is to establish, implement and maintain an officially documented risk assessment process that systematically identifies, analyzes and assesses the risk of the impact of the identified risk factors on the components of the CI.

3. Design of a physical protection system model for critical infrastructure

Definition of physical protection system

physical protection system: *An integrated set of physical protection measures intended to prevent the completion of a malicious act.* **[4]**

The design of the physical protection system (PPS), as part of its life cycle, is best achieved through a systematic approach, which consists of three phases (Figure 1), namely:

Phase 1: Identification of the objectives and requirements for PPS;

Phase 2: Design of the PPS to meet the objectives and requirements set out in Phase 1;

Phase 3: Performing an analysis and assessment of the PPS, designed in Phase 2, to achieve the objectives and requirements set during Phase 1.

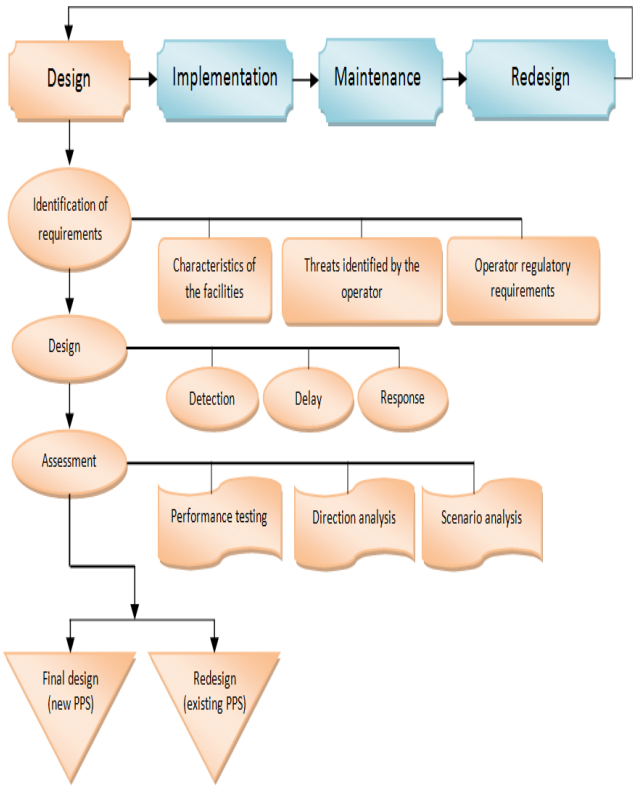


Figure 1: *PPS model design process.*

In Phase 1 of the PPS project design, the key asset management needs to determine how the state's requirements for physical protection of critical infrastructures are included **[4]**.

Several consecutive and interrelated steps need to be taken to identify these requirements:

- Characterization of activity and operating conditions of critical infrastructure;
- Analysis of the information on the threat provided by the state bodies and organizations, which will serve as a basis for the design]
- Defining targets, as well as their location on the object, that must be protected against possible impact.

In Phase 2, a new physical protection system is designed or the existing system is redesigned to ensure the implementation of new or updated physical protection measures, with regard to the timely detection of a probable risk event, delay its implementation and provide an adequate response to its neutralization.

Once the SPS has been designed and characterized, it must be analyzed and evaluated to ensure that it meets the requirements for physical protection.

In Phase 3, an assessment shall be made to determine whether the system meets the requirements set out in Phase 1,

- Confirmation of the functioning of the PPS in accordance with the requirements set in the process of its design and development;
- Identification of possible shortcomings of the system in the design or its implementation, which must be considered in order to provide adequate corrective actions;
- Analysis of possible improvements that may be needed to overcome the deficiencies and improve the functionality of the system;
- Re-evaluate the effectiveness of the PPS on an annual basis to take into account any changes in the objectives, functionalities of the system or the requirements to it.

All this should provide the PPS with the ability to ensure timely detection, maximum delay in implementation and adequate response to possible risk events through structural, technical and personnel measures.

Methods for assessing the effectiveness of PPS, based on results from the operation of this system, could include: analysis of dependencies between many variables; simulation and exercises.

4. General ISSM, applicable in their design

The ISSM schematically describes the purpose and activities of the security, the personnel who perform them, and the interrelationships and consequences of these activities. It could possess a structure set forth in the following.

Functions of the ISSM of the organization:

- Detection of probable risk impact, identification and response;
- Maintaining a constant readiness for reaction;
- Ensuring continuous and normal operation of CI.

The purpose of ISSM is through different and interconnected measures and activities to be identified threats and proposed response and to prevent unauthorized access to the protected area / protected areas of the organization.

The model consists of two parts:

- Organizational part - analyzes, evaluations, policies, strategies, plans, procedures;
- Technical part.

The organizational part consists of:

- Identification of threats;
- Risk analysis and assessment;
- Development of security and protection policy;
- Development of security and protection strategies;
- Development of a security and protection plan;
- Development of corrective preventive activities;
- Development of training programs.

Actions to prevent / repel unauthorized access to security areas must be planned in advance on the basis of scenarios that must correspond to the depth of penetration, location of the breach, separation of the region to prevent adverse effects from random people and taking measures to neutralize intruders and ensure the security and protection of security components. The extent of different levels of protection is determined by the level of risk, the response time, the technical means available and the characteristics of the area.

An important point in the risk assessment is the *vulnerability and criticality assessment* and based on that, determination of the structure of the *technical part* of the model of CI security and protection system.

Vulnerability and criticality assessment process

This process examines the review and analysis of the CI mission in relation to a probable threat (s). The review should assess the value of countermeasures with regard to lost or reduced mission effectiveness. It is then necessary to assess the level of acceptable risk for CIs and personnel, taking into account the level of expected failure in the effectiveness of the mission.

The data obtained from the vulnerability and criticality assessments process provide the CI management with a picture of the overall vulnerability to a likely critical risk impact. As a result, management organizes the development of a security and protection plan that covers all levels of probable threats, regardless of the current level.

The assessment includes:

- identification of key assets of CI;
- determining the possibility of duplicating critical functions in identifying different impact scenarios;
- determining the time needed to duplicate key assets or CI efforts if the key assets are temporarily or permanently lost;
- determining the vulnerability of key CI assets to probable risk events;
- prioritizing the response to the impact of probable risk events on key CI assets.

An important point in assessing the vulnerability and criticality of CI is the conduct of training. Multivariate games are the best test, apart from the actual risk event, to analyze the CI reaction. Trainings and exercises test suspected vulnerabilities and countermeasures. They also train CI management and personnel, as well as the leadership of the response forces, and help maintain a valid threat assessment by identifying and adapting to changing threats.

Given what has been said here, for the purposes of this article in the following lines will be discussed briefly a model of technical part of the ISSM.

Technical part of MISS

According to Directive 2008/114 / EC, security measures are subdivided into **[5]**:

- *permanent security measures* - for their implementation the necessary security investments and the funds to be used at any time are determined. These include a set of passive and active measures to prevent leakage of operational information on: general measures, such as technical measures (including installation of detectors, access control devices, protective and precautionary measures); organizational measures (including signaling and crisis management procedures); control and inspection measures; communication; awareness raising and training; and security of information systems.
- *graded security measures* - are implemented depending on the degree of various risks and threats. They are mainly related to protection against the effects of sudden risk events. These measures are achieved through a set of active safety measures and are applied in combination with permanent security measures. The graded security measures and procedures are regulated in the security plan of the organization / site, developed by the operator.

The combination of security measures defined by the Directive applies to structure the technical part of the MISS. The technical part of MISS outlines three models: a model of the territory on which the organization / object of the organization is located; a model of risks and threats and a model of security and protection equipment. The models determine the parameters determined by the probable means of impact by risk factors and natural disasters, the characteristics of the technical equipment for monitoring and warning of the reaction forces - transport, CIS, armament, assessment of the territory and determination of time to reach critical points, etc.

The generalized model of the technical part reproduces schematically, reduced by the structure and properties of the target by:

- model on the territory of the location of the CI;
- model of risks and threats for CI;
- model of the equipment for security and protection of CI.

Model of the territory on which the organization / object of the organization is located

It includes the development of a model on the territory of a key asset of the organization / object of the organization, considering in detail the peripheral security zone. The model covers all elements of the territory, assessment of risks and threats, and equipment of security components (including protection, if necessary). Areas with different levels of security are defined, and their size is in accordance with the importance of the asset for the functioning of the organization; the level of risk; reaction time; the constructed technical facilities; the terrain of the area, etc.

Actions to prevent/reflect unauthorized access to security and protection areas should be planned in advance on the basis of scenarios that should correspond to the depth of penetration, localization of passability, separation of the area in order to prevent adverse effects from random people and taking measures to neutralize violators and protect the components of the asset. These activities are part of the activities carried out within the organizational part of the model by the security force planning authorities and the specific objective.

The modeling of complex location of an object is done in order to present the security and protection of the object (in each area and segment) through a digital analogue of mathematical modeling and data processing. To solve this problem, the model of the territory on which the organization / object of the organization is located is described by zones, regions and segments.

Risk and threat model

The development of the model aims to analyze the possibilities for impact on the critical goal / critical asset on the basis of developed scenarios and risk assessment.

The model solves the following problems:

- identification of the most probable directions / lines for impact of a probable risk event;
- determination the personnel and equipment that will be used to carry out the impact on the CI/CI object.

The object of modeling is the most probable means of influence with which the probable violators are able to realize influences on the target.

Model of the equipment on the CI/CI object

The model of the equipment is built in order to specify the types of equipment, depending on the possibilities of the probable intruders to have an impact on the CI.

Anticipating the impact on equipment involves solving two types of challenges:

- assessment of the importance of the risk assets of the CI for ensuring the continuity of the activity of the organization in case of the expected impact of a terrorist attack;
- identification of potential means of influencing the risk assets of the CI, which may cause a suspension of operation for a certain period of time.

The development of the technical part of MISS must allow the combination of security features and procedures that work together to ensure the complexity of security and protection of CIs **[6,7]**. MISS functionality must relate to the systematic, integrated, ex-ante protection of CI assets, and not to provide a response to probable risk events after their occurrence. The technical part of MISS and in particular the model of the equipment (in particular the physical protection system) works better if the detection is as far as possible from the CI **[8,9]**, in the presence of a close link between the detection and evaluation processes or a combination of detection, delay and response activities.

5. Conclusion

The presented approach for developing a model of an intelligent security system, in the aspect of its technical part, is only a separate step in the development of a complete model. The main direction of determining the structure of the technical part of the model is 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 / certain risk factors. The essential point is the treatment of the act of threat as a set of risk factors, each of which is able to change the system of security and protection of elements of CI. The correct choice of the structure and the appropriate technical level of the elements of the physical protection system also play an important role here.

Also, the formal division of the technical part into three models allows for the exact distribution of functions between the management and the staff of the CI, with responsibilities in the field of security and protection. This means timely planning of the necessary funds for establishment and development of capabilities, for training and coaching, with a focus on prevention and counteraction of possible risk events that may affect CI.

Acknowledgement

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", co-financed by the European Union through the European Structural and Investment Funds.

Literature:

[1] Dimitar Dimitrov, "Comperatve evaluation of modeling and simulation techniques for interdependent critical infrastructure", International Scientific Journal "Security & Future", Issue 4/2019, Scientific Technical Union of Mechanical Engineering, 2019, ISSN:ISSN: 2535-0668 (print), 2535- 082X (online), p.p. 128-132;

[2] Dimitar Dimitrov, "Comparative assessment of techniques for modeling and simulation of interconnected critical infrastructure", Proceedings of the annual university conference, "Vasil Levski" National Military University Publishing complex, ISSN 1314-1937, p. 231 -241, 2020;

[3] Ventsislav Ivanov Pehlivanski, "Tests in the process of designing protection systems", Sofia 2020, IMSTCH-BAS; ISBN: 978-619-188-359-2;

[4] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, Vienna (2011);

[5] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;

[6] A. Tumbarska, "Trends in the development of non-lethal technologies and protection systems", Monograph. IMSTCH-BAS, 2020, ISBN: 978-619-7466-07-2, 402 ps.;

[7] 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;

[8] Georgiev, N.L. "Analysis of one class of specialized sensors for protection of objects from critical infrastructures", 2015, ISBN:978-619-90310-4-9, 170, monograph;

[9] Georgiev, N.L, "Summary description of the state of sensors by object protection systems", "Collection of scientific papers - Days of non-destructive control", 2015, ISSN: 1310-3946, p.p. 118-120.

Machine vision - important factor for the security development in systems

Stefan Tafkov[1], Gencho Stoitsov[2,*], Ivan Dimitrov[3]
University of Plovdiv Paisii Hilendarski, Bulgaria[1,2,3]
stoitzov@uni-plovdiv.bg

Abstract: *Biometry provides uniqueness in all of its main modalities or combinations between them usually applied for face recognition. A few examples are fingerprints, iris, face recognition, voice, structure of blood system and etc. Nowadays, biometric analysis has much more frequent application in developing digital community. Analysis and categorizing of a given subject behavior is an actual problem with serious application in the field of security. Apart from hardware requirements, the development of smart software methods and approaches for the recognition of suspicious faces and behavior is necessary. The searching of such solutions are directed to the realization of a software system for machine vision. For achieving the goals of this work, some of the most popular technologies such as High performance computing (HPC), cloud services (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Compute as a Service (CaaS)), neural networks (Artificial Neural Network), big data, machine learning and decision tree are studied. It must be mentioned that there is a possibility for the system to be applied with higher precision for predicting future actions.*
Keywords*: BIOMETRY; FACE RECOGNITION; MACHINE VISION, SECURITY, BEHAVIOR*

1. Introduction

Modern security systems are constantly evolving, providing a higher level of security. This is due to the improvement of the used hardware and software components. For example, the inclusion of biometric technologies, hardware components with intelligent functions, high resolution in video surveillance systems for a better image, the use of software systems with intelligent algorithms for analyzing events and scenarios. Biometrics is a current issue in the current development of security. It provides uniqueness in basic modalities or a combination of them for recognizing people. Some of them are: fingerprints, iris, facial recognition, voice, structure of the circulatory system, etc. It enables tracking of behavioral characteristics of individuals to categorize behaviour. The article comments on the initial stage of developing a system for recognizing suspicious faces and behaviour through the implementation of functionality related to machine vision [1-7]. The aim is to implement a prototype of an intelligent system for analysis of events and situations in places with high attendance and prevention of unwanted actions. For the purposes of this survey, technologies have been examined such as high performance computing (HPC), cloud services (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Compute as a Service (CaaS)), neural networks (Artificial Neural Network), Big Data, Machine Learning, Machine Vision, Decision tree.

2. Formal model of the system for analysis of events and scenes

The formal model for event and scene analysis is shown in Fig.1. The event is considered as a categorized signal from a security sensor or software. Occurring events, one or more, generate a scene in which their causes are identified as studied objects. Everything else is assigned to the environment, i.e. a set of objects falling within the field of observation. One or more scenarios can be derived from each scene, from which a conclusion can be made about the observed object and its behaviour. Under a script we will understand the description of the actions of the objects from the scene in an appropriate presentation, taking into account the surrounding environment.

For example, modern security cameras have built-in intelligent functions for line crossing, zone violation, face detection, audio detection, unattended luggage detection, object removal and more. We assume that the camera detected face and movement. The two events that occur form a scene containing the causative objects and their actions. It must be analyzed and saved in Big Data format. The causative agents should be isolated, processed, modeled and categorized, if possible, i.e. whether they are human, animal or inanimate object. In the presence of a person, facial recognition can help identify him; determination of eye and skin color, age group, sex, physique, gait; to establish whether he has past manifestations or not, whether he is prone to unwanted actions, etc. Regardless of the final result, the created model must be saved in the database with an option for later establishment or use. The specific characteristics of a person (body, nose, mouth, ears, eyes, fingers, eyebrows, hair), as well as their location, converted into small images are also preserved. The possibilities of the open source libraries Opencv and OpenFace were used for the realization of facial recognition.

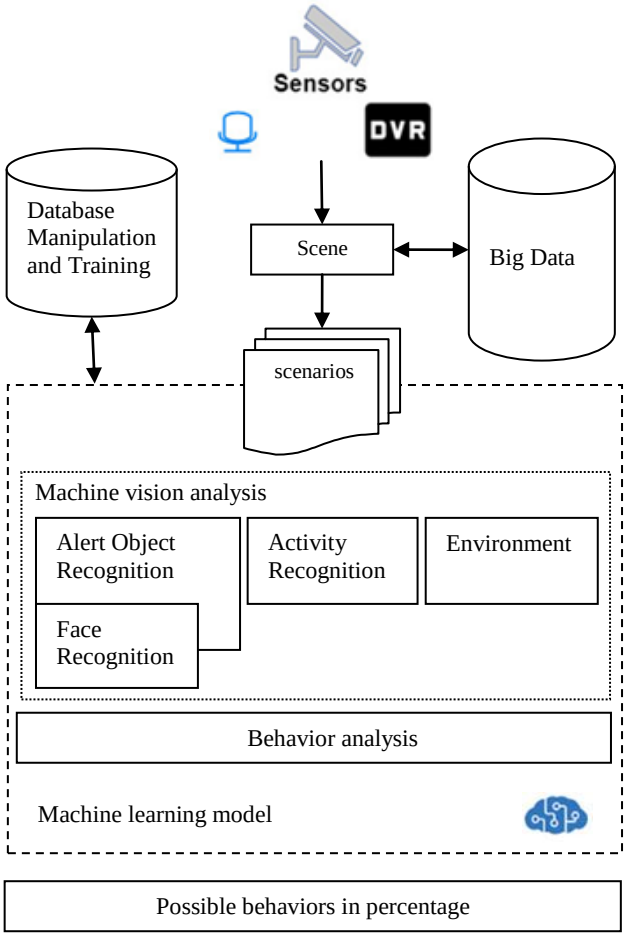


Fig. 1 *Formal model of the system for analysis of events and scenes*

For the environment, it is also necessary to create a model to support the analysis of behaviour. It can be a prerequisite for performing unwanted actions and its early assessment can prevent such circumstances, as well as help to categorize actions already performed.

3. Using Spiderweb AI

One of the goals of the project is to develop a prototype of spiderweb, which uses social networks to collect additional information about an individual using his profile, if any - years, date of registration in the social network, number of comments, number of likes from third parties on his posts, relationships, family, friends, etc. Collecting and analyzing data from third parties - Facebook, Instagram, Linkedin, twitter - increases the quality of analysis. For example, when choosing a platform such as twitter, in which people share their impressions and opinions on various topics, a conclusion can be made about a person's character and propensity for unwanted actions. An Instagram account of an individual could help in finding connections between suspicious people and events related to them.

The initialization of Spiderweb AI can be done with an already existing profile in the given social network and follow a certain set template. For example, the algorithm starts collecting data about the closest people, these are the friends, in the given profile, and then deepens the search depending on the template.

4. Application of the model in other areas

The proposed model is planned to be applied in a smart classroom management system in the initial stage of basic education [8]. Several service scenarios are provided:

Scenario 1: Reporting attendance / absence in class

The automatic determination of students present or absent from classes will definitely be beneficial for the teacher, who is obliged to do so at the beginning of each class. Usually the placement of students in the classroom is fixed for this stage of learning. This presupposes two possibilities for this scenario:

1. Determining the places with missing students, checking with the current template for their distribution by positions and finding the absent ones. This approach must ensure that there is no relocation of the students present. In this case, it is not necessary to turn on the facial recognition function.

2. Identification of all present students, verification with the current template for distribution by positions and determination of the missing or displaced students.

Scenario 2: Face recognition

In this procedure, the first step is to identify the student's face(s). This activity is not always easy to perform, given the many options for the way a person is available. Properly exposed facial areas can be used to extract their various features - eyes, nose, mouth and more. and correlations between them. The end result is facial recognition.

Another possibility is the recognition of facial expressions, which allows tracking the emotions of the student, against which a conclusion can be made about their attitudes for the lesson, their motivation.

Extracting facial features allows for lip reading.

Scenario 3: Recognizing high temperature

It often happens that students in this stage of education attend a class in poor health, for which the reasons can be different and numerous. Usually this type of condition is characterized by high fever. The ability to identify children with poor health, as a result of which they maintain a high temperature, can be transferred as a responsibility of the system. Its functionality must be able to identify a student with a similar problem and signal it to the teacher and parent.

Scenario 4: Behavior recognition

The recognition of behavior can be applied as a possible scenario in the case of school bullying and violence where identification of bullies is needed to be done. Also, vandalism can be a subject of this scenario.

5. Conclusion

The model realization is in its initial stage of development. At the moment, several components are being developed: face detection and recognition, classification of behavior type, neural network learning for face and behavior recognition, development of environment model and Spiderweb AI. Our expectations are associated with achieving high model functionality, which can be useful in the fields of security and realization of scenarios from the management of smart classroom.

