

INTERNATIONAL SCIENTIFIC JOURNAL

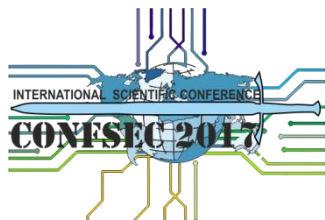
SECURITY & FUTURE

ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

YEAR VII,
ISSUE 2/2024

PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA



INTERNATIONAL SCIENTIFIC JOURNAL SECURITY & FUTURE

PUBLISHER:
SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING
INDUSTRY-4.0

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

ISSN (PRINT) 2535-0668; ISSN (Online) 2535-082X
YEAR VIII, ISSUE 2 / 2024

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

EDITORIAL BOARD

CHIEF EDITOR

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

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

CONTENTS

THEORETICAL FOUNDATIONS OF SECURITY

Critical infrastructure resilience through security systems development	
Valeri Panevski	41

NATIONAL AND INTERNATIONAL SECURITY

The effect of central bank digital currencies on asset confiscation	
Kolarov Todor	45
Demographic change as a risk for the pension system and the stability of the security forces - experience from the Czech Republic	
Jan Urbanec, Dana Junkova	49
IIoT and cyber security in industrial enterprises	
Petar Georgiev, Krasimira Dimitrova	53

INFORMATION SECURITY

Automated Web Application Scanning with Wapiti, Selenium, and SQLMap	
Zhaneta Savova, Stanislav Atanasov, Rosen Bogdanov	57
Comparison between Monolithic and Microservices Architecture in Web Applications Built with Java	
Ina Papadhopulli, Armada Alija	61
Storage Virtualization: Optimizing Data Center Efficiency and Performance	
Genka Slavova-Torres	65

TECHNICAL FACILITIES FOR ENSURING SECURITY

Experimental determination of fire resistance of steel elements (X-brace) protected with intumescent paint	
Neli Simeonova	67
Remote detection, recognition and tracking of objects in drones aircraft	
Ivanova Eleonora, Stefanov Ivan	71

Critical infrastructure resilience through security systems development

Valeri Panevski

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

Abstract: Critical infrastructure can be exposed to disruptive events and incidents caused by external or internal impacts. Some of these events are internally system-manageable, but others must be addressed through the additional application of appropriate security measures, which can be implemented through security systems.

The development of critical infrastructure security systems requires a careful definition of overall requirements, which in general is directly related to ensuring business continuity by determining the resilience of critical infrastructure elements.

This publication presents in a systematized form the author's experience in applying resilience assessment results as inputs to the development of CI security systems.

Keywords: RESILIENCE, SECURITY SYSTEMS

1. Introduction

Developing and subsequently strengthening the resilience of any set of critical infrastructure subsystems is a demanding process in terms of design, time and resources that requires well-defined initial as well as functional conditions. The definition of such conditions can be understood as the overall concept of resilience of these subsystems in the critical infrastructure (CI). Establishing the security management process of critical infrastructure elements, including the resilience framework, can be seen as a key initial condition. Conversely, the main functional condition is the unambiguous specification and perception of the factors determining CI sustainability. The security management process of critical infrastructure elements is an adaptation of principles based on a continuous management cycle PDCA (Plan-Do-Check-Act) (Plan-Do-Check-Act; Deming Cycle) [1] to fit of CI.

1. Organizational security management

The identification of critical infrastructure elements is the initial sub-process of security management, which depends on the correct formulation of criteria for the identification of critical infrastructure elements at the European, national and regional level. In this phase of the process, it is equally important to consider the resilience of applying an appropriate approach to element designation, which may be based on the top-down principle or vice versa.

The second sub-process of security management is the assessment of critical infrastructure elements. The key objective of this sub-process is the risk assessment, consisting of the assessment of relevant scenarios of destructive events and the assessment of the resilience of the relevant element, which includes the assessment of its resilience, recoverability and adaptability.

Securing critical infrastructure elements is the final security management sub-process consisting of risk management and resilience strengthening. Risk management involves the selection and implementation of one or more risk minimization options, i.e. risk retention, risk transfer and/or risk avoidance [2].

Improving resilience minimizes the vulnerability of subsystems, which in turn limits the occurrence, intensity and spread of failures and their impact on CI and society. The main functional condition for strengthening the resilience of critical infrastructure subsystems is the categorical specification and perception of the factors that determine it.

In this context, CI resilience should be understood as a cyclical process of continuous improvement of prevention, impact acceptance, recovery and adaptation.

➤ *Prevention.* By adopting preventive measures, management ensures that the subsystem is less vulnerable to future disruptive events; preparedness is therefore the outcome condition for prevention. Once a disturbance occurs, such a system will move from prevention to acceptance of the impact.

➤ *Accepting the impact.* Initiated if a subsystem is dysfunctional due to a disruptive event and is determined by the

resilience of the CI subsystem. Resilience is defined by the ability of a critical infrastructure element to absorb the effects of a disruptive event without causing any fluctuations in the services it provides.

➤ *Recovery.* It begins after the effects of a disruptive event have passed and is characterized by the subsystem's ability to restore its function to its original and/or required level of performance. The duration of the recovery phase is determined by the resources available and the time required to complete the individual recovery processes.

➤ *Adaptation.* Determines the ability of the organization to adapt a managed subsystem to the potential recurrence of a disruptive event - i.e. to learn from previous disruptive events. Accordingly, this phase represents the dynamic long-term ability of the organization to adapt to changes in circumstances.

2. Factors determining the resilience of critical infrastructure

The resilience of the critical infrastructure subsystem can be understood as a state formed by the following factors:

- Factors determining resilience;
- Factors limiting resilience;
- Factors affecting resilience.

CI resilience is determined by two main areas, namely technological and physical element protection and organizational management (Figure 1).

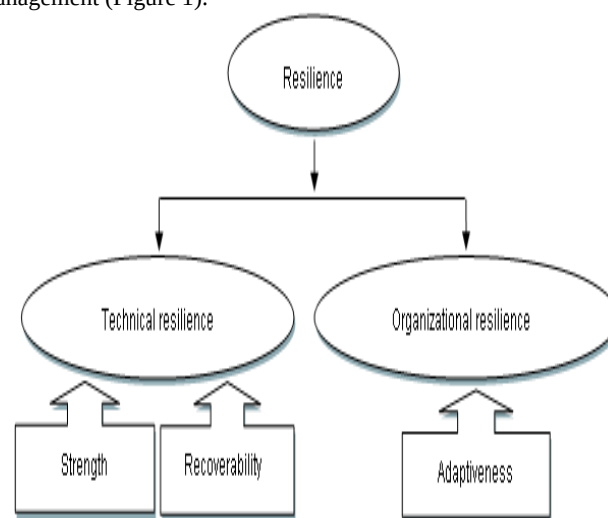


Figure 1: Components determining CI resilience.

The resilience of technological and physical security of individual elements, known as technical resilience, is determined by the strength and the ability to restore the elements of the system. The increase in technical resilience is achieved exclusively in

relation to a specific element or a group of identical or very similar elements.

Technical resilience is influenced by the following main factors:

- technological structure of the element;
- security measures of the item;
- destructive events that affect the durability of the element.

The resilience of the organization's management, known as organizational resilience, is determined by the level of the organization's internal processes, the main purpose of which is to create optimal conditions for adapting critical infrastructural elements to disruptive events.

Organizational resilience is formed simultaneously for all critical infrastructure elements managed by an organization. This type of resilience is formed, assessed and strengthened by the management of the organization already in the prevention phase and factors at the level of internal processes necessary for the adaptation phase of critical infrastructure elements, relying on the experience gained from previous response and recovery operations.

2.1 Strength factors

Strength is the ability of an element to absorb the effects of a destructive event. These impacts can be absorbed through the structural qualities of the buildings or the technologies used (structural robustness) and/or through security measures (security strength). Strength is determined by the variables, shown in Figure 2.

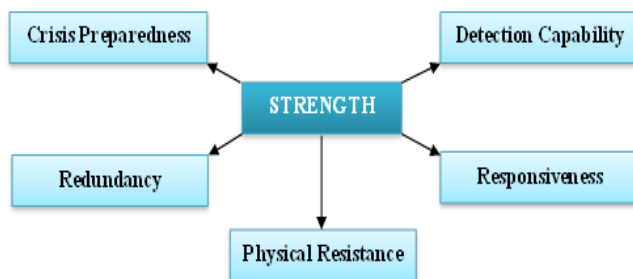


Figure 2: Possible variables of strength.

When the strength level reaches 100%, the corresponding item becomes resistant to the effects of the given destructive event. This means that it is able to fully withstand its effects without noticeable negative impacts on the service element provided.

2.2 Recoverability Factors

Recovery is the ability of an element to restore its function to the original (required) performance level after discontinuing the effects of a destructive event. With regard to CI, recovery is understood as recovery, in which case only the damaged or destroyed components of an element are repaired or replaced. The recovery is determined by the following variables: material resources (the presence of components for repair or replacement of damaged or destroyed parts); financial resources (to finance the rapid recovery); human resources (with the required level of qualification) and developed recovery processes (rapid restoration of the functionality required).

2.3 Adaptiveness Factors

Adaptability is the ability of a critical infrastructure operator to prepare an element for the recurring effects of a previous destructive event. It is the dynamic, long term ability of the CI to adapt to changes in circumstances. Adaptability is determined by the internal processes of an CI aimed at creating optimal conditions for strengthening stability. The main processes that improve the adaptability of critical infrastructure elements to destructive events are risk management, innovative processes and training processes.

Risk management is an important internal process of the organization, which is essential for ensuring security/safety and enhancing the stability of the prevention stage. This process consists of coordinated activities for directing and controlling a CI in terms of risk, and its level with respect to organizational resilience is determined by the criteria, outlined in Figure 3.

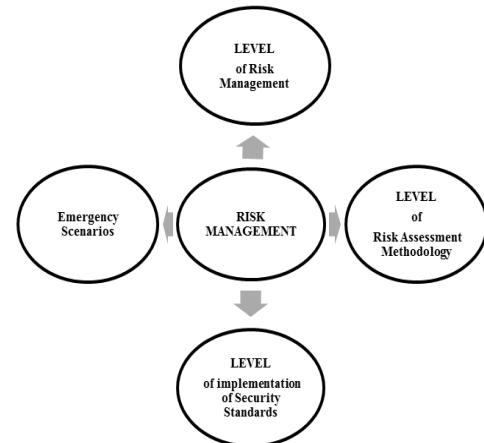


Figure 3: Possible structure of risk management to ensure the CI resilience.

Additional internal processes that significantly contribute to the strengthening of the resistance of the critical infrastructure elements at the prevention stage are the innovative processes of the organization.

From a strictly practical point of view, innovations are categorized as product, process, marketing and organizational. In terms of increasing resilience, process and organizational innovation, they are particularly important as they focus on the reliability and external security of the technologies used. The innovation process itself consists of the following phases: invention; science and research and application.

The level of the innovation process is determined by:

- the flexibility of the organizational structure;
- the level of implementation of a management system;
- organizational processes management methods;
- the level of innovation of the management process;
- the degree of implementation of technological innovation;
- level of innovation in security measures;
- the level of engagement in science and research;
- the level of investment in innovation by the organization.

3. Develop security systems to improve CI resilience

According to ISO 22316:2017 [3] the general principles that provide the basis for improving the state of organizational sustainability. These principles, which are closely related to the security systems development process, state that resilience:

„• f) is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise;

- g) relies upon effectively managing risk.“

Also, the design, development and coordination of management disciplines and their alignment with the organization's strategic goals are fundamental to improving organizational resilience, which gives complex importance to the development of security systems. In Annex A to item „5.8 Development and coordination of management disciplines“ [3], a sample list of 20 management disciplines is provided, as directly related to the development of

security systems I can point out: business continuity management; risk management and physical security management.

Therefore, the implementation of the Business Impact Analysis and Risk Assessment processes, according to ISO 22301:2019 [4] provides the necessary information for the development of security systems.

The correct and timely conduct of these two processes provides information on the likely impact of existing risks and threats (Figure 4) on the sustainability of the operation of critical CI assets, and thus on the structure and scope of security systems.

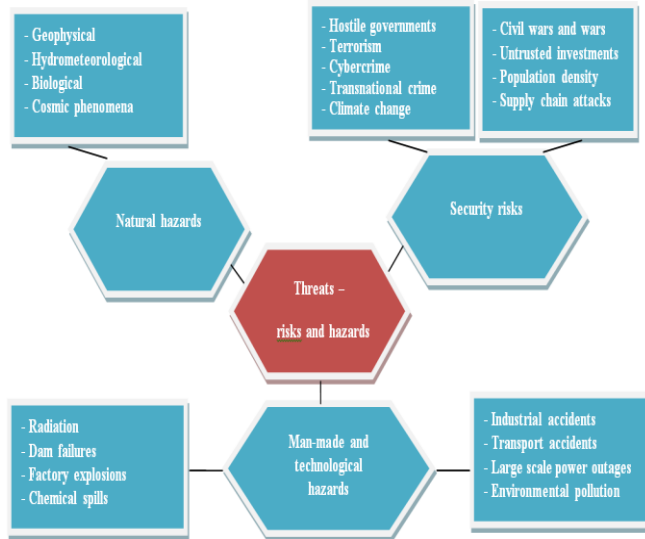


Figure 4: Threats to critical infrastructure - risks and hazards. [5]

I should note that:

➤ The business impact analysis is performed in accordance with ISO /TS 22317:2021 *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*;

➤ According to item “8.2.3 Risk assessment” of ISO 22301:2019, the risk analysis should be performed in accordance with ISO 31000:2018; Risk management — Guidelines.

Due to the dynamic nature of the organization's security function, it is strongly recommended that the Business Impact Analysis and Risk Assessment processes be reviewed regularly to identify areas for improvement.

As a result of what has been said so far, I can state with sufficient certainty that adaptability, as a direction of the process of organizational security, complexly related to the managerial disciplines of the organization, is a possible source of information for the development of security systems.

Also, depending on the complexity, value and importance of the CI asset for which security needs to be built, they can be developed as mechatronic security systems. The main document that is internationally accepted for implementation is the VDI 2206 guideline “Design methodology for mechatronic systems”, on the basis of which, according to the characteristics of the organization in which it is to be implemented, industry developments have been made.

Basically, in the theory and practice of developing mechatronic systems, the *hierarchical design method* and the “V-model” are applied.

The *hierarchical design method* considers the integration of mechatronic disciplines from the very beginning of the design process. Following this method, the mechatronic system is decomposed into mechatronic modules, which are further broken down into discipline-specific subsystems with each subsystem characterized by a “model pillar”. These models allow the system to

have different degrees of detail and views, which in turn is explained as a transition from a “hierarchy of models” to a “hierarchy of parameters” of the design..

The “V-model” has been adopted by software development to suit mechatronic systems. Model content includes: Requirements, System Design, Domain-Specific Design, System Integration, Property Provisioning, and Modeling and Model Analysis. For complex products, the “V-model” is executed multiple times, increasing product maturity by showing that system integration - verification and validation - are important and consistent with system requirements and design.

Briefly, the following summaries can be made:

- The *hierarchical design method* is a powerful approach in solving the design challenges of modern mechatronic systems. Within the research community, it has the greatest popularity in the design of mechatronic systems.

- The “V-model” cannot be ignored because it defines the level of the integration design process, presents harmonized levels of engineering in the individual domains and brings together the domain-specific design with a macro level of collaboration.

Therefore, it is recommended to apply methods that integrate both design methods so that the advantages of each method are used.

Proven experience in the development of security systems, including mechatronics, which improve the CIs resilience, is possessed by leading researchers from the IMSETHC-BAS. Through their developments in the range of sensor elements [6÷11], in the field of nuclear security [12÷13] and in methodologies and technologies related to the overall resilience of the organization [14÷15], they provide proven in national and international projects scientific and applied basis with a contribution to the development of security systems.

3. Conclusions

There are established in international standards and confirmed in practice interdependencies between the CI resilience and management disciplines adopted. Business continuity management, risk assessment and physical security management are the primary sources of information on the type, structure and scope of security systems, as well as their integration into the overall CI security system. This improves CI resilience by facilitating the adaptation of identified critical assets to the possible effects arising from likely risks and threats.

Precisely this approach was used in the scientific developments under Work package 2 “Intelligent security systems”, under the QUASAR project and under project #06.00 “Some directions in the modeling of mechatronic security systems” from the Plan for scientific research activities in 2023÷2025 of the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre“ Acad. A. Balevski” at the BAS.

4 References:

- [1] <https://deming.org/explore/pdsa/>;
- [2] ISO/IEC 27001—Information security management;
- [3] ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes;
- [4] 22301:2019 Security and resilience — Business continuity management systems — Requirements;
- [5] Valeri Panevski, “Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems development – peripheral security systems”, International Scientific Journal “Security & Future”, 5-ти, 1-ви, Scientific Technical Union of Mechanical Engineering “Industry 4.0”, 2021, ISSN:2535-0668 (print), 2535-082X (online)), pp. 3÷6.

- [6] Kolarov Al. P., „INFLUENCE OF SEAWATER CHARACTERISTICS ON THE EFFICIENCY OF UNDERWATER OPTICAL COMMUNICATION SYSTEMS“, TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY. 2024, YEAR VIII, ISSUE 17, ISSUE 1 (Q17), Scientific technical union of mechanical engineering “Industry - 4.0”, 2024, ISBN:-, ISSN:ISSN 2535-0315(Print), ISSN 2535-0323 (Online), pp. 21÷24;
- [7] Kolarov A.P., Naydenov R.V., “Trends in the development of measuring equipment for sea water parameters”, “International Scientific Conference “CONFEC””, YEAR VII, ISSUE 2, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, 2023, ISSN:ISSN 2603-2945 (Print), ISSN 2603-2953 (Online), pp. 90÷94;
- [8] Kolev S, Nenova B, Ivanov I., “Powerful hydroacoustic transmitter”, Collection of reports from the International Security Conference “ConfSec 2023”, YEAR 7, ISSUE 1(9), ISSN (PRINT) 2603-2945, ISSN (ONLINE) 2603-2953, pp. 86÷87;
- [9] Nesterov K.N., Pehlivanski V.I., Liaskov N.G., “Examination of System for counteracting low-flying targets”, Proceedings XI International Scientific Conference “Technics. Technologies. Education. Safety”, 6, 2, STUME, 2023, ISSN:ISSN 2535-0315(Print), ISSN 2535-0323 (Online), pp. 130÷133;
- [10] Yavor Boychev., „SEISMIC PIEZOELECTRIC SENSOR MODEL“, XIX INTERNATIONAL SCIENTIFIC CONGRESS „MACHINES. TECHNOLOGIES. MATERIALS“, YEAR V, ISSUE 2 (22), STUME, 2022, ISSN:2535-0021(PRINT), 2535-003X (ONLINE), pp. 166÷169;
- [11] Vladimir Varbanov, „Classification of multiple objects based on seismic signal using SVM“, Proceedings VI International Scientific Conference “CONFSEC 2022”, 5-8 December 2022, Borovets, Bulgaria, 6, 1, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, 2022, ISSN:2603-2953, pp. 94÷96;
- [12] Dimitrov D., „Developing the opportunities for building nuclear security“, Technics. Technologies. Education. Safety. 2021, Military sciences and national security., Proceedings 3, 3(13), Scientific Technical Union of Mechanical Engineering “Industry - 4.0”, 2021, ISSN:ISSN 2535-0315 (Print), 2535-0323 (Online), pp. 208÷211;
- [13] Dimitrov, D, Randelova, N., “Management systems for nuclear security”, International Scientific Journal “Security&Future”, 8, 1, STUME, 2024, ISSN:2535-0668 (print); 2535-082X (online), pp. 7÷10;
- [14] Tumbarska A., “Non-lethal technologies for forced stopping potentially dangerous vehicles and vessels”, International Scientific Journal “Security&Future”, 5, 2, STUME, 2021, ISSN:2535-0668, pp. 71÷74;
- [15] Valentina Nikolova, Ivan Ivanov, Lilia Damyanova, Oleg Lagunov, “Methodology for testing and determining the safe subsequent use of after-use of fire protection clothing cleaned after use in accidents”, Proceedings VI International Scientific Conference “CONFSEC 2023”, 2023, ISSN:ISSN 2535-0668 (Print) ISSN 2535-082X3 (Online), pp. 112÷117.

The effect of central bank digital currencies on asset confiscation

Kolarov Todor,

Law Department, New Bulgarian University, Sofia, Bulgaria

e-mail: tkolarov@nbu.bg

Abstract: *The purpose of the article is to assess the ramifications of the introduction of retail Central Bank Digital Currencies (CBDC) in the field of asset recovery. Through systemic legal analysis, it strives to foresee benefits and challenges. The piece argues that since retail CBDC customer accounts are with the central banks, there is a potential for improved efficiency in asset freezing, seizing and confiscation, including international cooperation, as central banks may act as turnkey operators in the process. Further, there are identifiable benefits in the disposal phase. Possible programmable features and privacy considerations are among the challenges, along with the sheer volume of information that needs processing in asset tracing. The value of this article lies in the assessment of the effect of fundamental changes associated with the introduction of retail CBDC in the field of asset recovery.*

KEYWORDS: RETAIL CBDC, ASSET RECOVERY, PRIVACY AND DIGITAL RIGHTS.

