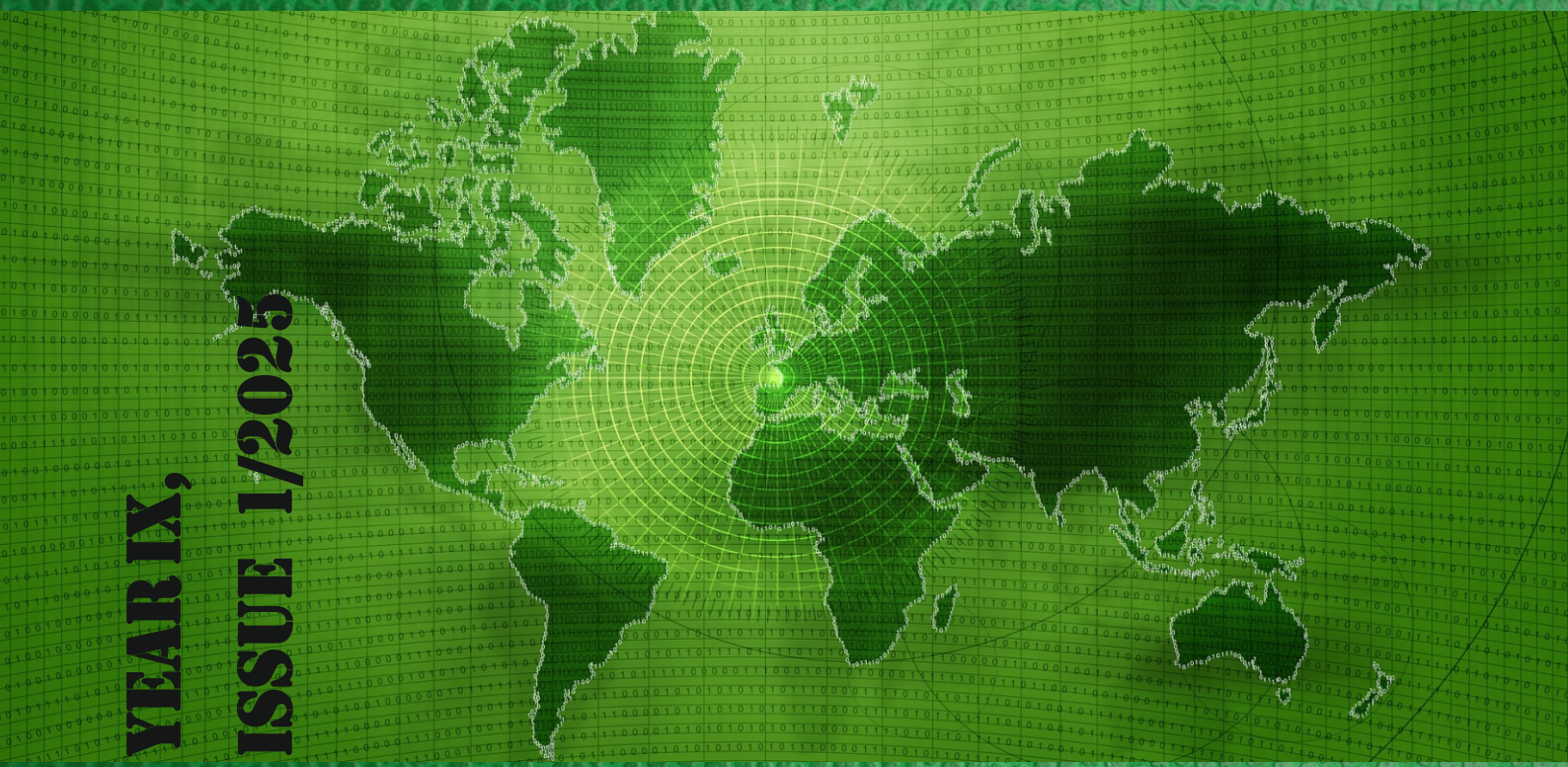
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

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



YEAR IX, ISSUE 1/2025

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 IX, ISSUE 1 / 2025

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

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov, New Bulgarian University, Sofia, BG

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

C O N T E N T S

THEORETICAL FOUNDATIONS OF SECURITY

Content Analysis Of Research In The Field Of Emotional Intelligence In Military Leadership
Eva Kozáková, Miroslav Polach 3

A systematic approach to training aimed to improve the efficiency of npp personnel training
D. Dimitrov, N. Randelova 7

State of technical inspctions implementation on the example of residental buldings destroyed as a result of fire
Sławomir Bałuszyński 9

NATIONAL AND INTERNATIONAL SECURITY

Electromagnetic support using software-defined radio
Ivan Ivanov , Sevdalin Spassov 12

INFORMATION SECURITY

Application of a Cyber Training Ground as a Solution for Training Cybersecurity Specialists to Ensure the Functionality of the National Situation Center and Crisis Management Center
Veselina Gagamova, Elitsa Pavlova, Violeta Vasileva 18

Smart contract in security
Nikolay Radulov, Teodora Lichev 21

Analysis of graphic and UX design for Bulgarian tourist applications
Veselka Stoyanova, Ilian Lilov 25

TECHNICAL FACILITIES FOR ENSURING SECURITY

An approach to monitoring, classifying and jamming underwater sound communications
Aleksandar Kolarov, Radostin Najdenov 28

Content Analysis Of Research In The Field Of Emotional Intelligence In Military Leadership

Eva Kozáková[1,*], Miroslav Polach[2]
University of Defence, Brno, Czech Republic
eva.kozakova@unob.cz, miroslav.polach@unob.cz

Abstract: *The article presents a literature review on the development of emotional intelligence in military leadership from 2020–2025, providing a comprehensive and objective view of the research area. Emotional intelligence and military leadership are a connection that is currently appearing in research activity and doctrinal army documents. The authors try to find and evaluate the benefits and limits of EI in the field of preparing military personnel. The study aims to identify research topics and suggest further research options for military leadership. For objective processing, the method of content analysis according to the established criteria and the method of synthesis were used to identify the main research.*
Keywords*: EMOTIONAL INTELLIGENCE, EMOTIONS, MILITARY LEADERSHIP, DEVELOPMENT*

1. Introduction

The Army of the Czech Republic (ACR), like the armed forces of other former Warsaw Pact countries, has undergone significant and dynamic changes since the end of the Cold War. These changes have been driven by the need to shift from a conscription-based, Soviet-style military structure to a professional, NATO-compatible force. The reform process has included structural reforms, doctrinal updates, modernization of equipment, and the adoption of Western standards in leadership, training, and operational planning. This development reflects not only a change in strategic direction but also a wider effort to improve the credibility and interoperability of the ACR within the collective defence framework of NATO.

Their efforts went beyond downsizing and modernization of the armed forces to include the transition to NATO standards in command and control, which was crucial for ensuring interoperability. Continuous evaluation and exploration of new approaches to personnel training modernization are vital for fulfilling the tasks of the Armed Forces of the Czech Republic and maintaining NATO standards.

Given the ACR development concept, which anticipates an annual increase of approximately 2,400 new soldiers, the area of personnel training and development is a top priority. A key role in recruiting candidates for service at the lowest officer ranks will be played by the University of Defence in Brno (hereinafter referred to as UO), as well as by direct recruitment and career progression [1].

Definition of the term "leadership": "Within the context of the Armed Forces of the Czech Republic (ACR), leadership represents the commander's ability to motivate, persuade, and engage individuals in their environment to actively contribute to the fulfilment of shared tasks, whether predetermined or anticipated shortly. The art of leading is one of the most essential qualities of any commander, and it is indispensable for effective command" [2].

This definition implies that, within the ACR, the concept of leadership is understood in the command-and-control system as a leadership style characterized by strong value orientation and motivational focus, embodied by the commander as a leader.

It follows, therefore, that in the ideal case, the values upheld by the ACR should correspond with the personal attributes of the individual commander-leader. The development of such personal qualities is the result of a complex interplay of upbringing, training, and education—factors that mutually influence one another and are closely linked to the process of individual maturation and the accumulation of both life and professional experience.

Current research suggests that the construct of emotional intelligence represents one of the potential avenues for developing the essential competencies of commanders, particularly in facilitating their interactions with subordinates. Emotional intelligence encompasses the ability to accurately identify emotions in oneself and others, to understand emotions and their underlying language, to regulate emotions both internally and externally, and to utilize emotions to support cognitive processes and motivate adaptive behaviour. It offers a wide range of practical applications.

The concept of emotional intelligence may help prevent social and interpersonal conflicts and increase the chances of success in relationships. It can positively affect the conditions needed to build stable, harmonious social bonds between soldiers and their commanders, especially in small military units. Scholarly literature and military leadership doctrines increasingly acknowledge the importance of emotional intelligence and its role in guiding military personnel. Recent research shows that emotional intelligence, along with the social environment, significantly influences the development of military commanders.

The concept of emotional intelligence is currently the subject of intensive research, not only within the domain of leadership. The term was first introduced by American psychologists Peter Salovey and John D. Mayer, building upon the work of Howard Gardner. These authors sought to highlight the prevailing societal tendency to perceive emotions as disruptive elements in cognitive processes—elements that must be controlled. They defined emotional intelligence as a subset of social intelligence, encompassing the ability to monitor one's own and others' emotions, to differentiate among them, and to use this information to guide one's thinking and actions [4].

Emotional intelligence constitutes a fundamental aspect of human behaviour, distinct from intellectual capacity (Bradberry & Greaves, 2013). The concept gained widespread public attention through the work of American psychologist Daniel Goleman, who emphasized that emotional dispositions and personality traits—particularly those influencing the quality of interpersonal relationships—play a decisive role in personal and professional success [5].

Consideration is being given to how the development of emotional intelligence can be integrated into the education, training, and development of leaders within the Armed Forces of the Czech Republic. The Czech Armed Forces define three fundamental levels of leadership as usual as other NATO countries:

a) Direct Leadership Direct leadership is characterized by a higher degree of certainty, lower complexity, and direct contact between the leader and subordinates. It focuses on specific tasks, linear problems, and the immediate application of competencies. Key elementsdevelopment and high-performing teams with a combat ethos, effective communication, leading by example, trust, respect, subordinate development, and fostering a positive unit climate. Direct leaders simplify complex situations, establish clear intent, and set expectations for outcomes.

b) Organizational Leadership Organizational leadership is marked by greater problem complexity, a larger number of subordinates, and a higher degree of uncertainty. It is applied at the operational level of command, addressing short- to medium-term organizational issues, planning joint operations, developing organizational structures, and supporting professional growth. It functions

indirectly through subordinate leaders, the establishment of principles and values, and the shaping of organizational climate. The core focus is to motivate subordinates to fulfill strategic objectives, set priorities, create vision, and allocate resources effectively in accordance with operational requirements.

c) Strategic Leadership Strategic leadership is exercised at the highest levels of command within the Czech Armed Forces and the Ministry of Defence. It operates under conditions of high risk and uncertainty, addressing complex problems with long-term impacts that extend beyond the military sphere. It focuses on leading change, national defence, aligning alliances and national interests, operating across multiple domains, and decision-making in uncertain environments. Strategic leaders must develop key competencies while considering security developments, political decisions, budgetary constraints, technological advancements, and the experiences of partner nations [6].

This review article aims to systematically map the development of research on the role of emotional intelligence in military leadership during the period 2020–2025. Based on an analysis of scholarly studies indexed in the Web of Science database, the article identifies the main research directions and methodological approaches. The review also highlights existing research gaps and offers recommendations for future inquiry in this domain. Equally important are the practical implications for military education and commander training, as the characteristics and trends of the contemporary security environment compel higher military education institutions to place significant emphasis on preparing future military leaders. Among the most critical competencies for commanders and staff officers are those related to effective leadership and personnel development.

2. Methods and data

Based on the analysis of selected articles, thematic areas were identified, to which specific articles were assigned according to the conducted research. Table 1 lists an overview of the number of articles on emotional intelligence that can be developed in military leadership in 2020-2025.

Table 1: *The overview of the number of articles on emotional intelligence in military leadership in 2020-2025*

Research domains	Number of articles
2025	6
2024	10
2023	12
2022	14
2021	8
2020	5

3. Results

Garcia Zea et al. (2020) examined the impact of emotional intelligence (EI) within the military context. They identified protective variables that may mitigate the effects of stress on the emotional well-being and behavioural issues of military personnel. Their findings indicate that EI training and EI-focused interventions contribute to enhancing and moderating individuals' ability to adapt to and cope with stress and traumatic experiences [7].

Silver et al. (2023) developed a course titled *"Adventure and Experiential Learning"* aimed at fostering interpersonal leadership skills among cadets. The results demonstrated a significant increase in emotional intelligence (EI) among course participants. Outdoor experiences may serve as an effective means of training EI-related skills. The research conducted by Silver et al. (2023) offers valuable insights into the potential of experiential learning as a tool for developing emotional intelligence (EI) in military training contexts. By integrating outdoor activities with leadership development, the study highlights a novel and engaging approach to enhancing interpersonal competencies among cadets. The observed increase in EI underscores the importance of incorporating non-traditional, experience-based methods into structured training programs. These findings support the growing recognition that emotional and social skills are critical components of effective leadership, particularly in high-stress environments such as the military [8].

Ayoko et al. (2023) investigated how a leader's perception of follower behaviour may influence the follower's perception of the leader's behavior, which can be associated with the evaluation of interpersonal relationship quality. When leaders effectively regulate their emotions, the positive impact of followers' perceptions on the quality of interpersonal relationships is enhanced. This study highlights the reciprocal nature of leader–follower dynamics, emphasizing that emotional regulation by leaders not only shapes their behaviour but also strengthens the relational feedback loop. It suggests that emotionally intelligent leadership can foster more positive and resilient interpersonal connections within organizations [9].

Cioranu et al. (2024) examined general competencies within the discipline of military leadership, aligning their analysis with competency-based learning outcomes. For the discipline "Military Leadership," they propose the inclusion of the following broadly defined thematic areas: military leadership (doing the right things, management vs. leadership, efficiency vs. effectiveness); definitions, theories, types, and principles of military leadership; emotional intelligence in leadership; critical thinking in leadership; vertical development of leadership; competencies and traits associated with leadership; and military leadership as a primary element in the integration of capability domains [10].

The military environment is characterized by high levels of stress and unpredictability, which activate psychobiological stress responses and may adversely affect both the health and performance of military personnel. Perceived stress, understood as a subjective sense of uncontrollability and uncertainty, tends to accumulate particularly under prolonged occupational strain. Within the framework of positive psychology, attention shifts from problem-focused approaches to the development of protective factors, among which emotional intelligence plays a pivotal role [10].

Individuals with a high level of EI can perceive stressful situations as challenges rather than threats, thereby reducing the negative psychological and physiological consequences. Emotional intelligence thus serves as a significant protective mechanism that facilitates coping with demanding circumstances and contributes to the reduction of perceived stress in military settings. In alignment with this perspective on emotional intelligence, a study was conducted by Feng et al. in 2025.

Drawing upon the frameworks of allostatic load and social self-preservation theory, this study investigates the role of emotional intelligence in shaping self-esteem through the mediating effect of perceived stress among a sample of 143 military personnel. The salivary alpha-amylase (sAA)/cortisol ratio was employed as a moderating variable to assess physiological stress regulation. Results from a conditional process analysis revealed a significant indirect pathway: individuals with higher emotional intelligence reported lower levels of perceived stress, which in turn correlated with elevated self-esteem. Notably, the sAA/cortisol ratio moderated this relationship—participants exhibiting higher ratios,

indicative of dysregulation in the psychobiological stress system, demonstrated a stronger indirect effect. Under such conditions, emotional intelligence emerged as a particularly robust protective factor for self-esteem [11].

These findings underscore the dynamic interaction between psychological stress appraisal and neuroendocrine functioning, illustrating how biological stress responses can modulate the impact of emotional competencies on self-perception. The study contributes to integrative models of stress resilience by advocating for the inclusion of physiological indicators alongside psychological traits in understanding adaptive functioning within high-stress environments [11].

Emotional intelligence was assessed using the Chinese adaptation of the Wong-Law Emotional Intelligence Scale (Wong & Law, 2002), comprising 16 items rated on a seven-point Likert scale (1 = strongly disagree to 7 = strongly agree). An example item is: "I am able to control my temper and handle difficulties rationally." The scale demonstrated high internal consistency, with a Cronbach's alpha of 0.92 [11].

Druham et al. (2023) present a study on the development and validation of an online training program aimed at enhancing EI in adults, grounded in theoretical and empirical foundations.

A total of 326 participants from the general population were randomly assigned to either the EI training group (n = 168) or a placebo control group (n = 158). Both programs consisted of 10–12 hours of online content, completed over one or three weeks. Participants in the EI training group showed significant improvements in both self-reported and performance-based EI measures, including emotion recognition, understanding, and regulation. These gains were sustained six months post-training. The program was also rated as engaging and helpful. The online EI training program is empirically grounded, well-received, and effective in enhancing emotional intelligence. Its scalability makes it suitable for diverse applications in personal and professional development [12].

Psychological stress significantly impacts the mental and physical health of military personnel. In a cross-sectional study involving 452 Chinese Navy soldiers, we examined the associations between stress, optimistic intelligence, and emotion regulation using standardized self-report measures. Findings revealed that higher stress levels were linked to lower perceived happiness and reduced capacity to cope positively with adversity, while showing positive correlations with emotion regulation strategies such as cognitive reappraisal and expressive suppression. These results underscore the importance of implementing positive psychology-based interventions to mitigate stress, promote well-being, and strengthen operational effectiveness within naval forces [13].