6. References

1. Ahonen, T., A. Hadid, M., Face Recognition with Local Binary Patterns, *Computer Vision - ECCV 2004*, Prague, Czech Republic, May 11-14, 2004. Proceedings, Part I
2. Burge M., W. Burger, Ear biometrics in computer vision, *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, Barcelona, Spain, 2000, pp. 822-826 vol.2, doi: 10.1109/ICPR.2000.906202.
3. Divya R., R. Lavanya, A Systematic Review on Gait Based Authentication System, *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2020, pp. 505-509, doi: 10.1109/ICACCS48705.2020.9074361.
4. Elrefaei, L., A. Al-Mohammadi, Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme, Journal of King Saud University - Computer and Information Sciences, 2019, https://doi.org/10.1016/j.jksuci.2019.10.011.
5. Hu, Y., Lu, M. & Lu, X. Driving behaviour recognition from still images by using multi-stream fusion CNN. *Machine Vision and Applications* **30,** 851–865 (2019). https://doi.org/10.1007/s00138-018-0994-z
6. Jalled, F., Face Recognition Machine Vision System Using Eigenfaces. ArXiv, abs/1705.02782, 2017
7. Kpalma, K., J. Ronsin. An Overview of Advances of Pattern Recognition Systems in Computer Vision. Prof. Goro Obinata and Dr. Ashish Dutta. Vision Systems, Advanced Robotic Systems, pp.26, 2007. (hal-00143842)
8. Stoitsov, G., G. Stoitsova, A suggestion for smart classroom's architecture in primary school, *SAI*, Sofia, October 3-5, 2019, 169

Selected aspects of the field training of the University of Defence students as a challenge for ensuring security in the future?

Luděk Rak, Pavel Zahradníček
University of Defence, Brno, Czech Republic[1]
rakl@unob.cz

***Abstract**: The article deals with the topic related to the training of the University of Defence students for the future security environment. The authors introduce their experience gained due to a specific method of training, which is aimed at a new generation of commanders-leaders. They present their results from 2016 to 2020 and the development of this course in consideration with new security challenges. The authors describe selected tools, by means of which the students achieve training goals, forms of multidisciplinary skills and the characteristics of cadets in one. The following results may initiate the discussion of the system and approach to the training of military cadets as potential workers in the field of national and international security.*
***Keywords:** ABILITIES, KNOWLEDGE, SECURITY, STUDY PROGRAM, TRAINING ON THE BATTLEFIELD*

1. Introduction

The training of the future security personnel is one of the important factors in preparing for new challenges in the field of national and international security. In addition to other components of the state, the Army or more precisely the Armed Forces have a dominant role in the security system. From the viewpoint of the organization and operation of the national security system it can be stated that the level of security will depend on capable people who are comprehensively mature personalities able to operate adequately in the system. The beginning of the career of a large part of security personnel starts just at military universities. They are able to form a generation of people who will be ready to face complex challenges and threats affecting national and international security through a well-designed study program and adequate staff coverage.

In 2019, the National Accreditation Bureau approved a new master's degree program entitled Management and Employment of the Armed Forces[1], the guarantor of which is Assoc. Prof. Ivo Pikner, Ph.D. As compared with the original one from 2014, the program was redesigned in many aspects. The new program also meant a practical change to one of the key military courses of the applied basis - Field Training. This course is divided into six semesters and is attended by an average of 200 students in each grade. The Department of Tactics is responsible for the organization, management and outputs.

The future security environment will require young officers to have advanced information skills. The status and mastery of this activity by students is one of the important aspects for field training. Not only for the needs of the course and the emphasis on the development of the ability to make decisions in the case of information (un)certainty, the authors of the article have decided to carry out an experiment. The intention was to test beginning students and their hitherto not very described ability to extract data. For this purpose, they are experimentally confronted with a source that has a surplus of data and rules on how to deal with it under the conditions of limited time and in the activities seemingly unrelated to the data source.

2. Literature Search

Basic literature concerning the experimental survey itself was used; from a methodological point of view, the principles of the work mentioned in the source [1] were also used for planning the experiment. The authors used research results [2] as well as literature dealing with the methodology of commanders´ effective decision-making [7]. The assignment and the very idea of the experiment were formulated on the basis of the results of the studies [10]. In his article, the author describes four acceptable scenarios of the future development of the security situation for the Czech Republic. As for each of the scenarios presented, a goal-directed, well-thought-out information effect of an entity able to produce data of a various type and to appeal to citizens, including the personnel operating in the field of security at least at the national level, may be essential. The social network appears to be the most probable method of this effect. The initial predictions of the authors based mainly on andragogical practice and commanders´ experience are in considerable mutual agreement with the result of the article [3]. The basic research questions of the experiment and the source documents for a final discussion were created on the basis of a sum of conceptual requirements for the needs of initial training of the security personnel in confrontation with the effects of andragogy, current possibilities of social networks and with the use of the article conclusions. [1]

3. Experimental conditions

The research questions were the following ones:

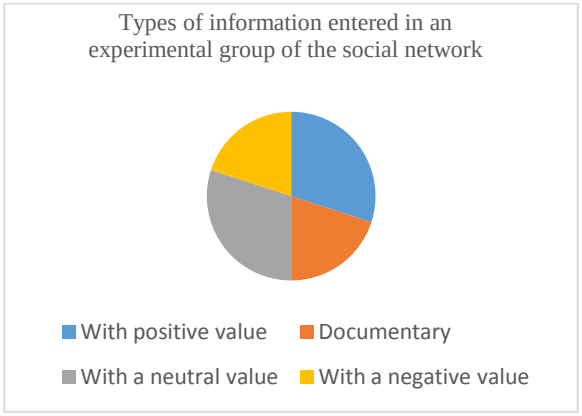
To what extent do the students work with indefinite data when fulfilling the scenario?

To what extent are the students able to use this data for their own benefit?

The experiment was focused on finding out the basic abilities of the University of Defence students, the 1998-2000 age group; it was focused especially on finding out the students´ aptitude for the acquisition, critical confrontation and the use of data provided by an entity with a significant information base working "for their benefit". The students are outstandingly educated people, with military experience of about 6 months, without more intensive training in the field of effect of information technology. The entry requirements for the research sample were supplemented only with the data on the currently favourable state of health. A total of 38% of students are enrolled in study programs in technical fields (including future informatic specialists or military pilots) of the University of Defence, the rest of the students are included in the portfolio of command specializations of the Faculty of Military Leadership of this university. The experiment was carried out as an "IN VIVO" experiment, i.e. a field experiment. The soldiers were divided into four- or five-member groups based on their own preferences. As an important part of the experiment, the scenario was created to test the abilities of the groups of students in basic military skills used in studying at the University of Defence. The whole scenario was realized under time pressure and at night in the municipal districts of Brno. An important factor was the possibility to use a mobile phone with an internet connection throughout the experiment and the students´ participation in a closed Facebook

[1] *Management and Employment of the Armed Forces, program code M1031P020001, date of approval on March 7, 2018, guarantor Assoc. Prof. Ivo Pikner, Ph.D.*

group created in favour of the scenario they were to fulfil. The group administrator (a fourth-year student of information technology) prepared a number of photos in advance from places and outside the places where the students occurred during the scenario. Due to a thorough preparation, about 60 photographs and 8 videos with students in various parts of the city were obtained or staged in advance. Additional information was obtained and sent in the online mode to the group administrator during realizing the race of groups according to the assignment of the scenario. The internet coverage in 90% of the scenario route was sufficient for all networks for the possibility to download and share videos, watch posts and possibly comment on them. The scenario was realized in two stages in February 2019, separately for the students of technical fields and separately for the students of command specializations. The main organizer of the scenario did not join any group; each group was managed exclusively by a designated administrator all the time. He provided the group with ad hoc 30% of posts (data, photos, videos) with an informative value in favour of the scenario, 30% of neutral posts that did not affect the ability of the groups to fulfil the scenarios. A total of 20% of the posts were documentary (photographs of the winners of individual sites, etc.) and a total of 20% of the posts were confusing, misleading, with a negative information value. The Facebook group functioned throughout the individual training groups´ participation in the scenario. The last posts were sent after the end of the whole scenario and were rather of a neutral or documentary nature. The environment of the social group in the Facebook network is presented in Graph. 1.



Graph 1: *Source: Authors´ own elaboration*

Student groups of four or five members were a dependent variable of the experiment; they had an available internet connection and an opportunity to be involved in a pre-created group within the social network. The soldiers in the groups had no medical restrictions, they were in a specified age range, with a specified education and an effort to fulfil scenario seemingly unrelated to the group. They were given information on the group that they could find valid and misinformation materials here and it was up to them whether and how they would use this information. At the same time, they knew that even without the use of this source, it was possible to manage the scenario. To fulfil scenario, the groups of students had to work under time pressure. The decision to put students into groups was made to create opportunities for social networking during the scenario. If the students worked independently and had to complete the tasks of the scenario, they would not have enough time for monitoring and reactions in the Facebook group. A total of 244 students participated in the research.

The group administrator equipped with the data in the above-mentioned ratio was an independent variable. He communicated with both the whole group and the individuals continuously throughout the realization of the scenario.

The intervening variables were mainly the abilities of the individuals in the group to critically evaluate the data, their physical and mental abilities to fulfil the scenario, and the degree of synergy among the members.

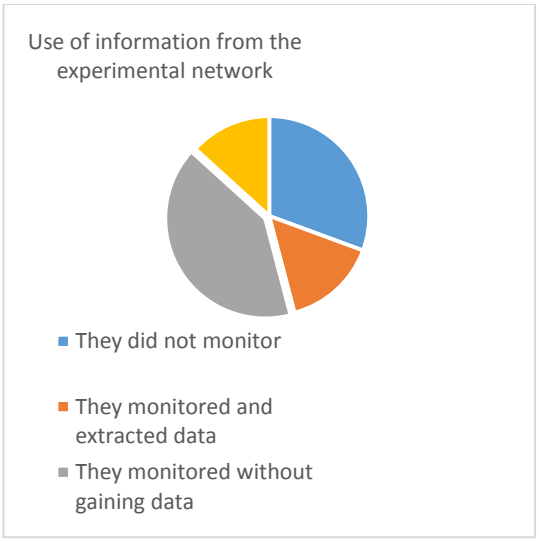
4. Experimental results

On completing the scenario, the students filled out a brief questionnaire related to the use of the requirements for virtual data and especially to the use of the Facebook group for their own benefit. The order of the individual groups was not emphasized during the evaluation of the questionnaires.

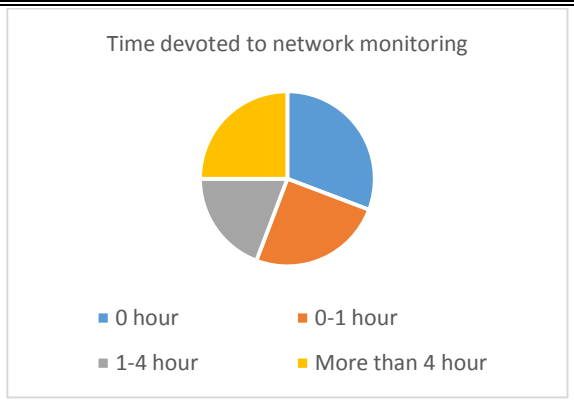
1. Use of data from the Facebook group for the scenario

Out of the total number, 16 groups (30.7%) stated that they had not used the data from this group for the entire period of fulfilling the scenario. 14 groups out of these 16 (26% of the total) stated they had been concerned about the data misinterpretation owing to the time constraint of the scenario. The rest of the groups answered the supplementary question in such a way that they had not had time to devote themselves to the network due to the complexity of fulfilling the scenario.

Other 36 groups, i.e. the mode of the dependent variable (69.3%), stated that during the tasks performed within the scenario, they had monitored events in the social group. 13 groups (25%) with low intensity (within one hour during about 8 hours of the scenario); 10 groups (19%) with medium intensity (i.e. 1-4 hours of the scenario); and 13 groups (25%) with high intensity (all the time, one student appointed by the group watched the network, or more people watched the network). Of this number, only 8 groups (15%) stated that they had managed to find the data that significantly helped them to fulfil their task. It is interesting that with one exception these were the respondents who stated that they had been involved in the network with medium intensity only. The majority, i.e. 21 groups (40%), claimed that the data had not helped them in any way, nevertheless, this data had not had any negative effect on the fulfilment of the scenario. The remaining 7 groups (13%) claimed that the data had bothered them, had guided them incorrectly or otherwise had made the scenario uncomfortable for them. This number also correlates with the information from the group administrator that the soldiers from these groups responded differently to the posts, tried to remove them or to rectify them. This verified the data provided in the questionnaires. It is interesting that more than 50% of these groups simultaneously stated that they had followed Facebook continuously.



Graph. 2*; Source: Authors´ own elaboration*



***Graph. 3**; Source: Authors´ own elaboration*

Overall, based on the data obtained, it can be concluded that during the scenario, only 15% of the groups were able to critically analyse the transmitted data and benefit from them. The remaining 85% of groups either did not monitor the data or were unable to successfully evaluate them, or the data meant an obstacle to fulfilling the scenario. A special feature of these groups was the ability to monitor the network for 1-4 hours only, i.e. not continuously. On the contrary, the groups that paid most attention to the data on the network were not able to use it; they even had difficulties with the data published. In addition, six groups of this category were constantly involved in social networking. Thus, 11.5% of students demonstrated a very low ability to work with information.

The answers to the research questions can be formulated on the basis of these data:

To what extent do the students work with indefinite data when fulfilling the scenario?

Nearly 70% of students worked with the data. Only 30% of them did not show interest in the data despite of the sense of a possible handicap during the scenario.

To what extent are the students able to use this data for their own benefit?

Only 20% of the groups using the data stated that they had been able to use it for their own benefit. The others were not able to interpret it or they misinterpreted it.

It has been found out in the research that the degree of ability to retrieve and convert the obtained data into valid information is very low, even though 80% of the information provided was minimally neutral. Although the overall results of the respondents freely correlate with the statistical normal (Gaussian) distribution, this result is insufficient in the context of the education of members of individual groups. This indicates the fact that students pay very little attention to the critical analysis of information provided by the social network. A partial apology as well as a value reducing this ability could be a generally low level of experience (the respondents were students of the 1st year of the University of Defence). Purposeful misinformation effect appealed to 28 groups (except for those who did not pay attention to the web at all and those who were able to evaluate the data appropriately), which represents an absolute majority (54%) of the entire research sample. Regardless of other consequences, a relatively clear conclusion can be drawn on the basis of the obtained data; that means that such an action can affect an enormous number of people.

Despite of the physically and mentally demanding scenario, there were a total of 23 groups (44%) that stated that they had devoted themselves to the social network continuously. It can be argued here that the research sample has generally demonstrated the ability to have an adequate access to the social network and the ability to determine one´s own limit for focusing on this information.

The introduction of a study subject, which should aim at the increase of students´ ability to critically evaluate the data available on social networks, would be of medium and great importance for a total of 85%, i.e. 207 students. Due to the expected development of this communication tool (not necessarily the Facebook network, but its successors), the number of respondents who did not devote to the network will very likely decrease and thus they will strengthen other groups proportionally.

It will be interesting to follow the development trends depending on the variable (i.e. time) and, at the same time, to confirm or refute the above-mentioned theory.

The whole experiment took place under time pressure; students were exposed to demanding tasks and a great deal of uncertainty. At the first glance, it would be possible to argue that if the respondents worked in a more comfortable environment, they would achieve diametrically different results. On the other hand, it is not possible to overlook the fact that social network users often write posts and comments when they do sports, wait for the train, on the way to work, practically all the time. Thus, the above-mentioned argumentation is inappropriate.

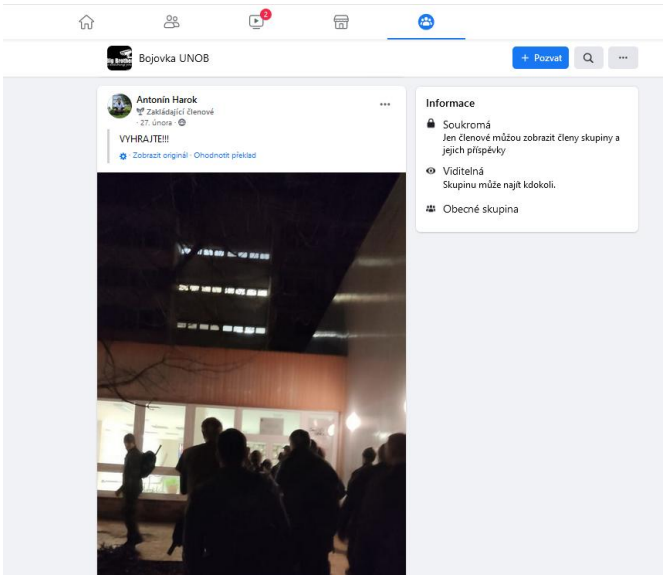


***Fig. 1** Recording of the group; Source: Authors´ own elaboration using the Facebook social network*

5. *Conclusion*

Generally, it can be said that the impact of social networks on the future security personnel is significant. At the same time, the upcoming generation of soldiers, i.e. the students with above-standard education, who have lived all their lives in the information age, does not have an automatic ability to work effectively and objectively evaluate the data obtained. It can be expected that this ability would increase with the age of the respondents, however, not as fast as would be desirable for the needs of the security force activity. For their ability to evaluate the required data quickly, it is necessary to create conditions for them at the beginning of their training, see [13]. The majority of reasonable people strengthen their attitudes to essential things in a long-term process. If they have a limited ability to critically assess data, it is possible to purposefully influence them to accept pre-prepared conclusions. This can be and probably will be one of the basic factors with a

critical degree of threat to national and international security, if these conclusions are not reflected in the adjustment of study subjects for the military school students. At the same time, the findings and the fact described indicate that the respondents, i.e. young educated people, pay little attention to the critical analysis of information from social networks. In the case of long-term high-quality results of selected students, whose work bears the basic elements of intelligence analysis from the beginning, cf. [12] or [11] (albeit in an intuitive way), it is possible to select individuals with a talent for working with information and then to continue to direct them in an appropriate way.

6. References

1. Jackobsen, J.T., European Journal of International Security, ***5(2)***, *The post-politics of public-private security governance:* An ideology critique of the complaints about Facebook. pp. 179-194. (2020)
2. Li, N., Das, S.K., 2019. Inforocm 2019 - IEEE Conference on Computer Communications Workshops, Infocom Wkshps, *Local View Based Connectivity Search in Online Social Networks*, pp. 372-377.
3. Pelletier, M.J., Horky, A.B. and Fox, A.K., Journal of Business Research **122,** *The effect of political and promotional communication from friends and family on Facebook exiting intentions*., pp. 321-334. (2020)
4. Baxa, F., Hodický, J., Melichar, J., Procházka, D. *Obranné plánování při řízení obrany státu*. (2020)
5. Rychtařík, K. (1975). Sociologický Časopis / Czech Sociological Review***11*****(6)„** *Experiment v sociologii*., pp.598-612. Retrieved October 18, 2020, from http://www.jstor.org/stable/41128968
6. Brooks, R., Stanley, E. A. 2007 *Creating military power: the Sources of Military Effectiveness.* (2007)
7. Černý, J.*Vojenský plánovací a rozhodovací proces v operacích.* 292 s. (2019)
8. Hodický, J., Hendandez, A. Simulation and Wargaming, *Wargaming, Automation, and Military Experimentation to Quantitatively and Qualitatively Inform Decision Making*. pp. 40-71 (2019)
9. Hubáček, M., Bureš, M., Břeňová, M., Šimková, K., Zerzán, P. 2017 International Conference on Military Technologies. *The Czech Republic DSM 1, the Quality of the Model in Areas Covered by Vegetation and Possibilities of its Use for Visibility Analysis*, pp. 268-272. (2017)
10. Kalous, M. In Obrana a strategie. Jak (ne)předvídat budoucnost? Rozbor několika průkopnických studií na poli české politické a bezpečnostní scénáristky. (2018)
11. Stodola, P. *Informační podpora rozhodovacího procesu velitele.* 2018. pp 160 (2018)
12. Vojek, J. Vojenské rozhledy **28 (1)**, Vybrané aspekty strukturované zpravodajské analýzy, pp. 059-072. (2019)
13. Vintr, Z. 67. seminář Odborné skupiny pro spolehlivost k problematice softwarová podpora pro spolehlivost. *Informace o spolehlivosti na Internetu*. pp. 3-11, (2017)

Application of Digital Signatures in the Electronic System for Public Procurement in Republic of North Macedonia

Maja Georgioska
University "St. Kliment Ohridski" - Bitola, Faculty of tourism and hospitality - Ohrid Republic of N. Macedonia
email: maja.georgioska@uklo.edu.mk

***Abstract**: The development of telecommunications and computer science has created a favorable climate regarding the increased development of electronic communication and has also led to an increase in the number of electronic documents that are being generated, stored or transmitted via computer networks. These documents are valuable but prone to manipulation by unauthorized persons that consequently leads to a need for enforced protection of the information contained in those documents from unauthorized third parties. Digital signatures provide required validation and verification of electronic documents and represent a series of units and zeros obtained from a particular digital signature algorithm. The article emphasizes the practical application of digital signatures in the electronic system for public procurement by introducing the manner of the electronic signing of documents depending on the application software used by users in the Republic of N. Macedonia.*

***keywords**: DIGITAL SIGNATURES, ELECTRONIC SYSTEM, APPLICATION SOFTWARE, HASH FUNCTIONS, MESSAGES, PUBLIC PROCUREMENT*

1. INTRODUCTION

Various new traditional businesses and applications carry out a huge number of electronic transactions that require information security and authentication. This technology is fairly new and ascending thus assumed to experience growth and wide application in the upcoming years. The need to create digital signatures appears in order to provide greater security and to solve the problem of counterfeiting or misrepresentation in terms of digital communication. A digital signature is a mechanism by which evidence of the authenticity and origin of an electronic document can be given. Additionally, the digital signature provides proof that the sender (signatory) agrees with the document, transaction, or message for which the digital signature is created. The digital signature ensures that the message comes from the right sender and has not been altered.

The efficiency and security of digital signatures depend on the efficiency and security of the used hash functions. If a hash function is not secure, then the digital signature based on it is not secure as well. Therefore, it is necessary to conduct active research and analysis of the hash functions, as well as the detection of possible flaws in their design.

