INTERNATIONAL SCIENTIFIC CONFERENCE ON SECURITY
11 to 14 December, 2017 at the Borovets winter resort, Bulgaria.

ORGANIZERS:

SCIENTIFIC-TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
INTERNATIONAL ACADEMY ON SECURITY

www.confsec.eu, e-mail: office@confsec.eu
THEORETICAL FOUNDATIONS OF SECURITY

SECURITY TODAY. CURRENT ISSUES
Prof. Radulov N. PhD ................................................................. 95

ELEMENTS OF THEORY TO SOLVE THE PROBLEM OF MANAGEMENT OF TRANSPORT SAFETY
L.N. Elisov, N.I. Ovchenkov ........................................................... 98

NATIONAL AND INTERNATIONAL SECURITY

APPLICATION OF MOBILE GIS SERVICES IN DISASTER MANAGEMENT
Assos. Prof. Milen Ivanov PhD, Yavor Yankov PhD ................................................................. 102

POLYMER WASTE MANAGEMENT – ENVIRONMENTAL SAFETY STRATEGY
Ass. Prof. PhD in Tehn. Sc. Malyshevska O., Prof. Dr. of Medical Sc. Garkavij S., Ass. Prof. PhD in Mineralogical Sc. Melnyk O.,
Prof. Dr. of Medical Sc. Mizyuk I., Ass. Prof. PhD in Biology Myshchenko I. ................................................................. 106

WAYS OF UPDATING THE TACTICAL AND FIRE TRAINING IN THE BULGARIAN ARMY AND MOI UNITS
Popov G., Assoc. Prof. Marinov R. PhD ................................................................. 109

INFORMATION SECURITY

ON THE CONTEMPORARY CYBERSECURITY THREATS
Assistant Prof. Linko G. Nikolov, PhD; Assistant Prof. Krasimir O. Slavyanov, PhD ................................................................. 111

TECHNICAL FACILITIES FOR ENSURING SECURITY

DRONE DETECTION IN URBAN ENVIRONMENT – THE NEW CHALLENGE FOR THE RADAR SYSTEMS DESIGNERS
Prof. M.Sc. Demirev V., PhD. ................................................................. 114

AN APPARATUS FOR RECORDING OF EXTREMES IN ELECTRICAL SIGNALS - FDI-1

A MEASURING DEVICE FOR WEAK SIGNALS WITH A HIGH-IMPEDEANCE INPUT - SPCE METER 1
M.Sc. Eng. Jordan Popov, Assoc. Prof. Ognyan Ivanov PhD, Prof. José L. Pérez-Diaz PhD ................................................................. 121

MONITORING OF THE NATURAL RADIOACTIVE FUND AND RADIOACTIVE POLLUTION - AN IMPORTANT FACTOR OF NUCLEAR SECURITY IN BULGARIA
Ass. Professor, Ph.D, eng. Dolchinkov N. T. ................................................................. 125

DETERMINATION OF CHANGE OF THE POINT OF THE FIRE SHOTS AT SHOOTING WITH FITTED CHAMBER TYPE SUPPRESSOR

STRUCTURAL RESPONSE OF A REINFORCED CONCRETE SPECIMEN SUBJECTED TO BLAST LOADING
M.Sc. Petkov Y., Assoc. Prof. M.Sc. Ganev R. PhD., Prof. MSc. Lilov I. PhD. ................................................................. 133
Security today is a category of special interest for both specialized organizations and ordinary citizens. Globalization, migration processes, the spread of terrorism, integrated with international organized crime, make people face modern challenges, the overcoming of which requires preparedness, creativity and self-denial.

I will discuss the following relevant aspects of security:

1. National security and migration processes

Linking the issue of migration to national security is particularly relevant, given the migratory waves from the Middle East to the EU countries, stimulated by the expulsion of IDIL outside this region. Migration exchange is a source and a transporter of terrorist and criminal threats. Over the last few years, Europe has been flooded with giant migratory waves. Millions of illegal migrants crossing the green border of at least three countries and committing in this way crimes under several local laws, have settled in the EU. Many of them are without papers and created a serious problem with clarifying their identity and origin.

This facts presupposed emphasis on ensuring national security especially in countries where there are significant groups of foreign immigrants. The special element of security is due to illegal migration and migrants with a Muslim religion or jihadist roots and intentions.

More and more security experts are addressing the problem in the context of "Illegal migration - a threat to national security". This is mainly due to the fact that each country is interested in its national security, satisfaction and compliance with its national interests, and uncontrolled migration flows can lead to significant changes in the socio-economic life of the country and change the traditional way of life of the local population. National security is not only protection against external threats; it is "government that ensures the integrity and ability to be an independent subject of international relations."

Military and political conflicts in a number of Muslim countries have forced people to seek safer living conditions: flows of immigrants from Libya, Syria, Afghanistan, Iraq have rushed into Western Europe. Just over the past few years, more than three million people have arrived in the European Union. And so far, every day, thousands try to enter the European countries on land and sea.

The problem of regulating migration processes as a possible threat to national security is extremely serious, and this is of great importance for a number of reasons. Among them undoubtedly are:

- The scale of migration flaws;
- Deterioration and increase of international conflicts;
- Non-compliance by migrants with the law of the host country as a result of the slow or failed process of integration into the local community. The flow of immigrants from the Muslim countries to Europe has led to a number of conflict points with the indigenous population on ethnic and religious base. In addition, the negative attitude of the local population towards the newcomers increased due to the inconsistency of the latest legal European and local norms and the cultural traditions of the countries.

Increase in crime, worsening of the criminogenic situation in the country or the EU countries. Migration experts say that inherently any kind of migration of population is potentially criminogenic as far as migrants fall under the new conditions, experience natural social and psychological difficulties that affect the increased criminal activity of this category of persons. The analysis of available statistics on the link between the creation of migrant communities and the increase in crime rates in individual European countries shows that the increase in crime rate is around 25% during the last migrant period from mid-2013 to the present. The percentage varies depending on the level of concentration in different countries and some of their regions. Only in Germany the committed crimes of migrants in 2017 are over 240,000.

- Non-compliance by migrants with established norms of conduct and cultural traditions. The thesis of multiculturalism proved completely wrong. It was touted for years, mixed with political correctness, understood as Christian patience and submission of the other cheek when slapped.

- Threat of terrorist acts. Of course, traditional communities of people of a different kind and origin, encircled and deployed around major European cities such as London, Paris, Marseille, Lyon, Brussels, etc., create no less threats and problems, but unresolved issues, for years concealed and neglected, were given new impetus to ignite due to migrant wave.

- Strengthening social tensions in the host society. A typical example is Germany. Immigrants from Turkey and other countries have pumped out the social system for years and exported considerable funds, but nearly 1.5 million new, official and as many illegal migrants blew up the hard-working and seriously taxed German citizens. Mrs Merkel's "open doors" policy is about to breathe new life into neo-Nazism. Not surprisingly, the results of the elections, making it difficult to form a government, because for much of the Germans, Mrs Merkel is directly responsible for the situation.

- Overloading resources of the country – to provide the people who arrive, food, shelter, programs for social integration. There are huge resources in the EU to solve such problems. So far, the migrant crisis has cost over 35 billion euros. Of course, these funds are used by local companies, but they are ultimately aimed not at solving the problems of taxpayers but on migrants and large companies. Organized crime, which is closely related to corruption, is directly involved in what is happening. The funds that go to migrants and refugees in Europe will be consumed in any way. Camps and small towns will be built, migrants will be cared for and fed, and large corporations are already aware of profits. A sum of nearly EUR 30 billion a year is available for absorption. Organizations with their own lobby in the European Union, local government structures and parliament are interested in migrants' concentration on the territory of Europe.

- Deterioration of psycho-climate and relations with other countries. The accusations against Mrs Merkel, the problem of illegal passage corridors, the attempts to build so-called "buffer grounds", to allocate the invited migrants through sole decision Lyon, Brussels, etc., create no less threats and problems, but unresolved issues, for years concealed and neglected, were given new impetus to ignite due to migrant wave.

Fearing of social and political instability as a result of frequent riots organized by migrants and after the failure of some temporary camps, several EU countries decided to restore the border control with other EU countries. These measures are due to the fact that a significant part of the countries of the European

Keywords: security, migration, organized crime, terrorism, special services
Union has signed the Schengen agreement, which provides for the free movement of persons, but such an approach leads to total impossibility of control and increases the dangers of illegal migration, terrorism, organized crime.

Some countries, as seen in actual practice, assume the burden of accommodation and care of migrants much more than others, with all the ensuing negative consequences. In 2015, the majority of asylum applications were submitted in Germany, Hungary, Sweden, Austria, Italy. The number of foreign nationals applying for asylum for the first time in Germany has increased from 173,000 in 2014 to 442,000 in 2015. The tendency to double the number of applications has so far remained. The total number of applications for temporary asylum in EU countries is increasing each year. In 2008 there were about 225,000, in 2012 – over 335,000, and in 2014 – more than 626,000. Record number was registered in 2015, when it was doubled compared to 2014 and amounted to about 1,322,825. In 2016 the number of asylum seekers has increased compared to 2015 by 40% and in 2017 by 15%.

A large proportion of refugees and migrants illegally enter European countries by land or sea, resorting to the services of smugglers, often risking their lives. Since they usually lack the basis for requesting refugee status for illegal entry through a land border, they try to bypass the law and use inappropriate boats across the sea border, with often accidents, threatening to live, creating conditions for refugee status. It should be noted that the business that provides the illegal migration of migrants is ranked third among the activities of criminal organizations, reiterating on efficiency only to the smuggling of drugs and weapons.

Measures are being taken in the EU to curb the activities of criminal groups dealing with smuggling of migrants, which is an integral part of the migration policy implemented in the Union for more than a decade. This way of doing practical implementation of common EU asylum policies based on solidarity and responsibility among EU Member States makes it clear that the Union is not ready to deal with such a huge number of people and to prevent the emerging issues.

For the economies and the countries as a whole the problem of illegal migration remains. As the practice shows in the past 3 years, it should be seen as a factor contributing to: the development of religious extremism, the revival and strengthening of nationalism, the increase of crime, the illicit trafficking of psychotropic and narcotic substances. In addition, members of terrorist organizations who contribute to raising the threat of terrorist acts on the territory of the country of final destination may be infiltrated by illegal immigrants. Of course, the migration flow is not the only cover for penetration, but in general in recent years it has contributed to the movement of fighters, emissaries or candidates for jihadists.

Given the changing migration situation in the world, it is necessary to improve the legislative and institutional framework for regulating migration flows, both at national and European level, in order to identify threats to the territorial integrity of the countries and create preconditions to prevent local socio-economic and political instability. Three levels of migration development in the EU countries and their attitude to the level of national security – geopolitical, economic and demographic – should be distinguished and analyzed. Each of these aspects largely determines the national security of the EU countries.

The geopolitical aspect of the interconnection of migration with national security is addressed in particular in the context of ethnic migration. Thus, in the face of emerging demographic problems, Germany’s indigenous population will probably decrease from 74.6 million in 2000 by 10-15% by 2050, while the number of foreign population will double from 7.4 million in 2000 year. With similar trends in demographic developments in a number of European countries such as Belgium, France, etc., some specialists conclude that an Asian civilization may arise at the place of the European one. Moreover, judging by the latest statistical research, the Arabic factor will not be the leading, but the Asian one.

**Economic aspect.** Associated with legal emigrants, it involves cheap labor but also exports of capital outside the host country. Migrants work in European countries but do not integrate and exist in encapsulated communities. They often do not pay taxes or social security contributions, or pay them only partially, and redirect the earned money to their home countries. Linked to illegal migration, which is almost as large as the legal one, the economic aspect is cumulative damages – a collection of criminal profits, corrupt practices, organized crime gains, and damage from terrorist actions. The European labor market is heavily dependent on the foreign workforce, especially in some types of professions not requiring high qualifications. However, it should be borne in mind that the low level of workers’ training and, accordingly, the quality of work pose a threat to society – construction, various social services, etc. Illegal migration also raises unemployment in the host country. Frequently, the pay of illegal migrants is significantly lower than what local residents receive, so they can not find a job. At the same time, industrial development in the countries requires a fresh influx of labor across borders, including illegal labor. As long as the use of the work of illegal migrants is hidden, states do not receive tax revenues from it. On the other hand, the economy of the host country loses money that economic migrants transfer to their countries of origin.

Finally, the demographic aspect of national security – European countries are experiencing a demographic crisis. This is really a serious problem because of declining fertility rates in Europe. One of the biggest misconceptions in the EU, which our politicians have been involved in, is that migration can solve demographic problems – population decline, aging, etc.

**Illegal migration is a serious threat to national security.** It poses a threat to the vital interests of the person, the society and the state, threats to the territory, values, culture. It is a collection of public relations involving the preparation procedures – individual or with the help of organizations conducting illegal migration – to the illegal movement of a person or persons through the state borders of two or more countries and their more extensive installation, often leading to the acquisition of a new legal status. National security is directly dependent on the political aspects of the illegal migration. As a result of the migration process, the internal integrity of the society, its integrity is eroded. This is particularly noticeable when migrants represent another, non-indigenous culture, religion, way of life.

In order to maintain a high level of national security, a number of active measures should be taken with regard to:

- Migration, migratory procedures and migrants themselves;
- Integrity of organizations monitoring and managing migration-related activities in the EU and individual Member States;
- Strengthening and developing the common European border protection structures.

When the situation calls for an adequate position on migration, the concept of national security is of major importance. Under such a concept, the state has a monopoly of national security and, moreover, the concern for its own territory and ethnic unity is advantageous. It should, by definition, be suspicious of migratory flows crossing the border, and be empowered to decide whether these streams are a real danger and should they regulate them by means of special legislation and measures. Although cross-border migration flows targeting the EU and crossing its borders are usually classified as a low-level threat, they are viewed by analysts as a system component of almost all other threats.

The only way to overcome the contradiction between migrants' rights and national security of European countries is to control the migration in order to transform it into a moderate and
even process, while ensuring dispersal of migrants and taking all kinds of measures the migrants to accept the basic values of host countries.

2. Civil security

After the attack on the twin towers, the situation in the security services sharply changed. Antiterrorism has become a goldfish. From the restrictions and resource constraints after the fall of the iron curtain, only a "bad memory" remained. Then the government decided that the secret services needed a reduction and they took their power and financial resources.

Today, huge funding (over $ 200 billion a year worldwide) and untying the hands of security managers has led to the need to search for a sphere of investment because the cost of new employees is a minimal part of the resource. The high-tech area of secret surveillance and information gathering tools has proven appropriate. High technology is now leading in intelligence, counterintelligence, counter-terrorism, and the work with people is neglected.

After the attack on the twin towers, security services proved to be resourced but lacking human intelligence. High technologies are not a panacea. Of course, it is impossible without them, but their capacity is known to the apologists of terrorist activity, and modern terrorism slides down a low technological plane under the antiterrorist radar. Spending billions on information systems and technology tools for gathering information (often illegal – if we remember the scandal with the "Prism" and before that with "Echelon") rarely leads to significant antiterrorist effect. However, the costs are related to new jobs, employment of the unemployed, successful measures to overcome the economic crisis, development of electronics, huge profits, commissions and preparation of future cozy nests in the private sector for the heads of the special services. This leads to a change in the overall concept of information advantages in the economy – the foundation of powerful systems that collect global corporations securing the logistics of special services. This resource is the foundation of powerful systems that collect global information, practically unrelated to crime and terrorism, but creating prerequisites for information advantages in the economy – espionage.

Overcoming the problem lies in implementing the concept of flexibility and using the overall toolbox of special services. The extensive approach of terrorists should be a counterpoint to a network of information sources located in identified threat areas, prepared to recognize signs of indoctrination, preparation and instigation of terrorism.

What is our readiness to provide a good civil security to meet today's challenges related to terrorism?

There is an analytical basis and prepared plans that fairly correctly allocate rights and obligations within the framework of counter-action. Unfortunately, the available resource is limited within the already chronically low provisioning of the Security sector. At the same time, the experience of the Sarafovo assault and the actions of anti-terrorist and special structures on various occasions in recent years (Lyaskovets, the lack of results in anti-corruption activity) show unreliability. Continuous scandals in the Ministry of Interior and SANS lead to lack of trust among citizens. Without it obtaining information and support counter-terrorism is a lost cause. The latest scandals surrounding the intrigue and conflict in the Specialized Counter-Terrorism Unit – the only tactical anti-terrorist structure in the country – show lack of adequate protection.

It is clear that citizens, prepared in a carefully planned learning activity would be a powerful anti-terrorist factor. In fact, they should be the most motivated because they are the most affected by the terrorist activity. It can certainly be argued that anti-terrorist activity could not be carried out effectively without serious civic participation. In order to realize such an approach, however, confidence in the police and special services must continuously be strengthened and enhanced.

In conclusion, we can state that the related components of national and civil security both in the EU and locally in Bulgaria are subject to serious test. In the light of the forthcoming EU presidency, the need for exceptional and urgent measures for their quality assurance can be considered vital.

