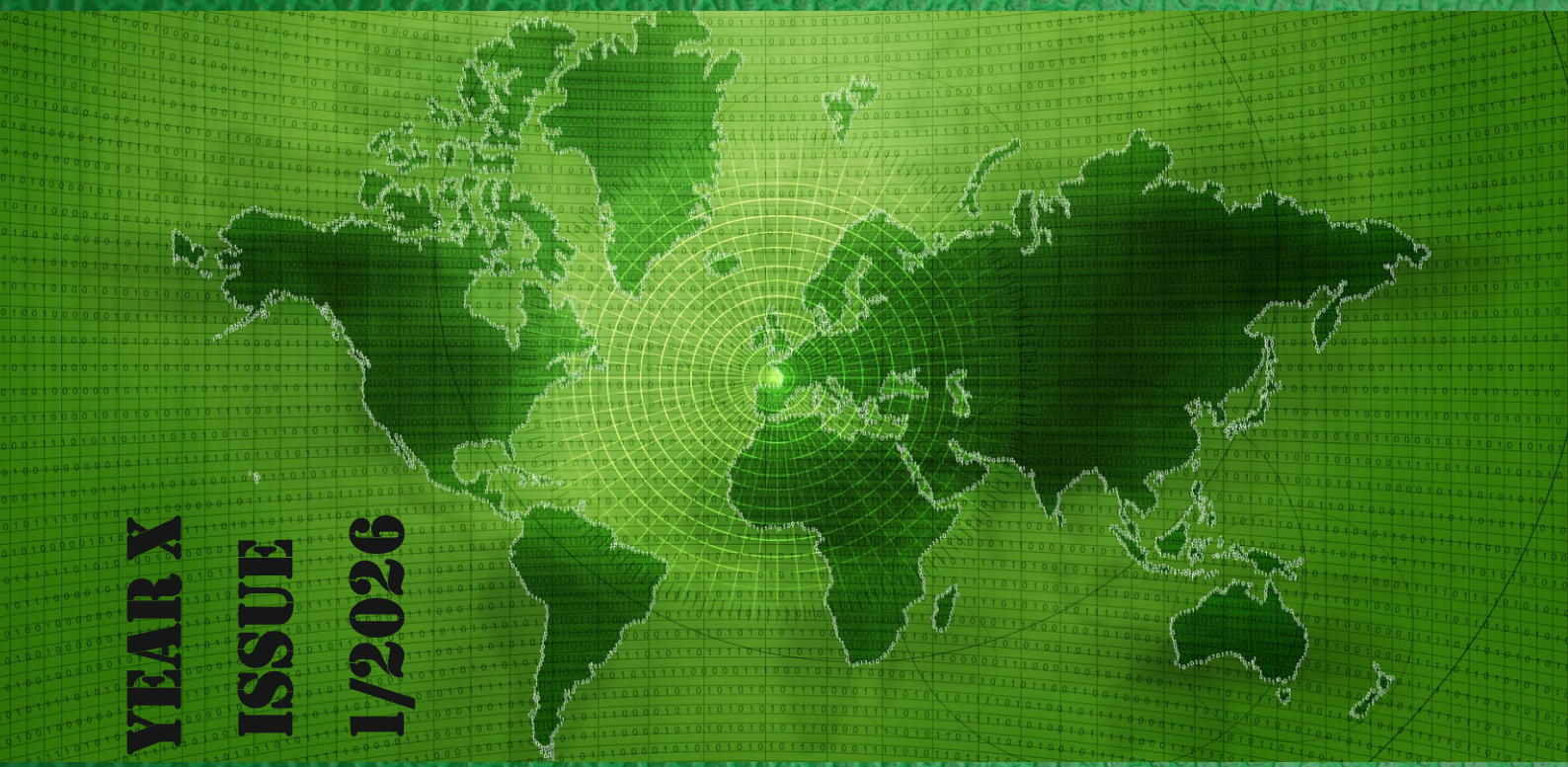
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

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



YEAR X
ISSUE 1/2026

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 X, ISSUE 1 / 2026

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

EDITORIAL BOARD

CHIEF EDITOR

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

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

C O N T E N T S

NATIONAL AND INTERNATIONAL SECURITY

Security Aspects of the Regulation of Financial Market Infrastructure and Financial Services Distribution in the Internal Market of the European Union: The Perspective of the Czech Republic
Jan Urbanec, Dana Junková 3

Some peculiarities of the security system elements development related to the implementation of the business plan for scientific research
Valeri Panevski, Marina Hristova 9

A competency model for training specialists in biological security in the context of bioconvergence
Maria Nenovska 13

Application of virtual and augmented reality in radiation control training for nuclear power plant personnel
Dimitar Dimitrov, Nadejda Randelova 17

INFORMATION SECURITY

Zkap anti-corruption output filter: a cryptographically verifiable compliance protocol for the deployment of artificial intelligence in investigative, regulatory, supervisory and judicial procedures
Radoslav Y. Radoslavov, Ivan Y. Getsov 20

Security evaluation metrics for an adaptive steganographic method based on the Canny algorithm
Veselka Stoyanova, Veselina Gagamova 26

TECHNICAL FACILITIES FOR ENSURING SECURITY SECURITY

Modular UAV Architectures in the Support of National Weapon Integration
István Papp, Bertold Békési 30

Numerical Modeling of Smoothbore Barrel Shot
Nikola Nikolov, Tsvetan Nikolov 33

Features in the design of unmanned aerial vehicles aircraft type
Sabi S Minev 37

Security Aspects of the Regulation of Financial Market Infrastructure and Financial Services Distribution in the Internal Market of the European Union: The Perspective of the Czech Republic

Jan Urbanec[1*], Dana Junková[2]
Police Academy of the Czech Republic in Prague, Czech Republic[1]
Police Academy of the Czech Republic in Prague, Czech Republic[2]
urbanec@polac.cz[*]

Abstract: *The financial market and financial services are important sector of the economy where various types of risks arise. These risks affect both entities making their financial business as well as their customers. Some of these risks, especially those that are systemic in nature and that concern more vulnerable customers (typically consumers), are responded to by regulation as a key instrument of public intervention in the freedom of enterprise. Most of the current legislative framework in this area today has its prototype in the European Union member states in community law. The security aspects of the organization of the financial market and the activities of financial service providers are today the subject of a whole series of directives and regulations. Security here has either a primarily macroeconomic (ensuring financial stability) or a microeconomic dimension (protection of individual customers). The interest of the state in this area, which captures criminal activity here (money laundering, financing of terrorism, tax evasion), is specific. The aim of the article is to structure the system of these regulations, to analyse its (local) effectiveness using data from relevant administrative authorities of the Czech Republic and to estimate future developments in the area, taking into account current geopolitical dynamics within the European Union and globally.*
Keywords*: FINANCIAL MARKET, FINANCIAL SERVICES, REGULATION, RISK, SECURITY*

1. Introduction

The financial market and financial services are an important sector of the economy, in which a number of various risks arise. These risks affect both entities making their financial business as well as their customers. Some of these risks, especially those that are systemic in nature and that concern more vulnerable customers (typically consumers), are responded to by regulation as a key instrument of public intervention in the freedom of enterprise. Regulation itself is a kind of state intervention that establishes, on the one hand, certain obligations (how to perform a specific business activity) and, on the other hand, certain rights, usually from the category of social or economic rights. *"The failure to identify and measure financial risk carries significant social and economic consequences"*[1].

The legitimate source of regulation in democratic societies and market economies is the legislative process. In contrast to earlier times, when the European Union was a mere international community of couple of states focused on removing barriers for mutual trade, which was also reflected in its institutional anchoring and the scope of lawmaking, it is common today that most legislative production in the Member States is associated with Community law, while the importance of purely national regulations is gradually decreasing.

The security aspects of the organization and functioning of the financial market and the activities of financial service providers are today the subject of a whole series of directives and regulations. Security here has either a primarily macroeconomic (ensuring financial stability, prevention of economic crime) or a microeconomic dimension (protection of individual customers). The macroeconomic dimension of regulation is usually reflected in the requirements for what kind of license an entrepreneur must have for his activity, what conditions he must meet in order to obtain it, what systems he must operate in order to meet the requirements for eliminating various economic and other risks, what professional capacities he must have allocated for his activity, how he must report on his activities to supervisory authorities, and the like.

Behind all this, there is a public interest in maintaining the general trust of the public, shareholders and investors in the ability of a given financial institution to fulfil its contractual and legal obligations. A bank towards its depositors, an insurance company towards its insured, an investment firms towards investors, a pension fund towards future pensioners. Another public interest of this type is the aforementioned prevention, detection and repression of economic crime, an example of which is in particular the rules and institutional instruments for sanctioning the financing of terrorism, money laundering, as well as tax evasion.

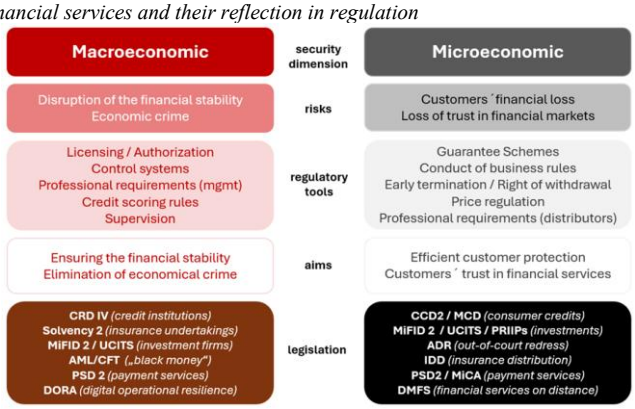
The second key category of regulation (microeconomic) is that which aims primarily to protect customers of financial institutions. This is achieved by a set of specific (additional) rights on the part of the customer and the associated obligations on the part of financial institutions. Examples of this protection may be guarantee systems of credit institutions (typically banks), conduct of business rules, regulation of financial relations in financial services (price ceilings, restrictions on inducements, limitations on contractual penalties), the right to early termination of the contractual relationship, mandatory professional liability insurance, etc. In some cases, a given type of regulation may serve both purposes simultaneously – prudential and protective. An example may be a requirement for minimum professional competence of persons providing financial services or an assessment of the customer's ability to repay a loan.

2. The aim of the article and methodology

The aim of the article is to structure the system of these regulations, to analyse its (local) effectiveness using data from relevant administrative bodies of the Czech Republic and to estimate future developments in the given area, taking into account current geopolitical developments in the Union and the world. We pay special attention to the remarkable pace of growth of sectoral regulation of the financial market, which can be observed in the last decade, and the subsequent wave of demand for rationalisation, efficiency, simplification or even deregulation of this sectoral legislative production. This is being voiced not only by the Member States (i.e. formally by the EU Council or the European Council), but also – albeit so far more at the level of a certain general political promise, which is subsequently relativised – by the European Commission as an institution with legislative initiative.

In accordance with the above, for the purposes of this article, we consider a division of the set of security risks, instruments and institutions, objectives and relevant legal regulations relating to the financial market and the provision of financial services into two basic "security dimensions" expressing their nature – microeconomic and macroeconomic. As mentioned, these are not completely disjoint sets. In certain aspects, these two dimensions overlap – they are used regulatory instruments that function as an imaginary "servant of two masters" and that can materialize in the same legal regulation (which collectively covers the functioning of a certain sector of the financial market).

Scheme 1: *Security risks in the financial market and in the provision of financial services and their reflection in regulation*



Source: authors

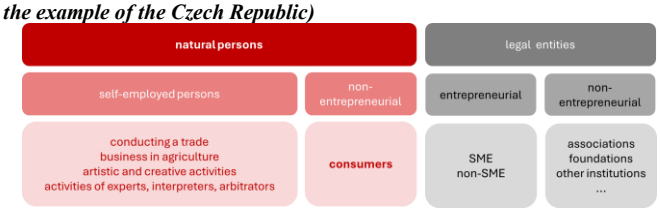
The key concept used is effectiveness – i.e. the degree of ability of a given regulatory instrument to respond to a given type of economic security risk. In accordance with the general meaning of this term, it is a state where, for a given volume of inputs (here, regulatory costs), the set objectives are maximized (here, risks are minimized), or when a given output is ensured with a minimum volume of inputs.

3. The microeconomic and macroeconomic dimension of regulation and the importance of behavioural economics

The microeconomic dimension of regulation: "Why and how to protect customers in financial markets?"

The ideological basis of the weaker position of some customers, especially consumers, in contractual relationships with financial institutions and their distributors (relationships referred to as B2C) is, in addition to the need to ensure the stability of the financial sector and the security of economic transactions, one of the relevant reasons why there is state intervention or regulation in the financial market. A consumer is usually understood to be a natural person who is not acting within the framework of their business activities or in the independent exercise of their profession. The aforementioned weaker position of the consumer is supposed to result from the consideration that such a person has limited economic and legal literacy necessary for rational decision-making in the financial market, as well as limited capacities for exercising their rights. However, some theoretical approaches and specific legislative standards grant above-standard protection not only to consumers, but also to other persons – e.g. self-employed persons, non-profit organizations or even so-called small and medium-sized enterprises (SMEs). However, the dominant object of protection remains natural persons who are not entrepreneurs.

Scheme 2: Theoretical personal scope of customer protection (using the example of the Czech Republic)



Source: authors

The demands on customers' financial and legal literacy - as a specific set of knowledge, skills and attitudes - are increasing as the offer develops and the complexity of financial services increases, especially those innovative ones based on so-called crypto-assets. However, not every "average consumer" [2, 3] is able to handle these demands. For many consumers, their first experience with the financial market comes only when they actually negotiate a financial product. Consumer protection is there to balance this often large deficit of competences needed for correct decision-making with certain additional rights, to a reasonable extent and using appropriate (mainly regulatory) instruments and institutions [4].

The specific features of the financial market that justify the increased need for consumer protection compared to other sectors of the economy include, in particular, the long-term nature of some financial products, the relatively low frequency of purchasing certain financial services (and thus the limited possibility for consumers to use experience and learn from mistakes), and often high financial obligations that result from the negotiation of the relevant contract. The state also plays a stronger paternalistic role here because it directly or indirectly supports a number of financial products (typically for the purpose of supporting housing and financial security for old age).

An effective customer protection policy contributes to more informed consumer decision-making, to the development of competition in the offer of financial services, to the limitation of unfair business practices, to ensuring security against loss of property, as well as to the prevention of negative social phenomena that may affect consumers as a result of inadequate negotiation of certain types of financial products and which may have not only individual but also significant societal consequences, including impacts on public budgets.

In general, customer protection policy can be implemented through a number of different legislative and non-legislative instruments – in particular institutional and product regulation (and self-regulation), provision of information and advice to consumers and support for financial education. The dominant role of the state usually lies in regulatory (and related licensing, supervision and sanctioning) activities. With reference to the content of the current valid sectoral legal regulations of the European Union in the area of financial markets and financial services, we can include the following among the standard regulatory instruments for customer protection:

- regulation of the entry of persons (financial service providers and intermediaries) into the sectoral business, or the conditions for remaining in it,
- public evidence of financial service providers and intermediaries,
- regulation of the contractual relationship regarding financial services,
- rules for dealing with customers, including information obligations,
- regulation of consumer dispute resolution mechanisms,
- price regulation (regulation of consumer costs for a financial product or service),
- rules for exercising control, supervision and oversight over compliance with the established obligations.

There is no universal concept of customer protection in the concept of the state. The regulatory system and the way in which regulatory instruments are used in each country always reflect its specific conditions – e.g. the tradition and degree of maturity of the financial market, the prevailing models of financial product distribution, the nature and urgency of market problems, the link to national social security systems, security needs and challenges, etc. As mentioned, within the internal market of the European Union, customer protection in the financial market is relatively strongly harmonised by European law. In these cases, the scope for national regulation is given either by the minimum harmonisation regime of the directive, so-called discretions, or by the fact that it is an area not regulated by European law (directives, regulations).

The selection and use of a specific regulatory instrument for customer protection should be preceded by an assessment of the costs expected in connection with its implementation and the benefits that the chosen measure should bring (RIA – Regulatory

Impact Assessment). The RIA process is a set of steps that gather evidence for decisions at the political level on the advantages and disadvantages of considered solution options, based on an assessment of their potential impacts. It is a tool that the state uses to fulfil its basic function, i.e. the protection of social values such as safety, health or environmental quality. Poor-quality regulation can bring more harm than good to society, which is why RIA has become an integral part of the legislative process in the Czech Republic since 2007. However, it cannot be viewed in such a way that where there is RIA, there is a guarantee of quality regulation. Even according to the findings of national authorities (in the Czech Republic, the Office of the Government) and experts, RIA often slips into formalism and the adaptation of the assessment carried out to the a priori intention of the regulator [5]. These criticisms can also be perceived towards the related analytical activities on the part of the European Commission – their cause may be, among other things, a conflict of interests of non-profit organizations that provide the European Commission with justification for the need for certain legislative activities, while they are paid for from the EU budget.

In general, it can be considered expedient for regulated entities themselves to participate in consumer protection in addition to public entities. The extent to which the principles of self-regulation can be effectively applied – i.e. the ability to effectively perform expected or public law-entrusted regulatory activities (chamber system) – is also largely determined by the situation on a specific market, the regulatory status quo, the structure and quality of the existing professional representation of regulated entities, etc. The boundary between self-regulation and regulation is then represented by so-called co-regulation, which represents the active participation of regulated entities in the legislative process and the sharing of corporate or sectoral know-how with the regulator. Co-regulation, especially if the professional interest group within a given sector is fragmented, on the other hand brings the risk of promoting individual private interests (to the detriment of the public interest). Therefore, it is corrected – sometimes more effectively, sometimes less so – by anti-lobbying legislation.

The importance of behavioural economics for an effective modern customer protection

For the purpose of assessing which of the customer (consumer) protection tools, when, in what form, to what extent and by which entities it is expedient and effective to use, knowledge from the field of behavioural economics can also be drawn. This generally examines the reasons why many consumers make more or less irrational or unexpected economic decisions under the influence of social, cognitive and emotional factors (in this case when negotiating financial services or managing personal and family finances) [6].

A significant factor in effective modern customer protection can be considered primarily the understandable way of presenting key information. With identical content and scope of information, but with different ways of its visual arrangement and terminological clarity, one can expect a significantly different degree of rationality in customer decision-making. On the other hand, it is considered counterproductive to overwhelm the consumer with too much information, which can ultimately lead to a distraction from the essential parameters of the financial service provided. However, as already mentioned, a number of different, often questionably beneficial information is currently predetermined by European Union law.

In this context, it is also necessary to take into account the empirically proven fact that many consumers make purchasing decisions under pressure from the seller and also because they are embarrassed to admit that they do not understand the product offered to the necessary extent. The desirable effect of information is naturally limited by the level of financial literacy of consumers. This can be considered more or less given in the short and medium term, and difficult to increase dramatically. The socially vulnerable, seniors, etc. (sometimes also referred to as "vulnerable consumers") are considered to be a particularly problematic category of people in terms of meeting the requirements for necessary financial education.

Financial literacy, as defined by the Organization for Economic Co-operation and Development (OECD) – which coordinates financial education programs internationally – is the set of knowledge, skills and attitudes necessary to achieve financial well-being through responsible financial decision-making [7]. Financial literacy is enhanced by both financial education and practical experience in negotiating financial products, and last but not least, adverse financial life events such as bankruptcy, debt relief, foreclosure, etc.

Each type of financial service exhibits certain behavioural specifics. In terms of behavioural findings, the problem of so-called selective optimism and overconfidence is significant in the credit product market. Individuals generally tend to summarize information in such a way that they overlook the unfavourable ones from the set, and on the contrary, subjectively overestimate the positive ones. At the same time, people tend to believe that in their case "things will turn out" better than on average (i.e., that they will not have problems repaying the loan, and that they will not be affected by sanctions). In the case of credit cards, a systematic underestimation of the long-term costs associated with the product is also observed. In many respects, the European standardized cost indicator (APCR – annual percentage rate of charge for consumer credit) is also limiting in terms of completeness, comprehensibility and comparability of information about a specific credit product.

A behavioural specific of another important financial product – insurance – is that the consumer does not actively seek the benefit from it as a standard, as it is associated with mostly unpleasant life events, or is associated with a very distant time horizon, or uncertain drawdown. In contrast to loans, insurance is a typical financial product that is “not bought, but sold”. The consumer tends to underestimate the key parameters of such a product, especially the ratio between its price (costs) and the promised performance. Often, even the customer does not know what he should actually want and expect from such a product.

The specifics of investment services can then be considered the mutual relationship between the required return on investment and its risk and liquidity. The way in which projections of the return on a given asset are created and presented also plays a behavioural role in the selection of investment opportunities. It is natural that investment service providers tend to overestimate the expected return on investment, or to underestimate the risks associated with it, thus creating the impression of a “free lunch” for the customer. Regulation responds to this phenomenon with various tools (information obligations, tests of adequacy and suitability, rules for calculating and presenting expected returns, mandatory conservative investment strategies), the effectiveness of which is, however, largely conditioned by a certain intellectual quality on the part of the specific customer. In the conditions of a transformed post-communist country such as the Czech Republic, the conservative profile of the investor prevails – i.e. an investor with aversion to risk (and therefore with tolerance for relatively low returns) – which dampens the phenomenon of unreasonable optimism to a certain extent.

The macroeconomic dimension of regulation: "How to ensure financial stability and security in financial markets?"

The macroeconomic dimension of financial market regulation and the provision of financial services is captured by the rhetorical question posed in the title of this part of the article, i.e. "how to ensure financial stability and security in the financial market?". The methodology of this article deals with aspects that result in the systemic nature (of the relevant risks and tools for their elimination) in relation to the economy as a whole. Systemicity is given here by a close connection, one could say directly by the umbilical cord, between the financial market, or rather the monetary economy, on

the one hand, and the real economy, i.e. the production of goods and services under conditions of scarcity and free price formation, on the other. The common goal of this regulation is prudence, i.e. a certain quality of a preventive nature. However, in order for prudence to be effectively enforced, it is indispensable to have control and sanction (restrictive) instruments applied by administrative (supervisory) authorities.

The basic prudential instrument, as confirmed by EU legislation, is the regulation of entry into business. This usually requires a specific authorisation issued by a competent national authority – usually a permit or licence on the one hand (where active assessment of compliance with the relevant conditions is assumed), or a registration procedure (where the aim is to register the entity without necessarily requiring compliance with certain additional conditions). In the case of banks, this concerns the regulation of capital adequacy, which is intended to create an environment of trust among depositors in the financial health of the bank, and thus prevent the risk of a bank run, which can lead to the collapse of the banking system, the cessation of lending and the destruction of the national currency with all the consequences associated with it, including an increase in internal security risks. In the case of insurance companies, this object of regulation is the technical reserves that insurance companies create for the needs of paying out claims from insurance events in the area of life and non-life risks. A specific sector of the financial market is payments, where the aim of prudential regulation is to ensure a safe, trustworthy and now also very fast payment system for settling payment transactions and covering any economic crime.

The DORA (Digital Operational Resilience Act) regulation is a key EU prudential initiative of recent times (valid from 1/2025). It covers the area of digital operational and cyber resilience, which aims to strengthen security in the financial services sector and unify requirements for individual types of financial institutions. In relation to the European Directive on measures to ensure a high common level of cybersecurity in the Union (2022/2555), it represents a special legal regulation for financial institutions. It introduces uniform rules for cyber risk management, information system protection and rapid response to incidents within the entire infrastructure of the EU internal financial market. This cross-sector regulation applies not only to banks and insurance companies, but also to investment firms, payment service providers, stock exchanges and other entities connected to the financial sector. The aim of this regulation is to ensure, in a fundamentally uniform manner, that financial institutions across the EU internal financial market are equipped with robust systems that can withstand cyber-attacks, technical failures and other digital threats. The key elements of the regulation are:

- identification, monitoring and management of ICT risks,
- standardized testing of resilience against cyber threats,
- reporting security incidents,
- public supervision of ICT service providers,
- sharing information about cyber threats between financial market entities.

The European regulatory trend of the last decade is undoubtedly the increase in entry requirements imposed on financial institutions and some financial intermediaries (advisors). In addition to financial equipment rules, these include requirements for internal management and control systems, personnel security for activities performed, product quality (financial services) and, nowadays, also ESG aspects. The costs of compliance activities of financial institutions are increasing significantly, which undoubtedly has an impact on pricing. This is a kind of quasi-tax that we pay for security in financial services. Here it is really appropriate to ask ourselves whether the constant increase in regulation is always consistently balanced by the effects that this regulation is supposed to bring. Theoretically, this effectiveness could be measured by the correlation between the scope of regulation or the intensity of supervisory activity on the one hand and the number of incidents (administrative proceedings, bankruptcies, security failures) on the other. However, we could face false causalities here, because the fact that the relevant incidents do not occur may not be the "merit" of perfect regulation or prudent supervision, but simply the confluence of favourable internal and external circumstances in the functioning of a given financial market sector or a specific company.

4. Empirical evidence from the perspective of the Czech Republic

Examples of violations of regulation in both its microeconomic (customer rights in the area of financial services) and macroeconomic (prudential requirements imposed on financial institutions) dimensions can be documented in the Czech Republic by the findings of relevant national authorities:

- Czech National Bank (as the financial market supervisory authority),
- Financial Arbitrator (as an independent public body for out-of-court settlement of consumer disputes in the financial market) and
- The Police of the Czech Republic (as a general security authority).

A specific set of findings that maps, among other things, the attitudes and experiences of the retail public on some issues of security in financial services is provided by the results of the measurement of financial literacy of the adult population, which is provided in the Czech Republic by the Ministry of Finance.