1. Introduction

In the present day, the majority of central banks around the globe consider a Central Bank Digital Currency (CBDC). While as of 2024 only Jamaica, the Bahamas, Nigeria and Zimbabwe have their CBDCs launched, a large group of countries is in the CBDC pilot stage, including on retail CBDCs. The European Central Bank (ECB) and U.S. Federal Reserve (the Fed), while being in the research stage, are actively discussing piloting its respective retail digital currencies.

This new type of central bank currency led to academic discussions on its various aspects. Among the purported benefits of CBDCs, is the reduction of crime in general and economic crime in particular, including money laundering[1]. Yet, both international standards, such as FATF Recommendations, and national laws[2] view asset confiscation as a pivotal tool in curbing money laundering. This logical chain prompted the International Monetary Fund to devote special attention to the interrelation between national anti-money laundering framework and CBDCs in its upcoming Handbook on CBDC[3]. In light of this nexus, the goal of this piece is to explore the potential ramifications of the introduction of CBDCs with respect to asset confiscation.

The article strives to explore both the potential for positive and negative effects. In doing so, in Part I it sets the stage by outlining the major relevant characteristics of CBDCs and their legal nature. Part II focuses on the potential benefits that introduction of CBDCs could bring for asset recovery, centering not only on the law-enforcement level but also discussing policy aspects on national and international level. Part III centers on the challenges associated with the introduction of CBDCs on the asset confiscation arena. Following the same pattern as in the previous part, this part addresses both law-enforcement and policy level concerns. A noteworthy limitation of the research is its focus on the legal framework in the EU and the U.S. and the respective CBDC proposals by the ECB and the Fed.

The findings of the study support the conclusion that CBDC introduction has the potential to improve the effectiveness and efficiency of asset recovery. This is contingent on the programmable features of CBDCs, including but not limited to the guarantees for digital rights.

2. Relevant characteristics and legal nature of CBDCs

Much like banknotes, CBDCs are fiat currencies issued by central banks. Both the digital currency and the banknotes have value only because the respective central bank declares them to have such. This declaration with respect to cash is backed by the promise of the liability of the central bank in the amount printed on the banknote. Similarly, the CBDC is a ledger registration that certifies that a central bank is liable for the particular amount to the person who has title of the account. In fact, should one choose to deposit her physical currency in a commercial bank, the latter may opt to deposit this physical currency in the central bank in its own account. The central bank may choose to destroy this same banknote. Thus, the physical currency becomes digital and the

liability of the central bank towards the commercial bank is reflected in a digital form. Respectively, the liability of the commercial bank to the depositor of the cash is also reflected in a digital form. Therefore, one may argue that digital currency exists even today. For the same reason, through debit cards there is digital currency that is presently in use, regardless of the fact that the CBDC is a central bank liability, while debit cards represent a liability of a private financial institution.

The above describes an important difference between cash and CBDC. While cash deposited in a commercial bank makes that commercial bank liable to the depositor, CBDC is a liability of a central bank to the depositor. Dissimilarly, when one deposits physical currency in the commercial bank that in turn deposits the physical currency in the central bank, the liability of the central bank is towards the commercial bank. Central bank guarantees of deposits up to a certain amount in commercial banks does not change the fact that deposits in commercial banks are liability of the commercial banks.

Due to its characteristic as fiat currency, CBDC demonstrates differences in comparison to crypto assets. Crypto assets are not currencies but assets with money-like characteristics[4] without any underlying liability[5]. As assets, crypto assets have value. Both crypto assets and CBDC are in a digital format and with this respect they are similar. However, the value of the crypto assets is not based on the central bank fiat and could even be “minted” by anyone. Thus, the term “cryptocurrency”, which is in use to describe crypto assets, is misleading. In *Jarrett v. United States*, No. 3:21-cv-00419 (M.D. Tenn.), this aspect of crypto assets is discussed in some details. For instance, it is argued by the claimant that reward tokens for baking new blocks on the Tezos blockchain, which he accrued, “are property newly created by him during the baking process”[6].

With regard to stablecoins, one definition characterizes them as “private digital tokens that have an identifiable issuer or represent a claim and/or underlying assets”[7]. They “are generally created ... in exchange for fiat currency that an issuer receives from a user or third-party. To maintain a stable value relative to fiat currency, many stablecoins offer a promise or expectation that the coin can be redeemed at par upon request. These stablecoins are often advertised as being supported or backed by a variety of “reserve assets”” such as bank deposits or treasury bills, commercial paper, corporate and municipal bonds, or other digital assets[8]. Thus, stablecoins are assets, not currency. Even if they materialize liability of a private party that could vary depending on the stablecoin. Unlike bank deposits, this private party is not regulated and the deposit is not insured.

A final point to this part is that the legal nature of CBDC as a currency is contested. On May 4, 2023, Indiana Governor signed into law Senate Bill (SB) 468, amending the Indiana’s Uniform Commercial Code. The amended text reads, “[m]oney” means a medium of exchange that is currently authorized or adopted by a domestic or foreign government and is not in an electronic form. The term includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more nations. The term does not include a central bank digital

currency that is currently adopted, or that may be adopted, by the United States government, a foreign government, a foreign reserve, or a foreign sanctioned central bank”[9]. On May 12, 2023, Florida Governor signed into law Florida SB 7054, which amends the Florida’s Uniform Commercial Code with respect to the definition of money. According to the amendment, “[m]oney” means a medium of exchange that is currently authorized or adopted by a domestic or foreign government. The term includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more countries. The term does not include a central bank digital currency”[10]. While the matter in the U.S. is to be resolved on a federal level, efforts to block CBDC are present in the U.S. federal legislator as well.

It is noteworthy, that the above mention state legislation does not target CBDC in general but rather retail CBDC that is issued directly to the public by the central bank. Florida’s Uniform Commercial Code for example explicitly defines CBDC as such that is made directly available to a consumer by the issuing authorities, thus, leaving, it seems, the wholesale CBDC out of the scope of the legislation. This is understandable in light of the proclaimed anti-surveillance nature of such legislation – a point discussed in part III of this paper. However, both the ECB and the Fed envisage their respective digital currencies to be retail CBDCs.

Thus, CBDC is a currency in digital form issued by a central bank, which currency, like cash, is the liability of a central bank. Yet, unlike cash, CBDC does not provide anonymity of the underlying transaction, which justifies the transfer of the currency and allows tracing of the funds.

3. The benefits of CBDCs in the asset confiscation domain

The potential of CBDCs to affect positively the effectiveness and efficiency of asset confiscation is associated with the systemic effect of two characteristics of this currency – i.e. that it is liability of a central bank and that the transaction is not anonymous. As CBDC is a liability of the central bank, it is on the bank ledgers of the central bank. The Eurosystem is to be in charge of the CBDC settlement, which involves two element - settlement verification that digital currency in the requested amount is available in the payer’s digital euro account and settlement recording the digital euro transfer between the accounts in the ledgers[11]. Similarly, the Fed is to be the settling financial institution for payment transactions between end users of the digital dollar[12]. The research of the Fed and the ECB does not remove commercial banks from the equation, which are retaining the role of intermediaries who service customers on the front end, leaving the central banks with the task to process the actual payment on the back end. Commercial banks are intermediaries retaining customers’ digital wallets, rather than holding the money. In their intermediary capacity, they are a natural insulator against direct cyber-attacks on the CBDC.

Further, both the U.S. and the EU reject the possibility of tokenized CBDCs, which would bring their CBDCs closer to the anonymity of cash. Such an approach would make the CBDC susceptible to money laundering, while the CBDC benefit underscored in the research phase on both sides of the Atlantic is curbing money laundering[13]. In a tokenized CBDC, similar to crypto assets, the process authenticates the validity of a token, while in account-based retail CBDC, which is proposed for the digital euro and the digital dollar, there is a verification of the identity of the account holder. Thus, account holder identification is part of the process.

As the CBDC customer accounts are with the central bank rather than the commercial banks, there is a potential for improved efficiency in asset freezing, seizing and confiscation. As all CBDC accounts are with the central bank, freezing, seizing and confiscation of currency could be executed through a single freezing, seizing or confiscation order on a central level that could be implemented promptly. Further, there is a potential for asset recovery authorities to enjoy expeditious access to operational information, possibly through the Financial Intelligence Units

(FIU), on the actual amount in the CBDC accounts. While it is true that commercial banks, in their role as intermediaries, are to continue performing the customer due diligence associated with their anti-money laundering obligations, a system that requires to channel asset freezing requests through the commercial banks to the central banks seems redundant. As central banks keep the customer CBDC banking information, such a detour may seem unwarranted even if assessed against other policy considerations. Yet, such a legislative solution may be contentious as part of the purported rationale for commercial banks to retain the customer’s digital wallet is the privacy issue. Putting the intermediary in place allows for the identification process by the central bank to be indirect, thus ensuring a level of privacy.

Notwithstanding of the solution on the above point, the innate characteristics of the retail CBDC require collection and retention of significant amount of information to record transactions[14]. Regardless of whether a central bank will be the one-stop-shop for asset recovery of the currency it issues, the collected information is yet another database providing and additional resource for identification of funds that are subject to confiscation in the asset tracing stage.

Further, CBDC have the potential to affect international cooperation in freezing, seizing and confiscation of money. As CBDC are liability of central banks, customers’ digital euros and digital dollars appear on the bank ledgers of the ECB and the Fed, respectively. Thus, a large portion of the freezing, seizing and confiscation process could be concentrated in several central banks, as most of the laundered money is integrated in a few currencies. Under the above scenario, according to which the freezing is performed directly by central banks, the asset confiscation has the potential to become more effective due to the developed legislation and practice in the respective jurisdictions.

Regardless of whether asset freezing, seizing and confiscation of CBDC is executed directly by the central banks or through the commercial banks acting as intermediaries, CBDC introduction is likely to have the benefit of incentivizing improved adherence to anti-money laundering rules by non-compliant jurisdictions, which in turn will have positive effect on asset confiscation. This is due to the necessity for enhanced cooperation among central banks following the introduction of CBDCs[15]. This is likely to make commercial banks in jurisdictions falling under the FATF Gray or Black Lists experience greater difficulties in operating with the electronic currencies of FATF compliant jurisdictions as cooperation with these jurisdictions is dependent on regulatory coordination[16].

Additionally, even if the commercial banks act as the intermediaries through which asset recovery authorities process confiscation request, the central banks in a few jurisdictions will have the ultimate control over the frozen or confiscated funds. This could ensure that the disposal phase of asset recovery is executed in compliance with the best international practices. Such trends are identifiable even as of today. For example, on two occasions, in 2005 and 2014, Swiss courts ruled the repatriation of “Abacha loot” money to Nigeria on the condition of effective monitoring of the disposal of the funds, including to earmarking such funds for specific development projects[17]. In 2022, the U.S. followed a similar *modus operandi* with respect to “Abacha loot” funds confiscated in the U.S.[18].

In summary, there are prospects that CBDC introduction may improve the effectiveness and efficiency of monetary asset tracing, freezing, seizing, confiscation and disposal. This is the case on both national and international level.

4. The potential challenges for asset recovery following CBDC introduction

Like any new development, the advent of CBDC has the potential to bring about challenges along with the potential benefits. One of the challenges is associated with the programmability of CBDCs. While there is no final solution on this aspect in the Eurozone and the U.S., it is worth discussing the effect of CBDC programmed to have a set and announced inflation. In other word, a

feature inspired by Silvio Gesell's stamped money[19]. This is a realistic scenario as China is exploring the possibility of an expiration date for the digital yuan. Should a CBDC has an incorporated set periodic depreciation, it may lead to considerable reduction of the monetary value that is subject to confiscation. Even if the CBDC is frozen, disputes over its sharing in a transnational confiscation scenario may effectively "eat-up" part of the assets that are not disposed of in a timely manner. The above-mentioned disposal cases of assets confiscated from the former Nigerian Head of State Sani Abacha in the U.S. is note to point. It took almost 10 years to agree on the repatriation of some of the assets.

Another challenge is associated with the sheer volume of information that requires processing in the asset recovery arena. The finiteness of human resources in performing the monitoring has already been identified in analysis justifying the deployment of artificial intelligence for the task[20]. The spike in the number of transactions that could be monitored following CBDC introduction has the potential to present greater challenges for the identification of assets in the asset recovery process. Even before CBDC introduction recognition of the finiteness of human resources among the authorities charged with identification of corrupt practices, economic crime and the ultimate beneficial owners of entities involved in such practices seems to have been behind the Fifth EU Anti-Money Laundering Directive[21] provisions on public registry for ultimate beneficial owners. In the same vein, it is recognized that public ultimate beneficial owner registries provide an additional check against corruption[22]. However, in light of the European Court of Justice (ECJ) case law, namely *WM (C- 37/20)* and *Sovim SA (C- 601/20) v. Luxembourg Business Registers* such an access is restricted due to articles 7 and 8 of the Charter of Fundamental Rights of the EU. This development reinforces the argument in favor of artificial intelligence application in the asset identification phase.

This highlights another problem that asset confiscation in the age of CBDC faces, namely the quantitative privacy and digital rights. The public in the EU is mostly concerned with the effect of CBDC on the privacy of individuals. According to the 2021 Eurosystem Report on the Public Consultation on a Digital Euro, 43% of respondents in the EU identify privacy as the most important aspect of the digital euro[23]. According to a 2023 Cato Institute CBDC National Survey Report, 32% of respondents in the U.S. identify privacy as a concern with respect to the digital dollar[24]. Further, a 2016 Cato Institute Criminal Justice Survey indicates that 84% of Americans oppose *in rem* asset confiscation. Based on the above, it is reasonable to address the challenge associated with a potential decline in public support for asset confiscation due to the effect of CBDC on privacy.

De lege lata, in *U.S. v. Miller*, 425 U.S. 435 (1976), the U.S. Supreme Court rules that there is no legitimate "expectation of privacy" in information voluntarily provided as part of a commercial transaction to the banks in the ordinary course of business. Following this ruling, the U.S. introduced the Right to Financial Privacy Act (1978), which mandates the government agency to seek authorization from the person, subpoena or summons, or search warrant to access financial information. However, there are multiple exceptions, including for FinCen, the U.S. FIU. Further, in the recent case of *Poliselli v. Internal Revenue Service*, 598 US _ (2023), the U.S. Supreme Court ruled that the Internal Revenue Service does not need to provide notice of a summons if the summons are in aid of collection, in aid the collection of an assessment made or a judgment rendered, and it aids the collection of assessments or judgments "against the person with respect to whose liability the summons is issued." Finally yet importantly, in a 5-to-4 vote, the U.S. Supreme Court ruled in *Carpenter v. United States*, 585 US _ (2018) "third-party doctrine" in *Miller*, does not apply to cell phone site location in a criminal investigation.

Thus, recalling that CBDC financial information is accessible to the Fed, the keeper of bank ledgers, the latter may have a *de facto* access to site location due to multiple daily CBDC transactions. *Mutatis mutandi Poliselli*, asset recovery offices seeking to collect

the funds subject to freezing, seizing or confiscation are to operate without giving notice to the customer if accessing financial information available with the Fed. However, in light of *Carpenter*, the sheer volume of information that will become accessible collaterally to the asset recovery agency raises the question on how to reconcile the public policy objectives to curb illicit enrichment with the quantitative protection of privacy and digital rights in the asset recovery arena[25].

Similarly, privacy concerns come to fore in the EU. It is argued that CBDC introduction has the potential to lead to "absolute loss of privacy", as regardless of the General Data Protection Regulation 2016/679 (GDPR)[26], CBDC user are to transfer their personal information, including financial information, in its entirety to the state[27]. This view is consistent with the stance of the European Court of Human Right (ECHR) in *Sommer v. Germany*, application no.73607/13 (2017). According to the ECHR, the wide scope of banking information, namely all applicant's transactions in the course of two years, provides a complete picture of his professional activity for the said period. It is an argument for the ECHR to find such a limitation on the personal life disproportionate.

Further, the question emerges on whether GDPR or the Law Enforcement Directive 2016/680(LED)[28] rules apply to the FIUs[29] and asset recovery offices in the CBDC domain. This question is relevant in the field of asset confiscation as the Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation explicitly indicates that asset recovery offices are to comply with the LED. While it is true that Article 1, of the Directive (EU) 2024/1260 explicitly limits its application to asset recovery in criminal proceedings (paragraph 1) and non-conviction based confiscation under the "dead, mad, fled" rubric (paragraph 2 and Article 15), the problem remains as asset recovery in a number of EU member states is within civil proceedings. *Ergo* the question on GDPR or LED application stands.

As protection of privacy is balanced with the public policy objectives, in the *Sovim* ruling, CJEU established that unhindered access to ultimate beneficial owner registries for the FIUs, as provided for in Article 30, para. 5 of GDPR, is justified. As a potent tool in curbing money laundering, ultimate beneficial owner information needs to be available for the purposes of asset freezing, seizing and confiscation. Article 44, paragraph, 1 (b) of GDPR seems to provide indirectly basis for such an interpretation. Applying the same principle to concerns for encroachment over Article 7 and 8 of the EU Charter of Fundamental Rights in the asset confiscation arena, the details on the mechanism for access of such authorities to CBDC financial information bears clarification. The view that asset recovery authorities should enjoy an exception similar to that of FIUs with respect to CBDC financial information is unlikely to gain traction due to the sheer volume of collateral information. There are calls for the CJEU to strengthen digital privacy protection. The Luxembourg Court is criticized that it tends to erase the delineation between interferences subject to assessment under the proportionality test and interferences with the fundamental rights core with respect to privacy and data protection. The Court is requested to introduce a case-by-case review of restrictions on the rights of privacy and data protection [30].

In summary, the challenges facing the CBDC in the asset confiscation field, and not only, center on the adequate protection of privacy and digital rights. The legislators recognizing the inevitable effect of CBDCs on human rights but are yet to address them.

5. Conclusion

In conclusion, introduction of CBDC has the potential to strengthen the effectiveness and efficiency of asset recovery on national and international level. Depending on the manner in which a CBDC is programmed, central bank information on transactions could facilitate asset tracing, freezing, seizing and confiscation. Even if asset recovery offices are to take a detour, channeling request through commercial banks, the volume of information and lack of complete anonymity is conducive to improved efficacy of asset recovery. Further, CBDC has the potential to improve

international cooperation in anti-money laundering compliance and asset recovery. While programmability could bring benefits on the asset recover arena, it could also pose challenges. Potential set and announced inflation could lead to depreciation of CBDCs in delayed sharing and repatriation agreements in transborder asset recovery cases. Yet, the most pronounced challenge is the balancing of the public policy objectives to curb unexplained wealth, on the one hand, and protection of privacy and digital rights, on the other.