We must not forget that the basic concept justifying the consumption of huge financial resources is the proactive, anti-terrorist activity, but it does not take place. A vicious circle is created. Terrorism justifies the allocation and use of a powerful resource that, to a large extent, goes into the hands of private corporations securing the logistics of special services. This resource is the foundation of powerful systems that collect global information, practically unrelated to crime and terrorism, but creating prerequisites for information advantages in the economy – espionage.

After the attack on the twin towers, security services proved to be resourced but lacking human intelligence. High technologies are not a panacea. Of course, it is impossible without them, but their capacity is known to the apologists of terrorist activity, and modern terrorism slides down a low technological plane under the antiterrorist radar. Spending billions on information systems and technology tools for gathering information (often illegal – if we remember the scandal with the "Prism" and before that with "Echelon") rarely leads to significant antiterrorist effect. However, the costs are related to new jobs, employment of the unemployed, successful measures to overcome the economic crisis, development of electronics, huge profits, commissions and preparation of future cozy nests in the private sector for the heads of the special services. Thus, one of the components of today's counter-crime, under the guise of problem securitization, is aimed at realizing socio-economic and political functions – increasing voters' employments, raising salaries, more business orders, etc.

But what happened to the quality of civil security, terrorism and its activities? Have they changed?

Since 9/11, terrorist organizations have been abandoned by their sponsors as a result of international pressure, so they have had to rebuild themselves to finance the most effective approach – through the symbiosis with organized crime. Their real leaders are not the dull, indoctrinated, self-excited shahids, but highly educated and erudite people who have received their education in the most elite world-class schools. Their knowledge of the possibilities of electronic espionage is equal to the employees of the special services. This leads to a change in the overall concept of indoctrination, preparation and implementation of terrorist acts. The transformation is extensive, relying primarily on human resources. Electronic communications are limited. The official bank transfers have been discontinued and replaced by money transfer via couriers or the grand grandmother of the modern banking system – the illegal banking "Havala".

Organizations are horizontally structured, divided into hermetic cells, so breaking one does not affect the system. After the Paris attack, it became clear that they also act for indoctrinating and encouraging unrelated fanatics to carry out isolated attacks, hampering even more the counteraction.

To summarize, on the one hand there are hierarchical (vertical) antiterrorist services relying on high technologies, on the other – horizontal terrorist networks that use minimal modern communication tools and high-tech systems. Obviously, the two types of organizations have difficulty reaching out to the point of contact that could lead to an anti-terrorism effect. So the only cross point is the already committed terrorist act.
ELEMENTS OF THEORY TO SOLVE THE PROBLEM OF MANAGEMENT OF TRANSPORT SAFETY

L.N. Elisov, N.I. Ovchenkov

Authors’ original problem-solution-approach concerning aviation security management in civil aviation applying parallel calculation processes’ method and neural computers’ usage is considered in this paper. Problem statement by setting secure environment simulation tasks for grid models, and neural networks’ usage is presented. The research subject area of this paper is airport services in civil aviation, considered from the point of view of aviation security, defined as the state of aviation security against unlawful interference into the aviation field. The key issue in this subject area is aviation safety provision at an acceptable level. In this case, airport security level management becomes one of the main objectives of aviation security. Aviation security management is the organizational regulations in modern systems that can no longer correspond to changing and increasingly complex requirements determined by factors of external and internal environment, associated with a set of potential threats to airport activity. Optimal control requires the most accurate identification of management parameters and their quantitative assessment. The authors examine the possibility of applying mathematical methods for processes and procedures’ security management modeling in their latest works. Parallel computing methods and network neurocomputing for modeling control processes of airport security are examined in this paper. It is shown that the methods’ practical application is most effective in the decision support system, where the decision maker plays a leading role. Decision support system on the aviation safety management should include risk assessment subsystem of adverse events.

Keywords: aviation security, boundary value problem, differential equations in partial derivatives, grid model, neural network.

1. The linguistic problem statement.

Aviation security is considered as the object’s security state [1,2]. Such the state occurs as a result of the confrontation of two systems that are physically implemented: threats’ systems and protection systems. This protection status is not physically implemented concept; it means that it is an imaginary concept. Lacan [3] proposed a fairly clear way for the study of such concepts: imaginary and symbolic - real. Security state is estimated with the help of vulnerability concept that answers to the following question: to what extent the subject meets the safety requirements. In this case, it is entitled to introduce the Lacan [3] proposed a fairly clear way for the study of such implemented concept; it means that it is an imaginary concept. and protection systems. This protection status is not physically implemented concept; it means that it is an imaginary concept. Lacan [3] proposed a fairly clear way for the study of such concepts: imaginary and symbolic - real. Security state is estimated with the help of vulnerability concept that answers to the following question: to what extent the subject meets the safety requirements. In this case, it is entitled to introduce the concept of “protection quality”, that is understood as degree of conformity to characteristics and requirements. It has the symbolic representation and, moreover, the quality can be measured [4]. Security is provided by a set of tools (mainly technical), each of which creates a separate object protection fragment, and together form the security environment. It can be represented as a security field, which is characterized by such a parameter as quality. In this case, the field is a real concept that can be studied with the help of a specific mathematical apparatus technique. Then target security management functionality includes the parameters of the object protection field, measured as the quality of the technical means to ensure aviation security. The analysis shows that a formal description of the object protection field can be represented in the format of the boundary value problem at a first approximation.


In the paper [2] the authors showed the fundamental possibility of solving aviation security management tasks as the solution of the boundary value problems described by the system of differential equations in partial derivatives. The statement of such the problem in the modeling of neural networks is presented below. It requires a finite-difference approximation of the original equation; it means replacing the field of continuous variation of the argument to its discrete area (grid) and replacing the differential operator to some difference ones, as well as replacement of difference analogues to boundary conditions, resulting in a system of algebraic equations.

Let us consider the finite-difference approximation of the Dirichlet problem for two-dimensional equation of elliptic type

\[
\frac{\partial}{\partial x} \left( \sigma(x,y) \frac{\partial u}{\partial x} \right) + \frac{\partial}{\partial y} \left( \sigma(x,y) \frac{\partial u}{\partial y} \right) = f(x,y), \quad (x,y) \in S,
\]

(1)

called net domain \(\Gamma\). Nodes that are nearest to the borderline are called border-straddling nodes.

Instead of functions \(u(x,y)\) of continuous arguments \(x,y \in S\) let us consider grid functions \(u_h(x_j,y_j)\) of grid points. Given a linear differential operator \(L\), related to function \(u\), then, changing included into \(Lu\) derivatives differential relationships, we will receive difference expression \(L_h U_h\) that is a linear combination of meanings of grid functions \(u_h\) on some multitude of grid steps that is called stencil. That is the template specifies a set of grid points included into the differential expression

\[
(L_h U_h)_{ij} = \sum_{x_k \in X(x_j)} A_{ij}(x_j, x_k) u_h(x_k),
\]

where \(A_{ij}(x_j, x_k)\) – coefficients, \(h\) – a grid step, \(N(x_j)\) – pattern in the grid \(X_j\). Such an interchange is called difference approximation of operator \(L\).
Using the integro-interpolation method and the five-point stencil, let us write difference approximation of the equation (1) for an internal node

\[
\begin{align*}
\frac{\sigma(x_i + h/2, y_j) + \sigma(x_i - h/2, y_j) + \sigma(x_i, y_j + h/2) + \sigma(x_i, y_j - h/2)}{h^2} u_{i,j} + \\
\frac{\sigma(x_i + h/2, y_j) + \sigma(x_i - h/2, y_j) + \sigma(x_i, y_j + h/2) + \sigma(x_i, y_j - h/2)}{h^2} u_{i+1,j} + \\
\frac{\sigma(x_i, y_j + h/2) + \sigma(x_i, y_j - h/2)}{h^2} u_{i,j+1} + \\
\frac{\sigma(x_i, y_j - h/2)}{h^2} u_{i,j-1} = f(x_i, y_j), \ (x_i, y_j) \in S_h
\end{align*}
\]

or

\[
a_{i,j} u_{i,j} - a_{i+1,j} u_{i+1,j} - a_{i-1,j} u_{i-1,j} - a_{i,j+1} u_{i,j+1} - a_{i,j-1} u_{i,j-1} = -f_{i,j},
\]

where

\[
a_{i,j} = \frac{\sigma(x_i + h/2, y_j) + \sigma(x_i - h/2, y_j) + \sigma(x_i, y_j + h/2) + \sigma(x_i, y_j - h/2)}{h^2},
\]

\[
a_{i+1,j} = \frac{\sigma(x_i + h/2, y_j)}{h^2}, \quad a_{i-1,j} = \frac{\sigma(x_i - h/2, y_j)}{h^2}, \quad a_{i,j+1} = \frac{\sigma(x_i, y_j + h/2)}{h^2},
\]

\[
a_{i,j-1} = \frac{\sigma(x_i, y_j - h/2)}{h^2}, \quad f_{i,j} = f(x_i, y_j), \ (x_i, y_j) \in S_h.
\]

Writing down the equation (3) for each node, where grid function is unknown, taking into account boundary conditions and moving all the known terms into the right side, we obtain a system of algebraic differential equations. In the case of the Dirichlet problem, the solution is sought only in internal nodes, the conditions (4) are taken into account in the differential equations of the form (3). In order to write down a system of difference equations in matrix form we number nodes of the grid area, where the solution is sought. In the case of lexicographical ordering nodes are numbered after successively along the lines of the grid area. In accordance with the ordering, grid functions can be combined into a vector \( \mathbf{X} \). Writing equation (3) in the order of the nodes and moving the known boundary conditions of the members to the right side, we find a record of the system of difference equations in the matrix form

\[
\mathbf{A} \mathbf{X} = \mathbf{F}
\]

In the case of two-dimensional equations the matrix \( \mathbf{A} \) has a block-tridiagonal structure

\[
\mathbf{A} = \begin{bmatrix}
T_1 & D_1 & 0 & 0 \\
D_1 & T_2 & D_2 & 0 \\
0 & D_2 & T_3 & 0 \\
0 & 0 & 0 & \ldots
\end{bmatrix}
\]

where \( T_i \ (i = 1, 2, \ldots, n) \) – square three-diagonal matrix, structures (6) and describing a two-dimensional grid line, \( D_1 \) – diagonal matrix.

In the case of three-dimensional equation and numbering nodes on layers of grid we obtain block tridiagonal matrix structure (7), wherein the diagonal blocks are of the form (7) and describe the single layer grid.

2. Final element analysis (FEA)

Final element analysis (FEA) consists in solution domain partition \( \Omega \) into set of nonintersecting subfields \( \Omega^e \) – finite elements (FE). Within each FE desired solution is approximated by a piecewise continuous function, usually a polynomial. The coefficients of this polynomial are expressed through advance unknown meanings of the required function at certain points of FE, called grid nodes of finite elements. The unknown nodal parameters are found, using an integrated problem formulation. Let us consider the basic steps of solving boundary value problems by finite element analysis [6].
Solution region is divided into **finite elements** as a preliminary. Triangular or rectangular finite elements are commonly used for two-dimensional problems, tetrahedrons, parallelepipeds and straight triangular prisms - for three-dimensional problems. Automatic generation of finite element grids and dividing into finite elements is an actual and extensive area [7,8].

**Approximating elements’ function** is determined. It is necessary to solve the problem of the approximate representation of the desired decision function through the meanings of the function at the nodes in each individual finite element. Lagrange finite elements are the most commonly used, using only the values of the function at the nodes. The approximated function is a polynomial interpolation of Lagrange in Lagrange elements. For Lagrange finite element meaning of function of decision \( \Phi^{(e)} \) in arbitrary point of \( e \)-th of finite element is approximated by a polynomial

\[
\Phi^{(e)} = A^{(e)} \mathbf{R} + a_0,
\]

where \( A^{(e)} \) - vector line polynomial coefficients; \( a_0 \) - constant term, \( \mathbf{R} = (x, y, z) \) - vector of coordinates of the considered point of the finite element.

In order to determine vector \( A^{(e)} \) and a constant term \( a_0 \) the condition of continuity of the desired function in the element nodes is used. Substituting the coordinates of element nodes and unknown meanings of the function at the nodes, we obtain the equations’ system

\[
X^{(e)} A^{(e)T} + A_0 = \Phi^{(e)},
\]

where \( A^{(e)} \) - vector of nodal values of the function for \( e \)-th of finite element, \( X^{(e)} \) - matrix of coordinates of element nodes, for example, for two-dimensional triangular elements Sim-Plex

\[
X^{(e)} = \begin{bmatrix}
x_i & y_i \\
x_j & y_j \\
x_k & y_k
\end{bmatrix},
\]

\( i, j, k \) - number of nodes (nodes are numbered, starting with an arbitrary node, moving counter-clockwise); \( A^{(e)T} \) - conjugate vector \( A^{(e)} \); \( A_0 \) - vector whose elements are all equal to \( a_0 \).

Solving systems (8), let us find vector \( A^{(e)} \), it means expressing the coefficients of the coordinates of the element nodes and unknown values of the function at the nodes (vector \( \Phi^{(e)} \)). Substituting vector \( A^{(e)} \), we receive

\[
\Phi^{(e)} = N^{(e)T} \Phi^{(e)},
\]

where \( N^{(e)T} \) - row vector, elements of which are called functions of forms of finite elements.

**The vector of nodal meanings of the function** is determined. Two main methods are used to solve this problem: a method based on the variational formulation of the problem, and Galerkin method [8].

Thus, the method of finite differences using regular grids is the easiest one to be implemented in a neural network basis. Cellular neural networks are perspective for solving the system-difference-equations approximating the differential equations in partial derivatives. More complex, but also very promising is the neural network implementation of the finite element method and an important part of this method - the problem of constructing an optimal finite difference grids.

When solving systems of equations that approximate the direct problems, the parameters of such neuro-networks are known in advance and must comply with the parameters of approximation. In the paper [9] such a network is called **formed neural networks**. Such networks can be called **networks of direct analogy** by analogy to models of direct analogy. It is necessary to respect the basic provisions of the theory of similarity when calculating parameters of such networks.

3. **Solution of boundary value problems on neural networks**

Solution of boundary value problems in the neural networks are built in accordance with the general method of solving **mathematical problems in neural network logical basis** [5,10], which comprises the following steps: a mathematical statement of the problem; geometric statement of the problem; neural network statement of the problem.

When solving systems of linear equations the realization is reduced to the implementation of instructions of the neural network structure defined by a mathematical formulation of the problem. Formed in such a way networks are called **formed neural networks**. Such networks can be called **networks of direct analogy** as well by analogy to models of direct analogy.

The structure of the neural networks for solving systems of linear algebraic equations is built on the basis of the chosen energy function (optimization of the functional or functional errors). The energy function must be selected in such a way that its minimum is reached on the exact solution of \( X^* \) system of linear algebraic equations. Differentiation of the energy function makes it possible to convert the problem of minimization to the system of ordinary differential equations. Analog neural network with continuous presentation time should be described by the resulting system of ordinary differential equations; it means neural network is an analog circuit for solving the resulting method described a system of ordinary differential equations. It is necessary to replace the differential equations to difference ones to construct a network operating in discrete time.

Let us consider the analog neural networks for solving systems of differential equations of the form based on the model of **continuous Hopfield network** [10]. Every \( i \)-th neuron is described by the ordinary differential equation

\[
c_i \frac{dU_i}{dt} = -g_{ii} U_i + \sum_{j \neq i} g_{ij} f(U_j) + I_i,
\]

Where \( U_i \) - input (status) of \( i \)-th neuron, \( C_i \) - input capacitance of neuron, \( g_{ij} \) - elements of the matrix connections, or synaptic weight (\( g_{ij} \) - conductivity connecting the output of \( j \)-th neuron with input of \( i \)-th), \( f(U_j) \) - activation function (continuous monotonically increasing linear function of the input \( U_j \)), \( I_i \) - input current (bias neuron) \( g_{ii} = \rho_i^{-1} + \sum_j g_{ij} \), \( \rho_i \) - input impedance of \( i \)-th amplifier (for modern amplifiers can be taken \( \rho_i = \infty \)).

Classically understood fully connected network, it means each neuron is associated with each other (in the expression (9) \( i, j = 1, 2, ..., n \), where \( n \) the number of neurons in the network).

Let us write the system (9) in a matrix form

\[
\mathbf{C} \frac{d}{dt} \mathbf{U} = -\mathbf{D} \mathbf{U} + \mathbf{T} f(\mathbf{U}) + \mathbf{I},
\]

where \( \mathbf{U} \) - vector network status, \( \mathbf{D} = \text{diag}(g_{11}, g_{22}, g_{33}, ..., g_{nn}) \) - diagonal matrix, \( \mathbf{T} \) - matrix of links of the outputs and inputs of neurons (
\[ T_{ii} = 0, \quad T_{ij} = g_{ij}, \quad f(U) \] vector activation function of neurons, \( I \) – vector of external neurons’ inputs (displacement), \( C \) – diagonal matrix of input neurons’ capacitances.

The solution of differential equations of the form will be sought in the state class-asymptotic asymptotically stable equilibrium neural network, described by a system of ordinary differential equations, (10). Neural network parameters must be set so that the point of asymptotically stable equilibrium of the network coincides with the solution system.