Author Ledzianowski discusses the importance of emotional intelligence in his work. He introduces the Wise Commander–Leader (MDL) model, designed in response to the evolving demands of modern military leadership. It outlines the preferred command structures, operational systems, essential competencies, and behavioral attributes required of today's commanders. The MDL model serves as a framework for cultivating leadership competencies within the armed forces. Additionally, the paper proposes a structured process for developing these competencies, offering practical guidance for achieving the MDL standard. Drawing on the experiences and accomplishments of a military academy, the study highlights effective approaches to leadership development tailored to the needs of contemporary military operations [14].

True et al. (2020) present a study in a military medicine journal. Physicians increasingly serve as leaders, prompting interest in leadership development within Graduate Medical Education (GME). Although not required by ACGME, some U.S. programs have begun incorporating leadership training. This study evaluated the impact of a pilot leadership course for internal medicine residents. In 2017, senior military residents participated in a four-part course covering leadership basics, emotional intelligence, teamwork, and conflict resolution. Feedback was collected through an 18-question survey. The project was approved as a quality improvement initiative. Out of 54 residents, 26 responded (48.1%). Most found the training useful (84.6%) and felt better prepared for leadership roles (80.8%). Additionally, 73.1% planned to pursue further leadership development. All agreed internists should lead clinical teams and that leadership should be taught during residency. Even brief training can positively influence residents' views on leadership. Based on these results, leadership education was integrated into all GME programs at the institution. A national ACGME requirement could support broader implementation and sharing of best practices [15].

In the USA army was conducted. The study confirmed a link between emotional intelligence (EI) and safety citizenship (SC) among Army pilots, with potential implications for improving aviation safety. Understanding how adaptability and self-esteem influence safety behavior could enhance pilot selection and training.

The research was based on a limited sample of military pilots, who may not represent the broader aviation community. Further studies involving general and commercial aviation pilots are recommended. A notable finding was the negative association between optimism and SC, which warrants deeper investigation. Future research should focus on training methods that strengthen adaptability and self-esteem in aviation settings [16].

Unfortunately, several articles are not available for free access, so they were not able to report in this article. The number of articles is not so high and shows 0 results in the Czech army.

4. Conclusion

Contemporary literature provides the professional community with evidence-based findings demonstrating that a high level of emotional intelligence is positively associated with decision-making, the establishment of constructive relationships, and effective leadership. Training in emotional intelligence and the development of its individual components—namely, emotional perception, emotional utilization, emotional understanding, and emotional regulation—would be beneficial for enhancing the ability to leverage emotions in support of cognitive processes, fostering creativity and more effective problem-solving, and managing emotions to promote personal growth [17].

Learning effective strategies for managing our own emotions, as well as assisting others in regulating theirs, is essential for establishing a strong foundation for the development of positive interpersonal relationships and fostering a constructive social climate within the unit. The ability to build positive relationships effectively across diverse environments is a key attribute of intercultural competence, which can be enhanced through emotional intelligence training.

The modern soldier is exposed to immense professional and emotional pressure within today's complex operational environment. The preparation of commanders should encompass the development of self-awareness, awareness of others, emotional regulation strategies, and techniques for coping with stressful

situations. Incorporating education in emotional intelligence is, without question, a step forward [18].

The development of emotional intelligence within the military remains a subject of ongoing research and discussion, with its benefits and limitations continually being explored. Findings indicate that a high level of emotional intelligence is positively associated with decision-making, the formation of constructive relationships, and effective leadership. Training in emotional intelligence and the enhancement of its individual components—namely, emotional perception, emotional utilization, emotional understanding, and emotional regulation—would be beneficial for the ability to harness emotions to support cognitive processes, improve problem-solving effectiveness, and manage emotions in ways that promote personal growth.

The authors' aim soon is to develop a methodology designed to enhance the individual components of emotional intelligence—namely, emotional perception, emotional utilization, emotional understanding, and emotional regulation—among participants, and to cultivate their ability to apply these competencies in practical command roles within the Armed Forces of the Czech Republic in all levels of leadership.

Acknowledgment

This work was conducted and financed within the framework of the project „Conduct of land operations (LANDOPS)"

5. References

1. Concept of Force Development 2030 of the Armed Forces of the Czech Republic, Prague: Ministry of Defence (2019).
2. Ministry of Defence of the Czech Republic. Doctrine of the Armed Forces of the Czech Republic. Prague: Ministry of Defence of the Czech Republic, (2004).
3. M. Penrod, Marie. Army Continuing Education System: The Role of Emotional Intelligence in Army Education Leadership as It Pertains to Team Performance. Georgia Southern University (2010).
4. J. Mayer, P. Salovey, & D. Caruso, Models of emotional intelligence. In R. J.Sternberg (Ed.), The handbook of intelligence (pp. 396-420). New York, NY: Cambridge University Press, (2000).
5. D. Goleman, Emotional intelligence. Prague: Metafora, (2011). ISBN 978-80-7359-334-6
6. M. Marek and A. Tesař. Leadership Development in the Conditions of the Army of the Czech Republic. (Military Perspectives, 31(4), pp. 050–070. (2022).
7. Zea G., D.; Sankar, S. A. Isna, . The Impact of Emotional Intelligence in the Military Workplace. Online. *Human Resource Development International*. Volume **26 (1),** S. 85-101. (2023) ISSN 1367-8868.
8. Silver, A. I.; Marshall, R.; Huston, Dave A. Gentry, G. Development of Emotional Intelligence During an Adventure and Experiential-Based Learning Course. Online. *Journal of Experiential Education*. **volume 47**, s. 341-357. (2024) ISSN 1053-8259.
9. O. Ayoko, P.Tan, Pao P a LI, Yiqiong. Leader–follower interpersonal behaviors, emotional regulation, and LMX quality. *Journal of Management and Organization*. **volume 19, (3),** s. 553-570. (2023)
10. I. Cioranu, I. A..L.Cucinschi, L.Scipanov, Professional Training and Personal Development: Essential Complementarity in the Military Educational Process. *Revista Romaneasca Pentru Educatie Multidimensionala.*,**volume 16, č. 4,** s. 509-541. (2024).
11. Yuting Feng, Bin Liu, Zhongying Wu, Zhujing Ma, Lei Song, Lin Zhang, Li Guo, Xiaodong Zhao, Hongchang Sun, Yinchuan Jin, Qun Yang, Emotional intelligence, self-esteem, and psychobiological stress: conditional indirect associations in military personnel, Personality and Individual Differences, **volume 244**, (2025), ISSN 0191- 8869.
12. Durham MRP, Smith R, Cloonan S, Hildebrand LL, Woods-Lubert R, Skalamera J, Berryhill SM, Weihs KL, Lane RD, Allen JJB, Dailey NS, Alkozei A, Vanuk JR, and Killgore WDS, Development and validation of an online emotional intelligence training program. *Front. Psychol*. **volume 14,** (2023) .
13. Cui, Y., Zhang, X., Liu, N., Liu, Q., Zhang, L., & Zhang, Y. A correlation study of military psychological stress, optimistic intelligence quotient, and emotion regulation of Chinese naval soldiers. *Social Behavior and Personality: an international journal*, **volume 50(5),** 1–14. (2022).
14. Ledzianowski, J., & Stachowicz, J. (2020). In K. S. Soliman (Ed.), *Education excellence and innovation management: A 2025 vision to sustain economic development during global challenges* (pp. 14786–14792). Proceedings of the 35th International Business Information Management Association Conference (IBIMA), Seville, Spain, (2020). International Business Information Management Association.
15. M.W.True, I. Folaron, J. A Colburn, J. L. Wardian, J. S Hawley-Molloy, J. Hartzell, Leadership Training in Graduate Medical Education: Time for a Requirement, *Military Medicine*, **volume 185**, Issue 1-2, January-February, Pages 11–16, (2020).
16. Dugger, Z. T., & McCrory, B. Emotional Intelligence and Safety Citizenship among Army aviators. *International Journal of Aviation, Aeronautics, and Aerospace*, **volume 8 (1).** (2021).
17. K. Hudson, Emotional Intelligence and Self-Efficacy in Military Leaders. USA: Bradman University, (2016).
18. J. Moriarty, Leadership in focus: Emotional Intelligence, Leadership and Resilience. (2018).

A systematic approach to training aimed to improve the efficiency of npp personnel training

D. Dimitrov[1], N. Randelova[2]
Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria[1]
Kozloduy Nuclear Power Plant[2]
E-mail: ddimitrov@ims.bas.bg, NSRandelova@npp.bg

Abstract: *The Systematic Approach to Training (SAT) is a logically structured process based on job analysis whose aim is to ensure that the personnel have the necessary knowledge, skills and attitudes to effectively perform their assigned tasks. The SAT is a flexible system that can be adapted to the needs of any nuclear power plant and any job position.*
KEYWORDS: *NUCLEAR FACILITIES, SYSTEMATIC APPROACH TO TRAINING, MANAGEMENT SYSTEMS, PROTECTION OF NUCLEAR INSTALLATIONS, REGULATORY FRAMEWORK*

1. Introduction

The Systematic Approach to Training (SAT) is a logically structured process based on job analysis, whose aim is to ensure that the personnel have the necessary knowledge, skills and attitudes to effectively perform their assigned tasks.
The SAT includes five interrelated stages:
1. Analysis;
2. Design;
3. Development;
4. Implementation;
5.Evaluation.
These stages are not applied linearly and in a one-off fashion, but in a circular and continuous manner so that the results of the evaluation feed back into the other phases. The SAT is a flexible system that can be adapted to the needs of any nuclear power plant and any job position.

2. Overview of the activities included at the different stages

Appropriate training ensures that each member of staff is informed about the meaning and significance of the work they are performing and about how their work contributes to safety and to the achievement of the Company's goals.

2.1. Analysis

The analysis phase aims to determine what knowledge, skills and attitudes are required for each job position. Methods used include:

- Job and task analysis;
- Competency analysis;
- Interviews, surveys, observation, documentation.

The ultimate goal is to produce a list of:

- Required knowledge, skills and attitudes;
- Critical tasks;
- Terms of performance;
- Frequency and importance of each task.

2.2. Design

At this stage, the following is determined:

- The structure of the training program;
- The learning objectives;
- The training methods (e.g. simulators, lectures, on-the-job training);
- The assessment methods – tests, practical demonstrations, observation.

The design stage ensures that all critical knowledge, skills and attitudes identified at the analysis stage will be covered by the program, and that the training will be aimed at achieving specific results.

2.3. Development

At this stage the following are created:

- Training materials (manuals, presentations, simulator scenarios);
- Assessment tools (tests, checklists, feedback forms);
- Instructor guides and lesson plans;
- Scenarios for emergency or extraordinary situations, if needed.

The development stage should provide all the necessary resources to deliver the training effectively and in accordance with the requirements set at the analysis and design stages.

2.4. Implementation

This is the stage in which the training is done for real, by using the materials and methods developed at the previous stages. Key aspects here include:

- Planning and organizing training courses;
- Teaching in the classroom, with a simulator or on-the-job training;
- Monitoring the effectiveness of the training;
- Documenting participation and results.

Employees must demonstrate that they have acquired the required knowledge, skills and attitudes before being allowed to perform their tasks independently.

2.5. Evaluation

Evaluation is a continuous process that is applied at every level:

- Trainees' assessment - have they achieved the objectives?
- Evaluation of the training program - is it effective?
- Trainers' evaluation - are they performing their role well?
- Impact evaluation - does the training contribute to better performance and safety?

The evaluation allows:

- Improvements in the training content or methods;
- Identification of new training needs;
- Evidence of regulatory and internal purposes;
- Feedback to the management on the effectiveness of the investment in the training.

The systematic approach to training is not just a "good practice" but a necessary system for managing the competence of the personnel in the nuclear sector. It provides structure, transparency, sustainability and continuous improvement.

3. Key features and benefits of SAT

SAT is recognized as **the best international practice** for developing and implementing effective training programs in the nuclear industry. Its application brings about a number of key benefits that cover the **quality, effectiveness and sustainability** of the training.

3.1. Key features of SAT

SAT is characterized by the following key features:
- Job-or competency-based analysis:
Training programs are based on a systematic analysis that determines what knowledge, skills and attitudes are needed to perform certain tasks in a job.
- Clearly defined learning objectives:
Each training module has specific and measurable objectives that indicate what the trainee should know and be able to do upon completion of the program.
- Content and methods tailored to the objectives:
Appropriate methods, tools, and materials are used that are directly related to the learning objectives and the trainees'' profiles.

- **Performance assessment**:
Trainees are assessed against predefined criteria. This includes theoretical tests, practical demonstrations, observation, etc.
- **Evaluation and feedback**:
Training programs are periodically evaluated to ensure they are relevant, effective and in line with the needs of the nuclear plant.

3.2. Main benefits of the implementation of the SAT

The implementation of the *SAT* leads to significant benefits for nuclear power plants and operating organizations, including:
- Increased safety: by providing adequate training, the employees are better prepared to respond appropriately to normal, abnormal and emergency situations.
- Increased efficiency and productivity: well-trained personnel work faster, better and with fewer errors.
- Optimal use of resources: SAT helps to direct training only at the really necessary KSAs, thus reducing unnecessary costs.
- Better documentation and traceability: every stage of the training process is documented, which facilitates audits and regulatory oversight.
- Increased motivation and satisfaction of personnel: trainees perceive the training as targeted, applicable and respectful of their roles, which improve staff engagement.
- Better preparation for new technologies and changes: SAT allows flexible adaptation of the training when introducing new equipment, software or organizational changes.
- Improved safety culture: by incorporating KSAs related to human factors, SAT promotes responsible safety behavior and thinking.

In summary, SAT is not just a training methodology - **it is a strategic tool for managing competence, risk and quality** in a nuclear power plant.

4. Applying the Systematic Approach to Training

4.1. Establishing a training system based on SAT

The training system in a Nuclear Power Plant should be formally recognized by the management of the operating organization and should have a clearly defined structure, responsibilities and resources. In this context, SAT is used as a methodology for:

- Developing training programs;
- Implementing effective training;
- Achieving and maintaining competence;
- Facilitating assessment and continuous improvement.

The system should be supported by written policies and procedures that clearly state:

- The objectives and scope of the training;
- The responsibilities of the different units;
- The interaction between the training organization and the operational departments;
- The quality control and performance evaluation mechanisms.

4.2. Stages in the introduction of SAT

The introduction of SAT into an existing training system requires a staged approach that ensures smooth transitions and makes maximum use of the resources already available.
Recommended stages include:
1. Analysis of the current training system:
- What programs exist?
- What methods are being used?
- How is effectiveness evaluated?
2. Training of key SAT staff:
- Training of managers, instructors and training specialists;
- Introductory courses and practical workshops.
3. Identifying priority positions and programs:
- For example: operators, electricians, maintenance personnel;
- Focusing on safety-related positions.
4. Developing and implementation of SAT-based programs for safety-related positions:
- Starting with pilot programs;
- Using the results to refine subsequent programs.
5. Expanding the scope of SAT to other positions and activities:
- Gradual inclusion of management, administrative and subcontractor staff.
6. Establishing a mechanism for continuous evaluation and improvement of the system.

4.3. Key conditions for the successful implementation of SAT

For the effective introduction and sustainable implementation of SAT it is needed:
- Active support from the senior management of the operating organisation and the nuclear plant;
- Appointment of a competent team responsible for the management of the training system;
- Ensuring sufficient resources - staff, budget, technical facilities, and premises;
- Continuous training and development of trainers and training specialists;
- Cooperation between the operational units and the training structure;
- Integration of SAT into human resources, quality and safety management systems.

5. Conclusion

- The implementation of SATs is not a one-off project but a continuous improvement process;
- Existing training programs can be adapted and not necessarily replaced in their entirety;
- SAT allows flexible implementation according to the capabilities and needs of the specific organisation;
- The initial effort is significant, but the long-term benefits outweigh the investment.

The implementation of SAT is a strategic investment in the **competence, safety and efficiency** of a nuclear power plant.

References

- Law on the Safe Use of Nuclear Energy;
- IAEA. Nuclear Power Plant Personnel Training and its Evaluation: A Guidebook. Technical Reports Series No. 380. Vienna: International Atomic Energy Agency, 1996;
- IAEA. Recruitment, Qualification and Training of Personnel for Nuclear Power Plants. Safety Guide NS-G-2.8, Vienna, 2002;
- Quality Management System. Requirements, ISO 9001:2015.

State of technical inspctions implementation on the example of residental buldings destroyed as a result of fire

Sławomir Bałuszyński
Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0009-0004-1897-7298
slawomir.baluszynski@uken.krakow.pl

Abstract: *In 2024, firefighters in Poland recorded 29,271 apartment fires, resulting in 295 deaths and 2,052 injuries. Additionally, due to the emission of "carbon monoxide" [1] , „firefighters recorded 4,329 interventions in which 52 people died from carbon monoxide poisoning, and 1,334 people suffered from poisoning" [2] . An analysis of the causes of fires in previous years, as well as in 2024, indicates several main factors. The most common causes of fires include: arson, improper use of heating devices, defects in electrical equipment and installations, and adult carelessness. The aim of this article is to analyze the state of implementation of technical inspections of utility installations in residential buildings as required by national regulations. The author also presents the results of their own research in this area, along with conclusions drawn from the conducted studies and observations.*

Keywords*: SAFETY, RISK, HAZARD, FIRE, FIRE PROTECTION MEASURES*

1. Introduction

Fire safety is not a precisely defined concept. Neither legal regulations nor the subject literature define it unambiguously, however, it is widely used. [3]. It is also mentioned in national and European Union laws, as well as in scientific and industry literature.[4] .

Therefore, it can be argued that fire safety is achieved through the effectiveness of the fire protection system, within which preventive measures are taken, as well as prevention, social education, and maintaining the capacity for rescue operations [5].

At the same time, meeting the requirement to ensure fire safety requires the implementation of specific actions defined by law [6].