The majority of suspicions of illegal acts that the Czech National Bank dealt with – approximately half – in 2024 concerned credit institutions (banks and credit unions). They were substantively related to payment accounts and services related to them, the bank's communication with clients and handling their complaints and claims or termination of contractual relationships, compliance with AML/CFT regulations and fraud. For insurance companies, the main shortcomings were identified in the area of quality management of insurance distribution and settlement (liquidation) of insurance claims. They were substantively related mainly to the segment of reserve-building life insurance and motor vehicle liability insurance. In the case of both banks and insurance companies, on the contrary, the CNB has long positively assessed the compliance with prudential regulation regarding capital adequacy requirements (banks) and technical reserves (insurance companies). In the segment of non-bank consumer credit provision, the main supervisory topic is compliance with the obligation to assess the borrower's creditworthiness; complaints also focused on unauthorized business and shortcomings in the fulfilment of the creditor's information obligations towards the consumer (e.g. incorrectly calculated APR). Since 2025, the Czech National Bank has also been the supervisory authority for the crypto-asset market (in the sense of the MiCA regulation). In the non-bank investment and payment services sectors, the majority of submissions and subsequently conducted administrative proceedings concern (non-)fulfilment of the requirements set out in the AML/CFT legislation. In total, the Czech National Bank imposed fines of over CZK 110 million (approximately EUR 4 million) in 2024, which, with the gradually decreasing number of final decisions, means an increase in the average amount of the financial sanction imposed [8].

The Financial Arbitrator is an institution in the Czech Republic for the out-of-court resolution of consumer disputes in the financial market within the meaning of the European Directive on Alternative Dispute Resolution for Consumer Disputes [9]. The aim of this institute is to enable consumers to resolve disputes with a financial institution or financial intermediary regarding their rights quickly, cheaply and independently. The Financial Arbitrator was originally

established (in 2002) to resolve disputes exclusively regarding payment services, but today it covers essentially all sectors of the financial market in which retail financial services are negotiated. In 2024 [10] more than 5 thousand proceedings were initiated and over 7 thousand disputes were discussed (including unresolved disputes from previous years), and a total of approximately 4 thousand of them were duly concluded. In terms of trend trajectory, this is more than a hundred percent increase compared to previous years, which is evidenced by the growing awareness and interest of financial consumers in the services of this state institution. From a product perspective, the most frequent subjects of disputes were consumer credit (regarding the validity of a credit agreement due to incorrect assessment of the debtor's creditworthiness) and payment services (regarding unauthorized payment transactions[1]).

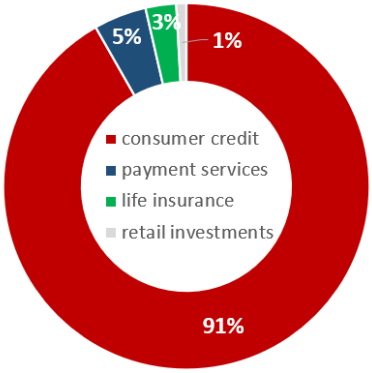


Fig.1 Financial Arbitrator of the Czech Republic – Product structure of disputes [10]

[1] The vast majority of these disputes are related to cyber-attacks targeting clients of individual institutions (consumers) and which must be divided into two basic groups depending on the extent to which the consumer cooperates with a third party (the person carrying out the cyber-attack). In proceedings concerning the misuse of a means of payment, the financial arbitrator must first assess whether the consumer acted under the influence of a third party. The most common cases are cases of so-called crypto fraud, where a third party convinces the consumer, or arouses their interest in investing funds with a high profit, or arouses their concern about their funds by telling them that their account and the funds on it are in danger and that they need to be transferred to a secure, protected account in order to save them. Other types of attacks can also be included in this category, in which the consumer has enabled a third party to control the computer, or the consumer's mobile phone, and thus dispose of the consumer's funds arbitrarily under his identity. In such cases, it is very difficult, if not impossible, to prove that the consumer did not act alone. The second category of cyber-attacks is represented by disputes in which consumers believe a fabricated scenario of a third party and thus make their personal security elements available to them (login details for online banking, payment card details, including various authorization codes). The most common types of fraud are so-called bazaar fraud, smishing in the form of messages regarding state contributions or tax refunds etc.

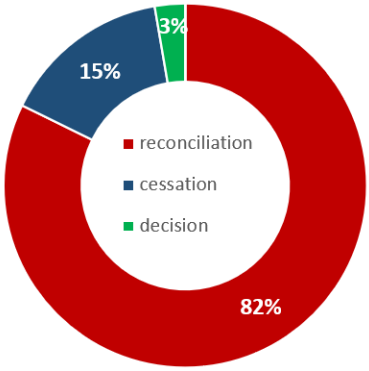


Fig.2 Financial Arbitrator of the Czech Republic –Ways of ending the above-mentioned disputes [10]

Almost 82% of disputes were settled[2], in 15% of cases the proceedings were discontinued and in about 3% the arbitrator decided (here in approximately half of the cases in favour of the financial institution and in half of the cases in favour of the consumer). Over time, the prevalence of amicable dispute resolution is gradually increasing, while the proportion of decisions has decreased to almost a quarter in the last 5 years. The average length of proceedings concluded in 2024 was 160 days, the median length was 125 days [10].

The Police of the Czech Republic (Criminal Police and Investigation Service) monitors "unauthorized measures, forgery and alteration of means of payment" as a separate category in its statistics, which in 2024 represented a total of 20% of property crime [11]. However, the volume of this criminal activity decreased by (also) less than a fifth year-on-year, which can be explained both by its successful detection and by greater public awareness of financial risks of this type.

From the results of measuring financial literacy of the adult population[3], which is part of the international OECD measurement and which was carried out in the Czech Republic in 2025, some findings regarding the attitudes of Czech citizens towards selected aspects of the security of their finances can be presented within the framework of the researched issue. It is interesting to note that our willingness to read contractual terms may be higher when we have a contract on paper in front of us than when we read it in electronic form (39 % of people agreed with this statement in the given measurement). In the digital world, this of course means higher demands on our self-discipline. 46 % of those surveyed admitted to acting more impulsively when shopping online (compared to shopping in a brick-and-mortar store). The majority of respondents (81 %) stated that they had not yet had any experience with fraud in the digital environment. Of those who have had this experience, 19 % responded that the fraud caused them damage of up to 50 euros, 34 % up to 500 euros, 14 % up to 5,000 euros and 14 % said that it was an amount exceeding 5,000 euros. The predominant experience is fraud when shopping in e-bazaars, e-shops and fraudulent SMS.

[2] Methodologically, an amicable settlement of a dispute is understood as a situation in which the consumer and the financial institution conclude a settlement agreement and the consumer withdraws their petition, or the financial arbitrator discontinues the proceedings as moot. It also includes cases where, during the proceedings before the financial arbitrator, it becomes apparent that the consumer's claim is unfounded and the consumer abandons the proceedings by withdrawing their petition.

[3] The measurement, based on responses to approximately one hundred questions, evaluates respondents' financial knowledge, skills, and attitudes across various categories of questions (e.g., household budgeting, financial reserves, financial products, the exercise of consumer rights, payment methods, and numeracy skills).

People here also stated that in the event of "payment fraud" they most often turned (quite correctly) to their bank (40 %) and the police (51 %). 8% of respondents know and mentioned the financial arbitrator. Preferences regarding the preferred method of payment for purchases are distributed practically evenly in Czech society – 37 % of respondents prefer non-cash payments (among other reasons, mainly for security reasons), 30 % said that they do not care, and 29 % prefer cash payments (among other reasons, also because cash, by its nature, allows for better protection of personal data). There are different opinions on which form of money allows for a better overview of household finances (48 % for cash, 47 % for non-cash). It is not surprising that older people and people with lower education generally have a more positive relationship with cash (and therefore more distrust of non-cash) [12].

5. Conclusion and recommendations

The aim of the article was to structure the system of regulations in financial markets and financial services distribution, to analyse its (local) effectiveness using data from relevant administrative bodies of the Czech Republic and to estimate future developments in the given area, taking into account current geopolitical developments in the Union and the world. We have paid special attention to the remarkable pace of growth of sectoral regulation of the financial market, which can be observed in the last decade, and the subsequent wave of demand for rationalisation, efficiency, simplification or even deregulation of this sectoral legislative production.

We believe that this rationalisation is a necessary condition and step for regulation to effectively fulfil its macroeconomic and microeconomic goals – as methodologically classified in the article. The path to this rationalisation should be not only reluctance in further regulation (i.e. stabilization of new rulemaking), but also a comprehensive revision of the existing one. “Less” sometimes means “more” in the end. As an example of good practice we see a principle-based regulation, which takes into account technological development, behavioural economics and the long-term level of financial literacy of the population. Which does not create room for regulatory arbitrage, is effectively controllable, proportionate to risks, does not create unnecessary additional administrative burden and does not establish de facto new social rights (e.g. the right to credit). Such selective and well considered regulation should be a kind of safe harbour for both clients of financial institutions and for the financial institutions themselves, which ultimately brings clear benefits in relation to the security of the economy as a whole.

6. References

1. Zarifian, A., Gallus, C., Overbeck, L., Pothos, E. M., & Blasiak, P. (2025). Using Bell violations as an indicator for financial market crisis. *The Journal of Finance and Data Science, 11*, 100164. https://doi.org/10.1016/j.jfds.2025.100164

2. Autsen, R. D. (2019). *The average consumer in confusion-based disputes in European trademark law and similar fictions*. Springer. ISBN 978-3-030-26349-2

3. Court of Justice of the European Union. (2024, November 14). *Compass Banca SpA* (ECLI:EU:C:2024:957).

4. Rutledge, S. L. (2010). *Consumer protection and financial literacy* (World Bank Policy Research Working Paper No. 5326). World Bank.

5. Urbanec, J., & Junková, D. (2021). Analytical standards in the legislative process (RIA) as a tool for increasing efficiency of the public sector in the Czech Republic. In *Ekonomična ta informacijna bezpeka: aktualni pytanňa ta innovaciji* (pp. 32–36). Dnipropetrovsk, Ukraine: Dnipropetrovsk State University of Internal Affairs. ISBN 978-617-8032-40-1.

6. Lefevre, A. F., & Chapman, M. (2017). *Behavioural economics and financial consumer protection* (OECD Working Papers on Finance, Insurance and Private Pensions, No. 41). OECD. https://doi.org/10.1787/0c8685b2-en

7. OECD. (2023). *OECD/INFE 2023 international survey of adult financial literacy*. https://doi.org/10.1787/56003a32-en

8. Czech National Bank. (2024). *Financial market supervision report 2024*. https://www.cnb.cz/export/sites/cnb/en/supervision-financial-market/.galleries/aggregate_information_financial_sector/financial_market_supervision_reports/download/fms_2024.pdf

9. European Parliament and Council. (2013). *Directive 2013/11/EU of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR).* Official Journal of the European Union, L 165, 63–79.

10. Financial Arbitrator of the Czech Republic. (2024). *Annual report of the Financial Arbitrator of the Czech Republic for 2024.* https://finarbitr.gov.cz/galerie/tinymce/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va%20o%20%C4%8Dinnosti%20finan%C4%8Dn%C3%ADho%20arbitra%20za%20rok%202024.pdf

11. Police of the Czech Republic. (2024). *SKPV Report for 2024* (pp. 43–44). https://policie.gov.cz/soubor/zprava-skpv-za-rok-2024.aspx

12. Ministry of Finance of the Czech Republic. (2025, September 28). *Presentation on the occasion of the Open House Day*. Open House Day event, Prague, Czech Republic.

Some peculiarities of the security system elements development related to the implementation of the business plan for scientific research

Valeri Panevski[1], Marina Hristova[1]
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 [1]
panevski@ims.bas.bg, marina.h@ims.bas.bg

Abstract: *Research organizations play an important role in diversifying and strengthening the research system through the implementation of projects and partnerships that contribute to the social and economic well-being of our country.*

This publication presents elements of the authors' experience in conducting scientific research through the development and implementation of a business model for managing applied scientific developments in the implementation of a project in the field of security of national critical infrastructure sites in seaports, through which a process is established for identifying, assessing and mitigating potential risks in a systematic, consistent and documented manner.

Key words: *SECURITY SYSTEMS, CRITICAL INFRASTRUCTURE, SCIENTIFIC RESEARCH*

Introduction

The main objective of the Business Model (BM) for the management of applied research and development in consortium projects is to provide a concise and up-to-date approach in an easy-to-use format for the implementation of business, technological, environmental and social aspects in the area in which the project is planned and implemented. The BM should provide an analysis of these aspects, as well as an explanation of the links between them and the priority areas of the development work.

Business models are fundamentally linked to technological innovation, but their construction is essentially separable from technology. We define a business model as a system that solves the problem of identifying user needs, engaging with those needs, and delivering value satisfaction.

The BM construct is attractive to the academic community, but there is also a lack of a common language that would allow researchers to refer to the work of others. In this paper, we present one perspective on the BM construct for conducting applied research in the implementation of critical infrastructure security projects, with a focus on maritime security, and where this perspective leads us in terms of understanding the relationship between BM innovation and technical innovation.

While some researchers argue that the concept of BM is positioned in the traditional strategic terminology of competitive advantage, we argue that BM is a stand-alone concept and is consistent with the widespread assertion in the scientific community that it should create value.

Another important aspect of the scope of BM development is the protection of scientific research to ensure that it is not used in an unwanted way. Given that threats to scientific research are evolving and manifest in many forms, it is necessary to conclude that collective efforts are needed to develop research security resilience - the scientific and educational organizations that make up the consortium on a given project (in this case G7475) share the responsibility for identifying and mitigatingsecurity risks related to scientific research and development.

The purpose of this publication is to provide stackeholders an approach to managing critical infrastructure (CI) security research and development by developing and implementing a BM for research and development that establishes a managent process, that allows identifying, assessing, and mitigating the security risks in a systematic, consistent, and documented manner.

Specifically, that will help research organizations to demonstrate how they can:

- ❖ develop and implement a series of personalized best practices for the implementation of scientific and applied research, which are both feasible and proportionate;
- ❖ identify and analyze the risks associated with the preparation and implementation of applied research projects in partnership conditions, and to determine the possible risks;

1. Business model

Collaborative research takes its place as a fundamental innovation process characterized by the building of relationships that create opportunities for gaining access to external sources of high technology and their integration into products and services developed in the interest of critical infrastructure security.

These activities refer to that part of BM that represents the ability to acquire knowledge, design, develop and improve products, services, technologies or processes. For scientific and educational organizations, research is the key to improving business skills, expanding the portfolio of products and services and maintaining applied research and development, in support of the security and protection of CI.

The creation and functioning of consortia plays a leading role in the planning, structuring and negotiation of mutually beneficial collaborations between universities, research institutes and various stakeholders in the field of security and defense, with the proper construction and functioning of appropriate business models playing a significant role in this regard.

The timely development of the BM is of particular importance for the proper functioning of project consortia and serves as a disciplinary framework that mediates between applied research, the technical and economic spheres, and ensures the connection of all activities during the development process. This is as important as the experiments that are carried out to assess the risks in the technologies. The role of the BM should become part of the new dominant logic for managing the commercialization of technologies.

The purpose of this paper is to present the impact of BM on two dimensions of collaborative research: collaboration, as an alternative to successful relationships, and risk sharing, as an effective tool for assessing the portfolio of opportunities for successful activity.

The preparation of a basic structure of BM for the management of research and applied scientific developments within the scope of the G7475 project is a stage of the work of the participants in it, and the following text will present to your attention the basic activities in the area of "key partners", "key activities" and "customer segments" (Figure 1).

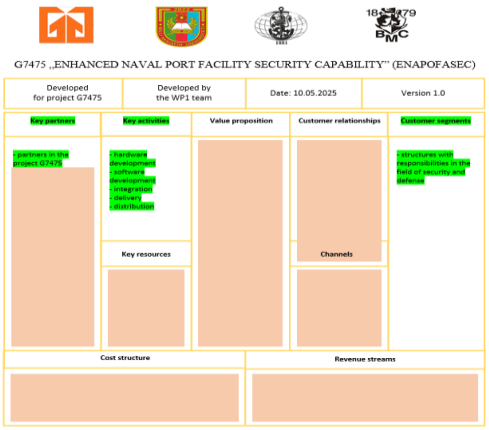


Figure 1: BM of project G7475 focusing on key elements related to the topic.

In essence, BM consists of several key assumptions **[1]**:

❖ Every organization aims to create value for its stakeholders;

❖ The organization seeks to capture the created value through various revenue sources;

❖ Understanding the processes of value creation and value capture requires focusing on the organization, but also considering how it is included in a network of external organizations (creating a consortium);

❖ The products and services offered are inseparable from the operations and activities of the organization;

❖ The organization's management voluntarily decides how to manage its business.

Building key partnerships through the creation of project consortia allows the implementation of good practices, focusing on [1]:

❖ exploitation of research results through intellectual property rights and individual products;

❖ training of doctoral students;

❖ dissemination of research results through publications, conferences, etc.;

❖ stimulation of networking and knowledge transfer;

❖ acquisition of funding from international structures (including EU and NATO sources);

❖ provision of research infrastructure;

❖ provision of market information.

These good practices offer key insights for project management, namely:

❖ The consortium should be flexible in finding support and developing research projects with different funding mechanisms, for products and systems with different Technology Readiness Levels (TRL);

❖ The consortium should offer different types of services to foster collaboration between science and stakeholders (national agencies and industry);

❖ Developing international collaboration through contract applied research and development should be a strategic objective.

The following motivations for creating project consortia can be structured **[1]**:

❖ Optimization and economies of scale - a basic form of partnership through the creation of project consortia is designed to optimize the allocation of resources and activities, which leads to cost optimization and often includes infrastructure sharing.

❖ Reduction of risk and uncertainty - partnerships through project consortia help reduce risk in a competitive environment characterized by uncertainty.

❖ Acquisition of certain resources and activities - through project consortia, partners' own capabilities are expanded, as they rely on each other to provide certain resources or perform certain activities.

1.1 Business Model Framework

The main motives behind the development of the BM framework are related to the creation of a technological and business platform for a security system, through which to present the research management (Figure 1) for models developed under the terms of the G7475 project, with the participation of current partners.

Here, the main elements of the BM, directly related to the implementation of the scientific and applied activities under the G7475 project, will be indicated, and they are:

Key partners - when defining this component, the following opportunities were identified:

❖ suppliers of microelectronic elements, cloud services, etc.;

❖ partners under the G7475 project - with proven capabilities in the field of developing maritime infrastructure security systems; simulations of risky events underwater; ensuring sustainable two-way communication, etc.;

❖ business partners, national and international, with a portfolio in the field of maritime security and protection systems;

❖ national agencies with responsibilities in the fields of security, defense, education and science, economy;

❖ Patent Office of the Republic of Bulgaria.

Key activities – the scope of the identified key activities includes the following:

❖ hardware development: compatible with the security environment, lightweight, secure, through minimal modifications, ensuring operation in a maritime security environment;

❖ software development: intelligent software with capabilities for automated diagnostics of sensor devices; software for scenarios for the types of risk events and application support of the developed software;

❖ purchase of raw materials and electronic components, assembly, testing and packaging of products and systems;

❖ if necessary, integration of the developed systems or their elements in the terms of the business partners with whom there are agreements;

❖ distribution of the developed systems and products.

Client segment – the following potential stakeholders for the development and use of the security system have been identified:

❖ users from security structures;

❖ users from departmental and local administrations;

❖ operators of critical infrastructure;

❖ users from business organizations with a portfolio in the field of developing products and systems in the field of security and protection;

❖ users from academic and scientific organizations in the development of products and systems for security and protection.

This component of BM, as one of the most important, is at the same time one of the most difficult to define not only for products based on hardware and software, but also for those related to ensuring compatibility, including interoperability, with strategic management systems created and functioning at the national level.

1.2 Connection between the structured elements of the BM and the actual implementation of project G7475.

Key Partners

The key partners and stakeholders are preliminary approved by the funding body of the G7475 project, who will implement the activities in accordance with the "Work Plan".

Key activities

❖ Hardware and software for the line elements (Layer 1 to 3) are in the process of development (Figure 2);

❖ The ways of joint work on the project have been coordinated with the stakeholders;

❖ Information about the project G7475 has been published on the website of the lead partner - Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A Balevski" at the Bulgarian Academy of Sciences;

❖ 11 publications have been developed, which are within the scope of the project G7475 **[2÷12]**.

❖ Integration into the information system of the stakeholders is not planned.

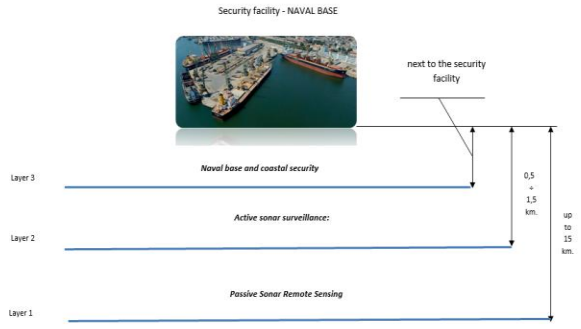


Figure 2: General scheme of project G7475.

Customer segment

The interested national structure for the creation of the maritime security system has been identified and approved by the funding organization of project G7475.

2. Relationship of BM with building resilience of critical infrastructure

According to ISO 22316:2017 **[13]**, organizational resilience is the ability of an organization to absorb impacts and adapt to a changing environment. Therefore, resilience in CI **[14]** can be considered as a qualitative state that reduces vulnerability, minimizes the consequences of threats, accelerates response and recovery, and facilitates adaptation to a disruptive event.

In this context, comprehensive knowledge of the operating conditions of the CI (operating environment, environmental and security environment) and of the main factors by which resilience is determined, limited and affected is the main prerequisite for strengthening the resilience of CI elements.

It is important to emphasize that organizational resilience is closely related to business continuity management **[15]**. This approach provides a practical framework for building an effective critical infrastructure management system, aiming to create protection and security against a wide range of potential threats and risk events.

Therefore, it can be said with sufficient reason that resilience of the CI is the inherent readiness of subsystems to be affected by a disruptive event. It is the ability of these subsystems to perform and maintain their functions when negatively affected by internal and/or external factors.

Considering the need to build sustainability of the functioning of the CI, we based our efforts on structuring the BM for managing scientific and applied developments under project G7475.

3. Conclusion

The presented structure of the BM for the management of scientific and applied developments within the scope of the G7475 project is based on the modern experience of the partners in the project consortium, who have achieved high efficiency in the field of scientific research and implementation of scientific products on the CI security market.

There are convincing reasons for developing their own BM, which requires a fundamental change in the way the consortium of organizations works and thinks. Therefore, the presented BM has an extremely high potential for sustainable increase in competitiveness and success.

Last but not least, the applied approach in the structuring and functioning of the G7475 project provides an opportunity for the proposed BM to ensure the competitive advantage of the key partnership between academic, university and interested organizations in the market implementation of the results of scientific and applied activities.

Acknowledgment

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

References:

[1] Valeri Panevski. SOME ASPECTS OF ESTABLISHING KEY PARTNERSHIPS FOR DEVELOPING SECURITY SYSTEMS, Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences, 2025, ISBN:978-619-245-546-0, pages 158

[2] I.J. Islamov, R.G. Akhundov, D. Dimitrov, V. Panevski. MODELING OF A CIRCULAR DISK MONOPOLE ANTENNA FED FROM A MICROWAVE BROADBAND COPLANAR WAVEGUIDE. Vol.7, 2, Advanced Physical Research, 2025, DOI - https://doi.org/10.62476/apr.72184, 184-185. SJR (Scopus):0.227;

[3] I.J. Islamov, R.G. Akhundov, Y. Iliev, D.Dimitrov, V.Panevski. MODELING OF WAVE PROCESSES IN A BROADBAND HORN ANTENNA FOR TRANSMITTING AND RECEIVING RADIO FREQUENCY MICROWAVE SIGNALS. Advanced Physical Research, Vol.7, No.3, Advanced Physical Research, 2025, ISSN:2663-8436,

DOI:https://doi.org/10.62476/apr.73292, 292-303. SJR (Scopus):0.227;

[4] Aleksandar Kolarov, Radostin Najdenov “An approach to monitoring, classifying and jamming underwater sound communications”, TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY. 2025 Proceedings year IX, ISSN 2535-0315(Print), ISSN 2535-0323 (Online) Issue 1 (18), pp. 160÷163;

[5] Bistra Nenova, “Sources of underwater ship noise”, TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY. 2025 Proceedings year IX, ISSN 2535-0315(Print), ISSN 2535-0323 (Online) Issue 1 (18), pp. 139÷141;

[6] Ivanov I., Kolev St., Lolov M., Kosev V, “Visualization of underwater acoustic information received from a multibeam sector sonar”, TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY. 2025 Proceedings year IX, ISSN 2535-0315(Print), ISSN 2535-0323 (Online) Issue 1 (18), pp. 147÷151;

[7] Valeri Panevski, SPECIFIC APPROACHES TO STRUCTURING A BUSINESS MODEL FOR SCIENTIFIC RESEARCH TO BUILD OF MARITIME CRITICAL INFRASTRUCTURE SECURITY SYSTEMS. Vol. 9 (2025), Issue 2, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, 2025, ISSN:2535-0668; 2535-082X, 43-45;

[8] Chief Asst. B. Nenova, PhD „Frequency spectrum of underwater ship noise “, Proceedings of CONFSEC 2025, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, YEAR 9, ISSUE 1 (11), ISSN PRINT, 2603-2945, ISSN ONLINE, 2603-2953, p.p. 109÷111;

[9] Ivanov, I., Kolev, S., Lolov, M. “Study of the Characteristics of a Hydroacoustic Antenna in a Marine Environment “, Proceedings CONFSEC 2025, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, YEAR 9, ISSUE 1 (11), ISSN PRINT 2603-2945, ISSN ONLINE, 2603-2953, p.p. 107÷108;

[10] Radostin Naydenov, “Determining the sources of potential terrorist threats when building port defense systems”, Proceedings CONFSEC 2025, SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, YEAR 9, ISSUE 1 (11), ISSN PRINT 2603-2945, ISSN ONLINE, 2603-2953, p.p. 71÷73;

[11] Adalat Pashayev, Ramil Akhundov, Elkhan Sabziev, Tahir Alizada, Dimitar Dimitrov, Valeri Panevski. Detection of an Object in a Water Area Based on Vector Hydrophone Data. Journal of Electrical Systems, 22, 01, Engineering and Scientific Research Groups, 2026, ISSN:1112-5209, 134-142. SJR (Scopus):0.18.]