Further on the article presents an analysis of the practical application of digital signatures in the electronic public procurement system in the Republic of N. Macedonia.

2. Digital signatures as a type of electronic signatures in the Republic of N. Macedonia

The electronic signature in legal electronic form is a technology whose application enables verification of the authenticity of the signatory, i.e. confirmation of the identity of the signatory in the system of electronic matters, protects the integrity of the transmitted data and enables irrevocability of the electronic signature on the date of the message, or the document.

Pursuant the Law on Data in Electronic Form and Electronic Signature of the Republic of N. Macedonia, the electronic signature is a set of data in electronic form that is attached to or logically related to other data in electronic form, used by the signatory for signing. [1]

A digital signature is an electronic signature that contains encryption; therefore, it is a type of electronic signature. By using the asymmetric encryption system, the digital signing involves the following steps: [2]

1. the sender writes a message
2. the sender of the message uses a private key to encrypt the message
3. the sender adds a second level of encryption, using the recipient's public key
4. the message has been sent
5. the recipient decrypts the message using his private key
6. the recipient decrypts the second level of encryption using the sender's public key

In addition to using the asymmetric cryptographic system, the digital signature also uses the so-called **hash function** used to create the so-called **printed message,** which is encrypted with a private key and asymmetric algorithm, and is a digital signature of the message.

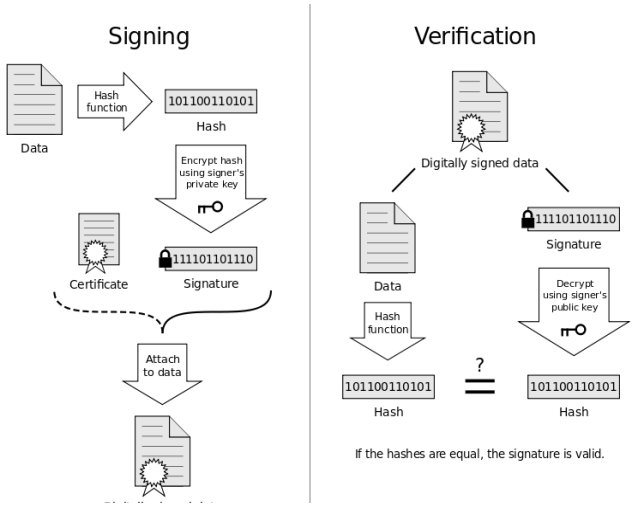


***Fig. 1** Creating and verification of digital signature [3]*

When the aforementioned digitally signed message is delivered to a recipient, it verifies the digital signature by decrypting the signatory's public key and verifies whether thus obtained hash value is identical to the hash value of the message that the recipient identified independently upon receipt. If the comparative data are identical then the verified digital signature and the authenticity of the data are confirmed. [4]

The digital electronic signature can be divided into **two** groups: [5]

- **Advanced electronic signature** - a digital signature based on an advanced certificate with unique identifier of the signatory. Signature keys are used with great confidence by the signatory (who has sole control over the signing key). In the eIDAS system, the electronic signature is considered advanced if it meets several requirements, including: [6]
  - unique identification and connection of its signatories
  - the private key used to create the electronic signature is under the control of the signatory
  - if the data is compromised after the message is signed, the signature must identify what happened
  - revocation of the signature in case the accompanying data changes

- **Qualified Electronic Signature** - an advanced digital electronic signature created by a QSCD and legally equivalent to a handwritten signature. For a digital signature to be considered as qualified electronic signature, it must meet the following three main requirements: [7]
  - the signatory must be connected and clearly identifiable for signing
  - the data used to create the signature must be under the control of the signatory
  - it must be possible to determine whether the data attached to the signature has been compromised by the signing of the message

There are two registered operators at the Ministry of Finance for procurement and installation of digital certificates for digital, electronic signatures in Republic of N. Macedonia, that are accepted in all operating systems and browsers, namely Clearing House KIBS AD Skopje and Telekom MK (Makedonski Telekom). [8]

KIBS [9] is a payment system operator for settlement between small bank payments, established in 2002 and is the first registered Certificate Issuer in the Republic of N. Macedonia. Currently, it operates through the **KIBStrust** brand. KIBS provides **authentication** (the certificate issuer verifies the identity of the certificate holder in the issuance process), **integrity** (digital signature guarantees to the recipient that the received signed data has not changed) and **irrevocability** (the signatory cannot deny the origin of the signature, because only he/she has access to the private key with which the signing is performed). KIBS is certified in accordance with the standards ISO 9001, 20000-1, 22301, 27001, which confirms the quality of the trusted service provider.

Telekom MK (Makedonski Telekom) [10] as a second economic operator has built an infrastructure of public key cryptographic keys (Public Key Infrastructure-PKI) and is a registered certificate issuer (CA-Certificate Authority), in accordance with the laws of the Republic of N. Macedonia and the European Union standards, since 2006. Makedonski Telekom CA is based on Entrust technology, a world leader in the field of PKI systems, certification bodies and protection of electronic operations. Makedonski Telekom CA operates on the basis of self-signed certificate issued by itself in the process of creating keys. Makedonski Telekom provides **authentication** (the identity of the certificate holder is confirmed), **integrity** (the data sent are protected from unauthorized changes), **irrevocability** (the transaction cannot be disputed by either the sender or the recipient) and **confidentiality** (the content of the message can only be read by the designated recipient). [11]

The significance of digital signatures as a type of electronic signatures in the Republic of N. Macedonia mostly breaks through in e-commerce and in electronic contracts signifies confirmation of the authenticity of both contracting parties. As the most important fields of application of digital signatures are e-business, e-commerce, e-banking, e-health-care, e-government and chip card payment systems (EMV). [12]

Additionally, the significance of digital signatures can be seen through the fact that they cannot be challenged or rejected as evidence just because of its electronic form or if it does not have a qualified certificate, or if the certificate is not issued by an accredited issuer or not set up for generally acceptable electronic signature funds. [13]

3. *Electronic system for public procurement in the Republic of N. Macedonia*

The development of technology and the dynamics of the overall socio-economic relations impose the need for public procurement users to be staffed and gain access to technology and electronic executors, in the context of the introduction of electronic public procurement, as well as electronic communication to the Public Procurement Bureau of the Republic of N. Macedonia (PPB). [14] Public procurement is increasingly being adapted to their implementation through electronic means and in the implementation of these procedures, special care should be taken to observe the principle of competitiveness, with particular attention not to prevent or disable the procedure.

In Republic of N. Macedonia, public procurement practice began with the adoption of the first Public Procurement Decree in 1996, the first Law on Public Procurement in 1998, [15] and further on the Law on Public Procurement in 2004, partially in line with EU Directives, and with the World Bank Public Procurement Rules. The amendments in 2005 ensured transparent publication in one place, obtaining timely information, ensuring the legal framework and the practical start and functioning of the new and first established national institution for service of the public procurement system, which is the Public Procurement Bureau. In this period the process of electronic public procurement begins for the first time in the Republic of N. Macedonia, while electronic auctions were introduced by law in 2007. [16] The last Public Procurement Law was adopted in February 2019. [17]

The PPB has managed to develop a sophisticated electronic public procurement system (ESPP), which is the only computerized system available on the Internet at https://e-nabavki.gov.mk, [18] which enables the completion and publication of tenders for the award of public procurement contracts, announcements for requests for bids, notifications for concluded contracts, records for requests for bids, annulment of the procedures, implementation of the procedures for awarding public procurement contracts using electronic means, as well as implementation of electronic auctions.

All actions in the procedures in electronic form can be performed through the ESPP, and at the same time an electronic auction can be conducted only if the technical specifications are precisely defined in the procedures according to the PPL, as well as in re-collection of bids in a multi-user framework agreement procurement system.

The system through which the electronic procurements are conducted is designed in such a manner that the user can use an electronic auction at which he will receive new prices corrected down below, i.e. new values for certain elements of the bids, whereby the auction is structured as a repetitive electronic process, which follows after complete initial evaluation of the bids and enables ranking of the bids with the methods for automatic evaluation.

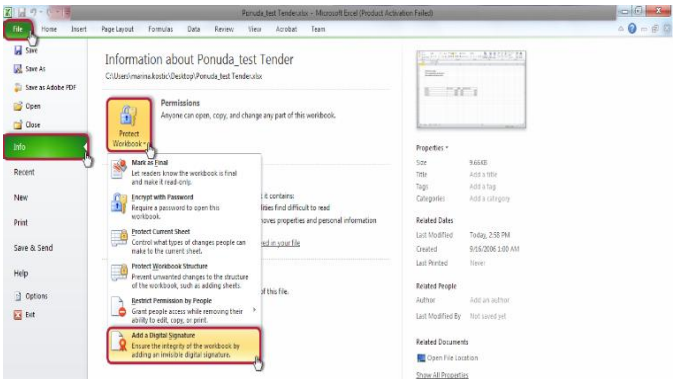
In order to ensure maximum stability and greater visibility, with the latest system upgrades, certain improvements have been introduced in the module for participation in electronic auctions, as well as improvements in the ESPP mailbox. The system provides a secure way of electronic communication between users. The use of the ESPP eliminates paperwork and ensures increased efficiency and budgeting in the implementation of public procurement procedures, which reduces the opportunities for corruption in this area.

4. *Practical application of digital signatures in the ESPP in the Republic of N. Macedonia*

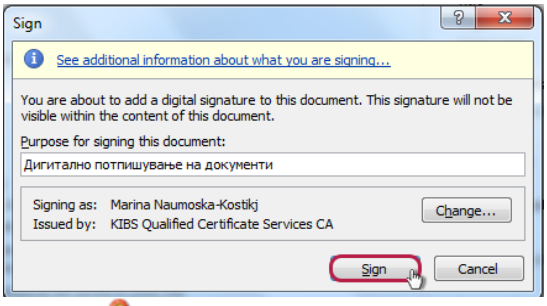
Pursuant the PPL of the Republic of N. Macedonia during the realization of the procedures that are carried out electronically, the documents that are attached and exchanged through the ESPP should be digitally signed with a valid digital certificate issued by the registered issuers of digital certificates KIBS or Telekom MK (Makedonski Telekom). After receiving the valid digital certificate, the participants will receive instructions from the issuer of the certificate on how to install it on their computer or to store and use it through another electronic medium (CD, token, smart card).

The method of electronic signing of documents differs depending on the application program used, so below are those that are most often used in the Republic of N. Macedonia. [19]

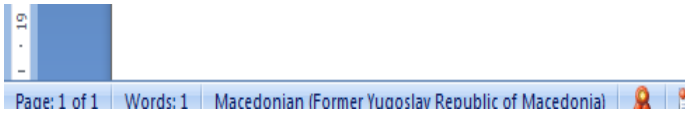
Microsoft Office 2010 - before signing the document, it must be saved under a specific name and the digital certificate / signature must be installed on the computer. The signing procedure is as follows: File -> Info -> Protect Document -> Add a Digital Signature.



Select the digital certificate and click the Sign button.



A red ribbon appears in the lower part of the document with the message that this document contains digital signatures, and if the user wants to see the details of the signatory of the document, he/she should click on the red ribbon and details will appear in the upper right corner (Signatures -> Signature Details).

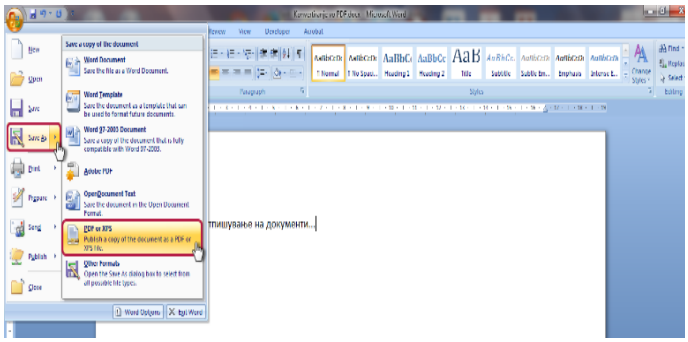


If a document that is digitally signed and the Microsoft Office 2007 package was used when signing, the digital signature would also be visible when opened in the Microsoft Office 2010 package.

PDF documents - to convert documents to PDF format, you need to have PDF Creator (Open Source application) installed on your computer, which can be downloaded from the Internet or directly from the link:

http://www.pdfforge.org/download.

If the user uses MS Office 2010, the document can be saved directly (Word or Excel) in PDF by clicking Save as, then PDF or XPS.



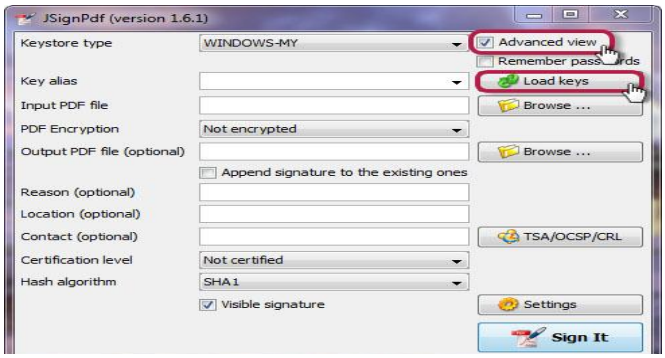
After taking this action, the user's application software will automatically convert the original document to PDF format, which will be ready for digital signing. Signing documents in .pdf format can also be done using the jsignpdf program (free - open source program).

Jsignpdf - for digital signing of PDF documents the user can use the jsignpdf software which can be downloaded for free at the following link: http://jsignpdf.sourceforge.net/.

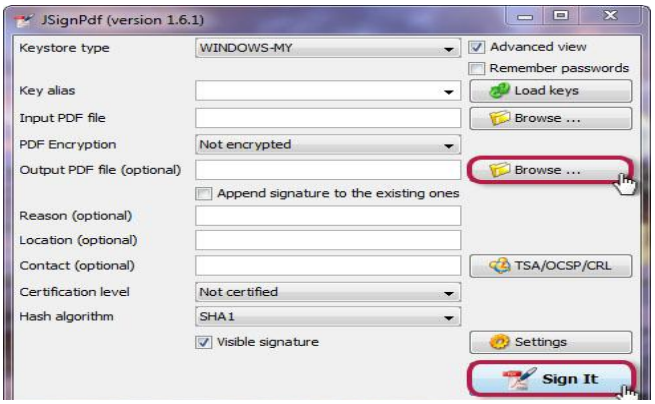
Complete installation documentation and how to sign with this software can be downloaded at the following link:

http://jsignpdf.sourceforge.net/uploads/JSignPdf.pdf

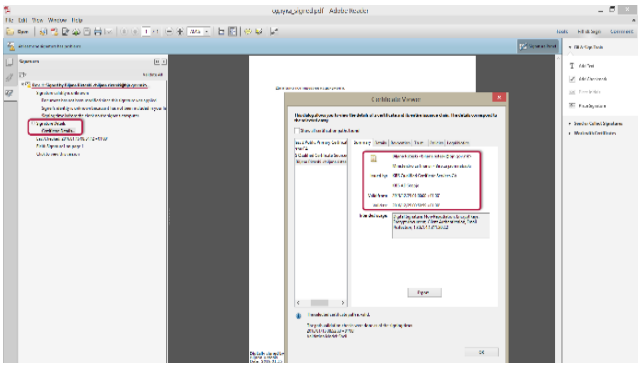
The user must have the digital signature installed on the computer beforehand. The user then opens the JsignPDF program and selects the **Advanced view** button to display additional options. In the **Load keys** field, select the digital certificate that the user has installed on the computer. If the user has installed several digital signatures, it is necessary to select the digital certificate from the authorized issuer of digital certificates intended for public procurement in the field **Key alias**.



In the Input PDF File row, click the Browse button and select the previously saved .pdf document. Finally click the Sign It button, then OK. The signed document is saved at the same location as the original document, only with the suffix signed in the title.



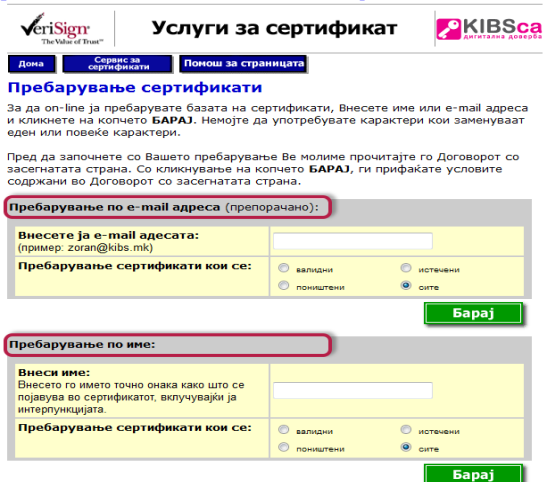
Below is an overview of a document signed in .pdf format.



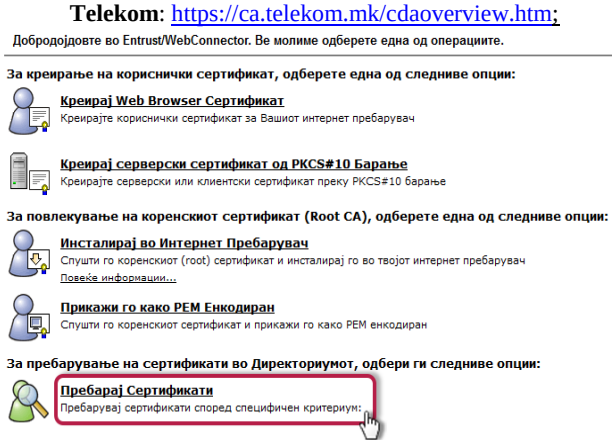
When checking the certificate, pay attention to the validity of the certificate, which can be checked in the applications of the issuers of digital certificates in the Republic of N. Macedonia.

Digital Certificate Validation Websites are:

KIBS
https://secure-ca.kibs.com.mk/services/qcmk/client/search.htm



Telekom: https://ca.telekom.mk/cdaoverview.htm;



If the document says **At least one signature has problems** when checking the validity of the document - it does not mean that the certificate is not valid. Therefore, the user should proceed with the evaluation of the certificate and check in the **Certificate Details-General,** in what name it was issued, by whom it was issued and the duration of validity.

CONCLUSION

The development of telecommunications and computer science has created a favorable climate for increased development of electronic communications, banking and commerce, and thus created conditions for an increase in the number of electronic documents that are generated, stored or transmitted via computer networks. Digital signatures can be considered as the digital equivalent of a handwritten signature or stamp affixed to a document. Digital signatures are a series of units and zeros derived from a particular digital signature algorithm. Digital signatures provide the necessary validation and verification of electronic documents.

Legally, pursuant the Law on Electronic Data and Electronic Signature of the Republic of N. Macedonia, the electronic signature is defined a set of data in electronic form that is attached to or is logically related to other data in electronic form used by the signatory for signing. In Republic of N. Macedonia, there are two registered operators at the Ministry of Finance for procurement and installation of digital certificates for digital, electronic signatures that are accepted in all operating systems and browsers, namely Clearing House KIBS AD Skopje (KIBS) and Telekom Mk (Makedonski Telekom).

In order to ensure maximum stability and greater visibility, with the latest system upgrades certain improvements have been introduced in the module for participation in electronic auctions, as well as improvements in the ESPP mailbox. The use of the ESPP eliminates paperwork and ensures increased efficiency and budgeting in the implementation of public procurement procedures and reduces opportunities for corruption in this area.

E-procurement is, of course, a perspective, but it should be systematically approached and establish balance between knowledge and familiarity with this area of administration on the one hand, and balance between the knowledge and skills of users on the other, and, finally, to pay special attention to the electronic equipment and IT infrastructure in the society so that the digital signatures can be fully applicable.

REFERENCES

[1] Закон за податоците во електронски облик и електронски потпис, Службен весник на Република С. Македонија 34/01, 06/02, 98/08, 33/15 и 244/19
[2] https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/
[3] https://crypto.stackexchange.com/questions/12768/why-hash-the-message-before-signing-it-with-rsa
[4] Рошкоски Т.: Хеш функции и нивна примена во дигитални потписи и дигитална форензика-магистерски труд, ФИКТ-Битола, 2016: 18-20
[5] https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf, 3
[6] https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf, 3
[7] https://podpis-kwalifikowany.pl/mk/%D1%87%D0%BF%D0%BF/
[8] http://transparency.cefta.int/bundles/appapp/documents/TradePortal/Macedonia/P2MK2MK2.pdf
[9] http://ca.kibs.com.mk/
[10] http://www.telekom.mk/business/?z=626
[11] http://ict.telekom.mk/digitalni-sertifikati.nspx
[12] https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zededu.pdf, 17
[13] Закон за податоците во електронски облик и електронски потпис... **op.cit**..., член 12
[14] Аргировски А.: Методи за хармонизација на националното законодавство со правото на Европската унија, Зборник од научна расправа на МАНУ, Скопје, 2008
[15] Службен весник на Република С. Македонија бр.26/1998, стапи на сила на 20 јуни 1998 година
[16] http://dkzjn.mk/files/pdf/zakoni/ZAKON_ZA_JAVNI_NABAVKI.pdf
[17] http://www.bjn.gov.mk/wp-content/uploads/2019/05/ZJN_Sluzben-vesnik_24-2018-od-01.02.2019.pdf
[18] https://e-nabavki.gov.mk/PublicAccess/Home.aspx#/home
[19] Општи и технички препораки при користење на ЕСЈН за економски оператори и договорни органи, БЈН, Скопје, 2016

CMS security tips and tricks

Liliana.Petkova
University of Library an0d Information technology (UNIBIT)
lilyanapetkova92@gmail.com

Abstract: *Content management systems become more popular and due to the speed provided during the development the number of websites developed with a CMS growns extremely. This is the reason the sites developed with a CMS become a more attractive target for cybercriminals. The CMSes are divided in 2 categories: free open-source and paid. According to that categorization the security level of the system is limitless. As part of my research, we are investigating only the free tools supporting the application development process and the presented tools and softwares are only from personal experience! So for the present article, we are going to present the Umbraco CMS with its integrated security tools and some other free to use tricks in order for the system we develop to be secure.*

Keywords: SECURITY, VULNERABILITY, UMBRACO, CONTENT MANAGEMENT SYSTEM

1. Introduction

It is not enough to just have a website, but to adapt with the emerging technologies and security flaws every single day.