Based on the regulation [7]. It is also worth mentioning that in § 4 section 1, it is prohibited to perform actions that may cause a fire, its spread, hinder rescue operations, or evacuation in the context of using technically faulty installations or those not subject to periodic inspections, with the scope and frequency defined by building law regulations, if this may contribute to the occurrence of fire, explosion, or fire spread.

Regardless of the above, § 6 [8] also contains detailed guidelines regarding the inspection of the technical condition and usability of building elements, including installations.

An analysis of general insurance company conditions also indicates provisions regarding the obligation of regular inspections of installations, which relate to the proper protection of the insured object, taking into account the necessity of complying with preventive regulations, including fire protection, as well as proper maintenance and operation of devices supervised by the person entering into the insurance contract.

The insured therefore has the obligation to maintain the technical condition of all installations, including recommended control tests and inspections. They are also required to equip the installations with all necessary systems (e.g., electric shock protection, surge protection, lightning protection, grounding) and operate them according to their intended purpose, operating instructions, and technical regulations.

Therefore, failure to fulfill these obligations may result in the insurer's liability being excluded if it influenced the occurrence or extent of the damage. This means that the lack of regular inspections may affect the amount of compensation or even lead to its refusal. The modern approach to fire safety assumes that it is not a state achieved once and for all, but a continuous process requiring systematic management, evaluation, and improvement. At the center of this concept is a process that serves as both the focal point and a symbol, integrating key elements that influence the effectiveness of fire protection. At the same time, the whole, presented in the form of a cycle, emphasizes the continuity and dynamics of actions.

However, fire safety does not end with the implementation of procedures. A constant requirement is continuous improvement and adapting the elements surrounding the process to changing conditions. These elements are::

1.Financing carried out by ensuring adequate financial resources for the replacement and purchase of modern fire-fighting equipment, training, modernization of alarm systems, and maintenance of safety infrastructure.

2.Theory

Scientific and normative knowledge in the field of fire safety engineering, psychology of behavior in crisis situations, and legal regulations, where a crisis situation is a phenomenon lasting over time, beginning from a state of equilibrium through instability to stability in a new situation, which is usually qualitatively different. The current model of the modern crisis management process, taking into account deviations from the normal state in fire safety, is based on the implementation of activities in four basic phases: prevention, preparation, response, and recovery.

3.Practice as operational activities: inspections of the technical condition of portable fire extinguishing equipment, fire protection devices, alarm system tests, trial evacuations, and personnel training.

4. Knowledge updating.

Continuous improvement of competencies through training, courses, participation in conferences, and updates on changes in regulations**.**

5. Verification of progress.

Monitoring the achievement of safety goals, analyzing reports from drills and incidents, internal audits.

6. Verification of knowledge.

Checking employees' level of preparedness to respond appropriately to both static and dynamic safety conditions, including hazards; knowledge tests; emergency situation simulations.

7. Response.

Readiness for immediate action in case of danger: evacuation procedures, detection and extinguishing systems, cooperation with rescue entities, including the leading formation, the State Fire Service.

8. Tools constituting technical and organizational measures supporting safety: smoke detectors, fire protection devices, smoke and heat removal systems, risk management applications.

2. Study of the implementation of the obligation to subject technical installations in residential buildings to periodic inspections.

Based on the author's participant observation method, appointed as a court expert registered on the list of experts of the District Court in Nowy Sącz in the field of determining causes and circumstances of fires, findings were made for fires that occurred over a four-month period, i.e., from December 15, 2024, to April 15, 2025, in 45 buildings affected by fire. The established causes of fires based

on conducted inspections in residential buildings—for a total of 45 fires—are as follows:
A. Defects in electrical installations, including the electrical devices in use, accounted for 23 fires.
B. Defects in solid fuel heating devices, including chimney flues: 16 fires.
C. Carelessness of adults, including accidental ignition, was the cause of 8 fires.
D. Intentional actions of third parties, arson: 6 fires.
E. Other incidents: 2 fires.

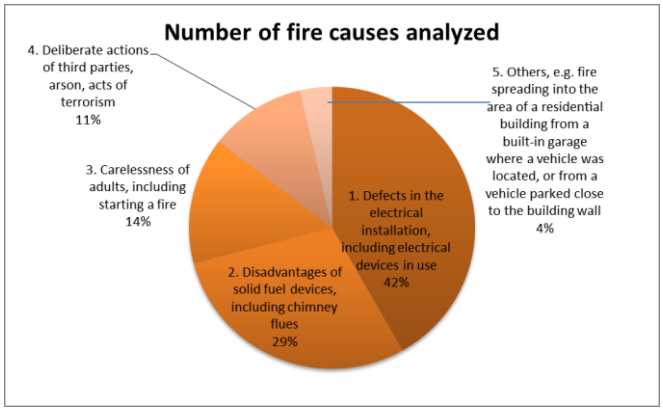


Chart 1. Analysis of Fire Causes , Source: Author's own study.

The above data shows that in the analyzed cases, the most common cause of fires was defects in electrical installations, including the devices powered by them. The second most frequent cause was defects in solid fuel heating devices, including chimney/flue systems. The third most common cause was the carelessness of adults, including accidental ignition.
With regard to the implementation of the obligation to conduct periodic inspections of utility installations in residential buildings, the conducted analysis shows that out of 45 residential buildings, 42 did not have up-to-date periodic inspections for gas installations, including gas appliances. In 4 analyzed buildings, the owners declared having up-to-date inspections of the electrical installation, despite the fact that inspections indicated, in 23 cases, that the cause of the fire was related to hazardous physical phenomena occurring in the electrical installation or in the electrical devices in use.
The highest number—12 out of the 45 analyzed buildings—had chimney inspections conducted. However, it should be noted that in 7 cases, the confirmations of chimney inspections carried out by authorized persons were either unreliable or not compliant with the regulations. These cases were linked to 16 fire incidents caused by chimney-related issues, which means that proper procedures were followed in only 5 buildings.
Additionally, in the collected interviews at the fire sites of the analyzed buildings, 41 owners or managers were unaware of the frequency with which the cleaning of soot and exhaust ducts should be conducted during their usage periods.
At the same time, the conducted research shows that among the 45 residential buildings, the respondents indicated that in 42 cases gas installation inspections are not required. Regarding chimney inspections, 19 people claimed there is no such requirement, 24 did not notice that the inspections were outdated, and 2 declared that they commissioned the inspections to an authorized person, but the inspections were not carried out.
In turn, regarding inspections of the technical condition of electrical installations, 29 respondents indicated there is no requirement for residential buildings, 11 did not notice that the inspections conducted were outdated, and 5 declared that they commissioned the inspections to an authorized person, but these were not carried out on time.

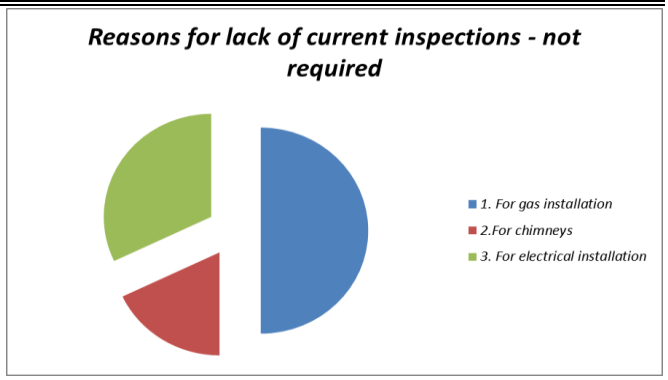


Chart 2. Indicated reasons for the failure to carry out technical inspections by authorized persons based on information obtained from residents during the conducted inspections. Source: own study.

3. Analysis of own research

1.It is necessary to strive for all residential buildings to be mandatorily equipped with devices detecting fire hazards or uncontrolled carbon monoxide emissions. In this regard, it is also proposed that equipping residential units with sensors should additionally include extended monitoring functions, such as sending alerts directly to users' mobile phones via an application.
2. There should be an effort to ensure that all residential buildings are mandatorily equipped with portable fire extinguishing equipment, enabling early intervention to extinguish fires in their initial stages.
3. Allow individuals investing in safety to deduct the purchase of technical devices such as smoke detectors, gas and carbon monoxide sensors, investments in portable fire extinguishing equipment, or fire protection devices installed in residential units or buildings from their personal income tax in the annual tax returns submitted to the relevant territorial tax offices. According to the author, this would increase interest in such investments.
4. Increase the intensity of educational campaigns through spots broadcasted in mass media, including the involvement of church institutions in the campaign.
5. It is necessary to consider organizing training sessions and informational campaigns focused on risk minimization related to the periodic inspections of technical installations operating in buildings, training on the use of portable fire extinguishing equipment, and the principles of operating autonomous sensors detecting fire hazards or carbon monoxide release, including ensuring financial support from state institutions.

4. Conclusions for Fire Safety in Residential Buildings Based on Research

The analysis of the condition of technical installation inspections, based on buildings destroyed by fire, reveals significant shortcomings in prevention and fire protection. The research findings clearly confirm that technical installations in residential buildings are, in the vast majority of cases, not subjected to mandatory technical inspections and proper maintenance, which consequently has a significant impact on the safety of the residents. Despite the growing public awareness of fire hazards, many residential units remain inadequately protected. Introducing stricter regulations regarding mandatory inspections of technical installations, incentives from the Government of the Republic of Poland, and increasing educational efforts could contribute to improving the current situation. In summary, ensuring effective fire protection requires both appropriate legal regulations and greater involvement from both the Polish state and residents in applying safety measures. Increasing the number of buildings where regular technical inspections of utility installations—potential fire causes—are conducted can realistically reduce the number of tragic incidents and material losses caused by fires.

I. Fire prevention
1. Designing residential buildings in accordance with applicable fire safety standards reduces the risk of fires.
2. Regular inspections of electrical and heating installations, which are key aspects of fire prevention in residential buildings.
3. The obligation to use smoke and carbon monoxide detectors in apartments improves the safety of residents.

II. Detection and alarm systems
1. The installation of alarm systems in residential buildings, including multi-family dwellings, enables a quick response in the event of a fire.
2. Smoke detectors in single-family homes allow for early fire detection, enabling timely defensive actions.
3. Carbon monoxide detection systems in apartments equipped with solid fuel and gas heating devices protect against poisoning.
4. Integrated fire monitoring systems in multi-family residential buildings enable faster emergency response by rescue services.

III. Evacuation routes
1. Proper design and maintenance of evacuation routes in residential buildings, including multi-family ones, is crucial for the safety of residents.
2. Regular evacuation drills increase residents' readiness to act in emergency situations.
3. Blocking emergency exits and storing bulky items in stairwells pose a life-threatening hazard to residents.
4. High-rise residential buildings require additional evacuation measures, such as fire elevators or external staircases.

IV. Education and awareness of residents
1. Educating residents about fire safety principles is a key element of prevention.
2. Children and elderly people require special education regarding behavior during a fire.
3. Social campaigns about fire safety help increase awareness of hazards.

Bibliography

1.Zintegrowana Platforma Edukacyjna Ministerstwa Edukacji Narodowej, Czad- zagrożenia, https://zpe.gov.pl/a/wlasciwosci-tlenku-weglaiv/DhbJALC4k. Dostęp z dnia 20.01.2024r.
2. Komenda Główna PSPS Statystyka Interwencji za lata 2018
2024r.https://www.gov.pl/web/kgpsp/statystyczne-podsumowanie-2024-roku za https://fgsystems.pl/blog/pozary-w-polsce-podsumowanie-2024-r.htm. Dostęp z dnia 20.01.2024r.
3. S. Bałuszyński, Ustalenie przyczyn i okoliczności powstania pożaru na zlecenie organu procesowego Komendy Powiatowej Policji , Zakopane 2023 -10923/24 s.7
4.S.Bałuszyński, Bezpieczeństwo pożarowe. Technologie pożarowe, Materiały dydaktycznej dla studentów inżynierii bezpieczeństwa UKEN, Kraków 2023, s.4
5.J. Zboina, Bezpieczeństwo pożarowe Rozważania na gruncie prawa i praktyki Józefów 2018, s.11.
6. Ustawa o ochronie przeciwpożarowej z dnia 24 sierpnia 1991 r., tj. Dz. U. z 2024 r. poz. 275.
7. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. z 2023, poz. 822 i 2024 poz. 1716).
8. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 1999 r. w sprawie warunków technicznych użytkowania budynków mieszkalnych (Dz.U. 1999 nr 74 poz. 836 ze zm).

Electromagnetic support using software-defined radio

Ivan Ivanov , Sevdalin Spassov
Bulgarian Defence Institute Sofia, Bulgaria
i.p.ivanov@di.mod.bg, s.spasov@di.mod.bg

Abstract: *The essence and main characteristics of Electromagnetic Support (ES) are examined, as well as its place in Electromagnetic Warfare (EW). The main elements of ES such as electromagnetic reconnaissance, direction finding and threat warning are examined. A definition and basic terms for software-defined radio (SDR) are given. The architecture and main characteristics of SDR are examined. Has been made a prototype of SDR used in electromagnetic support.*
Keywords*: ELECTROMAGNETIC WARFARE (EW), ELECTROMAGNETIC SUPPORT (ES), DIRECTION FINDING (DF), SOFTWARE-DEFINED RADIO (SDR), GNU RADIO - THE OPEN SOURCE SDR DEVELOPMENT ENVIRONMENT*

1. Introduction

The first decades of the 21st century do not differ significantly from the last decades of the last century – new ones are emerging and a large number of old, smoldering ones continue. A wide variety of means of warfare are used in these conflicts. Classical systems and means of fire destruction, such as artillery and missile systems, together with small arms remain the main means of warfare. However, along with them, a number of systems and means of destruction of the enemy's electronic equipment are increasingly being used. This is quite natural, because the opposing forces used their best communication systems. During this time, the most powerful armies continue to dominate the electromagnetic spectrum over opponents who do not have the ability to challenge their technological superiority. However, in recent years, some of the regional powers have demonstrated great capabilities in hybrid operational environments, including in the electromagnetic spectrum. These capabilities are also being demonstrated in the ongoing conflict in Ukraine in the form of jamming communications, the global navigation satellite system (GNSS), and the control systems of military drones.

Systems and means designed to defeat enemy electronic equipment belong to the arsenal of the electromagnetic warfare (EW). Since most modern military equipment uses electronic devices and systems, their defeat is becoming an increasingly important and responsible task in the course of combat operations. EW refers to military actions involving the use of electromagnetic and directed energy to provide situational awareness and achieve offensive and defensive results, and ensure superiority in the electromagnetic spectrum [1, 2]. This leads to the conclusion that in modern conflicts of medium and high intensity, electromagnetic warfare is one of the main areas of combat operations.

2. Materials and Methods

2.1. Electromagnetic Support as an element of the Electromagnetic Warfare. Essence, tasks and basic elements of Electromagnetic Support.

1) Electromagnetic Support (ES) as an element of the Electromagnetic Warfare

Electromagnetic Warfare [3-5] consists of three main elements: Electromagnetic Attack (EA), Electromagnetic support (ES) and Electromagnetic Protection (EP). These three elements are inextricably linked, as they are mutually dependent and are applied in a certain sequence. For example, information about the parameters of radio signals and the location of enemy radio assets, acquired by electromagnetic support, is used to synthesize jamming signals emitted by the transmitters of the electromagnetic attack.

Electromagnetic attack includes actions to prevent or reduce the effective use of the electromagnetic spectrum by the enemy through the use of electromagnetic energy. Electromagnetic attack consists of three main elements: electromagnetic jamming (EJ), electromagnetic deception (ED) and electromagnetic neutralization (EN).

Electromagnetic Protection (EP) is a complex of technical and organizational measures using electromagnetic energy to provide protection and effective use of the electromagnetic spectrum by allied forces, carried out in order to ensure the stable operation of their own systems and means of controlling troops and weapons, in conditions of electronic effects from the enemy. Electromagnetic protection is divided into active and passive.

Electromagnetic support (ES) is a component of electromagnetic warfare, which includes actions to search, intercept and identify electromagnetic emissions and locate their sources, in order to immediately recognize the threat and build situational awareness [6]. The essence and the main features of ES are discussed further.

Тази информация се използва след това за започване на двата основни процеса, показани на фиг.1. Conducting EW, during the course of the operation, usually begins with basic electromagnetic support (ES) actions such as: electromagnetic reconnaissance of the main parameters of transmitters (Electromagnetic Reconnaissance), direction finding of opponent's transmitters (Direction Finding), and threat warning (Threat Warning) – if one exists. This information is then used to initiate the two main processes shown in Fig. 1.

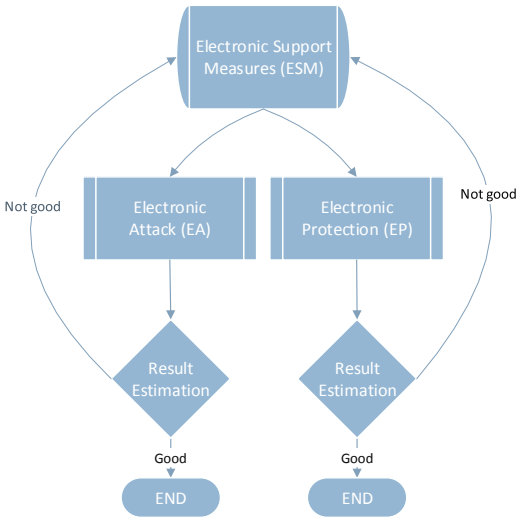


Fig. 1. *EW processes in the course of the operation*

The first process is related to electromagnetic attack actions and is depicted on the left side of the figure. It uses the results of electromagnetic support actions. After the basic parameters of the enemy emission sources are known and their direction is determined, electromagnetic attack (EA) actions follow such as emission of interference, electromagnetic deception actions or electromagnetic neutralization. The next step in this cycle is to evaluate the results of the electromagnetic attack and if they satisfy the set task, the execution of the process is stopped. If the results do not satisfy the set task, the process starts over with electromagnetic

reconnaissance. This process is repeated cyclically until the set EA task is fulfilled.