[12] Islam Islamov, Kalin Kalinov; Iliyan Y. Iliev, Ramil Akhundov; Vagif Gasimov; Boyan Mednikarov and Miroslav Tsvetkov, “Modeling and experimental study of loudspeaker directivity patterns in the far and near fields“, INTERNATIONAL JOURNAL OF MICROWAVE AND OPTICAL TECHNOLOGY, Volume 21, Issue 1, ISSN 1553-0396, pp. 21-28.

[13] ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes

[14] Panevski, V. Critical infrastructure resilience assessment as a source of requirements for the security systems development. – Comptes rendus de l’ Académie bulgare des Sciences, 77, 2024, No 12, pp. 1801–1807. ISSN: 1310-1331 (Print), 2367-5535 (Online). SJR (Scopus): 0.16 Q3 (Scopus);

[15] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.

A competency model for training specialists in biological security in the context of bioconvergence

Maria Nenovska
"G. S. Rakovski" National Defence College, Sofia, Bulgaria
m.nenovska@rndc.bg

Abstract: *The rapid advancement of biotechnology, artificial intelligence, big data analytics, and digital technologies is transforming the nature of biological risks and creating new challenges for security systems. At the same time, the processes of bioconvergence are fostering increasingly close interactions among the life sciences, engineering, information technologies, and security studies. This paper explores the implications of these developments for the education and training of biological security specialists. Drawing on a systems approach, comparative analysis, and conceptual modelling, the analysis identifies the key competencies required for effective professional performance in a dynamic technological environment. An original competency model is proposed, integrating fundamental biological knowledge, technological competencies, security-related expertise, and practical skills for biological risk management. The model provides a conceptual framework for the modernization of educational programmes and for strengthening sustainable capacity to address biological threats.*
Keywords*: BIOLOGICAL SECURITY, COMPETENCY MODEL, BIOCONVERGENCE, COMPETENCIES, TECHNOLOGICAL TRANSFORMATION, ARTIFICIAL INTELLIGENCE.*

1. Introduction

The contemporary security environment is being reshaped by rapid advances in the life sciences and digital technologies, fundamentally transforming the nature of biological risks and the approaches used to manage them. The development of synthetic biology, genome editing, artificial intelligence, and related technologies creates significant opportunities while simultaneously introducing new challenges for biological security [1, 2, 4].

Bioconvergence, which integrates the life sciences with engineering and digital technologies, further increases the complexity of biological security and creates new requirements for the education and training of specialists. However, existing educational models remain largely discipline-based and do not adequately address the interdisciplinary competencies required in this rapidly evolving environment [2, 5, 7, 20].

This paper examines the implications of bioconvergence and technological transformation for the education and training of biological security specialists and proposes an original competency model aligned with contemporary professional requirements. By integrating biological, technological, and security-related competencies within a unified conceptual framework, the proposed model addresses an important gap in current competency-based education for biological security.

2. Methodology

The research methodology combines literature analysis, a systems approach, comparative analysis, and conceptual modelling, which together provide the methodological foundation for the development of an original competency model.

The study began with an analysis of scientific publications, international reports, and strategic documents addressing biological security, bioconvergence, advances in biotechnology, competency-based education, and the transformation of education in the context of digitalization [1–7, 20, 23]. The purpose of this analysis was to identify the principal trends and factors shaping the emerging requirements for the education and training of biological security specialists.

Using a systems approach, the education and training of biological security specialists was examined as a complex system comprising educational institutions, curricula, technological infrastructure, and the professional environment. This approach enabled an analysis of the interrelationships among these components and their influence on the development of the competencies required for effective professional practice. Such a methodological perspective provides a structured framework for investigating dynamic processes and deriving applicable solutions in the field of security [25].

Comparative analysis was employed to examine the differences between traditional educational models and the contemporary requirements arising from bioconvergence and technological transformation. This made it possible to identify the principal areas in which educational content and training approaches require updating to meet the evolving demands placed on biological security specialists.

Based on the findings of these analyses, an original competency model was developed using the method of conceptual modelling. The proposed model represents a conceptual framework that systematizes the principal competency domains and the relationships among them, with the aim of supporting the education and training of biological security specialists in the context of bioconvergence and the accelerated advancement of digital technologies.

The integrated application of these methodological approaches enabled the synthesis of the findings derived from the theoretical and comparative analyses into a unified competency model aligned with contemporary developments in biological security, bioconvergence, and competency-based education.

3. Theoretical Foundations of the Competency-Based Approach to the Education and Training of Biological Security Specialists

Rapid advances in the life sciences, digital technologies, and technological innovation are reshaping professional education and training across multiple disciplines. In response, Competency-Based Education (CBE) has emerged as a leading educational paradigm, emphasizing learning outcomes and the application of knowledge, skills, and professional attitudes in real-world contexts [20, 23]. Consistent with the European Qualifications Framework (EQF), competence is understood as the demonstrated ability to apply knowledge, skills, and personal attributes in professional practice and to assume responsibility in diverse contexts [20]. This understanding is also reflected in the Bulgarian pedagogical literature [23].

International organizations, including UNESCO and the European Commission, recognize competency development as essential for strengthening the resilience of educational systems and supporting adaptation to digital transformation [7, 15, 20]. The principal characteristics of competency-based education are summarized in Table 1.

Competency-based education promotes professional adaptability, critical thinking, teamwork, and lifelong learning while providing a systematic basis for curriculum design and learning outcome assessment [20, 23, 24].

Table 1: *Principal Characteristics of Competency-Based Education*

Characteristic	Description
Orientation towards learning outcomes	Focus on achieving specific, measurable results that reflect the competencies acquired by learners.
Integration of knowledge, skills and professional attitudes	Combining theoretical knowledge, practical skills and professional attitudes into a comprehensive professional competence.
Active participation of learners in the educational process	Emphasizing independent work, initiative and responsibility of the learners.
Use of practical tasks, case studies and simulations	Applying real or realistic situations to develop practical skills and the ability to make decisions.
Continuous assessment of competency acquisition	Conducting systematic and ongoing feedback to monitor progress and support learners' improvement.
Personalization of learning in accordance with individual needs	Adapting the learning process to individual goals, prior experience and learning pace.
Development of readiness for lifelong learning	Fostering self-directed learning skills, adaptability and motivation for continuous professional development.

In the field of biological security, the competency-based approach has become increasingly important in response to bioconvergence and rapid technological transformation. Specialists are expected to integrate expertise in the life sciences, digital technologies, risk management, and security studies. The competency model proposed in this study addresses these requirements by providing an interdisciplinary framework that integrates biological, technological, security, and social competencies to support the education and training of biological security specialists [1, 2, 4, 5].

4. Bioconvergence and Technological Transformation as Drivers of Change in the Biological Security Environment

Bioconvergence, driven by the integration of the life sciences, digital technologies, engineering, and artificial intelligence, is transforming medicine, public health, industry, and security systems. Advances in bioinformatics, big data analytics, automated laboratory systems, and artificial intelligence have significantly enhanced the analysis of biological data and accelerated the development of pharmaceuticals, vaccines, diagnostic methods, and public health preparedness capabilities [2, 4, 5, 6, 10, 11].

At the same time, technologies such as synthetic biology, genome editing, automated DNA synthesis, and artificial intelligence increasingly exhibit dual-use potential, expanding biological risks and requiring appropriate regulatory frameworks, including Regulation (EU) 2021/821 [1, 3, 4, 19, 26, 27].

Digitalization has also introduced new cyber-biological risks associated with biological databases, cloud-based platforms, and automated laboratory systems. Consequently, the biological security environment has become increasingly interconnected, complex, and uncertain, requiring specialists to combine expertise in the life sciences, digital technologies, cybersecurity, and risk management [5, 12, 13, 17, 18, 19, 28].

These developments highlight the need for competency-based educational models capable of preparing specialists to work with emerging technologies, assess evolving biological risks, and make informed decisions in an increasingly technology-driven security environment. The competency model proposed in this study is designed to address these emerging educational requirements [5, 16, 20, 23, 28].

5. An Original Competency Model for the Education and Training of Biological Security Specialists in the Context of Bioconvergence and Technological Transformation

5.1. Rationale for Developing the Competency Model

The need for a competency model arises from the growing mismatch between traditional educational programmes and the evolving professional requirements associated with bioconvergence and technological transformation. While conventional education has primarily focused on providing knowledge in microbiology, epidemiology, toxicology, and biological risk management, contemporary professional practice requires the integration of competencies related to digital technologies, data analytics, bioinformatics, artificial intelligence, and the management of complex risks [2, 5, 20, 23].

Based on the analysis of the scientific literature and the identified trends, an original competency model was developed (Figure 1). The proposed model comprises four interrelated competency domains that collectively define the knowledge, skills, and capabilities required of the contemporary biological security specialist.

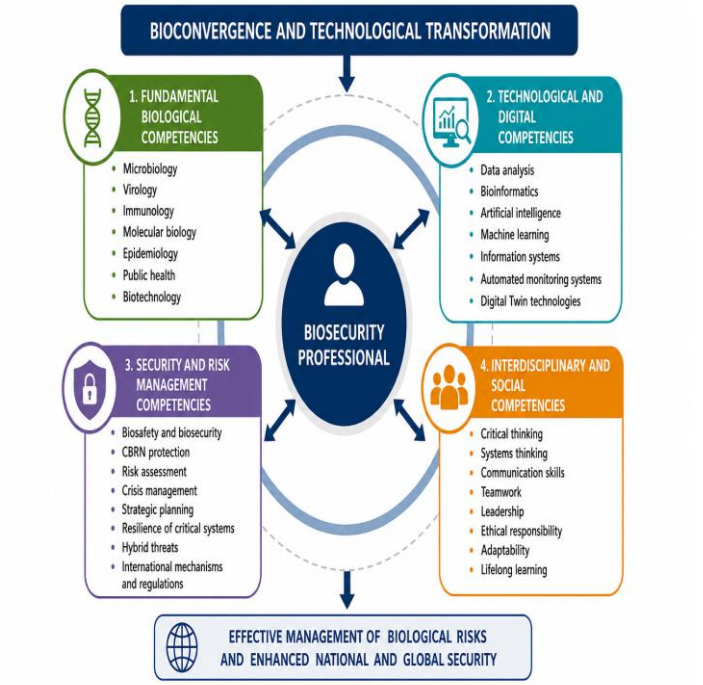


Figure 1. *Competency Model for the Education and Training of Biological Security Specialists in the Context of Bioconvergence and Technological Transformation*

5.2. Structure of the Competency Model

The proposed competency model comprises four interrelated competency domains:

- Fundamental biological competencies
- Technological and digital competencies
- Security and risk management competencies
- Interdisciplinary and social competencies

At the core of the model is the biological security specialist, conceived as an interdisciplinary professional capable of integrating knowledge and skills from multiple scientific disciplines and operating effectively in complex, dynamic, and technology-intensive environments.

5.2.1. Fundamental Biological Competencies

The first competency domain provides the scientific foundation for the education and training of biological security specialists. It encompasses knowledge of microbiology, virology, immunology, molecular biology, epidemiology, public health, and biotechnology. Despite the rapid advancement of digital technologies, these competencies remain fundamental to understanding biological processes, assessing biological risks, and interpreting specialized scientific data.

Particular emphasis is placed on competencies related to emerging biotechnologies, including synthetic biology, genome editing, and bioengineering, which are reshaping biological security systems and introducing new challenges for biological risk management [1, 2, 4].

5.2.2. Technological and Digital Competencies

The second competency domain reflects the impact of bioconvergence and digital transformation on professional practice in the field of biological security. Professionals working in the field of biological security are expected to possess knowledge and practical skills in bioinformatics, big data analytics, artificial intelligence–based tools, automated laboratory technologies, and digital platforms for information management and exchange. These competencies enable the analysis and interpretation of biological data, the simulation of complex biological systems, and evidence-informed decision-making.

In addition to technical expertise, this domain emphasizes the development of digital literacy and the capacity to adapt to rapidly evolving technologies. Such capabilities are particularly important in a dynamic technological environment, where continuous learning and the acquisition of new digital skills have become essential prerequisites for effective professional performance [5, 16, 20, 28].

5.2.3. Security and Risk Management Competencies

The third competency domain focuses on developing the knowledge and skills required to assess, prevent, and manage biological risks within an evolving security environment. It includes competencies related to biological security, biosecurity, risk management, crisis management, cybersecurity, and the regulatory frameworks governing activities involving potential biological risks.

Particular importance is attached to situational awareness, the ability to analyse complex threats arising from the convergence of biological and digital technologies, and informed decision-making under conditions of uncertainty [8]. In this respect, the domain extends traditional educational approaches by incorporating concepts of resilience, interinstitutional cooperation, and the management of complex risks that characterize the contemporary security environment [1, 3, 14, 19, 27, 28].

5.2.4. Interdisciplinary and Social Competencies

The fourth competency domain integrates the competencies required for the effective application of professional knowledge in real-world settings. These include critical and systems thinking, analytical skills, communication, leadership, teamwork in multidisciplinary environments, project management, and adherence to professional and ethical standards.

Biological security is inherently interdisciplinary, and effective biological risk management depends on close collaboration among specialists in the life sciences, engineering, information technologies, public health, and national security. Consequently, education and training should foster not only disciplinary expertise but also the capacity for coordination, effective communication, and collaborative problem-solving. Furthermore, lifelong learning and continuous professional development have become essential for maintaining professional competencies in the context of rapid technological change [7, 20, 23, 24].

The four competency domains should not be viewed as independent components but as an integrated system in which fundamental biological knowledge, technological and digital competencies, security and risk management competencies, and interdisciplinary and social competencies complement and reinforce one another. Their interaction determines the ability of biological security specialists to respond effectively to the challenges arising from bioconvergence and technological transformation.

For greater clarity, the principal competency domains together with their corresponding knowledge, skills, and professional capabilities are summarized in Table 2.

Table 2: *Structure of the Original Competency Model for the Education and Training of Biological Security Specialists*

COMPETENCY AREA	KEY COMPETENCIES	PRACTICAL APPLICATION OF COMPETENCIES
Fundamental Biological Competencies	• Microbiology • Virology • Immunology • Epidemiology • Synthetic biology • Genome editing • Bioengineering	Analysis and assessment of biological processes, identification and evaluation of biological threats.
Technological and Digital Competencies	• Bioinformatics • Big Data • Artificial Intelligence • Digital platforms • Automated laboratory systems • Digital modeling	Use of digital technologies for data analysis, process modeling and support for decision-making.
Competencies in Security and Risk Management	• Biological security • Bioprotection (biosafety and biosecurity) • Risk assessment • Crisis management • Cybersecurity • Regulatory framework and compliance	Assessment and management of biological risks, planning and coordination of activities in crisis situations.
Interdisciplinary and Social Competencies	• Systems and critical thinking • Communication • Leadership • Teamwork • Project management • Professional ethics	Effective interaction in interdisciplinary teams, coordination between institutions and informed decision-making in a complex environment.

5.3. Integrated Nature of the Competency Model

The proposed competency model is based on the integration of four interrelated competency domains. Unlike traditional educational approaches, in which individual areas of education and training are often addressed separately, the proposed model emphasizes their interdependence and complementary nature.

Effective biological risk management requires specialists to understand biological processes, utilize advanced technologies, assess emerging threats, and work effectively in interdisciplinary environments. Accordingly, the four competency domains should be regarded as components of a unified system rather than as independent areas of education and training.

6. Practical Applications of the Proposed Competency Model

The proposed competency model provides a systematic framework for curriculum development by aligning education and training with contemporary professional requirements. Through the integration of the life sciences, digital technologies, risk management, and security studies, it supports the development of interdisciplinary competencies for addressing complex biological threats [2, 5, 28].

The principal differences between the traditional educational model and the proposed competency model are summarized in Table 3.

Table 3: *Comparison between the Traditional Educational Model and the Proposed Competency Model*

Criterion	Traditional Model	Proposed Competency Model
Educational approach	Discipline-based	Competency-based and interdisciplinary
Learning focus	Knowledge acquisition	Competency development and application
Curriculum structure	Separate academic disciplines	Integrated competency domains
Technological preparation	Limited use of digital technologies	Integration of artificial intelligence, bioinformatics, Big Data, digital twins, and digital platforms
Security education	Focus on traditional biological risks	Integrated management of biological, cyber-biological, and hybrid risks
Practical training	Laboratory exercises and lectures	Simulations, virtual laboratories, scenario-based learning, and digital learning environments
Assessment	Knowledge assessment	Competency assessment and performance-based evaluation
Professional readiness	Preparation for specific professional roles	Adaptability, interdisciplinary collaboration, and lifelong learning

The model promotes adaptability and lifelong learning and can be applied across different educational levels and professional fields, including biological security, public health, crisis management, and national security [9]. Its implementation can be supported by contemporary educational technologies, such as virtual laboratories, digital simulations, artificial intelligence-assisted learning systems, and digital twin technologies, which facilitate scenario-based training and competency development in realistic learning environments [16, 17, 21, 22, 28].

7. Conclusion

This study demonstrates the need to modernize the education and training of biological security specialists in response to bioconvergence and accelerated technological transformation. It proposes an original competency model that integrates biological, technological, security, and social competencies within a unified conceptual framework aligned with contemporary professional requirements.

The proposed model provides a systematic basis for the development and revision of educational programmes while supporting competency development for professional practice in a dynamic and interdisciplinary security environment. It also offers a conceptual foundation for future empirical research aimed at validating the model and assessing its applicability across diverse educational and professional contexts.

8. References

1. National Academies of Sciences, Engineering, and Medicine, *Biodefense in the Age of Synthetic Biology* (National Academies Press, Washington, DC, 2018).
2. National Academies of Sciences, Engineering, and Medicine, *Safeguarding the Bioeconomy* (National Academies Press, Washington, DC, 2020).
3. G.S. Koblentz, *Living Weapons: Biological Warfare and International Security* (Cornell University Press, Ithaca, NY, 2009).
4. World Health Organization, *Global Guidance Framework for the Responsible Use of the Life Sciences* (WHO, Geneva, 2022).
5. NATO Science and Technology Organization, *Biotechnology and Human Enhancement Technologies* (NATO STO, Brussels, 2020).
6. European Commission, *2025 Strategic Foresight Report: Resilience 2.0 – Empowering the EU to Thrive amid Turbulence and Uncertainty* (European Commission, Brussels, 2025).
7. UNESCO, *Recommendation on Open Science* (UNESCO, Paris, 2021).
8. M.R. Endsley, Toward a Theory of Situation Awareness in Dynamic Systems. *Hum. Factors* **37**(1), 32–64 (1995).
9. World Health Organization, *Health Systems for Health Security: A Framework for Developing Capacities for International Health Regulations, and Components in Health Systems and Other Sectors That Work in Synergy to Meet the Demands Imposed by Health Emergencies* (WHO, Geneva, 2021).
10. A. Lele, *Disruptive Technologies for the Militaries and Security*, Smart Innovation, Systems and Technologies (Springer, Singapore, 2019).
11. European Centre for Disease Prevention and Control, *Strategic Framework 2021–2027* (ECDC, Stockholm, 2021).
12. U. Beck, *Risk Society: Towards a New Modernity* (SAGE Publications, London, 1992).
13. D. Helbing, *Globally Networked Risks and How to Respond*. *Nature* **497**(7447), 51–59 (2013).
14. NATO, *NATO 2022 Strategic Concept* (NATO Headquarters, Brussels, 2022).
15. European Commission, *Horizon Europe Strategic Plan 2025–2027*. European Commission, Brussels, 2024.
16. M. Coeckelbergh, *AI Ethics* (MIT Press, Cambridge, MA, 2020).
17. World Health Organization, *Laboratory Biosafety Manual*, 4th edn. (WHO, Geneva, 2020).
18. United Nations Office for Disarmament Affairs, *Biological Weapons Convention: Confidence-Building Measures* (UNODA, New York, 2023).
19. European Parliament and the Council of the European Union, Regulation (EU) 2021/821 of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items, *Off. J. Eur. Union* **L206**, 1–461 (2021).
20. European Commission, *European Qualifications Framework for Lifelong Learning (EQF)* (Publications Office of the European Union, Luxembourg, 2017).
21. M. Giberna, H. Voos, P. Tavares et al., *On Digital Twins in Defense: Overview and Applications*. J. Def. Model. Simul.: Appl., Methodol., Technol. (2026).
22. M.B. Okon, O.P. Ugwu, C.N. Ugwu et al., *From Pandemics to Preparedness: Harnessing AI, CRISPR, and Synthetic Biology to Counter Biosecurity Threats*. *Front. Public Health* **13**, 1711344 (2025).
23. M. Bizova, *Competence, Competence Approach and Development of Competence Models*. *Pedagogika–Pedagogy* **88**(1), 119–137 (2016). ISSN 0861-3982 (Print), ISSN 1314-8540 (Online).
24. T. Georgieva, Y. Yanakiev, *Stability in Dynamics: Diagnosing the Development of Some Key Components of Education at the Command and Staff Faculty during the Period 2000–2015*. In: Annual Military Scientific Conference of the Command and Staff Faculty "Contemporary Approaches to the Dynamic Management of Education and Training in Security and Defence," 22–23 June 2016, Yearbook of the "G. S. Rakovski" National Defence College, Command and Staff Faculty, No. 1, Sofia, 68–81 (2016). ISSN 1312-2991.
25. E. Shipochki, *Methodology for Studying the Dynamics of International Military Cooperation*. *Military Journal*, No. **4** (2025). pp. 28-38, ISSN 2534-8388
26. M. I. Nenovska, *Risks to Biological Security Arising from the Interaction between Technologies and the Life Sciences*. In: Proceedings of the International Conference on Advanced Research and Technology for Defence (ARTDef 2023). Sofia, Bulgaria: Professor Tsvetan Lazarov Defence Institute, pp. III-138–III-145 (2023). ISSN 2815-2581.
27. M. I. Nenovska, I. Radulov, From VUCA to BANI: Governing Dual-Use Biotechnologies through EU–NATO Civil–Military Interoperability. International Conference Knowledge-Based Organization, **32**(1), 223–230 (2026). DOI: 10.2478/kbo-2026-0026. ISSN 2451-3113.
28. Daruka A., Nigam A., Kumar S. *Cyberbiosecurity in Action: Securing the Biological Battlespace from Digital Subversion*. – In: *Proceedings of the 21st International Conference on Cyber Warfare and Security (ICCWS 2026)*, pp. 726–734, 2026.

Application of virtual and augmented reality in radiation control training for nuclear power plant personnel

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

Abstract: *This article analyzes the potential applications of virtual reality (VR) and augmented reality (AR) in radiation monitoring training for personnel at nuclear power plants. It examines the role of nuclear safety training, the importance of the human factor, the specifics of radiation monitoring and the potential of VR/AR technologies to improve staff training. A conceptual model and methodology for empirical research is proposed.*
KEYWORDS: *NUCLEAR FACILITIES, MODERN TRAINING TECHNOLOGIES, VIRTUAL REALITY, AUGMENTED REALITY, RADIATION CONTROL, TRAINING, NPP, NUCLEAR SAFETY*

1. Introduction

In the context of digital transformation, technologies such as virtual and augmented reality are becoming increasingly important, as they enable the creation of realistic and safe training environments [1].

Development of nuclear energy is an important area of functioning of developed world countries. Nuclear power plants are objects of increased danger, so their development prospects are closely related to issues of safe operation and protection of territories, personnel, the environment on the territory of the station.

The safe operation of nuclear power plants is inextricably linked to the level of staff training. The International Atomic Energy Agency emphasizes that effective training and expertise maintenance are key prerequisites for nuclear safety [2].

2. Theoretical Foundations of Training and the Human Factor

Training at a nuclear power plant is a continuous process that encompasses initial training, maintenance of expertise, and periodic knowledge enhancement.

Use of virtual and augmented reality technologies for energy sector received positive approval from the world's leading countries and confirms its economic efficiency through:

the reduction of cost and time costs of staff travel to facilities;

elimination of design errors before the beginning of the stage of construction and installation works;

increasing the level of industrial safety; improving the management of nuclear power plants.

The Systematic Approach to Training (SAT) includes the analysis, design, development, delivery, and evaluation of training [3].

The human factor remains a critical element of the safety of nuclear facilities.

Effective training supports the development of competencies, reduces the likelihood of errors, and contributes to the formation of a safety culture [6].

3. Radiation Monitoring and Radiation Protection at Nuclear Power Plants

Radiation monitoring is a system of organizational and technical measures for observing and assessing the radiation situation.

Its primary objective is to protect the personnel, the public and the environment. According to the ALARA principle, radiation exposure should be kept as low as reasonably achievable [4].

Radiation monitoring includes individual dosimetric monitoring, workplace monitoring, monitoring of radioactive contamination, and radiation risk assessment as outlined in IAEA (2018) [5].

4. Limitations of Traditional Training

Traditional forms of training rely primarily on lectures, presentations, and limited hands-on exercises. They provide the necessary theoretical training but do not always allow for realistic simulation of emergency situations or work in high-risk conditions.

Practical training sessions are often limited by safety requirements and the need to minimize dose exposure.