Attention is necessary to be drawn to usage of the theory of similarity, which serves as the basis for the choice of the scale. Scaling is a mandatory step when under-preparation of the problem to the solution of an analog computer, the correct choice of scale does not only establishes the correspondence between the mathematical model and analog circuitry, but makes it possible to reduce the modeling error as well.

In the paper [10] Hopfield network is proposed and studied for solving linear algebraic equations of a standard form. A linear function of activation is used \( f(u_{ij}) = -u_{ij}, \ C = E, \) where \( E \) – identity matrix. Neural network parameters are selected in the following way:

\[ D_{ii} = a_{ii}^2, \quad T_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj}, \quad T_{ii} = 0, \quad I_{i} = \sum_{k=1}^{n} a_{ki} F_{i}, \]

(11)

Given a linear activation function, and (11), the system (10) takes the form

\[ \frac{d}{dt} U = -A^T A U + A^T F. \] (12)

From the theory of solving systems of linear algebraic equations on analog computation-influential-machines it is known that the system

\[ \frac{d}{dt} U = -A U + F \]

has a sustainable solution, if the matrix \( A \) is a positive definite.

Matrix \( A^T A \) is symmetric definite positive, which ensures stability of the solution.


\[ H(U) = \frac{1}{2} (R, R) = \frac{1}{2} R^T R. \]

Where \( R = F - A U \) – nullity vector.

4. Concerning research’s margin of errors

The proposed mathematical approach for solving airport security’s aviation management tasks cannot be attributed to the class of simple tasks. At the mathematical formalization of the researcher is faced with many challenges. The key ones are the following:

- Considerable uncertainty in the linguistic description of the subject area,
- Methodological difficulties in finding adequate mathematical apparatus for formalization,
- Multicriterionality of the solved problem, defined by a high order matrix-criteria optimization of management, whose elements correspond to a plurality of types of object’s technical protection,
- The inevitable inadequacy of any of the proposed models, including the format of boundary value problem resulting from the ambiguity of the conceptual apparatus,
- Difficulties in setting the boundary and initial conditions associated with indeterminacy of source information,

- Practically insurmountable complexity of the study of the dynamics of control processes aviation security, since the introduction of the time factor into the model leads to uncontrolled growth of the complexity of the mathematical apparatus, or transforms the task into the class of NP-complex tasks without any solution.

It follows that the proposed approach concerning aviation security management does not provide accurate, even relatively accurate, solution.

However, the terms of the practical usage of the proposed approach to aviation security management do not require an exact solution taking into account the following circumstances:

- Absolute security does not exist; it can be only strived for, what is meant here is an acceptable level of aviation security,
- The quality, the quantitative value of which is determined by their qualitative (expert) methods, initially giving an approximation of (subjective) assessment is a controlled object protection field’s parameter,
- An actuator in the security management system is the ergatic, where the decision maker plays the key role.

Thus, the question of the margin of errors of the proposed approach is practically removed. It should be noted, however, that in this case aviation security control procedures should be complemented by risk assessment procedures occurrence negative events, which should be adequately integrated into the overall control scheme.

Conclusion

1. An approach to the modeling of management processes of aviation airport security in civil aviation is proposed, based on a usage of parallel computing processes and neuro-computers and presentation of the field of object protection in the format of a boundary value problem.
2. Practical application of the method is most effectively in supporting decision-making systems, where the leading role is given to the decision-makers.
3. The system of decision support for the management of aviation security should include risk assessment subsystem of occurrence of negative events.

REFERENCES

APPLICATION OF MOBILE GISERVICES IN DISASTER MANAGEMENT

Assos. Prof. Milen Ivanov PhD, Yavor Yankov PhD
NMU „Vassil Levski” Veliko Tarnovo, Bulgaria
e-mail milen_i1970@abv.bg
e-mail yavorchoo@yahoo.com

ПРИЛОЖЕНИЕ НА МОБИЛНИ ГЕОГРАФСКИ ИНФОРМАЦИОННИ СИСТЕМИ ПРИ УПРАВЛЕНИЕ НА ПРИРОДНИ БЕДСТВИЯ

Доц. д-р Иванов М. , д-р Янков Я.
Факултет „Общовойскови” – НВУ „Васил Левски” Велико Търново, Република България

Abstract: Increasing data heterogeneity, fragmentation and volume, coupled with complex connections among specialists in disaster response, mitigation, and recovery situations demand new approaches for information technology to support crisis management. Advances in GIServices show promise to support time-sensitive collaboration, analytical reasoning, problem solving and decision making for crisis management. Furthermore, as all crises have geospatial components, crisis management tools need to include geospatial data representation and support for geographic contextualization of location-specific decision-making throughout the crisis. This paper provides introduction and description of Mobile GIServices applied to crisis management activity. The goal of Mobile GIServices in this context is to support situational awareness, problem solving, and decision making using highly interactive, visual environments that integrate multiple data sources that include georeferencing.

Key words: DISASTER INFORMATION, NATURAL HAZARDS, GEOINFORMATION TECHNOLOGY, LOCATION-BASED SERVICES, MOBILE GIS, GLOBAL POSITION SYSTEMS.

1. Introduction

Present world is described with high speed and broad spatial range of changes, together with complex interdependences between running processes. This puts a lot of challenges for timeliness, accuracy and high quality about decisions and actions. Essential for implementation of these requirements must be Geographic information systems with incorporate Mobile technologies.

To meet the challenges of complex crisis management situations, new interactive visualization tools are in development to deal with large, complex datasets and similarly large and complicated analytical tasks. These systems must help enable connections between response, mitigation, and recovery specialists in disaster situations. Recent crises have revealed the need for visualization tools to support time-sensitive collaboration, analytical reasoning, problem solving and decision making in analysis, planning and time-sensitive response activities [1]. As almost all crisis management activity contains a geospatial component, these activities will necessarily include geospatial data.

To create a comprehensive disaster management system, our society needs to rely on advanced geospatial technologies and services [Ivanov M., Yankov Y., 2016 a]. Mobile GIS is one of the most vital technologies for the future development of disaster management systems. Mobile GIS and mobile Geographic Information Services (Mobile GIServices) extend the capability of traditional GIS to a higher level of portability, usability and flexibility. Mobile GIS are integrated software and hardware frameworks for access to geospatial data and services through mobile devices via wireline or wireless networks [8]. The unique feature of mobile GIS is the ability to Dynamic and Mobile GIS: investigating changes in space and time incorporate Global Positioning Systems (GPS) and ground-truth measurement within GIS applications.

This article introduces a new term, “Mobile GIServices”, which describes a framework to utilize Mobile GIS devices to access network-based geospatial information services (GIServices). Mobile GIServices can be adopted in various GIS applications and scenarios, including car navigation systems, utility management, environmental monitoring and habitat protection tasks. Disaster management and emergency response are one of the most popular domains in the recent development of Mobile GIServices.

For example, mobile GIServices can combine GPS and satellite images to assist the local government and emergency response teams in identifying potential threat areas. So critical “hot zones” can be immediately created. Near real-time spatial analysis models supported by GIS could be used to rapidly generate the most effective evacuation routes and emergency plans during natural hazard events, including wildfires, floods and tsunamis. Wireless Internet-based GIS could also assist public policy officials, firefighters and other first responders with identifying areas to which their forces and resources should be dispatched. To accomplish these goals, it is important to introduce these new mobile GIServices technologies to emergency management personnel and related organizations. Also, emergency managers and first responders need to realize both the advantages and the limitation of GIS technologies in disaster management.

2. Performance of mobile GIS

Mobile GIS is the expansion of GIS technology from the office into the field. A mobile GIS enables field-based personnel to capture, store, update, manipulate, analyze, and display
geographic information. Mobile GIS integrates one or more of the following technologies:

- Mobile devices
- Global positioning system (GPS)
- Wireless communications for Internet GIS access

Traditionally, the processes of field data collection and editing have been time consuming and error prone. Geographic data has traveled into the field in the form of paper maps. Field edits were performed using sketches and notes on paper maps and forms. Once back in the office, these field edits were deciphered and manually entered into the GIS database. The result was that GIS data has often not been as up-to-date or accurate as it could have been.

Edits were performed using sketches and notes on paper maps. Field data has traveled into the field in the form of paper maps. Field editing have been time consuming and error prone. Geographic information. Mobile GIS integrates one or more of the following technologies:

- Mobile devices
- Global positioning system (GPS)
- Wireless communications for Internet GIS access

Traditionally, the processes of field data collection and editing have been time consuming and error prone. Geographic data has traveled into the field in the form of paper maps. Field edits were performed using sketches and notes on paper maps and forms. Once back in the office, these field edits were deciphered and manually entered into the GIS database. The result was that GIS data has often not been as up-to-date or accurate as it could have been.

Edits were performed using sketches and notes on paper maps. Field data has traveled into the field in the form of paper maps. Field editing have been time consuming and error prone. Geographic information. Mobile GIS integrates one or more of the following technologies:

- Mobile devices
- Global positioning system (GPS)
- Wireless communications for Internet GIS access

Traditionally, the processes of field data collection and editing have been time consuming and error prone. Geographic data has traveled into the field in the form of paper maps. Field edits were performed using sketches and notes on paper maps and forms. Once back in the office, these field edits were deciphered and manually entered into the GIS database. The result was that GIS data has often not been as up-to-date or accurate as it could have been.

Figure 1 Using traditional GIS and Mobile GIS services.

Changes in wireless communications have enabled GIS to be taken into the field as digital maps on compact, mobile computers, providing field access to enterprise geographic information. This enables organizations to add real-time information to their database and applications, speed up analysis, display, and decision making by using up-to-date, more accurate spatial data. Firefighters, police officers, engineering crews, surveyors, utility workers, soldiers, census workers, field biologists, and others, use mobile GIS to complete the following tasks:

- Field mapping - create, edit, and use GIS maps in the field;
- Asset inventories - create and maintain an inventory of asset locations and attribute information;
- Asset maintenance - update asset location and condition and schedule maintenance;
- Inspections - maintain digital records and locations of field assets for legal code compliance and ticketing;
- Incident reporting - document the location and circumstances of incidents and events for further action or reporting;
- GIS analysis and decision making - perform measuring, buffering, geoprocessing, and other GIS analysis while in the field. For details see Appendix №1.

The term "Mobile GIS" can be defined as an integrated software/hardware framework for access to spatial data and services through mobile devices via wireline or wireless networks."Wireless GIS" is a subcategory of mobile GIS technology that focuses on the wireless networking capability of mobile GIS services. There are two major application areas of mobile GIS:

1. Field-based GIS, which focuses on GIS data collection, validation and update (spatial and attribute).
2. Location-based services (LBS), which focus on business-oriented location management functions, such as navigation, street routing, finding a specific location or tracking a vehicle.

3. Architecture of mobile GIS

The architecture of mobile GIS is very similar to that of Internet-based GIS, using a client-server architecture. Client-server applications usually implement what is referred to as a Three Tiered Architecture. This architecture divides the application into a presentation tier, a business logic tier and a data management tier. Each tier can be replaced or updated without affecting the others. The presentation tier consists of client side components which are used to send requests to the server and to view the results (maps and data). The business tier is the core of any solution and consists of the server side components including the Web server and application server. The data management tier is responsible for the management of both spatial and attribute data in the application. In some cases, one server is used for both the business and the data management tier. In other cases each tier can be on a separate server.

Applications that use LBS are limited only by developer's imagination, but there are some categories where need opportunities have been clearly identified:

1. Mapping, navigation and directions applications;
2. Emergency services;
3. "Finder" applications that use the user's location to help locate something;
4. Location-based reminder applications that prompt users when they reach particular locations.

Major LBS Technologies

LBS is mobile computing anywhere, anytime. In practice, it represents the merger of four technologies: Personal Digital Assistants (PDAs) and 3G (3rd generation) mobile phones; location acquisition (automatic or manual); wireless Internet technology and infrastructure; and GIS solutions for wireless (data and application).

Location Acquisition

For applications to become location-aware, the wireless network must trace the location of the wireless device. This can be done either automatically, or manually. Automatic location acquisition uses a positioning network to locate a device using technologies such as a GPS or cellular base stations.

Each of these automatic positioning technologies has its advantages and disadvantages. Cellular base stations are ubiquitous across most urbanized areas, but their positioning is not precise enough to accurately locate a user (accuracy within tens to hundreds of meters). In contrast, GPS can be extremely precise (accuracy within meters), but in some cases the signal is obscured inside buildings and in areas with high traffic, narrow streets and high rise buildings.

Applications can be designed to enable quick manual inputs for location acquisition. These include using landmarks, stored locations or addresses and Zip codes.
5. The potential of WebGIS

More attention has been focused on developing GIS functionality in the Internet, Worldwide Web, and private intranets (sometimes termed WebGIS) recently:

- WebGIS holds the potential to make distributed geographic information (DGI) available to a very large worldwide audience.
- Internet users will be able to access GIS applications from their browsers without purchasing proprietary GIS software.
- WebGIS will make it possible to add GIS functionality to a wide range of network-based applications in business, government, and education. Many of these applications will be run on intranets within businesses and government agencies as a means of distributing and using geospatial data.
- Many experiments are now underway in WebGIS and related mapserver applications for interactive cartography. One of the important areas of innovation involves "pay-for-use" mapping and GIS services.

The challenge of WebGIS lies in creating software systems that are platform independent and run on open TCP/IP-based networks, that is on any computer capable of connecting to the Internet (or any TCP/IP-based network) and running a Web browser. This task is different from running proprietary GIS software over local-area networks (LANs) or intranets on just a few types of computer hardware. Such systems already exist. Many strategies can be employed to add GIS functionality to the Web:

- Server-side strategies allow users (clients) to submit requests for data and analysis to a Web server. The server processes the requests and returns data or a solution to the remote client.
- Client-side strategies allow the users to perform some data manipulation and analysis locally on their own machines.
- Server and client processes can be combined in hybrid strategies that optimize performance and meet special user needs.

Developers can program their applications from scratch or now, more commonly, purchase the necessary GIS modules from commercial vendors. The visual design of the WebGIS interface, though not discussed in this unit, requires great care to assure that users can understand and make use of the information and functions provided by the system.

Although software usage has increased in the last few years, some emergency managers and staff are still reluctant to adopt computers and GIS for their main tasks (based on the authors' own experiences). One of the major obstacles is the concern for system portability and reliability. Traditional GIS are not considered portable by first responders (such as local police officers, fire fighters and emergency medical personnel who can arrive first and take actions to rescue people and protect property) [Ivanov M., Yankov Y., 2016 b]. Emergency managers are also worried that loss of electrical power during a disaster might cause the whole computer system to break down. Recent development of Mobile GIS and Mobile GIServices might solve these problems by providing their own independent power supply systems (batteries and Uninterruptible Power Supply - UPS) and having a great portability (cellular phones, Pocket PCs, etc.).

6. Online GIS

After its introduction, the Internet has been widely adopted and has experienced an enormous growth. Therefore, it has become a very important information and service dissemination medium for many companies. Nowadays GIS functionality has been implemented and is being offered on many sites over the Internet, so some authors have coined the term ‘Online GIS’ [8] to call this new way of working with GIS.

Most of the existing Online GIS systems are either spatial query systems (publishing of datasets with a viewing interface and some predefined GIS functionality), or map-building programs [10]. These sites offer mainly viewing and exploring capabilities and are therefore intended for the general public and do not offer actual GIS analysis or processing tools. And when they do, they can only be applied on predefined datasets, not on the user’s datasets. Therefore, Online GIS still cannot make general GIS analysis tools available, so more specialised GIS users that need to perform analytical or specialised tasks, can make use of these components and integrate them in chains to analyse their data. This is the issue on which the present research concentrates.

To have GIS components residing at different locations across the network would allow thousands of potential new ‘online users’ to access them. But this also sets the need for brokers who can control and coordinate the flow components to the clients [6]. Under a GIS components implementation the users would only pay for the few functions they need to use instead of buying complete GIS software licenses. They would be able to pick the GIS functions that better fit their requirements (robustness, price, data formats, etc.) from different providers as they require them [10]. The chosen components would be sent to their web browsers, without needing to locally install software. A well-developed implementation of this kind will allow the seamless integration of data and GIS functions, and the access to GIS by many new non-expert users who will only need to be connected to the Internet. Additionally, the approach of ‘Online GIS’ appears to be very appropriate for the actual topology of GIS projects which have moved from being stand-alone projects to multi-agency, multi-disciplinary and multi-software ones[10].

7. Conclusion

Disaster management is a complex domain of human activity involving multiple agencies and stakeholders, a collaborative approach utilizing state-of-the-art Mobile GIServices that can facilitate a comprehensive and functional disaster management plan. Many emergency tasks and disaster management works will need advanced GIS analysis functions that require significant computing power and computer memory. Most mobile GIS devices are tiny and only have very limited computing capability. The pre-processing and post-processing time for spatial analysis and remote sensing images might prevent the adoption of Mobile GIServices for real-time response tasks due to the hardware limitations. One possible solution is to send the complicated GIS model and spatial functions via the Internet to remote GIS engine services. Then, the analysis results will be sent back to the Mobile GIS devices via the network.