6. References

- [1] Schueffel, P., (2023) CBDCs: Pros and Cons - A Comprehensive List and Discussion of the Advantages and Disadvantages of Central Bank Digital Currency, Available at SSRN: <https://ssrn.com/abstract=4398748> or <http://dx.doi.org/10.2139/ssrn.4398748>.
- [2] Cassella, S.D., (2019) Nature and Basic Problems of Non-Conviction-Based Confiscation in the United States. "Veredas do Direito", Belo Horizonte, vol.16(34), pp. 41-65, 45.
- [3] IMF Policy Paper: IMF Approach to Central Bank Digital Currency Capacity Development (2023), available at <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/04/12/IMF-Approach-to-Central-Bank-Digital-Currency-Capacity-Development-532177> (last accessed Oct. 9, 2024).
- [4] Money and Payments: The U.S. Dollar in the Age of Digital Transformation. Research and Analysis of the Board of Governance of the Federal Reserve System (January 2022), p. 11.
- [5] Boar, C., Wehrli, A., (2021) Bank of International Settlement (BIS) Papers No 114. Ready, Steady, Go? – Results of the Third BIS Survey on Central Bank Digital Currency.
- [6] Parsons, A., (2022) Cryptocurrency, Legibility, and Taxation. "Duke Law Journal (Online)". Vol.72:1. p. 14.
- [7] Supra note 4 at p. 5.
- [8] President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. Report on Stablecoins. (November 2021), available at https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf (last accessed Oct. 9, 2024).
- [9] Senate Bill 468, available at <https://legiscan.com/IN/text/SB0468/id/2786710/Indiana-2023-SB0468-Enrolled.pdf> (last accessed Oct. 9, 2024).
- [10] Senate Bill 7054, available at <https://laws.flrules.org/2023/80> (last accessed Oct. 9, 2024).
- [11] 1.2. Settlement Model. Progress on the Investigation Phase of a Digital Euro – Second Report (ECB, December 2022), p. 6-7, available at <https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews221221.en.html> (last accessed Oct. 9, 2024).
- [12] Project Hamilton Phase 1. A High Performance Payment Processing System Designed for Central Bank Digital Currencies. Federal Reserve Bank of Boston and Massachusetts Institute of Technology Digital Currency Initiative, p. 1. Similarly, supra, note 3, p. 29.
- [13] Supra, note 3, p. 14.
- [14] Atako, N. N., (2021) Privacy beyond Possession: Solving the Access Conundrum in Digital Dollars. "Vanderbilt Journal of Entertainment and Technology Law" 23(821), pp. 821-854, 850.
- [15] Wang, H., Gao, S., (2023) The Future of the International Financial System: The Emerging CBDC Network and its Impact on Regulation, "Regulation and Governance", doi:10.1111/rego.12520.
- [16] Ibid.
- [17] World Bank Monitoring of Repatriated Abacha Funds, available at <https://www.worldbank.org/en/news/factsheet/2017/12/04/world-bank-monitoring-of-repatriated-abacha-funds>. (Last accessed Oct. 9, 2024).
- [18] United States Repatriates Over \$20 Million in Assets Stolen by Former Nigerian Dictator, available at <https://www.justice.gov/opa/pr/united-states-repatriates-over-20-million-assets-stolen-former-nigerian-dictator> (Last accessed Oct. 9, 2024).
- [19] More on the topic see J. Blanc, (1998) Free Money for Social Progress: Theory and Practice of Gesell's Accelerated Money, "American Journal of Economics and Sociology", 57(8), pp. 469-483.
- [20] Pavlidis, G., (2023) Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era, "Journal of Money Laundering Control". Vol. 26. No. 7, pp. 155-166. 158.
- [21] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU. OJ L 156, 19.6.2018, pp. 43–74.
- [22] Mooij, A. M., (2023) Reconciling Transparency and Privacy through the European Digital Identity, "Computer Law and Security Review", Vol. 48, doi.org/10.1016/j.clsr.2023.105796.
- [23] Available at https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf (last accessed Oct. 9, 2024).
- [24] Available at https://www.cato.org/survey-reports/poll-only-16-americans-support-government-issuing-central-bank-digital-currency?au_hash=xMsBqVIyxrCvcT_616tuU3kOKPBWjLIVDb251qmqZcE# (Last accessed Oct. 9, 2024).
- [25] On the term "quantitative privacy" and its substance see Citron, D. K., Gray, D. (2013) The Right to Quantitative Privacy, "Minnesota Law Review" 98(62).
- [26] OJ L 119, 4.5.2016, p. 1–88.
- [27] Montoya Santaolalla, C., (2023) Do Central Bank Digital Currencies (CBDC) Protect the Consumer or Are They a Mirage? [In]. Consumer Protection in the European Union: Challenges and Opportunities, Director & Coordinator: Santaolalla Montoya, C., European Commission Publishing, pp. 199-211, 207, ISBN 978-92-76-62083-9., available at SSRN: <https://ssrn.com/abstract=4371075> (last accessed Oct. 9, 2024).
- [28] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89–131.
- [29] Quintel, T., (2020) Data Protection Rules Applicable to Financial Intelligence Units: Still No Clarity in Sight. "ERA Forum", 23, pp. 53-74.
- [30] Brkan, M., (2019) The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning. "German Law Journal" 20, pp. 864–883, doi:10.1017/glj.2019.66.

Demographic change as a risk for the pension system and the stability of the security forces - experience from the Czech Republic

Jan Urbanec^{1*}, Dana Junkova²

Police Academy of the Czech Republic in Prague, Czech Republic¹

Police Academy of the Czech Republic in Prague, Czech Republic²

urbanec@polac.cz*

Abstract: At the end of 2022, the population of the Czech Republic reached 10,827,529, the highest ending population since the end of the Second World War. Although the migration wave from Ukraine, which included mainly children and women of working age, has slightly slowed the aging of the population, according to the Czech Statistical Office, the Economic Dependency Index has steadily increased between 2013 and 2022, from 57 to 72 non-productive age persons per 100 working-age persons. The sustainability of the financing of old-age pensions under the social security system is fundamentally conditioned by the demographic evolution of the population. The aging of society, which is a virtually universal phenomenon in the EU Member States, is, on the one hand, a manifestation of the desired rising standard of living, but at the same time, it creates pressure to find additional resources for the financial security of citizens in old age. The long-term imbalance of the pension system is a source of political demand for its adjustment, whether comprehensive or sub-parametric. Long-service allowances are an important financial instrument to increase the motivation of those interested in employment in the security forces. Thus, a possible reduction of its importance within the pension system, e.g. by relativizing the valorisation mechanism, may represent not only a threat to social reconciliation but also an indirect security risk for the state, consisting in a reduced demand for work in the police, firefighters and other professions. The paper aims to determine whether the general attitudes of the Czech public towards the pension system in the Czech Republic presented by the STEM agency correspond to the attitudes of full-time and distance learning students at the Police Academy of the Czech Republic in Prague, to identify any differences and to evaluate the possibilities of future long-term reduction of demographic risk for the pension system and for ensuring the stability of human resource capacity for the security forces.

Keywords: INTERNAL SECURITY, PENSION SYSTEM, POLICE, RISK, SECURITY FORCES

1. Introduction

At the end of 2022, the population of the Czech Republic reached 10,827,529, the highest ending population since the end of the Second World War. Although the migration wave from Ukraine, which included mainly children and women of working age, has slightly slowed the aging of the population, according to the Czech Statistical Office, the Economic Dependency Index has steadily increased between 2013 and 2022, from 57 to 72 non-productive age persons per 100 working-age persons.

Table 1: Characteristics of the age structure of the population of the Czech Republic¹.

Indicator	2023
Average age	42,8
Median age	44,0
Ageing Index	129*
Economic Dependency Index	71,9**
Note *	The number of people aged 65 and over per 100 children aged 0-14.
Note **	The number of children aged 0-19 and people aged 65 and over per 100 people aged 20-64.

The Czech Republic, like other EU countries, is facing unfavourable demographic trends that pose a risk to the sustainability of the public pillar of the pension system, which is based on the continuous financing of old-age pensions from the income of the economically productive population.

In terms of the economic and political background, it can be noted that: 1. While in 2000, approximately five economically active persons financed the pension of one pensioner, in 2050 this proportion should - with the unchanged demographic trajectory - change to only two workers per one pensioner; 2. In otherwise unchanged circumstances, this implies inexorable consequences - a reduction in the volume of resources for the payment of pensions (i.e. a reduction in the level of pensions) or a necessary increase in social contributions of the economically active population; 3. Another possible consequence is a further deepening of the deficit of the pension system, which is already subsidized by other public revenues within the state budget (taxes). In 2023, this deficit amounted to almost EUR 3 billion, representing a full 25 % of the total annual deficit of the state budget of the Czech Republic [2,3].

4. Developments show that the degree of political consensus needed to implement strategic change or even just parametric changes, has been insufficient for a long time. This can be illustrated by the fate of the pension reform pushed through in 2010-2011, which, in addition to the existing state-financed social insurance system (Pillar 1) and voluntary, state-subsidised and standardised commercial supplementary insurance (Pillar 3), introduced a new pillar also based on the fund principle and reducing the social insurance contribution obligation (Pillar 2). This new element was abolished by the new government with effect from 2016, having been judged unattractive, unfair, and negatively impacting Pillar 1.

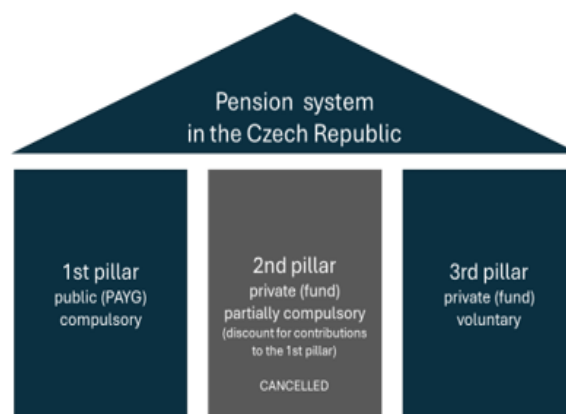


Fig. 1 Current pension system in the Czech Republic.

Subsequent attempts to find a new consensual basis for pension reform have already been unsuccessful, even though they relied on expert recommendations from government advisory bodies, which were represented by different currents of opinion. The only modifications that have been pushed through (2023) are those to increase the financial incentive to save or invest in the existing 3rd pillar. However, these also included controversial (and thus potentially revisable in the future) elements, such as the removal of state support from savings for economically active persons of retirement age. This part of the changes was even challenged by the opposition as unconstitutional (the Constitutional Court, which was asked to review the compliance of the changes with the Czech constitutional order, has not yet ruled on this matter).

2. Theoretical basis and selected facts

The starting point of the research is The Conceptual Field of Internal and External Security (Fig. 2), in particular the second and third dimensions of internal security, social influences of the organization, legal systems, and material aspects of human existence.

The conceptual field of the internal and external security	1 st dimension	2 nd dimension	3 rd dimension	4 th dimension
	Ideas, values. Mental wealth of man.	Social influences of the <u>organization</u> Legal systems	Material aspects of the human existence.	Cyber Space.
State forms of protection:	- Police - Army - Internal security - External security			
Private forms of protection	Private/business security services			
The time aspect	Past – present - future			

Fig. 2 The conceptual field of the internal and external security of the state⁴.

Security and security policy is becoming more and more a non-military concept, reaching into areas that were previously unthinkable and unimaginable in this context. Security forces in the Czech Republic defined by Act No. 361/2003 Coll., on the employment relationship members of the security forces, as amended, are the Police of the Czech Republic and the Fire Rescue Service of the Czech Republic, the Customs Administration of the Czech Republic, the Prison Service of the Czech Republic, the General Inspection of the Security Forces, the Security Information Service and the Office for Foreign Relations and Information.

The importance of the Police as a guarantor of internal security and now as one of the actors supporting society-wide resilience to crises is growing [5]. The consequences of the demographic ageing of the population can also be seen in the Police of the Czech Republic. Since 2010, the proportion of police officers over 40 years of age has been steadily increasing (in 2018 it reached one third), and the average age has increased by two years in just five years. At the same time, the structural understaffing of police officers is increasing faster than the restocking (in 2018 it grew three times faster than the restocking) [6].

Long-service allowances represent a specific incentive financial instrument within public finances to take into account the increased occupational risks in the security forces and thus strengthen the demand for this profession. The long-service allowance is paid to members of the security forces when they leave the service after serving at least 15 years. It is paid regularly every month. The more service a member has, the more long-service allowance he or she receives. The maximum amount is set at 60 % of the average monthly gross salary after 20 years of service. At retirement age, the long-service allowance may be received for a maximum of two years. In effect, it can be described as a supplement to the state pension for the recipient who is no longer economically active (increasing the benefit that would otherwise flow to the recipient from the standard old-age pension).

It is clear from Table 2 Retirement allowance versus the average old-age pension in the Czech Republic (2024, EUR), that the amount of the long-service allowance (at its maximum level) represents a significant supplement to the old-age pension for a member of the security forces. Considering the highest grades within tariff step 7 (up to 21 years of experience), which generally reflects education and rank, the pension ranges from 105 to almost 170 percent of the average old-age pension in the Czech Republic in 2024.

Table 2: Retirement allowance versus the average old-age pension in the Czech Republic (2024, EUR)^{7,8}.

Salary grade	5	6	7	8	9	10	11
Tariff salary, 20 years of experience	1444	1558	1683	1817	1964	2122	2294
Maximum amount of retirement allowance	867	935	1010	1090	1178	1273	1376
Retirement allowance versus average old-age pension	105 %	113 %	122 %	132 %	143 %	154 %	167 %

The consolidation state budget policy of the current government of the Czech Republic, initiated by the adoption of the so-called “consolidation package” at the end of 2023 (with effect from 2024), implies the intention to limit the increase of old-age pensions and financial rewards for civil servants, including the salaries and retirement allowances for members of the security forces.

Table 3: Annual growth of old-age pensions in the Czech Republic⁷.

Year	2024	2023	2022	2021	2020	2019
Average old-age pension (EUR)	826	809	692	615	577	536
Year-on-year increase	2 %	17 %	12 %	7 %	8 %	8 %

In the Czech Republic, the valorization of retirement allowance is closely linked to the valorization mechanism for old-age pensions (a 1% increase in pensions corresponds to a 0.5% increase in retirement allowance) [9]. However, such a significant reduction (cf. the increases in 2019-2023 and then 2024 - see Table 3.), consisting in the correction of the valorization mechanism for the security forces, may pose not only a threat to social reconciliation but also an indirect security risk for the state, consisting in reduced demand for work in the police, firefighters, customs officers, and other professions.

3. Solution of the examined problem

Public attitudes towards possible political reforms fundamentally determine the subsequent interest of the political representation in seeking possible solutions. Taking into account the previous developments in political decision-making described above, it can be concluded that ideas about a fair and effective approach to setting up a pension system diverge along the traditional left-right axis, similarly to, for example, the approach to the tax system or the necessity and meaningfulness of state intervention in the economy in general. Knowing the preferences of citizens must be seen not just as a corridor for undesirable populist policies, but as a prerequisite for finding the aforementioned long-term social consensus. The group of people who are aiming for a security-oriented university education represents a potentially statistically interesting segment in mapping public attitudes. It is a diverse group in terms of age, gender, and region. It represents a future and existing source of manpower in the security forces and thus makes it possible to analyse, among other things, the importance of the aforementioned concept of long-service allowances.

The aim of the paper is to determine whether the general attitudes of the Czech public towards the pension system in the Czech Republic presented by the STEM [10] agency correspond to

the attitudes of students at the Police Academy of the Czech Republic in Prague, to identify any differences and to evaluate the possibilities of future long-term reduction of demographic risk for the pension system and for ensuring the stability of human resource capacity for the security forces.

The questionnaire survey, carried out on a sample of 108 students of full-time and combined study programmes at the Police Academy of the Czech Republic in Prague, investigated attitudes to selected issues related to the setting of the pension system in the Czech Republic and its possible future changes. Approximately 65% of men and 35% of women responded. A full 60% of respondents are already working in a public sector job or service (of which over 75% are in the police, fire service or customs).

4. Results

The initial question focused on how respondents from the Police Academy of the Czech Republic perceive and generally evaluate the current pension system (especially the level of pensions). Respondents evaluated the pension system in the Czech Republic on a scale of 1-10 points (1 = completely unsatisfactory, 10 = completely satisfactory).

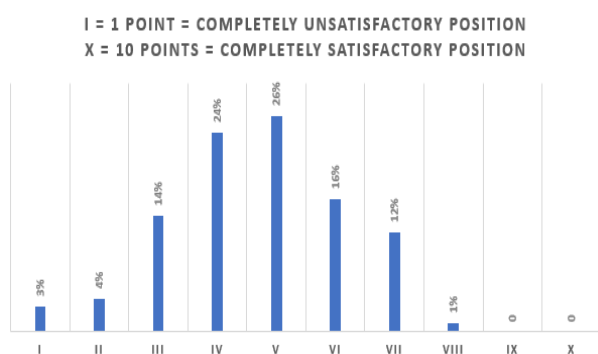


Fig. 3 Overall assessment of the current pension system (level of pensions) in the Czech Republic.

As shown in Fig. 3, 71% of respondents rated the situation below average on a scale of 1-5 points, 29% of respondents rated it on a scale of 6-8 points. The average score was 4.7 points and they rated the pension system as rather unsatisfactory.

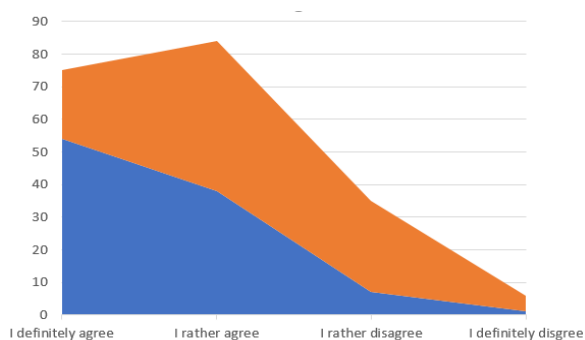


Fig. 4 Long-service allowances play a significant role in the decision to join the security forces (blue area) and long-service allowances make the salary competitive (orange area).

The respondents confirmed (Fig. 4) the crucial importance of long-service allowances as a motivator for applicants to apply for jobs in the security forces, with 54% identifying it as a very important element and a further 38% as important. For two-thirds of respondents, long-service allowances are an instrument without which the remuneration of security forces officers could not be competitive in the labour market.

Furthermore, opinion was sought on the reintroduction of individual pension savings (the so-called second pillar, compulsory individual savings), but with more favorable parameters and guarantees for the citizen who saves in this way. From the point of view of almost 60% of respondents (Fig. 5), it would be advisable to reinstate the so-called second pillar, provided, however, that there are adequate incentives (for entering this pillar) and guarantees (against investment risk).

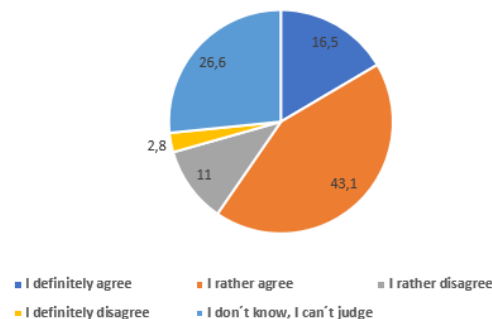


Fig. 5 Reintroduction of individual pension savings (the so-called second pillar).

At the same time, it was found that the vast majority (87%) of respondents declared that they were able and willing to save individually for their retirement in an amount higher than 2.5% of their regular earnings, and a fifth of them even more than 5%. The proportion of those who support and reject incentives derived from the number of children raised in the pension system is quite balanced.

Fig. 6 below shows the comparison of responses of respondents from the Police Academy of the Czech Republic in Prague (PA) and of respondents of the analytical institute STEM, which monitors and evaluates trends, attitudes, and moods that shape Czech society for the following questions: 1. Do you think the current pension system is fair? 2. In your opinion, is the average old-age pension sufficient to cover the basic needs of pensioners? Would you say that the current pension system allows people to spend a dignified old age? 4. Do you understand the rules by which the amount of the old-age pension is calculated today? 5. Would you say that the media has successfully described and explained the government's reform intentions in the following area – pension system?

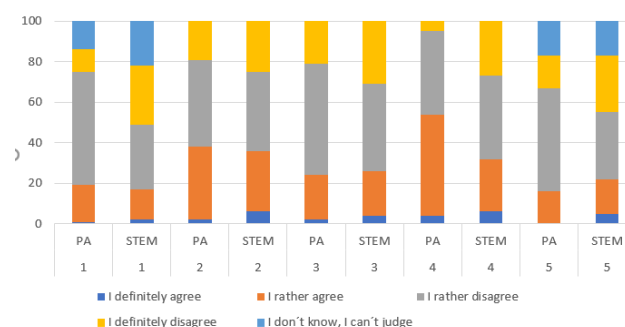


Fig. 6 The comparison of answers (to questions No. 1-5) of respondents from the Police Academy of the Czech Republic in Prague (PA) and of respondents of the analytical institute STEM.

In terms of comparing the attitudes of respondents from the Police Academy and STEM [10], it can be concluded that: (a) for questions No. 1, 2, 3, 5, there was basically a consensus: the majority of respondents (61-76%) expressed a disagreeing opinion in the category (rather no or definitely no); (b) For question No. 4, Police Academy respondents expressed a positive opinion (54% of them answered in the category rather yes and definitely yes), while

STEM respondents were more sceptical (68% answers were in the category rather no and definitely no).

Thus, it can be briefly summarised that both Police Academy and STEM respondents unanimously do not consider the current pension system to be fair; that the current average level of old-age pensions is not sufficient to cover basic needs, let alone to ensure a dignified life; and that the media has not been successful in adequately describing and explaining the government's intentions for pension reform. Respondents from the Police Academy were more optimistic about their ability to understand the rules by which the amount of old-age pensions are calculated today than STEM respondents.

5. Discussion and conclusion

The paper aimed to determine whether the general attitudes of the Czech public towards the pension system in the Czech Republic presented by the STEM agency correspond to the attitudes of students at the Police Academy of the Czech Republic in Prague, to identify any differences and to evaluate the possibilities of future long-term reduction of demographic risk for the pension system and for ensuring the stability of human resource capacity for the security forces.

Both empirical surveys, which are subject to this article, confirmed the thesis that finding a wider social consensus for the implementation of the necessary reforms of the Czech pension system, reflecting the long-term demographic trends, will be very difficult. It can be stated that the basic agreement now exists only on the fact that Pillar 1 should remain a main element of the pension system and that it needs additional financing. The political debate in the Czech Republic, which is currently being held, focuses dominantly on the parametric revision under Pillar 1 - on the possible revision of the retirement age, taking into account exemptions for so-called demanding professions, the setting of early retirement pensions or on the adequacy of self-employment contributions. Even here, however, the necessary consensus does not emerge, with some major opposition forces essentially questioning the very principle of the need to intervene in the first pillar and offering as a solution instruments consisting in better collection of taxes and insurance contributions to the state budget. The prospect of the forthcoming general parliamentary elections then offers no realistic prospect of virtually any proposals in this area being approved in this period, with the hope that they will not be substantially revised by the next political representation. Any possible wider change poses a risk of disrupting social harmony – both in the case of a possible increase in contributions imposed on the economically active population and in the case of insufficient valorisation of retirement benefits for elderly people, on the contrary. Also, the pro-family policy seems to be reaching its ceiling (when additional incentives for parents at the expense of non-parents are already beginning to be perceived as unfair).