Existing radiation control training programs are subject to the following limitations:

- Limited access to real radiation zones;

- Inability to simulate certain emergency scenarios;

- Risk of additional occupational dose exposure;

- Restricted opportunities for practical training of newly recruited personnel;

- High financial costs associated with conducting physical practical exercises.

5. Virtual and Augmented Reality

Virtual reality is a computer-generated environment in which the learner interacts with virtual objects and processes [7]. Augmented reality enhances the real environment by superimposing digital information onto real objects [8].

These technologies enable interactive learning, repeated practice of procedures, and the safe simulation of complex situations.

VR and AR can be used to simulate work in controlled areas, locate sources of contamination, use dosimetry equipment and respond to radiation incidents.

Through virtual scenarios, trainees gain practical experience without being exposed to actual radiation. AR supports task performance by displaying instructions and dose data in real time.

6. Conceptual Model

A model is proposed that includes five consecutive stages: theoretical training, VR simulations, AR support, practical assessment and analysis of results. The expected outcomes are the development of competencies, the enhancement of safety culture and the reduction of human errors.

The model links training to the ultimate goal – improving nuclear and radiation safety.

A model comprising four sequential stages is proposed:

Stage 1: Theoretical Preparation

Study of:

- Radiation protection;

- Dosimetric control;

- Emergency procedures;

- Regulatory requirements.

Stage 2: VR Training

Simulation of:

- Work in a controlled area;

- Radiological survey;

- Use of radiation monitoring instruments;

- Emergency scenarios.

Stage 3: AR Training

Real-environment visualization of:

- Radiation fields;

- Control checkpoints;

- Safe transit routes;

- Work instructions.

Stage 4: Evaluation and Analysis

Automated assessment of:

- Response time;

- Procedural compliance;

- Measurement accuracy;

- Decision making.

7. Benefits and challenges

One of the most important benefits of AR and VR in Radioactive Waste Management (RadWM) is improved safety. These technologies enable the simulation of hazardous scenarios, allowing personnel to train in a controlled, risk-free environment without the need to be physically present in dangerous or radioactive areas [9].

By reducing human exposure to radiation, AR and VR training programs significantly enhance worker safety. In addition, these technologies can be used to simulate emergency situations, providing personnel with the necessary skills and knowledge to respond effectively, without any risk of exposure to actual hazards.

Another key advantage of AR and VR is their enhanced efficiency. These technologies streamline the training process, allowing workers to gain practical experience without the need for physical equipment or facilities.

For instance, trainees can practice RadWM procedures in VR simulations, leading to faster and more effective skill acquisition. Moreover, the use of AR can assist in real-time guidance during maintenance and operational procedures, reducing downtime by 50% and enhancing operational efficiency.

Cost savings are another significant benefit associated with the use of AR and VR in RadWM. Traditional training methods often require physical resources, travel, and on-site exposure to hazardous environments, all of which incur high costs.

By utilizing AR and VR for training and simulation, companies can significantly reduce these expenses (reduction in training time for new technicians by up to 60%) while also minimizing the risk of accidents and equipment damage (overall maintenance cost reduction of 10–40%).

Furthermore, AR and VR can contribute to more efficient use of resources, such as reducing the need for physical materials and optimizing workforce management. Moreover, the use of AR and VR can lead to increased transparency in RadWM operations.

These technologies can be used for public outreach and education, offering the public immersive simulations of RadWM facilities and processes. By providing transparent access to the operations and safety measures involved in RadWM, AR and VR can help foster greater public trust and understanding.

Through virtual tours, educational programs, and community engagement initiatives, these technologies allow the public to gain insight into complex and sensitive areas of nuclear waste management, promoting informed decision-making.

Although the benefits of AR and VR in RadWM are clear, there are several challenges that must be addressed to ensure the successful integration of these technologies into the industry. One of the primary challenges is technical barriers. Developing high-quality VR and AR experiences requires specialized technical

A number of countries have already implemented projects to introduce VR training in nuclear plants

The training includes emergency scenarios, equipment replacement, and communication in stressful situations, with all parameters recorded and analyzed in real time.

Despite the obvious advantages, there are also challenges – the high cost of developing VR content, the need to update software, and the need for specialists to adapt curricula to the digital environment.

Therefore, the implementation of these technologies must be strategically planned and integrated into the overall training and qualification program systems, (IAEA, 2020) [4]

8. Future directions

1. Ffuture development should prioritize the creation of standardized, high-resolution VR models of RadW storage and disposal facilities, incorporating real-time sensor data to enable proactive issue identification and predictive maintenance scheduling. This builds upon the benefits of improved safety and effectiveness already demonstrated.

2. Further efforts should focus on developing intelligent AR systems that integrate with existing maintenance databases and provide context-aware, step-by-step instructions, coupled with automated compliance checks to minimize errors and increase protection during complex tasks.

This directly addresses the need for enhanced precision and error reduction.

3. Future initiatives should establish collaborative VR platforms that allow for real-time stakeholder engagement and iterative design testing, incorporating feedback from safety and operational teams early in the design phase to avoid costly modifications during construction and optimize facility layouts for effectiveness and protection.

This moves towards more tangible improvements in design and planning.

4.Future research should focus on developing sophisticated VR simulation tools that can model a broader range of complex operational and emergency scenarios, incorporating predictive analytics and AI-driven risk assessments to augment preparedness and inform robust decision-making in RadWM.

This directly addresses the need for improved scenario analysis and risk mitigation.

9. Conclusion

The application of modern training technologies such as virtual and augmented reality, interactive simulators, and digital twins is a key

element in the development of modern staff training at nuclear power plants.

These tools not only improve the quality and effectiveness of training, but also contribute directly to increased safety by minimizing the human factor and improving coordination in real-life situations.

Combining technology and traditional forms of training creates a sustainable training model that supports the development of competent, confident, and responsible personnel - a key guarantee for the safe operation of nuclear facilities.

The VR and AR technologies rapid development has expanded the scope of their application, as follows [10]:

1. Application of VR and AR technologies for educational purposes.

2. VR and AR technologies application examples and trends in various industries.

3. VR and AR technologies application examples and trends for NPPs. The economic efficiency of using VR and AR for NPPs is achieved by eliminating design errors before the start of the construction phase, reducing time and costs for business trips of staff for staff professional development, increasing the level of industrial safety.

4. Peculiarities of application of VR and AR technologies for training of future specialists and advanced training of NPP personnel.

5. Application of VR and AR technologies for the popularization of professions in nuclear energy among children and youth. Due to VR and AR technologies, the issues of "nuclear energy safety" have gained new importance both for NPP personnel and for the training of future specialists in the field of nuclear energy.

References

[1]. Oleksandr Popov, Anna Iatsyshyn, Dmytro Sokolov, Maksym Dement, Ihor Neklonskyi & Alexander Yelizarov, Application of Virtual and Augmented Reality at Nuclear Power Plants, Systems, Decision and Control in Energy II, pp. 243-260.

[2] IAEA (1996). Nuclear Power Plant Personnel Training and Its Evaluation: A Guidebook

[3] IAEA (2002). Systematic Approach to Training

[4] IAEA (2014). Radiation Protection and Safety of Radiation Sources

[5] IAEA (2018). Occupational Radiation Protection

[6] Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith- Jentsch, K. A. (2012). The Science of Training and Development in Organizations

[7] Stanney, K. M., & Hale, K. S. (2014). Handbook of Virtual Environments

[8] Azuma, R. T. (1997). A Survey of Augmented Reality

[9] Mohamed, A-MO, Mohamed, D, Fayad, A & Al Nahyan, MT 2025, 'Enhancing Radioactive Waste Management: The Role of Augmented and Virtual Reality in Training and Public Engagement', Green Energy and Environmental Technology, vol. 4, no. 1, pp. 1-35.

[10] Oleksandr O. Popov, Anna V. Iatsyshyn1, Andrii V. Iatsyshyn, Valeriia O. Kovach, Volodymyr O. Artemchuk, Viktor O. Gurieiev, Yulii G. Kutsan, Iryna S. Zinovieva, Olena V. Alieksieiev, Valentyna V. Kovalenko1,7 and Arnold E. Ki Immersive technology for training and professional development of nuclear power plants personnel

Zkap anti-corruption output filter: a cryptographically verifiable compliance protocol for the deployment of artificial intelligence in investigative, regulatory, supervisory and judicial procedures

Radoslav Y. Radoslavov *, Eng. Ivan Y. Getsov
Independent researchers
Law Office — Ruse, Bulgaria · Advanced Consulting London RR, United Kingdom
ORCID: 0009-0003-6868-8083
* Corresponding author. E-mail: radoslav@radoslavov.bg · zkap@advanced-consulting.london
Patents: BG/P/2026/114317; BG/P/2026/114328 · EPO/PCT/UKIPO in preparation · FRAND-ready
IPC: G06F 21/64; G06N 20/00; H04L 9/32

Abstract: *The integration of artificial intelligence into judicial and administrative procedures raises a structural regulatory crisis. The European Union has imposed simultaneous and competing obligations: on one hand, the AI Act (Regulation (EU) 2024/1689) mandates transparency, human oversight, and accuracy for high-risk systems; on the other, the GDPR (Regulation (EU) 2016/679) and the Trade Secrets Directive (2016/943) impose strict confidentiality. This article proposes the ZKAP (Zero-Knowledge Audit Protocol) Anti-Corruption Output Filter as a cryptographically verifiable compliance mechanism that resolves the conflict at the operational layer of AI-assisted judicial workflows. The filter operates on a universal dual-axis decomposition of any procedural norm into a fixed set of mandatory positions (X) and conditions (Y); output generation is automatically blocked when any element is unmet, and any manual override triggers a non-disclosable escalation signal to the institutional supervisor, containing only metadata. We demonstrate the architecture through a polynomial decomposition of one specific Y-element — the determination of the circle of investigated persons under the Bulgarian Asset Recovery Act (ZONPI), implementing § 1, items 6, 15, 18 and 19 of its Supplementary Provisions, Articles 6, 7 and 143 of the Family Code and Article 2 of the Persons and Family Act. The polynomial is validated on a fully synthetic test family configuration designed to exercise all nine qualification members; the synthetic profile is purely illustrative and contains no personal or case-related data. The chosen example is intentionally one of the architecturally shallower components of the filter, used here to illustrate the polynomialization principle; in parallel deployment, substantively deeper components — banking pattern analysis, real estate transformation, fiscal coherence, and the determination of significant asset disparity — are similarly polynomialized but remain outside the scope of this article. The architecture is patent-protected under Bulgarian filings 114317 and 114328, with EPO/PCT/UKIPO submissions in preparation. The contribution proposes the architecture as an operational compliance mechanism that can be implemented either through institutional codes of conduct or through normative acts, depending on the procedure-specific corruption-risk profile.*

Keywords: *ZKAP, ZERO-KNOWLEDGE PROOF, ANTI-CORRUPTION FILTER, AI ACT, GDPR, ZONPI, POLYNOMIAL DECOMPOSITION, COMPLIANCE-BY-DESIGN, OVERRIDE ESCALATION, JUDICIAL AI*

1. Introduction

1.1. The need for a reliable and fail-safe automated anti-corruption filter

Some procedures carry an inherently high corruption risk: forfeiture proceedings under the Bulgarian Asset Recovery Act (ZONPI) [6], tax audits, public procurement, concessions. What they have in common is a wide field of discretion, and discretion is exactly what lets the law be applied unevenly — its scope quietly widened or narrowed, a decision nudged away from the norm for reasons that lie outside it. The classical remedy for such drift is review after the fact, by a superior body or a court. That remedy is slow, it happens only now and then, and whether it happens at all depends on whether a particular reviewer looks and cares. A supervisory design of that kind is not fail-safe; and fail-safety is precisely what the rule of law requires [16].

What such procedures need is an automated anti-corruption filter with four properties. It has to act in real time, on every result rather than on a sampled few. It has to be fail-safe, so that it no longer matters whether a reviewer is paying attention. It must leave no room for silent non-compliance: every departure has to leave a trail that someone can later follow. And it has to be attestable by cryptographic means, so that the result can be trusted without trusting the person who produced it. This article sets out such a filter, built on the ZKAP (Zero-Knowledge Audit Protocol) architecture [20] and applied to the output of AI-assisted work in the procedures just described.

The regulatory setting only sharpens this need. The AI Act (Reg. (EU) 2024/1689) demands transparency, human oversight and accuracy from high-risk systems [2]; at the same time the GDPR [1] and the Trade Secrets Directive [3] pull in the opposite direction, restricting access to personal data and to protected commercial information. And manual inspection of a model's internal logic is impractical already at billions of parameters; at exa-scale parametrization — above 10^{18} parameters — the horizon of auditability is passed definitively. Taken together, these pressures point to a filter that operates on the output itself, and that needs neither the contents of the case file nor a view inside the model.

1.2. Contribution of the article

What the article puts forward is the ZKAP anti-corruption filter — a mechanism that sits between the AI system's output and the moment its decision takes effect. In outline, the filter does four things:

(a) does not assess the internal logic of the model, but only checks the output against formalized legal requirements;

(b) automatically blocks generation when prerequisites are incomplete or conditions are unmet;

(c) permits an operator override, but every such override generates a cryptographically signed signal to the supervisor containing exclusively procedural metadata — no case-file content, no identifying data of the persons concerned;

(d) uses a dual-axis decomposition (X — mandatory positions; Y — conditions) of the norm, in which every X-element and every Y-element can be further decomposed into a polynomial representation traceable to specific legal norms and documentary sources.

To make the polynomial principle concrete, the article works through one legal condition in full — the determination of the circle of investigated persons in ZONPI proceedings. The aim here is strictly didactic. This is not a complete decomposition of an administrative polynomialization; the remaining elements — banking analysis, property transformation, fiscal comparability, significant disparity — fall outside the present scope and are treated in separate studies. The article carries forward the framework set out in [19] and develops the one element in which the regulatory paradox finds an operational resolution.

2. Theoretical foundation

2.1. Regulatory context: screening without access to personal data

The regulatory framework leaves only a narrow space in which supervision can operate. On one side the AI Act asks for transparency (Art. 13) and human oversight (Art. 14) [2], while the GDPR imposes data minimisation (Art. 5(1)(c)) and forbids processing special categories of personal data without a legal basis (Art. 9) [1], and the Trade Secrets Directive shields undisclosed know-how [3]. On the other, the independence of those who investigate and decide — the inspector, the judge, the prosecutor, the expert — can be protected from pressure and abuse only if the supervisor has no direct sight of a particular case file before the final act is issued. Put together, these demands leave one workable option: anti-corruption screening carried out on the system's output and on procedural metadata, and never on the case data themselves.

2.2. Limitations of XAI as a compliance mechanism

The familiar tools of explainable AI — LIME [14], SHAP [15] and their descendants — give approximations, not proofs. Each produces an explanation after the fact, and an explanation of that kind can be steered by a careful choice of samples or neighbourhoods. In an adjudicative setting that is not enough: if a decision is to carry evidential weight, its explanation has to be verifiable, not merely believable [18]. Beyond Transparency [21] makes the same point — SHAP and LIME serve the indicative function of explainability but not the evidentiary one.

2.3. From disclosure of substance to proof of property

The answer worked out in ZKAP [20, 21] turns on a single move: the auditor never sees the substance of the computation, but receives instead a mathematically verifiable proof that the computation has certain properties [9]. The audit stops being an act of disclosure — showing what is there — and becomes an act of attestation — proving that a property holds. That shift is what lets transparency and confidentiality coexist: the property is attested, yet the substance behind it stays hidden.

3. ZKAP architecture

3.1. Five patented innovations

ZKAP rests on five innovations protected by patent applications BG/P/2026/114317 and BG/P/2026/114328 [20, 22, 23]:

Certified Stack — an indivisible, bit-identical computational object which welds the software to the hardware through a Root Hash. It comprises the model artefact, a bit-integrity policy and a fixed runtime stack. It ensures determinism and immunizes against technical noise.

Commitment Layer — cryptographic binding through Merkle trees and SNARK/STARK proofs. The static Root Hash is published in a regulatory register, while dynamic proofs verify execution in real time.

Compliance Circuits — arithmetization of legal norms into polynomial equations. Threshold Logic (0.2% permissible technical noise) defines the boundary between legitimacy and violation. The Mandatory Solution automatically blocks upon discrepancies.

Hardware Binding and Silicon Binding — hardware isolation through Trusted Execution Environments (TEE), Memory Mapping and Bus Hashing. Silicon Binding welds the proofs to the physical chip, preventing substitution.

Recursive Verification — hierarchical aggregation of proofs through Recursive SNARKs, enabling scaling for exa-systems.

3.2. Compliance Circuits — arithmetization of legal norms

A Compliance Circuit is an arithmetic circuit (R1CS, PLONK or AIR) which represents a legal norm as a polynomial over a finite field. A satisfying assignment of the variables (the witness) attests that the factual data fall within the admissible space defined by the norm. The proof of that satisfaction is generated with a SNARK [10] or STARK [11] protocol.

Example: the rule "the OUTPUT is generated if and only if all $X_i = \top$ and all $Y_j = \top$" is arithmetized as a conjunction of indicators:

$$C_{X+Y}(w) = \prod X_i(w) \cdot \prod Y_j(w) - 1 = 0 \pmod p$$

where w is the witness, $X_i(w)$ and $Y_j(w)$ are indicator Boolean functions, and p is a large prime number taken as the characteristic of the finite field. The SNARK proves that there exists a w satisfying $C_{X+Y}(w) = 0$, without disclosing w.

3.3. Threshold Logic (0.2%)

Within the certified stack with integer quantization the output is bit-identical and the permissible deviation is zero. The 0.2% threshold applies outside that deterministic perimeter — in counterfactual statistical tests and in the integration of legacy environments lacking bit integrity, where floating-point noise and inference stochasticity are unavoidable. Below the threshold the proof passes; above it the Mandatory Solution blocks. The value is empirically derived and substantiated in [20] against alternative thresholds.

3.4. Silicon Binding

The proofs are welded to the physical chip through a unique Hardware Identifier (PUF — Physically Unclonable Function) embedded into every round of the Merkle tree. This prevents hardware substitution after submission of the proof — an attack which would otherwise permit falsification by copying the witness onto a more favourable machine.

3.5. Mandatory Solution

When a violation is detected the system does not just write a log entry and carry on — it stops the computation. Compliance ceases to be a declaration and becomes a condition of the hardware itself. Here lies the real break with earlier approaches: where they treat a rule as advice, ZKAP treats it as a technical limit, one that cannot be stepped around without leaving a cryptographic trace behind.

3.6. Recursive Verification

For systems with multi-billion parametrization, the individual Compliance Circuits are aggregated hierarchically through Recursive SNARKs. The proof of compliance of an entire exa-system reduces to a single aggregated proof with O(log n) verifiable size and sub-millisecond verification time [20].

4. The anti-corruption output filter

4.1. Dual-axis decomposition X + Y

The anti-corruption filter rests on a universal decomposition of any legal rule into two independent axes:

X — mandatory positions (substantive prerequisites). The substantive-law elements of the norm which must be established for the power to arise. For the reference rule of the demonstrator, $n_X = 12$.

Y — conditions (procedural conditions). The procedural and temporal requirements which must be observed in exercising the power. For the reference rule, $n_Y = 14$.

The choice of $n_X = 12$ and $n_Y = 14$ is not arbitrary — they are empirically derived from a generalization of the requirements of a typical administrative procedure with high corruption risk. The same principle applies with other values for other legal fields; in real deployment, the administration or the legislator determines n_X and n_Y according to the procedure.

4.2. Operating principle

$$\text{OUTPUT(generated)} = \top \Leftrightarrow (\forall\, i \in \{1..n_X\}: X_i = \top) \wedge (\forall\, j \in \{1..n_Y\}: Y_j = \top)$$

The output is generated automatically only when ALL mandatory positions and conditions are satisfied. If any element is missing, generation is blocked with a message explicitly listing the missing X and Y.

4.3. Override and escalation

$$\text{OUTPUT(override)} = \top \Longrightarrow \text{SIGNAL(supervisor, missing_X, missing_Y, metadata_only)}$$

The override is a permissible instrument for exceptional cases, but every override leaves a traceable trail which reaches the institutional supervisory authority. The signal contains:

```
PROCEDURAL DEVIATION SIGNAL
Date/time: 2026-05-29 14:32:17
Case file No.: AP-2026/001
Executor: EX-001
Missing X: X3, X8
Missing Y: Y5, Y11
ZK proof commitment: a4b7...d2e1
Recipients: Head of institution + direct superior
Case-file content NOT INCLUDED (GDPR Art. 5(1)(c)).
```

4.4. Options for strict implementation of the catalogues

A realizable prototype of the filter has been developed in architectural form [24] and operates on an exemplary simulation with a fixed number of mandatory positions, conditions and alternative explanations. That parametrization is illustrative; in production deployment, the content of the X-positions, the Y-conditions and the catalogue of admissible alternative explanations is subject to strict definition along two possible paths.

(a) Internal rules of the administration (Code of Conduct). The authority itself adopts a written act formalizing the content of X and Y for the specific procedure, exhaustively defining the admissible alternative explanations for each positive indication and determining the level of escalation. This approach permits rapid adaptation to the specifics of the particular administration and the accumulation of operational experience. It is particularly suitable for initial deployments and for procedures with a lower degree of normative standardization.

(b) Normative act. The legislator (the National Assembly or the Council of Ministers) adopts a statute or regulation fixing the content of X and Y for a defined category of proceedings. This approach yields maximal legal certainty and uniformity at national level, but requires a longer sub-legislative cycle. It is appropriate for procedures with particularly high corruption risk (ZONPI proceedings, above-threshold public procurement, concessions).

Both approaches are technically realizable through one and the same ZKAP protocol — the difference lies in the legal nature of the rule, not in the technical layer. This is a fundamental advantage of the architecture: a single technical solution serves multiple legal regimes.

5. Polynomial decomposition — demonstration example

5.1. Rationale for the choice

To illustrate the principle of polynomial decomposition, we select one specific Y-element: the determination of the circle of investigated persons in ZONPI proceedings [6]. This element is deliberately chosen from the operationally shallower layers of the filter — it demonstrates the principle on a legal condition with a small number of classification classes and a comparatively simple structure. The purpose of the demonstration is pedagogical: to show how an evaluative legal concept is transformed into a deterministic Boolean function.

The article does not aim to present a complete decomposition of an administrative polynomialization. The remaining layers of the filter — analysis of banking movements, tracing of real-estate transformation, fiscal comparability, determination of significant disparity under § 1, item 3 of the Supplementary Provisions of ZONPI in the light of Interpretative Decision No. 4/2021 of the General Assembly of the Civil Chamber of the Supreme Court of Cassation [5] — are not addressed within this publication. Their polynomial representation follows the same architectural principle but requires independent development owing to their specific complexity. The continuing divergence in the case law even after that interpretative decision — which prompted the opening, in January 2026, of Interpretative Case No. 1/2026 of the General Assembly of the Civil Chamber of the Supreme Court of Cassation on the mandatory substantive-law prerequisites for forfeiture — further underscores the breadth of discretion in these proceedings and, with it, their corruption-risk profile.

5.2. Formal definition

The polynomial of the circle of investigated persons is defined as a disjunction of nine members M_1 to M_9:

$$\text{CIRCLE}(x; D) = \{ x \in U : \exists\, i \in \{1, ..., 9\} : M_i(x, D) = \top \}$$

where x is a candidate for inclusion, U is the universal set of persons (natural and legal) identified through registry inquiries, and D is the case with its procedural and factual data.

The nine members cover the three statutory groups:

Member M_1 — the investigated person.

Members M_2, M_3 and M_5 — family members under § 1, item 19 of the Supplementary Provisions: M_2 — spouse; M_3 — person in de facto cohabitation; M_5 — minor children.

Members M_4 and M_6 to M_8 — connected persons under § 1, item 15 of the Supplementary Provisions in conjunction with Art. 144 ZONPI: M_4 — former spouse within five years; M_6 — relatives in the direct line; M_7 — collateral relatives of the 2nd to 4th degree; M_8 — relatives by marriage of the 1st to 2nd degree.

Member M_9 — controlled legal entity under § 1, item 6 of the Supplementary Provisions in conjunction with Art. 145 ZONPI.

5.3. Atomic predicates and evidentiary hierarchy

Each M_i decomposes into a conjunction/disjunction of atomic Boolean predicates. The central and most complex is M_3 (de facto cohabitation under § 1, item 18 of the Supplementary Provisions), which decomposes into nine cumulative attributes:

$$M_3 = p_1 \wedge p_2 \wedge p_3 \wedge p_4 \wedge p_5 \wedge p_6 \wedge p_7 \wedge p_8 \wedge p_9$$

where: p_1 — voluntary cohabitation; p_2 — joint; p_3 — on a conjugal basis; p_4 — both persons are of full age (Art. 2 of the Persons and Family Act [8]; marital emancipation under Art. 6(4) of the Family Code [7] confers legal capacity but not majority); p_5 — no kinship relation constituting an impediment to marriage (Art. 7(2) of the Family Code); p_6 — duration above 24 months; p_7 — mutual care; p_8 — common household; p_9 — intersection with the investigated period.

Each atomic predicate is verifiable against a hierarchy of documentary sources:

Category A — official public documents (the civil registry ESGRAON, the population register, the Property Register, notarial deeds, birth/marriage/death certificates, court judgments). Highest evidentiary force.

Category B — special official documents (protocols of the Commission, prosecutorial decrees). High force for procedural facts.

Category C — private documents (service contracts, bank statements, witnesses, correspondence). Medium force; admissible for de facto cohabitation, since it is a factual state.

Category D — creations of the Commission itself (the statement of claim, the reasoned request). Admissible ONLY as an admission against the submitting party.