The second process is depicted on the right side of the figure and again begins with the execution of the three main actions of electromagnetic support (ES). As a result, the main parameters of electromagnetic interference emitted to our radio equipment by the adversary are determined and a decision is made on electromagnetic protection (EP). Then the selected electromagnetic protection measures are implemented, such as: control of own emissions (Emission control), reduction of own emissions (signature) in different frequency ranges of EM waves (Electromagnetic masking) or increasing the resistance to interference of own radio equipment (Electromagnetic hardening). The next step in this process is the evaluation of the results of electromagnetic protection (EP) and if they satisfy the set task, the execution of the process is stopped. If the results do not satisfy the set task, the process starts over with electromagnetic reconnaissance. This process is repeated cyclically until the set task of electromagnetic protection is fulfilled.

2) Essence, tasks and basic elements of Electromagnetic Support

Essence of the Electromagnetic Support

Electromagnetic Support (ES) is a branch of electromagnetic warfare, involving actions assigned by or under the direct control of the operation commander to search for, intercept, identify, and/or locate sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conducting future operations [2]. It provides a source of information necessary for immediate decision-making for electronic countermeasures and other tactical actions.

The main tasks of electromagnetic support are commanded by the operation commander and include performing some of the electromagnetic reconnaissance activities, direction finding of electromagnetic radiation sources and warning of electromagnetic threats.

Basic elements of Electromagnetic Support

The main elements of electromagnetic support are determined by its main tasks and include (Figure 2):

a) Electromagnetic Reconnaissance (with a limited scope of activities) including the following tasks:
- ✓ detection;
- ✓ assessment of basic parameters of electromagnetic emissions such as carrier frequency (or bandwidth/hopping), type of modulation, pulse sequence parameters (if pulse signals) and others, if necessary.

b) Direction finding to determine the following parameters:
- ✓ bearing;
- ✓ elevation;
- ✓ position determination (if necessary and using a multi-position ES system).

c) Electromagnetic Threat Warning:
- ✓ determining the type of electromagnetic radiation (classification);
- ✓ identification of sources of electromagnetic radiation (if sufficient information and time are available to do so);
- ✓ warning of imminent or potential threat.

d) Electromagnetic Warfare Reprograming.

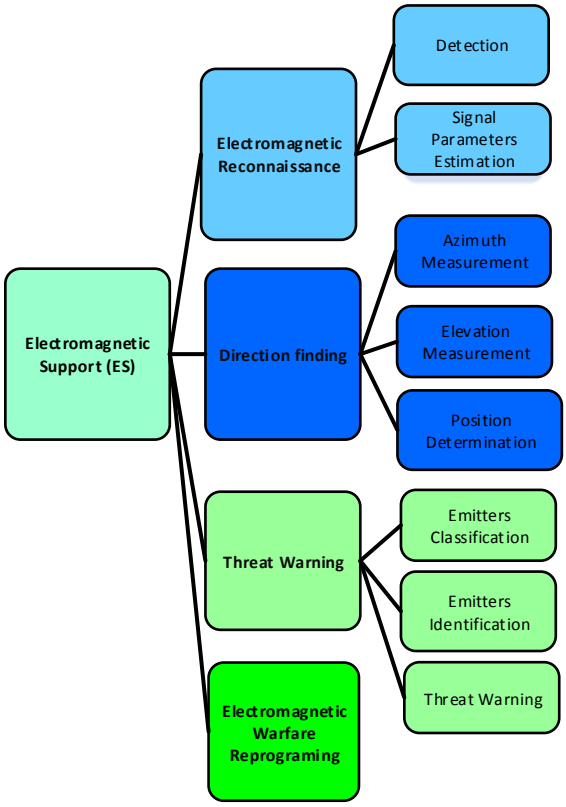


Fig. 2. *Components of Electromagnetic support*

The process of Electromagnetic Warfare Reprograming has been included as a new element of the electromagnetic support. Electromagnetic Warfare Reprograming is the deliberate alteration or modification of electromagnetic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. [6]. Several types of changes constitute EW reprogramming. These changes fall into three major categories of EW reprogramming. They are:

- ✓ Tactics. Include changes in procedures, equipment, settings, or EW systems mission-planning data. These changes are usually conducted at the Service level and implemented at the unit level using organic personnel and equipment.
- ✓ Software. Include changes to the programming of computer-based EW and target sensing software. This type of change requires software vendors to alter programmed look-up tables, threat libraries, or signal sorting routines.
- ✓ Hardware. Hardware changes or long-term system development are necessary due to tactics and software changes installed to resolve deficiencies. These changes usually occur tactical, and software changes are of such complexity that it requires hardware modifications or upgrades.

The goal of Electromagnetic Warfare Reprograming is to maintain high efficiency of one's own electromagnetic warfare activities. These basic activities are carried out for the purpose of immediate threat recognition, target designation, planning and conducting electromagnetic countermeasures during the operation. In this way, ES contributes to the implementation of electromagnetic countermeasures and the creation of an electronic battle formation. Since modern operations are dynamic and fleeting, the above-mentioned basic ES activities are carried out for a relatively short time of the battle (operation). In addition, for the purpose of timeliness and effectiveness of ES and EA, the volume of activities is limited. For example, they measure only the basic parameters of electromagnetic radiations sources such as frequency and type of modulation, and only the bearing is determined, not the exact location.

From all that has been said so far, it follows that ES has two main features:

- ✓ short-term – only for the battle (operation) duration;
- ✓ limited scope of activities.

It is precisely these two main features of ES that distinguish it from electromagnetic intelligence, which has a much wider range of activities and it is carried out over a longer period of time.

It is necessary to receive, digital process, analyze and storage of radio signals in a wide frequency range when conducting electromagnetic warfare. In addition, in order to be able to conduct electromagnetic support, it is necessary to perform electromagnetic reconnaissance, determine the main parameters of the intercepted signals and measure the directions to the sources of these emissions. All technical activities such as reception, digital processing, analysis and synthesis of signals can be performed using software-defined radio [7] (SDR).

2.2 General information about software-defined radio (SDR)

Software-defined radio is a modern paradigm for the practical implementation of radio communication systems. The foundations of the "software-defined radio" (software-defined radio - SDR) paradigm are associated with the research of DARPA and the US Air Force under the SpeakEasy project in the early 1980s on the creation of a prototype radio station covering the range from 2 MHz to 2 GHz and implementing about 10 communication standards [8]. Part of the results obtained in the field of system architecture were published by Mitola in the early 1990s, where the author [9] introduced the concepts [10] "software radio" and "software-defined radio" [11].

Each professional organization attempts to define a common framework of terms and definitions to allow for easy communication among professionals working in a common field. In the field of software-defined radio communications, the Institute of Electrical and Electronics Engineers (IEEE), through its working group P1900.1, has created definitions (Table 1) to ensure that everyone in the field has a common terminology [12]. A key definition in this brief ontic is that of "software-defined radio": a radio in which some or all of the physical layer functions are software-defined.

Table 1: *Ontic of concepts in the field of software-defined radio communications*

Concept	Definition
Radio	1. A technology for the wireless transmission or reception of electromagnetic signals enabling the transfer of information. 2. A system or device incorporating technology as defined in (1). 3. A general term applied to the use of radio waves.
Radio Node	A radio point of presence, including a transmitter and/or receiver.
Software	Modifiable instructions executed by a programmable processing device
Physical Layer	The layer within a wireless protocol that processes radio frequency (RF), intermediate frequency (IF), or baseband signals, including performing channel coding. It is the lowest layer of the 7-layer ISO model adapted for wireless transmission and reception.
Data Link Layer	The protocol responsible for the reliable transmission of frames over a wireless link by using appropriate error detection and control procedures and media access control.
Software Controlled	Software control refers to the use of software processing in the radio system or device to select operating parameters.
Software Defined	Software-defined refers to the use of software processing in the radio system or device to perform operational (but not control) functions.
Software Controlled Radio	A radio in which some or all of the physical layer functions are software controlled.
Software-Defined Radio	**A radio in which some or all of the physical layer functions are software defined.**
Transmitter	Equipment producing radio frequency energy for radio communication purposes.
Receiver	A device that receives a radio signal and provides information extracted from it.
Air Interface	A subset of waveform functions designed to establish communication between two radio terminals. This is the equivalent of the wireless physical layer and wireless data layer waveforms.
Waveform	1. The set of transformations applied to the information to be transmitted and the corresponding set of transformations to convert the received signals back to their information content. 2. Representation of the signal in space. 3. Representation of the transmitted radio frequency signal plus additional radio functions, including all network layers.

The definitions introduced allow not only to standardize the concept of SDR, but also to create a context in which this concept "lives". This allows the formation of other contexts in which SDR can be attributed to different entities.

A structural-functional block diagram of such a radio is shown in Fig. 3.

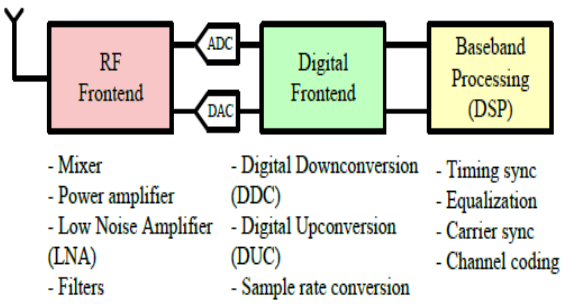


Fig. 3. *Software-defined radio architecture*

One of the main differences between the architecture of a software-defined radio and an ideal one is the presence/need of a radio frequency front-end operating in the analog space and implementing such functions as mixing, low-noise amplification, analog filtering, etc. Another architectural feature of modern SDRs is the implementation of digital processing by two digital blocks – a

digital front-end and a baseband digital signal processing block. The first block performs all conversions from transmitted to baseband (and vice versa) and those related to the clock frequency (frequency compression, expansion, etc.). The second block performs all conversions to baseband and is typically implemented by a general-purpose computer or a single-board microcomputer.

Typically, in current products on the market that allow experimentation and prototyping in the field of SDR, the analog RF front-end, ADC, DAC and digital front-end are combined into a common building block – RF digital front-end. This leads to the generalized, mass, modern SDR architecture shown in Fig. 4.

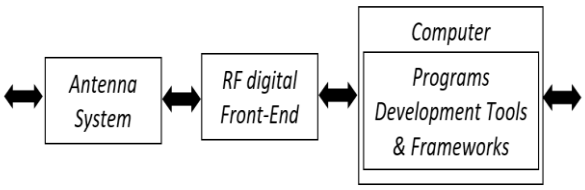


Fig. 4. *Generalized mass architecture of SDR*

The main characteristics of popular radiofrequency front-ends used to build SDRs are summarized on the Table 2.

Table 2: *Main characteristics of popular radiofrequency front-ends used to build SDRs*

Plat-form	Frequ-ency range	Channel band-width	Digital conver-ters bit resolution	Digital interface	Radio channel number
Hack RF One	10 MHz - 6GHz	20 MHz	8 bit	USB 2.0	1 Rx/1 Tx
Adalm PLUTO	325 MHz - 3.8 GHz	20 MHz	12 bit	USB 2.0	1 Rx/1 Tx
Ettus B210	70 MHz - 6 GHz	56 MHz	12 bit	USB 3.0	2 Rx/2Tx
Ettus N210	10 MHz - 6 GHz	40 MHz	14-bit ADC 16-bit DAC	1G Ethernet	2 Rx/2Tx
Ettus X210	50 MHz - 2,2 GHz 400 MHz - 4.4 GHz 1.2 GHz - 6 GHz	120 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 R x
Ettus X310	10 MHz до 6 GHz	160 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 Rx
Lime SDR	100 kHz - 3.8 GHz	61.44 MHz	12 bit	USB 3.0	6 Rx/4 Tx
Pico SDR	70 MHz - 6 GHz	56 MHz	12 bit	PCIe	4 Rx/4 Tx 8 Rx/8 Tx
RTL-	24 – 1766	3.2 MHz	8 bit	USB 2.0	1 Rx
SDR	MHz	(2.4 MHz typical)			

The analysis of the data in Table 2 shows the availability of capabilities for supporting a wide frequency range – part of HF, VHF and UHF, a wide bandwidth of the processed radio channel – up to 120 MHz, high data exchange speed with computer platforms – up to 10 GBit/s, support for multiple coherent radio channels, etc. These characteristics allow the implementation of technologies such as GSM, LTE, DVB, FMCW Radar, MIMO, etc. The SDR technology is supported by numerous software packages for computer modeling and simulation. The most famous of them are: Matlab, GNU Radio, LabVIEW, etc. The advantage of using such packages is the rapid transition from a computer module to a practical implementation.

3. Results and discussion

3.1. Usage of SDR as a tool for Electromagnetic Reconnaissance

A basic use case for SDR is monitoring frequency bands intended for national security purposes, such as VHF (30-88 MHz) or UHF (230 – 400 MHz). The analysis of the data in Table 2 shows the capabilities of commercially available mid-range RF front-ends for monitoring such frequency bands. There are many open source applications that allow monitoring of the frequency spectrum, compatible with different RF front-ends. Among the most famous are gqrx, SDR++, SDRAngel, openwebrx, gr-fosphor, etc.

Figure 5 shows a snapshot of the gqrx program working while monitoring the FM broadcast band status.

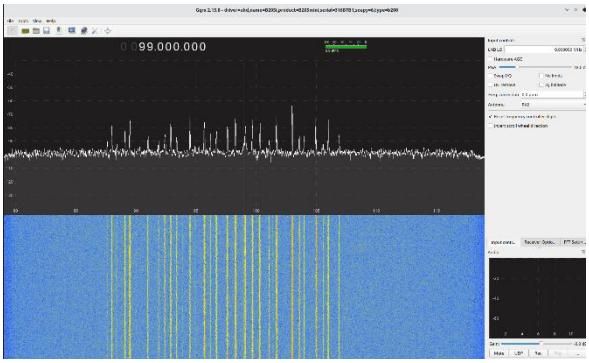


Fig. 5. *Snapshot of the gqrx program working while monitoring the FM broadcast band status*

In the upper box, a spectral diagram of the spectrum state is visualized, and below the spectrum is visualized through a waterfall diagram. The application allows manual modification of the operating frequency, the width of the frequency range for observation, a wide set of configuration parameters for the views, demodulation of FM signals, etc.

For cases where the instantaneous bandwidth of the RF frontend is not sufficient to monitor wider frequency bands, for example the entire NATO band IV (4.4 – 5.0 GHz), it is necessary to use several radio frequency modules in parallel or use one of them and a scanning program.

Figure 6 shows a structural view of the developed prototype of a software-defined scanning radio receiver for spectrum monitoring and control. The system architecture is according to Fig. 4 and consists of a general-purpose computer, the GNU Radio application framework, the USRP B210 radio frequency digital front-end and an antenna system. The technical capabilities of the specific RF front-end are given in Table 2, where they can be compared with

those of other similar products. The architecture of the SDR is flexible and allows the use of other RF front-ends supported by the application framework, as well as switching to other frameworks. Thanks to the SDR concept, the specific final functionality of the system is determined by the application developed in the GNU Radio environment.



Fig. 6. *A structural view of the developed prototype of a software-defined scanning radio receiver for spectrum monitoring and control*

Figure 7 shows an implementation of a software-defined scanning radio receiver for spectrum monitoring and control in the GNU Radio environment. Functionally, the application consists of an interface with an RF front-end, a user interface for managing control parameters, and a visualization.

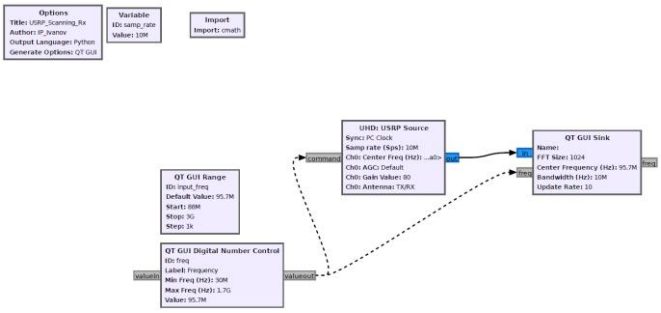


Fig. 7. *User application of a software-defined scanning radio receiver for spectrum monitoring and control in the GNU Radio environment*

The interface with the RF front-end is implemented by the USRP Source block. It is used to set such parameters as the operating frequency, sampling frequency, gain of the low-noise preamplifier, etc., as shown in Fig. 8. The block has an additional Command input, through which control parameters can be changed in run-time mode. The data on this input is formed by the Digital Number Control block. The QT GUI Range block provides a slider in the human-machine interface, through which the user can move along the frequency range

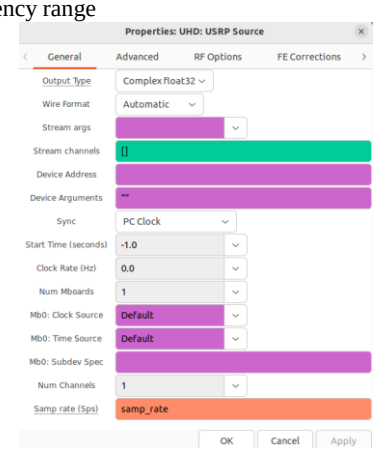


Fig. 8. *Menu screen for configuring the RF digital front-end via the USRP Source block*

The visualization of the output data of the USRP Source block is done through the QT GUI Sink. This block offers, through a tabbed menu selection, the display of the signal in the time, frequency and vector domains.