Of course, such a conclusion should not be an incentive to do nothing. The solution may, at least in part, consist in finding a compromise, where each part of the political spectrum brings its positive priorities to the reform (e.g. increasing the tax revenues of the state budget) while it accepts some of the positive priorities of its ideological opponents (e.g. strengthening the importance of individual savings or investing citizens for pension). Emphasis on the general financial literacy of citizens is also important so that they better understand the logic of redistribution and the limits of Pillar 1. During the reforms, special attention should be paid to future pensioners arising from members of the security forces. The long-term feeling of inadequately low financial remuneration, including the long-service allowances, can be a source of a decrease in interest in working in the security forces and lead to substitution on the labour market towards better-paid or less dangerous civilian professions.

6. References

1. J. Koukalová. Populační vývoj Česka v roce 2023. *Demografie*, 66, 3 (2024).
2. Ministry of Finance of the Czech Republic. The Czech pension insurance system performance report, (2024). <https://www.mfcr.cz/cs/rozpocetova-politika/statni-rozpocet/hospodareni-systemu-duchodoveho-pojisteni>
3. Ministry of Finance of the Czech Republic. Final account of the state budget of the Czech Republic for the year 2023 – executive summary, (2024). <https://www.mfcr.cz/cs/rozpocetova-politika/statni-rozpocet/rychla-shrnuti-statniho-rozpocetu/exekutivni-shrnuti-statniho-zaverecného-uctu-za-ro-55874>
4. D. Junková, M. Kný. Interakce znalostní teorie a policejní praxe se zaměřením na oblast důvěryhodnosti policejního sboru. In: *Důvěryhodnost Policiejního sboru na pozadí aktuálních otázek policajnej teórie a praxe*. Bratislava: Akadémia Policiejného sboru v Bratislave, S. 145-157, (2021). ISBN 978-80-8054-904-6.
5. D. Junková, M. Kný. Fuzzy Problems in Security Management: New Threats and the Importance of Tacit Knowledge in the Police of the Czech Republic. In: *Security in Central and Eastern Europe: cyberspace, police, prisons, transport, addictions, the media*. Krakow: University of Public and Individual Security "Apeiron" in Krakow, s. 52-64, (2020). ISBN 978-83-64035-72-2.
6. Policejní presidium České republiky. Koncepce rozvoje policie ČR do roku 2027, (2020). https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/koncepce_rozvoje_pol.pdf
7. Czech Social Security Administration. The average amount of solo retirement pensions in the Czech Republic, (2024). https://www.cssz.cz/documents/20143/99428/bPrumerna_vyse_solo_duchodu_v_CR_v_casove_rade.pdf/a9b4355f-343f-7f3c-eaef-485a15ec2098
8. Government Regulation No. 419/2022 Coll., on the scale of basic tariffs for members of the security forces.
9. Ministry of the Interior of the Czech Republic. Valorization of pensions and long-service allowances in 2025, (2024). <https://www.mvcr.cz/clanek/valorizace-duchodu-a-vysluhových-prispevku-v-roce-2024.aspx>.
10. Stem.cz. Česká veřejnost a důchodový systém v květnu 2024: postoje zůstávají, zájem o reform mírně klesá (2024). <https://www.stem.cz/ceska-verejnost-a-duchodovy-system-v-kvetnu-2024-postoje-zustavaji-zajem-o-reformy-mirne-klesa/>

IIoT and cyber security in industrial enterprises

Petar Georgiev¹, Krasimira Dimitrova²
 Technical University of Varna, Bulgaria¹
 Technical University of Varna, Bulgaria²
 petar.p.georgiev@tu-varna.bg

Abstract: Digital transformation and sustainable development are key concepts that are actively developing in modern business and society. They go hand in hand, creating opportunities to improve efficiency, reduce the negative impact on the environment and increase people's quality of life. The Industrial Internet of Things is a powerful tool for connecting industrial devices, sensors, and equipment to a network to improve monitoring, analysis, and process automation. With the increasing digitization of business in recent years, cyber-attacks are also on the rise. To protect against such actions, organizations need cybersecurity technology solutions, as well as reliable tools to detect, prevent, and respond to cybersecurity breaches. This publication presents an exploration of the combination and interconnectedness of IIoT and cybersecurity in industrial enterprises, which are necessary to keep these systems secure and protected from cyber threats. A conceptual framework for multi-layered cyberattack defense designed for industrial enterprises is proposed.

Keywords: IOT, IIOT, IIOT NETWORKS, CYBER-ATTACKS, CYBER SECURITY.

1. Introduction

Digital transformation is the process of integrating digital technologies into all aspects of a business or organization, resulting in significant changes in the way a business operates and creates value for customers.[9] Sustainable development is a concept that aims to meet the needs of the present generation without compromising the ability of future generations to meet their own needs. [13]

The concept of IoT first appeared as a term and as a concept in the late 20th century. British digital transformation expert Kevin Ashton is considered the founder of this concept. It defines the Internet of Things as a collection of identifiable connected objects using radio frequency identification (RFID) technology. According to Ashton himself, this concept considers the organization of such networks as a phenomenon capable of reorganizing economic and social processes in such a way as to exclude the need for human participation in some of the actions and operations. This practically marks the beginning of another revolutionary concept - Industry 4.0. This concept represents a profound transformation of the industrial sector, leading to new levels of productivity, efficiency, and sustainability. Combining technologies from different fields, it offers not only the improvement of existing processes, but also the creation of new opportunities for innovation and development. This integration will continue to change the way people live and work, ensuring a more sustainable and productive future.

IIoT is a specialized part of the broader IoT concept that focuses on connecting industrial devices and systems in a network. This technology aims to optimize industrial processes through real-time data collection and analysis, automation, and integration of various systems. [19] IoT is a concept where physical objects and devices are equipped with sensors, software, and network capabilities to collect and exchange data over the Internet. Key aspects of IoT are smart devices, data collection and analysis, automation and convenience, user applications, etc.

IoT and IIoT are two closely related but also different concepts that are used to improve processes and systems in different fields. Both technologies aim to use data and connected devices to improve various aspects of life and work but are used in different contexts and for different purposes.

At the same time, they are also strongly related to cyber security, as industrial IoT systems that connect machines, sensors and control systems are vulnerable to various cyber threats. IIoT networks automate and optimize industrial processes in sectors such as manufacturing, energy, and transportation, but also open new opportunities for cyberattacks that can cause serious damage to critical infrastructure. According to Fortinet's Forti Global Threat Landscape Report 2H 2023 [25], cybercriminals are exploiting new industry vulnerabilities 43% faster than the first half of 2023.

Organizations need a robust framework to help them define their approach to cybersecurity and minimize the consequences of a potential attack. It should emphasize protecting critical systems, detecting, and responding to threats, and recovering from an attack.

2. Industrial internet of things (IIoT)

For industrial enterprises, the concept of IIoT is of particular importance. IIoT represents a powerful tool for the transformation of industrial processes. Through the integration of connected devices, sensors, analytical tools, and automated systems, IIoT offers significant benefits such as increased efficiency, improved quality, and reliability, as well as greater flexibility. Although there is security, interoperability and change management challenges, the potential of IIoT to revolutionize the industry is significant and will continue to develop in the future.

IIoT offers significant advantages for optimizing production processes but requires complex infrastructure and advanced technologies. To ensure the security and efficiency of these systems, it is necessary to implement strict cyber security measures, use modern communication networks, cloud, and distributed computing resources, as well as constant monitoring and analysis of data. [19] These measures will help minimize risks and ensure the continuous operation of industrial systems in an increasingly digitized and connected environment.

IIoT integration in industrial enterprises brings significant advances in efficiency, productivity, and automation. However, it also introduces new cybersecurity challenges that must be addressed to protect critical infrastructure and sensitive data.

The most important benefits of IIoT for industrial enterprises can be classified as follows:

- *Improved operational efficiency:* IIoT devices enable real-time monitoring and control of industrial processes, resulting in optimized productivity and reduced downtime.
- *Predictive maintenance:* Sensors and analyses can predict equipment failures before they occur, enabling timely maintenance and reducing unplanned downtime.
- *Improved productivity:* Automation and data-driven decision-making streamline processes and increase overall productivity.
- *Supply Chain Management:* Real-time tracking and analyses improve supply chain visibility and efficiency.

Despite the benefits they bring to businesses, many industrial IoT devices are designed with an emphasis on functionality rather than security. This makes them easy targets for attacks. Connecting multiple devices creates a complex network where even a weak connection can open access for cybercriminals. Attacks against IIoT systems can have physical consequences, such as stopping

production or damaging equipment. Many IIoT devices do not support regular security updates, making them vulnerable to new threats. Therefore, as IIoT networks evolve, cybersecurity becomes a critical aspect for these technologies.

3. Cybersecurity challenges in IIoT

While IIoT offers numerous benefits to industrial enterprises, it also presents significant cybersecurity challenges that must be proactively managed. Implementing robust cybersecurity measures, being aware of emerging threats, and continuously updating security protocols are essential steps to protect industrial systems and ensure the reliable and secure operation of Internet of Things networks. [8] By prioritizing cybersecurity, industrial enterprises can fully take advantage of IIoT benefits while minimizing risks. Some of the most serious IIoT challenges are related to:

- *Cybersecurity*: Protecting connected devices and data from cyberattacks is critical.
- *Data and Privacy*: Ensuring data privacy and integrity.
- *Compatibility*: Integration of devices and systems from different manufacturers requires standardization and compatibility.
- *Change Management*: Adapting new technologies and processes can be complex and requires effective change management.

The study is done in close cooperation with specialists from Schneider Electric Bulgaria Ltd.24 and Testel Engineering Ltd.

The results can be summarized as follows:

- *Expanded scope for attack*: The proliferation of connected devices expands potential entry points for cyberattacks.
- *Legacy obsolete systems*: Many industrial systems were not designed with cybersecurity in mind and are vulnerable to modern cyber threats.
- *Complexity and integration*: Integrating IIoT devices with existing information and operational technologies and networks adds complexity, making security management more challenging.
- *Data confidentiality*: Ensuring the confidentiality and integrity of data collected and transmitted by IIoT devices is critical.

The results show that IIoT requires a complex infrastructure and multiple complementary technologies to ensure efficient connectivity, processing, and data transfer.

4. Key tools and techniques used in cyber attacks

Cyber-attacks pose a serious threat to modern computer systems, networks, and data. Attackers use a variety of tools and techniques to compromise systems and achieve their goals. The main tools and techniques used for cyber-attacks can be grouped into several groups:

1. Malware: [18]

- *Viruses*: Programs that spread and infect files on computers, changing or deleting data.
- *Trojans*: Malware that pretends to be legitimate and is used to gain access to the victim's system.
- *Worms*: Only spreading programs that spread over networks and cause damage to systems.
- *Spyware*: Programs that track and collect information about the user without their knowledge.
- *Ransomware*: Software that encrypts the victim's data and demands a ransom to restore access to it.

2. Attack tools [14]

- *Metasploit*: A popular framework for developing and executing exploits and penetration tests. Often used for vulnerability testing. [16]
- *Nmap*: A network scanning tool that helps detect active hosts and open ports. [1]
- *Wireshark*: A network analyzer used to capture and analyze network traffic. It can be used to monitor communication and discover data. [24]
- *Burp Suite*: A web application analysis tool used to identify vulnerabilities and weaknesses in web-based applications. [22]
- *Aircrack-ng*: A set of tools for analyzing and cracking WEP and WPA/WPA2 cryptographic protocols in wireless networks. [7]

3. Techniques and Strategies

- *Phishing*: Social engineering, where attackers send fake messages (emails, messages) in order to gain personal information or access to systems. [4]
- *DDoS attacks (Distributed Denial of Service)*: Attacks that use multiple compromised devices (botnets) to overwhelm the target server with traffic and make it unavailable.[6]
- *SQL Injection*: Attack where malicious code is injected into an SQL query to gain unauthorized access to a database. [2]
- *Cross-Site Scripting (XSS)*: A technique where malicious code is embedded in a web application to execute in the user's browser. [21]

5. Key cybersecurity measures for IIoT

To protect IIoT networks, companies are taking measures as:

- *Network segmentation*: Isolate IIoT devices from other network segments to contain potential breaches.[25]
- *Strong authentication and authorization*: Implement multi-factor authentication and strict access control to ensure only authorized users and devices access the network. [5]
- *Encryption*: Encrypt data both in transit and at rest to protect it from interception and tampering. [12]
- *Regular updates and fixes*: Ensuring that all devices and systems are regularly updated with the latest security patches. [10]
- *Monitoring and detection of anomalies*: Using advanced monitoring tools and anomaly detection systems to identify and respond to suspicious activity in real time. [15]
- *Incident response planning*: Develop and regularly update incident response plans to quickly and effectively respond to cyber security incidents. [17]

Exploitation and analysis tools

- *Cobalt Strike*: An attack simulation and network defense testing platform used by security professionals and cybercriminals.
- *Empire*: A command-and-control framework was discovered that allowed attackers to control compromised systems.
- *Kali Linux*: An operating system specifically designed for penetration testing and vulnerability analysis, featuring multiple cybersecurity tools. [11]

6. Tools for ongoing evaluation and maintenance

- *Nessus*: A vulnerability scanning tool that identifies potential weaknesses in systems. [20]

- *OpenVAS*: A vulnerability management system that scans and assesses vulnerabilities in networks and systems. [23]
- *Snort*: Network intrusion detection and network traffic analysis tool. [3]

7. Preventive protection measures

The common preventive measures that companies apply are:

- *Regular updates*: Keeping software and systems up to date to protect against known vulnerabilities.
- *Password security*: Use of strong and unique passwords and implementation of two-factor authentication.
- *Training and awareness*. Constant training and caution when opening files and links from unknown sources, recognizing phishing attempts and safe browsing practices.
- *Monitoring and reaction*: Implementing incident monitoring and response systems to detect attacks in time and respond quickly.
- *Regular backup*: Regularly back up critical data and systems to recover information in the event of an attack. Maintaining up-to-date archives of important data. Storage of backup copies in a safe place - offline or in a cloud structure with enhanced security measures
- *Attention by email*: Beware of email attachments and links, especially from unknown or unsolicited sources.
- *Network security*: Implementing special network security measures, including firewalls and intrusion detection systems.

Understanding the tools and techniques used by hackers is an important part of building an effective cybersecurity and data protection strategy.

The information from this survey shows that more than half of the survey participants face challenges related to the many failed tools and individual solutions for data protection, security, sovereignty, localization, storage, and privacy. That information clearly shows the need for a multi-purpose and multi-aspect cyber security system that covers all processes and resources of industrial enterprises.

8. Multi-layered protection against cyber attacks

Based on the literature review and the study of global practices and in close cooperation with specialists in the field of information and communication technologies, the idea was born to develop a conceptual framework of a model for the multi-layered protection of all assets and processes of the industrial enterprise from cyber-attacks.

This defense against a cyberattack is a cybersecurity strategy that involves the use of several layers to prevent and minimize the risks associated with attacks. It is because no single defense mechanism is reliable, therefore several different systems are implemented at different levels to provide a more complex and sustainable protection.

Multi-layered cyber defense is an approach that involves the use of various defense measures at multiple levels to provide maximum protection against cyber threats. This approach is important because cybercriminals use a variety of methods and tools, and no single measure can provide complete protection. The protection provides flexible and comprehensive protection by combining different technologies and strategies to address diverse cybersecurity threats. By integrating various security measures and approaches, organizations can reduce the risk of successful attacks and provide a higher level of security to their systems and data. The need for this type of reliable protection is becoming more and more tangible and imperative, especially in industrial enterprises, given the fact that they create and operate a large volume of sensitive information about their products, processes, customers and partners, as well as for

scientific research, innovation, markets, contracts, etc., which is directly related to their competitiveness and sustainable development. This information is very often subject to malicious attacks.

IIoT and cybersecurity are critical aspects of modern industrial automation. As connected devices and systems increase, so does the risk of cyber attacks. Cybersecurity for IIoT is critical because these devices are often connected to the Internet and are vulnerable to various types of cyberattacks. Cyber attacks are a global problem and every organization needs to find the most secure and effective way to protect itself.

In the development of the concept of the model, well-known cyberattack protection tools were used, but they were integrated and interconnected in a system that provides three-layer protection against cyberattacks in real time to all assets, processes and resources of the enterprise. The model is universally applicable, and additional software modifications can be made for each specific enterprise, with a view to adapting it to the specifics of its activity.

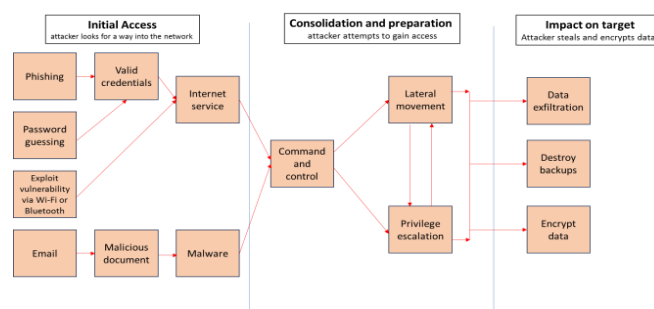


Fig. 1. A multi-layered cyber attack protection model designed for an industrial enterprise (Cybersecurity Framework)

The proposed network security concept is three-level:

First level (Initial Access) - at this level, the protections that operate stop the attacker and his access to the network by providing protection for the services performed in the Internet space (Internet-exposed services). The actions that are performed at this level are:

- Protection of Internet-exposed services act after Valid credentials and Exploit vulnerability and before Internet service,
- Correction of devices (Patching) works after Exploit vulnerability and before Internet service.
- Implementation of MFA (Multi-Factor Authentication) works before Valid credentials and before Internet services.
- Disable macros works after Malicious document and before Malware.
- Application allowlisting works after Malicious document and before Malware and also works at the end of Level 1 and before Level 2.
- Use of logging and alerting (Logging and alerting) operates immediately after Valid credentials, Exploit vulnerability and Malicious document and after the end of Level 1 and before Level 2.
- Password manager works after Password guessing and before Valid credential.

At the second level, Consolidation and Preparation, the defenses that work together to prevent an attacker from accessing network devices are:

- Correcting the devices (Patching), using network Network segmentation,
- Applying the principle of Principle of least privilege,
- Application of MFA (Multi-Factor Authentication)
- Logging and alerting usage.

All of these protections work after Command and control and before Lateral movement and Privilege escalation.

At the third level, Impact on Target, protections that try to stop or reduce the impact of an attacker from stealing or encrypting data are:

- Using Logging and alerting works before Encrypt data and Data Exfiltration. Using and maintains of (Backups) works before Destroy backups.
- Using a list of permitted applications (Application allowlisting) operates before Encrypt data.

These levels represent three layers of protection for all parts of the information system. The goal is that if one level is overcome by the attack, it will be stopped at the next levels, thereby limiting the damage to the security, data and information of the enterprise. The proposed protection framework provides an opportunity to significantly reduce the risk of successful attacks and improve the resilience of industrial systems and networks.

9. Conclusion

In an increasingly interconnected and digital world, robust vulnerability management is paramount to protecting critical information assets and maintaining the integrity of network infrastructures.

IIoT offers significant benefits to industrial processes, but these benefits come with new security risks that require a proactive and comprehensive approach to cybersecurity.

This study provides a comprehensive overview of the vulnerabilities of information security systems in industrial enterprises and the tools to counter cyber attacks against them. As a result of the study, a conceptual model of a system for multi-layered protection against cyber-attacks, designed for industrial enterprises, is proposed. The multi-layered protection provides an effective and reliable cybersecurity strategy that aims to minimize the risks associated with cyber-attacks. Different levels of protection provide a comprehensive approach to protecting data, infrastructure, and users, reducing the likelihood of successful attacks, and increasing the safety of the company across the country.

10. Acknowledgment

The authors express special thanks to Schneider Electric Bulgaria Ltd. and Testel Engineering Ltd. for the assistance provided in conducting the study and developing the concept of multi-layered cyber attack protection model.