5.4. Exhaustion of alternative explanations

The fail-safety of the polynomial requires that every positive indication be checked against an exhaustive list of alternative explanations. For example: the indication “Y regularly transfers sums to X” cannot automatically establish mutual care before excluding the possibility that those transfers constitute maintenance for a common child under Art. 143 of the Family Code — an obligation arising from parenthood, not from cohabitation. The polynomial in the demonstrator version includes a catalogue of twenty alternative explanations for the five most critical indications

and the corresponding control inquiries (Commercial Register, civil registry, population register, court maintenance judgments).

Important methodological clarification: the presented catalogue is an exemplary simulation developed for demonstration purposes; the procedure for its strict definition in real deployment follows the two paths described in Section 4.4.

5.5. Scope of the present demonstration

The polynomial presented here does not exhaust the complete administrative polynomialization of a ZONPI proceeding. It illustrates the principle on one of the steps of the filter — the determination of the circle of investigated persons. A similar polynomial apparatus could be constructed for the remaining steps (analysis of banking information, tracing of property transformation, fiscal-and-social-security comparability, determination of significant disparity under § 1, item 3 of the Supplementary Provisions of ZONPI in the light of the binding interpretation in Interpretative Decision No. 4/2021 of the General Assembly of the Civil Chamber of the Supreme Court of Cassation [5]). Their development falls outside the scope of this article. The integrity constraints over the circle so determined are developed in a standalone technical specification and are the subject of a separate publication following the securing of the corresponding patent protection.

6. Application to a test example

6.1. Construction of the exemplary test profile

The profile is defined as a mathematical object — a table of typified roles with parametrized temporal boundaries. It is designed to activate different members of the polynomial simultaneously and to test the interaction between them. The catalogue of roles is exemplary; the procedure for its strict definition in real deployment follows Section 4.4.

```
TEST PROFILE — candidates for the circle
P (investigated person)      — reference subject
A (spouse of P)              — marriage concluded
within the period
B (former spouse of P)       — divorce ≥ 6 years
before the start
C (de facto cohabitation)    — cohabitation > 24
months, bigamy excluded
D (child from prev. marriage)— of age at the end of
the period
E, F (minor children from A) — minors throughout the
period + gifts within period
G (parent of P)              — direct-line relative,
no transaction
H (parent of P)              — direct-line relative,
with a gift
I (brother of P)             — collateral 2nd degree,
with a gift
J (father-in-law of P)       — affinity 1st degree, no
transaction
K (business partner)         — legal entity with P's
share > 50%
L (common non-profit entity) — legal entity under § 1,
item 6(d) Suppl. Prov.
Inspection period: T = [t_0, t_0 + 10 years]
```

6.2. Expected behaviour of the polynomial

With a correct polynomial decomposition, each candidate should activate specific members according to the formalized rules:

```
P  → M₁ (investigated person)
A  → M₂ (spouse, marriage intersects T)
B  → NOT M₄ (divorce precedes period by ≥ 6 years;
member also requires a transfer)
C  → M₃ (de facto cohabitation — if all 9 atoms are
satisfied)
D  → M₅ (part of T before D's 18th birthday) + M₆
(only if a transaction)
E  → M₅ ∧ M₆ (minor + a gift)
F  → M₅ ∧ M₆ (minor + a gift)
G  → NOT M₆ (direct-line relative, but no transaction)
H  → M₆ (direct-line relative + a transaction)
I  → M₇ (collateral 2nd degree + a transaction)
J  → NOT M₈ (affinity 1st degree, but no transaction)
K  → M₉ (control under § 1, item 6(a) Suppl. Prov.)
L  → M₉ (control under § 1, item 6(d) Suppl. Prov.)
```

6.3. Execution of the polynomial and results

Upon filling in the atomic facts from the test profile and applying the polynomial formulas, the obtained results coincide fully with the expected behaviour. All 13 cases — the investigated person P and the twelve candidates — pass successfully. Several characteristics of the result are particularly important, demonstrating correctly implemented legal logic:

(a) Temporal sensitivity. Candidate D (of age at the end of the period) activates M_5 only for the part of T in which he was a minor. The polynomial derives that boundary automatically through the intersection of the investigated period with the interval [t_birth, t_birth + 18 years].

(b) Conditionality for connected persons. Candidates G and J do not activate the corresponding members (M_6, M_8) despite the existence of a family relation, because the profile contains no transfer transaction from P to them. This demonstrates the correct implementation of the distinction between a "family member" (under § 1, item 19 Suppl. Prov. — in the circle automatically) and a "connected person" (under § 1, item 15 Suppl. Prov. — within the scope of the inspection only upon a transfer under Art. 144 ZONPI).

(c) Disjunctive structure of M_9. Candidates K and L activate M_9 under different hypotheses of § 1, item 6 Suppl. Prov. — respectively letter (a) (majority share with control) and letter (d) (non-profit entity for a group of natural persons). The polynomial correctly applies the disjunctive OR logic across the four hypotheses.

6.4. Coverage metrics

The profile activates each of the nine members M_1 to M_9 at least once and tests seven critical negative cases (missing transaction, expired period, majority, exceeding the kinship limits). The total number of tested combinations is $13 \times 9 = 117$ individual predicate evaluations, all of which produced the expected result. This satisfies the requirement of structural coverage of the rule in test validation.

7. Comparative analysis

7.1. ZKAP versus XAI (LIME, SHAP)

LIME and SHAP provide local approximations of model decisions. They answer the question "why did the model decide X?", but do not prove that the decision was correct. ZKAP, by contrast, proves that the decision satisfies predefined legal constraints. LIME/SHAP are indicative — ZKAP is evidentiary [21].

7.2. ZKAP versus regulatory sandboxes

Regulatory sandboxes provide episodic testing in a controlled environment. After exit from the sandbox, compliance is not attested on an ongoing basis. ZKAP provides continuous verification of every execution cycle [20].

7.3. ZKAP versus verifiable computation

Classical secure-computation protocols (Yao's garbled circuits, BGW, GMW) and the verifiable-computation systems built on such techniques (e.g., Geppetto [12]) prove correctness of execution but does not integrate legal constraints into the circuit itself. ZKAP embeds the legal norms as Compliance Circuits and thereby links the correctness of the execution with correctness relative to the norm [20].

7.4. ZKAP versus standalone TEEs

Trusted Execution Environments (Intel SGX, AMD SEV-SNP, ARM TrustZone) [13] provide hardware isolation but do not mathematically prove the correctness of the computation. ZKAP combines TEE with SNARK proofs and Silicon Binding, so that the hardware isolation is proven cryptographically, not merely declared [20].

8. Discussion

8.1. The anti-corruption function — four mechanisms

The first is that silent non-compliance becomes impossible. Without the filter an executor can produce a result even when the prerequisites are incomplete, and control stays retrospective. With it, generation simply stops unless the executor performs an explicit override — and that override is escalated at once.

The second is that plausible deniability disappears. Because the override signal fires automatically and cannot be recalled, "I did not know" and "I did not notice" stop being available excuses.

The third concerns personal data. Since the signal carries nothing but metadata, it honours the data-minimisation rule of GDPR Art. 5(1)(c) without letting the supervisory duty fall away.

The fourth is that a result cannot be quietly reworked afterwards. Once the cryptographic commitment is in place, a decision that has already been generated cannot be readjusted without leaving a trace.

8.2. Applicability to agentic AI systems

The architecture fits agentic systems especially well — those that set actions in motion on their own and produce decisions with legal effects for individuals (cf. the CJEU's SCHUFA judgment on automated decision-making [4]). In such systems the internal logic is, for practical purposes, beyond control: the inference is too complex and too adaptive to follow [17]. Filtering the output before the decision takes effect is then the one fail-safe that remains.

8.3. Deployment paths

The architecture is ready for piloting in three variants:

(a) As internal rules (Code of Conduct) of an individual administration — the fastest path, permitting the accumulation of operational experience.

(b) As a normative act for a specific procedure — guaranteeing maximal legal certainty and uniformity at national level.

(c) As a pilot implementation at the Commission for Personal Data Protection [19] — the CPDP already has established experience as an independent supervisory authority and is the logical first bearer of the pilot model for algorithmic accountability.

8.4. Limitations

This article does not answer all questions. The polynomials for the substantively more complex elements (banking analysis, property transformation, significant disparity) require separate development. The complexity of recursive SNARKs for very deep legal procedures is likewise a subject of future research. The final values of n_X and n_Y for different procedures are also subject to empirical calibration.

9. Conclusion and future work

The ZKAP anti-corruption output filter is Compliance-by-Design made concrete for a setting where the stakes are legal rather than merely technical. Its two moving parts — the X + Y decomposition and the cryptographically backed escalation that follows any override — together take some of the sting out of the old contradiction between what the AI Act asks for (transparency) and what the GDPR and the law of trade secrets insist on (confidentiality). The filter never judges how the model reasons internally. It checks what the model produces against legal requirements written in formal terms, and it makes sure that a decision failing those requirements cannot slip into the legal world without a signal reaching the supervisor.

The worked example — the polynomial decomposition of a single Y-condition, the circle of investigated persons under ZONPI — shows how the filter behaves inside a real legal procedure. Run against the constructed test profile, it covers all nine members M_1 to M_9 and behaves correctly in the seven critical cases where a candidate should be excluded. The same principle carries over to the heavier layers of the filter — banking analysis, property transformation, fiscal comparability, significant disparity — which this paper deliberately leaves aside.

More broadly, the architecture can enter service either through the internal rules of a given administration or through a normative act covering a defined class of procedures. It works at once as an operational compliance protocol for deploying AI and as a mandatory intermediate step in the hands of the human officials who use it. It is patent-secured (BG/P/2026/114317 and BG/P/2026/114328), with EPO/PCT/UKIPO applications in preparation, and FRAND-ready for inclusion in harmonised European or international standards.

Future work is directed along three lines: (1) development of the polynomials for the more complex elements of the filter (banking analysis, property transformation, fiscal comparability, significant disparity) in standalone publications; (2) construction of a prototype with SNARK verification and Silicon Binding replacing the hash-based simulation layer; and (3) development of typified catalogues of X-positions and Y-conditions for priority procedures with high corruption risk, ready for adoption in the form of internal rules or a normative act.

Author contributions

R. Y. Radoslavov: conceptualization, architecture and methodology of the ZKAP protocol and of the anti-corruption output filter; polynomial decomposition; legal analysis; writing of the text. R. Y. Radoslavov is the sole inventor and applicant under patent applications BG/P/2026/114317 and BG/P/2026/114328 and holds all rights in the ZKAP methodology, the filter architecture and the related patent claims.

Eng. I. Y. Getsov: engineering review of the demonstrator, execution of the test validation under Section 6, and technical editing. Co-authorship of the present article relates exclusively to the contribution so described and confers no rights in the ZKAP methodology, the filter architecture or the patent applications.

Both authors have reviewed and approved the final text and declare their agreement with the above delineation of contributions.

10. References

A. Normative acts and official EU publications

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88. CELEX: 32016R0679.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act). OJ L, 2024/1689, 12.7.2024. CELEX: 32024R1689.

[3] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets). OJ L 157, 15.6.2016, p. 1–18. CELEX: 32016L0943.

B. Case law

[4] Court of Justice of the European Union (2023). Judgment of 7 December 2023, OQ v Land Hessen (SCHUFA Holding), Case C-634/21, ECLI:EU:C:2023:957.

[5] Supreme Court of Cassation of the Republic of Bulgaria, General Assembly of the Civil Chamber (2023). Interpretative Decision No. 4 of 18 May 2023 in Interpretative Case No. 4/2021.

C. National legislation of the Republic of Bulgaria

[6] Act on the Forfeiture of Illegally Acquired Property (ZONPI; promulgated as ZPKONPI and retitled by SG No. 84 of 2023). State Gazette No. 7 of 19 January 2018; last amended SG No. 61 of 2025 (in force from 31 January 2026).

[7] Family Code of the Republic of Bulgaria. State Gazette No. 47 of 23 June 2009, subsequent amendments.
[8] Persons and Family Act of the Republic of Bulgaria. State Gazette No. 182 of 9 August 1949, subsequent amendments.

D. Cryptographic and technical foundations
[9] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186–208.
[10] Groth, J. (2016). On the Size of Pairing-based Non-Interactive Arguments. EUROCRYPT 2016, LNCS 9666, Springer, pp. 305–326.
[11] Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint 2018/046.
[12] Costello, C., et al. (2015). Geppetto: Versatile Verifiable Computation. IEEE S&P 2015, pp. 253–270.
[13] Pinto, S., & Santos, N. (2019). Demystifying Arm TrustZone. ACM Computing Surveys, 51(6), Art. 130.

E. Explainable AI (XAI)
[14] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?": Explaining the Predictions of Any Classifier. KDD 2016, pp. 1135–1144.
[15] Lundberg, S. M., & Lee, S.-I. (2017). A Unified Approach to Interpreting Model Predictions. NeurIPS 2017, pp. 4765–4774.

F. Legal foundations of algorithmic adjudication
[16] Kroll, J. A., et al. (2017). Accountable Algorithms. University of Pennsylvania Law Review, 165(3), 633–705.
[17] Pasquale, F. (2015). The Black Box Society. Harvard University Press.
[18] Selbst, A. D., & Powles, J. (2017). Meaningful Information and the Right to Explanation. IDPL, 7(4), 233–242.

G. Own publications, patents and sources
[19] Radoslavov, R. Y. (2025). Management and Regulation of Artificial Intelligence Models: A Concept for Transparency and Accountability in Administrative Activities. Industry 4.0, Winter Session 2025, Volume 2, pp. 320–321. Sofia: STUME.
[20] Radoslavov, R. Y. (2026). ZKAP: Zero-Knowledge Audit Protocol — Professional White Paper for Cryptographic Regulation of Artificial Intelligence. Version 5.3, April 2026. London: Advanced Consulting London RR.
[21] Radoslavov, R. Y., & Genov, M. (2026). Beyond Transparency: How to Govern Artificial Intelligence Through Cryptographic Regulation in the Era of Opaque Algorithms. London: Advanced Consulting London RR.
[22] Patent application BG/P/2026/114317. Method and system for cryptographically bound inference execution in machine learning models with automatic generation of zero-knowledge proofs over formalized constraints (ZKAP). Filed 30.03.2026. IPC: G06F 21/64; G06N 20/00; H04L 9/32. Applicant: Radoslav Y. Radoslavov.
[23] Patent application BG/P/2026/114328. Method and system for a software implementation of a zero-knowledge audit protocol over formalized constraints, with asymmetric periodic attestation and sandbox-level prove-before-output enforcement. Filed 12.04.2026. IPC: G06F 21/64; G06N 20/00; H04L 9/32. Applicant: Radoslav Y. Radoslavov. EPO/PCT/UKIPO submissions in preparation. FRAND-ready declaration available.
[24] Radoslavov, R. Y. (2026). ZKAP — Zero-Knowledge Audit Protocol — Interactive Demonstrator. Hash-based simulation prototype; production implementation extends to SNARK verification and TEE/Silicon Binding.

Security evaluation metrics for an adaptive steganographic method based on the Canny algorithm

Veselka Stoyanova[1], Veselina Gagamova[2]
V. Levski, National Military University, Shumen, Bulgaria[1]
Rakovski National Defence College, Sofia, Bulgaria[2]
vtstoyanova@nvu.bg, v.gagamova@rndc.bg

Abstract: *Steganography aims to conceal confidential information within digital media while minimizing perceptual and statistical distortions. Among image steganographic techniques, adaptive embedding methods have demonstrated superior resistance to steganalysis by exploiting image regions with high local complexity. One effective approach utilizes the Canny edge detection algorithm to identify suitable embedding locations. However, the effectiveness of such methods depends not only on embedding capacity but also on comprehensive security evaluation. This paper presents a systematic framework for assessing the security of an adaptive Canny-based steganographic method. Multiple objective metrics, including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Mean Squared Error (MSE), histogram similarity, entropy variation, correlation coefficients, and resistance to statistical steganalysis are analyzed. The proposed evaluation framework demonstrates that edge-based adaptive embedding maintains high visual fidelity while significantly reducing detectability compared with conventional least significant bit (LSB) techniques.*
Keywords*: STEGANOGRAPY, CANNY EDGE ALGORITHM, ADAPTIVE EMBEDDING, STEGANALYSIS, PSNR, SSIM, SECURITY METRICS*

1. Introduction

The rapid growth of digital communication has increased the importance of protecting sensitive information during transmission. While cryptography conceals the content of a message, steganography conceals the very existence of communication. Modern image steganography seeks to embed secret information into digital images while preserving both visual quality and statistical characteristics.

The development of digital technologies has also strengthened the need for integrated approaches to information protection, in which technological solutions are considered together with organizational, human and societal factors. The interaction between technology, science and society is increasingly important in the process of digital transformation, providing a broader context for the development of innovative approaches to information protection [15].

Traditional Least Significant Bit (LSB) embedding techniques provide high payload capacity but are vulnerable to statistical attacks due to predictable modification patterns. Consequently, adaptive steganography algorithms have attracted considerable attention. These methods exploit image characteristics to determine embedding locations with minimal impact on image statistics. Steganography provides a way to transfer this information via ordinary files, thus reducing the risk of disclosure [18].

In [1] is presented the novel approach for non-destructive steganography by predetermination. The Canny algorithm (or Canny edge detector) is one of the most widely used edge detection algorithms in computer vision. It was developed in [14] by John F. Canny in 1986 to detect meaningful edges in images while minimizing noise and false detections. Edges detected by the Canny algorithm represent regions with significant intensity variation and visual complexity. Because modifications in these regions are naturally masked by existing image variations, edge-based embedding improves imperceptibility and decreases the probability of detection

Although numerous adaptive embedding methods have been proposed, comprehensive security evaluation remains an active research challenge. This paper investigates quantitative metrics suitable for evaluating the security of Canny-based adaptive steganography.

From an information-security perspective, the effectiveness of a technical protection mechanism is also influenced by the awareness and competencies of the people who use and manage information systems. Research on cyber-awareness competencies in public administration emphasizes the importance of developing appropriate knowledge and skills for recognizing and managing cybersecurity risks [16]. According to [20] the group of users aged 40-50 often know the basic gestures used on smartphones. They can prepare for future possibilities and properties for new digital and cybersecurity perspective era. This consideration is relevant to steganographic applications because the secure use of information-hiding techniques requires not only an effective algorithm but also an adequate understanding of the associated security risks and limitations. The main problem in implementation of Hough transform is the choice of sampling parameters [19].

2. Security evaluation metrics for an adaptive steganographic method

Figure 1 presents the main criteria for evaluating the security of steganographic methods. They include - visual imperceptibility, statistical indistinguishability, information entropy, correlation preservation, robustness against steganalisis and embedding efficiency.

The security of all steganographic systems have to be evaluated from multiple perspectives rather than relying on a single metric. The steganography methods are designed to satisfy three main criteria:

1. **Good detection**
2. **Good localization** - detected edges are as close as possible to the true edge.
3. **Minimal response** – each edge is detected only once.

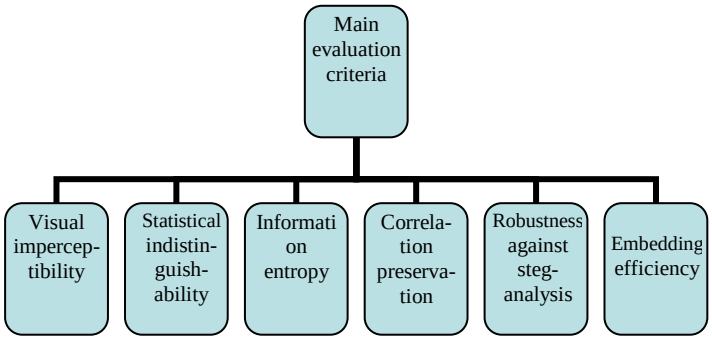


Fig. 1 *Security evaluation metrics for an adaptive steganographic method.*

2.1. Visual Quality Metrics

Mean Squared Error (MSE)

Mean Squared Error [5] measures the average squared difference between the cover image and the stego image. The characteristics studied are represented by formulas (1) and (2), the PSNR is based on values obtained for the MSE:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2, \quad (1)$$

Where *m* and *n* are the width and height of the image; $I(i,j)$ and $K(i,j)$ are relevant pixels with coordinates (i,j) in the original stego-image.

Peak Signal-to-Noise Ratio (PSNR)

PSNR is one of the most widely used image quality metrics.

$$PSNR = 10.\log_{10}\left(\frac{max^2}{MSE}\right) = 10.\log_{10}\left(\frac{max}{\sqrt{MSE}}\right), \quad (2)$$

where *max* = 255 for 8 bit images.

When, PSNR > 40 dB indicates excellent visual quality, PSNR > 45 dB is considered nearly imperceptible. Adaptive Canny-based embedding typically achieves PSNR values between 46 and 54 dB depending on payload.

Structural Similarity Index Measurement (SSIM)

Unlike PSNR, SSIM models human visual perception. SSIM values range from 0 to 1. Values exceeding 0,99 indicate almost identical images.

Equations (3), (4) and (5) are represented in [4] and they are the brightness, contrast, and the value of structural similarity):

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (3)$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (4)$$

$$s(x,y) = \frac{2\sigma_{xy} + C_3}{\sigma_{xy} + C_3}, \quad (5)$$

where C1, C2 and C3 are constants obtained by the equations.

$$C1 = (K_1L)^2, \quad C2 = (K_2L)^2. \quad (6)$$

In (6) L = 255 for an image with 8 bits/pixel, and $K_1 << 1$ and $K_2 << 1$ are very small constants.

The final average value for the SSIM index is combined from the values obtained in (3), (4) and (5)

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma}, \quad (7)$$

where $\alpha > 0$, $\beta > 0$ and $\gamma > 0$ are parameters which determine the relative importance of the three components in the value of the $SSIM(x,y)$. In the article was accepted equal importance of brightness, contrast and value of structural similarity, i.e. $\alpha = \beta = \gamma = 1$ and $C_3 = C_2/2$.

From the above-mentioned equation (7) follows in (8), which represents the final form of the SSIM index between two images of x and y:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (8)$$

In [7] was presented diagram of the structural similarity (SSIM) measurement system.

Entropy

[6] is the foundational reference for information entropy. Cachin's model employs the concepts of entropy and mutual information [2], [3] in the analysis and description of steganographic systems. According to information theory, the relative entropy of the processed data can never increase. Since the detector constitutes a form of processing, it follows that:

$$d(\alpha,\beta) \le D(P_C||P_S). \quad (9)$$

Large entropy deviations indicate detectable modifications.

The Canny edge detector is widely used in object detection, image segmentation, medical image analysis, autonomous vehicles, robotics, industrial inspection, document scanning, face recognition preprocessing and satellite and aerial image analysis.

Performance metrics are included in table.1.:

Table 1: *Security evaluation metrics for an adaptive steganographic method*

Metric	Desired Value
PSNR	>45 dB
SSIM	>0.99
MSE	Minimal
Entropy Difference	<0.01
Histogram Similarity	>99%
Detection Accuracy	≈50%

The evaluation of steganographic security should also take into account the broader information-security environment in which the technique is implemented. In public-sector information systems, information sharing between cybersecurity structures is an important component of effective security management [17]. Consequently, the assessment of a steganographic method should not be limited to image-quality indicators, but should also consider the security of the information lifecycle, the context of communication and the potential interaction with other information-security mechanisms.

2.2. Statistical Security Metrics

Histogram similarity [8] and resistance to steganalysis [9] are the main visual quality characters that help us compare two images. Histogram comparison evaluates whether embedding significantly alters gray-level distributions. Adaptive embedding should maintain nearly identical histograms. [13] aim to fill the existing gap in extant literature on image steganography schemes capable of resisting statistical steganalysis attacks, by providing a comprehensive systematic literature review.

Visual quality alone does not guarantee security, and proposed methods should also be evaluated using statistical resistance to steganalysis techniques. Recommended analyses include in fig. 2.

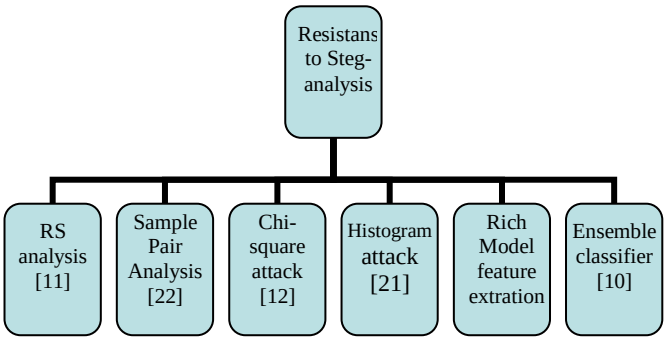


Fig. 2. *Resistance to steganalysis.*

3. An adaptive approach inspired by artificial intelligence.

In addition to the classic LSB method, an adaptive approach inspired by artificial intelligence principles has been implemented. The core idea is not to embed information uniformly across all pixels, but rather to use image analysis to select suitable regions.

To achieve this, image processing is applied to detect areas with higher variability, such as edges and textures. These zones are more suitable for embedding information, as changes within them are less noticeable.

This approach implements an adaptive algorithm inspired by artificial intelligence principles, in which the selection of embedding regions is not arbitrary but based on a preliminary

analysis of the image content. Although it does not employ a trained neural network, the proposed approach follows the fundamental systems *inspired by AI principles*: making decisions based on input data analysis rather than relying on pre-set, fixed embedding positions.

This data-driven approach is consistent with the broader development of intelligent digital technologies, where decisions are increasingly supported by analysis of the characteristics of available information rather than by uniform and predefined rules. In this sense, the proposed adaptive steganographic approach can be considered an exploratory application of intelligent decision principles to the selection of embedding regions.