With recent advances of GIS technology, it is now possible to map and determine the risks (together with their magnitude) of different natural hazards and man-made catastrophes. Very large amounts of data can be processed, quantified and displayed on digital maps, allowing decision makers to assess the situation rapidly and take appropriate actions.

The use of advanced tools for computation and modelling of natural hazards such as floods can be combined with a GIS that has the capability of decision support and advanced visualization to produce the models that will represent the risks of natural hazards and man-made disasters in the form of risk maps, where
the risks are categorized and quantified. Furthermore, we have shown that these processes can be automated, enabling near real-time access to the risk maps. This can greatly help decision-makers with the emergency measures and mitigation in most of the cases. What is more, their significance for decision-making and risk prevention can be evaluated for future real-life situations.

Appendix №1

Mobile GIS Application Areas and Crises Management

<table>
<thead>
<tr>
<th>Task</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Mapping</td>
<td>Government: Recording Building Footprints, Right-of-Way Mapping, Based mapping</td>
</tr>
<tr>
<td></td>
<td>Utility and Infrastructure: Centerline Review and Mapping, Facility Mapping</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td>Environment: Forest Boundary Mapping, Trail Mapping, Geochemical Mapping, Volcanic Deposit Mapping, Wetlands Delineation</td>
</tr>
<tr>
<td></td>
<td>Public Safety: 911 Address Mapping, Minefield Mapping, Military Fieldwork and Mapping</td>
</tr>
<tr>
<td>Asset Maintenance</td>
<td>Government: Road Condition Survey, Streetlight Survey, Patient Registration</td>
</tr>
<tr>
<td></td>
<td>Utility and Infrastructure: Power Pole Maintenance, New Equipment Installation, Routine Condition Assessment</td>
</tr>
<tr>
<td></td>
<td>Environment: Crop Management, Vacant Land Condition Management, Timber Harvest Management, Drainage System Management</td>
</tr>
<tr>
<td></td>
<td>Public Safety: Locating Buried Infrastructure, Recording Avalanche Observations, Facility Maintenance Survey</td>
</tr>
<tr>
<td>Inspections</td>
<td>Government: Road Pavement Management, Code Enforcement, Health Inspection, Housing Condition, Water Rights Enforcement</td>
</tr>
<tr>
<td></td>
<td>Utility and Infrastructure: Meter Reading, Septic System Inspection, Documentation, Compliance Monitoring, Dam Safety Inspection</td>
</tr>
<tr>
<td></td>
<td>Environment: Habitat Studies, Wood Abatement, Well Sampling, Wildfire Sightings</td>
</tr>
<tr>
<td></td>
<td>Public Safety: Damage Inspection, Tracking Violations, Street Sign Inspection, Flood Risk Assessment</td>
</tr>
<tr>
<td>Incident Reporting</td>
<td>Government: West Nile Virus Incidents, Public Nuisance Surveys</td>
</tr>
<tr>
<td></td>
<td>Utility and Infrastructure: Locating Outages, Regulatory Compliance</td>
</tr>
<tr>
<td></td>
<td>Environment: Animal Migration Tracking, Oil Spill Assessment, Radiative Contamination Tracking</td>
</tr>
<tr>
<td></td>
<td>Public Safety: Property Damage Assessment, Accident Reporting</td>
</tr>
<tr>
<td>GIS Analysis</td>
<td>Government: GIS Data Validation, Routing to Locations, Property Records Management</td>
</tr>
<tr>
<td></td>
<td>Utility and Infrastructure: Locating Customers for Meter Reading and Billing, Routing to Locations, Trading Network Outages</td>
</tr>
<tr>
<td></td>
<td>Environment: Agricultural Statistics, Vegetation Boundary Validation</td>
</tr>
<tr>
<td></td>
<td>Public Safety: Locating Customer Address for Investigations, Emergency Identification of Affected Areas, Navigating to Accident Locations</td>
</tr>
</tbody>
</table>

**Literature**

7. MC 296/1 NATO Geospatial Policy, 2006.
12. www.isaca.org
1. Introduction. Increasing of production and usage of polymers continually raise their wastes amount. The latest research of the world market of plastic package consumption, carried by company Smithers Pira shows that its world production was 16,7 million in 2015 with the annual gain in 3,8%. As a result, the consumption of plastic will increase by 4,8% up to 15,5 million tons in 2016. During the next 5 years, the consumption is believed to be 21,1 million tons in 2021, with annual increasing by 3,8%. Despite economic factors, increasing in plastic package consumption remains stable [1]. We predict more intensive increasing of consumption in 2016 mostly due to increasing of bottled water usage rate and decreasing of PET resins price as well. This process is provided by regions where glass and metal package for milk, juice, beer and wine continuously replaced by plastic one. Creating of waste less ecological-friendly technology based on mechanic recycling of polymeric waste and material containing polymeric waste is one of the most actual and safe ways of waste processing.

2. Preconditions and means for resolving the problem. It's known that synthetic fibers have low wettability and consequently bad adhesion with cement stone (fig. 1). Adhesion of filling agent and cement stone has a determinative influence on physical-mechanical properties of concrete. Adhesion is caused by close attachment and joining of cement stone with the filling agent which is achieved due to a rough surface of the filling agent. The best attachment and joining have the filling agents with different hooks on their surface and so on [3, 4]. In response to the problem of adhesion between polymers and cement matrix, it's necessary to create conditions of growing of cement matrix crystals on the surface of the polymeric filling agent. Towards the solution of this problem, we suggest milled polymeric wastes were mechanically activated in a specially made device [5]. Conducted experimental research proved correctness and efficiency of that choice.

Solution of the examined problem. In order to solve the set problem, we conduct several experimental pieces of research for obtaining concrete mixtures filled with polymeric wastes which will meet requirements of Union State Standards specifically adhesion with cement stone, compressive strength and flexural strength, durability, convenience laying, hardening rate.

Researches were carried out with the usage of polymeric wastes. During experiments, the following parameters were changed: proportions of filling agents in the mixtures, type of polymeric filling agent (mechanically activated). Our aim was to achieve an optimal composition of cement mixtures and appropriate limits of polymeric wastes addition without deteriorating of concrete physical and chemical properties. For obtaining of polymeric filled cement mixture it's necessary to mix previously milled and mechanically activated polymeric wastes with adding of cement, sand and water.

The composition of experimental samples: cement-sand-water (3:1:0.4), the polymeric filling agent from 1-15% from a total sand mass. Experimental investigation of procedure. Milled polymeric wastes were mechanically activated in a specially made device [5]. Then processed wastes were added to sand and cement mix. The dry
mixture was blended in the mixer for 2.5-3 min after that water was added. After addition of water to the mixture, cement grout was mixed for 3 minutes, left for 5 min and mixed again for 2 min. Repeated mixing is used for prevention of premature concrete setting. The mixture was laid in layers and compacted by a metal rod in molds with size 160x40x40 mm. After the laying, samples were vibrated during 1 min, then were left for 15 min and were vibrated again for 2 min.

By the variety of researchers, it has been established that colloid structure which is formed at the end of the first stage can be easily changed in a certain required way. Repeated vibration conducted at the end of the stage when electroconductivity of concrete mix is maximal allows to increase concrete strength and to reduce its permeability. In this way, 6 samples of each kind of concrete mix were made. Then these samples were left in molds during 24 hours (± 1 hour). After they were placed in a container with water during two days. In 72 hours (± 2 hours) from the moment of preparation, according to methodologies BS EN 12390-3:2009, BS EN 12390-5:2009 [6, 7] compressive strength and flexural strength tests were conducted. The same researches were carried out after 28 days when the concrete stone has maximum strength with the other half of the samples. During the experiments, the method of mathematical planning was used. Analysis of the experimental data was carried out using a statistical analysis package "STATGRAPHICS" by multifactor model’s construction.

Results and discussion. Obtained results of compressive strength and flexural strength tests of concrete samples show their dependence on the amount of filling agents (polymer wastes) and in the concrete mixture. Figure 2 presents results of compressive strength test. As it can be seen, control sample had on concrete strength of compressive 10.27 and 26.6 H/mm2 on the 3rd and 28th days accordingly. The presence of polymer wastes in the concrete samples changed this index. The best results were obtained for samples containing 7% of polymer wastes. After three days, these samples compressive strength 11.34 H/mm2, on the 28th day this index increased up to 29.87 H/mm2 which exceeded results of control sample on 10.4% (3rd day) and 12.3% (28th day).

Results of flexural strength test are shown in Figure 3. Comparing with the control sample, the best strength had those ones containing 7% of PET wastes. As it could be seen from the Figure 3, after three days of setting, flexural strength of samples with 7% of polymer wastes was improved on 21.65% of samples with polymer wastes in comparison with the control sample.

After 28 days obtained results were not so significant but the main trend was the same. Maximal flexural strength was observed for samples with 7% of PET wastes. Improvements were 5.35%.

All samples with polymer wastes can be characterized by:
- the absence of cracks formation at visual observation;
- decreasing of concrete shrinkage;
- reducing of concrete weight up to 21.3% without loss of its strength properties;
- increasing of cohesion of polymer wastes with the concrete stone which was confirmed by mechanical researches;
- improving of concrete compressive strength and flexural strength, especially at the initial stages of concrete formation due to reinforcing and more even distribution of cement particles in samples.

Conclusions and prospects of further researches. Experimental researches proved that mechanical activation of polymer wastes leads to improvement of cohesion of polymer wastes in concrete. Increasing in the amount of polymer wastes up to 10% doesn’t have a negative impact on physical properties of the concrete stone.

New concrete mixtures filled with polymer wastes have been prepared. Obtained mixtures have improved physical and mechanical characteristics and better adhesion of polymer wastes with cement matrix.

It allows to:
- reduce amount of polymeric wastes;
- put into practice basic international principles in ecological policy creating the non-waste technology of polymeric wastes recycling;
- obtain goods with better physical properties;
- use polymer wastes instead of expensive raw materials;
- achieve an essential saving of raw materials, energy and money resources;

Obtained results are underlying and will be used for further researches for determination of limit doses of polymeric wastes which can be added to concrete mixtures.

Present research proceeds innovative approach in the utilization of polymeric wastes by adding into their composition concrete mixtures.

Reference.
2. www.trotuar.ru/forms/dobavki/fibra2.shtml


WAYS OF UPDATING THE TACTICAL AND FIRE TRAINING IN THE BULGARIAN ARMY AND MOI UNITS

Popov G., Assoc. Prof. Marinov R. PhD
Vasil Levski National Military University – Veliko Tarnovo, Bulgaria

Abstract: This paper examines the particular nature of the tactical and fire training of the special units of the Bulgarian Army and the Ministry of Interior and the ways of improvement.

The complex use of tactical and shooting habits is a foundational element in practice when performing special tasks. The skillful use of the right solutions in extreme situations implies the use of all types of firearms at different distances in the course of psycho-physical loads under the influence of distracting factors, combined with the use of techniques of hand-to-hand combat and special means. Along with this, the personnel of these units should be able to move tactically, taking into account the peculiarities of the surrounding environment and to use the firearms effectively.

Keywords: TACTICAL AND FIRE TRAING, SPECIAL UNITS, HABITS AND WAYS OF IMPROVEMENT.

1. Introduction

In today’s conditions, the development and maintenance of combat readiness of the formations is difficult to be fulfilled without focusing on the role of the human factor. This makes it possible to logically link the individual qualifications of soldiers, sergeants and officers and its effective use in teamwork in order to meet the objectives and implement the mission of the formation.

The analysis of the training system shows that tactical and shooting training does not ensure full implementation of the revised requirements for the content and their quality of action in contemporary conditions, which necessitates the generalization, systematization and updating of the methods which forming professional readiness in the Army and MoI personnel, to work under the new changed conditions.

2. Results and discussion

Tactical shooting takes place after the tactics classes. Their aim is to improve the tactical actions of the MoD and MoI personnel and to organize tactically teams at executive and management level in case of necessity of using firearms as well as to increase the psychological resilience of the personnel.

Tactical shooting can be performed by designating the actions of the perpetrators with targets, posters with human bodies, dummies on which models imitating firearms or cold weapons are placed. Prior to conducting tactical shooting exercises with live ammunition, tactical classes and tactical practice sessions are held, with blanks and cartridges with rubber, plastic and shock bullets with full protective equipment. A plan is drawn up for conducting tactical shooting training, which includes the topic, the objectives, the questions, the place and time, the safety measures, the order and content of the activities, the scheme of the situation, the positions and routes of the personnel.

In order to achieve the goals of formation of professional readiness to act in extreme conditions when conducting tactical shooting, it is advisable to use a "house"-type shooting range for shooting with live rounds.

At the "house"-type shooting range the personnel and the teams train and improve their tactical move capabilities; they neutralize targets, practice different ways of accessing, recognizing threats and targets in various situations during the day and at night.

The "house" - type shooting range is an indoor area for shooting with live rounds as it is presented in fig.1. The terrain for shooting with live rounds is one-floor construction with an attic platform for observation and eight rooms with video which can be used for holding briefings and analyses of the tactical actions. The walls are constructed in such a way to stop the bullets and to prevent ricochets. There are four entrances, one on each side of the range. Changeable portable panels which imitate doors and are different from the real doors, used for accessing the building.

This “house”-type shooting range has a crane system mounted on the roof, which is used for lifting and moving doors and hollow panels that are not necessary for training and replacing them with solid wall sections. With regard to safety measures, the polygon has no windows in its construction.

Fig. 1 General view from outside of the “house ”-type shooting range

Fig. 2 presents a general view from inside of the “house”-type shooting range which has improvised entrances and a planning scheme of the rooms and corridors. It is of great importance for the teams to be familiar with it prior to accessing the building.
Tactical shooting training for actions in extreme conditions can range from domestic to hostage crises and terrorist attacks.

When conducting tactical shooting at the firing range of a “house” type, only small arms are used, calibers: 9x18 mm, 9x19 mm, 5,56x45 mm, 5,45x39 mm and 7,62x39 mm.

It should be taken into consideration that the shooting range is not intended for shooting with antitank grenade launcher, under-barrel grenade launcher, hand grenades and the use of smoke ammunition caliber: 7,62x54mm /1908/30 yrs/ and calibre7,62x51mm NATO, antiaircraft ammunition caliber: 12,5x108 mm and caliber: 14,5x114mm, as well as ammunition with armored, tracing and inflammatory action.

Conducting a training – the personnel and the teams follow tactical scenarios based on real times and past crises of extreme nature. The following rules and procedures must be followed when conducting tactical shooting at the “house”-type shooting range:

1. To identify the critical moments in conducting tactical actions and select those tasks that support the requirements for conducting actions in extreme conditions.
2. To prioritise the tasks to achieve the goals.
3. To assess the level of professional qualifications of the personnel (their strengths and weaknesses) and determine the degree of difficulty of each task. Training scenarios should start with a relatively easy task and proceed with more complex ones, this inspires confidence in the training staff.
4. Identify the individual and team tasks that need to be trained.
5. Individual training has to be done first, as it is the basis for team and group training. Improving individual skills is an essential prerequisite for effective team tactical training.
6. Creating learning conditions based on a unit of command. First, the condition is basic until you reach a level of proficiency and professionalism. Increasing difficulty and realism goes hand in hand with increasing the training process.

3. Conclusion

We can note that the professional readiness of the personnel from the structures which act in extreme conditions is a complex of psycho-physical, technical and tactical knowledge, skills and habits aimed at fulfilling the professional tasks in overcoming the impact of external and internal factors in order to preserve the health, life and fitness of the personnel with their structure and content, the formation of which requires professional training. To develop the professional readiness of the employees from the force structures for action in extreme conditions, it is necessary to develop and apply specialized methodology.

Literature:

2. Krustev К., Optimization of the preparation of contingents for joint tactical operations in operations other than war, Dissertation for Acquisition of Doctor’s degree, Vasil Levski NMU, 2013.
Cybersecurity is one of the most commented areas in IT nowadays. Plenty of network and application attacks are possessed worldwide. Security becomes serious issue for corporations and governmental computer networks as functionality of applications rises in technological aspect. Most affective and widely used network attacks and application vulnerabilities are commented in this reviewing paper. Primary solutions for network security are proposed.

Abstract: Cybersecurity is one of the most commented areas in IT nowadays. Plenty of network and application attacks are possessed worldwide. Security becomes serious issue for corporations and governmental computer networks as functionality of applications rises in technological aspect. Most affective and widely used network attacks and application vulnerabilities are commented in this reviewing paper. Primary solutions for network security are proposed.

Keywords: CYBERSECURITY, NETWORK ATTACKS, APPLICATION VULNERABILITIES, SQL INJECTION

1. Alert for networks and computers

The information era is an old word already. Contemporary Internet users have known instantaneous access to web-applications and live video-calling a long time ago. The computer network infrastructures of governments and corporations grew bigger and are deploying worldwide. Internet access and web-site front end seems inevitable since commercialism and publicity is the target direction. Artificial Intelligence (AI), Internet-of-Things (IoT) and even Internet-of-Everything (IoE) play the main role in the world’s communication scene nowadays.