11. References

- [1] A. Orebaugh, B. Pinkard, *Nmap in the Enterprise: Your Guide to Network Scanning*, Elsevier, (2011), ISBN 0080558747, 780080558745
- [2] A. Sadeghian, M. Zamani and S. M. Abdullah, "A Taxonomy of SQL Injection Attacks," (2013) International Conference on Informatics and Creative Multimedia, Kuala Lumpur, Malaysia, (2013), pp. 269-273, doi: 10.1109/ICICM.2013.53
- [3] B. Caswell, J. Beale, A. Baker, *Snort Intrusion Detection and Prevention Toolkit*, Syngress, (2007), ISBN 0080549276, 9780080549279
- [4] B. B Gupta, A.Tewari, Jain, et al. Fighting against phishing attacks: state of the art A.K. and future challenges. *Neural Comput & Applic* **28**, 3629–3654 (2017). <https://doi.org/10.1007/s00521-016-2275-y>
- [5] B. Vaidya, D. Makrakis and H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network," in *IEEE Network*, vol. **27**, no. 1, pp. 5-11, January-February (2013), doi: 10.1109/MNET.2013.6423185
- [6] C. Douligeris, A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, *Computer Networks* Volume **44**, Issue 5, 5 April (2004), pp 643-666, <https://doi.org/10.1016/j.comnet.2003.10.003>
- [7] E. Baray and N. Kumar Ojha, "'WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique'," (2021) 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, (2021), pp. 23-30, doi: 10.1109/ICCMC51019.2021.9418230
- [8] F. Arat, S. Akleyek, (2023), Attack Path Detection for IIoT Enabled Cyber Physical Systems: Revisited, *Computers & Security*, Volume **128**, May (2023), 103174, <https://doi.org/10.1016/j.cose.2023.103174>
- [9] G. C. Kane, D. Palmer, A. N. Phillips, D. Kiron, N. Buckley. (2015). Technology, drives digital transformation - becoming a digitally mature enterprise. *MIT Sloan Management Review*. Retrieved January 24, (2018), from <https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/>
- [10] G. Li, H. Liu, X. Chen, H.S. Gunawi, S. Lu (2019) Dfix: automatically fixing timing bugs in distributed systems. *PLDI (2019): Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation* pp 994 – 1009, <https://doi.org/10.1145/3314221.3314620>
- [11] G. Najera-Gutierrez, J. Ansari, *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*, 3rd Edition, Packt Publishing Ltd, (2018), ISBN 1788623800, 9781788623803
- [12] G. J. Popek, C. S. Kline, *Encryption and Secure Computer Networks*, *ACM Computing Surveys (CSUR)*, Volume **11**, Issue 4, pp 331 – 356, <https://doi.org/10.1145/356789.356794>
- [13] J. Sachs, C. Kroll, G. Lafortune, G. Fuller, F. Woelm – (2022). *Sustainable Development Report* (2022), Cambridge University Press, ISBN 978-1-009-21003-4,
- [14] M. Baykara, U. Gurturk and R. Das, "An overview of monitoring tools for real-time cyber-attacks," (2018) 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, (2018), pp. 1-6, doi: 10.1109/ISDFS.2018.8355339
- [15] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," in *IEEE Communications Surveys & Tutorials*, vol. **16**, no. 1, pp. 303-336, First Quarter (2014), doi: 10.1109/SURV.2013.052213.00046
- [16] M. Moore, "Penetration testing and metasploit", (2017), https://www.researchgate.net/profile/Michael-Moore-22/publication/318710609_Penetration_Testing_and_Metasploit/links/5978fddda6fdcc30bdc32be2/Penetration-Testing-and-Metasploit.pdf
- [17] N. Shinde, P. Kulkarni, *Cyber incident response and planning: a flexible approach*, [https://doi.org/10.1016/S1361-3723\(21\)00009-9](https://doi.org/10.1016/S1361-3723(21)00009-9)
- [18] O. Or-Meir, N. Nissim, Yuval Elovici, Lior Rokach, *Dynamic Malware Analysis in the Modern Era—A State of the Art Survey*, *ACM Computing Surveys (CSUR)*, Volume **52**, Issue 5 Article No.: 88, pp 1 – 48, <https://doi.org/10.1145/3329786>
- [19] R. A. Mouha, *Internet of Things (IoT)*, *Journal of Data Analysis and Information Processing*, Vol.**09** No.02(2021), Article ID:108574,25 pages, 10.4236/jdaip.2021.92006
- [20] R. Rogers, *Nessus Network Auditing*, Elsevier, (2011), ISBN 0080558658, 9780080558653
- [21] S. Gupta, B.B Gupta, Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management* Volume **8**, pp 512–530, (2017), <https://doi.org/10.1007/s13198-015-0376-0>
- [22] S. Wear, *Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite*, Packt Publishing Ltd, (2018), ISBN 1789539277, 9781789539271
- [23] V. Ndatinya, Z. Xiao, V. Rao Manepalli, K.Meng and Y. Xiao, Network forensics analysis using Wireshark, *International Journal of Security and Networks* Vol. **10**, No. 2, ISSN: 1747-8405, eISSN: 1747-8413, <https://doi.org/10.1504/IJSN.2015.070421>
- [24] W. R. Simpson, K. E. Foltz, *Network Segmentation and Zero Trust Architectures*, *Proceedings of the World Congress on Engineering* (2021) WCE 2021, July 7-9, (2021), London, U.K., ISBN: 978-988-14049-2-3, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)
- [25] Fortinet, *Global Threat Landscape Report 2H (2023)*; <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>

Automated Web Application Scanning with Wapiti, Selenium, and SQLMap

Zhaneta Savova¹, Stanislav D. Atanasov¹, Rosen Bogdanov¹
National Military University "Vasil Levski", Bulgaria¹
zh.savova@mail.bg, r61@abv.bg

Abstract: The security of web applications has become a crucial aspect in protecting users' data and personal information. The potential for vulnerabilities in web applications to result in data theft, loss of trust in service providers, and significant financial loss underscores the significance of robust automated web application scans. This research paper examines the use of tools such as Wapiti, Selenium, and SQLMap for automated web application testing. The primary objective is to assess the efficacy of automated scanning for a specific web application and to establish a benchmark for evaluating the results. The scope of the analysis encompasses the various security aspects covered by these tools and assesses their effectiveness and accuracy in detecting vulnerabilities.

Keywords: Automated Web Application Scanning, Vulnerability Scanning, Ethical Hacking, Wapiti, Selenium, SQLMap

1. Introduction

As society becomes increasingly dependent on the Internet and web technologies, web application security has become a critical aspect of protecting users' data and personal information. The presence of vulnerabilities in web applications can result in severe consequences, including data theft, loss of trust in service providers, and significant financial losses. Therefore, effective testing and detection of these vulnerabilities is of paramount importance both in the design stages and in the use of web applications.

The rapid evolution of web technologies has rendered manual security testing methods less effective, particularly in light of the growing needs of the digital age. Automating the web scanning process not only saves valuable time and resources, but it also enhances the accuracy and scope of testing [1 – 3].

This paper presents a study of the use of tools such as Wapiti, Selenium, and SQLMap for automated web application testing. The primary objective is to assess the efficacy of an automated scanning process for a specific web application and to establish a benchmark for evaluating the results. The scope of the study encompasses an analysis of the security aspects covered by these tools and a comprehensive assessment of their effectiveness and accuracy in vulnerability detection.

2. Automated Web Application Scanning Tools

The following paragraph describes the possibilities for automated scanning of web applications with three distinct software tools: Selenium, Wapiti, and SQLMap. It outlines the functionalities and main features of these tools.

2.1. Automated Web Application Scanning with Selenium

Selenium [4] is a widely utilized open-source software tool employed for the automation of web browsers. Selenium enables developers and quality assurance engineers to devise test scenarios for web applications by emulating user actions in the browser, encompassing navigation, interaction with elements such as buttons, forms, and links. Primarily, Selenium is used for automated web application testing; however, it can also be employed for other tasks, including data extraction from websites (web scraping) and the automation of routine browser actions..

Selenium is comprised of multiple components, each of which is responsible for a distinct function:

1. **Selenium WebDriver:** It is the main component that enables interaction with web browsers. WebDriver executes the test scripts by communicating directly with the browser through its application programming interfaces (APIs). WebDriver is compatible with a range of browsers, including Chrome, Firefox, Safari, and Edge, with a dedicated driver for each browser.
2. **Selenium IDE:** It is an integrated development environment (IDE) that allows users to record and reproduce tests directly in the browser. The IDE is suitable for rapid prototyping of tests and for users who are less experienced in writing code. However, it is not as flexible as WebDriver.

3. **Selenium Grid:** Grid allows running tests on multiple machines and different browsers in parallel. This allows for a significantly faster testing process, especially in environments with multiple browser and operating system configurations.
4. **Selenium RC (Remote Control):** This is an older version of Selenium that was previously utilized by WebDriver to automate web browsers through the use of JavaScript. Currently, WebDriver is more efficient and directly communicates with the browser, in contrast to RC.

Selenium automates web browsers by performing actions that a real user would execute, but under the control of a pre-written test script.

2.2. Automated Web Application Scanning with Wapiti

Wapiti [5] is an open-source web application security testing tool that is used to scan and detect vulnerabilities. In contrast to other tools such as SQLMap, which focus on specific vulnerabilities such as SQL injections, Wapiti scans a wide range of vulnerabilities in web applications. Rather than performing direct attacks, it checks for vulnerable points that can be exploited.

The main features of Wapiti are:

1. **Black-box Testing:**
 - Wapiti performs a comprehensive examination of the web application from the viewpoint of an external user. It does not require access to the application's source code, making it an optimal choice in instances where developers lack access to the application's internal code (such as when testing external services).
2. **Wide range of vulnerabilities:** Wapiti is capable of detecting a range of potential vulnerabilities, including:
 - **SQL injections.**
 - **Cross-Site Scripting (XSS)** – attacks in which malicious code is injected from web pages that users visit.
 - **File Inclusion** vulnerabilities, such as Local File Inclusion (LFI) and Remote File Inclusion (RFI), provide malicious actors with the ability to gain unauthorized access to and execute files on the system they are targeting.
 - **Command Injection** – vulnerabilities permitting the execution of commands on the server.
 - **Cross-Site Request Forgery (CSRF)** – attacks where malicious commands are executed through the user's browser.
 - **XXE (XML External Entity)** – vulnerabilities related to XML (Extensible Markup Language) processing.
 - **Open Redirect** – redirections to malicious sites.
 - Vulnerabilities related to file processing, such as uploading malicious files.
3. **Passive and active scanning:**
 - **Passive scanning:** In its initial phase, Wapiti performs a passive scan, whereby it does not send any dangerous requests to the server. Instead, its sole

objective is to analyze the responses it receives from the server.

- **Active scanning:** Following the completion of the passive scan, Wapiti initiates the transmission of test requests, the objective of which is to detect and assess specific vulnerabilities.
4. **Flexibility and configurability:**
 - Wapiti affords users the ability to specify which modules are to be executed during the scanning process. This enables the user to concentrate on specific types of vulnerabilities that are pertinent to the particular case in question.
 - Additionally, the tool permits the utilization of proxies for enhanced anonymity during testing and is capable of processing both HTTP and HTTPS requests.
 5. **Support for different HTTP methods:**
 - Wapiti is capable of working with a variety of HTTP methods, including GET, POST, PUT, and DELETE. This enables it to assess the functionality of web applications that employ disparate REST API methods or interactions.
 6. **Integration of cookie and session files:**
 - Wapiti is capable of working with both cookies and sessions, which enables it to scan the secure sections of a web application that require authentication. This is a crucial capability if the objective is to test the full functionality of an application, rather than merely the public-facing aspects.
 7. **Generation of comprehensive reports:**
 - Once the scan is complete, Wapiti generates comprehensive reports in a variety of formats, including HTML, JSON, XML, and text files. These reports facilitate the analysis and documentation of results, providing detailed information about each vulnerability identified and recommendations for potential fixes.

2.3. Automated Web Application Scanning with SQLMap

SQLMap [6] is an open-source Python-based security testing tool that automates the process of discovering and exploiting SQL injection vulnerabilities and gaining control of database servers. It has a powerful detection engine, a host of specific features for advanced security professionals, and a rich set of options ranging from database identification and data extraction to accessing the underlying file system and executing operating system commands through external connections. It automates SQL injection detection by generating different types of SQL queries and analyzing the responses.

The main features of SQLMap are:

1. Full support of multiple database management systems, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB, Aurora, OpenGauss, ClickHouse, and Virtuoso.
2. The software offers comprehensive support for six distinct SQL injection techniques, including logical condition-based, time-based, error-based, UNION queries, stacked queries, and external connections.
3. The capacity to establish a direct connection to the database is enabled through the provision of credentials, IP address, port number, and database name, obviating the necessity for SQL injection.

4. The tool offers comprehensive support for the listing of users, password hashes, privileges, roles, databases, tables, and columns.
5. Automatic recognition of password hash formats and the ability to crack them via a dictionary-based attack.
6. The software enables the user to extract complete tables and specific records and columns in accordance with their preferences.
7. The functionality to search for specific databases, table or column names in databases is a valuable tool for locating sensitive information.
8. Ability to download and upload files from the main server file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
9. The ability to execute arbitrary commands and retrieve their output from the underlying database server operating system is supported.
10. The ability to establish an external TCP connection between the attacker's machine and the database server operating system provides an interactive command environment, a Meterpreter session, or a graphical user session (VNC).
11. The user privilege escalation of the database process via Metasploit's Meterpreter getsystem command is also supported.

3. Verification of the Automated Web Application Scanning Process

A comparative analysis of the three automated web application scanning tools, Wapiti, Selenium, and SQLMap, was conducted on the following criteria: vulnerability detection, accuracy of results, ease of use, and scanning speed. The results of this analysis are presented in Table 1.

Table 1: Comparative analysis of automated scanning tools Wapiti, Selenium and SQLMap

	Wapiti	Selenium	SQLMap
Vulnerability detection	Wide range of vulnerabilities including SQLi, XSS, and CSRF	Limited coverage, depends on combination with other instruments	Specialized in SQL injections
Accuracy of results	Good accuracy, but can have false positives and negatives	Depends on configuration and integration	High accuracy for SQL injections
Scanning speed	Fast, but depends on the size and complexity of the application	Can be slow, depends on complexity of test scenarios	Fast for SQL injections, but depends on query complexity
Ease of use	Easy to set up and use, but may require additional configurations	Requires programming and integration with other tools	Easy to use for SQL injections but requires SQL knowledge

In consequence of the benchmarking process, the Wapiti tool was selected for the purpose of performing an automated scan of the www.nvu.bg website. The reasons for this choice are as follows:

1. Wapiti is capable of addressing a multitude of vulnerabilities, including SQLi, Cross-Site Scripting (XSS), Local File Inclusion (LFI) and Remote File Inclusion (RFI), Command injection, Cross-Site Request Forgery (CSRF), XML eXternal Entity (XXE), and Open Redirect.
2. The tool demonstrates high accuracy, although in suboptimal configurations, it may produce false positive and negative results.
3. It is easy to set up and use but may require additional configurations.
4. It is fast, and its speed depends on the size and complexity of the application.

Wapiti starts by scanning passively, then actively sending test requests to find specific vulnerabilities. Users can choose which modules to run during the scan and use proxies for anonymous testing. Wapiti can handle HTTP/HTTPS requests and work with cookies and sessions, allowing it to scan secure parts of a web application that require authentication.

The Wapiti tool generates comprehensive reports following the conclusion of the scan, providing detailed information about each identified vulnerability and recommendations for potential fixes. The test, conducted in accordance with the methodology outlined in [7], required over 25 hours and yielded the report depicted in Fig. 1. The scan identified five vulnerabilities, distributed across two categories. A concise overview of these vulnerabilities is presented in Table 2.

Wapiti vulnerability report
Target: <https://www.nvu.bg/bg>
Date of the scan: Sat, 08 Sep 2024 19:30:45 +0000. Scope of the scan: folder

Summary	
Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	4
Cross Site Request Forgery	0
HTTP Secure Headers	1
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0

Fig. 1: Part of the detailed report generated by Wapiti for www.nvu.bg.

3.1. Discussion

The setting of attribute values in detected vulnerabilities (see Table 2) enables web developers to regulate the loading and execution of resources on web pages. This serves as a protective measure against common attacks, such as Cross-Site Scripting, Data Injection, and other forms of attacks that aim to insert malicious code into web pages. In the event that a web page attempts to load a resource that is not permitted by the policy defined by these attributes, the browser blocks that resource and prevents its execution.

In this context, there is a trade-off between the security of the designed web application and its ability to generate profit from advertisements, which is contingent upon the volume of traffic it receives.

In the contemporary era, external resources and applications related to the collection and processing of data for the analysis of user behavior, such as Google Analytics, are being utilized with increasing frequency. These external resources are managed by third parties and may load other related resources from a variety of domains over which the web application has no control.

Furthermore, there are antivirus software programs, such as "Kaspersky," that inject their own scripts into every single page that a user opens through their browser so that they can scan and protect more effectively.

In this scenario, if the CSP content security policy is enabled and correctly configured, there is a significant probability that specific features or even the entire web application will cease functioning adequately. Conversely, if the CSP is incorrectly configured, it is imperative to rely on established internet protocols and user awareness (carefully monitoring the links they click on), antivirus software, and other protective measures to protect users.

Table 2: Description of the vulnerabilities discovered by the Wapiti scanning tool

Nº	Vulnerabilities	Description of the vulnerabilities
Category „Content Security Policy Configuration (CSP)“		
1	CSP attribute “ default-src ” is missing	The default-src attribute specifies from which sources resources can be loaded if there is no other, more specific attribute for a given content type (for example, script-src can be used for scripts, img-src for images, etc.). If there is no specific attribute for a resource type, the browser will use the rule set by default-src .
2	CSP “ script-src ” value is not safe	The script-src rule enables the web developer to specify which JavaScript sources are permitted. All other scripts loaded from sources not included in the rule will be blocked.
3	CSP attribute “ object-src ” is missing	The object-src attribute specifies where content can be loaded for the <object> , <embed> , and <applet> elements.
4	CSP attribute “ base-uri ” is missing	The base-uri attribute allows developers to restrict from which sources a <base> element can be set. This prevents the injection of malicious <base> elements that can alter the loading behavior of resources on the page, such as CSS, JavaScript, images, and more.
Category “HTTP Secure Headers”		
5	X-XSS-Protection is not set	The HTTP response header “ X-XSS-Protection ” is a feature of legacy browsers that allows websites to control their XSS auditors. The server is not configured to return the “ X-XSS-Protection ” header, which indicates that all pages on this website may be at risk of an XSS attack. If support is not required by older browsers, it is recommended to use “ Content-Security-Policy ” instead, without allowing dangerous scripts in the line.

3. Conclusion

A comparative analysis of the main features of the automated web scanning tools Wapiti, Selenium, and SQLMap, as well as their verification process with a specific web application, reveals the following conclusions:

1. Selenium is a robust web test automation tool that offers comprehensive support for an extensive range of browsers and programming languages. It plays a vital role in the continuous integration and development process, assisting development and

testing teams in ensuring the quality of their web applications. Despite its inherent limitations, its extensive flexibility and capabilities make it one of the most widely used tools for automated web application testing.

2. As a consequence of its operations, Wapiti produces a comprehensive report containing the identified vulnerabilities and offers detailed suggestions for their remediation. This tool provides an effective solution to enhance the security of web applications and mitigate the risk of exploitation of vulnerabilities. The integration of this tool into the development and testing process can significantly reduce the time required to detect vulnerabilities and facilitate the remediation process.

3. To protect against SQL injections, it is necessary to implement a multi-layered approach that includes parameterized queries, input validation, minimum database privileges, and regular vulnerability scanning with SQLMap. In addition, the use of Web Application Firewall or other security systems is recommended. The implementation of these measures significantly reduces the risk of successful SQL injections.

4. The Wapiti tool is an optimal choice for the initial automation of web application scanning processes due to its high accuracy in detecting a wide range of vulnerabilities and the comprehensive reports and remediation recommendations it generates. In the event of certain suspected vulnerabilities, it is advised to conduct further testing with the robust Selenium tool by creating specific scenarios. Alternatively, for SQL injections, it is recommended to utilize SQLMap, which provides a multi-layered approach to parameterized queries for the database.

3. References

1. V. K. Velu, *Mastering Kali Linux for Advanced Penetration Testing*, Fourth Edition, Packt Publishing Ltd. (2017).
2. A. L. Doupe, *Advanced Automated Web Application Vulnerability Analysis*, University of California, (2014), Accessed 19.03.24 at https://www.academia.edu/23627654/Advanced_Automated_Web_Application_Vulnerability_Analysis.
3. M. Shema, *Web Application Security for Dummies*, John Wiley & Sons, Ltd (2011).
4. Selenium. Suite of tools for automating web browsers. Accessed 10.11.24 at <https://www.selenium.dev/>.
5. N. Surribas, Wapiti. The web-application vulnerability scanner, Accessed 10.11.24 at <https://wapiti-scanner.github.io/>.
6. A. G. Bernardo Damele, M. Stampar, SQLMap. Automatic SQL injection and database takeover tool, Accessed 19.03.24 at <https://sqlmap.org/>.
7. E. Saad, R. Michell, *Web Security Testing Guide v4.2*, Accessed 19.03.24 at <https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf>.

Acknowledgement:

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

Comparison between Monolithic and Microservices Architecture in Web Applications Built with Java

Ina Papadhopulli, Armada Alija

Faculty of Information Technology, Polytechnic University of Tirana, Albania

E-mail: ipapadhopulli@fti.edu.al, armada.alijsa@fti.edu.al

Abstract: In today's times, people demand fast, stable, and reliable applications. Therefore, it is essential to choose the right software architecture before implementing functionalities adopted in the project. The monolithic architecture is implemented as a single unit, integrating all functionalities within a single codebase. In contrast, the microservice architecture decomposes the application into several independent services, each responsible for a specific business logic. Key factors such as scalability, fault tolerance, and data consistency are analyzed. Performance metrics, simplicity, flexibility, and the challenges of implementing and maintaining each architecture are gathered and compared. This study offers valuable insights into the practical implications of choosing between monolithic and microservice architectures, especially in the context of applications. It serves as a comprehensive guide for software developers to make informed decisions when designing scalable and reliable systems.