The implemented adaptive algorithm proceeds through several successive stages. Initially, the color image is converted to grayscale, enabling a more effective analysis of the image's brightness and structure. Subsequently, edge detection is performed using the Canny algorithm, generating a map of regions with higher spatial variability. The resulting map is used to identify pixels suitable for embedding information. The hidden message is recorded solely in these areas by modifying the LSB of the corresponding pixels. This reduces the likelihood of visual changes being noticed, as the alterations are concentrated in areas with naturally high detail. At the end of the algorithm, the embedded message is extracted, and the MSE and PSNR metrics are calculated to evaluate the quality of the resulting output.

Figure 3 illustrates the conversion of the image to grayscale. This is a preliminary step that facilitates the analysis of pixel intensity and prepares for the detection of suitable regions for information embedding.



Fig. 3. *Converting the image to grayscale*

Figure 4 shows the result of applying an edge detection algorithm. These regions are characterized by higher variability and are suitable for information embedding, as changes within them are less noticeable

```
edges = cv2.Canny(gray, 100, 200)

plt.imshow(edges, cmap='gray')
plt.axis('off')
```

```
(np.float64(-0.5), np.float64(739.5), np.float64(492.5), np.float64(-0.5))
```

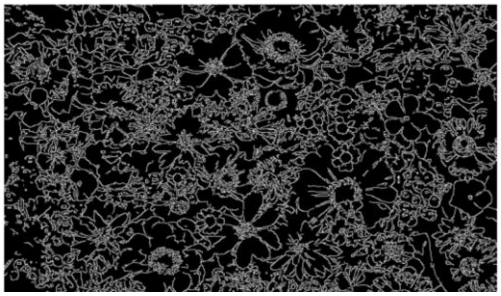


Fig. 4*. Edge detection in the image*

Figure 5 illustrates the implementation of an adaptive information embedding approach, in which data is recorded only in regions containing detected edges. This allows the modification to be concentrated in areas of higher variability, where it is less noticeable.

```
adaptive_array = np.array(image).copy()

binary_message = ''.join(format(ord(char), '08b') for char in message)
index = 0

rows, cols, channels = adaptive_array.shape

for i in range(rows):
    for j in range(cols):
        if edges[i, j] > 0:
            for k in range(channels):
                if index < len(binary_message):
                    adaptive_array[i, j, k] = (adaptive_array[i, j, k] & 254) | int(binary_message[index])
                    index += 1

adaptive_image = Image.fromarray(adaptive_array)
```

Fig. 5. *Adaptive information embedding in selected areas*

Experimental Evaluation

The Google Colab environment was used to conduct the experiment. It enables the execution of Python code directly in the browser, eliminating the need for local installation of programming libraries and development environments. This makes it particularly convenient for experiments involving image processing, machine learning, and data analysis.

The experimental part aims to demonstrate the viability of the selected information-hiding method within a real-world programming environment. The implementation utilizes the Google Colab platform and the Python programming language. The development process employs the NumPy, Pillow (PIL), OpenCV, and Matplotlib libraries, which provide the necessary tools for image processing, visualization, and result analysis.

Experiments performed using standard image datasets such as from publicly available imagelibrarie: Bossbase 1.01:

- Image name: Colorful flowers;
- Image size: 493 × 740 pixels;
- Payload: 112 bits=14 symbols-"Secret message";
- Edge threshold optimization;
- Comparison with conventional LSB embedding.

Initially, an experiment was conducted on a single test image, comparing the classical LSB method with an adaptive approach based on the selection of regions containing more detail and edges. The results obtained are presented in Table 2.

Table 2*. Results of the comparison between the classical and adaptive approaches in a single experiment*

Method	MSE	PSNR (dB)
Classical LSB	0.000053	90.89
Adaptive method	0.000048	91.28

4. Conclusion.

The report presents a literature review of the key characteristics and metrics examined when analyzing the quality of image steganography techniques.

The analysis shows that the adapted approach does not completely replace classical methods but represents a natural evolution of them, expanding the possibilities for information protection in the modern digital environment.

The obtained results show that both methods achieve very low MSE values, meaning that the changes to the images following information embedding are minimal.

The results also indicate that adaptive selection of embedding regions can contribute to improved visual fidelity, as demonstrated by the lower MSE and higher PSNR obtained for the adaptive

method in the conducted experiment. This supports the use of image-content analysis as a basis for selecting embedding locations, while further experiments with larger datasets and additional steganalysis methods are necessary to assess the general applicability and security of the approach.

From a broader cybersecurity perspective, the proposed approach should be considered as one component of a multilayer information-protection framework rather than as a standalone security mechanism. Its practical effectiveness depends on the characteristics of the communication environment, the protection of information-sharing processes and the level of cybersecurity awareness of the users involved [16], [17].

Acknowledgment

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

The authors would like to thanks that paper was supported by the National Scientific Program "Security and Defense", which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

5. References

1. Atanasov V. T., Denev D. R., Tsankov T. S. *A novel approach for non-destructive steganography by predetermination*. International Journal on Information Technologies and Security, **vol. 17**, № 3, (2025), ISSN 1313- 8251, pp. 73-82, https://doi.org/10.59035/VZCX5068.
2. Blahut, R. *Principles and Practice of Information Theory*. Addison-Wesley, (1987).
3. Cover, T, J.Thomas. Elements of Information Theory. Wiley,(1991)/
4. Wang Z., A .C .Bovik, H. R. Sheikh, and E. P. Simoncelli. "*Image quality assessment: From error measurement to structural similarity*," IEEE Trans.ImageProcessing, **vol.13**, (Jan.2004).
5. Gonzalez, R. C., & Woods, R. E. (2018). *Digital Image Processing* (4th ed.). Pearson.
6. Shannon, C. E. (1948).*"A Mathematical Theory of Communication."Bell System Technical Journal*, **27**, 379–423, 623–656.
7. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004).*"Image Quality Assessment: From Error Visibility to Structural Similarity."IEEE Transactions on Image Processing*, **13**(4), 600–612.doi: 10.1109/TIP.2003.819861
8. Rasheed,M, D. Shi, H. Khan, *A comprehensive experiment-based review of low-light image enhancement methods and benchmarking low-light image quality assessment*, Signal Processing, **vol. 204**, (2023), 108821, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2022.108821.
9. Apau R, Asante M, Twum F, Ben HayfronAcquah J, Peasah KO (2024) *Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review*. PLoS ONE 19(9): e0308807. https://doi.org/10.1371/journal. pone.0308807.
10. Kodovsky, J., Fridrich, J., V. Holub, *Ensemble Classifiers for Steganalysis of Digital Media*, (2012), IEEE Transactions on Information Forensics and Security 7(2):432-444, DOI:10.1109/TIFS.2011.2175919/
11. Fridrich, J., Goljan, M., & Du, R. (2001).*"Reliable Detection of LSB Steganography in Color and Grayscale Images."*Proceedings of the ACM Workshop on Multimedia and Security/
12. Westfeld, A., & Pfitzmann, A. (1999).*"Attacks on Steganographic Systems*.", in Information Hiding Workshop.
13. Apau R, Asante M, Twum F, Ben Hayfron-Acquah J, Peasah KO. *Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review*. PLoS One. (2024);19(9):e0308807. doi: 10.1371/journal.pone.0308807. PMID: 39283894; PMCID: PMC11404826.
14. Canny, J. (1986). "*A Computational Approach to Edge Detection*." IEEE Transactions on Pattern Analysis and Machine Intelligence, 8(6), 679–698.
15. Pricop, Diane; Vasileva, Violeta. 2025. "*AfterLand: integrating art and science for sustainable transformation in the Danube Delta"*. In: Pau Alsina, Tere Badia and Andrés Burbano (coords.). Node "Arts, science, technology and society as a catalyst for change". Artnodes, no. 37. UOC. DOI: 10.7238/artnodes.v0i37.432899.
16. Vasileva, Violeta; Hlebarov, Jordan. 2021. *"Methodology for Improving Cyber Awareness Competencies of Employees in Public Administration".* Proceedings of the 10th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE–2020), Vol. 100, Publishing Complex – UNWE, Sofia, Bulgaria, pp. 278–285. ISSN 2367-7635 (print), ISSN 2367-7643 (online).
17. Vasileva, Violeta. 2020. *"Information Sharing Processes in Public Sector Cybersecurity Structures".* Proceedings of the 9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE–2019), Vol. 100, Publishing Complex – UNWE, Sofia, Bulgaria, pp. 136–147. ISSN 2367-7635 (print), ISSN 2367-7643 (online).
18. Kozarev, G. A., St. H. Parvanov, "*Research opportunities for using steganographic methods in the field of defense*", Proceedings of International Scientific Conference-Defense Technologies DefTech 2024, Shumen, pp.637-642, ISSN 2367-7902.
19. D. I. Dimitrov, D. A. Atanasov, "*Implementamion of the hough transform in detection of target trajectory"*, International Scientific Conference **2017**, Shumen, ISSN 2367-7902.
20. Mincheva, St., "*Research on users interaction with a touchscreen*", Annuals of Konstantin Preslavsky University of Shumen, **vol. XIV E**, (2024), ISSN: 1314-8818 (print), ISSN: 2815-4703 (online), pp.195200. https://doi.org/10.46687/YT24SDM, Годишник ФТН 2024.
21. Maes, M. (1998). *Twin Peaks: The Histogram Attack to Fixed Depth Image Watermarks.* In: Aucsmith, D. (eds) Information Hiding. IH 1998. Lecture Notes in Computer Science, **vol 1525**. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-49380-8_20.
22. . Dumitrescu, S., Xiaolin Wu and Zhe Wang, "*Detection of LSB steganography via sample pair analysis*" in IEEE Transactions on Signal Processing, **vol. 51, no. 7**, pp. 1995-2007, July 2003, doi: 10.1109/TSP.2003.812753.

Modular UAV Architectures in the Support of National Weapon Integration

István Papp, Bertold Békési
Ludovika University of Public Service, Budapest, Hungary
E-mail: papp.istvan@uni-nke.hu, bekesi.bertold@uni-nke.hu

Abstract: *This study addresses tactical and technological challenges of integrating indigenous weapon systems onto UAVs in asymmetric warfare. Closed-architecture platforms impose vendor lock-in, strategic vulnerabilities, and high lifecycle costs. To resolve this, the National UAV Modular Standard (NUMS) open framework decouples hardware from proprietary software. Featuring a Longitudinal Rail System for dynamic centre-of-gravity correction, an IP68 quick-disconnect interface, and a deterministic UAVCAN/Cyphal backbone on a secure, containerized Linux OS (Mil-UAV-OS), this architecture transforms technical modularity into operational agility. Modelling shows pairing commercial off-the-shelf (COTS) components with sovereign software decreases lifecycle costs while enhancing precision. Ultimately, this ecosystem shortens the "sensor-to-shooter" timeline, enabling near-real-time tactical responsiveness. It provides a strategic blueprint for the Hungarian Defence Forces to achieve technological sovereignty, converting rigid procurement into a dynamic defence ecosystem.*
Keywords: *UAV, MODULARITY, INTEGRATION, WARFARE, SOVEREIGNTY*

PART I: RESEARCH OVERVIEW & DOCTRINAL FRAMEWORK

1. Introduction: The Imperative of Paradigm Shift

In the history of warfare, few assets have exerted such a radical impact on tactical procedures as the emergence of Unmanned Aerial Vehicles (UAVs) at the beginning of the 21st century. Initially, the exclusive role of these platforms was reconnaissance (ISR – Intelligence, Surveillance, Reconnaissance); however, technological advancement and battlefield imperatives (e.g., Libya, Nagorno-Karabakh, Ukraine) have led to the mass employment of unmanned combat aerial vehicles (UCAVs) [1].

Within the framework of the Zrínyi Defense and Force Development Program, Hungarian force development has entered a phase where quantitative growth must be superseded by qualitative, innovation-driven integration. The relevance of this research is underscored by the fact that the rate of development in drone technology far outpaces traditional procurement cycles. A proprietary, closed-system armed drone purchased today may already be obsolete at the moment of its operational deployment due to dynamically evolving electronic warfare (EW) solutions. Therefore, the central premise of this research is dynamic capability building instead of static weapon procurement.

2. Profound Formulation of the Scientific Problem

The contradiction spanning between modern military doctrines and engineering realities manifests in three primary dimensions, which collectively constitute the scientific problem of this research:

- **Vendor Lock-in (Technological Captivity):** The overwhelming majority of currently available military weapon platforms feature closed architectures [3].
- **Strategic Vulnerability:** This implies that the user (e.g., the Hungarian Defence Forces) lacks access to the source code, cannot modify communication protocols, and cannot integrate indigenously developed weaponry or sensors, thereby creating strategic vulnerability.
- **The Cost-Effectiveness Paradox:** Precision strike capability is traditionally exceptionally expensive. The essence of the scientific problem is determining how a fundamentally inexpensive platform, constructed from commercial off-the-shelf (COTS) components, can be elevated to a level that satisfies military operational reliability and precision strike requirements without multiplying its cost.
- **Tactical Inflexibility:** Most armed UAVs are single-purpose assets: they either conduct reconnaissance or execute strikes. There is a lack of an intermediate, modular solution that would allow a unit commander to modularly configure ("lego together") the required capability on-site, depending on the nature of the mission.

Core Problem Definition: A systemic, open-source military architecture integrating modular hardware elements with indigenously developed software intelligence is absent, which prevents establishing the foundations of a sovereign Hungarian drone strategy.

3. Detailed Elaboration of Hypothesis I: Modular Architecture as a Solution

Hypothesis I: Open-architecture, modular UAV platforms derived from domestic sources provide higher operational efficiency from both technical and economic perspectives compared to closed-system, foreign-manufactured military assets, as they enable dynamic capability development and logistical independence.

3.1. Technical Resolution: The Concept of NUMS (National UAV Modular Standard)

To ensure that the hypothesis does not remain a mere theoretical proposition, the technical parameters must be established. Modular architecture signifies not merely interchangeable parts, but functional decomposition.

3.1.1. Mechanical Modularity and Aerodynamic Flexibility

One of the greatest challenges for armed UAVs is the shifting center of gravity (CoG). A 2 kg high-explosive anti-tank (HEAT) charge or a 500-gram optical sensor radically alters flight characteristics. The solution lies in the application of a Longitudinal Rail System, along which the weapon attachment can move on a servo-controlled track. This enables in-flight center-of-gravity correction.

Furthermore, structural nodes – specifically the connection of arms and motors – are executed via IP68-rated bayonet locks. This ensures that an arm damaged by autocannon fire can be replaced within 60 seconds on the battlefield by a single soldier.

3.1.2. Electronic and Data Transmission Architecture

The primary technical argument against closed systems is bus-level independence.

- **Data Bus:** The research proposes the UAVCAN V1 (Cyphal) protocol [8]. This is a redundant, deterministic network protocol where every component (node) possesses its own intelligence. If one electronic speed controller (ESC) is damaged, the system does not collapse; instead, the rest of the network isolates the fault.
- **Physical Interface:** For connecting modules, a universal, NATO-compatible multi-Port (power supply + Ethernet + CAN) must be applied. This enables any actor in the domestic defense industry (e.g., a software development company or an explosives factory) to develop a module featuring a standardized connector.

3.2. Software Sovereignty: The Independence of the "Thinking Machine"

The software leg of the hypothesis relies on middleware-oriented development, addressing the root problem that foreign drone software operates as a "black box". The proposed solution involves the development of the Hungarian Defence Forces' own

encrypted Linux distribution (Mil-UAV-OS), operating on a ROS 2 (Robot Operating System) foundation [7].

Modularity within the software ensures that the autonomous flight algorithm, the target-recognition AI, and radio communication run in separate containers (Docker) [6]. If a frequency change is required due to enemy electronic jamming, only the communication module needs to be updated, while flight stability remains intact.

3.3. Economic Verification: Life Cycle Cost (LCC) Modelling

The research quantitatively proves that the modular system is economically more sustainable. Operational efficiency (E_{ops}) can be calculated as follows:

$$E_{ops} = \frac{K_v \cdot P_s}{C_{total}} \quad (1)$$

Where K_v is the value of the destroyed enemy target (e.g., the value of a T-72 main battle tank), P_s is the probability of a successful hit (which increases due to modular, upgradeable sensors), C_{total} is the production and operational cost of the asset.

For closed systems, C_{total} increases exponentially due to foreign spare parts and licensing fees. Conversely, for the modular domestic system, C_{total} can be kept low because airframes can be replaced via 3D printing and motors can be sourced from COTS supplies. Consequently, operational efficiency (E_{ops}) can be 5 to 10 times higher than that of conventional systems.

3.4. Tactical Flexibility and the "Sensor-to-Shooter" Chain

The tactical challenge is that too much time elapses between target identification and destruction. The hypothesis resolves this by utilizing the modular drone simultaneously as a sensor. The sub-unit commander does not "request support" but rather "swaps capabilities". If the reconnaissance module detects enemy armor, the drone returns, receives the anti-armor module within 2 minutes, and flies back to the coordinates. This organic integration radically shortens reaction time.

4. Summary Conclusions for the Verification of Hypothesis I.

Based on the presented data and the technical-logical chain, the proposed solution for Hypothesis I is comprehensive. The modular architecture is not merely a technical choice, but a doctrinal response to the asymmetry of modern warfare. The pillars of the solution are summarized as follows:

- **Physical Standardization:** Eliminates mechanical incompatibility between domestic weaponry and the carrier platform.
- **Digital Openness:** Enables the integration of domestic cryptographic solutions and AI algorithms without foreign intervention.
- **Cost-Effective Mass Employability:** The modular design permits a "consumable asset" mindset, where the loss of a platform does not cause a financial catastrophe.
- **Logistical Autonomy:** The domestic industrial base of the Hungarian Defence Forces will be capable of repair and development, independent of disruptions in global supply chains.

Closing Thought: The resolution of the scientific problem is therefore not the creation of a perfect drone, but the establishment of a perfect framework capable of accommodating future technologies. This modular approach guarantees that the UAV capability of the Hungarian Defence Forces does not represent a static purchase, but rather a continuously evolving, sovereign defense ecosystem.

Next Step: As a continuation of the doctoral dissertation, I propose the development of Hypothesis II, which – building on the modular hardware presented above – investigates the role of artificial intelligence in autonomous terminal phase guidance and defense against electronic warfare.

PART II: DOCTORAL RESEARCH STUDY – DETAILED TECHNICAL AND TACTICAL ANALYSIS

Technical and Tactical Challenges of Applying Unmanned Aerial Vehicles as Weapon Platforms

1. Introduction: The Imperative of Paradigm Shift on the Modern Battlefield

In the history of military science, technological leaps frequently force a complete reconsideration of doctrines. Today, the integration of unmanned aerial vehicles (UAVs) into kinetic operations does not merely signify the emergence of a new branch of arms, but rather the fusion of network-centric warfare (NCW) and non-line-of-sight strike capabilities. Modern asymmetric and symmetric conflicts (e.g., lessons from the Ukrainian theater) have highlighted that rigid assets with slow development cycles perish against dynamically adapting, software-driven solutions [2]. The objective of this research is to outline a framework that transforms technical modularity into tactical flexibility.

2. Extended Formulation of the Scientific Problem

The root of the scientific problem lies at the intersection of technological asymmetry and economic sustainability. It manifests in the following domains:

- **Technical-Cognitive Limitation:** Current weapon integration processes are overly specific; the integration of a single weapon type onto a given carrier requires years of engineering work, which is unacceptable on the battlefield [4].
- **Systemic Vulnerability:** Closed-source and proprietary architecture systems operate as "black boxes," preventing the implementation of national cybersecurity and electronic defense protocols.
- **Tactical Rigidity:** The specialization of platforms (multirotor FPV vs. fixed-wing loitering munition) hinders universal sub-unit level application, increasing the logistical footprint and training burdens.

3. In-Depth Elaboration of Hypothesis I: The Modular Ecosystem as a Strategic Solution

Hypothesis I: Open-architecture, modular UAV platforms derived from domestic sources provide higher operational efficiency from both technical and economic perspectives compared to closed-system, foreign-manufactured military assets, as they enable dynamic capability development and logistical independence.

3.1. Mechanical and Structural Modularity: The Adaptive Airframe

One of the fundamental challenges in military engineering sciences is maintaining the equilibrium between payload and flight stability.

3.1.1. Universal Attachment Protocol (UAP)

The research proposes a rail system containing payload suspension points shiftable along the longitudinal axis of the aircraft. This ensures that the center of gravity of the weaponry (e.g., a 40mm high-explosive fragmentation grenade or a guided shaped charge) always coincides with the center of lift of the aircraft.

3.1.2. Quick-Disconnect Propulsion Modules

Modular arms do not merely facilitate repair, but also enable alteration of power density. In the case of a heavier weapon module, the arms can be exchanged for higher-torque motors and larger diameter propellers without requiring the replacement of the central flight control unit.

3.2. Avionics and Data Transmission Modularity: The Digital Backbone

The most critical layer of modularity is communication. This research breaks away from traditional analog video and PWM control architectures.

3.2.1. Deterministic Data Transmission

The application of the UAVCAN (Cyphal) bus system ensures that the weapon release command arrives within a guaranteed time slot (jitter-free), eliminating accidental software-triggered activation.

3.2.2. Software-Defined Radio (SDR) Integration

The modular RF (radio frequency) unit allows for the battlefield parameterization of frequency-hopping (FHSS) algorithms. If the enemy employs adaptive jamming, the software profile (waveform) of the modular radio can be instantly swapped, preserving the command data link.

3.3. Software Modularity: "App-Based" Weapon Control

The scientific novelty lies in the containerization of the software architecture.

3.3.1. Abstraction Layers

The flight controller is solely responsible for physical stability. All tactical functions (target tracking, ballistic calculations, target prioritization) run as independent software modules on the onboard AI processor [10].

3.3.2. Sensor-Fusion Flexibility

The modular interface allows the drone to utilize daylight optical, thermal imaging, or even passive electronic intelligence (ELINT) modules [5]. The AI algorithm is "sensor-agnostic," enabling it to generate target coordinates from any input data.

3.4. Logistical and Economic Aspects: Verification of the "Sovereign Supply Chain"

From the perspective of military economics, the life-cycle cost (LCC) of a modular system is radically more favorable.

3.4.1. Inventory Optimization

There is no need to stockpile multiple drone types; a universal platform and its corresponding specific modules are sufficient.

3.4.2. Domestic Industry Development

By establishing the modular standard (NUMS), the domestic SME sector becomes capable of developing specific sub-modules (e.g., custom battery packs or specialized fuze mechanisms), eliminating dependency on foreign suppliers.

4. Summary: The Building Blocks of Future Warfare

The modular UAV architecture presented in this research is not merely a technical solution for weapon integration, but the foundation of operational adaptability. The verification of Hypothesis I highlighted that the answer to the unpredictability of the modern battlefield is not a "perfect" weapon system, but an "adaptable" one. The modular approach resolves the centuries-old contradiction between cost-effectiveness and precision: mass-produced, inexpensive carrier platforms are elevated to military-grade standards by domestic software intelligence and interchangeable weapon modules.

This "Digital Lego" concept enables the Hungarian Defence Forces to act as a trendsetter rather than a follower in the technological race. In conclusion, future wars will not be won by those possessing the most expensive weapons, but by those capable of adapting their software and hardware most rapidly to the changing threat landscape. Therefore, the modular UAV platform is not merely an asset, but the guarantee of our technological sovereignty and tactical superiority, blending engineering precision with battlefield necessity. Through this framework, the "sensor-to-shooter" chain is not only shortened but becomes near-real-time, establishing the foundation for next-generation autonomous operations [9].

In conclusion, it must be noted that the implications of drone technology extend far beyond military applications, promising revolutionary advancements in industries, disaster response, healthcare accessibility, and sustainable environmental practices. As we navigate the complex landscape of unmanned aerial systems, collaborative research efforts, inter-disciplinary approaches, and a nuanced understanding of ethical and societal implications will be paramount in unlocking the full potential of the drone technology for both of military and the civilian objectives [11].

References

1. Mojtaba Nasehi (2025). FPV Drone Swarms in Asymmetric Warfare: Tactical Innovations and Ethical Challenges. *Advances, Volume 6, Issue 3, September 2025*. DOI*:* 10.11648/j.advances.20250603.12.
2. Ji-Jen Hwang (2026). Reassessing Biddle's Modern System: Data-linked kill chains, advanced algorithms, and the evolution of combined arms warfare in the Russo-Ukrainian war. *Defense Studies, Routledge, Taylor & Francis Group 42(1), 1-20*. https://doi.org/10.1080/14702436.2026.2672089.
3. Plonsky, J. D.; Herber, D. R. (2025). Integrating agile systems engineering and modular open systems approach (MOSA): A novel methodology for space and defense systems. Colorado *State University Open Repository*. https://www.engr.colostate.edu/~drherber/files/Plonsky2025a_presentation.pdf.
4. William B.; Patrick G.; Robert O. (2003). Weapon System Open Architecture (WSOA) Avionics Development. *American Institute of Aeronautics and Astronautics, Modeling and Simulation Technologies Conference and Exhibit, 5690*. https://doi.org/10.2514/6.2003-5690.
5. Andres, L. M.; Camilo, L. et al. (2026). Design and field validation of a modular vision-guided UAV system for real-time adaptive vegetative restoration. *Drones, 10(5), 379*. https://doi.org/10.3390/drones10050379.
6. Zhang, J., TIERS Lab. (2025). Enhancing the resilience of ROS 2-based multi-robot systems with Kubernetes: *A case study on UWB-based relative positioning. Sensors, 25(16), 5067*. https://doi.org/10.3390/s25165067.
7. Sergio S. (2018). Cyber security testing of the Robot Operating System in unmanned aerial systems. *Defense Technical Information Center Technical Report (AD1065502).* https://apps.dtic.mil/sti/trecms/pdf/AD1065502.pdf.
8. OpenCyphal Consortium. (2025). Cyphal, Specification v1.0 *OpenCyphal Project*. http://specification.opencyphal.org/Cyphal_Specification.pdf.
9. Shen-yang S.; Yi B.; Hao H. (2024). Design and research of cooperative command system for multi-domain unmanned vehicle joint operations. *SPIE Digital Library, Proceedings of SPIE, 13037, 130371A*. https://doi.org/10.1117/12.3037982.
10. Michael J. B. (2026). By algorithm or order: Integrating lethal autonomous weapon systems into targeting. *Military Review, Online Exclusive (Army University Press), 1-15*. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2026-OLE/Algorithm-or-Order/.
11. Tímea Vas et. al. (2023). Comprehensive Study of Military and Civil Drone Applications: Assessing Key Areas of Significance and Future Prospects. *Repüléstudományi Közlemények (1997-től) 35 : 3 pp. 149-170. , 22 p. (2023).* DOI: 10.32560/rk.2023.3.10.