One decade ago the situation was narrow availability of attacker tools, script kiddies and platform homogeneity. Challenges were client-side attacks and many alerts and logs for network administrators to review. Nevertheless, Threat Management and Security Operations Centers were the armors against hackers. After 2010, attacker ecosystems and tools matured, challenges changed to lateral movements and persistent targeted attacks. Focus on security is Risk Management and independency of CIS Officer functions.

Fig. 1 Attackers’ paths representing cybersecurity risk [7]

On Figure 1 a variant of paths for conducting a network and web application attack is depicted according to [7]. What web developers and network administrators should have in mind is that these paths are sometimes trivial to find, but sometimes are distributed in code and difficult to recognize. Technical and business impact estimation in combination with evaluation of threat agent, attack vector and security weakness helps determining the risk of the organization.

Fig. 2 Attack vectors for industry [4]

Having those evolutional processes in communication and computer systems brings the issue of security. Company rivalry, cyber war and database access appetite are one of the vast number of motivations for attacking the network and systems inside. With the Internet connectivity and widely deployed Wireless networks, physical access is no more a breakpoint for attackers.

2. Network attacks and the impact

A network attack can be described as passive or active. Active attack aims system resources altering or affecting their operation. Passive attack tries to learn or make use of system information but does not affect resources (e.g., wiretapping). An attack can be perpetrated by an insider or from outside the organization. An “inside attack” is an attack initiated by an entity inside the security perimeter (an "insider"). An “outside attack” is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments. In the common literature on network security, main network attacks are as follows:

- Denial-of-Service;
- Man-in-the-middle;
- ARP poisoning;
- Ping flood;
- Ping of death;
- Smurf attack, and more.

The most famous network attack is the Distributed Denial-of-Service – DDoS. Its purpose is providing network malfunction by different ways: buffer overflow, TCP SYN flood and etc. Another well-known network attack is the Man-in-the-Middle attack. It is achieved by the means of ARP Spoofing and ARP Snooping. Its main purpose is data sniffing, stealing and if possible – offline data traffic decrypting including private cryptographic keys.

In a continuous live network attack monitoring from Norse Corporation [8] the most interested countries for network attacks are the United States, followed by United Arab Emirates, Spain and Philippines (table 1).

<table>
<thead>
<tr>
<th>№</th>
<th>Top 10 attack origins</th>
<th>Top 10 attack targets</th>
<th>Attack type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>United States</td>
<td>smtp</td>
</tr>
<tr>
<td>2</td>
<td>China</td>
<td>United Arab Emirates</td>
<td>telnet</td>
</tr>
<tr>
<td>3</td>
<td>Netherlands</td>
<td>Spain</td>
<td>http-alt</td>
</tr>
<tr>
<td>4</td>
<td>Ukraine</td>
<td>Italy</td>
<td>rfb</td>
</tr>
<tr>
<td>5</td>
<td>Czech Republic</td>
<td>France</td>
<td>ms-wbt-server</td>
</tr>
<tr>
<td>6</td>
<td>South Korea</td>
<td>Singapore</td>
<td>microsoft-ds</td>
</tr>
<tr>
<td>7</td>
<td>Germany</td>
<td>Norway</td>
<td>xsan-filesystem</td>
</tr>
<tr>
<td>8</td>
<td>Pakistan</td>
<td>Saudi Arabia</td>
<td>netis-router</td>
</tr>
<tr>
<td>9</td>
<td>India</td>
<td>Belgium</td>
<td>netbios-dgm</td>
</tr>
<tr>
<td>10</td>
<td>Spain</td>
<td>Thailand</td>
<td>mysql</td>
</tr>
</tbody>
</table>

Most DDoS attacks are divided into three categories targeting the network infrastructure. Measured in [Mbps] Volume based attacks saturate a site’s bandwidth, which blocks client’s access.
OSI Model layers protocol attacks compromise servers and intermediate communication equipment in order to tie up enough of these resources to lead to denial of service. This is measured in packets per second. The third category is application layer attacks, which are measured in requests per second. These types of attacks crash web-servers by means of flooding requests that appear legitimate. Sometimes the victims of a DDoS attack may not realize they were targeted. Hackers’ motivations may have political intentions, business competition, use it as a means of stealing money, or just distracting victims while performing another malicious activity. One example is the Mirai botnet used for targeting Internet of Things (IoT) devices acquiring massive scale. It brings the next top cyber threat: IoT [3].

From the American research and advisory firm “Gartner” it is estimated that by 2020, consumers and businesses will be using more than 20 billion IoT devices. We are to expect more attacks in 2018 on smart devices, often incompatibly monitored or secured. IoT security fail is the leverage that a malicious hacker could prevail over a large healthcare organization if manages to gain access to the amount of electronic protected health information stored on the organization’s network of medical devices. Vulnerable networked video cameras and camera enabled smart devices provide criminals access to sensitive recorded audio and visual information behind closed doors at target organizations.

IoT typically includes webcams, smart TVs, and even internet-connected refrigerators. IoT actually comprises a broad range of products – electronics, sensors, actuators and software soon to be built into everything from car-vehicles to homes: technology to unlock the gate and switch on the lights when entering home; technology allowing cars to talk to other cars and traffic lights to prevent accidents; technology to regulate breathe air quality, manage energy distribution, and control water supply all in real-time, each with thousands of sensors, all communicating through a city-wide network [4]. Implants for heart monitoring, pathogen monitoring for food, environmental waste monitoring, feedback sensors for firefighters in search and rescue and much, much more are in the potential of IoT. According to the CEO of Cisco, Chuck Robbins, the IoT industry is expected to be worth $US19 trillion globally by 2020 [9].

As for the classification of network attacks, Wi-Fi traffic is also a subject of attack having the air interface open. Linux commands like airendump-ng; aireplay-ng and aircrack-ng define Wireless Network Interface Cards (NICs) as an attacking hardware tool which by the means of the operating system can crack access passwords. This imposes the risk of unauthorized network access and Wi-Fi network de-authentication processes, leading to air-interface network malfunction and later - unauthorized access.

3. Major computer systems and application attacks

Computer systems are being protected against viruses, worms and Trojan horses by antivirus software [1], but having in power some programming skills, attacks could be successful. Common host attacks are:

- Buffer overflow;
- Heap overflow;
- Stack overflow;
- Format string attack, and more.

Computer systems execute codes of applications. Most common application vulnerabilities and attacks are:

- Backdoor;
- Denial-of-service attack;
- Direct-access attacks;
- Eavesdropping;
- Spoofing;
- Tampering;
- Privilege escalation;
- Phishing;
- Clickjacking;
- Social engineering, and more.

As is shown in Table 2 injection tries are the most used in web applications. Typical example is SQL Injection where attacker can “inject” unwanted code in the field of username and password (see Fig. 3). The methodology of injection is as follows: from the web-browser the front end of the site is accessed (most of the times via protocol HTTPS); the user sends “request” queries and data to the web server; and then the scripting language connects to database (such as SQL) storing values to it or retrieving data from it. The front end is usually coded in JavaScript, .NET or PHP scripting languages. The database stores tables in the backend of the site by MySQL, SQL Server, Oracle or other. With the commands shown in fig 3 an injection can be executed.

A found vulnerability in the JavaScript scripting language is here exploited. In another explanation, "SQL Injection" can be defined as subset of unverified/unsanitized user input vulnerability. The idea here is to convince the victim’s application to run SQL code that is actually not intended (see fig. 3). Should the application create SQL strings naively on the fly and then running them, no later real surprises will be on the go.

![Example of SQL injection script](image-url)

The best goal achieved by SQLi is username and password stealing. This would break the authentication barrier. Broken authentication is the second most important security risk which leads to sensitive data being compromised. In this type of risk attackers have in power millions of usernames and passwords, default administrative account lists as well as advanced cracking tools which use lots of calculating power including Graphic Processing Units (GPU).

Another famous attack nowadays is the Cross-site scripting (XSS). It is a code injection attack that allows a hacker to execute malicious JavaScript in victim’s web-browser, for example - in a blank text field of a blogger website. The path for running this malicious activity is injecting the code into a page, downloaded from a web-site and surfed by the victim. Cross-site scripting aims cookie stealing, which contain sensitive information, even though it is in an encrypted form. Decrypting mechanisms would extract passwords and usernames if dictionary or brute force attacks are successful. There are two main types of XSS: Persistent and Reflected. In persistent XSS malicious strings originate from the

<table>
<thead>
<tr>
<th>No.</th>
<th>Type of risk</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Injection</td>
<td>2017</td>
</tr>
<tr>
<td>2</td>
<td>Broken Authentication and Session Management</td>
<td>2017</td>
</tr>
<tr>
<td>3</td>
<td>Sensitive Data Exposure</td>
<td>2017</td>
</tr>
<tr>
<td>4</td>
<td>XML External Entity (XXE) (new risk)</td>
<td>2017</td>
</tr>
<tr>
<td>5</td>
<td>Broken Access Control</td>
<td>2017</td>
</tr>
<tr>
<td>6</td>
<td>Security Misconfiguration</td>
<td>2017</td>
</tr>
<tr>
<td>7</td>
<td>Cross-Site Scripting (XSS)</td>
<td>2017</td>
</tr>
<tr>
<td>8</td>
<td>Insecure Deserialization (new risk)</td>
<td>2017</td>
</tr>
<tr>
<td>9</td>
<td>Using Components with Known Vulnerabilities</td>
<td>2017</td>
</tr>
<tr>
<td>10</td>
<td>Insufficient Logging and Monitoring (new risk)</td>
<td>2017</td>
</tr>
</tbody>
</table>
website’s database, while in reflected XSS the malicious string originates from victim’s HTTP GET request.

The future impact will be on network Confidentiality (e.g. Wikileaks, Doxing, etc.). Impact will also affect data integrity - malware such as Ransomware. And last but not least - Availability (Bricking Firmware, MBR Wiper, etc.).

4. The social engineering phenomenon

Social Engineering as a cyberattack underlies on end-users low-level security awareness. It is an information gathering methodology. An attacker can gain access by fooling an authorized user by means of e-mails that lead to clicking or opening an external web-link or a file, whose masquerade is actually a hidden virus or a malware executing malicious function. Such activities are called E-mail scam and phishing. Actual example of a real e-mail scam is shown of Fig. 4:

![Example of existing real e-mail scam letter](Fig. 4)

The red color ellipse is pointing out the link to be open from the “fooled” user and if done, malicious software would execute. Such an e-mail can be constructed easily from the “SET” tool in KALI Linux operating system [10].

As from the Security experts: humans are the biggest cybersecurity vulnerability leading to intentional and also unintentional network breaches. Often are the results of employee’s carelessness; a disgruntled employee seeking revenge, or the victimization of an employee by a sophisticated hacker. "Social engineering" said in another words is “tricking” a user into opening sensitive information. Most employees assume they can identify a spam e-mail meant to scam the recipient out of money. What they don’t assimilate is that attacks are becoming much more sophisticated. Hackers’ tactics that rely on social engineering, like spear phishing, succeed because the attacker has an intimate understanding of an employee’s motivations and role within an organization so that these can be precisely exploited. Black hat hackers gain enough information about the personal and professional lives of their victims, then effectively impersonate someone the victim trusts or craft an email or popup window that looks legitimate to someone without sufficient security knowledge. Human errors leave networks open to opportunistic cyber criminals. Poor password hygiene is due to a struggle to remember strong passwords for multiple devices of most consumers and employees.

Busy high volume businesses like healthcare organizations may have difficulty managing privileged users effectively, leading to inappropriate access. Human beings increasingly rely on technology to make their lives easier and achieve aims that they could not reach using people power alone. But there has yet to be technology to make their lives easier and achieve aims that they could not reach in inappropriate access. Human beings increasingly rely on technology to make their lives easier and achieve aims that they could not reach in inappropriate access. Human beings increasingly rely on technology to make their lives easier and achieve aims that they could not reach in inappropriate access.

Improving resiliency includes User Education and Awareness. Lessons such as: “Don’t open suspicious e-mails even from friends and colleagues, and moreover – the included files or links inside!” are essential for the future cybersecurity.

Another point assuring cybersecurity is proper planning and preparation – a network with enough resources and predicted situations can be a key to less stress of systems and of the monitoring personnel.

Having in mind that hacker attacks are unpredictable by nature, detection and recovery is the first aid. It includes deployed IDS/IPS systems and also Incident response teams educated for the company/organization. And the most famous advice of security devices providers: Firewall, OS and Antivirus - all patched regularly! As for countermeasures against the highest risk nowadays – Structured Query Language injection (SQLi):

- Prepared Statements (with Parameterized Queries);
- Sanitizing and validating the input field;
- Check the web server & DB configuration (some offer built-in features);
- Strong passwords for SA and Administrator accounts;
- Apply least privilege rule to run the application that access database;
- Use a properly configured WAF, and more.

Against Cross-Site Scripting (XSS) the countermeasures proposed are:

- Validation of input data;
- Encrypting;
- Cookie flag HTTPOnly to be available for all languages;
- Content Security Policy implementation;
- Usage of Auto-Escaping Template System;
- Usage of X-XSS-Protection Response Header – already available in most browsers.

The Web-Application Firewall is the most effective technical solution to achieve web app protection. Basically it’s an application filter for HTTP applications. It applies a set of rules to an HTTP conversation, which protect against attacks such as XSS, SQLi, etc.

Useful advices are to conduct regular penetration tests and vulnerability assessments. Furthermore, advantage of threat intelligence should be taken in order to determine who is targeting an industry branch, what approaches the hackers employ, and whether your institution is likely to be targeted. A remediation strategy should be developed allowing vulnerability or compromise resolution with a minimum disruption of business processes, of hardware control and of customers or users application experience.

References:
Abstract: Small UAVs and micro-drones are becoming more and more available to the general public for leisure activities and exploited in commercial applications. However, there is growing concern for accidental or even criminal misuse of these platforms. Radar systems can provide good capabilities, especially at long ranges and poor visibility conditions. Design considerations for distributed micromillimeter wave radar networks, particular suitable for high density populated urban areas, are given in the report. Special attention is given to: The choice of suitable working frequency bands; The use of antenna beam-forming networks, based on proposed by the author Random Phased Radial Line Slot Antennas and correlation signal processing; The radar signal waveforms in order to obtain un-ambiguity autocorrelation function and small radar resolution volume, as well as to the use of the external coherency principles of Doppler detection.

Keywords: UAV, DRONE, DOPPLER RADAR, RP-RLSA.

1. Introduction

Small Unmanned Aeronautical Vehicles (UAVs) and micro-drones are becoming more and more available to the general public for leisure activities and exploited in commercial applications (inspections, professional filming, support to agriculture, deliveries). However, there is growing concern for accidental or even criminal misuses of these platforms (privacy violation and illegal filming, flying over restricted areas, collision hazard with other aircraft, smuggling of illicit substances, use in terrorist attacks with explosives or chemical payloads) [1].

Radar systems can provide good capabilities, especially at long ranges and poor visibility conditions (thick fog, night-time), but conventional radars are not optimized to sense these platforms, as they are smaller and slower than traditional aircraft and fly at lower altitude. The proposed on the market and in literature anti-drone radar systems are not suitable for urban environments due to the very limited lines of sights and the big number of false radar targets, moving with the same speed as the expected drones.

Design considerations for anti-drone radar sensors are considered in this report. The sensors are parts of distributed millimeter wave radar network, particular suitable for high density populated urban areas.

1. UAV detection by Doppler radars

Radar is believed to be a valuable sensor in dealing with the detection and classification of a variety of targets in crowded littoral and urban environments [2]. However radar detection of micro UAVs present challenging factors, as these tend to be low and slow flying, with a small Radar Cross Section (RCS). Low altitude and reduced velocities may lead to difficulties in separating the target from a significant clutter response. Low RCS makes the detection within cluttered environments very demanding. In addition to detection the drones need to be distinguished from biological targets like birds and insects frequently present in the same surveillance volumes. Birds and UAVs may have comparable RCS values and flying patterns which present a very tough challenge for classifiers to separate them. Micro-Doppler based techniques is a promising approach to solve the problem. Whereas the total RCS is important for target detection, the energy backscattered from rotating parts like propeller and rotors are crucial for extraction of useful micro-Doppler signatures. Tri-copter, quad-copter and octo-copter like UAVs normally use rotor blades made of carbon, fiber or plastic materials. The smaller the drone the larger probability it has plastic blades. This choice of material may be important when it comes to the visibility of the blades in radar systems. While carbon fiber blades are believed to behave close to a perfect electrical conductor, plastic material may have dielectric properties closer to air, thus resulting in little reflection back to the transmitter.

In order to investigate these aspects, paper [2] presents RCS simulation results and their comparison to real measurements taken of rotor blades made from different materials. The blades under test were taken from the platform of interest, which was the easily available DJI Phantom Vision 2+ micro drone. The DJI drone platform was then measured using an experimental pulsed Doppler radar system, NetRAD. The NetRAD system is a coherent, 2.4 GHz, 45 MHz bandwidth, 0.2 W (in low power configuration) radar. The radar was configured to take pulse to pulse interleaved horizontally and vertically polarized measurements. The interleaved operation allowed for the direct comparison of HH and VV data. The DJI drone flew in a straight line at approximately 2 m height from the ground at ranges of 70 m to 150 m from the radar. The drone was configured to use carbon fiber rotor blades rather than the reduced RCS typical plastic blades.