Keywords: ARCHITECTURE, MONOLITH, MICROSERVICE, APPLICATION, JAVA

1. Introduction

Monolithic architecture has traditionally been used and continues to be utilized. Based on this, applications are built on a single database, and functionalities are closely interconnected, following a linear structure. However, while this model is simple, it can become very difficult and complex to manage as the application grows. Some issues that can be mentioned include the dependency between project modules, longer integration time for new developers, and longer deployment times.

Therefore, to address this issue, Microservice architecture promises to simplify project management and maintenance as things become more complex.[1] Many companies are interested in migrating their applications to microservices. However, this is not an easy path. This challenge will be explored through a case study approach, by implementing an application based on Java, utilizing both types of architectures. The problem can be formulated as:

What are the key challenges and benefits of transitioning from monolithic architecture to microservices architecture in developing and managing scalable applications?

2. Objectives and Research Methodologies

The main goal is to present the elements that demonstrate the connection between Monolithic and Microservices architectures, analyze or highlight their specific characteristics, and compare the performance and scalability of monolithic and microservice architectures in a web application. Additionally, the necessary mechanisms for transitioning from Monolithic to Microservices in the most practical way have been evaluated.

The defined objectives are listed as follows:

- Introduction of two architectures: monolithic and microservices and a practical case study comparing their characteristics.
- Quantitative evaluations of performance metrics such as responsivity, scalability, and fault tolerance.
- Insights into best practices
- Highlighting the challenges that arise during the use of each of them.

3. Case Study Implementation

Application: Sales Management Platform is a simple Java-based web application that is implemented twice and uses both architectures. It includes functionalities for user authentication, warehouse management, client data, and order processing.[19]

Technologies: Java, Spring Boot, Spring JPA, Hibernate

Java is a platform-independent, object-oriented programming language designed for high performance and versatility, enabling the development of secure, scalable, and portable applications.[3]

Spring Boot is a Java-based framework that simplifies application development by providing pre-configured setups.

Spring JPA is a module of the Spring Framework that provides a repository abstraction by enabling efficient and declarative interaction with relational databases.

Hibernate is a Java-based ORM framework that implements JPA, facilitating the mapping of Java objects to relational database tables while automating SQL generation and transaction management.

Database: PostgreSQL.

PostgreSQL is an advanced, open-source relational database management system that supports both SQL (relational) and JSON (non-relational) querying.

IDE: IntelliJ IDEA

IntelliJ IDEA is an integrated development environment (IDE) developed by JetBrains and used for developing computer software written in Java, Kotlin, Groovy, Scala, and more.

Testing: Postman, Gatling, Resilience4j

Postman is a tool for manual and functional API testing. It includes debugging, simple automation, and validation.

Gatling is a tool for performance and load testing. It is designed for high-concurrency simulations of API or web service performance.

Resilience4j is a library that evaluates fault tolerance and durability. It is used to implement fault-tolerance patterns like Circuit Breaker, Retry, Timeout, Bulkhead, and Rate Limiter, in applications. Also, it can be used to simulate fault scenarios for testing purposes when combined with tools like JUnit.

Device: The application is developed and tested on an HP Laptop with an Intel Core i7, 16GB RAM, x64-based processor, 2.7 GHz, and Windows 10 operating system.

3.1 Monolithic Architecture

Setup: Single codebase and database for all functionalities.[19]

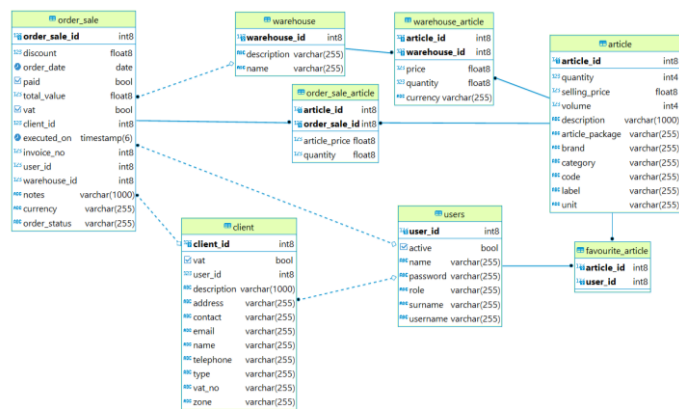


Fig. 1 Entity Relationship Diagram (ERD) for the Sales Management Platform implemented in a Monolithic Architecture

The monolithic system is implemented as a single WAR file, deployed on a Tomcat server. The PostgreSQL database contains tables for users, clients, orders, and warehouse inventory.

Performance: Using Gatling, the monolithic system handled up to 10,000 – 100,000 concurrent requests with acceptable latency. However, increasing requests beyond this threshold resulted in significant degradation, as all processes relied on a single deployment instance.[17]

Limitations and Fault Tolerance[18]:

Single Point of Failure: A monolithic application is typically a single, tightly integrated unit. A failure in any part of the application, e.g., a database connection failure or a critical module, can bring down the entire system.

Performance Bottlenecks: As all components share the same runtime environment and resources e.g. CPU, and memory, it can lead to performance issues. A bottleneck in one part of the application, such as excessive database queries, can slow down the entire system.

Deployment bottleneck: Re-deploying required restarting the entire system, causing downtime. Since monolithic applications are deployed as a single unit, failures due to incompatible changes in a module or server issues can bring down the entire system. This also limits the ability to perform isolated updates or rollbacks.

Resilience4j patterns that are used to handle these failures[12]:

Circuit Breakers and Timeouts: These are essential for ensuring that failure in one part of the application does not bring down the entire system. For example, a service call within the monolith might fail due to database issues or external dependencies, and a circuit breaker prevents this failure from affecting the rest of the application.

Bulkheads: These are used to isolate critical internal actions, e.g. order execution, from other less critical actions, ensuring that failure in one section doesn't disrupt the entire application

Retries: Retries help resolve temporary issues, such as brief network failures, by retrying operations before failing altogether.

3.2 Microservices Architecture

Setup: Individual services for authentication, warehouse, client, orders and favorite articles. Each service has its own database.[19]

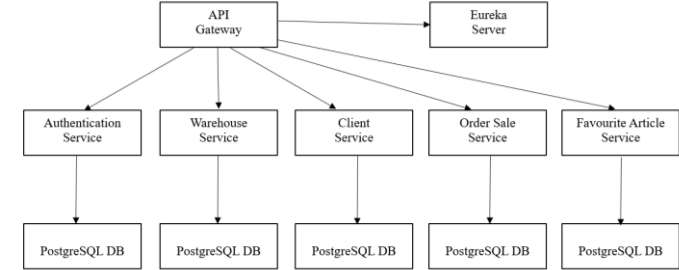


Fig. 2 Microservices Architecture for the Sales Management Platform

Eureka Server is a popular tool for implementing service discovery and registration in microservices architectures. Eureka acts as a centralized registry where all service instances register themselves. Other services can use Eureka to dynamically find the location of instances they want to communicate with. OpenFeign helps to simplify this communication by acting as a declarative HTTP client.[16]

API Gateway acts as a single entry point for all client requests, routing them to the appropriate microservices. It serves as a service aggregator and load balancer, enabling dynamic routing to various backend services that are registered with a service discovery tool such as Eureka. The API Gateway interacts with service registries to dynamically discover the locations of microservices, facilitating fault tolerance and scalability by rerouting requests to available instances in case of failure.

The Users table will be included in the Authentication Service and is related to system authentication. The Article, Warehouse, and WarehouseArticle tables will be included in the Warehouse Service. The Client table will be included in the Client Service. The OrderSale and OrderSaleArticle tables will be included in the Order Service. The FavouriteArticle table will be included in the Favourite Article Service.

Implementation: Each functionality was split into independent services, each with its own database. For instance, the Warehouse Service managed inventory-related operations using its specific PostgreSQL instance. [11]

Performance: Gatling tests revealed that microservices scaled effectively, handling over 100,000 concurrent users by distributing workloads across services.

Limitations and Fault Tolerance[20]:

Load Balancing Failure: Load balancing in microservices ensures that incoming traffic is distributed across multiple instances of services to avoid overloading a single instance, maintaining high availability and responsiveness. Resilience4j's Rate Limiter and Circuit Breaker help mitigate traffic overloading and prevent cascading failures in a load-balanced system.

Database Failure: Database failures can impact any service that depends on data persistence. These failures can be caused by issues with the database itself or the interactions between microservices and the database. Circuit Breakers and Retry Patterns help ensure service reliability by enforcing limited retry logic and ensuring that requests don't overload the database.

Service Unavailability: Service unavailability occurs when one or more microservices in the architecture fail, preventing requests from being processed. This failure can be due to network issues, crashes, or resource exhaustion. Circuit Breaker and Fallback mechanisms contribute to improving system availability and reducing the impact of service unavailability.

Throttling: Throttling is a method used in microservices architectures to control the flow of requests to a service to prevent overload and ensure fair usage. Rate Limiter and Bulkhead patterns enable fine-grained control over how requests are processed, preventing service overloads while ensuring fairness and optimal resource usage.

Authentication/Authorization Failure: Authentication and authorization failures occur when a service cannot verify the identity of a user or system, or when a user/system is not authorized to perform a certain action. By analyzing the security breach or token expiration processes, Retry and Circuit Breaker patterns can be used to minimize the risk of authentication failure affecting the system as a whole[14].

Performance	Performance can degrade as the system grows due to resource bottlenecks	Performance is optimized since each service can run independently, allowing specific tuning for performance gains
Durability	Single database and component structure may reduce long-term durability if updates are not frequent	Higher durability since individual services can be updated and maintained without disrupting the whole system
Fault-Tolerance	Lower fault tolerance; a critical failure in one module can affect the entire system	High fault tolerance, as a failure in one service, does not cascade to others, keeping most of the application functional
Scalability	Inability to scale when needed	Scalable (scale on demand)
Maintenance	A large code base is difficult to understand	A small code base is easier to be managed
Security	Secure, as a single system, data management is straightforward	Security is complex due to inter-service communication, requiring additional safeguards like API gateways

Table. 1 Comparison between Monolithic and Microservices Architecture[4],[5],[6],[7],[8],[13].

4. Comparative Analysis of Monolithic and Microservices Architecture

	Monolithic Architecture	Microservice Architecture
Component	Module	Microservice
Component size	Large	Limited
Elasticity	Single point of failure. Hard to handle new changes	Each service can be scaled independently
Deployment	The whole application is deployed as a single module	Each service is created and deployed independently
Storage mechanism	Shared database	Private database
Technology	The programming language and framework used must be the same from the start to the end of the application	Heterogeneous languages and frameworks
Resiliency	A single bug can compromise the entire system	Issues in one service do not affect the functionality of others
Agility	Adopting new technologies is difficult due to the tight-knit structure	Easily integrates new technologies to meet business needs

5. Challenges of transition to Microservices

Despite its simplicity, monolithic-based applications can become very challenging and complex to manage as the application scales.[2] Some issues include:

- Dependencies between project modules
- Longer integration time for new developers
- Extended deployment times

To address these challenges[10], microservice architecture promises to simplify project management and maintenance as complexity increases. Many companies are interested in migrating their applications to microservices, but this is not an easy path.[15]

The microservices concept is to separate each business logic into distinct services. Each microservice is considered an independent API application with its lifecycle, allowing for independent development, deployment, and scalability according to customer needs, and management.[12]

Challenges observed during the migration to microservices include:

- Separating the database of the application built with monolithic architecture
- Managing transactions within microservices

- Ensuring the normal operation of the monolithic application until the microservices architecture is complete
- Adapting developers to the new architecture

6. Conclusions

Monolithic architecture, being a traditional and straightforward model, offers simplicity in deployment and development. It is an excellent choice for small-scale applications where modularity and scalability are not the primary concerns, as selecting a microservices architecture would not make a significant difference. So, for small applications, monolithic architecture allows for easier debugging, reduced latency in internal system communication, and simplified management due to a unified codebase.

However, as applications grow, the inherent limitations of monolithic structures become evident, particularly in terms of scalability and maintenance. The tight coupling of components makes the system more rigid, slowing down development processes and increasing the likelihood that updates or changes will introduce unwanted side effects throughout the system. Furthermore, deploying new versions requires the entire application to be restarted, which is inefficient for large and complex systems.

While monolithic architecture may be more suitable for smaller, less complex applications, microservices offer significant advantages in terms of scalability and fault isolation for larger and more dynamic systems.

7. References

- Newman, Building Microservices., O'Reilly Media, Inc., (2021)
- Momil Seedat, Qaisar Abbas Qureshi, Alessia Amelio, Transition Strategies from Monolithic to Microservices Architectures: A Domain-Driven Approach and Case Study. (June 2024)
https://www.researchgate.net/publication/381290696_Transition_Strategies_from_Monolithic_to_Microservices_Architectures_A_Domain-Driven_Approach_and_Case_Study
- Desiree D. Martinez, Axl Heart P. Remegio, Darllaine R. Lincopinis, A Review on Java Programming Language, (May 2023)
https://www.researchgate.net/publication/371166744_A_Review_on_Java_Programming_Language
- J. Fritzsche, J. Bogner, A. Zimmermann, and S. Wagner, "From monolith to microservices: A classification of refactoring approaches," in Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment: First International Workshop, DEVOPS 2018, Chateau de Villebrumier, France, (March 5-6, 2018)
- Nada Salaheddin, Nuredin Ali Salem Ahmed, Microservices vs. Monolithic Architectures: The differential structure between two architectures, (9 Sept 2022)
<https://www.minarjournal.com/dergi/microservices-vs-monolithic-architectures-the-differential-structure-between-two-architectures20221202031410.pdfscal>
- E. Axelsson and E. Karlkvist, "Extracting microservices from a monolithic application," (2019)
- Grzegorz Blinowski, Anna Ojdowska, Adam Przybylek, Monolithic vs. Microservice Architecture: A Performance and Scalability Evaluation, IEEE, (18 February 2022)
- C. Richardson, "Microservices-Pattern: Microservice Architecture," (March 2014)
<http://microservices.io/patterns/microservices.html>
- Guozhi Liu, Bi Huang, Zhihong Liang, Minmin Qin, Hua Zhou, Zhang Li, Microservices: architecture, container, and challenges, (2020) IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)
https://qrs20.techconf.org/QRSC2020_FULL/pdfs/QRS-C2020-4QOuHkY3M10ZU1MoEzYvg/891500a629/891500a629.pdf
- Pooyan Jamshidi, Claus Pahl, Nabor C. Mendonça, James Lewis, Microservices: The Journey So Far and Challenges Ahead, IEEE Software, Published by the IEEE Computer Society, (2018)
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8354433>
- A. Furda, C. Fidge, O. Zimmermann, W. Kelly and A. Barros, "Migrating Enterprise Legacy Source Code to Microservices: On Multitenancy, Statefulness, and Data Consistency," in IEEE Software, vol. 35, no. 3, pp. 63-72, (May/June 2018)
- Mohit Kumar; Christian Engelmann, Models for Resilience Design Patterns, (2020)
<https://ieeexplore.ieee.org/document/9306940>
- Taibi, K. Systä, From monolithic systems to microservices: A decomposition framework based on process mining, (2019), pp. 153–164
- Architecting with microservices: A systematic mapping study J. Syst. Softw., 150 (2019), pp. 77-97
- Victor Velepucha; Pamela Flores, Monoliths to microservices - Migration Problems and Challenges: A SMS, (23-25 March 2021)
- Yalemisew Abgaz; Andrew McCarren; Peter Elger; David Solan; Neil Lapuz; Marin Bivol; Glenn Jackson, Murat Yilmaz, Decomposition of Monolith Applications Into Microservices Architectures: A Systematic Review, pp. 4213 – 4242, (June 2023)
<https://ieeexplore.ieee.org/document/10160171>
- Konrad Gos, Wojciech Zabierowski, The Comparison of Microservice and Monolithic Architecture, April 2020
https://www.researchgate.net/publication/341956559_The_Comparison_of_Microservice_and_Monolithic_Architecture
- E Punithavathy, N Priya, Performance of Dynamic Retry Over Static Towards Resilience Nature of Microservice, (June 2024)
https://www.researchgate.net/publication/381136184_Performance_of_Dynamic_Retry_Over_Static_Towards_Resilience_Nature_of_Microservice
- Kapil Bakshi, Microservices-based software architecture and approaches, IEEE, (2017)
<https://ieeexplore.ieee.org/document/7943959>
- Muhammad Waseem; Peng Liang; Gastón Márquez; Amleto Di Salle, Testing Microservices Architecture-Based Applications: A Systematic Mapping Study, IEEE, (2020)
<https://ieeexplore.ieee.org/document/9359275>

Storage Virtualization: Optimizing Data Center Efficiency and Performance

Genka Slavova-Torres^{1,*}

Institute of Information and Communication Technologies
Bulgarian Academy of Sciences Sofia, Bulgariagaria
genka.torres@iict.bas.bg

Abstract: In this article they are presented some of the main functionalities of IBM's SVC: Hyper Swap, Global Mirror and Metro Mirror, IBM Flash Grid technology, Automatic Storage Tiering (Auto-Tiering), Compressed Volumes.

Keywords: PERFORMANCE, OPTIMIZING, DATA CENTER

1. Introduction

It is fundamental for every modern data center to virtualize its own storage. By doing this, pooling the physical storage from multiple devices and organizing them in a ways that the hosts will see just one single device, it is optimizing the utilization, the performance and the management. This technology relies on software which is identifying the available storage from all the available devices (no matter the vendor and the operating system) and creates pools which after that are converted to Virtual disks and this is what the virtualization is presenting to the hosts. The Host will see there virtual disks, created by heterogeneous storages as a single storage, no matter where all this physical storages are located.

Such solution is IBM SAN Volume Controller, or SVC and IBM Spectrum Virtualize. How Virtualization Works Storage virtualization primarily operates in a network-based environment such as a Storage Area Network (SAN), where storage devices are interconnected via Fiber Channel (FC) or iSCSI. Here's how it functions: Pooling Resources: Storage virtualization software identifies and aggregates storage capacity from diverse vendors and platforms, creating unified storage pools. Creation of Virtual Disks: These pooled resources are then organized into virtual disks, which are presented to host systems as single, cohesive storage units.

SVC supports storage arrays from multiple vendors, enabling a unified storage pool that abstracts the underlying hardware. This allows organizations to maximize their existing investments while simplifying storage management. By pooling storage resources, SVC can easily scale to meet growing data needs without the need for disruptive hardware upgrades[1,2,3].