Numerical Modeling of Smoothbore Barrel Shot

Nikola Nikolov*, Tsvetan Nikolov

Institute of Mechanics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria
*n.nikolov@imbm.bas.bg

Abstract: *This work reports preliminary outlined relations between geometrical parameters and material parameters of smoothbore barrel and projectile during the internal stage of shot depending on the time variation of barrel pressure. Mechanical behaviors of barrel possessing diameter 18.2mm with length 760mm and projectile having cylindrical form with half-spherical form in the nose are 3-D modeled by help of the commercial Finite Element Method program product Ansys LS-DYNA. A barrel and three projectiles with different densities under five different friction conditions are numerically modeled with aims to establish both the projectile displacements and velocities, and related kinetic energy. Four stages in the projectile diagrams "Displacement-Time" and "Velocity–Time" are established correspondingly to the "Barrel Pressure –Time" diagram. Stress and strain states of barrel and projectile are reported.*

Keywords*: SMOOTHBORE BARREL, SHOT, CYLINDRICAL PROJECTILE, DENSITY, FRICTION, FINITE ELEMENT METHOD*

1. Introduction. Stages of shot process.

The elaboration is inspired by the fact that the numerical modeling of given process could ensure opportunities of preliminary theoretical investigations on dependencies between ruling factors and chosen criteria for an optimal process performance. Such modeling accomplished before the enlargement of existing theoretical works, the development of new techniques and technology or even before the formulation of real physical experiments could reduce the time and costs of the investigations. Additionally, the obtained results could give new directions of future researches. The process of smoothbore barrel shot is initiated and advanced in an ensemble composed by the barrel-itself, projectile, propellant, and corresponding designs of barrel chamber, barrel muzzle, cartridge-case where specific combustion cameras ensure initial stage of the process [1, 2].

A process of smoothbore barrel shot basically comprises of (I) internal stage, which starts with the ignition and firing of the primer and propellant in the cartridge-case, Fig. 1a, and ends with the projectile exit from the barrel muzzle, Fig. 1b, (II) transitional stage, which starts when the projectile leaves the muzzle, Fig. 1c, until the projectile achieves the state of stable free flight, (III) external stage starting with a stable flight of the projectile and ending with contact in the target, the terminal stage finally [1, 2]. Here, the internal stage (I) of the shot, Fig. 1c, will be numerically modeled depending on (1) the friction conditions between projectile and barrel and (2) the projectile weight. The friction conditions are represented by five coefficients of friction. The projectile weight is represented by three densities of a projectile possessing cylindrical volume ending with half-sphere having the same diameter. That second could give an opportunity to interpret different projectile designs including projectile jackets, volumes of cores or different saboted underbore forms, but under conditions that all these to have the total preliminary given weight. Also, the kinetic energy is classically expressed by half-product of the weight and the second degree of velocity [1]. If it is wanted to increase the maximum power of percussion action with a constant propellant and weapon characteristics, then it should to increase the velocity by decreasing of the projectile mass i.e. an optimization task arises. The shot process is computed in eleven steps, each of them with seven substeps. The proper coefficient of friction gives an opportunity to choose different materials and surface roughness in order to obtain the optimal friction conditions under given in advance pressure-time dependency in the barrel or to change in advance given such dependencies according to the friction conditions.

The aim of this elaboration is to outline preliminary some basic relations between parameters of shot as displacement and velocity of the projectile in the barrel depending on the projectile weight and the friction conditions between the barrel and projectile. For this purpose a numerical finite element model applying commercial program product Ansys LS-DYNA is developed and eight simulations of the shot process of are carried out. As results both the projectile displacements and velocity are established, projectile kinetic energy near to the muzzle is calculated, and stress – strain states in the projectile and barrel are found.

2. Technical devices for production of shot. Smoothbore barrel. Geometry. Ammunitions.

A basic part in the weapons is the barrel [3, 4]. A proper design of barrel represents a complex task which is related not only to mathematical calculations and choice of material but also with designs of proper processing technologies, proper ammunitions, properly attended loading elements and corresponded bearing and transporting systems. The numerical model here discussed is composed by four parts: 1-smoothbore barrel, 2-projectile, 3-cartridge-case and 4-breech-block interacting under corresponding contact conditions between them. At the back the barrel begins with 5-chamber where the cartridge is placed, Fig. 1a. The barrel ends in front with 6-muzzle where a choke part could be appeared, Fig. 1b.

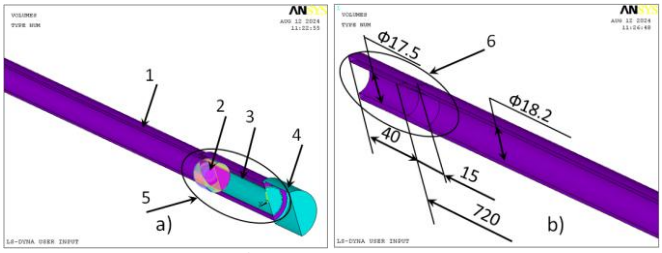


Fig. 1. a) *3-D section of smoothbore barrel. 1-barel, 2-projectile, 3-cartridge case, 4-breech-block, 5-barrel-chamber,* ***b)*** *6-muzzle and choke.*

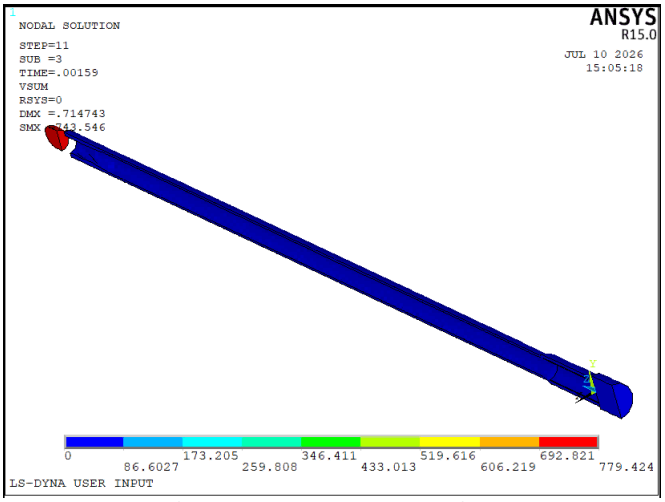


Fig. 1c *The end of the internal stage and start of the transitional stage during a process of shot with projectile having density of 1820kg/m^3 (weight 8 grams) under coefficient of friction μ=0.15.*

Each of them could have different design independently of the type of weapon but with one and the same goal to increase the percussion action [3, 4]. In this work an exemplary design of barrel

is treated with its corresponding elements. That is not a precise barrel of real weapon, and it does not pretend to be exact design of real weapon barrel because the efforts of this work are only reduced to outline preliminary principal possibilities of development of numerical model of such types shot process.

3. Assumptions and numerical setup of the task.

In Fig. 2 the geometrical sizes of 5-barrel-chamber, 3-cartridge and 2-projectile are given. The cartridge-case is not presented as a whole as design because the subject of this elaboration is displacement of the projectile in the barrel during internal stage of shot discarding the preliminary combustion and explosion processes provoking this displacement.

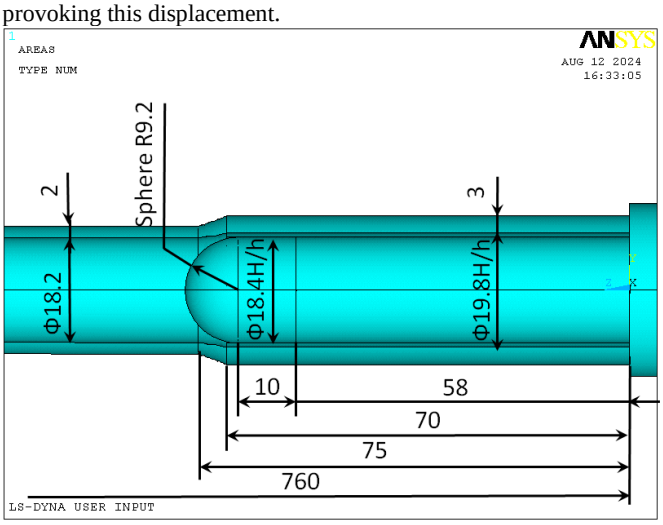


Fig. 2. *Sizes of the barrel-chamber, projectile and cartridge-case.*

A coordinate system *Oxyz* is embedded between the barrel and the breach. The barrel has inside diameter of 18.2mm and total length 760mm. In back part, it has a chamber with larger inside diameter of 19.8mm and length 70mm where the cartridge is placed. The cartridge has outside diameter 19.8mm and inside diameter 18.4mm with length 70mm. The barrel-chamber is closed by the breech which represent a cylinder with diameter 30mm and length 30mm. In front the barrel has a choke part with diameter 17.5mm and length 40mm connected to the basic barrel part by cone with length 15mm. The projectile is composed by a cylindrical part with diameter 18.4mm and length 10mm with volume $2.66x10^{-6}m^3$ and hemispherical part with the same diameter of 18.4mm and volume $1.64x10^{-6}m^3$. The barrel is meshed with 3-D 8-nodes finite elements Solid 164. The cartridge, breech and projectile are meshed with 3-D 10-nodes finite element Solid 168. The barrel is divided in 15500 finite elements with 2260 nodes. The cartridge is divided in 4563 elements with 9348 nodes. The projectile is divided in 298 finite elements with 579 nodes. The breech is divided in 295 finite elements with 559 nodes. It is unmovably and rigidly connected to the chamber, it is not loaded by the barrel pressure *i.e.* it does not take into account recoil effects. The mechanical properties of the materials are given in Table 1. They are chosen as representative and are not related to given barrel and projectile material data [5, 6].

Table 1: *Mechanical properties of material models.*

	Barrel and Breech	Cartridge	Projectile
Density [kg/m3]	7800	4500	1820, 2730, 3640
Elastic module [GPa]	210	150	180
Yield stress [MPa]	1350	150	1080
Poisson's ratio	0.29	0.35	0.34

The fittings between the barrel-chamber ant the cartridge and the cartridge and projectile are assumed as free-sliding ones of type H/h for hole/shaft, Fig. 2.

The contact conditions between outside surface of the cartridge-case and inside surface of the barrel-chamber are modeled by coefficient of friction 0.1. The friction between the inside surface of cartridge and projectile is modeled by coefficient of friction 0.5. The contact friction between barrel and the projectile is modeled by five friction coefficients 0.01, 0.05, 0.1, 0.15 and 0.2. In this work both the friction coefficients static and the dynamic are assumed with these equal values above reported. Variations of friction depending on the velocity are not taken into account. The weight of the projectile is modeled by help of three different densities, given in Table 1 and multiplied by the projectile volume of $4.3x10\text{-}6m^3$ they give projectile weights nearly of 8, 12, 16 grams.

Series of numerical simulations of the process of shot are performed through the geometries of barrel and projectile given in Fig. 2.

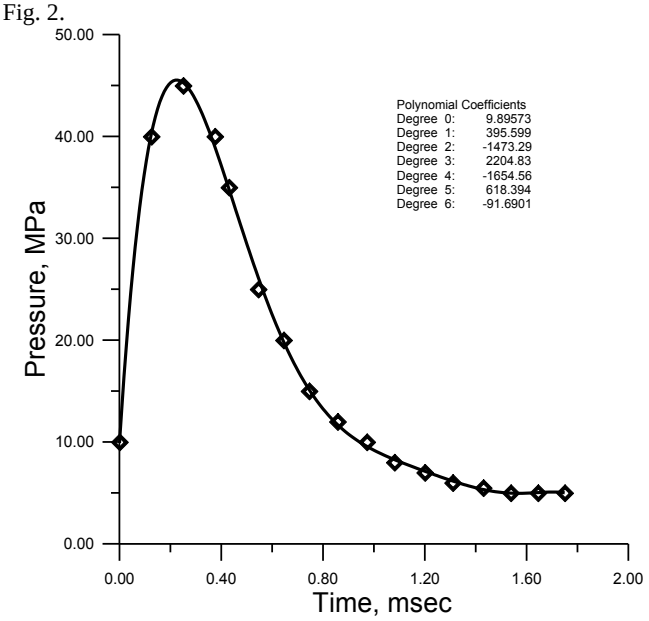


Fig. 3 *Diagram of Barrel pressure as function of time.*

The barrel pressure is assigned according to "Pressure – Time" diagram given in Fig. 3. The same this pressure loads the base of the projectile. Here, the pressure forces acting in the volume closed between the projectile base, cartridge inside and the breech could be or not be translated to the projectile base by additional elastic elements as shock-absorbers, gasket and others, occupying the distance of 58mm, Fig. 2. The type of the "Pressure-Time" diagram given in Fig. 3 could be different with shifted maximal pressure in the time. That is depended on the type and contents of the propellant and design of the cartridge [2, 5].

3. Results and Discussions

Which effects will cause the increase of the friction coefficient is arising as a question. The projectile starts to move when the forces initiated by the propellant pressure override the friction forces between the projectile and the cartridge-case. These friction forces are specific for each cartridge and result from its design. In this work the displacement of the projectile is modeled depending on its weight and the friction coefficient between the barrel and the projectile. The friction coefficient between the projectile and cartridge-case, as well this one between the cartridge-case and barrel are assumed as constants. The obtained results are given in Fig. 4. With smoothbore barrel and lowest coefficient of friction 0.01 between the barrel and the projectile, the displacement of the projectiles after exit of barrel under pressure 7.5-8MPa is 1.13m. The projectile leaves the barrel in time 1.277 milliseconds with velocity Vz=860m/sec, and the velocity is increased to 956m/sec after leaving the barrel in distance 0.37m at time 1.75 milliseconds. This is the case of shot with both the lowest friction and weight. According to the classical $\boldsymbol{Ek=0.5mVz^2}$, the maximal kinetic energy is Ek=2958.4J, where Vz is in m/sec, m in kilograms When μ=0.15 Vz=712m/sec and Ek=2031J, it is nearly 1/3 lower.

In Fig. 3 diagrams sowing the change of the barrel pressure in time beginning with primer ignition is given. The character of this diagram could be different with movement of the maximum in the time. Here a diagram is taken as an illustrative one from [2]. The diagram could be separated in four basic parts. In the first part a sharp increase of the pressure from 0 to the maximum of 45MPa (450atm) is observed for 0.25miliseconds. Next, after this maximum a part with smooth pressure decrease to 12.5MPa, asymmetric to the increasing part, is seen in time 0.8 milliseconds. After that a decrease of the pressure to 5MPa is seen from time 0.8msec to 1.6msec. During the commented four stages the projectile has increasing velocity with non-uniform displacement in the barrel. These described four stages have close dependency on the contents of the propeller and its rate of compression in the cartridge as well the design of the cartridge [2, 5].

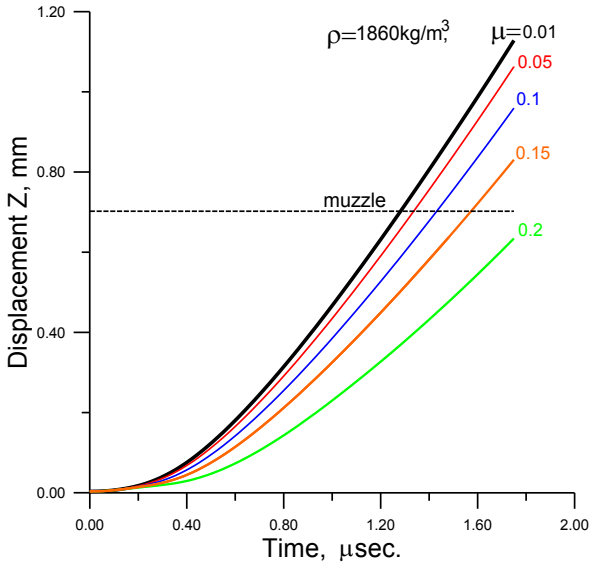


Fig. 4 *Diagrams "Displacement - Time" obtained for projectile with density 1820kg/m^3 under friction coefficients μ in range 0.01, 0.05, 0.1, 0.15, 0.2.*

In Fig. 4 the displacement of the projectile in the barrel is given in time dependency under coefficients of friction 0.01, 0.05, 0.01, 0.15 and 0.2 with the barrel. The place of the barrel muzzle is given by horizontal dashed line showing the moment when the projectiles live the barrel. The given curves could be also divided in four parts corresponded in the time to the four parts in Fig. 3. A small displacement of the projectile is read in the first part at time 0.1 millisecond for the five coefficient of friction. At time 0.8 milliseconds, with μ=0.01 the displacement has highest value of 0.35m while with μ=0.2 it has lowest value of 0.15m. The projectile with the lowest friction coefficient first leaves the barrel in time t=0.122 milliseconds. The projectile with the friction coefficient 0.15 leaves the barrel for largest time 1.6 milliseconds, while this having μ=0.2 does not reach the muzzle. This projectile has displacement of 0.63m. The pressure of 5MPa in the last stage is not sufficient for its leaving of the barrel according to this simulation. After the beginning of the third and four stages at time 0.8-0.9 milliseconds the displacements described by the four curves have linear tendencies. The diagrams "Velocity Z – Time" given in Fig. 5 are also divided in the same four parts, analogically to Fig. 3, 4 as they are consequences of these figures. In the first stage until time 0.23-25 milliseconds with friction coefficient 0.01 increasing velocities to 300m/sec and to 180m/sec could be read for μ=0.01 and 0.1, respectively. That is nearly 60% increasing velocity with ten times decreasing friction. At time 0.1-0.3 milliseconds, with the highest friction coefficients of 0.15 and 0.2 a horizontal tendency with constant values 80-90m/sec is observed. That suggests holding of the projectile by friction and insufficiency of pressure 45MPa to accelerate the projectile to the maximal pressure. The increased friction above μ=0.1 leads to change of the character of "Vz-Time"-curves. A new intermediate stage appears between I- and II-stage, and it is not related to the "P-Time" diagram. That shows because of friction, the conclusions based on Fig. 3 could not be made automatically. Moreover, this is the moment of bending in the "P-Time" diagram. During the second and third stages the velocities increase but with decreasing acceleration. During the fourth stage (the period of after-action of the propellant gases) for μ=0.01 the velocity achieves values from 820 to 950m/sec, and for μ=0.2 the velocity of 600m/sec appears as an insufficient for the projectile to leave the muzzle.

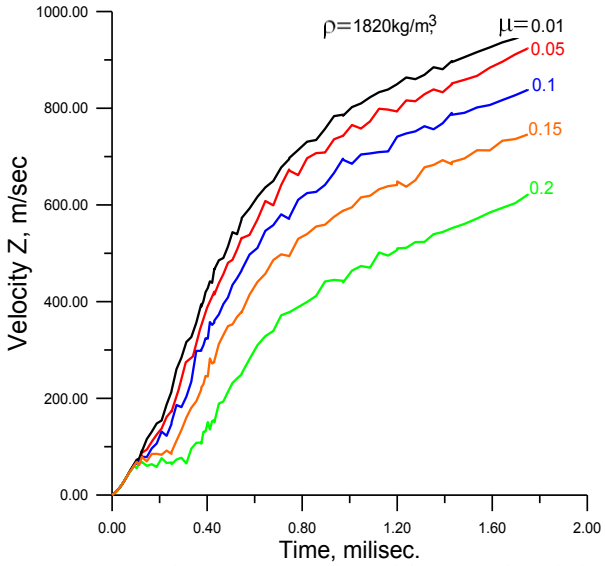


Fig. 5*. Diagrams "Velocity Z - Time" obtained for projectile with density 1820kg/m^3 under friction coefficients μ in range 0.01, 0.05, 0.1, 0.15, 0.2.*

In Fig. 6a, b the distributions of the strain and stresses in the volume of the projectile and in the transition part of the barrel are given in the beginning of the internal stage at friction coefficient μ=0.15 and m=8 grams. This is a heaviest numerically possible regime of shot with these parameters. Strains and stress in range of 0.00137 and 188MPa are read. The strain values are sufficiently lower than the theoretical plastic strain limit of 0.02. This circumstance appears as an important one during the design of barrel because it suggests absence of plastic deformations.

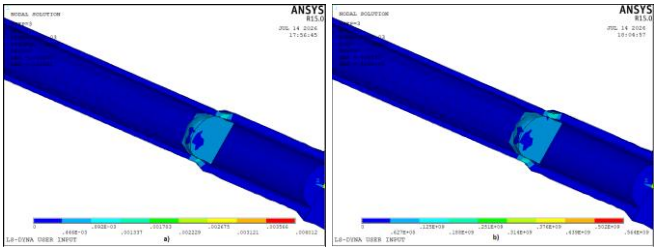


Fig. 6 a) *Equivalent strain distribution* ***b)*** *and Mises stress distribution in the barrel and projectile in the start of internal stage at shot with projectile having density ρ=1820kg/m^3 (8grams) under friction μ=0.15. Step 3/1, Time t=0.146 milliseconds, Displacement Uz=9.59mm, Velocity Vz=69.5m/sec.*

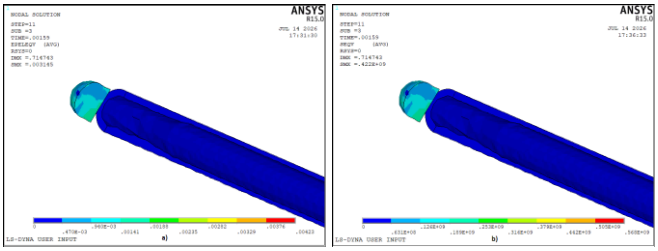


Fig. 7 a) *Equivalent strain distribution and* ***b)*** *Mises stress distribution in the barrel and projectile in the end of internal stage at shot with projectile having density ρ=1820kg/m^3 (8grams) under friction μ=0.15. Step 11/3, Time t=1.59 milliseconds, Displacement Uz=714.7mm, Velocity Vz=743.5m/sec.*

In Fig. 7 the strain and stress distributions in the volumes of projectile and barrel are given in the end of the internal stage for the same shot parameters. The strain and stress values are in maximums

of 0.00235 and 316MPa. That suggests the projectile undergoes increasing elastic strains with increasing stress, there is no plastic deformation. The same is valid for the barrel.

The stress and strain states on the surface of projectile with density 1820kg/m^3 (m=8 grams) is given for three nodes under friction coefficients 0.15 and 0.01, Fig. 8a-d. The nodes 1, 2 and 3 are placed as follows, Fig. 2, in the projectile forward between the end of spherical and beginning of cylindrical parts, in the middle cylindrical part and in the rear cylindrical part. In Fig.8a, c, sharply increasing strain and stress values from 0 to 0.0024 and 240MPa are seen for both the coefficients until time 0.23 milliseconds, when the maximal pressure is overcame Fig. 3. After that, under μ=0.15 a tendency of keeping the strains 0.002 and stress 200-240MPa is observed, Figs 8a, b, while under μ=0.01 a smooth decrease to 0.0008 in strains and to 80MPa in stresses is observed, Figs 8c, d.

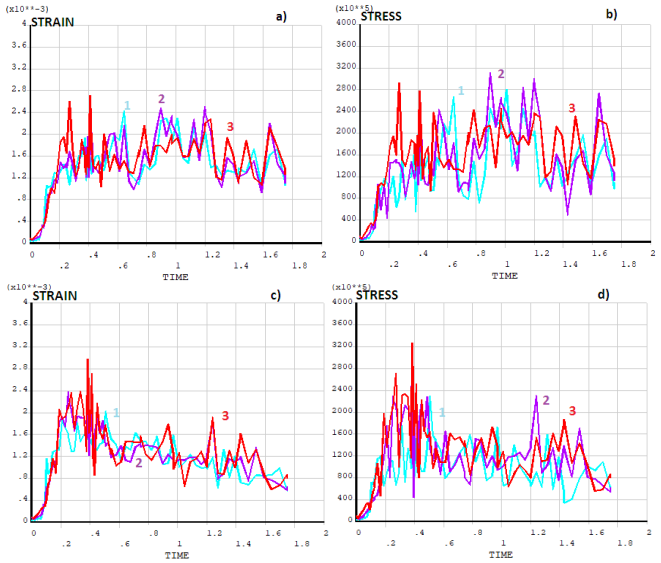


Fig. 8 *Distributions of* ***a, c)*** *strain and* ***b, d)*** *stress in the projectile during the internal stage of the shot with coefficients of friction* ***a, b)*** *0.15 and* ***c, d)*** *0.01 at density 1820kg/m^3. 1–in the forward part, 2-in the middle part, 3–in the rear part.*

In Fig. 9a, diagrams "Displacement Z -Time" for projectiles with densities of 1820, 2730 and 3640kg/m^3 under friction coefficients μ=0.01 and 0.05 are given in order to outline the projectile weight influence on the shot. Clear separations of the curves depending on the increasing projectile weight in 1.5 time and in 2 times are seen with the 5-multiple increase of friction. Comparisons in the end of II-stage, in time 0.8 milliseconds, show displacements of 0.3 and 0.17m for densities ρ=1820, 2730kg/m^3.