The data from the Horizontal (HH) and Vertical (VV) channels have been analyzed using micro-Doppler processing algorithms. A Short Time Fourier Transform (STFT) was applied to the range gates the target was present within. For this processing a window length of 0.3 seconds, with a 95 % overlap was applied to data which was generated at a PRF of 10 kHz, which gave equivalent PRF of 5 kHz after de-interleaving. The results from a 5 second capture of HH and VV data can be seen within fig. 1 (a) and (b) respectively [2].

The Micro-Doppler components from the two different polarizations is markedly different. The horizontally polarized result has two key features, this first is the slanted line of the main bulk motion of the drone moving away from the radar relatively close to the 0 Hz line at -50 to -70 Hz. The second is the multiple discrete signatures from the rotor blades up to 1 kHz in frequency. The VV polarized result only has signal from the main body of the drone, no components of the rotor blades are visible. From the simulation results these components are expected to be 30-40 dB lower in VV polarization and hence were below the sensitivity of the radar. These key differences show the importance of polarization when hoping to observe the blade contributions to a small drone platform Doppler signature. The micro-Doppler contributions contain additional information on the target and show good potential for target classification purposes.
Due to very small dimensions and high maneuverability, the drones are extremely difficult to detect [3]. According to the radiophysics, objects smaller than the radar wavelength does not reflect the signal at all. Therefore, conventional radar systems operating in the centimeter and decimeter waves are powerless against drones as were engineered for the identification of large airborne targets like planes and helicopters. Drone is composed of many small parts and traditional radar does not see it. To detect the drone, it is required to use radar operating in the millimeter wave range, as wavelength is smaller than the drone parts. The proposed by ELVA-1 anti-drone radar DDR-76 [3] operates at 76 GHz (wavelength of 4 mm), catching the returning signal from a variety of small drone parts.

According to the Bulgarian National Radiofrequency Plan, harmonized with the European, the frequency band 76 – 77,5 GHz is allocated on primary status for short range radar equipment. This frequency band is very attractive for use in anti – drone systems, but it needs implementation of new reliable and cheap semiconductor technologies, suitable for mass production.

Another benefit of the used 77 GHz band is the expected substantial increase of the reflected vertical component due to the fact, that the transverse rotor blades dimensions are several wavelength larger than the experiment at 2,4 GHz, shown in fig.1–b.

2.3. External coherency principles of Doppler detection

Coherent radar uses coherent signals and signal processing [4]. Coherence provides the ability to maximize signal-to-noise ratio, to measure target radial velocity, and to provide Moving Target Indication (MTI) and other Doppler-based clutter rejection techniques. Coherent pulsed radars are the most widely used types, although coherent Continuous Wave (CW) radars appear in specialized applications such as missile guidance and police speed-control radar. Coherent pulsed radars are classified as truly coherent or pseudo-coherent, also known as coherent-on-receive. Both types are known as internally coherent, to distinguish them from externally coherent types, which use the clutter itself as a phase reference.

Advantages of internal coherence lie in the high sensitivity and the possibility of measuring the Doppler frequency shift with good accuracy. Disadvantages are the relative complexity and need to ensure high stability of all the oscillators used in the system. Most of the proposed anti-drone radar architectures use internal pulse coherent radar approach.

In a radar with external coherence, the system local COHerent Oscillator (COHO) is phased not by the transmitted signal but by a clutter signal, or the clutter itself is used as the reference voltage. Advantages of the external coherence lie in the possibility of suppressing extended interference. A disadvantage is that the detection of moving targets in them is possible only if there is extended clutter present. If the clutter does not enter the antenna pattern of the radar, then phasing of the COHO is controlled only by target signals, which leads to suppression of those signals.

The implementation of the extended clutter based coherent principles in anti-drone radars could be very promising, due to:  
- The reflected from the drone body signals can be considered as extended clutter (fig.1 – the spectrum line centered at 70 Hz). They could be compared with 1 KHz Doppler signal, obtained from rotor blades, in a correlator. Its output signal will be with difference frequency and will not carry information about the drone speed. It will contain the specific multiple discrete signatures from the rotor blades up to 1 kHz in frequency. When the used radar frequency lies in 77 GHz band, the corresponding difference frequency will be about 30 KHz.
- The experimental RCS results [2] show very low back scattering from plastic rotor blades. This will be problem for the design efforts to create universal anti-drone radar sensors. In such cases another physical propagation...
phenomena could be very useful. The plastic blades will shadow partially (if they introduce substantial losses) and will introduce additional phase shifts for the signals, reflected from some parts of the drone body. The final effect could be even better then in the case of metal rotor blades. Simulations of these phenomena should be done in experimental way.

2.4. **Antenna beam-forming networks, based on SCP-RPSC technology**

The Spatial Correlation Processing – Random Phase Spread Coding (SCP-RPSC) is an entirely new approach in the field of microwave beam forming antenna theory, developed by the author one decade before. The goal was solving the problems of the tracking microwave antenna systems for mobile satellite communications. It was studied first in receive mode (SCP technology) [5, 6], where its main objectives include:

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

The SCP approach uses simple and cheap passive Radial Line Slot Antenna (RLSA), suitable for mass production in Ku and Ka frequency bands, as well as one channel microwave receiver with simple signal processing.

The transmit mode (RPSC technology) [7, 8] is based on transmission of broadband microwave signals in the open space by means of multi element random phased antenna arrays. The sum of the different element signals in a given point in the space has Gaussian probability distribution and noise like properties. The sums in the different directions of the space are not correlated each other. In such way the proposed principle solves simultaneous the problems of signal spreading and beam forming of the future sophisticated microwave terrestrial and satellite communication and radar systems with fixed and mobile applications.

The “magic” properties of the SCP-RPSC technology, applied in the future sophisticated millimeter wave anti-drone radars, could be very attractive. One simple and cheap RLSA will be used both for transmission and reception, ensuring simultaneous high antenna gain and omni-directivity, typical for low gain antennas. The typical for SCP-RPSC procedure of correlation among several thousand random phase spread information and pilot signals will be replaced with correlation among the phase spread in the same manner signals, reflected by the drone body and its rotor blades.

2.5. **Radard signal waveforms for obtaining un-ambiguity autocorrelation function and small radar resolution volume**

In radar, resolution is the ability to separate the signals from adjacent sources [4]. The ability to distinguish one target from another is defined by a four-coordinate radar response, so angular, range, and Doppler resolutions typically are distinguished. The common measure to consider two targets to be resolved in a particular dimension is when they are separated by a distance equal or more than half-power width of the radar response in this dimension: angle, range (time), or velocity (Doppler frequency).

The resolution element [4] is a spatial and velocity region, contributing echo energy that can be separated from that of adjacent regions by action of the antenna or receiving system. In conventional radar, its dimensions are given by the beam-widths of the antenna, the transmitter pulse-width, and the receiver bandwidth. It is also called the resolution cell. When the resolution element is only spatial region (angular and range), it is called resolution volume.

Very important requirement to the proposed anti-drone radars, which is common for all kinds of microwave intruder alarm Doppler sensors, is the use of very small resolution volumes, which can be done using step by step approach. In such way the signal to interference from another targets ratio increases in maximal way. The first step is to reduce the virtual antenna beam-width, which is final results of the used basic SCP-RPSC principles. The second step is the use of modulated waveforms, ensuring narrow and un-ambiguity autocorrelation function in time (range) domain. A possible solution here is the use of Frequency Modulated – Continuous Wave (FM-CW) signals with sinusoidal FM [9]. In such way several advantages appear, as follows:

- The used FM will de-correlate the off-diagonal terms of the SCP-RPSC correlation matrix and their sum will be zero for all space directions. It is very important in order the rules of Central Limits Theorem (CLT) to be valid;
- The beam-width of the autocorrelation function in time (range) domain depends on the dispersion of the Gaussian random process and is inverse proportional to the number of the used random phase spread signals, obtained from the different antenna elements (slots if RLSA is used).
- If pure Doppler processing is used, the amplitudes of the correlator output signals are time (range) depending as Bessel function of zero order [9]. This fact reduces the resolution volume too.

2.6. **Drone detection multistatic radar networks**

Drone Detection Multistatic Radar Networks (DD-MRN), using the basic principles of the SCP-RPSC technology, could be very promising if the knowledge of the exact drone coordinates are of great importance [10].

3. **Conclusion**

In this paper design considerations for anti-drone radar sensors are considered in details. The sensors are parts of distributed millimeter wave radar network, particular suitable for high density populated urban areas. The report can benefit manufacturers of sensors and systems for drone detection and classification, regulators and air traffic controllers as well as commercial operators and manufacturers of drones by providing a safer and better managed operational context for drones. The same is valid for law enforcement authorities, responsible for protection of national assets and infrastructure, which may be threatened by criminal usage of drones.

**Reference**

[1] University of Glasgow, Radar detection and classification of small UAVs and micro-drones”, Internet “media_480052_en”.
AN APPARATUS FOR RECORDING OF EXTREMES IN ELECTRICAL SIGNALS - FDI-1

1 Georgi Nadjakov Institute of Solid State Physics, Bulgarian Academy of Sciences, Bulgaria
2 Universidad de Alcalá, Spain
3 University of Chemical Technology and Metallurgy, Department of Electrotechnics and Electronics, Bulgaria

Abstract: In this work a new device for measuring the parameters of a fog is described. It is developed by our team and is called Fog Detector Indicator 1 (FDI-1). It is a part of a sensor system for control of the parameters of a fog which is used for decontamination of objects polluted by different circumstances. FDI-1 is a custom indication unit used in various systems for evaluation of fog parameters that gives the operator a visual result for the change of the input voltage. The main function of the indicator is to show the measured voltage applied on its coax input. Usually, this measurement can be done with a regular voltmeter, but the nature of the measurement of a fluid (fog) density, droplet diameter or contamination assumes very rapid changes of the measured values and also very short peaks of the maximum and the minimum of the measured variable. FDI-1 is can be used namely in such cases.

Keywords: FOG PARAMETERS, MEASURING DEVICES, SECURITY, MILITARY APPLICATIONS, DECONTAMINATION

1. Introduction

During the last 20 years terrorist attacks represent a big problem for many countries of the civilized world, including European ones. Security measures should be taken to prevent terrorist attacks and also to deal with consequences of these attacks. Measuring equipment plays an important role in analyzing these consequences. In general, measuring devices used for military applications should be reliable, easy to use, easy to transport and they should work in a large temperature range, during heavy rain, withstand big pressures and be resistive to mechanical hits by different objects.

Chemical weapons are still used, in spite of the fact that their use is prohibited by the international humanitarian law. The international humanitarian law regulates the conduct of war. Its aim is to protect the people that don’t participate in hostilities during an armed conflict. Obviously, the international humanitarian law is not respected in some countries. One recent example is the use of chemical weapons in Syria where many people (including civilians) were killed in suffering. Generally, the areas where the chemical weapons are used are not safe for the people for weeks after the attack, so the attacked areas should be chemically cleaned. This cleaning is performed by using a system for spreading a fog in the contaminated area.

2. Prerequisites and means for solving the problem

For the purpose of cleaning the contaminated area it’s important to monitor the parameters of the fog. We have created such devices. They convert the parameters of the fog to electrical signals. These signals change very fast and in order to be able control the fog, it’s necessary to measure and register these maximums even when there isn’t a person near the devices. This was the reason to create the FDI-1 (Fog Detector Indicator 1). FDI-1 can be also used for other purposes where it is needed to measure and register maximums of electrical signals as a result of some ongoing processes. The cleaning properties of fog are known and used in material science [1], applied medicine [2], biology [3], etc.

Another important application of fog is connected to the security of persons in their homes, at work places and during trips. It’s the use of fog against fire. The water fog can be used against fire but with caution during winter time because freezing is possible. Also, in some cases water can react with chemicals and as a result of this reaction an explosion can occur [4]. A water fog is used for decontamination of equipment of fire fighters. The decontamination task depends on the type, quantity and concentration of the pollution material, the type of the decontamination agent and the medium, the available decontamination agents and equipment. Except water, other decontamination materials are used depending on the type of the pollution [5].

The parameters of fog are also important in the meteorology [6, 7] and the FSO (Free Space Optics) [8]. For measuring the parameters of fog are used droplet size spectrometers and systems with fog sensors.

3. Solution of the examined problem

In this work we present a new device for measuring the parameters of a fog. It has the following advantages:

• It has small size (portable to any location);
• It is easy to handle with power from an ordinary adaptor or battery;
• It is easy to operate;
• It measures and saves the maximum of the input signal which changes very fast;
• The device has an LCD display and a LED bar graph for visualization of the results;
• It can operate in two modes and is able to measure and save the maximum of the input signal, even without an operator.

The measuring device called FDI-1 (Fog Detector Indicator 1) has overall dimensions of 133 mm x 95 x 30 mm. It is a part of a sensor system for control of the parameters of a fog. When there is a terrorist attack with chemical substances, the attacked area can be checked and cleaned by spreading a fog. Then the parameters of this fog are measured by sensors which are directly connected to FDI-1. The command signal for FDI-1 is an electrical tension delivered by the output of the sensors which are located in the fog. This system can perform 24 hour measurements of the parameters of fog and the results are easy to read on the display of the device. Also, for better visualization of the results, FDI-1 has a LED bar graph. The operator can choose between two different operating modes of the measuring device. The device has a good sensitivity to the fast changing parameters of the fog. The power supply of FDI-1 is ensured by a standard 12V adapter.

3.1. Description of the FDI-1

Fog Detector Indicator 1 (FDI-1) is a custom indication unit used in various systems for evaluation of fog parameters that gives the operator visual results of the change of the input voltage. The main function of the indicator is to show the measured voltage applied to its coax input. This measurement can be done with a regular voltmeter, but the nature of the measurement of the fluid
(fog) density, droplet diameter or contamination assumes very fast change of the measured value and also very short peaks of the maximum and the minimum of the measured variable. Moreover, the indication should be easy to read. FDI-1 has taken into account all the specific requirements, which come from the nature of the measurements. It has a bar-graph indication for fast evaluation of the results, an LCD display for showing the actual values of the measurements with refresh rate, fast enough to meet the requirements. The internal logic allows the implementation of an average function, which is important to exclude the flicking of the input signal, in order to obtain proper measurements. The device allows the operator to choose base level and upper level for the measurement which is important for compatibility with various systems with different sensitivities and output ranges.

### 3.1.1. Overview of FDI-1

In Fig. 1 an overview of the FDI-1 device is presented. On its right edge there is a power jack for plugging a standard 12V adapter (1), also there is the BNC input (2), where the measured voltage should be applied. On the front panel at the upper left side there is an LCD indication display (3) and LED bar-graph indicator (4) next to the display. At the bottom side of the front panel there is a switch (5) for choosing between positive and negative measurement and also 3 buttons (6) for control. At the upper right corner there is also a special function button, named “Alarm reset” (7).

### 3.1.2. Hardware description

The hardware implementation of FDI-1 is based on Atmel’s Atmega 328P 8Bit microcontroller unit (MCU). A block diagram of FDI-1 is shown in Fig. 2.

The required power supply for FDI-1 is in the range 8V – 16V, which makes possible the use of standard battery pack or any universal power supply adapter for supplying the device. Be aware if you are using any third party power supply that the positive electrode is inside the connector (Fig. 2). FDI-1 includes a reverse polarity protection circuit, but it is not recommended to attach unproved power supplies.

### 3.1.3. Software description

The general software flow diagrams are shown on Fig. 3 and Fig. 4. There are mainly two parts of the software. First is the “menu” part (Fig. 3), where the user sets the limits of the measurements. The second part is the main measuring and calculation system (Fig. 4).
3.2. Principle of operation of FDI-1

The signal that should be evaluated must be connected to the dedicated coax connector, which is referenced to ground (the negative pole of the power supply). The maximum measurement range is 0V – 5V DC. However, the input is protected to accept +/-10V input signal.

The device has four buttons (Enter, Up, Down and Alarm Reset) and one switch for choosing the measurement mode (Positive or Negative). The needed user information is displayed on one four-row dot matrix display. Additional LED bar-graph is presented on the front panel for discrete light indication of the measured value. The user interface of FDI-1 is presented in Fig. 5.

The first menu offers the user to choose between ‘Positive mode’ and ‘Negative mode’. The user can change the mode through the switch. When the mode is chosen the user should press the ‘Enter’ button to continue.

The second menu gives the user the ability to change the base level of the measurement (from what voltage value to start the measurement). This is normally the steady state signal value of the measurement system without fog. By default the base is equal to the measured level of the coax input at the current moment, but the user can change this level by using buttons ‘Up’ and ‘Down’. When the proper base level is chosen the user should press the ‘Enter’ button to continue.

The third menu offers the user to choose a measurement limit level (to what voltage value the measurement should end). This limit level should correspond to the maximum signal value that can be achieved (sometimes the boundaries of the input range 0-5V cannot be reached). This setting is only needed for the diodes to indicate correctly. By default the value of the limit is set to 5V, but the user can change this level by using buttons ‘Up’ and ‘Down’. When the proper limit level is chosen the user should press the ‘Enter’ button to continue.