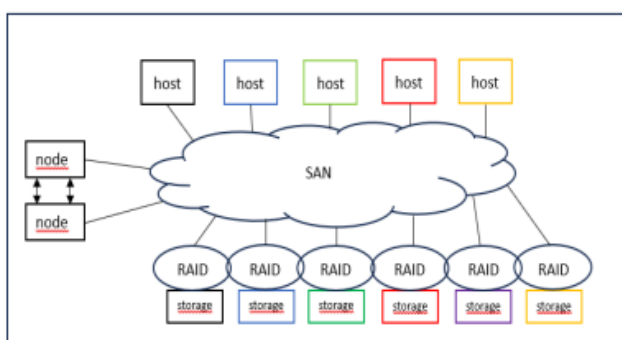


Fig. 1 SAN Environment, Virtualized Storages *Грешка! Источникът на препратката не е намерен.*

2. Advance data serving

These are some of the main functionalities of IBM's SVC: 1. Thin Provisioning - A thin-provisioned volume displays a different capacity to hosts than it uses in the storage pool. These volumes are supported in both standard and data reduction pools, offering benefits like capacity savings and efficiency improvements. Standard pools do not support capacity reclamation, whereas data reduction pools reclaim space automatically when no longer needed

by hosts. Thin-provisioning allows for flexible capacity management, presenting large virtual capacities to applications while adjusting real capacity as needed. Extra metadata is required for thin-provisioned volumes, which can impact I/O performance compared to fully allocated volumes. 2. Deduplicated Volumes - Deduplication can be enabled for thin-provisioned and compressed volumes in data reduction pools to enhance capacity savings by eliminating duplicate data copies. It works by identifying unique data chunks, known as signatures, and only writing new data if its signature does not already exist in the system. When new data matches an existing signature, a reference is created instead of storing the duplicate data, saving storage space and potentially improving read performance. The deduplication process relies on a hash-based solution, where a repository containing data signatures helps determine if incoming data is unique. This repository is distributed across all nodes in the I/O groups with deduplicated volumes, ensuring efficient use of memory and seamless updates when nodes are added or removed. 3. Compressed Volumes - When creating volumes, you can enable compression to save storage capacity. Compressed volumes store data in a compressed format as it is written, which conserves space, and decompress the data when read by hosts. Compression is part of the data reduction features available in the system, and compressed volumes must be part of data reduction pools to utilize this feature. Data reduction pools also automatically reclaim unused capacity when hosts release it using SCSI unmap commands, redistributing the reclaimed space. For compressed volumes in data reduction pools, the capacity values include real capacity (allocated from the pool), virtual capacity (available to hosts), and used capacity (actual space used after compression). Automatic Storage Tiering (Auto-Tiering) - Auto-tiering is a feature that optimizes storage costs and performance by allowing logical volumes or LUNs to span across different storage tiers and automatically move portions of the volume between these tiers. This movement is controlled by autotiering algorithms or policies, enabling cost-effective storage solutions without requiring applications to be redesigned for storage awareness or needing manual data classification. Typically, auto-tiering implementations support various storage tiers, including solid-state disks (SSDs), Fibre Channel (FC), Serial-Attached SCSI (SAS), and Serial ATA (SATA) or nearline disks[4,5]

3. High availability and disaster recovery

HyperSwap - When setting up a HyperSwap topology, the system is divided between two sites for data recovery, migration, or high availability. Each node, enclosure, storage system, and host must be assigned to one site, ensuring that both node canisters of an I/O group are at the same site as the external storage systems providing the managed disks. This setup ensures that each HyperSwap volume copy is independent and located at a different site. HyperSwap volumes automatically replicate data to both sites, providing continuous access if one site fails. Ownership groups must manage access to ensure both copies and users are correctly assigned. A 2-site HyperSwap can extend to a third site for disaster recovery using IBM Spectrum Virtualize 3-Site Orchestrator, which coordinates data replication across three locations. HyperSwap volumes automatically create relationships between copies at each site, switching access based on availability and keeping data up to date. Consistency groups ensure coordinated failover of all related copies. The SCSI protocol's ALUA state helps the system

recommend local nodes for I/O requests, optimizing performance by prioritizing paths to nodes at the same site as the host. Global Mirror and Metro Mirror - When setting up a HyperSwap topology, the system is divided between two sites for data recovery, Metro Mirror and Global Mirror are remotecopy operations that create relationships between two volumes, where updates to one volume are mirrored on the other. These operations support both intersystem (different systems) and intrasystem (same system) configurations, maintaining two data copies for backup or disaster recovery. The system designates one volume as primary, receiving all write operations, while the secondary volume mirrors these updates. Metro Mirror provides synchronous copying, ensuring identical data on both volumes before confirming writes, and supports distances up to 300 km [6,7]. Global Mirror offers asynchronous copying, allowing primary volume writes to complete before mirroring, with secondary volumes typically less than a second behind. Metro Mirror ensures immediate data consistency, while Global Mirror allows for slight delays to reduce performance impacts, both crucial for disaster recovery strategies. IBM Flash Grid technology - The latest hot invention from IBM, the Flash Grid, revolutionizes storage system expansion by integrating multiple independent systems into a federated cluster. Flash Grid significantly enhances scalability compared to traditional scale-out systems using I/O groups, supporting up to eight systems per grid with linear growth in performance, capacity, volumes, hosts, and snapshots. Systems within a Flash Grid can be independently updated, and diverse hardware models and generations can be incorporated, allowing for seamless hardware replacement or tiering. Non-disruptive Storage Partition Migration enables smooth migration of storage partitions between systems within the grid. Flash Grid requirements include: Support for a single I/O group, with multiple I/O groups compatibility mode disabled. A 'standard' system topology. A 'replication' system layer. Systems in a Flash Grid securely communicate through certificate exchange, with the default use of system-signed certificates or optionally CA-signed certificates that meet specific criteria. These are some of the main functionalities; however, it is beyond the scope of this article to enumerate all of them or delve into their specific operational mechanisms. Instead, I will focus on discussing another significant IBM innovation: the evolution of FCM drives, known as IBM FlashCore Modules (FCMs)[8,9,10]. IBM has a rich history in developing advanced flash memory solutions, particularly through its FlashCore Modules (FCM). These modules are designed to optimize both performance and reliability by separating control and data paths within the module. This innovation ensures that data access and transfer are efficient without any performance degradation from control operations. Additionally, IBM has integrated endurance features and RAID directly into the FCM modules, further enhancing their durability and reliability. The evolution of IBM's FCM technology began with the introduction of the FlashCore MicroLatency Module, initially using SLC flash media and later transitioning to MLC flash to improve performance. Subsequent advancements led to the adoption of NVMe interfaces, standardizing the form factor and interface while maintaining performance efficiency. The latest FCM2 and FCM3 generations embraced QLC flash, a move that defied industry norms by demonstrating superior performance compared to TLC-based predecessors[11,12,13].

In 2024, IBM launched FCM4, which introduced innovative features like Ransomware Threat Detection. This groundbreaking capability identifies potential security threats in real-time, enabling swift responses to safeguard data integrity. Moreover, FCM4 incorporates advanced data reduction technologies, supporting up to 3-to-1 data compression to maximize storage efficiency without compromising performance.

Key to IBM's FCM technology is its proprietary Variable Voltage technology, which optimizes flash cell longevity by dynamically adjusting voltage levels over the lifecycle of the drive. This proactive approach minimizes the occurrence of uncorrectable errors, ensuring sustained performance and reliability. FCM drives

also integrate unique capabilities such as inline compression and encryption, executed at the hardware level without imposing overhead on system performance. This feature set, combined with IBM's Variable Stripe RAID (VSR) technology, enhances data protection and operational efficiency by managing data redundancy within each module. IBM's FCM series stands out in the market for its superior endurance, cost-effectiveness, and performance optimization. Leveraging innovations like Smart Data Placement, which optimizes data storage between SLC and QLC flash types based on usage patterns, IBM ensures consistent low-latency performance tailored to diverse workload demands. In summary, IBM's FCM modules represent a culmination of decades of flash memory expertise, offering unparalleled reliability, performance efficiency, and advanced security features like Ransomware Threat Detection. These capabilities make FCM drives an ideal choice for enterprises seeking robust storage solutions that deliver long-term value and operational resilience in dynamic IT environments. Storage virtualization with solutions like IBM SVC and Spectrum Virtualize transforms storage infrastructure into agile, efficient, and resilient environments capable of meeting the dynamic demands of modern enterprise applications. By abstracting physical storage complexities and consolidating heterogeneous storage resources into unified pools, these solutions enable organizations to achieve higher utilization rates, improved performance, and simplified management. This approach not only optimizes storage efficiency but also enhances scalability and flexibility, supporting business growth and ensuring continuity in today's rapidly evolving digital landscape. Furthermore, IBM's FlashCore Modules [14,15]

(FCMs) integrated within these virtualization solutions enhance storage capabilities by providing advanced features such as inline compression, encryption, and Ransomware Threat Detection. These innovations bolster data security, optimize storage efficiency, and ensure sustained performance, making FCMs essential components for robust and reliable storage infrastructure in modern IT environments.

3. References

1. Süß, R., Süß, Y. (2024). Storage and Virtualization. In: IT Infrastructure . Apress, Berkeley, CA. https://doi.org/10.1007/979-8-8688-0077-1_4
2. A. Singh, M. Korupolu and D. Mohapatra, "Server-storage virtualization: Integration and load balancing in data centers," SC '08: Proceedings of the 2008 ACM/IEEE Conference on Supercomputing, Austin, TX, USA, 2008, pp. 1-12, doi: 10.1109/SC.2008.5222625.
3. <https://stormagic.com/resources/beginners-guides/virtualized-storagebeginners-guide/>
4. <https://www.ibm.com/docs/en/flashsystemv9000/8.2.x?topic=volumes-thin-provisioned>
5. <https://www.ibm.com/docs/en/flashsystem-5x00/8.4.x?topic=csfhyperswap-function-8>
6. <https://www.ibm.com/docs/en/spectrumvirtualsoftw/8.2.x?topic=functions-metro-mirror-global-mirror>
7. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.
8. <https://www.dbta.com/Editorial/News-Flashes/IBM-StorageAssurance-Offers-IBM-Flash-Grid-Technology-to-Simplify-StorageManagement-163889.aspx>
9. <https://newsroom.ibm.com/2024-04-25-IBM-Transforms-the-Storage-Ownership-Experience-with-IBM-Storage-Assurance>
10. https://ibmdocs-test.dcs.ibm.com/docs/en/flashsystem-870-lts-reviews_test?topic=started-flash-grid
11. <https://www.redbooks.ibm.com/redpapers/pdfs/redp5725.pdf>
12. <https://www.techtarget.com/searchstorage/definition/storagevirtualization>
13. https://en.wikipedia.org/wiki/Storage_virtualizationibm
14. <https://blocksandfiles.com/2024/02/27/ibm-adds-realtime-malware-iodetection-to-its-flash-drives>

Experimental determination of fire resistance of steel elements (X-brace) protected with intumescent paint

Neli Simeonova

Academy of the Ministry of Interior - Sofia, Bulgaria

e-mail: neli@sim@abv.bg

Abstract: The report presents and analyses data from tests of steel elements with different cross sections (massivity factor) protected with three different coating thicknesses. The obtained results are presented in graphics. Comparisons between the different protections in terms of fire resistance are made. The tests are part of a large-scale study of the behaviour of the same steel sections with applied reactive protection - intumescent paint (this report) and passive protection - plasterboard and rock wool.

KEYWORDS: FIRE RESISTING, STEEL ELEMENTS, FIRE TESTING, X-BRACE IN CONSTRUCTIONS, INTUMESCENT PAINT

1. Introduction

Fire protection of steel structures, especially in single-storey buildings, is a serious problem in building practice. This is due to several main factors [1]:

- the use of steel profiles with high mass factors;
- the application of high loads in individual structural elements;
- critical location of the structure under the influence of fire - the steel structure is located in the zone of above average temperature, etc.

These factors lead to a reduction in the fire resistance (FR) of the building [2].

The implementation of the horizontal and vertical braces, which ensure the spatial stability of the building during lateral loads, are mainly made of steel elements with a high mass factor. Often, these mass factors are outside the scope of the test standards and therefore a suitable tested and certified fire protection product (system) cannot be found.

2. Prerequisites and ways to solve the problem

The purpose of this report is to present the results of tests carried out on steel members with a mass factor (FM) outside the scope of EN 13381-8 [3], protected with intumescent paint [4] and to compare the data with calculations made according to the Eurocode. Building elements of this type are subjected to a four-sided fire impact during a fire and for this reason, the tests were carried out on short columns as the standard fire impact for this type of element is four-sided.

3. Solution to the studied problem

The report discusses the types of horizontal and vertical braces relevant to the spatial sustainability of buildings. The types of specimens selected for testing are tailored to the section types and massing factors most commonly used in practice.

The tests are part of a large-scale study [5] of the behaviour of the same steel sections with applied reactive protection - intumescent paint (this report) and passive protection - gypsum fiber boards [6] and rock wool.

A brief description is made of the tests carried out, the equipment used, the time taken for the temperature to rise above the critical temperature for the different types of profiles and the protection when applying a standard fire effect. A brief analysis of fire protection systems for steel members is carried out.

3.1. Types of horizontal and vertical braces

All buildings and structures are volumetric and spatial objects, both in geometric and static sense. They can absorb and bear loads and impacts in all directions.

In buildings with a frame structure, the metal consumption increases significantly in order to meet the stiffness requirements. In such cases, the use of vertical (lattice) braces is resorted to, as they essentially form the stiffness of the structure for horizontal actions. The most commonly used braces are "L"-, "X"- and "K"-shaped grid braces, the "X" braces providing the greatest reliability under seismic actions.

Advantages of grid systems are:

- economical and relatively easy to design;
- ability to carry all lateral loads, so columns and beams should be designed against gravity loads only;
- are critical to maintaining the stability of the steel structure in the event of a fire.

The commonly used cross sections for "X" lattice brace are:

- rectangular hollow sections;
- equal-arm anchors ("L"-shaped profile);
- tubular welded (round) sections.

Other commonly used sections for braces are:

- hot-rolled ("I" and "H" - shaped) profiles;
- hot-rolled ("U" - shaped) profiles.

3.1.2. Determination of the parameters of the test specimens

For the purpose of this study, the following profiles with a unit length of 1000 mm were selected:

- profile with a circular cross-section (Figure 1);



Figure 1 - Profile with circular section

- L-shaped profile (Figure 2);

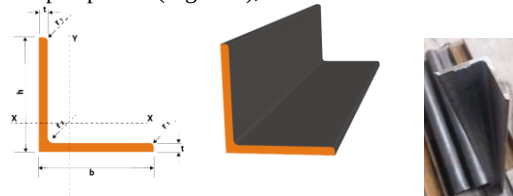


Figure 2 - L-shaped profile

- profile with a square cross-section (Figure 3).



Figure 3 - Square section profile.

- U-section profile (Figure 4).

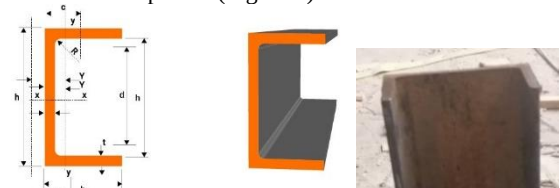


Figure 4 - U-section profile.

The parameters of the profiles are given in Table 1:

Table 1. Parameters of the tested profiles

Section of steel element	Dimensions	Thickness	Cross-sectional area	A/V without protection
		t	V	
	mm	mm	cm ²	m ⁻¹
Round hollow	88,9	2,0	5,46	511
L	50,0	4,0	3,89	514
Square hollow	60,0	3,0	6,74	356
U	52/120/52	8,0	14,12	310

3.1.3. Description of the protection used

A one-component intumescent paint in water emulsion consisting of synthetic resin was used for the tests. The paint is specifically designed for fire protection of load-bearing steel, reinforced concrete and composite steel-reinforced concrete structures. Three series of tests were conducted with three different coating thicknesses (Figure 5). The thicknesses are given in Table 2.

Table 2. Tested reactive paint thicknesses

Tests conducted in the FPlus laboratory	Sections and thicknesses of protection:			
				
	Thicknesses of the protections in mm:			
First test	0,76 ± 0,01	0,86 ± 0,018	0,82 ± 0,009	0,62 ± 0,004
Second test	1,62 ± 0,002	1,64 ± 0,004	1,72 ± 0,006	1,53 ± 0,019
Third test	1,79 ± 0,011	1,83 ± 0,014	1,95 ± 0,011	1,88 ± 0,012



Figure 5 - Protection with reactive paint

3.2. Experimental part

3.2.1. Study of tests performed

The intumescent protection tests are based on the introduced European standard EN 13381-8. Application should be airless or by hand using rollers. For elements with smaller cross-sections this poses a problem, as it is extremely difficult in practice to achieve a coating of uniform thickness over the entire surface of the element. In addition, airless application on these elements results in a large material overrun. In the case of higher FR or high-profile mass factor, several coats of paint are required and, for this reason, the total application time may be a limitation, as separate drying of the coats is necessary (typically around 24 hours). Intumescent paints have a limited service life and are relatively sensitive to abrasion and impact.

FR ranges from R 30 to R 180. It is recommended to use up to a maximum of R 60. Above this value, the number of layers and the thickness are irrational and the actual reliability in case of fire decreases as the layers peel off and fall off when intumescent.

This report complements a scientific study carried out on reactive and passive protections applied to the described profiles with mass factors outside the scope of the EN 13381 series of standards.

3.2.2. Test conditions

The protected specimens were tested under four-sided fire, which is the more severe test case and increases the ultimate mass factor. A standard temperature mode and test procedure described in [7] and EN 1363-1:2020 [8] was used.

The temperature of the steel was measured using K-type thermocouples. They are positioned, depending on the cross section of the steel members, at a minimum of two cross sections spaced along the height of the specimens.

3.2.3 Test results

3.2.3.1. First series of tests

The profiles described in section 1.2 were tested with applied protection from 0.76 mm to 0.86 mm thick. The rise in temperature of steel members is expressed graphically in Figure 6 for the different section types.

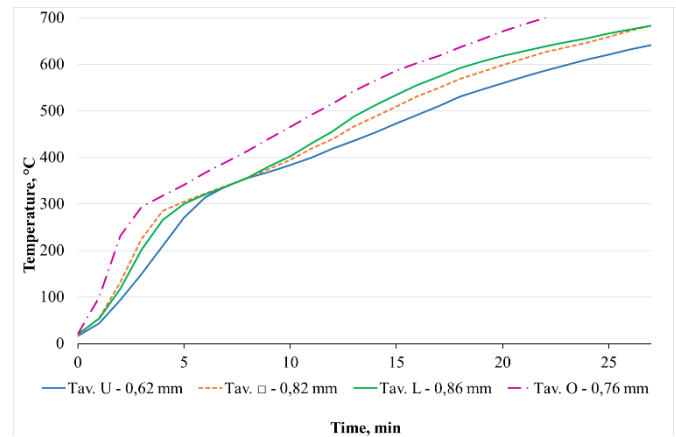


Figure 6 – Average temperatures (*Tav.*) of profiles (□, □, U, L) for reactive coating protection with thicknesses from 0.62 to 0.86 mm

3.2.3.2. Second series of tests

The profiles described in Section 1.2 were tested with protection applied in thicknesses ranging from 1.53 mm to 1.72 mm (Figure 7).

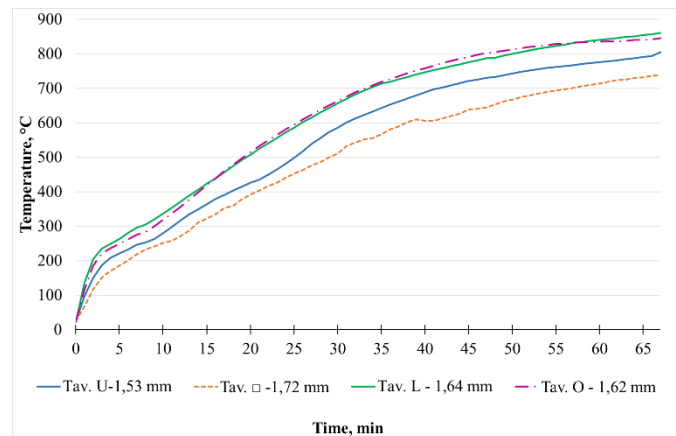


Figure 7 - Average temperatures (*Tav.*) of profiles (□, □, U, L) for reactive coating protection with thicknesses 1.53 to 1.72 mm

3.2.3.3. Third series of tests

The profiles described in Section 1.2 were tested with protection applied with thicknesses ranging from 1.79 mm to 1.95 mm (Figure 8).

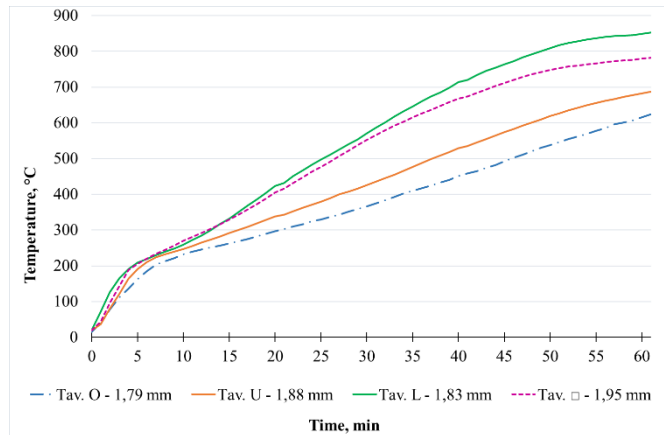


Figure 8 - Average temperatures (T_{av}) of profiles (O, U, L) for reactive coating protection with thicknesses from 1.79 to 1.95 mm

3.2.4. Calculational determination of the fire resistance of steel connections

Using the relationships given in Eurocodes EN 1990:2003 [9], EN 1991-1-2:2004 [10], EN 1993-1-1:2005 [11] and EN 1993-1-2:2005 [12], the critical temperatures of the test specimens in tension under actual roof construction have been calculated. The critical temperature of the three sections is $\theta_{a,cr} = 540^\circ\text{C}$.

To calculate the FR of the profiles, the Software for Investigation of Temperature Field Variation in Unprotected Steel Members was used. This is the time for the temperature in the steel member to reach (rise) to a critical value (Figure 9).

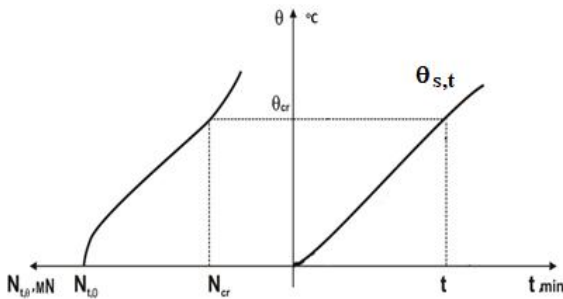


Figure 9 - Variation of bearing capacity as a function of temperature and time of fire of an unprotected steel connection

The calculated FR for the four unprotected profiles at $\theta_{a,cr} = 540^\circ\text{C}$ is:

- for the round hollow section - 6 min;
- for the L-shaped section - 6 min;
- for the square hollow section - 7,3 min;
- for the U-section - 9,1 min.

4. Results and discussion

This section summarises the calculation data (by Eurocode without protection) at $\theta_{a,cr} = 540^\circ\text{C}$ and the results of the tests carried out on each type of profile when protected with the three different thicknesses of reactive paint.