With the discovery of content management system(CMS) solutions the web development becomes faster and more flexible through money, time and support. Which makes the choice of working with CMS inevitable. The main goal of our research is to focus on the free perspective of software development.

Understanding the sources of vulnerabilities and learning to program securely is imperative to protecting the Internet and ourselves from attack. [11][12][13]

The third and most comprehensive method integrates security and risk management into the development cycle, either with involvement of security team members or by developing a core security focus on the part of developers. [13]

The present article demonstrates secure websites' development with an open source CMSs in the .NET world. All of the provided samples are gained through personal experience and helped preventing several different attacks or having options to increase the security level of a site.

As a result we provide security analyses on websites developed by us with the help of one open source CMS - Umbraco CMS.

2. Content Management System

A content management system, or abbreviated CMS, is a software that provides speed in developing a website without the need of specialized technical knowledge. But having the necessary skills as a developer we can build powerful and enough secure websites. [4]

Content management systems provide an automated control on the collection, management and the distribution of information.

The functionalities of a CMS are: Collecting (authoring process, acquisition process, automatic format conversion, aggregation process, information reusability and consistent content segmentation into metadata); Management (system security, content storage in a neutral format, automatic indexing, simple and rapid research system, utilisation of standard technologies and languages, simple content modifying, document versioning, content management through a single interface, management of all type of formats, possibility of automatic updating, possibility of automatic deletion, compatibility with other applications, content condivision with other applications, system scalability, automatic workflow, system simplicity and flexibility, security of all content approval processes); Publication (template utilisation to create publications, automatic content conversion, simultaneous creation of more publications, advanced personalisation system, multiple-language interface). [4][5]

In our personal experience we are working on ASP.NET platforms, so the CMS analysed in the current research is also based on .NET: Umbraco CMS.

3. Security Options For Umbraco CMS

The security options list provides most of the details necessary for securing a website developed with Umbraco CMS. [2][3]

Due to the different versions of that CMS, there might be differences in the settings necessary for version 7 and version 8 of Umbraco CMS. As we are analysing the Umbraco CMS we are going to provide not only the setting but the difference too.

3.1. SSL/HTTPS

One step in securing a website is by enabling the HTTPS protocol. There are a lot of benefits in using HTTPS, such as: protection against phishing attacks or "Man in the middle" attacks (which incepts a communication between two systems[1][2]). Another benefit of using HTTPS protocol on the website is the "preference" of Google search engine of the HTTPS over HTTP. As we already have investigated SEO perspective in website security, the ranking of sites with HTTPS protocol enabled is higher.[9][10]

Sample 1: *SSL/HTTPS configuration Umbraco 8 CMS*

```
<add key="Umbraco.Core.UseHttps" value="false" />
```

Sample 2: *SSL/HTTPS configuration Umbraco 7 CMS*

```
<add key="umbracoUseSSL" value="false" />
```

Once the site is HTTPS configured, there should be a redirect rule attached in order to redirect all requests to HTTPS. That way all requests, services, backoffice handlers will be denied.

Sample 3: *HTTPS force rule*

```
<rule name="HTTPS force" enabled="true" stopProcessing="false">
  <match url="(.*)" />
  <conditions>
     <add input="{HTTPS}" pattern="^OFF$" />
  </conditions>
  <action type="Redirect"
url="https://{HTTP_HOST}{REQUEST_URI}"
redirectType="Permanent" />
</rule>
```

3.2. HTTP headers

In one of our previous researches we have presented more detailed the purpose of the HTTP headers. Their use globally protects the entire website from a user-end perspective. But the Umbraco backoffice needs additional protection.

According the Security Headers researcher Scott Helme 7 out of 10 are the most valuable headers which should be included in a site: X-Frame-Options; Strict-Transport-Security; Content-Security-Policy; X-XSS-Protection; X-Content-Type-Options; Referrer-Policy and Feature- Policy! [7]

As the backoffice provides the website's content management, the headers we should definitely use is the Content Security Policy header, which as we have already investigated "reduce the harm caused by content injection attacks". [8]

So in addition to the global site HTTP headers in order to protect the Umbraco backoffice we need to add additional configuration.

To set it up we need to add location related to the Umbraco backoffice access and use the already known code structure!

Sample 4: *HTTP headers security*

```
<location path="umbraco">
  <system.webServer>
   <httpProtocol>
    <customHeaders>
      <remove name="X-Frame-Options" />
      <add name="X-Frame-Options" value="SAMEORIGIN" />
      <remove name="Content-Security-Policy" />
      <add name="Content-Security-Policy" value="default-src 'self'
www.gravatar.com player.vimeo.com *.vimeocdn.com
packages.umbraco.org our.umbraco.org;script-src 'self' 'unsafe-inline'
'unsafe-eval';style-src 'self' 'unsafe-inline';img-src 'self' data:
www.gravatar.com umbraco.tv;font-src 'self';" />
    </customHeaders>
   </httpProtocol>
  </system.webServer>
</location>
```

3.3. Backoffice users

As Umbraco is an open source content management system, developers all around the world can contribute to that CMS with various additional code packages.

3.3.1. Password rules configuration

Every application using password for some reason, needs to configure the password a complex structure to be hard to guess. In Umbraco CMS websites this is managed through the web.config. Websites using Umbraco CMS though need to make this configuration for users which use the front end website, called members, and for users which use the Umbraco backoffice. From a programming point of view each of them is managed with different security providers which are not that different except for the reason that are used for different website sides (*UsersMembershipProvider for users* and *UmbracoMembershipProvider for members*).

For the structure we can define the minimum characters need to be used in the password (***minRequiredPasswordLength***), the need of symbol characters (***minRequiredNonalphanumericCharac ters***), also we can define a regular expression for mapping the password to some kind of model (***passwordStrengthRegularExpression***), and so on (*see Sample 5*).

Sample 5: *User Password configuration*

```
<add name="UsersMembershipProvider"
type="Umbraco.Web.Security.Providers.UsersMembershipProvider,
Umbraco" minRequiredNonalphanumericCharacters="1"
passwordStrengthRegularExpression="^(?=.*\d)(?=.*[a-
z])(?=.*[@#$%^&amp;+=])(?=.*[A-Z]).{12,}$"
minRequiredPasswordLength="12" useLegacyEncoding="false"
enablePasswordRetrieval="false" enablePasswordReset="true"
requiresQuestionAndAnswer="false" passwordFormat="Hashed" />
```

3.3.2. Two steps authentication

The two steps authentication is always a plus in order to protect the application you use or develop. Each well secure software provides that additional authentication proof! As an open source developers can develop such plugins or use already developed packages.

Such packages we have used in several websites developed by us, is the Umbraco 2FA package (*see Figure 1*)!



Figure 1: *Umbraco 2FA*

After its quick backoffice installation, the set up is even quicker than this.

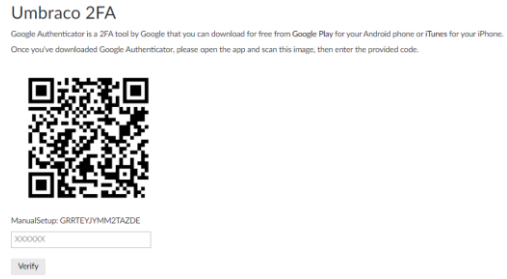


Figure 2: *Umbraco 2FA setup*

By just pressing the Setup button from the backoffice (*see Figure 2*) and installing the Google Authenticator mobile application (*see Figure 5*), after entering the provided code or just scanning the QR code, the setting up is done.



Figure 3: *Google Authenticator code*

And whenever the user tries to login to the backoffice, the second step is just to enter the code from the Google Authenticator application (*see Figure 3*) and the user is logged in (*see Figure 4*).

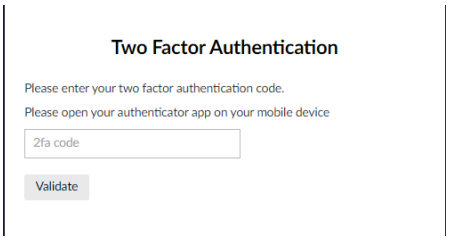


Figure 4: *Two factor authentication Umbraco form*

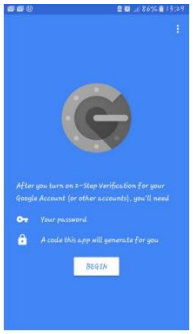


Figure 5: *Google Authenticator application*

The best part of using the Google Authenticator application is that the code is updated in every 45 seconds, so remember it is not an option.

3.3.3. Health Checks

Health Checks is a plugin of Umbraco backoffice which provides a list of areas to check to see if Umbraco is configured and working according to the best practices.

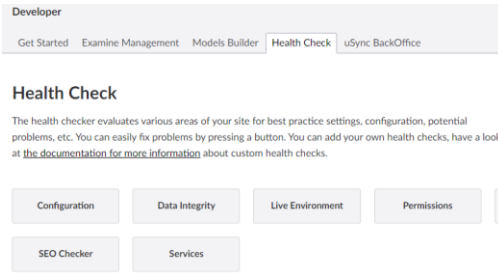


Figure 6: *Health Check plugin*

In the security section the Health Check evaluates potential vulnerabilities and flaws and provides options to fix them, such as *sniffing vulnerabilities, cross-site scripting , HTTPS configuration*, and other checks (*see Figure 7*).

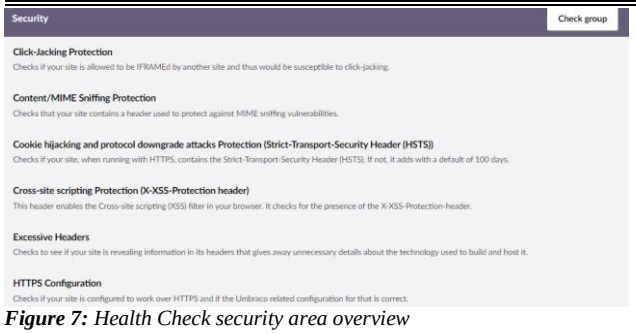


Figure 7: *Health Check security area overview*

4. Results

Our research is based on analyses on several security checks on a few preselected web applications. In our previous articles we have used the ALEXA analytical insight to choose six websites from an excerpt of 50 sites based on a selected Country category - Bulgaria. [7][8][9][10]

But as part of this current research we are looking for websites developed by Umbraco CMS. For that purpose the current analyses are based on websites developed from our personal experience. We are not going to present the name of sites due to law and policies restrictions! [6]

Table 1: *Security statistic*

	site A	site B	site C	site D	site E	site F
HTTP headers	+	-	-	+	-	-
SSL//HTTPs	+	+	+	+	+	+
Health Checks	+	+	+	+	+	+
Password configuration	+	+	+	+	+	+

The results from Table 1 show that the web applications developed from us are not fully secure according to the options we have reviewed so far. Most of the reasons for the lack of security are related to the clients requirements or the fact that we have not still reached the software development phase [6] for integrating the necessary security level in the website.

5. Conclusion

As part of web development, the security perspective takes a major role in it. Being up-to-date with the newelest technologies is one of the biggest steps which can help protect our applications and keep the attackers away.

From the analytics we have provided we have to consider that the use of CMS for web development can give the necessary level of protection. Which as always if not properly integrated, its purpose stays unachieved.

Our entire research is based on personal experience!

References

[1] OWASP Secure Headers Project
[2] Umbraco community, https://our.umbraco.com/
[3] Wahlberg,, N., Sterling, P., Umbraco User's Guide, 2011
[4] Canavan, T., CMS Security Handbook: The Comprehensive Guide for WordPress, Joomla, Drupal, and Plone, April 2011
[5] Benevolo, C., Evaluation of Content Management Systems (CMS): a Supply Analysis, January 2017
[6] Petkova, L., SECURITY STANDARDS in software development, 2017
[7] Petkova, L., HTTP SECURITY HEADERS, 2018
[8] Petkova, L., CONTENT SECURITY POLICY VALIDATION, 2019
[9] Petkova, L., SEO SPAM AND MALWARE, 2019
[10] Petkova, L., SECURITY'S LEAKS IN SEO SPAMMING, 2019
[11] ICT Security Trends, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-766-2
[12] Software testing, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-765-5
[13] ICT Security Model, Willian Dimitrov, Sofia, 2018, Avangard, ISBN 978-619-160-950-5

Approaching a DoS attack using change and risk management methods

Stefan Pavlov[1], Vesna Dimitrova[2], Ljupcho Antovski[3]
Faculty of Computer Science and Engineering
Ss. Cyril and Methodius University, Skopje, R.N. Macedonia[1,2,3]
stefan.pavlov47@gmail.com, vesna.dimitrova@finki.ukim.mk, ljupcho.antovski@finki.ukim.mk

Abstract: *The Information Technology security threats are emerging with each day passing by. The implementation of the technology into every field of society brings changes. Finding a way to manage these changes would be a success, and, by doing so, it would mitigate the risks they bring. Data transmission nowadays is unsecure like never before. Challenging is the way that should be found to cope with these kinds of evolutionary changes. Among the top threats in networks lies the DoS attack. It has been a long time since this kind of attack is around, but that doesn't reduce the fact that this type of attacks is still dangerous and devastating. In order to cope with this kind of attack, we need to know how to manage risks and changes during a DoS attack. Because of this, it is very important that defensive mechanisms are implemented and integrated so that unauthorized access would be prevented from accessing your network or data. This refers to individuals and everyone else working in companies that are working in the field of IT, because at some point, we all share the same thing-devices (mobile phones, personal computers, devices at work, etc.). The base of the IT foundation is knowing how to protect yourself and your data. Due to this, we need to work hard and exploit every possible threat and attack from the inside out. Not only to reduce or mitigate the already occurred impact, but also to prevent these types of failures from happening in the future.*
Keywords*: CHANGE, RISK, SECURITY, DATA*

1. Introduction

It is certain that when dealing with Information Technology (IT), changes will occur. In order to make progress in this area of technology, you have to be able to make the right decisions at the right time, and by doing so, you will be effective. As it is said in [1], if you want to be able to act efficiently and make wise decisions, most of your IT personnel must assess the risks involved in making the change. By the comprehension of the risks, the project manager can be at ease when dealing with changes on entire projects. These changes may affect the project a lot, including the budget, quality, sources etc. The main source of risks today comes from the cyber area, or the main threats are the cyber threats.

This is why in this paper we discuss risk associated with late changes which are done to a network by a recent DoS attack. The paper itself covers the risk and the change management methods when dealing with a DoS attack. At the end of the paper, there is an example which can provide the reader with adequate opinions which can be useful while handling DoS attacks. By doing this, the already occurred damage from a DoS attack would be reduced to its minimum.

2. Change and Risk Management in IT

As the innovation of technology does not tire, it has brought new threats. In fact, the threats are emerging faster than they can be assessed. This refers to the whole world of IT professionals. This technology may have made our lives easier, but it is met by similar innovation technologies which could take advantage of cyber systems for other gains. It is possible that the threats are sponsored by nation-states and the defense systems against those kinds of threats are failing.

While facing these types of threats, we need to provide ourselves with the best defensive mechanisms, which are provided by the change and risk management methods in order to prevent such attacks from happening.

These are modern times, and in modern times with modern technology, come modern network threats. About these threats you can read below.

In [2], a modern network threat paper that has been done recently, ranks the top fifteen threats. If we go back in 2018, the threats that were causing the most network security issues were: Malware, Web-Based Attacks, Phishing, Denial of Service (DoS), Spam, Botnets, Data Breaches, Insider Threat, Physical Manipulation/Damage/Theft/Loss, Information Leakage, Identity Theft, Cryptojacking, Ransomware and Crypto Espionage.

According to [2], among the top fifteen, as mentioned above, are the DoS attacks which are slowly but surely, emerging. More and more DoS attacks occur every day, and this is why, we need to find a way to cope with these types of attacks. In order to understand the attack, we need to know how to analyze and understand the threat first.

As we move on further in [2], there is a classification done on DoS attacks. This classification is based on the idea that if we are willing to deal with the threat, it is essential to understand the source of it. Just as it is said [2], we can see that there are two types of issues regarding this topic and those can be noted as threat agents and attack vectors. As pointed out before, threat sources consist of two entities:

Threat Agents

By [2], the threat agents are the actors, individuals or organizations, who are able to generate or create a threat. The main concern of these agents is their identity. That is why they try to mask it and they claim identification with another group. They usually do this by posting such materials in fake news and social media.

Attack Vectors

Regarding the attack vectors, they are the path by which a threat agent can gain access to a computer or network for the purpose of malicious activity. The table below is as well from the paper mentioned above or [2].

We can see that the DoS attacks to networks are numerous and potentially devastating. Regarding [3], we as well think that many types of DoS attacks are well known and the bigger part of them are quite effective to stop the communication in the networks. This is because this kind of attacks include the use of single computer or multiple computers, called zombies. This is a technique known as simple DoS attack and later on as Distributed Denial of Service (DDoS) attack.

The following part involves a brief description of DoS attacks in order to better comprehend the rest of the paper. If we try to define it, then a DoS attack would be an attack which is launched to make networks and systems' resources unavailable for the legitimate users.

In [3], it is said that most of the hackers have three things in mind. The first one is to find a way through which they can get the secret information. And this would be the way to compromise the confidentiality. The second one involves gaining access to the confidential information to change or modify it. This means the compromising of integrity. The third one is done to compromise the availability. Many of the DoS attacks are made by exploiting the

weaknesses in TCP/IP stack protocols. The classical examples of those DoS attacks are TCP Syn Flood, UDP Flood, ICMP Flood, Smurf and Incomplete HTTP Requests, etc.

Table 1: *Annual change in raking of the top fifteen threats according to the Evolution Threat Landscape (ETL)* [2]

Top Threats	Year						
	2018	2017	2016	2015	2014	2013	2012
Malware	1	1	1	1	1	2	2
Web-Based Attacks	2	2	2	2	2	1	1
Web Application Attacks	3	3	3	3	3	3	3
Phishing	4	4	6	8	7	9	7
Denial of Service	5	6	4	5	5	8	6
Spam	6	5	7	9	6	10	10
Botnets	7	8	5	4	4	5	5
Data Breaches	8	11	12	11	9	12	8
Insider Threat	9	9	9	7	11	14	-
Physical Manipulation/Damage/Theft/Loss	10	10	10	6	10	6	12
Information Leakage	11	13	14	13	12	13	14
Identity Theft	12	12	13	12	13	7	13
Cryptojacking	13	-	-	-	-	-	-
Ransomware	14	7	8	14	15	11	9
Cyber Espionage	15	15	15	15	14	-	-
Exploit Kits	-	14	11	10	8	4	4

A) Classification of DoS Attacks

The Table II, which is from paper [3], shows the classification of DoS/DDoS attacks.

Table 2: *Classification of DoS attacks [3]*

DoS/DDoS	
IPv4	IPv6
Layer 4 (Transport layer) Attacks	Layer 4 (Transport layer) Attacks
Layer 7 (Application layer) Attacks	Layer 7 (Application layer) Attacks
-	Neighbor Discovery Protocol Attacks

B) Layer 4 Attacks

Wireless TCP-Flood Attack

When a client tries to make a connection with a server, both machines, the clients' and the server, exchange a set of messages sequentially. This is known as Three Way Handshaking. As it is described in [3], first, the client sends a SYN (synchronization) message to the server. The server then sends back a SYN-ACK (acknowledgment) message to acknowledge the SYN message send by the client. Finally, the client then responds with an ACK message to finish the establishment of the connection. At last, the connection is then opened and as a result, data exchange between the server and the client start taking place. To exploit this, the one who attacks, sends a series of SYN messages to the user, or the victim, and as a result, the victim responds back with a SYN-ACK message and then it waits for some time for an ACK to come back to finish the connection establishment. Due to the fact that the attacker has sent the SYN messages with spoofed source address, there will not be any ACK return due to absence of such addresses. And, as a final result, the several partially opened connections fill the queue and memory buffers, and due to that, users will not be able to get services any time soon.

UDP-Flood Attack

The UDP-Flood occurs when two services CHARGEN (character generator) and ECHO of UDP protocol generate a technique through which the flood can be launched. It happens so that the attacker targets and overwhelms random ports on the host.

ICMP(v6)-Flood Attack

ICMP (v6)-based utility ping (Packet Internet Groper) uses a technique known as echo response mechanism. When conducting this attack, the attacker sends large amount of packets to the victim with different spoofed invalid source IP addresses.

Smurf Attack

This type of attack is similar to the ICMP (v6) flood attack because it uses the echo response mechanism of ICMP (v6). It is mentioned in [3], that in this attack, the attacker does a broadcast of packets with spoofed source IP address targeted to the victim. Because the packets are received by all the nodes within the network, each and every node responds back. Then, the victim's machine gets large amount of echo responses, and it gets exhausted.