Due to the required logic implementation, it should be noted that:
- For positive measurements, the limit must be higher than the base.
- For negative measurements, the base must be higher than the limit.

After applying the required settings, the measurement can start. On the user display you will have information about the current voltage level applied on the coax input, the extremum of the measurement, the chosen base and limit levels. The extremum value in positive mode is the highest value reached during the measurement. In negative mode the extremum value is the minimum value reached during the measurement.

The LED indication bar-graph will show current value of the voltage applied on the coax input, while the limit value is higher (for positive mode) or lower (for negative mode) than the base level and the measured voltage is more than base voltage +0.3V (for positive mode) or less than base voltage -0.3V (for negative mode).

If those conditions are not satisfied, the device will enter in alarm mode – the LED bar-graph will start blinking with the value of the extremum until the conditions for voltage are fulfilled or the user presses the ‘Reset alarm’ button.

If the user wants to change the type of the measurement, the base or the limit, it is needed to switch the ‘Mode select’ switch. This operation will let the user to change all the settings that was previously set.

4. Results and discussion

We have performed investigations of the maximum amplitudes reached during measurements of contaminated fog as a function of the concentration of a pollutant. For the actual measurements we have dissolved 4 grams of the substance monopotassium phosphate (KH₂PO₄) into different quantities of water (200 ml, 300 ml, 400 ml, 500 ml, and 600 ml).

![Fig. 6 Change in the signal generated by the sensor head as a function of pollutant concentration in the fog.](image)

The results clearly show that the amplitude of the generated by the sensor’s alternating electrical signal changes with changing the concentration of the pollutant.

This device also can be used in other systems to measure the changing of other non-electrical parameters. The non-electrical parameter should be converted to electrical tension which represents...
the input signal for FDI-1. For example, the device can be used in systems for measuring the temperature of ovens for chemical changes, ovens for drying or hardening, diesel engines, the temperature of liquid flow in industrial cooling systems, where the used sensor is a thermocouple. FDI-1 can also be a part of heating systems for measuring the current temperature. The device can measure some other non-electrical parameters, such as pressure, light flow and many others.

4. Conclusion

In this paper a new device – Fog Detector Indicator 1 (FDI-1) - for measuring of fog parameters of is described. It is small in size and therefore portable, it can be supplied with power from an ordinary adaptor or battery, it is easy to work with and operates fast. It has the ability to measure and save the maximum of the input signal which changes very fast. The device has an LCD display and a LED bar graph for visualization of the results. It supports two operating modes and it can measure and save the maximum of the input signal autonomously. In the case of a terrorist attack with chemical or biological substances, the contaminated area can be checked with it and cleaned by releasing a cleaning fog.

The presented results clearly show that the amplitude of the generated by the sensor’s alternating electrical signal changes with changing the concentration of the pollutant. This is exactly the function of FDI-1 – continuously measuring and controlling the parameters of fog.

FDI-1 is a solution to the growing need of measuring devices which are easy to use, with clear indications and portable to any location. It is expected that this device has the potential to be very helpful for security applications and military missions for achieving a safer world.

Acknowledgements:

The European Commission is acknowledged for supporting the work described in this paper by EU FP7 Security program under Contract 312804.

References:

Abstract: Measurement device, specifically developed to capture and quantify low-amplitude surface photo-charge effect signals. It can also modulate and power a laser in various modes, and extract the processed signal as an output. The device is compatible with all of our surface photo-charge effect-based systems. The device is part of a portable system for detection of pollution in fogs or aerosols.

Keywords: OPTICAL SENSORS, FOG DETECTION, PHOTOELECTRIC EFFECT, AIR POLLUTION, SECURITY

1. Introduction

Contamination of the environment as a result of industrial accidents, disasters, terrorist attacks, wars, etc., is in a lot of cases spread to large areas due to atmospheric dispersion. This is possible as the harmful agents - chemical, biological, radiological and nuclear agents, are usually dispersed as aerosol mixed with a carrier liquid [1]. One of the most efficient ways to decontaminate the polluted areas (indoors and/or outdoors) is through the spraying of fog with specific pressure and composition. Fog is an aggregation of a large number of microscopic water droplets spread in the air. The specifically controlled fog has the potential to sweep along a large number of impurities in the air, i.e. small particles, dust particles, chemical compounds, etc. and facilitate their condensation on the ground together with the water droplets. In such way, the fog effectively decontaminates the air. For more efficient decontamination, specific neutralizing substances are added to the fog. As these substances can also be potentially hazardous to human health, the spraying of fog needs to be optimized.

The application of this technique for decontamination with fog requires sensors for continuous monitoring of fog and its admixtures. Such detectors should be triggered on when the harmful substance appears in the environment and triggered off when the concentration of this substance falls below a threshold value. The perfect sensor will be with small size, rather inexpensive, with a simple construction, stable in the various conditions and portable. It should also be capable of online monitoring of small and large areas.

To address these needs, we have developed portable sensors [2] and monitoring devices for contamination in fog in the framework of EU FP7 Security project COUNTERFOG [3]. Most of the developed sensor systems operate on the basis of the Surface photo-charge effect (SPCE).

The SPCE is registered during the interaction of any solid with an electromagnetic field and is described as the induction of an alternating electric potential difference in the solid with the frequency of the incident field [4], [5]. The SPCE response has a significant dependence on the characteristic properties of the studied sample. This gives rise to opportunities for rapid and contactless analysis of solids, liquids, and gasses [6], [7], [8] and chemical agents dispersed in aerosols [2]. The sensors based on this effect have demonstrated good analytical capabilities [7], [9].

Here, we present a portable device for measuring the SPCE signals – SPCE Meter 1. The device allows different experiments to be conducted by irradiation of samples with laser pulses and the measurement of the associated photoelectric effects. The experiment is done with a fixed frequency of 28.5 kHz. The control of the laser, with respect to its specification, can be done with the passing of sinusoidal or square signal with given frequency.

2. Experimental setup.

The device is designed for conducting experiments with a semiconductor laser influencing a sample made of semiconductor material. During the experiment on the sample, an impulse is being created with amplitude from tens up to hundreds of microvolts. The lower amount of the accumulated charge and amplitude of the voltage demand the usage of a preamplifier with large input impedance and low level of external interference and internal noises.

The device has the following technical parameters: supply voltage (220 +/- 10) V; (50 +/- 1) Hz; Operating frequency (28,5 +/- 0,5) kHz; input impedance – over 100 MΩ. Output signal is: a) sinusoidal, with adjustment of the amplitude and the operating frequency; b) square, with TTL level, duty cycle (50 +/- 3) % with operating frequency; c) square, with TTL level and manually adjustable duty cycle /PWM/ in the approximate range of 3.5 – 86.5 %, with operating frequency. d) DC voltage proportional to the amplitude of the sample signal received in parallel to the measuring digital voltmeter; e) pulse signal with square form and manually adjustable amplitude (0 – 12) V, duty cycle (50 +/-3) % and with operating frequency.

Besides the above-mentioned pulse signals, a manually regulated DC voltage (2 - 12) V can be generated from the device, which can be controlled with a digital voltmeter. Maximum current which can be produced with the built-in stabilizer is 200 mA.

The device for conducting experiments is made of the following blocks and nodes, shown in the block diagram of the device (Fig. 1): Input matching block (1); High-frequency filter (2); Resonance differential amplifier (3); Matching HF transformer (4); Power supply filters circuit. The above blocks are located in different shielding housing provided with BNC type connector; Sinusoidal generator (5); Shaper of TTL signal (6); PWM regulator (7); Output TTL drivers (8); Fast-acting transistor switch (9); Amplitude detector for the acting signal – sinusoidal or pulse (10); Amplitude detector for the sample signal (11); Power supply +/- 12 V (12); Power supply + 5V (13); Adjustable power supply + (2 – 12) V (14); Galvanic isolated power supply 9V for the digital voltmeters (15).

To expand the potential of the device, a few types of changes (modulation) of the controlling signal are provided. If the output power of the laser is proportional to the instantaneous value of the control voltage, it is possible the value to be with controllable form, as the power of the irradiation is linear or close to a linear function of the controlling signal. The possible changes of the signal are as follows:

A) Adjustment of the amplitude of the sinusoidal voltage. It is possible to be used if the structure of the laser allows control (modulation) of the irradiation with a signal which has an arbitrary linear function for the control voltage. The voltage of the output of the device to the control input of the laser is adjusted with potentiometer on the front panel, noted with the symbol \(\text{522}\).
is possible to be used if the structure of the laser allows control (modulation) of the irradiation with a signal which has an arbitrary linear function for the control voltage. The voltage of the output of the device to the control input of the laser is adjusted with a potentiometer on the front panel, noted with the symbol “…” (Fig. 2, Pos. 2). The output signal is received from the connector type BNC, noted with the label “sin 28.5”, which is on the back panel (see Fig. 3).

B) Adjustment of the amplitude of the sinusoidal voltage. It is possible to be used if the structure of the laser allows control (modulation) of the irradiation with a signal which has an arbitrary linear function for the control voltage. The voltage of the output of the device to the control input of the laser is adjusted with a potentiometer on the front panel, noted with the symbol “…” (Fig. 2, Pos. 2). The output signal is received from the connector type BNC, noted with the label “sin 28.5”, which is on the back panel (see Fig. 3). The output signal is connected to the output of the high-frequency active filter with a cutoff frequency of 10 kHz. This filter eliminates the noise to a great extent with the frequency of 50 Hz from the surrounding network. The output of the filter is connected to the differential amplifier. The coil of the resonant circuit is wound bifilarly and connected in series, which puts the AC voltage into antiphase. The differential amplifier has a differential amplifier, a resonant filter is used. It is set to the first harmonic of the operating frequency. Therefore, the reading on the display is the difference voltage of the laser.

The amplitude of the voltage from point A to point B can be measured when we use the switch located between the two potentiometers (Fig. 2, Pos. 3) and we choose the respective symbol of the voltage. The reading is done on the display over the potentiometer (Fig. 2, Pos. 1). It is important to take into account a number of issues.

1) The signals from the potentiometers are submitted directly to the output connectors. The load which is added to the connectors must be with impedance 50-100 kΩ.
2) When the sinusoidal voltage is measured the display shows its amplitude and not the effective value.
3) When the laser is controlled with a TTL signal and the relation between the investigated effect and the duty cycle of the pulse is not under investigation, an output labeled “TTL PWM”. With the help of the potentiometer, the duty cycle can be varied within approximately 4-85%. The control of this parameter can be performed by an additional instrument, for example, oscilloscope connected to the output.
4) In order to explore the dependence of the researched impact of the duty cycle of the control pulse, the signal that controls the laser can be taken from “TTL PWM”. With the help of the potentiometer, the effective value of 100 µV.
5) If the laser permits, the intensity of its radiation can be adjusted manually by varying the supply voltage. For this purpose, an additional galvanically separated supply voltage is provided. This voltage can be adjusted manually with a potentiometer (Fig. 1 Pos. 7), and the result is displayed in volts (Fig. 2, Pos. 5). This power supply is obtained from a separate connector on the back panel, labeled “DC 2-12V” (Fig. 3).

Methods 3) and 4) can be combined with method 5) to build groups of characteristics of the effect. In methods 1) and 2) where the radiation of the laser is adjusted with the amplitude of the input voltage, the DC source can be used by setting it to the prescribed power-supply voltage of the laser.

3. Experimental procedure

When the appropriate method for supplying the laser is chosen, we can proceed with measurement of the SPCE impact effect. In the preamplifier, a trimmer-potentiometer is provided for correction of the gain. It is located next to the BNC connector. In the right-most position (CW) of this potentiometer, the meter is calibrated and the reading on the display (Fig. 1, Pos. 8) is in µV. The switch under the display (Fig. 1, Pos. 9) must be in position “20 mV”. Then the maximum display value of the voltage can be 199.9 µV. If the supply to the display voltage is over this value, the switch must be changed to “200 mV”. Then the maximum display value of the voltage will be counted to 199.9 mV. The measurement must be done in the following order: 1) connection of all the necessary circuits; 2) turning on the power supply unit; 3) turning on the laser and choose of operating mode; 4) the switch under the display is placed in position “20 mV”; 4) positioning an opaque barrier in the way of the laser beam and without disconnection of the laser, shifting the reading on the display as close as possible to 0 mV. The potentiometer for the signal shift is on the back panel, over the connector type “DB-9”; 5) removing the opaque barrier and check if the display is not overloaded. In case of overload switch to “200 mV” and the procedure of the reset is repeated.

From the experiments is established, that the voltage on the device input, does not have sinusoidal form. It closely resembles a saw. So as to secure sufficient enough protection from disturbance, in the preamplifier, a resonant filter is used. It is set to the first harmonic of the operating frequency. Therefore, the reading on the display is proportional to the amplitude of this harmonic and do not take into account the impact of the second, third, etc. harmonics. The calibration of the device is done as the input is submitted with a sinusoidal voltage with low-frequency generator with an effective value of 100 µV.

The device for experiments works as follows: the signal is fed to the matching block, which has very high input impedance. Its output is connected to high-frequency active filter with slope 12db/oct and a cutoff frequency of 10 kHz. This filter eliminates the noise to a great extend with the frequency of 50 Hz from the surrounding network. The output of the filter is connected with an inductive connection to the differential amplifier. The coil of the resonant circuit is wound bifilarly and connected in series, which puts the AC voltage into antiphase. The differential amplifier has...
the capability of manual adjustment of the limits (10 ÷ 500) times. The output via broadband transformer is connected to the main block.

In the main block, this signal is detected and its amplitude is shown with the digital voltmeter. The same voltage appears in BNC type connector for connection to an additional external device.

The operating frequency of the device is made of RC sinusoidal generator with Wien bridge. It is implemented via a powerful integrated circuit – final low frequency (LF) amplifier. The shaping of the square signal is done with CMOS Schmitt – trigger. The regulation of the width of the pulse is made with the help of a waiting multi-vibrator made with schemes with hysterisis. These two signals are supplied to separate outputs through drivers, each containing three parallel connected CMOS inverters. With this, we secure amplitude of the output voltage to almost 5V, which enables the outputs to connect devices with CMOS or TTL input.

A square signal with filling 50% and adjusting the amplitude is obtained from a fast transistor switch. With the switch for choice of source of the signal (sinusoidal or pulse) these voltages are fed to the amplitude detector and are reported with a separated digital voltmeter. The outputs with adjustable amplitude (sinusoidal and square signal) require load resistance over 50 kΩ. Keep in mind that the sinusoidal voltage is shown as amplitude and not as effective value.

A few stabilized power sources are used to make the power supply of the device. The analog part (sinusoidal generator and operational amplifiers) require voltage +/- 12V. They are received from the network transformer with the middle point of the secondary winding, symmetric rectifier, and two integral stabilizers – for positive and negative voltage. The necessary 5V for the digital integrated circuits are produced from the stabilized positive voltage using a linear integrated circuit. Although the bigger heat losses the preferred solution is with linear stabilizers and not with pulsed, so to avoid the possibility of penetration of noises in the circuits of the power supply.

The three digital voltmeters which are located on the front panel require galvanic separated power supply voltage 9V. It is obtained from the separated winding of the second transformer and is also stabilized with the linear integrated circuit.

The manually adjustable DC voltage for the power supply of the semiconductor laser is also galvanically separated from the measuring part with the purpose to lower the internal noises. It is secured in a separated winding in the second transformer, rectifier, and linear stabilizer.

Constructively the device is installed into two housings – main and supporting, which are connected with a flexible multicore cable via a DSUB-9 connector. The supporting housing is made out of a metal casting, to provide shielding of the sensitive to noises input circuits.

For heat dissipation, the linear integrated circuits for power supply and sinusoidal generator are installed on the radiators. The upper cover of the main housing is with openings for ventilation

4. Results and discussion.

The SPCE was applied for measurements of the cleaning properties of fog created by the full-scale Fog Dynamics Laboratory, in CIEMAT, Madrid designed in the framework of project COUNTERFOG. The special design of the SPCE meter allowed for it to be installed in the Laboratory and measurements with different types and concentrations of pollutants to be performed.

The most numerous measurements were made with the chemical contaminator: potassium dihydrogen phosphate (KH₂PO₄). Potassium dihydrogen phosphate (KH₂PO₄) was chosen as a harmless simulant of the highly lethal class of nerve chemical warfare agents from the G- and V-series. In solution, KH₂PO₄ dissociates to give phosphate ions which are very similar to the behavior of the mentioned class of chemical agents’ molecules. In Fig. 4 is presented the signal obtained from the SPCE meter at spraying of fog containing KH₂PO₄ as a function of time. It can be seen that according to time the evolution of the SPCE signal can be divided into four groups – before the start of spraying (before point A), during spraying (between point A and B), signal build-up (between point B and D) and relaxation of the signal (point D). It is seen that in the before the start of spraying, the SPCE signal is rather constant due to the lack of pollutant on the sensor surface. With the start of fog spraying (point A), there is characteristic peak which is formed (between point A and B). This peak is due to the influence of the fog particles that alter the effective surface of the sensor. After the initial peak, there is a significant change in signal amplitude for the duration of tens of seconds (B-D). This is the period in which the pollutant sprayed in the environment interacts with the surface of the sensor and the signal is accumulated. After the relaxation of the fog, the amount of pollutant decreases and so thus the measured signal (point D and beyond).