4.1. Profile with circular section:

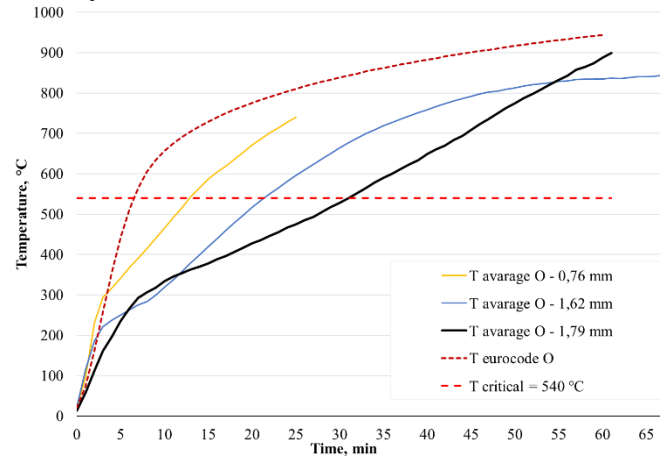


Figure 10 - Average temperatures of circular section with and without protection ($T_{eurocode}$)

4.2. L-section profile:

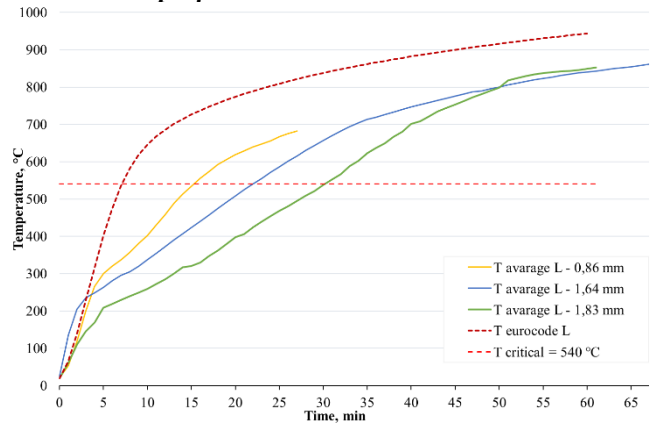


Figure 11 - Average temperatures of L-section profile with and without protection ($T_{eurocode}$)

4.3. Profile with square cross-section:

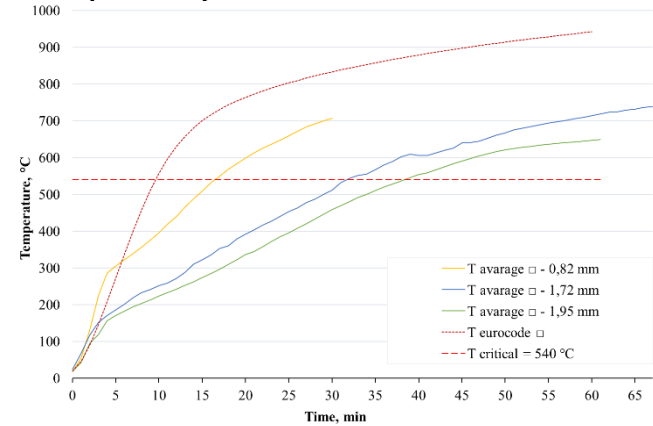


Figure 12 - Average temperatures of a square section profile with and without protection ($T_{eurocode}$)

4.4. U-section profile:

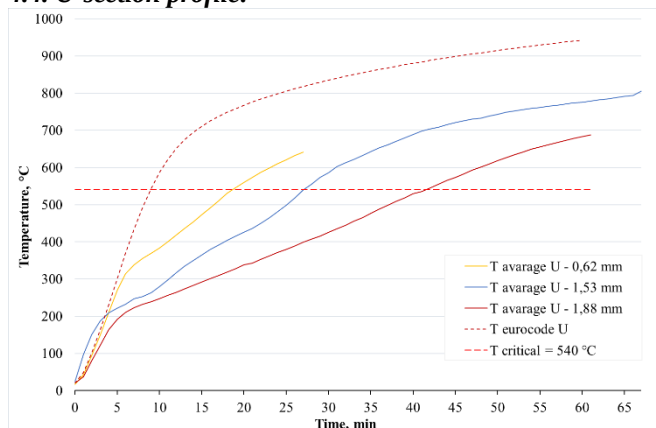


Figure 13 - Average U-section profile temperatures with and without protection ($T_{eurocode}$)

The summary results for $T_{cr.} = 540\text{ °C}$ are given in Table 3:

Table 3. Comparison of fire resistance of profiles

Profiles and mass factor:	○ $A/V = 511\text{ m}^{-1}$				□ $A/V = 356\text{ m}^{-1}$			
	I.	II.	III.	Eurocode	I.	II.	III.	Eurocode
Coating thickness in mm	0,76	1,62	1,79	-	0,86	1,64	1,83	-
FR in min at $T_{cr.} = 540\text{ °C}$	14	21	31	6	17	32	38	7,3
Profiles and mass factor:	└ $A/V = 514\text{ m}^{-1}$				$A/V = 310\text{ m}^{-1}$			
	I.	II.	III.	Eurocode	I.	II.	III.	Eurocode
Coating thickness in mm	0,82	1,72	1,95	-	0,62	1,53	1,88	-
FR in min at $T_{cr.} = 540\text{ °C}$	16	22	30	6	20	27	42	9,1

5. Conclusions

Based on the test results the following conclusions can be drawn:

- 1) at a critical temperature of $T = 540\text{ °C}$, it is questionable to reach even R30. For this reason, the main conclusion is that reactive paints are not suitable for the protection of steel structural elements with a mass factor outside the one defined in EN 13381-8;
- 2) it is extremely difficult to apply protection of uniform thickness over the entire surface of the profiles;
- 3) due to the small cross sections, the airless painting method cannot be applied;
- 4) doubling the thickness of the protection does not result in a double increase in fire resistance;
- 5) due to the uneven application of the coating, in some cases, even with greater coating thickness, the results are worse.

6. References

- [1] Todorov, Iv. et al. S. Пожароустойчивост и пожарозащита на строителни конструкции. [Fire resistance and fire protection of building structures.] Edition "Firefighter", 1998.
- [2] Todorov Iv., Hr. Prodanov. S. Изследване на изменението на носещата способност на стоманена колона при пожар съгласно БДС EN 1993-1-2:2005 [Study of the change of load-bearing capacity of a steel column in fire according to EN 1993-1-2:2005.]. Bulletin No. 23 Academy of Ministry of Interior, 2014, 32-41.
- [3] EN 13381-8:2013 Test methods for determining the contribution to fire resistance of building elements. Part 8: Reactive protection applied to steel members.
- [4] Spasov, D., S. Разработване на комплексна система за оценка границата на огнеустойчивост на стоманени строителни конструкции и елементи. [Development of a complex system for the assessment of the fire resistance limit of steel building structures and elements], Technical Council RIFSCP, 2002.
- [5] Simeonova N., Stanishkov Al. S. Brief analysis of methods for testing and evaluation of fire resistance of steel elements (braces). Proceedings of scientific reports part two - Jubilee international scientific conference - 50 years of higher education at the Academy of the Ministry of Interior. ISBN 978-954-348-184-2. 2019, 194-200.
- [6] Simeonova N., Tsonev Sv. S. Експериментално определяне на огнеустойчивостта на стоманени елементи (връзки), защитени с гипсфазерни плоскости. [Experimental determination of fire resistance of steel elements (braces) protected with gypsum fibreboards.]. Bulletin No. 2 of the Faculty of Fire Safety and Civil Protection. ISSN 1318-6687 (print), 2022, 45-53.
- [7] Spasov D., El. Hlebarova. S. Огнеустойчивостта - основна пожарна характеристика на строителните елементи и конструкции. [Fire resistance - basic fire characteristic of building elements and structures]. Safety and Occupational Medicine. Issue 3, 2010.
- [8] EN 1363-1:2020 Fire resistance tests. Part 1: General requirements.
- [9] EN 1990:2003 Eurocode. Fundamentals of the design of building structures
- [10] EN 1991-1-2:2004 Eurocode 1: Effects on building structures. Structural engineering - Part 1-2: Principal effects. Effects on structures exposed to fire.
- [11] EN 1993-1-1:2005 Eurocode 3: Design of steel structures. Part 1-1: General rules and regulations for buildings.
- [12] EN 1993-1-2:2005 Eurocode 3: Design of steel structures. Structural engineering - Part 1-2: Basic rules. Design of structures against the effects of fire.

Remote detection, recognition and tracking of objects in drones aircraft

Ivanova Eleonora, Stefanov Ivan

1Faculty of Computer Systems and Technologies, Technical University - Sofia, Blvd. Kliment Ohridski 8, 1000 Sofia, Bulgaria

E-mail: el_ivanova@tu-sofia.bg, ivan.ts.stefanov@tu-sofia.bg

Abstract: A review and analysis of methods for the detection and recognition of unmanned aerial vehicles (UAVs) has been carried out. UAV detection channels were considered - acoustic, optical, radar, infrared, radio reconnaissance channel. The advantages and disadvantages of the channels used are compared and evaluated. In the case of small UAVs, there are a number of significant difficulties and limitations. One of the directions in UAV detection is acoustic observations. The noise created by the UAV's power plant and propeller is an important unmasking feature. The creation and improvement of methods for the detection, direction-finding and recognition of small UAVs by receiving and processing their sound signals is an urgent task. In the implementation of this method of detection of UAVs are used frequency spectra, spectrograms, normalized autocorrelation functions and phase portraits of acoustic signals. Information features of the UAV sound image can be estimates of spectral coefficients determined from a discrete implementation containing a given number of samples, as well as parameters of autoregressive models.

KEYWORDS: MULTISENSOR SYSTEM, DETECTION AND CLASSIFICATION, UNMANNED AERIAL VEHICLES, ARTIFICIAL INTELLIGENCE, HUMAN FACTOR, COMMUNICATION AND INFORMATION SYSTEM, NETWORK-CENTRIC ENVIRONMENT

1. Introduction

One of the most important tasks in ensuring security against threats arising from the use of unmanned aerial vehicles (UAVs) is their detection and determination of their movement parameters.

The following requirements apply to UAV detection equipment:

- high target detection efficiency; ease of use; profitability (low cost); safety for people and wildlife; absence of obstacles in the operation of other technical systems.

2. Methods for detection and determination of UAV motion parameters

Currently, the most common methods for detecting and determining UAV movement parameters are:

- radio technical control (RTK); radar control; optical control; acoustic control.

In radiotechnical monitoring, two methods of obtaining information are used: search and observation. [1]

The search includes detection of radio signals from radio emission sources (ERS), their technical analysis, recognition of radio signals of ERs, recognition of ERs themselves and processing of spatial parameters of radio signals (bearing of ERs) to determine the coordinates of emitters.

The surveillance includes the implementation of radio interception operations of RES messages, tracking of the trajectory of RES, technical analysis of radio signals and recognition of RES signals.

The main tasks of radio technical control are:

- search and detection of UAV radio signals during panoramic viewing in the required frequency range or when tracking a fixed set of frequencies; determination of parameters and type of modulation of detected signals; demodulation of certain types of signals; determination of the type and structure of binary sequences (protocols), types of synchronization, primary and noise-resistant coding;

decoding and extracting messages; logging signals and messages, archiving data; direction finding of radioactive sources and determining their location during search; tracking the trajectory of the UAV during surveillance.

To solve these problems, it is necessary to use automated radio engineering control systems that provide:

- setting alerts; automatic scan (review) in a set range with display of scan results; determination in automatic mode and in dialogue mode with the operator of the modulation parameters of the analyzed signals; demodulation of certain classes of signals; Recording of signals on computer media; maintaining a database of processed signals; signal classification and exposure detection; direction finding and location determination of the UAV. [2]

Currently, unmanned aerial vehicles (UAVs) are widely used in various fields of human activity. For example, in agriculture, UAVs with GPS navigation are used to pollinate plants in fields. At the same time, significant savings in chemicals and more thorough crop treatment are achieved compared to manned aircraft. UAVs are used to deliver medicine and humanitarian aid to hard-to-reach areas and can be used to inspect power lines and pipelines. Drones,

another name for UAVs, can also be used by the state emergency service for surveillance and forecasting, as well as for the control of dangerous sites.

3. Main types of UAVs

Based on the variety of designs, there are four main types of UAVs. Fig. 1.

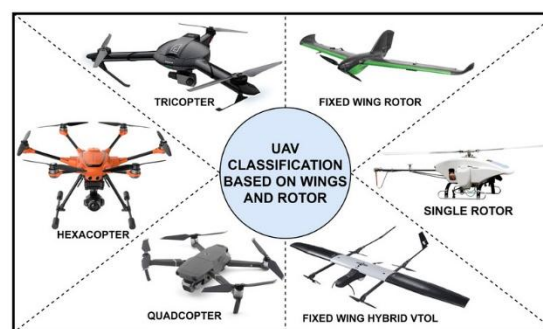


Fig. 1. Classification of UAV based on wings and rotors.

Multicopter drones are a flying platform with brushless motors and propellers. They have the ability to take off vertically or hover over an object and are the cheapest and most accessible version of UAVs. [3] Fixed-wing UAVs fulfill the structure of an aircraft and are ideal for long-range operations. Single-Rotor Drones – Unmanned helicopters are much more efficient than the multi-rotor versions. They have longer flight times and can even be powered by internal combustion engines. Hybrid drones are also known. As drones become more common, the issue of detecting UAVs in the air becomes more relevant. The following methods and means are used for this: radar, optical and acoustic. UAV optical detection is highly dependent on environmental factors. Increasing the detection range is achieved by narrowing the field of view, reducing the field of view and increasing the search time. Therefore, visual sensors are inefficient search devices. The use of acoustic channels for UAV detection is becoming more and more relevant. Acoustic sensors allow ground assets to search for and detect UAVs in passive mode, thereby reducing the likelihood of the enemy identifying their own positions. Therefore, modifying existing acoustic search systems or creating new systems can provide a reliable method of UAV detection. Drones can also be detected by receiving and analyzing radio signals: communication and control links, radar altimeters, active jammers and radar stations. However, this method can only determine the direction to the UAV, and the accuracy of the determination increases as the observation time increases. Some low-frequency communication links can be detected over considerable distances. Emissions from airborne radar stations (radar) and active jamming of UAVs can be detected at even greater distances. This method requires minimal equipment and allows you to quickly determine the direction of the target for further issuing target designations to optical or infrared surveillance equipment. [4, 5] Searching for UAVs using active radar stations is quite productive, since they have a relatively large

pulse search volume and a significant detection range. A significant drawback of the radar method is that most UAVs are made of composite materials that reflect electromagnetic waves rather poorly. Radio waves penetrate the surface of the device and are only partially reflected by it. Another problem is that due to the small size of UAVs, bandwidth limitations and, importantly, high cost, surveillance radars cannot be used often, especially when a network of radars needs to be deployed to ensure full coverage of the controlled area. Continuous wave (CW) and frequency modulated continuous wave (FMCW) radars currently represent the most attractive and cost-effective solution to this problem. An FMCW signal consists of a linearly modulated continuous wave transmitted in the desired direction. These types of signals differ from a CW signal where the operating frequency does not change during transmission. In most cases, target detection aims to detect the presence of objects that are not constant in the observed scenario, that is, objects that can dynamically appear or disappear. The moving target indicator is a mode of operation of the radar that allows the system to distinguish the target both among noise and among stationary objects in the observation area. This property is based on the Doppler effect, since stationary targets do not cause any Doppler frequency shift in the observed signals. Thus, the main method for detecting UAVs at significant distances is the radar method and the corresponding radars, characterized by a significant energy potential.

In world practice, there are two approaches to detecting objects using infrared (IR) images. The first approach is related to identifying an object by its own radiation using thermal imaging cameras. The spectrum of the object's own radiation is in the range of 7-14 microns. Modern thermal imaging cameras have a light temperature sensitivity of about 0.05 K. In the future, such systems should be equipped with a zoom lens up to 10-20 times. The second approach involves the use of active infrared laser illumination, for example, an infrared laser of 903 nm or 1560 nm for object detection and identification, topography of the area with subsequent identification of moving UAVs against the background of moving wildlife objects. In order to be able to detect UAVs at a distance of up to 2 km, the authors suggest using 1560 nm with a pulse duration of 1 ns, a repetition rate of 1 MHz and a pulse power of 700 kW. The divergence of the laser beam is of the order of 0.5 degrees. In this case, the system is equipped with a matrix photodetector (150 x 20 pixels) and an optical system so that the angular field of view of the matrix photodetector corresponds to the angular field of the laser beam. In other words, the system works by recording the reflected signal from the UAV in a given angular space from a matrix photodetector unit (PDU). The scanning system is equipped with a high-speed galvanometric mirror ($f = 1$ kHz) for sequential scanning of the laser illumination field. Such systems also perform the function of a laser range finder - LIDAR. [6, 7] Fig. 2.

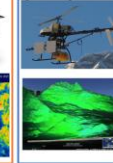
RGB-camera	Multi-spectral camera	IR-camera	SAR	LIDAR
Function: Captures visible light, providing high-resolution color imagery; Limitations: Limited to day light conditions	Function: Captures data across multiple spectral bands, aiding vegetation identification and classification; Limitations: Might limited spatial resolution	Function: Detects infrared radiation for identifying temperature; Limitations: Cannot detect geological feature directly; Might limited spatial resolution	Function: Penetrates through clouds and darkness, providing all weather and day/night monitoring; Limitations: Lower spatial resolution, complex data processing	Function: Measures distance using laserpulses creating 3D terrain model directly. Limitations: Can be affected by atmospheric conditions, cost
				

Fig. 2. Functions and limitations of on-board sensors.

4. Optical spectral methods

The ability to use optical spectral methods to solve problems with the detection and recognition of unmanned aerial vehicles against the background of wildlife objects largely depends on the power of the radiation sources, which decreases with increasing distance to the object and the sensitivity of the recording equipment . Estimating the potential maximum detection distances

of UAVs using optical methods requires further basic science research. The goal of such research should be to develop the scientific foundations for remote detection, identification, tracking and determination of UAV parameters and UAV membership in different groups using optical localization methods and optical spectroscopy, as well as automatic optical recognition in different environments of the background of moving live objects. Research should encompass existing and promising spectral optical methods aimed, among other things, at identifying new informative detection features. [8, 9] For their implementation, an experimental bench is created, which enables the implementation of the research objectives.

5. Conclusion

The analysis of the modern state of methods and technical means, optical location and optical spectroscopy showed the prospects for use in problems with the detection and identification of moving objects. At the same time, a complete effective system for spectral optical control of UAVs has not yet been created, as many unsolved problems, such as the speed of neural networks and the need for their constant training; physical limitations of the range of different types of optical methods; the complexity of the task of remote differentiation of objects of different nature. To solve them, it is necessary to combine methods of optical location and spectral analysis, methods of statistical theory, graphics, machine learning, neural networks and automatic control methods, which is an interdisciplinary fundamental scientific problem.

6. References

[1] Iliev, T.L., The role of unmanned aviation systems in creating information superiority in modern operations, Collection of reports from the Annual International Scientific Conference of the Aviation Faculty of Vasil Levski National Military University - Dolna Mitropolia, 19 - April 20, 2018, Faculty of Aviation of Vasil Levski National University, 2018, ISBN 978-954-713-114-9 - author.

[2] Iliev, T.L., Choosing an aviation surveillance system when creating information superiority in modern operations, Collection of reports from the Annual International Scientific Conference of the Aviation Faculty of Vasil Levski National Military University - Dolna Mitropolia, April 11 - 12, 2019, Faculty of Aviation of Vasil Levski National University, 2019, ISBN 978-954-713-123-1 - author.

[3] Iliev, T.L., Classification of objects related to the activity of terrorist organizations, as part of a recognition system, Collection of reports from the annual university scientific conference June 27 - 28, 2019, Vasil Levski National University, Veliko Tarnovo, 2019, ISSN 2367-7481 - author.

[4] Hunt, E., Artificial Intelligence, Academic Press, New York, San Francisco, London, 1975

[5] Olusiji O M., Martins Ezuma, Adrian P Lauf, and Ayodeji A Adeniran, Hierarchical Learning Framework for UAV, Detection and Identification, an Air Defense Regiment, Swedish Armed Forces, Sweden Center for Applied Intelligent Systems Research (CAISR), Halmstad University, Halmstad SE 301 18, Sweden c RISE, Lindholmospiren 3A, Gothenburg SE 417 56, Sweden 2012

[6] Medaiyese Olusiji O., Abbas Syed, Adrian P. LaufMachine Learning Framework for RF-Based Drone Detection and Identification System, 2021 2nd International Conference On Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), pp. 58–64. <https://ieeexplore.ieee.org/document/9617168>

[7] Hubenov, E., Z. Chiflidzhanova, Modeling of processes in event-oriented communication information systems, Scientific journal "Mechanics Transport Communications", no. 3, 2013, DS-23-29

[8] Hubenov, E., G. Sotirov, Z. Hubenova, Unmanned aviation systems with elements of artificial intelligence in the Internet environment. Seventeenth International Scientific Conference "Space, Ecology, Safety", PROCEEDINGS SES`21, pp. 121-127, Sofia, p-ISSN 2603 - 3313; e-ISSN 2603 - 3321. http://space.bas.bg/SES/archive/SES%202021_DOKLADI/PROCEEDINGS%20SES%202021.pdf

[9] Net-Centric Environment Joint Functional Concept Department of Defense USA, version 1.0 2005 <https://apps.dtic.mil/sti/pdfs/ADA490440.pdf>