C) Layer 7 Attacks

Incomplete HTTP requests using GET method

If we pay attention to what is written in [3], then this attack is based on how the client sends the data to the web server while communication goes on between them. In this attack, the client sends HTTP requests to the web server but in a different way. After sending multiple incomplete requests, the client exhausts the server's resources. As a result, these requests consume all the available resources on the server, thereby denying the legitimate users' requests.

Incomplete HTTP requests using post method

By [3], this type of attack is almost the same as the Incomplete HTTP requests using GET method. The thing that is different here is that the client himself is the one who is sending the incomplete HTTP requests with the aid of POST method and not GET.

HTTP requests using HEAD method

As it is referred to in [3], this attack, or HEAD method differs from the GET method only because while using HEAD method, while the server is giving the response, it must not include a message body. But, if it does include a message body, the process itself will save resources on the attacker's side which helps the attacker find out which page is more expensive for the server.

3. Approaching a DoS attack using change and risk management methods

The nature of the denial of service attacks, as mentioned in [4], lies in making the resources unavailable to the victim. It can be described as an attempt by the attackers to try and stop legitimate users of a computer service from using it. However, as any sort of information issue connected to network security, the fight against denial of service is some type of a training in risk and change management. In order to reduce the risk to its minimum, you must

be able to make right decisions at the right time, as well as technical decisions at critical times.

If we want to cope with the risks posed by denial of service, we would need a multi-pronged approach, recommended in [4]. This includes:

A) Make your business as robust as you possibly can so it can survive all the threats and attacks. This means that your business should be able to adapt and survive at all costs.
B) You need to commit yourself and your team on designing a line of defensive mechanisms, which will ensure that the services will continue to work despite an eventual attack or a failure.
C) In most countries people say that good things happen to good people, but that cannot refer to the "netizens". With other words, if you are a good netizen, it does not mean that you will not get attacked or your system will not fail. So, you need to brace yourself because the threat done to your network is proportional to the extent that a lot of attacks might follow in the future.

When speaking about this sort of network threat, we need to consider the finance or the money factor. This means that every lousy job may cost you a lot of finances, and on the other hand every well spent finances may get you more users and more profit.

If we look at some DoS attacks one time, we cannot see the clear picture. DoS attacks should be reviewed few times, then analyzed, and then you might get an idea of what the attack might be about. This means that there are hidden costs which are associated with this type of attack. For an example, as in [4], the direct target of DoS or DDoS attack may not be the only victim. So, the attack against one of the sites, can and might affect the network resources of several or all sites. This works the same with resources, when the resources you share with your parties are consumed, you will be left with no resources, and that is when you are left out with no service. If this happens to you, it means that you will have lag or increased network latency or packet loss, or it might even come to a full outage.

Fair amount of finances should be spent on the logging systems, because those are the systems that need to handle significant deviations when there is a big amount of data being logged during attacks.

It would be ideal, if logging systems used an out-of-band channel, just so that logging traffic would not add up to the DoS traffic and then passed to the network. If this comes to its culmination, then the next thing you know is having full mail queues and an incoming outage.

There are a lot of options to consider here, when referring to the defense mechanisms of a network system, since the source of the attack is always unknown. That is why we need to keep our systems up to date, and upgraded, in case anything happens. just so we and our data would be safe and sound.

4. Security spending example

Let's make a story worth telling here. You are an owner of a TV services provider, and its an IP TV company. You are located in Macedonia, and the budget to defend in this country against these types of attacks is $ 20,000. I know its not much, but if you were here, it would mean a lot for you due to the fact that an average salary in this country is $ 450 according to the Macedonian State Statistical Office. Just to be clear, this is your budget that should cover all your costs on staff, equipment etc. Going back to the story, in my opinion, this is how your organization should spend those funds:

Example 1

You will be obliged to excess the capacity just so you could absorb some attacks, then you must hire experienced staff, and at last, you must provide defensive network equipment. So this is how your expenditures should look like:

$4,000 extra bandwidth and router through put

$10,000 experienced, highly skilled staff

$6,000 firewall, load-balancing, traffic-shaping technology

This is not the only option though. You may consider changing anything in this illustration. According to [4], when deciding on your company's response to DoS attacks, consider these couple of questions: What are the chances of an attack hitting your company? What are the chances of an attack being of a certain type and/or magnitude? What level of risk is acceptable? How important is the Internet to your business? How long can you function without some or all Internet services? Which services you cannot function without?

Meaning that we would like to make a discussion out of these questions, it would probably turn out to be like the following.

Starting with the first one, or what are the possibilities of an attack on your company? The possibilities of getting a DoS attack vary on the popularity of your company. This means that if you are a low profit company or organization, you have nothing to worry about, or you probably will not be a target. On the other side, if you have lot of costumers and working personnel in your company it would mean that you have a lot of data stored in your base. Cracking that base would be a challenge for an attacker, because a lot of data leads to a lot of money.

Moving on to the second one, or what are the chances of the attack being a certain type or magnitude? This question can be answered similarly to the previous one. Basically, if you are a low-profile organization, the attack you might expect might cost few thousand dollars, and on the other hand, if you are a high-profile organization, the attack that penetrates your systems might cost you millions of dollars or even more.

The third one, or what is the level of risk that is acceptable? This is an issue regarding the staff on the top of the pile in the company. Those are the ones who should make the decisions and put the boundaries on which risks are and which risks are not acceptable. Of course, the answer of this question would be, any risk that can be mitigated, is acceptable.

The fourth one refers to the importance of the Internet to your business. As a thing that makes our lives easier with all the feeds and notifications on our screens that provide us with the information we need, one would say that the Internet has become a pretty important part of our lives.

Last but not least, how long can you function without Internet services? The answer of this question is simple. If your working position depends on Internet services, then you cannot function without them. However, if you can do your job while not being online and not needing any Internet services, then you can go back to the dark age and not bother with these things.

And the last one, what are the services you cannot function without? For me, personally, the wireless services are something that has changed everything in terms of technology. Everything you need or everything to want is on the palm on your hand – on your screen. Through our mobile devices and gadgets, we can do anything we want and the coolest thing is that we are not bonded by any wire or cable or any kind of physical transmission medium.

5. Conclusion

The purpose of this paper is to give the reader a work framework when facing a DoS attack while using change and risk management methods, which includes:

- Change and risk management in IT,
- Modern day network threats, and
- Approaching a DoS attack using change and risk management methods.

This work describes what you need to know when facing a DoS attack on any type of network. And by doing that, you will either prevent your network from getting attacked or mitigate the attack's impact that has already occurred.

Besides the change and risk management in IT, which provides us with essential information on how to cope with DoS attacks, in this work, you can find the most recent research done on DoS by Imperva Research Lab as well as an example on how you should spend a budged in order to have a safe and well protected network.

To conclude, the topics that this paper provides are the fundamental key elements in getting to know DoS attacks and security issues regarding them.

6. References

1. Byron J. Williams, Jeffrey Carver, Ray Vaughn, *Change Risk Assessment: Understanding Risks Involved in Changing Software Requirements*, (Department of Computer Science and Engineering, Mississippi State University, MS, USA, **2**, 2006).
2. Houssain Kettani, Polly Wainwright, *On the Top Threats to Cyber Systems*, (The Beacom College of Computer and Cyber Sciences, Dakota State University, S.Dak., USA; Department of Computing and Information Sciences, Valparaiso University, IN, USA, **2**-**4**, 2019).
3. Nikhil Tripathi, B.M. Mehtre, *DoS and DDoS Attacks: Impact, Analysis and Countermeasures, Institute for Development and Research in Banking Technology*, (Hyderabad, India, **2**-**5**, 2013).
4. Allen Householder, Art, Manion, Linda Pesante, George M. Weaver, *Managing the Threat of Denial-of-Service Attacks*, (Carnegie Mellon University, PA, USA, **1**-**4**, 2001).

Audio recording system for underwater monitoring with fast notification for detected sound anomaly

Nikolai Georgiev[1], Aleksandar Kolarov[1], Ilian Iliev[2]
[1] Bulgarian Academy of Sciences - Institute of metal science, equipment and technologies with Hidroaerodynamics centre "Acad. Angel Balevski", e-mails: niki0611@abv.bg, aleksandar_kolarov@abv.bg
[2] Naval Academy "N. Vaptsarov", Varna, Bulgaria e-mail: i.iliev@nvna.eu

Abstract: *To enforce the Republic of Bulgaria's "Maritime Spaces, Inland Waterways and Ports Act" and EC Decision 2010/477/EU is a need for an underwater monitoring system in the national maritime spaces. As an element of such a system, a prototype of a bottom-positioned modular system has been developed at IMS-BAS, designed for reading and recording and transmission of hydro physical, hydro chemical, biological and ecological data for the marine environment, sounds from biological sources and anthropogenic noises, registration and classification of a sound anomaly, a fragment of it is overwritten wirelessly in an autonomous radio beacon, which quickly floats and transmits the information to a base station on a radio channel, and then acts as a radio marker. One of the radio buoys is connected to the central airtight body by a rope wound on a spool. Its purpose is in case of technical problems or pre-programmed to float and signal on a radio channel. After lifting the station to the surface, the recorded information is taken off and maintained.*

Keywords*: SEL, SLP, underwater monitoring, anthropogenic noise, sound anomalies, radio buoy.*

1. Introduction

As a result of human activities in the marine environment, various types of fields are excited such as sound, light, electromagnetic, thermal, hydrodynamic, etc. Of all these fields, the sound field is distributed over the longest distances from the source. That is why great attention is paid to the assessment of the energy impact of sound waves on marine species. A harmful underwater sound field is one in which exposure causes temporary or permanent damage to the fauna of the marine ecosystem. In theory, when such a field is created as a result of human activity, it is referred to as harmful anthropogenic noise. Anthropogenic noise is recognized as a serious stress factor for most marine mammals, many marine fish, crustaceans and other marine organisms. The degree of noise impact depends onthe sound exposure level, which is abbreviated as .It is calculated according to the formula [1]:

$$SEL = 10 \left(\int_0^T \frac{p^2(t)}{p_o^2} dt \right) \ (\mathrm{dB/\mu Pa^2 s}), \quad (1)$$

where $p(t)$ the instantaneous value of the sound pressure in (μPa); p_o - relative pressure equal to 1 (μPa).

The degree of impact of anthropogenicyat noise on marine animals depends on its type. Two types of anthropogenic noise, pulsed (emission of pulsed sonar, explosions at seismic studies, etc.) and continuous (for example, noise from shipping, dredging and underwater power plants, etc.). To assess the impact of anthropogenic pulsed and low-frequency continuous sounds in the marine environment, as required by EC Decision 2010/477 / EC and the "Guide to the monitoring of underwater noise in European seas" under the Marine Strategy Framework Directive (RDMS) 2008/56 / EC, a "noise" register should be established, which will describe all human activities that generate pulsed and continuous noise in marine areas, which are carried out under regulated conditions and are licensed, as well as specialized research and military operations (if permissible). Noise emissions from ships will be included in the noise register. The creation of a "noise register" will help to determine the overall spatial and temporal scale of the spread of anthropogenic noise sources, as well as to establish the initial levels (baseline values) of the current state of the measured environment and trends in its change relative to these levels. The noise register will provide not only monitoring data, but also data for planning measures to reduce / prevent negative impacts on the marine environment [2,3,4].

2. Assumptions and ways to solve the problem

The planned measures in the Program of Measures to the Marine Strategy for Environmental Protection in the Sea Waters of the Republic of Bulgaria envisage the monitoring under indicator D11C1.1 in fulfillment of the requirements of the RDMS to be performed on the basis of the analysis of data and information to be collected in the national "noise" register. The register will describe all human activities that generate impulse sounds in the sea area of the Republic of Bulgaria. Data on noise emissions from different types of ships will be collected from ship manufacturers / owners or specialized information systems (eg national AIS system, etc.), as well as from measurements by underwater noise monitoring stations. Data and information on anthropogenic activities will be collected continuously throughout the year and the noise register will be periodically updated. The monitoring under indicator D11C2.1 will cover the coastal and shelf zone (up to 100 m depth), for which purpose 4 stationary autonomous hydrophone systems for underwater noise measurement will be used, located in areas of high and low intensity of navigation, and areas of Nature 2000, which cover the most probable habitats of marine animal species. Due to the small number of hydrophone systems, their location will change monthly (subject to the above conditions) to cover the whole assessment area. Measurements of the noise level in the marine environment will be performed continuously throughout the year. Seasonal measurements will also be performed with a mobile hydrophone system. In parallel with the acoustic observations, the hydrological parameters of the aquatic environment will be measured: temperature, salinity and speed of sound [14]. In addition to legally regulated activities that create anthropogenic noise in marine areas, short-term sound anomalies are possible, such as the sound of leaking gas in the event of a pipeline breach, or an uncharacteristic level of anthropogenic noise in protected or prohibited areas and water activities, noise from the use of bottom trawls for fishing, etc., which may cause significant harmful effects. Their timely registration and response to the authorities authorized by law can significantly reduce the harmful consequences.

3. Solution to the studied problem

As an element of an underwater monitoring system in the national marine areas, IMS-BAS has developed a prototype of "Audio recording system for underwater monitoring with rapid notification of detected sound anomaly" /ARSUM/, designed for recording, classification and recording of sounds from biological sources (marine mammals, fish, shrimp, etc.), anthropogenic noise - pulsed (as a result of seismic surveys, laying pylons for wind farms and platforms on the seabed, use of pulsed sonar, underwater communications, underwater explosions, etc.) or long-term (caused by shipping, dredging, leaks in underwater gas and oil pipelines, actions of power plants, acoustic signals from artificial radiation, etc.) [5,6]. The main elements of the system are shown in Fig. 1:

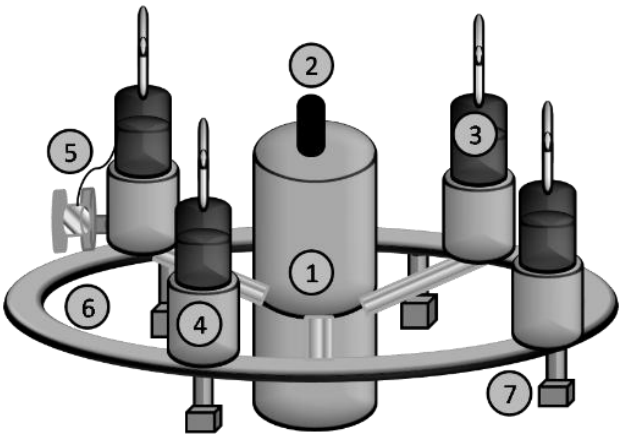


Fig.1 *Basic elements of ARSUM*

where: 1 - The central airtight body;
2 - Receiving hydrophone;
3 - Radio buoy with positive buoyancy;
4 - Socket for radio beacon with electromagnetic locks;
5 - Reel with rope attached to the emergency beacon;
6 - Hermetic ring for the cable connection between the sockets and the central body;
7 - Legs of the supporting structure for stable positioning of the bottom.

When detecting, recording and classifying a sound anomaly (eg sound of a leaking gas in the event of a pipeline breakage, noise from the use of bottom trawls for fishing or an uncharacteristic level of anthropogenic noise in protected or prohibited areas and for certain activities in the water area and etc.) a fragment of the information is recorded, with a duration sufficient for the classification of the event [7]. This fragment is transmitted wirelessly in an autonomous beacon from the device kit, where it is overwritten. Upon completion of the information transfer process, the radio beacon floats and transmits the critical information via radio to a shore, ship or air base station acting as an operations center. It is then used as a radio beacon to indicate the location of the event. One of the radio buoys is connected by a rope wound on a spool to the supporting structure. Its purpose is for technical problems related to breach of the seal, depletion of battery capacity and more. programmed to float and signal on a radio channel for the occurrence of the undesirable event in the base station. After lifting the station to the surface, the information stored in it is taken off and maintained [8].

4. Results and discussion

The main electronic modules in the composition of ARSUM perform the following functions:

• Reception and digitalization of underwater acoustic broadband signal and determination of the sea noise level;

• General detection of underwater acoustic broadband signal above the threshold level and production of control signals;

• Classification of the signal after the general detection and production of control signals;

• Recording at general detection of underwater acoustic broadband signal;

• Transmission / reception of data for a signal representing a sound anomaly after classification of the detected underwater acoustic broadband signal.

The functional diagram of the ARSUM hydroacoustic channel for detection and classification of objects according to their own noise with possibilities for recording the noises from the general detection and classification of SD cards and transmitting the file for the classified purpose by radio channel in analysis center is shown in Fig. 2.

Arduino microprocessor platform was chosen for the implementation of the channel, whose modules and software are available, while providing the minimum requirements in terms of speed and own noise [9].

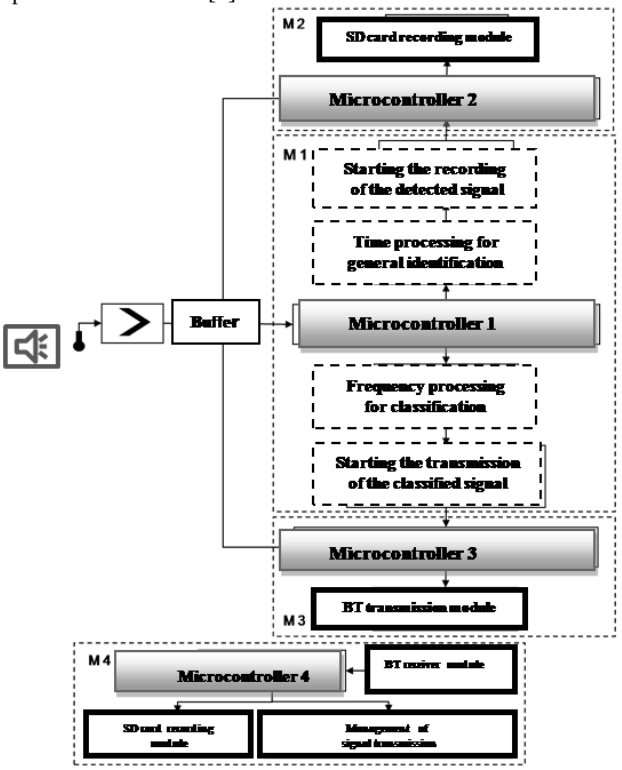


Fig.2 *The functional diagram of a prototype of the hydro acoustic channel of ARSUM*

The microcontrollers of this series operate with a frequency of up to 84 MHz, allowing the input of an analog signal with LSB up to 0.8 (mV) and a sampling rate of up to 70 kHz, which is sufficient for processing acoustic signals with a frequency spectrum up to 35 kHz. In addition to the analog inputs, the microcontrollers have a built-in analog output, programmable digital inputs/outputs and support the communication standards USB, SPI, CAN and I2C (TWI), as well as the network Ethernet standard. These characteristics of the platform allowed on its basis to realize an acoustic reception channel with cyclic signal input and processing through a built-in software DSP processor.

The diagram shows the functional connection between the individual modules of the hydroacoustic channel and the operations performed by them on the received signal. The buffer circuit is used to match the output of the amplifier with the ADC inputs of microcontrollers 1, 2 and 3, as well as to disconnect the three inputs.

The M1 module is designed to receive and process a broadband hydro acoustic signal with the ability to control external devices. It is designed to detect and classify a broadband hydro acoustic signal in the frequency band from 100 Hz to 8 kHz. The analog part of the module includes a hydrophone with a frequency band of reception in the specified range and a preamplifier with a band pass filter. The digital part of the module is realized on microcontroller 1, where after digitization of the analog hydro acoustic signal signal processing is performed in the time and frequency domains. The processing in the time domain is performed by the method of broadband detection and after fixing the moment of detection the process of recording the detected signal is started. The signal is digitized at a frequency of up to 70 kHz with a resolution of 12 bit. The detection is performed by averaging the signal strength in a crawling window and comparing the obtained values with a dynamically changing threshold [10,11]. The dynamic threshold is obtained on the basis of previous statistics of the instantaneous values of the signal power, their averaging in the window of selected length and their multiplication by a factor taking into account the level of false alarm. Detection is fixed when the signal level in the current window exceeds the dynamic threshold level.

The end of the recording is determined by the average time the target stays in the observation area of the sensor. The classification of the broadband hydroacoustic signal is performed in the frequency band from 100 Hz to 8 kHz on open discrete frequencies of special interest. To solve this problem in microcontroller 1, the signal is transformed into the frequency domain by FFT [12,13]. The signal is digitized at a frequency of up to 80 kHz with a resolution of 12 bit, and its conversion in the frequency range is performed by 256-point window FFT. The selected ADC and FFT conversion parameters allow narrowband signal processing in 156 Hz bandwidths. After fixing the presence of a certain discrete component in the broadband signal, the module starts the module for transmitting the signal via VT to the module for recording and transmission to the Analysis Center.

The module 2 is designed to record the hydroacoustic noise signal detected during broadband detection. For this purpose, a second microcontroller is used, which digitizes and records the data in audio format. The recording is started and stopped by a command from microcontroller 1. The sampling frequency for recording is 18 kHz with a resolution of 12 bit. The information for each detected signal is recorded in consecutive files.

Module 3 serves to transmit the classified hydroacoustic signal via BT. It includes a microcontroller 3, which digitizes the signal and controls the transmission of data over a built-in VT network, and a unit for transmission via VT. The VT circuit is programmed to work in "Master" mode, which ensures the construction of a VT network. The start and stop of the transmission is performed by a command from microcontroller 1 after classification. The sampling frequency of the transmitted classification signal is 18 kHz with a resolution of 12 bit.