For cases where there is asynchronous information transmission, the detection of the moment of emission, estimation of basic parameters of the radio channel and, if necessary, recording of the radio signal are of interest. The SDR concept allows the development of devices with a convenient interface for programming this task. Fig. 9 shows a screen of an application running in the GNU Radio environment, including an energy detector and an estimator of the width of the radio channel. The detection level, the average operating frequency, the width of the observed spectrum, etc. parameters are configurable.

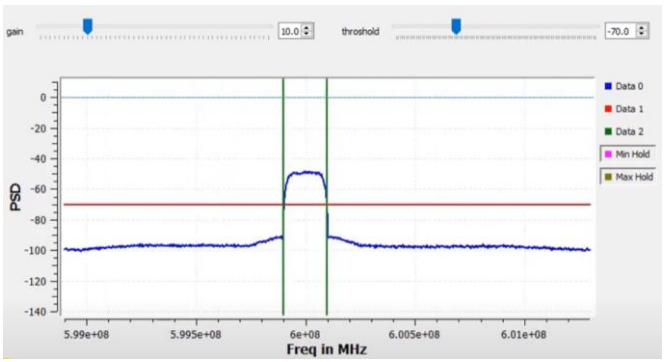


Fig. 9. *Screenshot of an application in the GNU Radio environment for Electromagnetic Warfare Reprograming.*

In case the Electromagnetic Reconnaissance object is a transmitter with a known radio protocol, then even with COMSEC measures applied, the SDR concept allows for monitoring of radio traffic and extraction of meta-information. Numerous applications are available for analysis of:

- 2G/3G4G/5G cellular systems – SRS RAN, gr-lte, Open5GS, OpenLTE, OpenBTS-UMTS, LTE-Cell-Scanner, etc.;
- wireless computer networks - gr-ieee802-11, grc-ieee802154, gr-lora, etc.;
- navigation systems - gr-air-modes, gr-ais, GNSS-SDR, etc.

One of the difficult computational tasks in Electromagnetic Reconnaissance is the classification of the observed radio channel and the identification of the protocol. To solve such a task, reverse engineering applications are available: Baudline, Inspectrum, Dspectrum, etc. Significant progress in solving this task has been made with the use of AI [13].

3.2. Usage of SDR as a tool for Direction Finding

The availability of multi-channel RF front-ends on the market makes SDR technology a convenient tool for solving the Direction Finding problem. One popular solution in this area is the KrakenSDR product, shown in Fig. 10. The architecture is based on the KrakenSDR RF front-end, a Raspberry PI single-board computer, and a general-purpose mobile phone/computer.

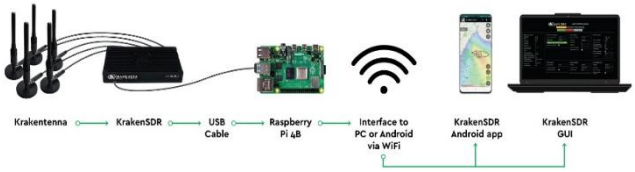


Fig. 10.: *Architecture of a multi-channel software-defined radio receiver with spatially distributed elements [14]*

Another SDR solution for Direction Finding is the GNU Radio add-on package – gr-aoa [15], which has developed a set of building blocks for developing an application for angle of arrival (AOA) estimation. Fig. 11 shows a view of the application using the Multiple Signal Classification (MUSIC) algorithm.

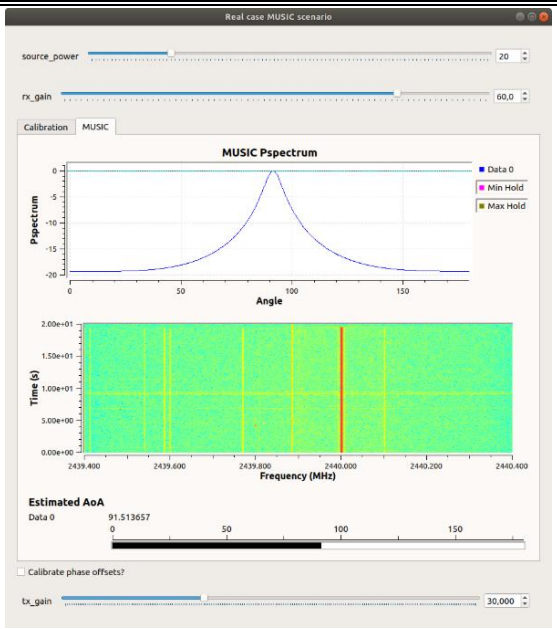


Fig. 11.: *Example of AOA estimation with usage of application gr-aoa*

The gr-aoa package also provides blocks necessary to provide phase synchronization of USRP devices.

3.3. Threat Warning and classification of electromagnetic emissions

The threat warning task includes electromagnetic reconnaissance broadcast recognition and their protocols. The presence of general purpose input/output (GPIO) ports facilitates application development for this purpose.

3.4. Electromagnetic Reprograming

The SDR architecture, in its fundamental essence, is based on the programming of functional elements and naturally helps to realize this doctrinal requirement.

4. Conclusions

SDR can be used as a tool to perform many of the tasks of Electromagnetic support.

One of the main use cases of SDR was demonstrated - monitoring of frequency bands intended for national security needs, for example in the VHF or UHF frequency ranges. Mid-range RF front-ends available on the market have capabilities for monitoring such frequency bands. There are many open source applications that allow monitoring of the frequency spectrum, compatible with various RF front-ends.

The availability of multi-channel RF front-ends on the market makes SDR technology a convenient tool for solving the Direction Finding task. For this purpose, ready-made products such as KrakenSDR can be used or other solutions such as the GNU Radio add-on package – gr-aoa, which contains many blocks for developing an application for estimating the angle of arrival (AOA).

The SDR architecture, by its fundamental nature, is based on the programming of functional elements and naturally facilitates the implementation of Electromagnetic Warfare Reprograming.

The Threat Warning task requires the recognition of emissions and protocols in Electromagnetic Reconnaissance. Measuring the parameters of electromagnetic emissions, recognizing their protocols, and automatically classifying them requires appropriate algorithms and a large amount of computing power. This is one of the directions for future work.

5. References

1. US Department of the Army, *Cyberspace operations and Electromagnetic Warfare FM 3-12*, (2021)
2. US Air Force, *Air Force Doctrine Publication 3-85, Electromagnetic Spectrum Operations*, (2023)
3. NATO, *Allied Administrative Publication AAP-6*, **p.93**, (2004)
4. NATO, Electromagnetic warfare, https://www.nato.int/cps/en/natohq/topics_80906.htm, (2023) (last visited 07.2025)
5. US Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations JP 3-85*, (2020)
6. S. Spassov, K. Paraskov, P. Kokudeva, J. Petrov, *Concept of use and operational requirements for passive defense software-defined radar systems, ARTDEF*, **p. II-105 – II-118**, (2023)
7. H. Pirayesh, H. Zeng, *Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey*, IEEE Comm. Surveys & Tutorials, **Vol. 24**, Issue: 2, (2022)
8. NATO, *Allied Joint Doctrine for Electronic Warfare AJP-3.6*, (2020)
9. R. Lackey, D. Upmal, *"Speakeasy: The Military Software Radio"*, IEEE Comm. Mag., (1995)
10. J. Mitola III, *"Software Radios: Survey, critical evaluation and future directions"*, IEEE Aerosp. and Electr. Syst. Mag.,**Vol. 8**, Iss. 4, pp. 25, (1993)
11. J. Mitola III, *"The Software Radio Architecture"*, IEEE Comm. Mag., pp. 26–38, May (1995)
12. A. Margulies, J. Mitola III, *"Software Defined Radios: A Technical Challenge and a Migration Strategy"*, Proc. of the IEEE 5th Int. Symp. on Spread Spectrum Technologies, pp. 551–556, Sept. (1998)
13. Y. Sun, W. Wu,, *Survey of Research on Application of Deep Learning in Modulation Recognition*, Wireless Pers. Comm., **133 (3), pp. 1483–1515**, (2023)
14. *KrakenSDR. A phase-coherent software-defined radio with five RTL-SDRs*, https://www.crowdsupply.com/krakenrf/krakensdr (last visited 07.2025)
15. https://github.com/MarcinWachowiak/gr-aoa (last visited 07.2025)

Application of a Cyber Training Ground as a Solution for Training Cybersecurity Specialists to Ensure the Functionality of the National Situation Center and Crisis Management Center

Veselina Gagamova[1,*], Elitsa Pavlova [2], Violeta Vasileva[3])
G. S. Rakovski National Defence College Sofia, Bulgaria[1]
University of National and World Economy /UNWE/, Sofia, Bulgaria[2]
Future Innovation Labs[3]

v.gagamova@rndc.bg, epavlova@unwe.bg, violetta.ziv@gmail.com

Abstract: *Cyber education is one of the global challenges in recent years. Attacks are becoming increasingly sophisticated and ensuring a safe working environment is difficult. Hyper-realistic virtual environments, called cyber training grounds, help to raise the level of cybersecurity training. The report analyses applicable methods, software and implemented solutions, which are cyber training grounds. The purpose of the study is to outline the types of cyber training grounds and their characteristics, functionalities and requirements for training through a cyber training ground, according to EU regulations, with the aim of applying them as a solution for training cybersecurity specialists to ensure the functioning of the National Situation Center and Crisis Management Center*.
Keywords*: CYBER TRAINING GROUNDS, CYBER SECURITY LABORATORY, ARCHITECTURE, CYBERSECURITY TRAINING*

1. Introduction

Cyber training grounds are one solution for training cybersecurity professionals to ensure the functionality of the National Situation Center (NSC) and Crisis Management Center (CMC). Whether it's simulations, competitions or labs, cyber training grounds visualize what students are learning in theory. "It's this virtual environment where you can practice skills and simulate attacks safely," says Rebecca Michael, executive director of Ohio Cyberspace, University of Cincinnati. Once basic skills are acquired, students can use simulations to not only focus on penetrating systems, but also be prepared to defend themselves against such attacks.

The study "Cyber Ranges and test platforms for education, training and research"[1] shows that most cyber training grounds are used for research, training and exercises. Security challenges are SQL injection, malware analysis, risk management, information security economics, IT governance.

The purpose of this report is to create a conceptual model (CM) that will be used as a tool for developing interactive approaches for training cybersecurity specialists to ensure the functioning of the National Situation Center and Crisis Management Center. The main users may be students studying in specialties related to the field of IT and cybersecurity, as well as employees holding leadership positions in important structural units. The study is based on various approaches to e-learning.

The implementation of new approaches in training, information exchange and teamwork will improve and transform all processes and services in training cybersecurity specialists to ensure the functioning of the National Situation Center and Crisis Management Center. The need for trained people, by combining practical experience with educational courses and cybersecurity competitions, continues to outstrip supply.

The literature search covers the databases of Science Direct, Springer, MDPI, IEEE Explore, Wiley, Research Gate, Google Scholar, as well as previous studies and related research projects, with the aim of identifying the main characteristics of cyber training grounds. The focus is on the most recent publications, with an emphasis on those from the last five years. The keywords used for the search are cybersecurity training, cyber training grounds, cyber laboratory.

The Cyberspace Federation project aims to build a cyberspace across the EU. The ECHO project, launched by the European Commission, has the vision of creating and managing a network of competence in the field of cybersecurity. The construction of a Cyber Range depends on design features such as flexibility, scalability, isolation, interoperability, efficiency, service-based access and risk assessment. Examples of successfully used Cyber Ranges are KYPO Platform, TELECOM Nancy, RISE, Airbus, RI CODE, Virginia.

2. The Essence of Cyber Range

A review of existing definitions identifies two ways to define a cyber training ground, as a simulation environment and as a platform. A simulation environment is defined in a static way because it is designed to meet specific use cases and requirements. A platform is defined as a group of technologies that are used as the foundation for other applications and processes. This view of a cyber training ground is more dynamic because there are different functionalities in using the simulation environment.

Cyber training grounds are used as a safe place to train through exercises and test employees on how to respond to cyber-attacks. Training includes simulations of secure software, risk assessment, incident management, social engineering, and network attacks.

According to the National Institute of Standards and Technology (NIST)[6], Cyber polygons are defined as interactive systems, tools and applications. They provide a safe environment for gaining practical experience and can operate independently or with other cyber polygons, supporting certain network services. In the Cybersecurity Guide, cyber polygons are described as "tools for simulating possible attacks against IT infrastructure, networks, software platforms, applications, firewalls and other [2].

The European Cybersecurity Organization provides an overview of hyper realistic virtual platform, focusing on their functionalities and capabilities, the technologies used for development, and the limitations of their integration [5]. The organization characterizes Cyber platforms according to different types of users: institutions, security professionals, military agencies, security operations centres, educators, students, researchers, etc. A study "Cyber Ranges and Security Testbeds" defines a taxonomy that includes their capabilities, functions, scenarios, tools, and architecture [8].

According to the report "The Spider Cyber Range", the type of Cyber Range is determined by its goals and the roles that participants adopt [7]. Cyber Ranges can be used for security research, testing, and certification, security training and competency building, and national and international cybersecurity competitions. Educational and certification courses require instructors and cybersecurity experts to conduct cybersecurity courses. The role of instructors is to monitor the efforts of learners and intervene when learners are struggling. The role of cybersecurity experts is to perform technical tasks, such as configuring, infrastructure, debugging, and injecting vulnerabilities. Participants in different courses may assume different roles, working individually or in

teams. The development and operation of Cyber Ranges require significant resources in terms of funding, skilled people, and working time [5].

Technical requirements - applicable methods, software and implemented solutions:

- Tools for various security testing techniques
- Simulation environment of high-scale scenarios with support for various IoT devices with different technical characteristics.
- Tools to support modelling and risk assessment.
- Automated security-testing tools.
- Network tools for packet sniffing and port analysis.
- Attack simulation.
- Intrusion detection and monitoring tools.
- Common cryptographic and protocol libraries.
- Specific tools for programming IoT devices.
- Tutorials and guides for using the tools.
- Debugging environment

Requirements for the communication equipment on which the exercises are conducted or which is used as an environment for the exercises:

- Resilience to maintenance failures.
- Encrypted communications.
- Lifecycle support, including software updates and patches.
- User accounts.

Some of the requirements for executing the attacks used in the work environment include automated execution and detailed reporting of the attack results. Requirements for the personnel who plan and execute the exercises include good knowledge of security testing and assessment and common attacks.

3. Cyber Range Architecture

Hyper realistic virtual platforms can be classified into three main categories according to their technical characteristics. Simulation platforms use software tools to form the Cyber Range network without the need for physical network equipment. These systems are scalable and flexible. Overlay Cyber Ranges operate on physical network devices and computing equipment. They provide greater accuracy than simulation Cyber Ranges but involve hardware costs and possible changes to the existing infrastructure. Emulation mimics the physical infrastructure of specific business networks, providing a high level of realism and repeatability of performance. They can usually be optimized by sharing resources and using virtualization technologies.

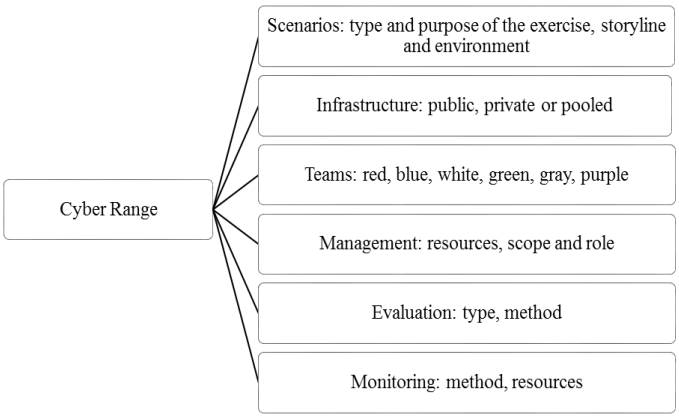
The infrastructure encompasses all physical and virtual hardware and software resources used in the development of the platform. Infrastructure elements include the physical layer, cloud, virtualization and isolation. Cyber platform implementation can be implemented through a public cloud, private cloud or hybrid model. In the public cloud, the management of the infrastructure is entirely performed by the cloud service provider, and users receive access to services without commitment to infrastructure management. A private cloud provides complete control and privacy over applications and data stored in the cloud infrastructure. A hybrid cloud infrastructure combines control over data security with infrastructure scalability.

Virtualization allows for the dynamic allocation of computing resources to virtual machines, as well as the reconfiguration and reconfiguration of the network infrastructure. Isolation means separating projects and exercises from the operating system, virtual machines, and containers running on the same hardware. For security and control, projects must be isolated from external networks and systems.

Davis and Magrath's study shows the available options for building and managing Cyber Ranges [4]. Researchers categorize Cyber Ranges as simulations using software models of real-world scenarios, overlays if they use real-world production equipment and emulations if they run real-world applications on separate equipment. Cyber Ranges can be classified based on their infrastructure – public (e.g. CISCO), private, or federal (e.g. Cyber Ranges such as CRD, CRATE, NATO, and Raytheon).

Hyper realistic virtual platform can be implemented on an infrastructure that uses multiple networks with different topologies, computers, and other devices. The infrastructure consists of the physical layer (workstations, servers, mobile devices, network devices, operating systems, database management systems, etc.), cloud computing technologies, virtualization technologies, and isolation technologies that enable a fully configurable and integrated environment. Cyber Range policies can include rules that prohibit specific tools, techniques, and activities, such as attacking the workspace and platform.

The study „Cyber Ranges and Security Testbeds" identifies the architecture [8]. The architecture shown in Fig. 1 and includes scenario, infrastructure, teams, management, evaluation, monitoring. The scenario unites the type and purpose of the exercise, the storyline and the environment in which it is conducted. The selection of teams depends on the scenario. Management includes resources, scope and role. All areas of the architecture are consistent and interconnected.



.

Fig. 1 *Cyber Range Architecture.*

Source: Cyber Ranges and security testbeds: Scenarios, functions, tools and architecture [3].