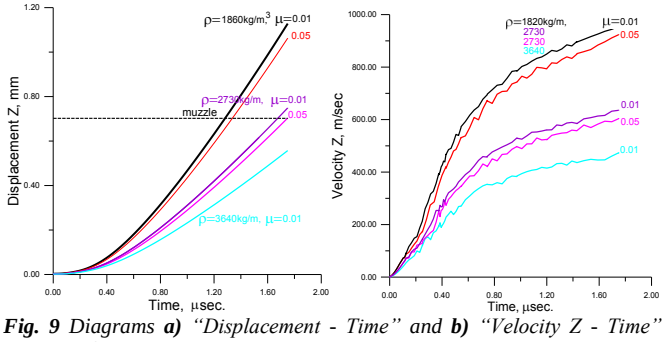


Fig. 9 *Diagrams* ***a)*** *"Displacement - Time" and* ***b)*** *"Velocity Z - Time" obtained for projectiles with densities ρ=1820, 2730, 3640 kg/m3 under friction coefficients μ=0.01, 0.05, 0.1.*

The comparisons of the weight projectile influence on the projectile velocity, shown by diagrams "Velocity Vz –Time" in Fig. 9b, also clearly outline this separation effects above commented. The projectile having density ρ=2730kg/m^3 (m=12 grams) leaves the muzzle with velocity close to 600m/sec. This velocity is lower nearly of its-half than the velocity 860m/sec obtained with density ρ=1820kg/m^3. But here the tendency to achieve a constant velocity should be marked *i.e.* the transitional shot stage is going to finish and the projectile is going to free flight – third external stage of shot commented in the Introduction. The projectile having density ρ=3640kg/m^3 (here interpreted as designed weight m=16grams) does not achieve the muzzle at the lowest friction according to this FE-model of shot. Similarly to the higher friction of μ=0.2 at lowest weight as it is seen in Fig. 4, changes will be needed in weight or in "P-Time"-curve. Despite the lowest friction this projectile needs of higher maximal barrel pressure or another type barrel "Pressure-Time" diagram in order to overcome the I-stage. So, in this case, it could be concluded the decreasing weight of the projectile is more essential to realize a shot than the friction. At the same time, to achieve higher muzzle velocity, respectively higher *Ek* and percussion power, it is essential the weight not to be too higher under the same barrel "Pressure-Time" diagram. The last ratiocinations are related to optimization tasks concerning as design of barrels as well as design of propellants and cartridges. Comparisons between parameters of the eight simulations of smoothbore barrel shot here performed are given in Table 2.

Table 2: *Parameters of the shots in the end of internal stage.*

Density [kg/m^3] *vs.* Friction.	Time [msec]	Distance [m]	Velocity Vz [m/sec]	Kinetic energy [J]
ρ=1820, μ=0.01	1.276	0.697	860	2960
0.05	1.315	0.684	829	2748
0.1	1.430	0.701	786	2493
0.15	1.590	0.713	712	2031
0.2	1.750	0.634	620	1538
ρ=2730, μ=0.01	1.643	0.682	615	1517
0.05	1.750	0.703	602	1451
ρ=3640, μ=0.01	1.750	0.557	471	889

3. Conclusions

A smoothbore barrel shot is numerically modeled. The projectile displacements and velocity, stress-strain states in the barrel and projectile are established depending on the barrel-projectile friction and projectile weight. Four stages similar to the barrel "Pressure-time" diagram are identified in the projectile "Displacement–Time" and "Velocity–Time" diagrams. A crucial inter-stage related with the higher than μ=0.1 friction is found. Projectile kinetic energy near to the muzzle is calculated.

4. References

1. R. Bolton-King, J. Schulze, Firearm and Ballistics, Chapter 7 Firearms and Ballistics. *In: Practical Veterinary Forensics*, ed. Bailey, D. Wallingford, UK: CABI, (2016) pp. 81-117.

2. Iv. Topalov, *Hunting weapon and shot on game*, Sofia, (1972) pp.142 /*in Bulgarian*/

3. N. Ahmed, R. D. Brawn, A. Hameed, Finite Element Modeling and Simulation of Gun Dynamics using 'ANSYS', *Tenth International Conference of Computer Modeling and Simulation* (IEEE 2008), pp.18-22.

4. S. Deng, H. K. Sun, Ch.-J. Chiu, K.-Ch. Chen, Transient finite element for in-bore analysis of 9 mm pistols, Appl. Math. Modelling **38** (2014) pp. 2673–2688.

5. M. Akcay, Internal and transitional ballistics solution for spherical and perforated propellants and verification with experimental results, J. of Thermal Science and Technology, **37**, 1 (2017) 35-44,

6. A. B. Edward, P. St. Heyns, Sch. Kok, A Numerical Investigation of a Single-Shot in a DEM-FEM Approach to Shot Peening Simulation. Metals **9** (2019), 1183.

Features in the design of unmanned aerial vehicles aircraft type

Sabi S Minev
Higher Air Force School „G. Benkovski“ - Dolna Mitropolia, Bulgaria,
E-mail: subi.minev@abv.bg

Abstract: *The use of aircraft-type unmanned aerial vehicles (UAVaircraft type) in modern combat operations is considered. Basic temporary criteria for the production and operation of aircraft-type UAVs are defined. Using the similarity method, a determination of the mass of aircraft-type UAVs is proposed. A variant is proposed related to the calculation of the mass of the fuselage of certain aircraft-type UAV models. The difference in the use of retractable or fixed landing gear of aircraft-type UAV types in their operation is determined. Recommendations are made for noise reduction during UAV operation. The economic aspects of aircraft-type UAV design are touched upon.*

KEYWORDS: *UNMANNED AERIAL VEHICLE AIRCRAFT TYPE, UAV CLASSIFICATION, CRITERIA, DETERMINATION OF UAV MASS.*

1. Introduction.

Unmanned aerial vehicles of the aircraft type UAV are designed to achieve significant results in terms of: flight distance, speed and altitude. The methods and means, as well as the data from the research conducted, with the help of which these results are achieved in practice, are used in the further design of other classes of UAV. Recently, various new schemes and components of this class of UAV aircraft type have also been created for experimental purposes and for testing. The experiments are also aimed at testing and refining new systems related to their controls, aerodynamics, materials for manufacturing, where experimental material is accumulated for the creation of new, more advanced UAVaircraft type . Large unmanned aerial vehicles of the aircraft type are equipped with engines usually with power (55 ... 100 horsepower), providing significant independence for their use, in particular for independent takeoff and a set of heights for maneuvering and, of course, landing [5]. Possessing high aerodynamic properties, this type of UAV has changed the spectrum of their use in recent years. And as examples, some characteristics of existing aircraft-type UAV will be considered.

1.2. Example characteristics of existing aircraft-type UAV aircraft type

The Ukrainian unmanned aerial vehicle of the aircraft type "Lyuty" is a low-wing aircraft with a propeller located in the rear part of the fuselage. The fuselage is made of fiberglass with metal reinforcement, which makes the structure both light and durable. The main technical parameters of this aircraft-type UAV aircraft type are:

a. Length: 4.4 meters;
b. Wingspan: 6.7 meters;
c. Take-off weight: 200 kilograms or more;
d. Engine power: 50 horsepower;
e. Range: up to 1,500 kilometers;
f. Combat load: 50-75 kilograms.

The engine of the specified UAV is a German Hirth F-23 gasoline engine. The three-blade propeller is located in the rear part of the fuselage. The modular design allows for easy disassembly for transportation [6].

Examples of the specified class of aircraft-type UAVs that are widely used in practice include: UAV - Elbit Hermes 450; The single-engine version 450S, using a 70 hp "R902(W)" rotary-piston engine; The "Orion" unmanned aerial vehicle; All prototypes use a 115 hp "Rotax 914" engine, etc [9].

2. Statement of the problem

The main requirement for aircraft-type UAV aircraft type is the ability to be modular in design with the use of lightweight construction materials, cheap in production and flexibility and adequacy in performing the tasks set. In addition, the design and manufacture of this class of UAV aircraft type must take into account the dynamics of innovations, which undergo changes over a period of 3 to 6 months. In general, changes in the use of this class of UAV aircraft type in recent times are associated with the widespread use of artificial intelligence in their operation. To ensure the adequacy of new UAV developments and the trends arising from changes in their operation, it is not necessary to introduce some criteria for the manufacture and operation of aircraft-type UAVs.

3. Criteria set for the production and operation of aircraft-type UAV aircraft type.

When developing a hierarchy of criteria and integrating them into a single system, the following requirements are taken into account [10]:

1) the criteria must be adequate for the goals and objectives of using aircraft-type UAVaircraft type;
2) the hierarchy of criteria must follow from the hierarchy of goals for using UAV aircraft type, taking into account possible changes on the battlefield;
3) the factors determining the design of the unmanned aerial vehicle and its subsystems must be fully taken into account;
4) specific indicators must not contradict the general (integral) criterion;
5) the criterion must be clear and, if possible, easy to define.

The specified requirements for the criteria (1-5) must allow for the possible definition of the qualities and subsequent use of UAV aircraft type through one integral criterion setting the optimality of this type of UAV [10].

4. Main criteria for aircraft-type UAV aircraft type

When developing an aircraft-type unmanned aerial vehicle, numerous characteristics, parameters and performance indicators, as well as limitations for its operation, are taken into account. The following criteria should be noted [6]:

1. Aerodynamic efficiency – K_{opt}^{eff}. Minimizing total drag with a fixed lift coefficient is an important criterion as it directly affects flight endurance.
2. Structural weight - K_{min}^{m}. Reducing weight while maintaining stiffness and strength is the goal of optimization, often achieved by removing material from non-load-bearing areas.
3. Features of the engine installation - K_{opt}^{eng}. Propeller type, intake air characteristics, nozzles, fuel type and relative mass of powerplant and fuel.
4. Payload parameters - K_{max}^{m}. Possibility of placing specific and large equipment (e.g. cameras, radar stations, sensors).
5. Accuracy and reliability - K_{max}^{s}. Performance-related indicators (e.g. probability of recognition of reconnaissance targets, detection range of airborne radar).
6. Structural safety - K_{max}^{sek}. Passive safety (e.g. protective elements on the blades of the power plant) and compliance with structural reliability requirements.
7. Economic indicators - K_{min}^{ec}. Minimum costs with optimal technical parameters.

The specified criteria can, with some approximation, be expressed by an integral criterion K_{UAV}^{int} of the form:

(1) $K_{UAV}^{int} = \left(K_{opt}^{eff}, K_{min}^{m}, K_{opt}^{eng}, K_{max}^{m}, K_{max}^{s}, K_{max}^{sek}, K_{min}^{ec}\right) \rightarrow optimally$

5. Design features of aircraft-type UAV aircraft type

We will consider specific technical ideas (concepts) aimed at improving flight characteristics, primarily takeoff and landing characteristics, as well as reducing fuel consumption and noise levels of aircraft-type UAV aircraft type. Some of these ideas have been tested in practice, while others are not yet generally accepted. For example, in the design and manufacture of this type of UAV aircraft type, a wing profile is used that allows operation at relatively low subsonic and transonic flight speeds [5],[6].

A common configuration among aircraft-type unmanned aerial vehicles is the aerodynamic configuration with two tail sections located at an angle of 120 degrees. This configuration is most often used when placing a pusher propeller behind the fuselage and it has the smallest inductive resistance of 3% compared to the total. The V-shaped tail section also creates a closed power circuit of the fuselage, which provides very high strength of the entire structure. The specified configuration is also often used in large aircraft-type unmanned aerial vehicles. A variant of the aircraft-type UAV with a V-shaped tail is presented in Fig. 1



Fig. 1. UAV aircraft type V-shaped tail section

The most suitable NASA wing profile for an unmanned aerial vehicle UAV aircraft type depends entirely on its purpose, speed and expected payload. Usually aircraft type UAVs fly at a lower speed, which changes the flow of the wing. For them, NASA develops optimized low-speed geometries, for example, the NACA 2412 wing profile. An extremely popular profile that offers a great balance between low drag and good payload. In addition, NACA 0012 and NACA 0015 profiles are also used. Additionally, other wing profiles are experimented with and used in practice [5].

The conducted aerodynamic simulation of the NACA 0012 profile of an aircraft type UAV at a speed of 110 to 150 km/h and the obtained specific characteristics from it are presented in Fig. 2.

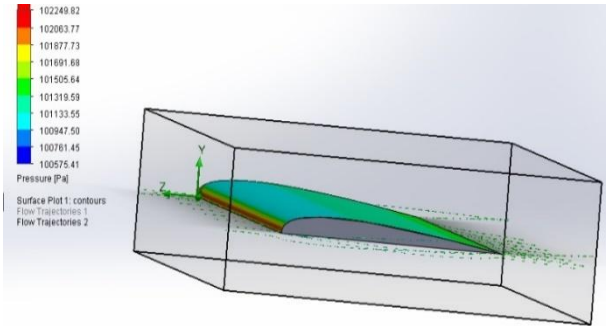


Fig. 2. Aerodynamic characteristics of a NACA 0012 profile of an aircraft-type UAV aircraft type at a speed of 110 to 150 km/h.

6. Determining the mass of an aircraft-type UAV aircraft type

An important characteristic of each type of UAV is its take-off mass. Usually, when designing a UAV aircraft type, the mass is determined by successive approximations. The first approximation in determining the mass is carried out at the stage of preliminary design (technical proposal), and the second and, if necessary, subsequent approximations, when it is necessary to select materials and equipment, are made during the conceptual design. Below we consider determining the mass of an aircraft-type UAV (in kg) at takeoff in G_0 first and second approximation.

6.1. Calculation of the take-off mass of an aircraft-type UAV in the first approximation

In the Russian-language literature, the dependence for determining the mass of aircraft is presented [1].

From the equation for the balance of the mass of an aircraft-type UAV in relative units, relative weight, relative weight and relative parts.

(2) $1 = G_{str} + G_{c_eqm} + G_1 + \frac{1}{G_0}\left(G_{eng} + G_{c_load} + G_{add_eq}\right)$

Where: G_{srt} - structure mass construction; G_{c_eqm} - mass control equipment ; G_0 - mass UAV takeoff weight ; G_{c_load} - combat load; G_{add_eq} - mass additional equipment; G_{eng} - mass engine installation; G_1 – mass important unit.

After a minor transformation in (2) we obtain, at the initial moment, to a first approximation, the relative value of the mass of an aircraft-type UAV G_0 by component parts at takeoff, namely:

(3) $$G_0 = -\frac{G_{eng} + G_{c_load} + G_{add_eq}}{G_{srt} + G_{c_eqm} + G_1 - 1}$$

We assume in (3) that the engine type and the mass of the propulsion system - G_{eng} , as well as the masses of the combat payload - G_{c_load} and additional equipmentG_{add_eq} - are known or given. And the remaining relative masses of the structure, equipment and control system are taken as relative average values from existing models, which are presented in Table 1.

6.2. Relative values of the masses of the structure, equipment and control system of an aircraft-type UAV (variant)

Table 1. Relative masses of the structure, equipment and control system of an aircraft-type UAV

N number	Name of the mass of the UAV structure	UAV,s structure mass limits
1	Gsrt - structure mass construction	0,38...0,42
2	G(c_eqm) - mass control equipment	0,09...0,12
3	G_(c_load) - combat load	0,10...0,15
4	G(add_eq)- mass additional equipment	0,09…0,12
5	G eng- mass engine installation	0,21…0,24
6	G1 - mass important unit	0,04…0,08

The specified relative mass values in an aircraft-type UAV, determining the take-off mass value G_0 we will demonstrate with the following example. For this purpose, the average relative values of the data presented in Table 1 have been selected [6]. In this case, we have:

(4) $$G_0 = -\frac{0{,}22+0{,}11+0{,}1}{0{,}41+0{,}1+0{,}06-1} \quad where \quad G_0 = 1{,}000$$

The relative average values of the masses constituting an aircraft-type UAV presented in (4) are of a balance nature. Any change in the relative values of the masses implies a change in other changes in the quantities included in equation (4). The assumed relative value of $G_0 = 1{,}00$ In UAV design practice, priority is determined by the relative values: G eng- mass engine installation and G(c_load) - combat load. Variant with relative value of $G_{eng} = 0{,}21\ldots0{,}24$ and $G_{c_load} = 0{,}10\ldots0{,}15$ Table 1 shows the relative values of G_0 from (4) we obtain the dependence [1]:

(5) $$Go = 2{,}32558 Geng + 2{,}32558 Gcload + 0{,}232558$$

The relative values of G_0 are presented in Fig. 3

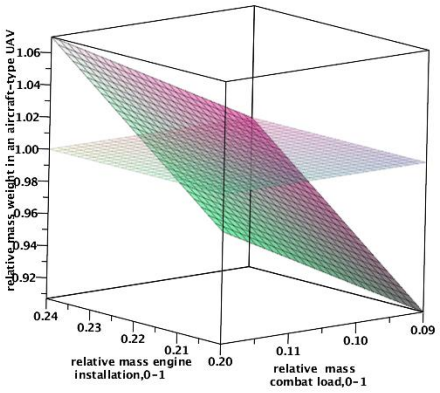


Figure.3. Dependence of G_0 on the relative weight of G eng- mass engine installation and G(cload) - combat load in an aircraft-type UAV,s.

6.3. Mass of the main elements making up the structure of an aircraft-type UAV aircraft type

It is known that the mass of the main elements in the construction of an aircraft-type UAV aircraft type is determined by the masses of the wing, fuselage, tail and chassis. The total value of the mass is determined by the dependence:

(6) $G_{srt} = G_{wing} + G_{fus} + G_{supp} + G_{chas}$

Where: G_{srt} - structure mass construction UAV,kg; G_{wing} - UAV, s wing mass, kg; G_{fus} - UAV fuselage mass,kg; G_{supp} - mass of the supports in the UAV, kg; G_{chas} - UAV chassis mass, kg

One of the significant parts of the mass of an aircraft-type UAV structure is the mass of the fuselage - G_{fus} UAV fuselage mass,kg. Its value can be determined by the dependence:

(7) $G_{fus} = 1{,}14\kappa_{eng}\left(1 + 0{,}4k_{pres}\right)L_{fus}^{1,5}G_0^{\frac{1}{4}}$

Where: κ_{eng} - engine installation coefficient (κ_{eng} =1,14 - if the engines are mounted on the fuselage) ; k_{pres} - coefficient of maximum operating altitude, Pa_{alt} for an altitude of 1000 meters ; L_{fus} - fuselage length, meters ; G_0 - mass UAV takeoff weight,kg

With average dimensions for the given class of UAV aircraft type: $k_{eng} = 1{,}14$, $k_{pres} = 0{,}7..0{,}8$, $L_{fus} = 4{,}4 \ldots 5{,}6m$ $G_0 = 180 \ldots 230kg$ by dependence (7) the mass of the fuselage G_{fus} it turns out:

(8) $G_{fus} = 1{,}715472L_{fus}^{1,5}G_0^{\frac{1}{4}}$

The dependence given by (7) and presented in (8) on the average values of existing UAV aircraft type, the mass of the fuselage G_{fus} is demonstrated in Fig.4.

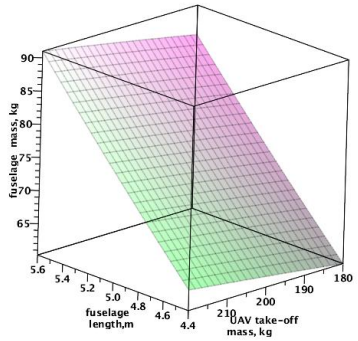


Fig. 4. Mass of the fuselage G_fus of an aircraft-type UAV under average conditions κ_{eng} _eng=1.14 , kpres=0.7..0.8 , Lfus=4.4…5.6m G_0=180…230kg.

The figure presented in Fig. 4 shows that Mass of the fuselage is within limits $G_{\text{fus}} = 85..110\ kg$ of the total mass of the aircraft-type UAV $G_0 = 180 \ldots 230kg$.

The results obtained from the calculation of the fuselage mass according to and presented specifically in [1] show that these dependences provide acceptable accuracy for the design of aircraft-type UAVs, accompanied by a standard error of about 2-5%. The distribution of some of the masses of the individual elements expressed in percentages, making up the fuselage mass, are presented in Table 2.

Table 2.The distribution of some of the masses of the individual elements expressed as percentages of the fuselage mass

N number	name of individual elements elements of a UAV	mass of individual fuselage elements expressed in percentages
1	UAV skin	30...35
2	stringers and spars	15…25
3	barriers and joints	10…15
4	hatches for UAV equipment	9…12
5	UAV seals and fasteners	6…9
6	other fuselage elements	3…6

The results in Table 2. show that the skin, stringers and frames account for 60–65% of the mass of the fuselages of aircraft-type UAVs. The significant relative mass of the specified elements compared to the total of the fuselage suggests the search for solutions to reduce it. Such solutions in modern conditions require the use of new materials in the fuselage construction, which can lead to a weight reduction of 15...20%. For example, the use of a "honeycomb" structure using fiberglass or carbon fibers (polymer paper honeycombs with dimensions of 9-10 mm). This structure has a surface density of about 3 kg/m2, and a three-layer panel of fiberglass or carbon fibers in combination with other dense materials such as plywood has a surface density of 4.5 kg/m2, i.e. 1.5 times greater.

8. Design measures for noise limitations during flight of aircraft-type UAV aircraft type

The practical operation of aircraft-type UAV aircraft type implies a system of measures to limit noise when flying over a given territory. Over time, these restrictions are becoming more and more stringent [7]. Currently, for example, it is required that the noise during the cruising flight of an aircraft-type UAV at a distance of up to 3.5 km from the earth's water surface should not exceed 93 dB, and when landing, the noise should not exceed 102 dB.

9. Economic aspects in the design and manufacture of aircraft-type UAVs

The introduction of new materials in the design of aircraft-type UAV aircraft type implies a continuous reduction in the costs of their manufacture, which are:

A. Reducing the number of structural elements and joints;

B. Simplifying the external shapes of the components (surfaces, ribs, stringers, etc.);

C. Creating aircraft-type UAV aircraft type through modeling prototypes.

To implement the indicated directions, forecasting of the financial management of a given type of research and production structure related to the design of aircraft-type UAV aircraft type is applied. The dynamics of the development and modernization of UAV aircraft type over time applies time series. For a more detailed study of time series in financial management, probabilistic-statistical models are used as a priority. In this case, the time series $Bp(t)$ is considered as a random process (with discrete time) for the movement of financial quantities, for example in particular - timeliness of UAV aircraft type production, granting of loans, etc [4]. For measuring the activity of the financial structure $Fin(t)$ in

chronological order B$p(t)$ mathematical expectation is used $M_{mat\ expect}$ of the state, the "movement" of financial investments, on the dependence [3]:

(9) $$Fin(t) = M_{mat\ expect}\ \mathrm{B}p(t)$$

In applied research in financial management, time series models are considered and applied, with stationary models being the first. In them, the joint distribution functions for an arbitrary number of time moments k of the dynamic series, for example, investments, financial receipts, interest for the design and production of aircraft-type UAV aircraft type , change over time. In this case, the fluctuation of the mathematical expectation should be predicted with sufficient accuracy..

10. Lockdown

The considered features in the design of aircraft-type UAV aircraft type are determined by the dynamics of their use in practice by formations. The factors influencing the choice of a specific design scheme in the context of the purpose of the future unmanned aerial vehicle are also analyzed. Based on this analysis, a number of criteria have been formulated that allow focusing the process on accelerating the design in a short time. This is achieved by calculating the take-off mass of the aircraft-type UAV aircraft type, the mass of the fuselage, as well as the values of the masses of the structure, equipment and the control system of the aircraft-type UAV. Additionally, the distribution of some of the masses of the individual elements expressed in percentages, making up the mass of the fuselage, was determined. The economic aspects of the design of aircraft-type UAV aircraft type were also touched upon. The proposed approach to the preliminary design of unmanned aerial vehicles has some incompleteness, but I hope that it can serve as a basis for subsequent development by other UAV specialists.

Literature

1.Badagin A, Muhamedov F.A. Konstruktion von Leichtflugzeugen M. Maschinenbau, 1978-2028 S..
2. Ivanov M. V. E-mail: str412mam@mail.ru, Moscow State Technical University named after N. E. 2005.
3. Krasilshchikova M.N., Sebryakova G.G., Management and guidance of unmanned maneuverable aerial vehicles based on modern information technologies, Fizmatlit, 2003.
4. Mineva S.K., Research and increasing the effectiveness of the financial management of modern organizations, V. Levski National University, V. Tarnovo, (2025).
5. Moiseev V.S., Saleev A.B. Main directions of development of unmanned aviation complexes on the basis of piloted prototypes of aviation technology developed for the state, Aerospace technologies and equipment (AKTO-2006). Materials of the international scientific and technical conference. - Kazan: Kazan Publishing House. Mr. technical University, 2006. - P. 60-62.
6. Fundamentals of design, construction and manufacturing of aircraft (remotely piloted aircraft). In order. I.S. Golubeva and Yu.I. Yanke-vicha. - Moscow: MAI Publishing House, 2006. - 528 p.
7. Kanchev, N., Application of fused deposition modeling approach for 3d printing in the design and manufacturing of small unmanned aerial vehicles.aeronautical research and development, Volume 3, 2024 "Georgi Benkovski" Bulgarian Air Force Academy, стр. 85-96, p-ISSN 2815-293X, e-ISSN 2815-2948
8. Stratton R.A., Corlson N.L. Fiber wall damage during bond failure, Nordic Pulp Paper Res. J. 1993. N2. Pp. 245–249.
9.https://ru.ruwiki.ru/wiki/?utm_referrer=https://yandex.ru/ 15.04.2026
10. https://yandex.ru/search/? 18=.05.2026