The module 4 is designed to receive the classified signal on VT. Includes microcontroller 4, BT reception circuit operating in slave mode and SD card recording circuit. The reception and recording of the data is performed automatically after the data starts to be transmitted by the module 3. In addition to the control functions of the connection and recording circuits, the microcontroller 4 controls the floating processes and the radio transmission of the data to the analysis center.

The technical implementation of the main elements of ARSUM is shown in the following figures:

- Radio beacon (Fig 3):

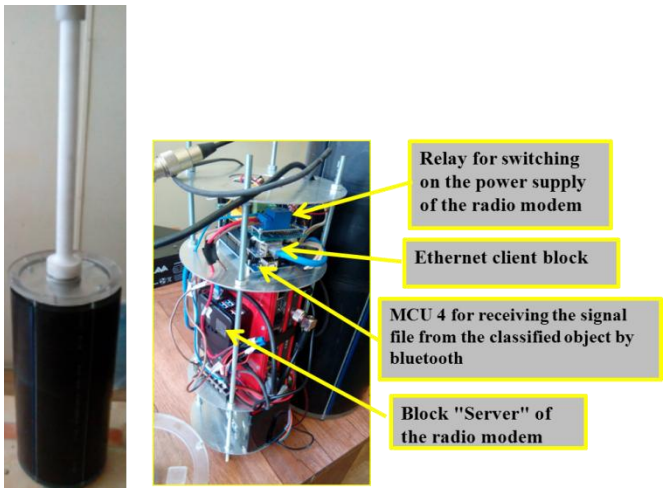


Fig. 3 *Construction of an experimental sample of a radio beacon.*

The buoy bottom made of transparent material provides an opportunity for BT communication and for activating the light relay for connecting the power to the radio modem and the server to it, MCU 4, GPS and the SD card recording scheme.

- Central airtight body (Fig 4):

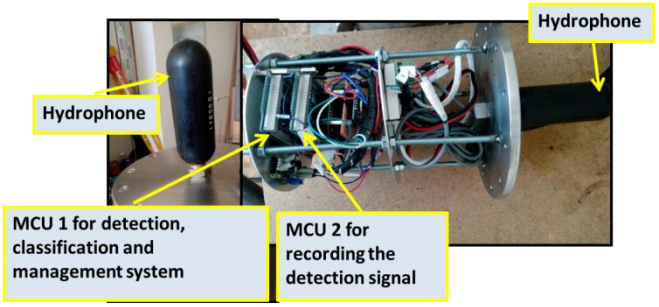


Fig. 4 *Construction of an experimental sample of the central hermetic body*

- Radio buoy socket with electromagnetic locks (Fig. 5):

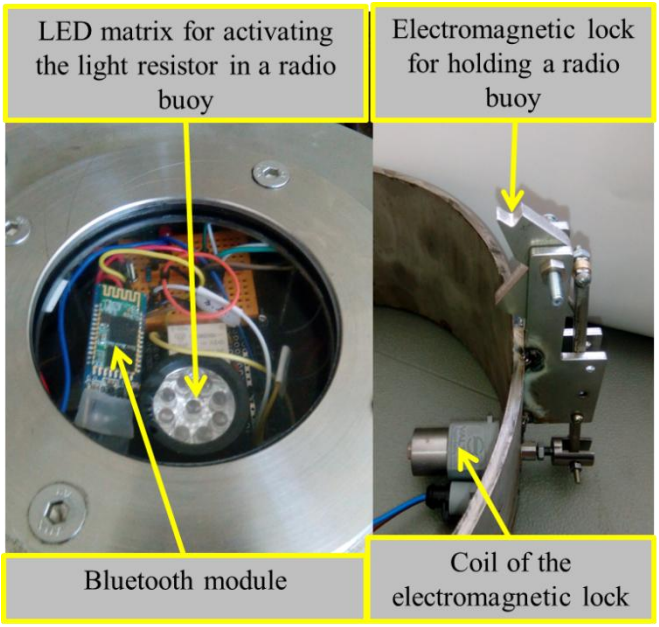


Fig. *5* *Construction of the radio beacon socket*

- General configuration of ARSUM (Fig. 6):

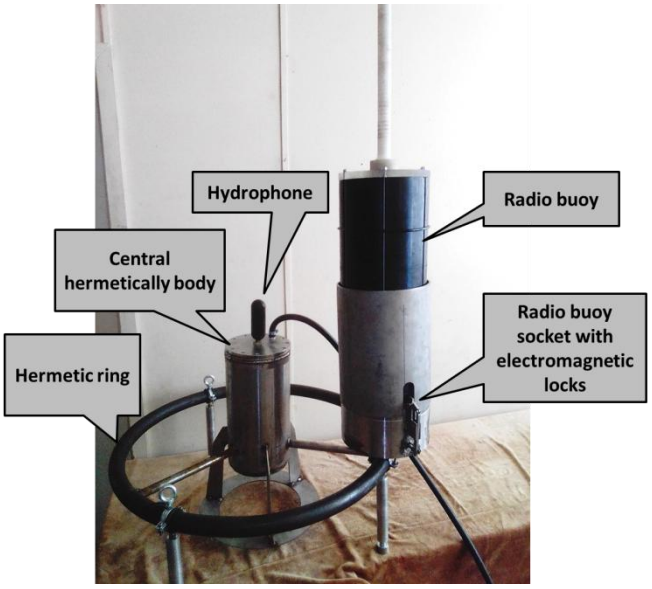


Fig. 6 *General configuration of an experimental sample of ARSUM*

In Fig. 7 and Fig. 8, the amplitude and spectrum, respectively, show the correspondence between the signal before broadcasting via Bluetooth channel (in black) and there after (in blue):

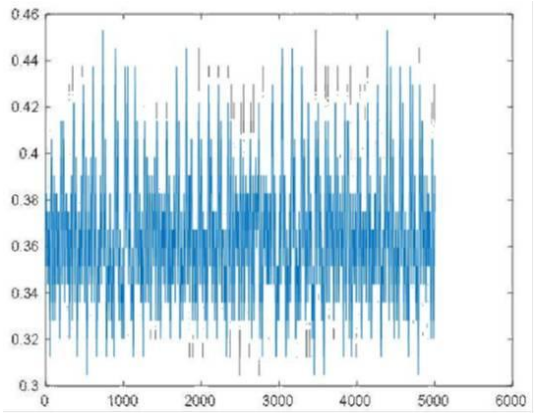


Fig. *7.* *The correspondence between the amplitudes of the audio signal before and after translation*

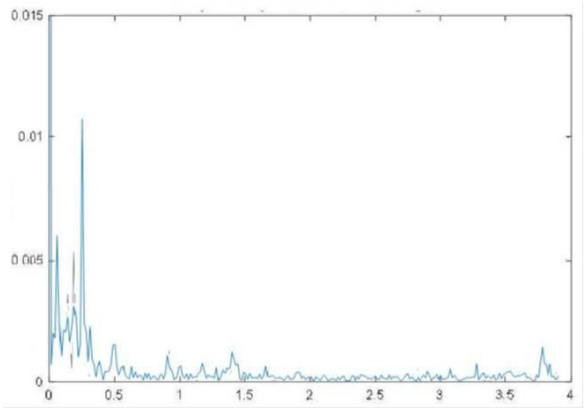


Fig. 8 *The correspondence between the spectrum of the audio signal before and after translation*

It can seen that the correspondence between the signals before and after the translation by Bluetooth channel in amplitude was 97% ÷ 98%, on the distribution of the frequency spectrum than 99%. This means that the attenuation and distortionof the signal is up to 3%, which is practically negligible.

5. Conclusion

The prototype developed at the institute is "Audio recording system for underwater monitoring with rapid notification of detected sound anomaly" /ARSUM/, provides registration, classification and recording of sounds from biological sources (marine mammals, fish, shrimp, etc.), anthropogenic noise - pulsed (as a result of seismic underwater phenomena, seismic surveys, laying of pylons for wind farms and seabed platforms, pulsed sonar or communication means, explosions, etc.) or long-term (caused by shipping, dredging, leaks in underwater gas and oil pipelines, actions of power installations, acoustic signals from artificial radiating means, etc.) of ARSUM allow the full provision of information on all human activities that generate pulsed and continuous noise in marine areas, which are carried out under regulated conditions and are licensed, as well as specialized research and military operations (if permissible), as well as noise emissions from ships for the establishment of a "noise register", in accordance with the requirements of EC Decision 2010/477 / EC and "Guidelines for monitoring underwater noise in European seas according to the RDMS". In addition, upon detection, registration and classification of sound anomaly or uncharacteristic level of anthropogenic noise in protected or prohibited for navigation and for certain activities areas of the water area, a recorded fragment of information wirelessly in an autonomous radio beacon is transmitted to the Analysis Center, which responds in an appropriate manner.

6. Acknowledgements:

The results can also 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. 1. I. Iliev, "Hydroacoustic Measurements", “Nikola Vaptsarov Naval Academy”, Varna, 2016, ISBN 978-954-8991-84-1
2. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat I, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36341-2
3. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat II, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36339-9
4. MSFD Technical Subgroup on Underwater Noise, „Monitoring guidance for underwater noise in European sea”, Prat III, Luxembourg: Publications Office of the European Union, 2014, ISBN 978-92-79-36340-5
5. M. Todorov, On the models of interaction of dug pipelines, International Conference UACEG 2009, October 29-31, 2009, ISSN 1310-814X;
6. Ilov G., Germanov T., Zhelev J., Kirov B., Denev D., Mihova L., Varbanov R., Totsev A., Todorov M., Ivanov Iv., "Guide to Geotechnics", Eurocode 7, KIIP , 2011, ISBN 978-954-92275-8-1;
7. M. Todorov, “Cyclic Soils Properties”, Seventh Iinternational Structural Engineering and Construction (ISEC-7), Hawaii, June 18—23, 2013, ISBN-10: 981-07-5354-2;
8. Miroslav Todorov, Vladimir Kostov, Earth Mechanics, First Edition - 2015, ISBN 978-954-724-081-0;
9. Vladimir Kostov, Miroslav Todorov, FOUNDATION, First Edition - 2015, ISBN 978-954-724-082-7;
10. M. Todorov, „Problems in reconstruction of pile-raft foundation“, EURO-MED-SEC-1, The First European and Mediterranean Structural Engineering and Construction Conference, Istanbul, Turkey, 05.2016, ISSN: 2644-108X, ISBN: 978-0-9960437-2-4, http://doi.org/10.14455/ISEC.res.2016.42;
11. M. Todorov, “Non-Cracking Techniques For Grouting”, International Structural Engineering and Construction Conference in the beautiful and historic harbor, ISEC9, city of Valencia, Spain, July 24-29, 2017, ISBN 978-0-9960437-4-8, doi: 10.14455/ISEC.res.2017.80
12. Miroslav Todorov, Durability and deformations of geotechnical systems, ISBN 978-619-91513-1-0, 2020;
13. Miroslav Todorov, Peculiarities of the model of interaction of dug pipelines and soil massif, ISBN 978-619-91513-0-3, 2020;
14. 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;

World Radiocommunication Conference WRC'19 - Impact over security of the modern human society

Veselin Demirev.
Technical University-Sofia, Bulgaria
E-mail: demirev_v@tu-sofia.bg

Abstract: *ITU's World Radiocommunication Conference 2019 (WRC 19) is playing a key role in shaping the technical and regulatory framework for the provision of Radiocommunication services in all countries, in space, air, at sea and on land. It will help accelerate progress towards meeting the Sustainable Development Goals (SDGs). It is providing a solid foundation to support a variety of emerging technologies that are set to revolutionize the digital economy, including the use of artificial intelligence, big data, the Internet of Things (IoT) and cloud services. The last items are very close related to the security of the modern human society. The importance of the WRC,19 decisions is discussed in the report. Two new radio-communication principles, named Spatial Correlation Processing - Random Phase Spread Coding (SCP-RPSC), are analysed from WRC, 19 decisions point of view. They were proposed by the author a decade before as antenna transmit-receive beam forming methods with many applications in microwave frequency bands.*
Keywords*: WRC-19; 5-G; IMT; IoT; SMART CITIES; SCP-RPSC*

1. Introduction

ITU's World Radiocommunication Conference 2019 (WRC 19) is playing a key role in shaping the technical and regulatory framework for the provision of Radiocommunication services in all countries, in space, air, at sea and on land [1]. It will help accelerate progress towards meeting the Sustainable Development Goals (SDGs). It is providing a solid foundation to support a variety of emerging technologies that are set to revolutionize the digital economy, including the use of artificial intelligence, big data, the Internet of Things (IoT) and cloud services. The last items are very close related to the security of the modern human society.

Every three to four years the conference revises the Radio Regulations (RR), the only international treaty governing the use of the radio-frequency spectrum and satellite orbit resources. The treaty's provisions regulate the use of telecommunication services and, where necessary, also regulate new applications of Radiocommunication technologies. The aim of the regulation is to facilitate equitable access and rational use of the limited natural resources of the radio-frequency spectrum and the satellite orbits, and to enable the efficient and effective operation of all Radiocommunication services.

Each World Radiocommunication Conference affects the future development of information and communication technologies (ICTs) in many ways, including:

- Introducing and expanding access to the radio spectrum for new Radiocommunication systems and applications;
- Protecting the operation of existing Radiocommunication services and providing the stable and predictable regulatory environment needed for future investments;
- Avoiding the potential for harmful interference between radio services;
- Allowing the provision of high-quality Radiocommunication while protecting vital uses of the radio spectrum, particularly for distress and safety communications;
- Facilitating international roaming and increasing economies of scale, thereby making it possible for network and user devices to be more affordable.

The importance of the WRC,19 decisions over the future security of the modern human society is discussed in the report. Two new radio-communication principles, named Spatial Correlation Processing - Random Phase Spread Coding (SCP-RPSC), are analyzed from WRC,19 decisions point of view. They were proposed by the author a decade before as antenna transmit-receive beam forming methods with many applications in microwave frequency bands.

2. WRC-19 activity and decisions

2.1. Introduction

WRC 19 was held in Sharm El-Sheikh, Egypt, from 28 October to 22 November 2019. A record 3400 participants attended WRC-19, including delegates from most of the 193 ITU Member States as well as more than 260 members of the ITU Radiocommunication Sector (ITU-R) representing international organizations, equipment manufacturers, network operators and industry forums, who attended as observers. Its agenda covered a wide range of Radiocommunication services and activities, dealing with security of the modern human society.

2.2. Deployment of non-geostationary satellite (NGSO) systems in specific radio-frequency bands and services

The agreement reached at WRC-19 establishes regulatory procedures for the deployment of NGSOs, including mega-constellations in low-Earth orbit. The agreement struck in Sharm el-Sheikh reflects the rapid pace of satellite innovation that is driving an increase in the deployment of non-GSO constellations. Indeed, with the availability of launch vehicles capable of supporting multiple satellite launches, mega-constellations consisting of hundreds to thousands of spacecraft are becoming a popular solution for global telecommunications. This includes extensive low-latency broadband coverage, remote sensing, space and upper atmosphere research, meteorology, astronomy, technology demonstration and education, close related to human security.

2.3. International agreements that will help pave the way for better smart-city transportation

The agreements at ITU's WRC-19 aim to improve traffic management, public transportation systems, road safety, train safety and railway traffic control – among other aspects of transportation that aim to leverage information and communication technologies (ICTs) to make the world's cities safer and smarter. Specifically, delegates representing governments from across the world have approved a new Recommendation on Intelligent Transport Systems (ITS) and a new Resolution on railway Radiocommunication systems between train and trackside (RSTT).

2.4. Additional radio-frequency bands for High Altitude Platform Station (HAPS) systems

These easily deployable stations operating in the stratosphere (layer of the Earth's atmosphere starting at 20 kilometers) are high enough to provide service to a large area or to augment the capacity of other broadband service providers. Technological innovations in recent years — and the growing urgency to expand the availability of broadband – led to the development of HAPS systems. The

agreements reached at WRC-19 help pave the way to connect more of the world's people to the benefits of today's digital economy, particularly in underserved communities and in rural and remote areas. A new Resolution passed at WRC-19 also mentioned that "current technologies, such as HAPS, can be used to deliver broadband applications for broadband connectivity and disaster-recovery communications with minimal ground network infrastructure". HAPS systems can be used to provide both fixed broadband connectivity for end users and transmission links between the mobile and core networks for backhauling traffic. Both types of HAPS applications would enable wireless broadband deployment in remote areas, including in mountainous, coastal and desert areas.

Delegates at WRC-19 agreed that allocations to the fixed service in the frequency bands 31-31.3 GHz, 38-39.5 GHz will be identified for worldwide use by HAPS. They also confirmed the existing worldwide identifications for HAPS in the bands 47.2 – 47.5 GHz and 47.9 – 48.2 GHz are available for worldwide use by administrations wishing to implement high-altitude platform stations. They agreed to the use of the frequency bands 21.4-22 GHz and 24.25-27.5 GHz by HAPS in the fixed service in Region 2.

2.5. The deployment of Earth stations in motion (ESIM)

Earth stations in motion (ESIM) address a complex challenge: how to provide reliable and high-bandwidth Internet services to moving targets. They provide broadband communications, including Internet connectivity, on platforms in motion.

There are currently three types of ESIM: ESIM on aircraft (aeronautical ESIM), ESIM on ships (maritime ESIM) and ESIM on land vehicles (land ESIM). They connect people on ships, aircraft and land vehicles and ensuring their safety, security and comfort on the move. Advances in satellite manufacturing and earth station technology have made ESIM more readily available and more practical. When ships are at sea or aircraft cross the oceans, they are out of reach of terrestrial networks. ESIM systems can provide continuous and consistent service with very wide, or literally global, geographic coverage as ships and aircraft operate at or over almost any location. In addition, the typical data rates currently provided by terminals operating in networks serving ESIM are around 100 Mbit/s. That is much higher, or faster, than those provided historically by mobile-satellite service (MSS).

To address the increasing need for radio-frequency spectrum for ESIM, while protecting other services, delegates at WRC-19 decided on the regulatory and technical conditions under which the frequency bands 17.7 19.7 GHz (space-to-Earth) and 27.5-29.5 GHz (Earth-to-space) can be used by the three types of ESIM communicating with geostationary (GSO) space stations in the fixed-satellite service (FSS).

2.6. Identification additional radio-frequency bands for International Mobile Telecommunications (IMT), which will facilitate the development of fifth-generation (5G) mobile networks

5G is expected to connect people, things, data, applications, transport systems and cities in smart, networked communication environments [2]. It will transport a huge amount of data much faster, reliably connect an extremely large number of devices and process very high volumes of data with minimal delay.

5G technologies are expected to support applications such as smart homes and buildings, smart cities, 3D video, work and play in the cloud, remote medical services, virtual and augmented reality, and massive machine-to-machine communications for industry automation. 3G and 4G networks currently face challenges in supporting these services. These new functionalities and new services necessitate a new way of deploying advanced mobile services, as well as new approaches in making 5G technologies work together in industrial settings by machine-to-machine communications, Internet of Things (IoT) or with connected vehicles.

While identifying the frequency bands 24.25-27.5 GHz, 37-43.5 GHz, 45.5-47 GHz, 47.2-48.2 and 66-71 GHz for the deployment of 5G networks, WRC-19 also took measures to ensure an appropriate protection of the Earth Exploration Satellite Services, including meteorological and other passive services in adjacent bands.

In total, 17.25 GHz of spectrum has been identified for IMT by the Conference, in comparison with 1.9 GHz of bandwidth available before WRC-19. Out of this number, 14.75 GHz of spectrum has been harmonized worldwide, reaching 85% of global harmonization.

In addition, WRC-19 has also defined a plan of studies to identify frequencies for new components of 5G. As an example, to facilitate mobile connectivity by High Altitude IMT Base Stations (HIBS). HIBS may be used as a part of terrestrial IMT networks to provide mobile connectivity in underserved areas where it is difficult to be covered by ground-based IMT base stations at a reasonable cost.

IMT-2020, the name used in ITU for the standards of 5G, is expected to continue to be developed from 2020 onwards, with 5G trials and commercial activities already underway to assist in evaluating the candidate technologies and frequency bands that may be used for this purpose. The first full-scale commercial deployments for 5G are expected sometime after IMT-2020 specifications are in force.

3. SCP-RPSC approach

3.1. Introduction

SCP-RPSC (Spatial Correlation Processing – Random Phase Spread Coding) is an entirely new approach in the field of microwave beam forming antenna theory. It was developed by the author before more decade [3,4,5,6]. The goal was to solve the problems of the tracking microwave antenna systems for mobile satellite communications.

3.2. SCP technology

The main objectives of the SCP technology [3,4,5,7] are:

- To receive one or more radio signals coming from one or several spatially distributed signal sources (satellites, base stations), insuring high gain of the antenna systems and using fixed or mobile receiving terminals, equipped with SCP signal processing equipment;
- To ensure spatial selectivity high enough to cancel the same frequency channel interference, coming from different space directions, using simple one channel receiver.

The objectives stated above are achieved by a patented by the author method for radio communications, which proposes application of additional pilot signal transmitted in the band of information signals and available in the receiver by Code Division Multiple Access (CDMA). The SCP receiver terminal is equipped with antenna array with random phase aperture excitation. The phase shifts among the signals, coming from the antenna elements, are random at the antenna output, regardless of the information source direction. These random phase spread signals correlate with the recovered pilot signal, phase spread in the same manner, in a signal recovery unit. The result of the correlation process between pilot and information signals is the recovered information signal at base band.