The proposed architecture of the Cyber Range includes a working platform, user interface, scenarios, projects and infrastructure. The user interface forms a realistic cyberspace consisting of real devices and virtual machines. The scenarios involve developing the workspace and defining the objects describing the elements, as well as the conditions and vulnerabilities that need to be included. The scenario defines the steps that the participants must follow to complete the exercise. Teamwork is extremely important to evaluate the attack scenarios in real conditions.

4. Conclusion

In conclusion, it can be summarized that in the conditions of escalating and increasingly sophisticated cyber threats using cloud technologies and collaborative systems with applications in the defence of the state and the security of society, the need for effective and sustainable solutions for training cybersecurity specialists is gaining critical importance. The analysis showed that

hyper realistic virtual environments are a strategic tool for building knowledge, skills and operational readiness, consistent with European regulatory requirements. The studied types of Cyber Ranges, their functionalities, architecture and organizational requirements prove that their implementation in the training of personnel is a key factor for the effective functioning of the National Situation Center and the Crisis Management Center. In this context, Cyber Ranges not only help to improve the quality of training, but also ensure technological superiority and sustainable protection of critical infrastructure in the face of global challenges.

Acknowledgements

This report was written thanks to funding from the Ministry of Education and Science in implementation of the National Strategy for Research Development 2017-2030 under the National Scientific Programme "Security and Defence", adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

5. References

1. Chouliaras, Nestoras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. "Cyber Ranges and TestBeds for Education, Training, and Research." Applied Sciences 11 (February 2021): 1809. https://doi.org/10.3390/app11041809.
2. Cybersecurity Guide. "What Is a Cyber Range?" Accessed March 29, 2023. https://cybersecurityguide.org/resources/cyber-ranges/.
3. CYBERWISER.Eu. "Cyber Range & Capacity Building in Cybersecurity." 2025. https://cyberwiser.eu/.
4. Davis and Magrath. "A Survey of Cyber Ranges and Testbeds." Semanticscholar.Org. https://www.semanticscholar.org/paper/A-Survey-of-Cyber-Ranges-and-Testbeds-Executive-Davis-Magrath/687ff7737f9e32b85cf885db88341b73892aa8ae.
5. ECSO. "European Cyber Security Organisation." ECSO. https://ecs-org.eu/publications.
6. paul.hernandez@nist.gov. "Cybersecurity." Text. NIST, June 30, 2016. https://www.nist.gov/cybersecurity.
7. Rebecchi, Filippo, Antonio Pastor, Alberto Mozo, et al. "A Digital Twin for the 5G Era: The SPIDER Cyber Range." Zenodo, March 11, 2022. https://doi.org/10.5281/zenodo.6347532.
8. Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture." Computers & Security 88 (January 2020): 101636. https://doi.org/10.1016/j.cose.2019.101636.

Smart contract in security

Nikolay Radulov, Teodora Lichev
New Bulgarian University
n.stefanov5@gmail.com, teodora_licheffa@abv.bg

Abstract: This comprehensive document explores the role and implementation of smart contracts in security systems, with particular emphasis on their application in law enforcement, intelligence, and counterintelligence operations. The analysis covers both theoretical foundations and practical applications within Industry 5.0 context.
Keywords: Blockchain; Smart contract, Intelligence; Security

1. Introduction

Smart contracts are self-contained computer programs that automatically execute, manage, or verify the terms of contractual agreements using blockchain technologies. Their significance in the context of Industry 5.0 and security is particularly important as they contribute to new norms of data protection and transparency in business operations.

Blockchain technology is the fundamental foundation for the functioning of smart contracts and offers numerous advantages and unique features that make these two concepts interconnected and complementary. In the following lines, we will examine the features, properties and specificities of blockchain technology that make it an ideal platform for the execution of smart contracts.

2. Features of blockchain technology

The blockchain functions as a single and reliable source of information with the following characteristics:

Decentralization:

Blockchain is a decentralized platform, which means that there is no single controlling authority. Instead, data and information are distributed across multiple nodes that interact with each other. Adding a piece of information requires all nodes on the blockchain to agree and approve it. This reduces the risk of manipulation and abuse due to the lack of central control.

Immutability

Once information is on the blockchain, it cannot be changed or deleted without leaving a trace, and without these changes being approved by all participants in the chain. Each block contains information about the previous block, making the system extremely resistant to attempts at manipulation.

Transparency

All transactions and operations performed on the blockchain are publicly available and visible to network participants. This provides a high degree of transparency, allowing anyone to track the history of transactions and smart contracts.

Cryptographic security

Blockchain uses cryptographic security methods, which increases the protection of data and transactions. Each block is provided with a unique hash, and the data in it is encrypted, which prevents unauthorized access and manipulation. A hash contains 64 characters and is a combination of 26 letters and 10 numbers.

3. Properties of Blockchain

- Auto-executed:

Smart contracts implemented on a blockchain platform work automatically if the specified conditions are met.

Intelligent contracts (also called smart contracts – from the English. Smart Contracts) are electronic contracts that are written in blockchain code and are based on the " if / when ... then ..." function

This means that under certain conditions, the contract automatically performs pre-set actions, without the need for human intervention.

- Proof of performance:

Every transaction and execution of smart contracts is recorded on the blockchain, providing conclusive proof of actions. This feature is of great importance for resolving disputes or verifying the legality of actions.

- Low cost and speed:

Process automation through smart contracts, combined with blockchain technology, can reduce execution costs and transaction processing times. Without the need for intermediaries, the costs of services related to bureaucracy and paperwork are significantly reduced.

4. Specifics of blockchain and smart contracts

Cross-vertical integration

Blockchain enables the integration of different sectors and industries, which provides flexibility in the application of smart contracts. They can be applied in a variety of areas — from financial services to supply management and healthcare.

Proof of authenticity

Blockchain ensures the integrity and authenticity of information. Every contract or transaction made on a blockchain is given a unique identifier that confirms its legitimacy. Once added to the blockchain, it is almost impossible for the information to be manipulated, deleted, or

Identity Management

Blockchain can be used for digital identity management, allowing participants in smart contracts to verify their identities without the need for centralized authorities. This provides advantages in terms of security and protection of personal and sensitive data.

Blockchain technology provides a solid foundation for the functionality of smart contracts, offering decentralization, immutability, transparency, and security. These properties and features make blockchain extremely suitable for integrating smart contracts into various industries and applications, with the potential to transform the way transactions and interactions between participants are carried out. The importance of blockchain for smart contracts cannot be underestimated, as it not only provides the necessary infrastructure, but also offers mechanisms for safe and trusted interaction.

5. Essence and content of smart contracts

Smart contracts, as mentioned above, operate on the blockchain, which allows them to be tamper-proof and offer a high level of security. They require predefined conditions, programmable in languages such as Solidity for Ethereum, which are automatically executed when certain criteria are met. The content of smart contracts usually includes logic that describes the terms of the transaction, what actions to take in different situations, and how the system should respond to changes.

Form

Smart contracts do not have a physical form, they are a complex of programmed codes located on the blockchain. This form provides not only security, but also decentralization, since the information cannot be changed from a central location. Any participant in the network can check the terms and status of the contract, ensuring transparency.

Opportunities

Smart contracts offer numerous security opportunities, including but not limited to:

- Automation: Processes become automated, which reduces the need for third-party intervention.
- Cost reduction: Removing intermediaries leads to lower operational costs.
- Increased security: The use of cryptography in blockchain technologies provides high data protection.

- Speed: Processes are performed in near real-time, which increases the efficiency of business practices.

Challenges and problems

Despite their many advantages, smart contracts also face several challenges:

- Legal and regulatory issues: The lack of a clear legal framework regarding smart contracts may be an obstacle to their widespread adoption.
- Technical barriers: Implementing complex smart contracts requires specialized IT skills, which can be a barrier for small businesses.
- Fault tolerance: If the terms of the contract are not properly programmed, they can lead to unintended consequences.

Efficiency

The effectiveness of smart contracts in Industry 5.0 is manifested by improving process transparency, accelerating transactions, and reducing costs. By optimizing operational activities, smart contracts enable the organization of activities based on real, verifiable data, thereby achieving sustainable business performance that meets the requirements of Industry 5.0 for sustainability and human orientation.

Smart contracts in the context of Security 5.0 present an innovative tool for managing business relationships and protecting data, significantly improving market dynamics, but also posing several challenges that require attention and resolution.

The use of smart contracts in the management of security services, such as the police, intelligence and counterintelligence, is an innovation that could lead to significant improvements in operational efficiency, transparency and security of information processes. In the following lines, we will examine how smart contracts can be integrated into these systems and what positive and negative effects they can have.

6. Smart contracts in the police

Automated data management: Police handle large amounts of information, such as reports and evidence. Smart contracts can be used to automate the storage, sharing, and verification of documents and data. Blockchain ensures the correct and secure digitization of inheritance records and registries. For example, when a new legal norm is implemented, smart contracts could automatically update databases and notify the relevant authorities.

Informant Contract Management: Police often work with informants who provide valuable information. Smart contracts can be used to formalize relationships with informants, providing automated payments for reporting important information. These contracts could include provisions to protect the anonymity and safety of the informant.

Regulating cooperation with other agencies: Smart contracts can define the terms of cooperation between different security services and international agencies. The parameters of cooperation, information exchange, and resource allocation can be strictly fixed and monitored through smart contracts.

7. Smart contracts in intelligence

Secure communication channels: Intelligence agencies work with sensitive information. Smart contracts can provide structured and encrypted channels for information exchange between agents, which would increase data security and reduce the risk of espionage, information leaks, or malicious actions.

Risk monitoring and assessment: Intelligence often involves threat and vulnerability assessment. Smart contracts can automate the process of collecting and analyzing risk data, providing intelligence officers with up-to-date and accurate threat data.

Systems Integration: Smart contracts can be implemented into various platforms and systems used by intelligence agencies to improve interaction and coordination between different divisions and services.

8. Smart contracts in counterintelligence

Automated identity verification: Counterintelligence needs to monitor and verify multiple identities. Smart contracts can be used to automate background checks, which would help prevent potential espionage threats.

Covert Operations Management: Smart contracts can automate projects and funding of covert operations, reducing the risk of exposure and abuse by providing detailed tracking of every phase of the operation.

Accountability and transparency: By implementing smart contracts in counterintelligence operations, accountability and the possibility of subsequent checks are ensured, useful for preventing abuse and illegal actions.

Challenges and problems

Despite the many advantages, the introduction of smart contracts in security services is accompanied by several challenges:

- Legal and ethical issues: The implementation of automated data management and action systems may encounter resistance related to legal regulations and data protection. Clear frameworks and guidelines are needed for the use of smart contracts in sensitive areas. The ultra-rapid development of technologies significantly exceeds legislative initiatives and frameworks to regulate their use.

- Technical hurdles: Integrating new technologies into legacy security systems can be challenging, especially when it comes to training employees and adapting existing infrastructure. Most information systems are built in a way that they are not compatible, and data migration is a challenge.

- Cybersecurity: Although blockchain provides a high level of protection, systems still remain vulnerable to attacks. The strength of smart contracts depends on the strength of the blockchain infrastructure and the network itself.

Smart contracts offer significant opportunities to enhance the efficiency and security of security services, but their implementation requires a careful balance between innovation, legal regulations and ethical considerations. The success of such initiatives will depend on active partnerships between technological companies, government institutions and public organizations aimed at building transparent and fair systems that support public safety and protection.

Management

Smart contracts offer a new, innovative approach to security management. By integrating blockchain technology and automating contractual relationships, these tools can significantly improve management efficiency in various areas, including policing, intelligence, and counterintelligence.

In the following lines, we will examine how smart contracts can be incorporated into every phase of the governance cycle, with particular emphasis on their specific application in the security sector.

Analysis

Analysis is a fundamental step in the management cycle, where current conditions, resources, and problems are assessed. Smart contracts can help in this phase by automatically collecting and processing data from various sources.

- Data collection: Smart contracts can automatically extract and analyze information from numerous databases, including information about previous cases, criminal records, and data from intelligence operations.
- Vulnerability Assessment: By analyzing live data, they can identify security vulnerabilities by automatically generating risk reports.

Forecasting

After analysis, the next step is to predict future trends and threats. Smart contracts can provide important information based on reliable data and algorithms.

- Threat Modeling: By applying algorithms and machine and deep learning, smart contracts can predict future threats and criminal activities based on historical data.

- Scenario planning: Automatic data processing can help in developing different threat scenarios, which will inform security management.

Decision making

Based on the analysis and predictions, the decision-making stage follows. Smart contracts can provide real-time information to facilitate the decision-making process.

- Objectivity in decisions: Smart contracts guarantee transparency and objectivity in decision-making, as all conditions and criteria are predetermined and clearly formulated.
- Automated solutions: Under certain conditions set in their programming, smart contracts can trigger certain actions themselves, for example, notifying the relevant authorities of attempted security breaches.

Planning

Planning is a critical stage for which smart contracts can provide significant added value.

- Strategic Planning: Smart contracts can be used to automate planning processes related to resource deployment, operations management, and conduct training modules.
- Budget Management: Through automated expense reports and commitments, smart contracts can improve financial planning by pragmatically determining the costs of various operations based on previous executions.

Organizing

Organizing resources and operations is key to the successful functioning of security services. Smart contracts can increase the efficiency of resource management.

- Resource Optimization: Smart contracts can automatically determine how and where to use available resources to achieve maximum efficiency.
- Coordination between teams: Smart contracts can automate communication and coordination between different departments and teams, providing a platform for information exchange while minimizing the risk of errors.

Control

Control is the final stage of the management cycle and is of utmost importance, especially in security management.

- Performance Monitoring: Smart contracts can track the execution of certain tasks and conditions, automatically providing reports on performance and regulatory compliance.
- Preventing violations: The control system, powered by smart contracts, can automate alerts when anomalies or unmet conditions are identified, allowing for rapid response from management.

The integration of smart contracts into security management offers unique opportunities to increase efficiency, transparency, and security. By automating key management functions, such tools can not only improve operational performance but also instill more trust in decision-making processes. Despite the prospects, it is important to put in place adequate legal and ethical frameworks to ensure that the implementation of smart contracts does not violate personal rights and good practices in the field of security.

Smart contracts a tool for humanity and ethics

Smart contracts can play a significant role in the implementation of special intelligence tools (SIPs), especially when it comes to ensuring legality and compliance with ethical standards. Through automation and transparency, they can help protect both citizens and security service personnel. In the following, we will examine how smart contracts can provide the necessary legal prerequisites for the use of special intelligence tools.

Determining the legal conditions

The smart contract can be programmed to contain specific details regarding the legal conditions required to activate the special intelligence tools. These conditions should include:

- Clear criteria: Defining specific cases in which SRCs can be used, such as the presence of evidence of serious crimes or threats to national security.
- Legal permissions: A smart contract may require prior approval from competent authorities (such as a court) before activating the SCC, ensuring legality.

Automate approvals

Smart contracts can automate the approval process by integrating mechanisms to verify legal conditions:

- Integration with legal databases: Smart contracts can connect to central legal databases to verify the availability of necessary permits and approvals in each individual case.
- Launch conditions: The smart contract can be structured to only start after validating the legal conditions, automatically recording the data integration.

Control and monitoring of implementation

Smart contracts offer mechanisms for control and monitoring during the implementation of special intelligence tools:

- Activity Tracking: Whenever CPCs are activated, the contract can record the time, method of activation, and subsequent usage, thus providing the necessary transparency and accountability.
- Notifications: The smart contract can automatically send notifications to responsible authorities and control institutions upon activation of the SRC, thus ensuring access to information and monitoring.

Conditions for termination of operations

The smart contract may also include mechanisms to automatically terminate SRC operations if certain conditions are not met or violated:

- Data analysis: The smart contract can analyze data in real time and terminate the operation if, for example, no suspicious activities are detected within a certain period.
- Reporting requirements: After termination of the operation, the smart contract can generate a report of the activities performed to be shared with the authorities responsible.

Protection of citizens and employees

Through the listed mechanisms, smart contracts serve as a protective barrier for both citizens and security service employees:

- Transparency and accountability: Ensuring monitoring and accountability prepares scenarios that show clear responsibility of employees for the implementation of the SRC, which reduces the risk of abuse. Smart contracts can perform routine processes in the work cycle and employees can concentrate on specialized and expert work.
- Legal protection for employees: Smart contracts provide protection for employees from unintentional violations of the law. In the event of an improper application of the SRC, the contract can provide evidence of the actions taken, including the time and conditions of activation.

Smart contracts offer an innovative solution for the legal and ethical application of special intelligence tools in the security sector. By automating legal conditions, dynamic risk assessment, and transparency of actions, they can ensure the protection of the rights of both citizens and employees. This automation creates a new norm of accountability and legal compliance necessary for the modernization of intelligence structures, strengthening public trust and the effectiveness of security services.

Smart contracts represent a key innovation that has the potential to support the realization of concepts such as humanity, ethics and human-centeredness in the context of Security 5.0. This new era of security emphasizes not only technology and automation, but also social responsibility and protection of individual rights. As a basis for smart contracts, we can consider the following aspects:

Humanity and protection of rights

Smart contracts offer mechanisms that protect citizens' rights and ensure that technological innovations in security are aimed at

ensuring the well-being of society. They can be programmed with extreme attention to ethical standards:

- Automation of Justice: Through smart contracts that automatically check legal requirements, violations of individual rights can be prevented. For example, the use of special intelligence tools (SIPs) can be automated and controlled in a way that ensures compliance with legal and ethical norms.
- Access to justice: Smart contracts can streamline processes and reduce the cost of legal services, which would allow more citizens to gain access to justice and legal protection.

Ethics in processes

Smart contracts can be programmed to follow specific ethical principles, which provide greater transparency and accountability in the management of data and resources:

- Transparency and accountability: Smart contracts offer an immutable record of action, always allowing for verification of the authenticity of the procedure. This is especially important in the security field, where unethical practices can lead to significant social and legal consequences.
- Consent and awareness: Through smart contracts, participants in the system can give consent to the processing of personal data, and contracts themselves can encrypt and protect data, ignoring consent whenever informational conditions are not met.

Human-centeredness and focus on the individual

At the heart of Security 5.0 is the concept of human-centricity, which puts individuals and their needs first. Smart contracts can play a critical role in this dynamic:

- Personalized Services: Smart contracts offer the opportunity to tailor individual services provided to citizens. For example, in public safety management, personalized smart contracts can reflect the needs of the respective community, ensuring more effective and targeted measures.
- Community engagement: Smart contracts can provide a platform for citizen participation in decision-making processes, giving them a voice and participation in the management of local security initiatives.

Sustainability and integrity

The resilience and integrity of systems in Security 5.0 can be strengthened through smart contracts that provide durable and sustainable solutions to security problems:

- Supporting sustainable development: Smart contracts can be programmed to implement sustainable development principles, such as managing security resources in a way that minimizes negative impact on the environment and society.
- Data integrity: By protecting data from manipulation and unjustified changes, smart contracts ensure the integrity of the information needed for security services to make informed decisions.

Conclusion

Smart contracts play an important role in promoting humanity, ethics, and human-centeredness in the Security 5.0 ecosystem. They offer mechanisms to protect citizens' rights, ensuring transparency and accountability, as well as the possibility of personalized and sustainable security management. The importance of these aspects is essential for building trust between citizens and government institutions and for creating safe and fair public systems. With the help of smart contracts, we can achieve a balance between technological innovation and ethical obligations to individuals and the community.

Literature

1. Личева, Т. „Сигурност на данните с блокчейн технологията" В. Сб. Док. от годишната научна конференция на ВТУ „Васил Левски" – 8-9 юни 2023 г., ISSN 2367-7481, с. 383
2. Личева, Т., Модерна сигурност в управлението, изд. 2023, НТС по машиностроене „Индустрия 4.0", ISBN 978-619-7383-30-0, с. 61
3. Радулов, Н., „Сигурност 4.0", 2019, изд. Научнотехнически съюз по машиностроене „Индустрия 4.0, ISBN 978-619-7383-15-7 стр.307-309
4. A Guide to Smart Contract Security, https://hedera.com/learning/smart-contracts/smart-contract-security
5. Blockchain-based smart contracts as new governance tools for the sharing economy, https://www.sciencedirect.com/science/article/abs/pii/S0264275121002250
6. How smart contracts will change the way the world works, https://www.deltacapita.com/insights/how-smart-contracts-will-change-the-way-the-world-works
7. Smart Contracts for Estate Planning and Administration, https://susqublockchain.medium.com/smart-contracts-for-estate-planning-and-administratio-c400114e8a58
8. The Future of Smart Contracts: Trends and Predictions, https://www.rapidinnovation.io/post/the-future-of-smart-contracts-trends-and-predictions
9. Blockchain Technology in Law Enforcement and Security: Overview, https://www.ijraset.com/research-paper/blockchain-technology-in-law-enforcement-and-security
10. How smart contracts work with blockchain, https://www.britannica.com/money/how-smart-contracts-work
11. Human-Centric Collaboration and Industry 5.0 Framework in Smart Cities and Communities: Fostering Sustainable Development Goals 3, 4, 9, and 11 in Society 5.0, https://www.mdpi.com/2624-6511/7/4/68

Analysis of graphic and UX design for Bulgarian tourist applications

Veselka Stoyanova[1], Ilian Lilov[2]
Artillery, AD and CIS faculty, National Military University V. Levski, Shumen, Bulgaria[1],
National Military University V. Levski, Veliko Turnovo, Bulgaria[2]
vtstoyanova@nvu.bg

Abstract: *Four of most of popular Bulgarian application were selected, namely "100 Places Bulgaria", "I Love Bulgaria", "Опознай.bg" and "The one hundred national tourist sites of Bulgaria", and compare them. Data collection was performed through an electronic questionnaire, which was based on Google Forms. The article presents the need for a solid theoretical foundation for understanding the complexity and multi-layeredness of user experience (UX) and user interface (UI) in the context of digital transformation.*
Keywords*: GRAPHIC DESIGN, UX DESIGN, USER INTERFACE, TOURIST WEBSITES*

1. Introduction

Graphic design is closely intertwined and of enormous importance in UX design and is widely spread due to its presence everywhere in the online space, as well as the continuous amateur and professional creation of graphic elements that enhance and develop perceptions. In the modern world, applications that look good and improve user experience and comfort in their use lead to repeated usage. The use of mobile applications with a pleasant and intuitive interface is a necessity and dictates their continuous improvement and the need for research to understand the ever-changing user and their increased demands. It is widely accepted that graphic design can be described as an art and a craft that gives aesthetic, functional, and organized structure to various types of texts and illustrations [1], [2].

Smartphones with touchscreen-based interfaces are increasingly used by non-technical groups including the elderly [10].

Travel websites are widely used by travellers for their travel bookings, but very little is known about sales performance and the emotional experiences for the customers [3].

From an economic point of view, graphic design contributes to:

- increased business profitability;
- improved brand image and presence in the international market;
- reduced marketing costs through effective communication;
- job creation in the creative industries;
- growth of exports of creative services.

Figure 1 shows the cycle of consumer experience***: user-problem-solution***.

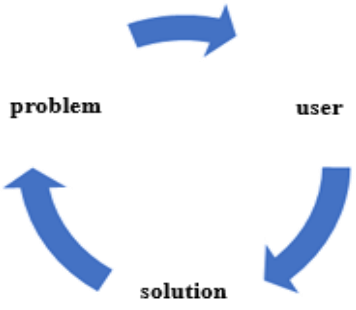


Fig. 1 *Cycle between user-problem-solution*

2. Basic methods for measuring user experience.

Qualitative and quantitative methods

According to [4], all user experience evaluation studies involve a participant performing certain tasks on one or more designs. In such a study, two types of data can be collected (Fig. 2):

- Qualitative data consisting of observational findings that identify easy or difficult to use design features.
- Quantitative data, in the form of one or more metrics (such as task completion rates or task completion times), that reflect whether the tasks were easy to complete.

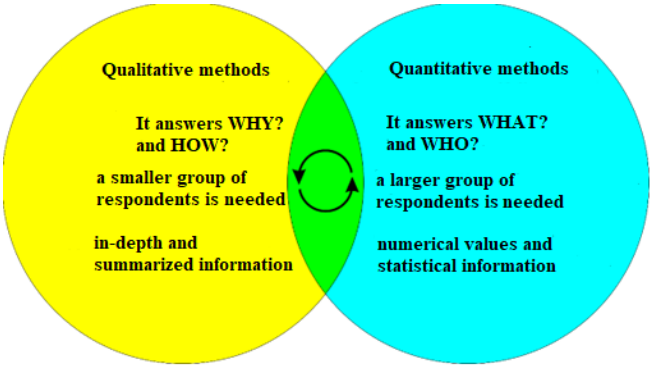


Fig. 2. *Presentation of qualitative and quantitative methods*

Researchers and user-centered design practitioners have described over 100 different methods for measuring user experience. These methods focus entirely on how users feel when interacting with the product, service, or system being evaluated. Measuring user experience is a multifaceted process that combines various research techniques to obtain a comprehensive picture of the interaction between the user and the system.

The total num digitalization is the basis for the development of a modern economy, and this process covers all aspects of management, including consumer behaviour in the environment [9].

Bulgarian tourist applications

The plan and consistency in managing a project and the knowledge of all possible stages is key to the success of any project[10]. According to [11] the group of users aged 40-50 often know the basic gestures used on smartphones (Tap, Scroll, Flick), but rarely use complex gestures such as Bundle and Multi-finger Drag. Younger users (21-24 years) similarly to adults perform the same actions and tasks, but their interaction is much more intuitive.

Figure 3a) shows the results of a Statista survey for 2024, which shows that 70% of tourists in Europe use mobile apps to search for objects, 52% use them for routing and logistics (Fig. 3b),



a) b) c)

Fig.3. *Mobile app usage by consumers in 2024*

and Fig. 3c) shows that 33% use mobile apps for social sharing and "gamified" experiences (e.g. achievements, badges, loyalty).

Figure 4 presents the logos of the four applications studied, allowing for a breadth of impression and subsequent emotional impact. This allows for easy comparison and commentary on design possibilities.



a) Logo of 100 Places Bulgaria[8]



b) Logo of I Love Bulgaria[5]



c) Logo of The hundred national tourist sites of Bulgaria [6]



d) Logo of Опознай.bg [7]

Fig. 4. *Logo of the applications*

The application **100 Places: Bulgaria [8]** is a modern attempt to digitalize the popular tourist initiative known for its paper booklets for stamps. A main UX focus is placed on gamification and visual identity - the interface is built around a personal profile where the user marks the places they have visited and earns virtual badges. The design is vibrant, with graphic icons and colour palettes that create a sense of adventure.

The **I Love Bulgaria** app [5] is a digital travel guide combining cultural, natural and historical routes. It was developed with the cooperation of state and private institutions, which gives it the character of a national brand. Its interface is visually rich, with high contrast and intuitive icons that represent sites, routes and user progress.

Опознай.bg [7] is a mobile extension of the online platform of the same name, which provides detailed information about tourist sites, events and activities in Bulgaria. The application is oriented towards functionality and information richness, as the user can filter the results by category, location, reviews and accessibility. The UI design is minimalist, with predominantly neutral tones and a linear structure.

The latest application, **The Hundred National Tourist Sites of Bulgaria** [6], is an official digital interpretation of the classic tourism initiative of the Bulgarian Tourist Union (BTU).

Summary data

Game elements included in some of the applications use specific characteristics of the users to encourage them to use the respective application. The inclusion of gamification is of significant help in keeping the user's attention. The types of users according to the Bartle model [12] are achievers, explorers, socializers and competitors. It should be noted that not all users fit into one type, which makes it necessary to provide a variety of challenging experiences.

Table 1 presents a comparison of the applications by criteria regarding discoverability, application popularity, and most importantly, user satisfaction.

Table 1. *Comparison of the studied applications*

Application / **Criteria**	**100 Places Bulgaria**	**I Love Bulgaria**	**The Hundred National Sites of Bulgaria**	**Опознай.bg**
Available on Google Commerce Ltd	+	+	+	+
Published on	11.04.2021 г	04.08.2016	13.08.2019	26.01.2016
Downloads:	over 1 000	over 10 000	over 10 000	over 100000
User rating on Google Play (user rating)	4.2 (37review)	3.8 (315 reviews)	4.7 (401 reviews)	4.3 (3000 reviews)

The results from the table 2 show the interpretation of how users react not only rationally, but also emotionally, which is key in UX/UI design in tourism applications.

Table 2*: Summary data compared for emotional assessment*

Applications	*Position in the chart*	*Emotional assessment*
100 Places Bulgaria	Excited Pleasant	Engaging and inspiring
I Love Bulgaria	The average between Excited и Average Pleasant	Moderately pleasant
The one hundred national tourist sites of Bulgaria	Calm Pleasant / Calm Neutral	Relaxed, balanced, a little boring
Опознай.bg	Average / Excited Unpleasant	Stressful, overwhelmed

Measuring emotions includes many well-known methods, such as Emocards or Emofaces, which overcome the intangible nature of measuring emotions by replacing verbal measurements with images. Evaluators describe their experience of using a product by choosing one of a number of predefined images.

3. Conclusions:

The article presents the need for a solid theoretical foundation for understanding the complexity and multi-layeredness of user experience (UX) and user interface (UI) in the context of digital transformation.

1. The analysis of the conceptual framework clearly showed that UX is an overarching concept focused on the overall user experience, while UI represents its visible and interactive part.
2. The connection between strategic design, visual impact and consumer behaviour highlights that design today is transforming from a purely aesthetic function into a strategic asset that directly influences brand perception, trust and consumer engagement.
3. Systematic and multifaceted research into the user experience is necessary to enable improvement and relevance, regardless of the time period.

4. Acknowledgement

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

5. References:

1. Coney, M. B., & Steehouder, M. (2000). Role playing on the Web: Guidelines for designing and evaluating personas online. Technical communication, 47(3), 327-340
2. Цонев, А, (2021), 5 нива на потребителско изживяване. Основни елементи, https://alystal.com/resursi/post/pet-niva-na-potrebitelsko-izjiviavane
3. Mincheva, S., & Stoyanova, V. (2025). Research on the Impact of the User Experience for the Success of a Virtual Product: Bulgarian Travel Agency Websites. In *Proceedings of the 16th International Scientific and Practical Conference* (Vol. 2, pp. 237-241), https://doi.org/10.17770/etr2025vol2.8591, [Accessed: June. 30, 2025].
4. Raluca Budiu (2019). Quantitative vs. Qualitative Usability Testing https://www.nngroup.com/articles/quant-vs-qual/ [Accessed: May. 02, 2025]
5. Ilovebulgaria.eu, Местен уеб сайт за пътувания https://play.google.com/store/apps/details?id=net.loyalty&hl=en, https://ilovebulgaria.eu/ [Accessed: May. 02, 2025]
6. Стоте национални туристически обекта на България, Местен уеб сайт за пътувания, https://play.google.com/store/apps/details?id=es.benesoft.turist&hl=bg [Accessed: May. 02, 2025]
7. Opoznai.bg, Местен уеб сайт за пътувания https://play.google.com/store/apps/details?id=bg.opoznai&hl=bg, https://opoznai.bg/ [Accessed: May. 02, 2025]
8. 100te обекта, Местен уеб сайт за пътувания, https://play.google.com/store/apps/details?id=com.futurist_labs.bg_places&hl=en [Accessed: May. 02, 2025]
9. O. Mancheva-Ali, "The digital economy and its impact on consumption in the regions of Bulgaria". presented at 3rd International Conference Spatial Development of Territories (SDT 2020). Atlantis Press, 2021. p. 256-261. [Accessed: May. 02, 2025]
10. St. Mincheva, "Creation of a mind map and an algorithm for project management", Proceedings of International Scientific Conference - Defense Technologies, Shumen, (DefTech 2024), pp.851-858, ISSN 2367-7902, [Accessed: May. 12, 2025].
11. St. Mincheva, "Research on users interaction with a touchscreen", Annuals of Konstantin Preslavsky University of Shumen, vol. XIV E, (2024), ISSN: 1314-8818 (print), ISSN: 2815-4703 (online), pp.195-200. https://doi.org/10.46687/YT24SDM, Годишник ФТН 2024, [Accessed: May. 12, 2025].
12. Bartle's Player Types for Gamification, IxDF, 2024. Web Site. [Online]. Available from: https://www.interaction-design.org/literature/article/bartle-s player-types-for-gamification. [viewed 2025-06-05].

An approach to monitoring, classifying and jamming underwater sound communications

AleksandarKolarov, RadostinNajdenov
Institute of Metal Science, Equipment and Technologies with the Center for Hydro- and Aerodynamics "Acad. A. Balevski"-
Bulgarian Academy of Science, Sofia, Bulgaria
aleksandar_kolarov@abv.bg, radonaydenov@yahoo.de

Abstract: *The task of jamming underwater voice communications with and between divers and communications with / between autonomous submarines in port security systems and coastal infrastructure facilities as well as anchored ships plays an important role in operations against asymmetric and military threats. Underwater jammers can be classified as autonomous, with remote control via hydro acoustic channel and with cable control from a shore-based or ship-based base station. While in the first two when receiving hydro acoustic signals above a set threshold level is performed program amplitude-frequency analysis and a decision is made to emit a jamming signal, in coastal / ship performance the decision to activate may be taken by the operator on other signs, which are analyzed in this report.*
Keywords*:UNDERWATER VOICE COMMUNICATIONS, JAMMING,,REGISTRATION OF SIGNALS, OPERATOR*

1. Introduction

Marine resource collection and development are almost inseparable from underwater communication. In addition, underwater wireless communication (UWC) plays a vital role in underwater navigation and is a key technology for underwater sensor networks.

Traditional underwater communication methods mainly include underwater acoustic communication (UAC), underwater radio frequency (RF) communication and underwater wireless optical communication (UWOC). UAC is considered the most practical way to transmit data over long distances of up to several tens of kilometers based on underwater acoustic waves. However, UAC suffers from a relatively low data transmission rate of the order of kbps due to the low system bandwidth of about kHz, and the low bandwidth is limited to the low carrier frequency (10 Hz–1 MHz). The propagation speed of the acoustic wave in the underwater channel is five orders of magnitude lower than that of the radio wave, resulting in a propagation delay of about 0.67 s per kilometer.

In addition to useful applications, including in the military field, underwater wireless communications can also support terrorist activities that lead to political, economic and moral losses for many countries and can quite realistically paralyze the economy of countries dependent on sea supplies of energy resources, raw materials, food and other necessary goods. Objects of attacks by underwater saboteurs can be ships and floating facilities, port and hydrotechnical facilities, coastal industrial enterprises, including nuclear power plants, oil platforms, underwater pipelines and cables, etc. The use of autonomous underwater vehicles and robots can ensure the actions of both special operations forces and terrorists, as well as participation in maritime operations, primarily as a source of intelligence information, etc. Therefore, one of the approaches to increasing the effectiveness of port, naval base and anchorage protection systems is to disrupt or significantly complicate underwater communication with and between underwater swimmers and/or with and between autonomous underwater vehicles and robots. This can be achieved by building a parallel functioning, as part of the other elements of the protection system, or an independently (autonomously) operating system for countering underwater communications, which would terminate (to a large extent disrupt) the management process (control of combat operations). The system should be adaptable to the existing capabilities and elements of a broad port protection system, i.e. be of a modular type, which will allow it to perform a full range of functional capabilities for detecting and registering signals from underwater communications, synthesizing a jamming signal and broadcasting it for a certain period of time [1].