The main features of the SCP approach are:

- Simple, cheap and flat passive antenna, suitable for mass production even in mm-Wave frequency bands;

- One channel convenient microwave receiver with simple signal processing;
- Omni directional for the cooperative signal source, but with high Figure of Merit G/T;
- Selection of the different signal sources and polarizations by PN-codes;
- Multi-beam and soft handover features.

3.3. RPSC technology

The RPSC technology was proposed and patented by the author too [6]. It is based on transmission of broadband microwave signals in the open space by means of multi element random phased antenna arrays. The sum of the different element signals in a given point in the space has Gaussian probability distribution and noise like properties. The sums in the different directions of the space are not correlated each other. In such way the proposed principle solves simultaneous the problems of spreading and beam forming.

The main features of the RPSC technology, when it is used in the up-links of the wireless communication links, additionally include:

- Omni-directivity for the cooperative receiving terminal, but high equivalent (at base-band) Equivalent Isotropic Radiated Power (EIRP);
- Selection of different terminals and polarizations by Pseudo-Noise (PN) codes;
- Soft handover and virtual multi-beam features;
- The coherent demodulation by means of pilots (specific property of SCP technology), cancelling the Doppler shift and the phase jitter, introduced by local oscillators in the wireless communication system;
- RPSC up-link protection against terrorist jamming, coming even from points, close situated to the transmitting stations;
- The knowledge of the receiving terminal positions for the transmitting equipment is not necessary;
- The SCP-RPSC approach is a breakthrough technology, leading to unpredictable increase of the frequency reuse factor in the wireless broadband networks. Close situated subscriber terminals could communicate with base stations, using the same frequency channel without interference. The isolation between the terminals is provided by their specific random phase spread coding, aiming to RPSC-MA (Multiple Access).

All of the listed above new Radiocommunication technologies, subjects of the WRC-19 activity, are planned for centimetre and millimetre microwave frequency bands. SCP-RPSC principles and technologies could be successfully used there in order to improve the parameters of the future communication technologies and networks. May be the most important benefit will be transition from “shaped beam” to “steerable beam” mobile networks without complex and expensive electronically scanned multi-beam antenna arrays.

4. Conclusion

The practical SCP-RPSC technology implementation as antenna beam-forming and pattern diversity approach in the future wireless fixed and mobile Radiocommunication systems, subject of the WRC-19 activity, will drastically change the existing paradigm in the broadband terrestrial, HAPS and satellite communication systems in general. Many of the existing problems, dealing with frequency reuse, orbital positions, narrow antenna beam pointing, pattern diversity, terrorist jamming, etc. will be solved successfully. The results of the 25 years long author research activity will be a very strong Bulgarian contribution for the improvement of the security of the modern human society.

5. References

1. Managing spectrum for evolving technologies, ITU News Magazine, N 5, 2019.
2. Johnson, M., - "5G, Opening a new era of digital economy", Sixth Wuzhen World Internet Conference, 21, October 2019 - Wuzhen, China.
3. Demirev, V., “Spatial Correlation Processing – the New Approach in the Broadband Satellite Tracking Systems”, Journal of Electrical and Control Engineering, Volume 3, Issue 5, pp. 49-54, October, 2013.
4. Demirev, V., “Some Important Parameters of the Spatial Correlation Processing Technology “, Journal of Electrical and Control Engineering, Volume 3, Issue 5, pp. 55-64, October, 2013.
5. Demirev, V., “Recent Trends and Future Developments of Vehicle Mounted Satellite Tracking Communication Systems“,CEMA,13, Sofia, pp. 66-69, October, 2013.
6. Demirev, V., “Random Phase Spread Coding – the New Way to Communicate with Noise Signals at Microwaves“, Journal of Electrical and Control Engineering, Volume 4, Issue 2, pp. 1-9, April, 2014.
7. Demirev, V., “Space diversity – essential factor for the security of 5-th G communications”, International Scientific Conference “ConfSec,18”, Borovets, 2018; Security & Future, N 2, pp.72-75, 2018.

Investigation of characteristics of cylindrical piezoceramic transducers used in systems for underwater monitoring and management

Ivan Ivanov[1], Stojan Kolev[1], Bistra Nenova[1], Vassil Kossev[2]
1 - ivo1942@abv.bg; 2 - s_kolev@abv.bg; 3 - bistranenova@hotmail.com; 4 – backomail@yahoo.com
1 - IMSETHC-BAS, Sofia, Bulgaria; 2- Accenture Bulgaria, Sofia, Bulgaria.

Abstract: *The frequency characteristics of hydroacoustic cylindrical piezoceramic transducers in transmission and reception modes have been determined. The measurements were performed in pulse mode in a pool measuring 200x20x6 meters. The processed results from the measurements of the main characteristics are shown with tables and graphs.*

Keywords*: UNDERWATER ACOUSTIC CYLINDRICAL PIEZOCERAMIC TRANSDUCERS***.**

1. Introduction

For the study and development of the underwater space in most cases the specific features of the propagation of hydroacoustic signals in the aquatic environment are used [1].

2. Experiments and results

In the control systems of objects in the underwater space, undirected (circular) radiation and reception of hydroacoustic signals in the horizontal plane is required. This is realized through the use of cylindrical hydroacoustic antennas constructed on the basis of cylindrical piezoceramic elements.

Effective underwater monitoring is realized by electronic scanning of diagrams with well-defined orientation in the horizontal and vertical planes. This is ensured by multi-element hydroacoustic antennas with a cylindrical active surface.

A study of cylindrical hydroacoustic antennas constructed on the basis of cylindrical piezoceramic elements with outer diameters: 19mm, 28mm, 42mm and 54mm from left to right (Fig. 1) and a multi-element module for hydroacoustic antenna with a cylindrical active surface (Fig.4). The cylindrical antenna based on a piezoceramic cylinder with an outer diameter of 28 mm is shown in the form before hermetically sealed.

The measurements were performed in the deep-water basin of the Center for Hydro and Aerodynamics at IMSTCA-BAS. On the Fig.2 shows the schematic diagram of the measurement process used to measure the antennas. Measuring instruments from the company Bruel§Kjær are mainly used, namely: frequency generator type 1013, gating system type 4440, measuring hydrophones type 8100 and type 8101. The signals are monitored on the oscilloscope screen.

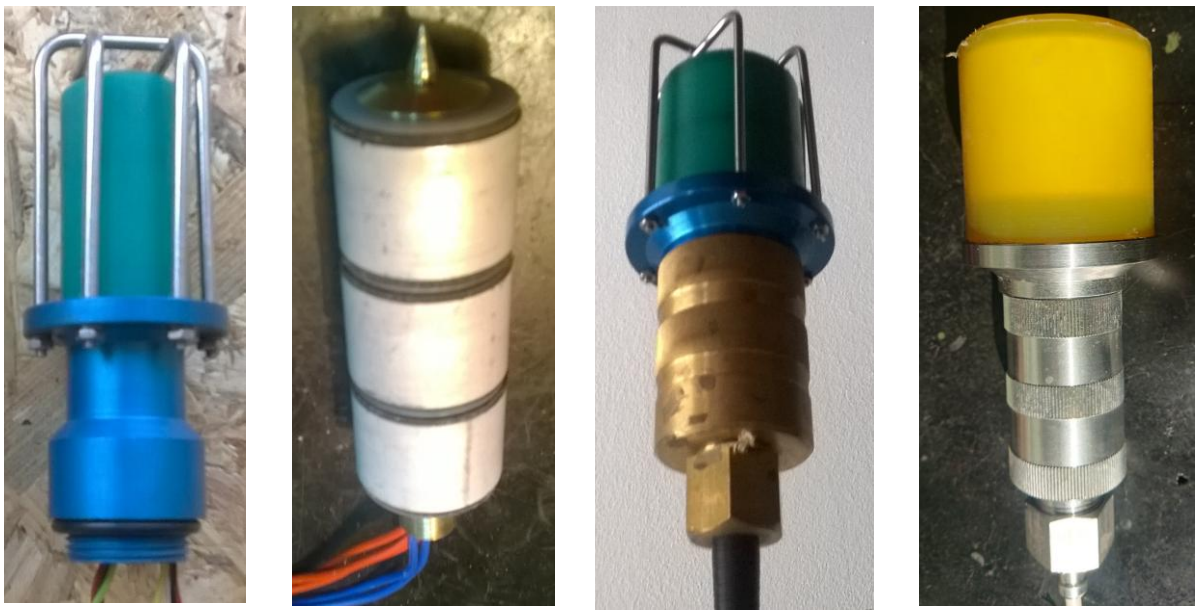


Fig.1. *The studied cylindrical underwater acoustic antennas*

During the measurements, to determine the characteristics of the tested antennas in radiation mode, the antennas and the hydrophone type 8101 are immersed at a depth of 3m and at a distance of 3m between them.

Both hydrophones used to determine the characteristics of the tested antennas in reception mode are from the company Bruel§Kjær.The tested antenna and the hydrophone type 8101 are located at a distance of about 1m from each other and at a depth of 3m. The type 8100 hydrophone is used for broadcasting and is located 3m from the imaginary line connecting the tested antenna and the receiving hydrophone tin 8101 also at a depth of 3m.

The shape of the signals is observed on the screen of the oscilloscope, and their current values are read by the measuring amplifier type 2607. The measurements use pulses with a duration of 2ms, where there is no overlap between the direct and reflected pulses.

In all measurements, the transmitter is excited with a peak voltage of 8V. Figure 3 shows the graphs of the frequency characteristics of the tested antennas. The different level of radiation of the resonant frequencies of the antennas is a result of their characteristics of directivity in the vertical plane (left graphs). The decrease in their sensitivity in the reception mode is due to their smaller receiving surface.

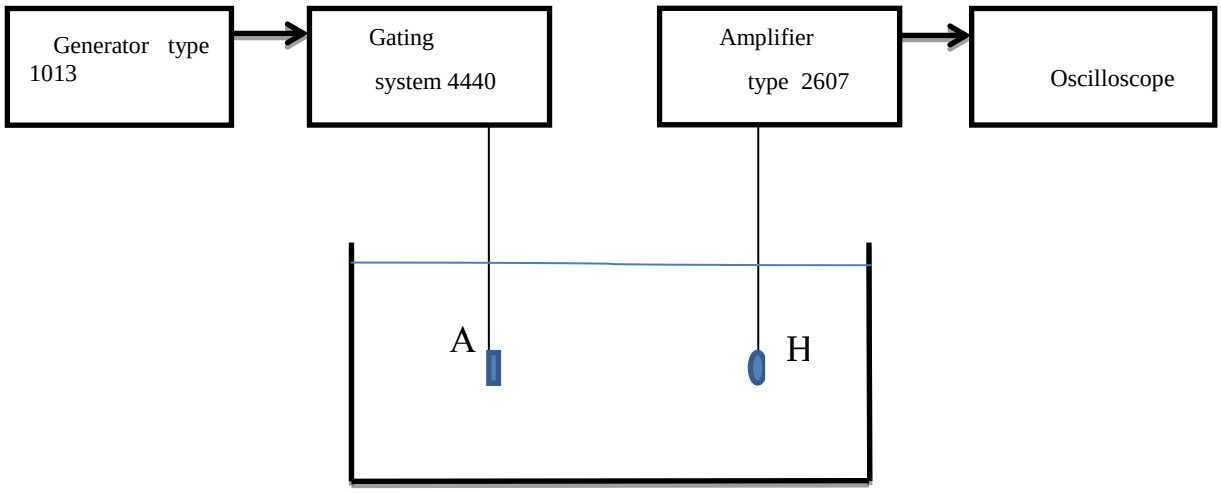


Fig.2. *Schematic diagram of the measurement process*

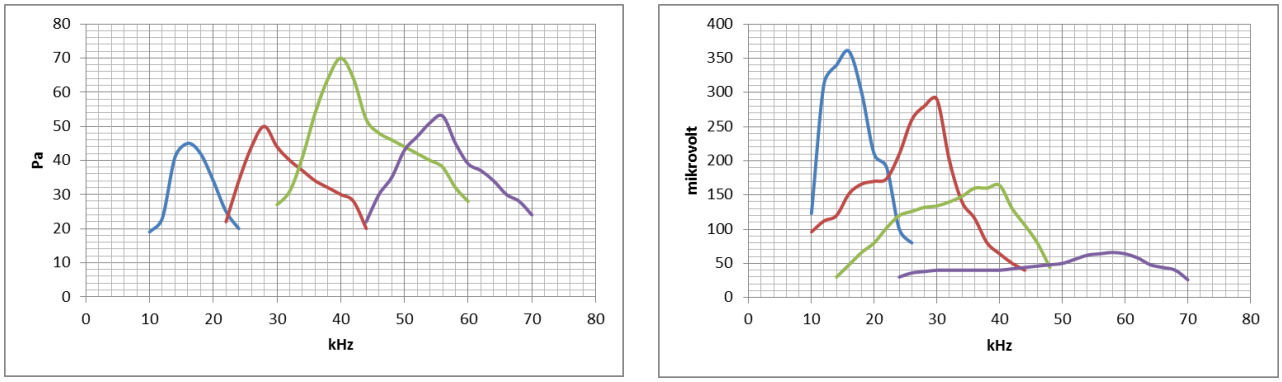


Fig.3. *Frequency characteristics of the antennas - on the left in broadcasting mode, on the right in receiving mode: blue - diameter 54mm, red - 42mm, green - 28mm and violet - 19mm*

The change in the directional characteristics of a multi-element module (Fig. 4) for a underwater acoustic antenna with a cylindrical active surface at frequencies other than its resonant one was studied.

The module contains 96 piezoceramic elements divided into 16 groups of 6 elements. They are mounted on a cylindrical surface with a radius of 330mm and a sector width of 172mm. Eight groups are used for one directional diagram. By switching the displayed groups, three directional diagrams can be formed.

A device has been developed to ensure the measurement of the directivity patterns of the module. It, together with the module, is mounted on the trolley of the deep-water pool. This ensures that the module is immersed to a depth of about 2 m. The distance between the module and the receiving hydrophone, which is immersed at the same depth, must fulfill the condition $\mathbf{R} > \mathbf{D}^2 / \boldsymbol{\lambda}$ [1], where **D** is the maximum linear size of the module and $\boldsymbol{\lambda}$ is the length of the emitted acoustic wave.

At **D** = 0.18m the distance between the module and the measuring hydrophone must be greater than 2.3m at $\boldsymbol{\lambda}$ = 0.014m. In the process of measurements the distance between them is 3m. The measurements are performed using the schematic diagram of Fig.2.

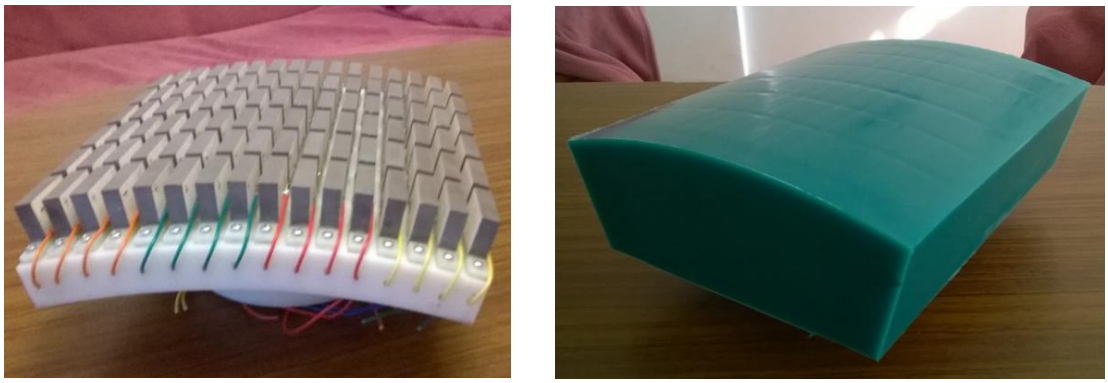


Fig. 4. *Multi-element cylindrical underwater acoustic antenna module: before hermetically sealed (left) and after - (right)*

The measurement process begins with immersing the module and the hydrophone at the same depth and at a distance between them of three meters. The monitoring of the signals is performed on the screen of the oscilloscope - fig.5. The leftmost pulse, observed on the screen of the oscilloscope is the electrical impulse applied to some of the elements of the module. The middle pulse is the acoustic pulse received by the hydrophone. It is the carrier of the information about the directed properties of the part of the module, which is connected to the generator through the gating system, when it is rotated around its axis. The rightmost pulse is the signal reflected from the surface of the pool. Pulses with a duration of 1 ms are used in the measurement. The maximum of the signal is sought by turning the module. The maximum of the received signal is then sought by changing the immersion depth of the measuring hydrophone. After completing these procedures, the resonant frequency of the antenna (module) is determined. For the given module it is 107kHz.

When the module is rotated in the horizontal plane, the levels of the signals received by the hydrophone are measured from the oscilloscope screen. After processing the measured data we get the graphs from fig.5. Each of the graphs presents the pattern of orientation in the horizontal plane for a certain part of the elements of the antenna array. The blue was obtained by emitting the left eight vertical groups of the modulus. Red - in the broadcast of the middle eight groups and green is the result of the broadcast of the left eight groups. The width of these directional diagrams at the minus 3dB level is 8˚. The angle between two adjacent diagrams is also 8˚.

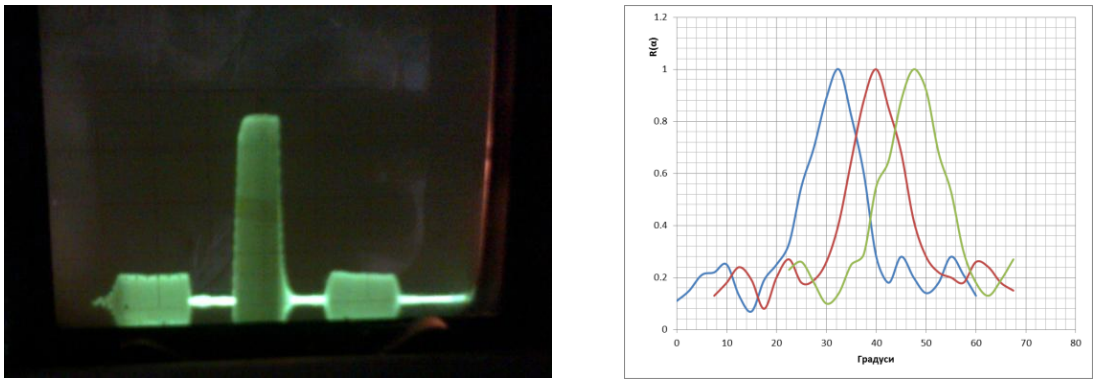


Fig. 5. *The signals from the oscilloscope screen on the left and the measured directivity diagrams of the module on the right*

Measurements were performed to determine the radiation patterns of the module and the frequencies 102 and 112kHz, which is a deviation of ± 5kHz from its resonant frequency. Processing of the results showed that the width of the horizontal radiation patterns of the module changes by ± 1.5˚. At larger deviations from the resonant frequency we do not have effective radiation.

3. Conclusion

The studied cylindrical hydroacoustic antennas, realized on the basis of piezoceramic cylinders, are used in the one-way hydroacoustic system for control of underwater objects Som1 [2] and in the two-way one Som1 / 2 [3] and ensure their efficient operation with high reliability.

An echogram from the screen of a sector sonar [4], the antenna of which is realized on the basis of the module studied by us, is shown in fig.6. The arrow shows the trajectory of a diver from 80m to 180m in an area with a depth of about 10m. In areas with depths of about 20 meters, the movement of divers is effectively observed at distances up to 220 meters.

The research of the frequency characteristics of underwater acoustic cylindrical piezo ceramic transducers is related to the creation of a system for underwater protection of coastal infrastructure objects aimed at the implementation of Work Package 2 "Intelligent Security Systems" of project BG05M2OP001-1.002-0006 "Construction and development of a Center for competence "Quantum communication, smart 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.