The presented results are based on a number of literary sources and, above all, on the research conducted at the Institute of Metal Science, Equipment and Technologies with the Center for Hydro- and Aerodynamics "Acad. A. Balevski"- Bulgarian Academy of Science.

2. Prerequisites and ways to solve the problem

Modern underwater communication systems implement the process of transmitting/receiving information in the form of modulated sound (ultrasound), electromagnetic or optical waves. Each of these techniques has advantages, disadvantages and limitations.

Hydroacoustic communication is currently the most versatile and widely used technique. In recent years, the main goal of underwater acoustic communication is to overcome the performance limitations caused by the high-dispersion channel, while maximizing the efficiency of the frequency band [2].

The summarized parameters of the products offered on the market for general and military use for communication between divers and between divers and a base station, which have a major influence on the design of an underwater communications jammer, are shown in Table 1.

Table 1. The summarized parameters of diver-to-diver communication systems and a base station

PARAMETER	**RANGE OF ACTION**		
	small	medium	large
Connection distance,m	50-500	1500-3000	6000-10000
Acoustic power output,W	0.5	5-10	50-70
Frequency range (most used),kHz	30-40 (31-33)	20-30 (25-29)	8-20 (8-11)
Signal modulation	Amplitude-unit frequency band with suppressed carrier frequency		
Receiver sensitivity	-120dBv (≈1V/1Pa)		
Automatic gain control	80-120 dB		
SL-Acoustic intensity	172-185 dB re1μPa at a m		

The general parameters of the communication means for the management and control of the movement of underwater vehicles and robots (AUVs) are shown in Table 2.

Table 2. and General parameters of the communication means with underwater vehicles robots (AUVs)

	PARAMETER	**RANGE OF ACTION**		
		small	medium	large
1	Connection distance,km	0.5-1	1-10	10-100
2	Acoustic power output,W	3	10-50	

3	Frequency range (most used)kHz	40-150	20-40 (34-38)	7-20 (8-15)
4	Signal modulation	2/4/8 PSK;8/16/64 QAM		
5	Receiver type	Coherent equalizer with synchronization		
6	Transmission speed	150kbps	10 kbps	1 kbps
7	SL-Acoustic intensity	157-207dB re 1μPa at a m		
8	Mutual Access Protocol	TDMA,CDMA		

The means of underwater voice communication, which can be used in the areas of ports, naval bases and offshore facilities, will mainly have parameters with values shown in Table 3:

Table 3. The general characteristics of underwater voice communication devices

№	Parameter	Value
1	Carrier frequency	8 ÷ 45 kHz
2	Wafelength	0.1 ÷ 0.5 m
3	ChannelBandwidth	2 ÷ 3 kHz
4	Signalingrate	~ 2 ksimbols/s
5	Simbolduration	~ 500 μs
6	Carriercycles/symbol	~ 5
7	Platformspeed	3 ÷ 15 km/h
8	CarrierDopplershift	~ 3 x 10^{-3} %
9	Multipath time spread	50 ÷ 100 ms
10	Simbolsinthattime	100 ÷ 2000
11	Carrier frequency modulation	SSB (USB, LSB), MFSK, DPSK. ***Fig. 1, 2, 3.***

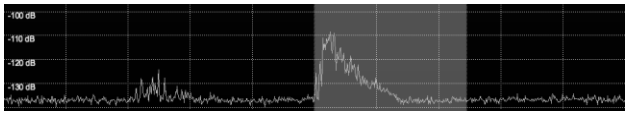


Fig. 1.Oscillogram of a modulated SSB signal



Fig.2. Oscillogram of a modulated MFSK signal

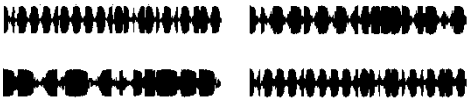


Fig.3. Oscillogram of a modulated DPSK signal

For the purposes of analyzing the necessary and sufficient values of the parameters of an underwater communication jammer, the following conclusions can be drawn:

• The output power (PEP) of the transmitters of the underwater communication stations between and with divers is expected to be in the range of 30 ÷ 70 W, which ensures a communication distance of up to 6000 m. The products available on the market, which are expected to be used by terrorist divers, provide a distance of up to 1000÷1200 m at transmitter output power values of up to 5 W;

• The signals emitted in underwater voice communication are usually amplitude-pulse modulated on a single frequency band with a suppressed carrier frequency (SSB);

• The frequency ranges in which underwater voice communication systems operate can be systematized depending on their purpose and, as follows:

- 8 ÷ 10 KHz – for military needs for combat communication with underwater swimmers from a control post (coastal stationary or mobile (ship, helicopter, submarine, etc.);

- 25 ÷ 28 KHz for military needs for combat communication between underwater swimmers in the group;

- 30 ÷ 35 KHz – for communication between divers engaged in sports, underwater work, etc.

• The sensitivity of the receivers of underwater voice communication systems, with within 100 ÷ 120 dBv, and automatic gain adjustment – 90 ÷ 110 dB;

To solve the task, a team from the Institute of Metallurgy, Facilities and Technologies with a Center for Hydro- and Aerodynamics at the Bulgarian Academy of Sciences /IMSTCHA-BAS/ created a prototype of a shore-based jamming system "RACK-CS" – Fig. 4, designed to register specific underwater communication signals, which are then classified by an operator who can decide to actively block them for a certain period of time by emitting powerful hydroacoustic pulses in an appropriate frequency range.



Fig. 4. Composite underwater communications jammer RACK-CS

The underwater part of RACK-CS is positioned on the seabed at a depth of up to 30 m and registers the exchange of information between ultrasonic underwater communication devices in the frequency range of 10 - 60 kHz. Effective suppression of underwater communication is achieved by emitting pulsed interference signals with a frequency close to that of the communication signals and an amplitude sufficient to reach a level above the receiver threshold.RACK-CS is designed to meet the following requirements:

• to register the presence of communication signals in a sea area;

• to receive and analyze hydroacoustic signals emitted in the full frequency range of underwater communication systems;

• to be remotely activated via cable when information about possible underwater targets is received from radar, sonar, visual means, etc.;

• to emit a series of pulses with tonal interference;

• ensuring non-isotropic signal emission – unidirectional emission in the horizontal plane and directional radiation in the vertical plane.

The observation, recording and classification of underwater communication signals is carried out by an operator using a shore/ship station located on the shore or on board a ship. The underwater part of the RACK-CS is connected to the base shore/ship station via an underwater cable. The base station receives information from a hydroacoustic receiver, sends command signals and supplies 24V DC voltage to charge the power supply batteries. Switching the silencer to the active operating mode is carried out by an operator command and is sent via cable. Returning it back to standby mode (listening) is done in the same way.Upon command given by the operator, the silencer is activated and begins to emit for a certain period of time (about 3 minutes) a pseudo-continuous wave consisting of a set of short pulses with an acoustic power of not less than 1600 - 1900 Pa/m (180-185 dB re 1μPa per 1m), which

are filled with a random frequency from the spectrum of the selected frequency (sub)range.

3. Solution to the studied problem

In general, the functioning of the "RACK-CS" can be described in the following sequence:

• The monitor of the shore/ship station displays the noise picture in the surrounding sea area;

• In the main operating mode, the operator analyzes the noise situation and classifies the signals that may be due to underwater communication;

• If the classification is positive, the operator determines the frequency range of the communication, subbands and frequency band;

• Using the control unit keyboard, the operator selects the appropriate combinations that determine the parameters of the jamming signal;

• At the operator's command, the jammer starts emitting a jamming signal within the specified frequency within a specified frequency subband for a period of 3 minutes. During this time, the hydroacoustic receiver is blocked [3].

The information from the hydroacoustic receiver is visualized and analyzed by specialized software (Underwater Jammer Commander (UJC)), based on which it is decided whether there is a communication signal and what its frequency range is. UJC consists of a settings row and three built-in windows, marked with green numbers in Fig.5.

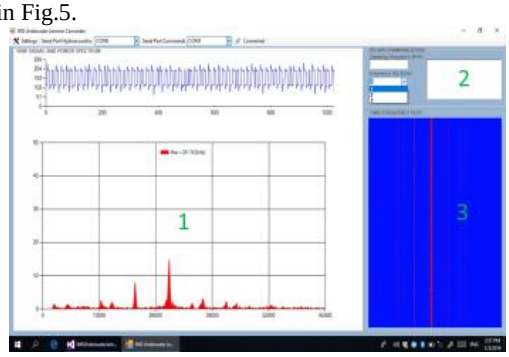


Fig. 5. Laptop indicator for UJC program in "Receive" mode

It is designed to perform jamming with selected frequencies. A hydroacoustic serial port and a serial command port can be connected using the settings menu. The window marked 1 represents the raw signal and the power spectrum. The window marked 2 is used to select the jamming frequency range. In the frequency (X-axis)-time (Y-axis) graph window, marked 3, the power of the received hydroacoustic signal is shown in color (red for high values and blue for low values).

The jamming procedure follows the following steps:

• Selection of the jamming frequency after analyzing the input signal and the power spectrum;

• Selection of the jamming frequency range (window 2);

• Start of the jamming with the virtual button "Start jamming" (Fig.6);

• Following the time-frequency graphs (window 1).

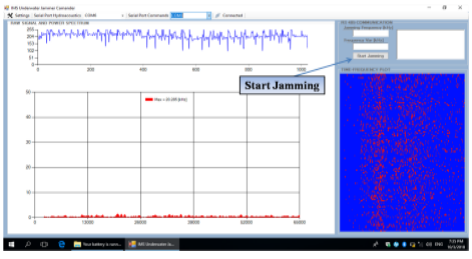


Fig. 6. Laptop indicator for UJC program in "Broadcast" mode

In the main mode of operation, the operator analyzes the noise situation and classifies the signals by deciding whether there is an underwater communication signal and what is its frequency range. To perform this task, the operator must determine from tactical considerations whether the amplitude of the received signal corresponds to the probable output acoustic power and the probable distance to the underwater communication device.

The next stage is to determine from the registered oscillogram whether the shape of the received signal corresponds to the probable modulation of the carrier signal – see Fig. 1, 2, 3. At the same time, the operator must assess whether the oscillogram and spectrogram indicated on the screen correspond to those of human speech or to some representatives of the fauna characteristic of the area and some specific ones, such as [4,5]:

• Bottlenose dolphins - produce a large number of vocalizations, including whistles, buzzing, croaking, popping, rustling sounds of hinges, screams and clicks – Fig. 7;

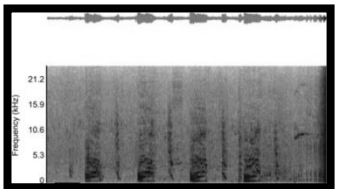


Fig. 7. Oscillogram and spectrogram from bottlenose dolphin

• Common dolphin - the most common sounds are tonal whistles (maximum frequency below 50 kHz) and high-frequency echolocation clicks (above 100 kHz) – Fig. 8;

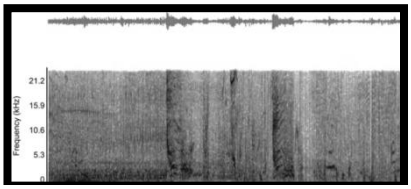


Fig. 8.Oscillogram and spectrogram from a common dolphin

• Belugas are widely known for their diverse and frequent echolocation and communication vocalizations with a mid-frequency range of 2.0 to 5.9 kHz. They are trainable and can be used for combat missions – Fig. 9;

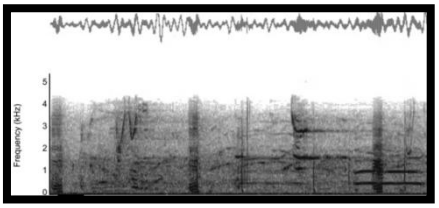


Fig. 9. Oscillogram and spectrogram of beluga

• Harbor seals produce a wide variety of vocalizations, with their underwater vocalization described as a roar with a peak frequency of approximately 1,2 kHz –Fig. 10;

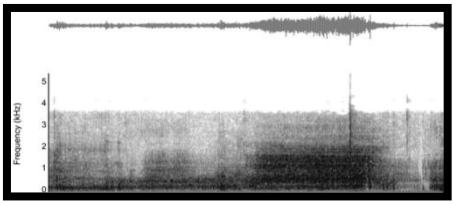


Fig. 10. Oscillogram and spectrogram from a seal

• From a motorboat – Fig. 11;

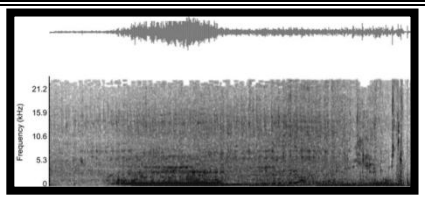


Fig. 11. Oscillogram and spectrogram from a motorboat

• From scuba diving – Fig. 12

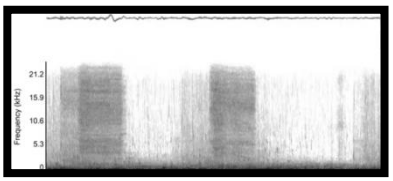


Fig. 12. Oscillogram and spectrogram from a scuba diving

3. Conclusion

Underwater communication is a complex process that requires specialized technologies and methods for transmitting information underwater. Spectrograms are visual representations of the frequency components of sound signals over time and can be used to analyze acoustic data in the context of underwater communication.

Underwater communication is a complex process that requires specialized technologies and methods for transmitting information underwater. Analyzing underwater sounds is challenging due to the complexity of the aquatic environment that affects the propagation of sound waves. Factors such as temperature, salinity, depth, and the presence of obstacles can significantly affect the quality of the signal. Spectrograms are visual representations of the frequency components of sound signals over time and can be used to analyze acoustic data in the context of underwater communication [6]..

Spectrograms provide a graphical representation of the frequency spectrum of sound over time. They show how the different frequency components of sound change over time. This can be useful for analyzing different types of underwater sounds, including those used for communication between submarines or other underwater devices. Spectrograms can be used to identify different types of underwater sounds, such as the sounds made by marine animals, noises from ships, or specific signals used for communication between underwater vehicles.

In conclusion, spectrograms play an important role in the analysis of underwater sound signals and can be a powerful tool for understanding and improving underwater communication, and their interpretation by an operator should take into account:

1. Axes: A spectrogram has three main axes:

• X-axis: Time (seconds).

• Y-axis: Frequency (Hz).

• Color/Intensity: Sound amplitude (dB). Brighter colors generally indicate louder sounds.

2. Frequency bands: Different frequency bands represent different tones. For example, low-frequency sounds will be represented at the bottom of the Y-axis, while high-frequency sounds will be at the top.

3. Temporal changes: how the frequency spectrum changes over time. This can help identify different sound events or patterns.

Context: The context of the recording should always be taken into account. Knowing what type of sound is expected (for example, a dolphin sound or a submarine signal) can help interpret the spectrogram more accurately.

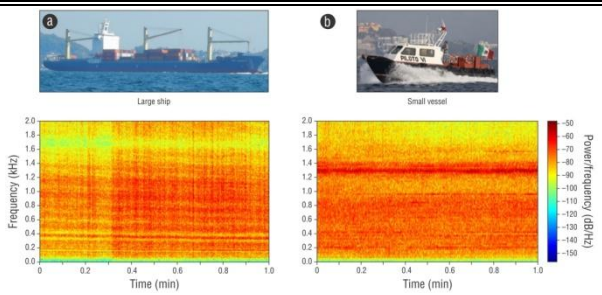


Fig. 13 Examples of sound contribution from a large ship (a) and a small vessel (b) showing the image and spectrogram

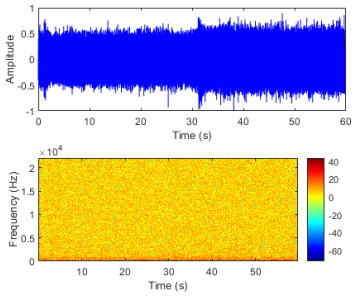


Fig. 14 Spectrogram of mixed acoustic signal

The prototype of a shore-based jamming system "RACK-CS" created at the Institute of Marine Engineering and Technology-BAS, designed to register specific underwater communication signals, requires subsequent classification by an operator, who can decide to actively block them for a certain period of time by emitting powerful hydroacoustic pulses in an appropriate frequency range. The report proposes a method for preliminary preparation of the operator to analyze the parameters of the registered signal – oscillogram shape, modulation type, frequency spectrum – spectrogram and power, displayed on the base station indicator using specialized UJC software.

Acknowledgment

This publication was carried out under project G7475, funded by the NATO Science for Peace and Security Programme.

4. Literature

1. Yik-Chung Wu * Rui Min. Joint channel estimation and data detection for multihopofdmrelayingsystem under unknown channel orders and doppler frequencies. IEEE Communications Magazine,(January):97–102, 2012;

2. Dario Pompili and Ian F. Akyildiz. Overview of networking protocols for underwater wireless communications. Comm. Mag., 47(1):97–102, January 2009;

3. E.Kozaczka, GrażynaGrelowska, Theoretical model of acoustic wave propagation in shallow water, Polish Maritime Research 2 (94) 2017 Vol. 24; pp. 48-5510.1515/pomr-2017-0049;

4. Hague, D.A.; Buck, J. An experimental evaluation of the generalized sinusoidal frequency modulated waveform for active sonarsystems. J. Acoust. Soc. Am. 2019, 145, 3741–3755;

5. Kolev S, Nenova B, Ivanov I. Influence of seawater depth in hydroacoustic transmission of binary numbers. International Scientific Journal "Security&Future", 4, 3, Scientific Technical Union of Mechanical Engineering – Bulgaria, 2020, ISSN:2535-082X, 119-120