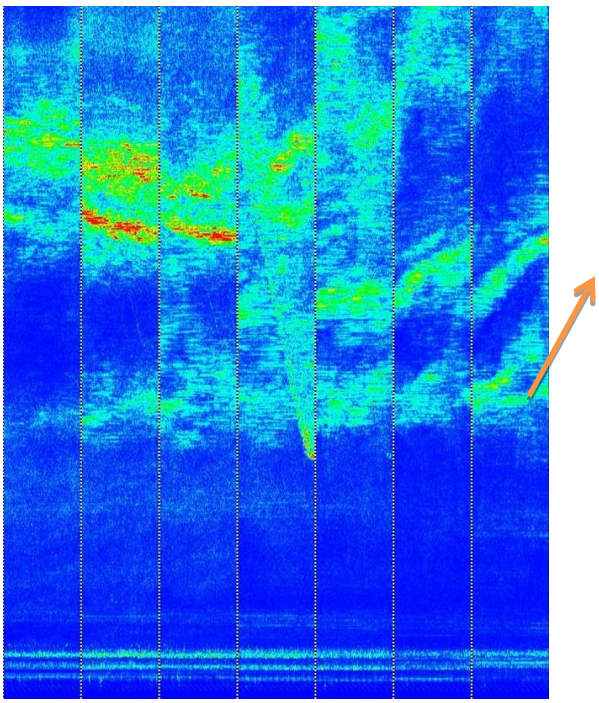


Fig.6. *The echogram from the screen of a sector sonar*

4. References

1. P.J. Bobber, *Hydroacoustic measurements*, translation, Mir publishing house, Moscow (1974)

2. I.K. Ivanov, S. G. Kolev, Hydroacoustic system for management of underwater objects, collection "Protection of ports", pp.145-149, Sofia (2011)

3. S.G. Kolev, I.K. Ivanov, Two-way hydroacoustic system for control and monitoring, Collection of papers from *the Sixth National Conference with international participation Metallurgy, Hydro and Aerodynamics, National Security '2017*, pp. 240-244, ISSN 1313-8308, Sofia (2017)

4. I.K. Ivanov, S.G. Kolev, Sonar with electronic scanning, Collection "Protection of ports", pp.135-144, Sofia (2011)

Influence of the clock of the encoding pulses in hydroacoustic transmission of binary numbers

Stoyan Kolev*, Bistra Nenova, Ivan Ivanov
Institute of Metal Science, Equipment and Technologies, with Hydro- and Aerodynamics Centre "Acad. A. Balevski", Bulgarian Academy of Sciences, Sofia, Bulgaria
s_kolev@abv.bg

Abstract: *Hydroacoustic waves are used to experimentally transmit binary numbers underwater. The numbers are first encoded into pulse sequences, according to the encoding scheme: two consecutive short pulses for a digit zero and two consecutive long pulses for a digit one. A clock period determines the timing of the encoding pulses. The influence of the clock period duration on the number of correctly transmitted binary numbers is tested in 30m deep coastal seawater, at a 1500m distance. The performance is compared at three different periods of the clock: 10ms, 20ms and 40ms. Increasing the clock period of the encoding pulses leads to an increase in the number of correct transmissions. At the longest tested clock period of 40ms all the transmissions of binary numbers are successful. Certainty of correct transmission increases at the longer clock periods of the encoding pulses due to attenuated interference from reflected signals.*
Keywords*: UNDERWATER ACOUSTIC TRANSMISSION, HYDROACOUSTICS*

1. Introduction

Acoustic communication is the most widely used technology for underwater wireless data transmission [1, 2, 7]. Acoustic waves are used as the primary carrier for underwater wireless communication systems due to the relatively low absorption in underwater environments [1]. The channel attenuation is frequency - dependent. Acoustic propagation is best supported at low frequencies, and the bandwidth available for communication is extremely limited [3]. The speed of sound underwater is low – approximately 1500 m/s. The acoustic system is affected by multipath signal propagation due to reflection and refraction. The channel delay spread can be very large (tens of milliseconds, for example), which results in severe intersymbol interference. In addition, the communication channel is affected by ambient noise and has variable characteristics. Effective modulation and demodulation techniques are required to overcome these problems.

Our object is to evaluate the influence of the clock period, used to encode binary numbers into rectangular pulses, on the number of successful acoustic transmissions in seawater.

2. Experimental device

Hydroacoustic waves are used to experimentally transmit binary numbers underwater. The experimental device is a pair of transmitter and receiver, shown in Fig.1. In the transmitter, a number between 0 and 511 is converted to binary and padded with leading zeros to form a 9-digit binary number. Remote transmission is accomplished by encoding the numbers into pulse sequences, formation of pulse bursts with two frequencies between 10 and 40kHz, synchronously with the encoding pulses, and an acoustic antenna [4]. The Motorola protocol, used in MC145026 integrated circuit [5, 6], is selected for encoding of the binary digits. It is developed especially for event transmission and gives very high reliability. As shown in the waveforms in Fig.2, "0" is encoded as two consecutive short pulses and "1" - as two consecutive long pulses. A clock period determines the timing of the encoding pulses. The duration of one digit is 8 periods of the selected clock, and the duration of the short and long pulses is 1 and 7 half-periods of the clock, respectively. Every 9-digit sequence is followed by a pause. The implementation of the protocol on a microcontroller allows the clock period duration to be selected between different values. In the receiver, the input acoustic signal is received through a piezoceramic antenna, amplified and decoded. Two sequential identical numbers are required for a valid reception.

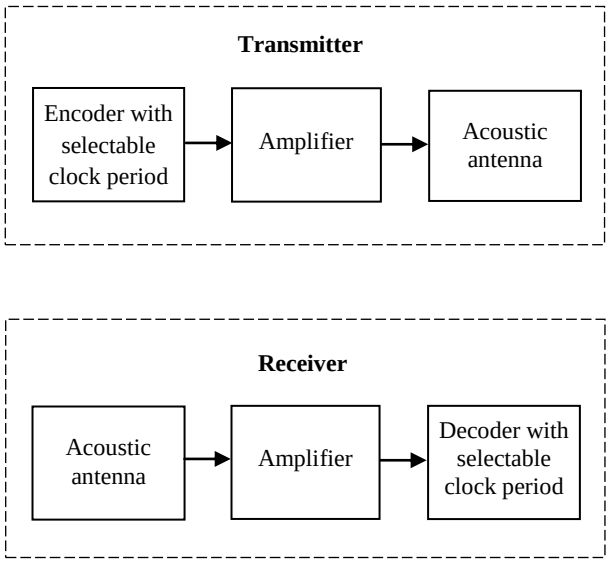


Fig.1. *Experimental device for hydroacoustic transmission*

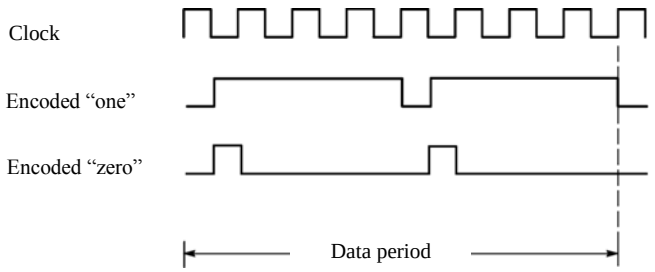


Fig.2. *Encoding waveforms*

3. Experimental results

Binary numbers are experimentally transmitted underwater using acoustic waves. The digits are first encoded into pulse sequences. The timing parameters of the encoding pulses are determined by a clock period. The influence of the clock period duration on the number of correctly transmitted binary numbers is tested in seawater in the southern Bulgarian Black Sea region. The experiments are conducted in shallow waters with a depth of 30m. The bottom is sandy with small stones. The transmitting and receiving antennas are located at about 1500m distance from each other, at several different locations.

Table 1. *Experimental results*

Clock period, ms	10	20	40
Correct transmissions, number	34	45	50
Failed transmissions, number	16	5	-
False transmissions, number	-	-	-

The performance is compared at three different periods of the clock: 10ms, 20ms and 40ms. 50 numbers in the range from 0 to 511 (converted to binary) are transmitted for each of the clock periods. The numbers of correct transmissions, failed transmissions and false transmissions are presented in Table 1. Fig.3 shows a graph of the number of correct transmissions versus the clock period. The experimental results show that increasing the duration of the clock period of the encoding pulses leads to an increase in the number of correct transmissions. At the longest tested clock period of 40ms all the transmissions of binary numbers are successful due to attenuated interference from reflected signals. The two shorter clock periods of 20ms and 10ms resulted in 45 correct transmissions vs. 5 failed ones and 34 correct transmissions vs. 16 failed ones, respectively. The encoding into pulse sequences successfully prevented false transmissions, but it is at the expense of significantly increased transmission time.

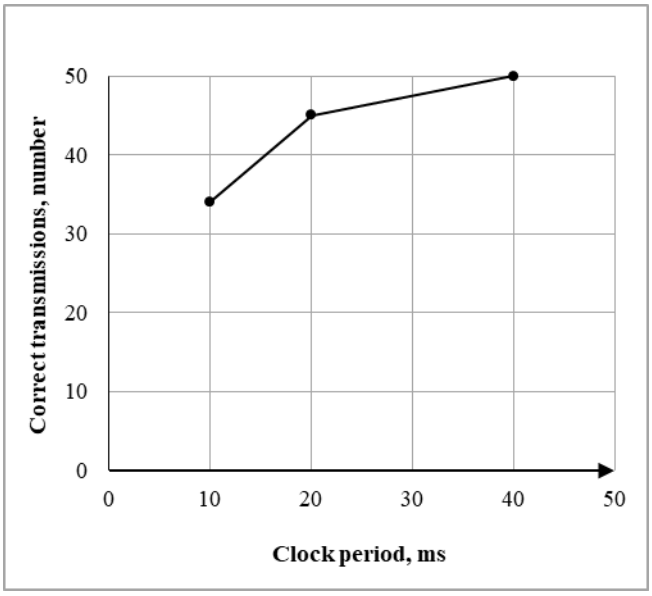


Fig.3. *Number of correct transmissions versus the clock period of the encoding pulses in 30m deep seawater*

4. Conclusion

Hydroacoustic waves are used to experimentally transmit binary numbers underwater. The numbers are encoded into pulse sequences, the timing of which is determined by a clock period. The influence of the clock period duration on the number of correctly transmitted binary numbers is tested in 30m deep coastal seawater, at a 1500m distance. The performance was compared at three different periods of the clock: 10ms, 20ms and 40ms. The experimental results show that increasing the clock period of the encoding pulses leads to an increase in the number of correct transmissions. At the longest tested clock period of 40ms all the transmissions of binary numbers are successful. The encoding into pulse sequences prevents false transmissions, but it is at the expense of increased transmission time. Certainty of correct transmission increases at the longer clock periods of the encoding pulses due to attenuated interference from reflected signals.

Acknowledgement

The experimental results could be used for the development of intelligent security systems within the project “Building and Development of the Competence Center QUASAR”, Work Package 2, funded by the Operational Programme "Science and Education for Smart Growth".

References

1. L. Liu, S. Zhou, J.-H. Cui, Prospects and Problems of Wireless Communication for Underwater Sensor Networks, Wireless Communications and Mobile Computing, **8** (8), 977-994 (2008)

2. J. Partan, A Survey of Practical Issues in Underwater Networks, Computer Science Department Faculty Publication Series, 133 (2006)

3. M. Stojanovic, J. Preisig, Underwater Acoustic Communication Channels: Propagation Models and Statistical Characterization, IEEE Communications Magazine, **47** (1), 84-89 (2009)

4. I. Ivanov, R. Rainov, Ch. Ormanov, B. Monev, S. Vodenicharov, S. Kolev, Marine Mines Control System, Patent 99649/15.01.1997. (not publicly available)

5.http://pdf.datasheetcatalog.com/datasheet/motorola/MC145026.pdf

6. A. Bensky, Radio Communication Basics, *Wireless Security: Know It All*, 77- 136 (2008)

7. Н. Георгиев, А. Коларов, В. Пехливански, Тенденции в развитието на безжичните подводни комуникации, Инженерни науки, год. LVI, 2, 19-30 (2019)

Safety of the technological process in the production and storage of explosives and ammunition

Damyanova Liliya [1], Nikolova Valentina [2], Yaneva Svetlana [3]
IMSETH-BAS-Sofia [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 examines the main dangers that arise in the production and storage of explosives and ammunition. A classification of places where an explosive atmosphere may occur has been made. The obligations of the employer arising from the risks posed by the production of ammunition and pyrotechnic articles are described.*

Keywords*:SAFETY CONDITIONS, EXPLOSIVES, AMMUNITION, PRODUCTION*

1. Introduction

Every strong economy relies on the manufacturing industry and it is of the biggest importance that companies provide safe working conditions for their workers. Ensuring the safety of employees leads to greater efficiency and improved product quality. In the production process there are a large number of risks and dangers for both workers and production. This report presents five main safety risks that are known in the technological process in the production of explosives and ammunition.

2. Main safety hazards in the explosives and ammunition manufacturing industry

2.1. Uncontrolled combustion

Combustion and welding equipment are examples of controlled fire that may be present in a production environment. These are critical points in many production processes. The reason for a large percentage of accidents in the production and storage of explosives and ammunition is the occurrence of uncontrolled combustion, shown in fig.1.



Fig.1

Production environments must be equipped with smoke detection and fire extinguishing devices in order to localize the occurrence of uncontrolled flames. Workers must be provided with and trained to use fire extinguishers, as well as be familiar with evacuation plans. The required evacuation exits must be provided in each production or storage facility. It is necessary for the evacuation exits to be well marked, as well as for regular fire drills to be carried out in order to ensure the safety of the workers and residents of the building.

In order to ensure the necessary level of safety in addition to the provision of proper technological equipment used for the production and storage of explosives and ammunition, it is also necessary to ensure the necessary degree of protection of lighting and electrical systems.

2.2. Hazardous materials

Many industries require workers to manage and handle hazardous chemicals on a daily basis - fig. 2. These are often key elements in the production process. It is essential for the health and life of workers that they be trained to use them correctly and safely. Examples of hazardous chemicals include corrosive cleaning solutions, battery acid and flammable substances such as ethanol. First of all, workers using these chemicals need to know how to transport and load them and how to safely manage the processes using these chemicals. This will ensure safety in normal and predictable uses.



Fig.2

Incidents with hazardous substances and chemicals occur largely in unforeseen circumstances. For this reason, employees need to be trained to treat damage from hazardous chemicals. It is also vital that evacuation procedures are put in place to ensure that the relevant emergency response specialists have access. Keeping basic safety instructions nearby is a great way to help workers make decisions when exposed to a hazardous chemical. All hazardous chemicals must be clearly and visibly labeled so that in the event of a spill, workers and rescue teams can identify the hazard.

2.3. Protection of machines

Proper protection of the machines is essential to ensure the safety of the workers who work with them on a daily basis.

Improperly installed machine fuses pose a danger to employees, which can lead to life-threatening accidents. The machines intended for work in rooms in which there is a danger of explosion need to be in explosion-proof design - fig.3.



Fig.3

2.4. Movement of machines in the premises

Forklifts (Fig. 4) are a key risk factor, and accidents related to them are one of the most common in the manufacturing industry. These include risk to human life, likelihood of injury to workers and damage to goods and materials.



Fig.4

2.5. Slipping and falling in the workplace

Falls are a constant danger in the manufacturing industry. Working on high platforms, ladders or other raised areas poses a personal risk, not only is there a possibility of serious injury to workers, but there is also a risk to their lives. Although the use of safety equipment and helmets is mandatory in manufacturing plants, falling from a great height is the main cause of injuries and deaths among workers.

It is crucial that workers are periodically instructed and trained to understand the signals given to them from the ground, and use the necessary protective equipment and protective clothing.

3. Ensuring the safety and health of workers in the production of explosives and ammunition

Ordinance № 11 of 27 December 2004 on the minimum requirements for ensuring the safety and health of workers in the event of a potential risk of explosive atmosphere lays down the minimum requirements for ensuring the safety and health of workers exposed to the potential risk of an explosive atmosphere.

The employer is responsible and must take all necessary measures to ensure the safety and health of workers. It is the obligation of the employer to provide the necessary conditions for prevention and protection against explosions, as well as to take technical and/or organizational measures, consistent with the nature of the work and in accordance with the following priorities and basic principles:

- prevention of the formation of an explosive atmosphere;

- preventing the ignition of explosive atmospheres and reducing the dangerous effects of explosions so as to ensure the safety and health of workers.

The employer is obliged to take the necessary measures in all places where an explosive atmosphere could occur to an extent that would endanger the safety and health of workers or other persons in order to ensure:

1. Work environment in which the work is performed safely;
2. Appropriate control of the working environment at work, which is in accordance with the risk assessment and is carried out using appropriate technical means. [1]

Site managers are required to provide:

1. The organization of the production process in accordance with the requirements for safety and fire protection;

2. Training of workers with explosives on occupational safety when working with these materials;

3. The development of instructions on occupational safety when working with explosives;

4. Those working with explosives with special work clothes suitable for their working conditions, the necessary personal protective equipment and auxiliary devices;

5. Monthly inspection of the procedure for storage, acceptance and reporting of explosives;

6. Order and security during unloading and transportation of explosives to warehouses and workplaces;

7. Timely investigation of accidents and incidents when working with explosives and development of measures to prevent them;

8. Fulfillment of the prescriptions of the control bodies on labor safety when working with explosive materials. [1-6]

4. Classification of places where an explosive atmosphere may occur

4.1. Places where an explosive atmosphere may occur are classified into two groups:

(a) hazardous places;

b) non-hazardous places.

4.1.1. The classification of areas where an explosive atmosphere may occur shall take into account the presence of flammable and / or combustible substances.

4.1.2. Layers, accumulations and amounts of flammable dust are reported as any other source that can form an explosive atmosphere.

4.2. Classification of hazardous places.

4.2.1. Hazardous areas are classified into zones on the basis of the frequency and duration of explosive atmospheres. The scope of the measures to be taken is determined by this classification - Fig. 5 and Fig. 6.

ZONES		
mixture with air of flammable substances in the form of gases, vapors and aerosols	mixture with air of flammable substances in the form of in the form of combustible powders	Zone definition
1 0	2 20	3 an explosive atmosphere exists permanently, continuously or occurs frequently
1	21	an explosive atmosphere can sometimes occur during normal operation
2	22	an explosive atmosphere is formed during normal operation or is formed in a short time

Fig. 5

4.2.1.1. Zone 0

A place where an explosive atmosphere consisting of a mixture of flammable substances in the form of gases, vapors or aerosols and air exists permanently or for a long time or occurs frequently.

4.2.1.2. Zone 1

A place where an explosive atmosphere consisting of a mixture of flammable substances in the form of gases, vapors or aerosols and air is likely to occur occasionally under normal operating conditions.

4.2.1.3. Zone 2

A place where an explosive atmosphere consisting of a mixture of flammable substances in the form of gases, vapors or aerosols and air is unlikely to occur under normal operating conditions, and if it does occur, it will only be for a short time.

4.2.1.4. Zone 20

A place where an explosive atmosphere, in the form of a mixture of dispersed flammable dust and air, exists permanently or for a long time or occurs frequently.

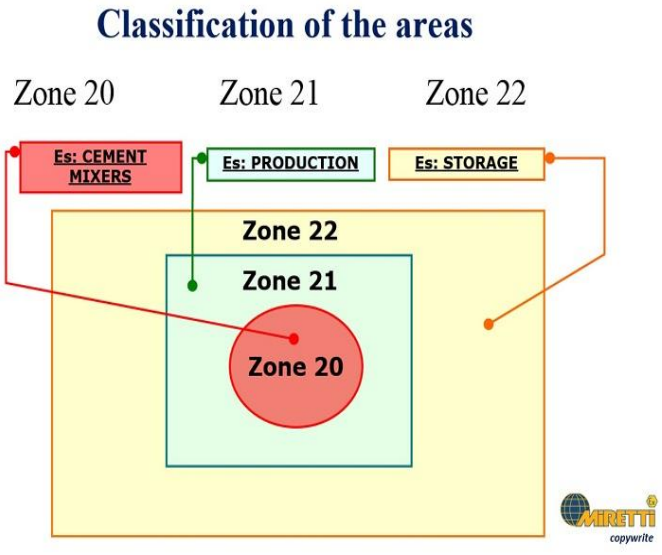


Fig. 6

4.2.1.5. Zone 21

A place where an explosive atmosphere, in the form of a mixture of dispersed flammable dust and air, is likely to occur occasionally under normal operating conditions.

4.2.1.6. Zone 22

A place where an explosive atmosphere, in the form of a mixture of dispersed flammable dust and air, is unlikely to occur under normal operating conditions, and if it does, it will only be for a short time.

3. Conclusions

In conclusion, each workplace has its dangers, but the production of explosives and ammunition poses a higher risk of injury and loss of life than many other modern work environments.

A safe production process can be ensured by training personnel to work with hazardous materials, risk assessment, conducting the necessary briefings and strict adherence to work and production discipline.

Compliance with regulatory requirements and safety regulations regulated by laws and regulations leads to improving the quality of work performed and minimizing the risk of accidents in the production and storage of explosives and ammunition.

The results are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of 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

Ordinance № 11 of 27 December 2004. On the minimum requirements for ensuring the safety and health of workers at potential risk of an explosive atmosphere, Prom. DV. issue 6, 18/01/2005, amended DV. no. 101, 04/12/2007

1. Regulations on labor safety during blasting works, in force from 01/07/1997.

2. M. Todorov, V. Kostov, Prediction Of The Development Of Long Term Deformations In Deposit Bodies, SGEM2017 Vienna GREEN Conference Proceedings, ISBN 978- 619-7408-28-7 / ISSN 1314-2704, 27 - 29 November 2017, Vol. 17, Issue 43, 139- 146 pp; DOI:10.5593/sgem2017H/43/S18.018, https://sgemworld.at/sgemlib/spip.php?article11001;

3. Мирослав Тодоров, Дълготрайност и деформации на геотехнически системи, ISBN 978-619-91513-1-0, 01.2020 г.;

4. Мирослав Тодоров, Особености на модела на взаимодействие на вкопани тръбопроводи и почвен масив, ISBN 978-619-91513-0-3, Публикувана книга на базата на защитен дисертационен труд за присъждане на образователна и научна степен „доктор“, 01.2020 г.;

5. M. Todorov, Mihail Todorov, G. Kamenarov „Landslide Investigation Aspects“, ISEC EURO MED SEC 3 - Holistic Overview of Structural Design and Construction, Limassol, Cyprus, June 22-27, 2020, ISSN: 2644-108X, doi: 10.14455/ISEC.res.2020.7(1).GFE-05;

6. M. Todorov, Mihail Todorov, “Structural Concepts Implemented While Surveying Buildings Of Historical And Cultural Significance”, ISEC EURO MED SEC 3 - Holistic Overview of Structural Design and Construction, Limassol, Cyprus, June 22-27, 2020, ISSN: 2644-108X, doi: 10.14455/ISEC.res.2020.7(1).AAE-20.