5. Conclusion

A portable device capable of measuring the surface photo-charge effect is demonstrated. The design, the principles of work and the capabilities of the device SPCE Meter 1 are described in this report. It relies on selection and amplification of the weak SPCE signal from the sensor. The capabilities of the device are demonstrated in real on-site measurements of pollution decontamination with fog.

Acknowledgement

This work has been funded by EU FP7 Security program under contract COUNTERFOG 312804

References:


MONITORING OF THE NATURAL RADIOACTIVE FUND AND RADIOACTIVE POLLUTION - AN IMPORTANT FACTOR OF NUCLEAR SECURITY IN BULGARIA

НАБЛЮДЕНИЕТО НА ЕСТЕСТВЕНЯ РАДИАОКТИВЕН ФОН И РАДИАОКТИВНОТО ЗАМЪРСЯВАНЕ – ВАЖЕН ФАКТОР НА ЯДРЕНАТА СИГУРНОСТ НА БЪЛГАРИЯ

Ass. Professor, Ph.D, eng. Dolchinkov N. T.

„Vasil Levski“ National Military University, Veliko Tarnovo, Bulgaria

n_dolchinkov@abv.bg

Abstract: The radioactive contamination has actual national and international importance. It is related to the increasing the prevention measures of accidents as consequences of exploring the nuclear energy for peaceful purposes, and in the military purposes as well. The optimization and management of operational systems for monitoring of radioactive background should bring the increasing of nuclear Bulgarian safety, and the quality of the population defense from expose to radiation, as a consequence of changing the characteristics of the natural radioactive background.

Keywords: radioactive contamination, measures of prevention, optimization, monitoring, radioactive background, population defence, expose to radiation

1. Introduction

Nuclear power worldwide provides around 30% of global electricity production. Under normal operation of the NPP there is no major risk and the potential damage to the population and nature is much lower than in the areas around the TPP or the large chemical plants. Nevertheless, the danger of radiation and nuclear accidents should not be overlooked. In both cases we can expect significant radioactive contamination of the environment. Properly controlled control of possible radioactive contamination depends on the preservation of human, animal health and possible decontamination actions in the environment and food products.

At present, more than 510 Nuclear Power Units operate in the world. Of these, 163 are in Western Europe, 121 in the United States, 45 in Russia, and the rest in 29 other 5 continents.

2. NPP

It is known that atomic reactors are devices to maintain a controlled chain reaction. For fuel, the isotopes Uranus 233, Uranus-235 and Plutonium -239 are mainly used. The division of the kernels of these elements does not occur spontaneously, as with the nuclear weapon, but is controlled so that the separated heat is used to produce electrical energy. A stationary controlled chain reaction is carried out in the reactors. Critical chain reaction conditions are created, in which the neutron multiplication factor is close to one (K = 1). Therefore, for a stationary chain reaction, it is necessary for at least one neutron from the first division of the first generation to cause a second division and at least one neutron from the second division (second generation) to cause a third division, . When K <1 occurs under subcritical mode, the number of divisions gradually decreases and the reaction stops. At K> 1 counts of fission nuclei increase and the chain reaction is amplified. It is these conditions that make it possible to control the operation of each reactor, depending on the consumption of electrical energy. Thus, in case of shortage of electric energy, the velocity of the chain reaction increases, and in the case of excess energy, we reduce the rate of division.

It is known that all reactors consist constructively of: an active zone in which the fuel elements are located and which is surrounded by a neutron reflector. Fuel elements are made of uranium oxide or metallic uranium, placed in thin-walled metal sheaths (steel, aluminum and various alloys). The metal envelope must provide a high degree of sealing and long-term reliability of the fuel elements.

Neutron retarder uses graphite, heavy water, plain water. Water, heavy water, liquid sodium, nitrogen, diphenylmethane and other combined liquids may be used as a coolant or cooler. An important element is the rate-control system of the chain-nuclear reaction. It provides a critical mode or the reaction can be delayed or stopped altogether. The larger number of reactors uses cadmium, boron and other materials that absorb the neutrons. They are removed or introduced into the core area, thereby regulating the chain reaction. Additionally, the reactor should have protective devices that reduce the dose of gamma rays and neutrons emitted from the core. This is the reactor casing, which consists of 3 layers - lead, cadmium and concrete. Synchronized operation of the reactor is accomplished by a remote control console.

The operating reactors at the Kozloduy NPP are of the 1000 W water-type type (BBEP-1000). The water of the so-called primary circuit serves as a retarder of neutrons and as a coolant. It is heated by the fuel elements to a high temperature and is under high pressure. Through it the heat is transmitted to the water of the second loop, which is converted into steam entering the steam generator and the turbine for generating electrical energy.

The water from the first circuit in the water-water reactors is always contaminated with radioactive substances. This is due to the neutron irradiation of metal corrosion products as well as the impurities and contamination of the liquid coolant in the core and become secondary radioactive. In addition, in the case of impaired leakage of fuel elements, nuclear fission products may be introduced into the first loop. Water contaminated with radioactive substances from the first contour is subject to decontamination and purification by means of ion exchange filters. In modern types of NPPs, such purification is also provided for water from the second contour. The radioactive elements emitted from the heat carrier are fed into the atmosphere through high chimneys where they are diluted in a large volume of air. It is obvious that the normal operation of the NPP is related to a certain, low level of environmental pollution with radioactive substances. For the most common reactors - water-water, the major radiological pollutants are the radioactive isotopes of noble gases and iodine. In the radioactive mixture were found the isotopes of the crypton, 15 of the xenon and 20 of the iodine. More important for the formation of the radiation environment around the nuclear power plants are crypton - 85, xenon - 133 and xenon - 135, iodine - 131 and iodine - 133. They have a small half-life and are in insignificant quantities. It should be noted that atmospheric discharges in the normal operation of the reactor, the so-called controlled discharges, do not pose a risk of environmental pollution. This process is technically

125
controlled, resulting in completely safe dilutions that do not lead to an increase in the radiation background.

Much more dangerous for the radioactive contamination of the biosphere are the accidents that can occur at the NPP.

A radiation accident is called a breach of safe operating ranges, where radioactive products or ionizing radiation go beyond the norms, and disruption of normal operation of devices and equipment containing sources of ionizing radiation is required.

A nuclear accident is called the damage to the nuclear reactor fuel elements and emergency exposure to personnel.

For normal NPP operation it is assumed that up to 1% of the fuel element cladding has gas permeability (micro cracks) with respect to isotopes of cryopentone, xenon and iodine and up to 0.1% non-hermetic, allowing contact of coolant with nuclear fuel. The magnitude of the accident and the corresponding environmental consequences vary widely. The majority of previous accidents are small and have caused increased contamination with radioactive elements in restricted areas near the reactor. The worst and most dangerous accidents in the nuclear power plant have so far been due to a sharp increase in reactor power due to the acceleration of the chain steam explosion, which could destroy various installations and dehumidify the system. From the information related to some major accidents in the NPP, the reasons are the following: Operator errors, failure of the equipment and deficiencies in the construction. The most frequent cause of past accidents is the mistakes of the personnel servicing the installations of the individual reactor.

3. Radionuclides

A characteristic feature of the discharges is that the majority of the radioactive aerosols are deposited by the mechanism of local deposits near the plant itself. Another part, depending on the magnitude of the accident, may fall into the troposphere and fall to the ground as tropospheric deposits. From the character of the distribution of radionuclides in the atmosphere and their deposition on the Earth's surface will also be the individual doses of irradiation of the people, located on the radioactively contaminated territory. Formation of dose of gamma- and beta-emitting isotopes from discharges under emergency conditions at NPPs has a direct and indirect impact. The direct path refers to external radiation with gamma-quanta and beta-particles of radioisotopes contained in the atmosphere or fallen on the Earth's surface. This fact suggests the relevance of this study as it is directly related to the proper organization of radioactive contamination control.

It should be noted that in the period 1945-1991 the total number of nuclear explosions on our planet is 2059, including 508 in the atmosphere. The largest number of such outbreaks were committed in the United States - 1085 and 205, respectively. Secondly, Russia 715 and 215 respectively, France 182 blasts (45 in the atmosphere). Britain, respectively 42 (21 in the atmosphere). China respectively 35 (22 in the atmosphere). It is known that until 1962, the main source of environmental contamination with radioactive substances was nuclear weapons. After the conclusion of the treaty banning nuclear experiments in the air, on the Earth's surface and under water, the radioactive contamination of the Earth significantly decreased. Despite the 1962 ban, separate nuclear blasts were committed by France, India, Pakistan and North Korea.

On the other hand, the widespread adoption of modern technologies in the national economy, medicine, science and industry using sources of ionizing radiation creates a risk of radioactive substances being released into the external environment. The most important prerequisite for radionuclide dissipation in the biosphere arises in the disruption of the mode of operation and in accidents in the constantly increasing number of atomic reactors, which leads to the release of radioactive aerosols into the atmosphere.

Radioactive aerosol split products fall onto the earth's surface in the form of local, tropospheric or stratospheric deposits. As a result, they accumulate in the soil, plants, animals, water of open waters and their flora and fauna. This undoubtedly calls for a stable organization of radioactive contamination control. This organization should also include the study of the migration patterns of radio stones important in terms of radio storing strontium-90 and cesium-137 in the different sites of the biosphere. For example, strontium-90 is distributed in objects similar to the calcium element and the second (albeit to a lesser extent) potassium. Here are the group chemical similarities of these radioactive elements. This has important practical implications both for the intelligence of contaminated sites and for the elimination of the consequences of degraded nuclear power plants. Under the same conditions in the biosphere sites contaminated with radioactive substances, the maximum concentration of strontium-90 in them is always found in the organs physiologically rich in calcium (bones, egg shells) and the maximum concentration of cesium-137 in sites rich in potassium (muscles).

The formation of radioactive contamination depends largely on the state of atmospheric air. Radioactive aerosols by degree, area of distribution, fall and radiochemical composition form radioactive contamination in the local spaces around the accident, in the troposphere, as well as in the stratosphere.

Local radioactive contamination is formed in the area of the accident and forms different zones of contamination, which can be tens and hundreds of kilometers in size. The shape and contours of the radioactively contaminated area are mainly determined by the energy of the explosion, the weather conditions (the complex system of winds at different heights and their velocity), the relief of the area, the particle size, the duration of the discharges, the physico-chemical status of the dividing products.

Local radioactive contamination settled on the Earth's surface within 24 hours. They are dry, i.e. fall regardless of the rain. The speed of their fall is under the influence of gravity. Chemically, they are a mixture of nuclear fission products, with the predominance of short-lived isotopes. The major radioisotope is iodine-131, which has a half-life of 8 days. Depending on the level of radioactive contamination in the area, a gamma-field of different power is formed. Due to the rapid decomposition of the short-lived radioisotopes, the activity of the area relatively quickly diminishes. Danger of increased local fall of radioactive products after a radiological emergency occurs under adverse weather conditions. Thus, in the event of heavy clouds after the blast, rain may fall as radioactive particles become condensation centers. When the radioactive cloud mixes with a rainy front, it can take a significant amount of split products together to produce rays and a high level of radioactive contamination of a limited area together with raindrops. Similarly, snow attracts radioactive products and can cause severe radioactive contamination of the Earth's surface. This requires particular attention in predicting accidents as well as in conducting intelligence to delineate areas of actual contamination.

In more powerful blasts (like the Chernobyl nuclear power plant), dividing products can fall into the troposphere. A characteristic feature of these radioactive contamination is that they fall very slowly, on average for about 30 days. There is a large radioactive trace, sometimes sometimes up to several thousand kilometers. The density of soil contamination with them, compared to local deposits, is much smaller. In the troposphere, the main meteorological processes occur - cloud formation, precipitation, air currents, cyclones, etc. The radioactive cloud in the troposphere from which the tropospheric deposits form, changes its original volume under the influence of gas and turbulent diffusion. Gradually the air currents tear it apart. Vertical displacement of atmospheric layers may lead to intensive deposition of radioactive substances in separate areas of the Earth's surface. Of much greater importance for the rapid displacement of radioactive particles in the troposphere have the dominant horizontal air currents.

The most important factor to purify the troposphere from the radioactive particles is precipitation. Especially important is their importance in moderate latitudes. Atmospheric precipitation changes the three main characteristics of radioactive contamination: density of 24-hour deposition, specific activity of rainwater and concentration of radioactive products in the ground air layer.
In the absence of rainfall, only the nearest air layer is subject to the removal of radioactive particles. It is in constant contact with the Earth's surface and as a result of the turbulent motion is constantly being renewed. Increased deposition of dividing products is observed, with an increase in atmospheric pressure when air masses from the top of the troposphere begin to move in the direction of the ground. The amount of radioactive particles that fall as a result of the above processes varies considerably on days.

Radioactive aerosols form different fractions in the troposphere, which are removed from there at different rates. A late fall (1-2 years after the accident) of radioactive products was found. This is explained by the presence of aerosol fractions smaller than 5 micrometers, which due to their physicochemical properties are washed less than the rain.

Radioactive substances that fall on the soil and form the pollution zones depend on the following factors: the physico-chemical properties of the isotopes, the type of chemical compounds, some parameters of the external environment, etc.

One of the main properties of radioactive substances determining their soil behavior is their water solubility. According to the literature, about 1-10% of the division products that are formed in a radiation accident are soluble. These include the compounds of strontium, cesium and iodine. The rest of the radioactive substances fallen to the ground is practically insoluble. It is noteworthy that about 60-70% of strontium-90 deposited on the soil is in soluble form available to plants.

The large insoluble particles of the dividing products are retained in the top layer of the soil. They have a very limited ability to penetrate into depth. The smaller ones adhere to the soil components. The quantity and qualitative composition of humus also influence. The rate of migration and depth of penetration depend not only on the type of soil but also on its water regime (groundwater level). Severe clay soils retain more heavily radioactive substances than sandy ones.

It is estimated that 80% of the radioisotope deposited on the ground is retained in the upper layer (from 0 to 25 cm) of the clay soils. In other soils, they penetrate to a few tens of centimeters. It is known that the major part of the radiochemistry is located in the soil layer 0-10 cm thick. This is the area in which the root system of the pasture plants develops. 40-80% of the isotope were in the 0-5 cm layer, and 20-60% penetrated deeper. The movement of the radioisotope in depth on the precipitous sandy soils takes place alongside the downstream waters. In hardly permeable clay soils, the transfer in the same direction is mainly due to ionic and molecular diffusion.

We must take into account the special moments in the cesium-137 movement, which is radionuclide-important radionuclide. Not all of its ions are equally tightly bound to the soil. Some of them are attached to the soil particles by cation exchange and form the exchange fraction of the isotope. Another part is fixed for the mineral constituents of the soil and it is an unchanged fraction. Over time, the quantitative ratio of the two fractions changes as part of the non-variable fraction becomes available to plants. Compared to clayey, sandy soils are more easily attributed to the non-quench fraction.

Radioactive strontium retains well from the soil, but unlike radioactive cesium, its relationship to soil elements is not stable. Under the influence of the neutral salts contained in the soil solutions, it is easily distributed in groundwater and plants. The amount of strontium-90 that comes to the plants through the roots depends on many factors: the radioisotope concentration in the soil, the presence of free calcium, the plant species, etc. Like radioactive cesium, it translates into larger quantities of sandy than clay soil and rich in organic impurities. There are known examples showing that the amount of radioactive strontium passed to the plants is about 3% of the total amount of soil occupied by the root system.

As noted, the main pollutant of the NPP biosphere is iodine-131. It has a relatively short half-life, and its absorption from plants through the roots is a slow process. Therefore, soil contamination with iodine-131 is of no practical significance for the implementation of the air-soil-plant-animal-human migration chain.

Pollution of water in open waters - rivers, lakes, dams, with radioactive substances can be different. Most important is the release of liquid radioactive waste or the accidentally discharged from the NPP aerosols, which are subsequently precipitated under the water surface. It is also dangerous to wash out the rains of radioactively contaminated terrestrial areas.

Radioactive elements infiltrated into the pond may have different behavior depending on their concentration in water, the nature of the pollution and the radiation situation on the shore. The following factors are important: type of joint, water composition, temperature, etc. The isotopes retained on the solid particles floating in the water are gradually deposited at the bottom of the pond. The rate of precipitation depends on the particle size, the nature and magnitude of the electrical charge, the velocity of the water flow, the presence of a turbulent motion. The majority of radioactive substances are deposited at the bottom of the basin, and a smaller part on the aquatic plants. The distance that radionuclide passes into the pool is determined mainly by its solubility and its half-life. Soluble long-lived radioisotopes can pass enormous distances.

As a result of the precipitation of radioactive substances, the surface layer of the bottom is most intensively polluted. Very important in this respect is the type of soil from which it is formed. Highest sorption capacities have bottoms that are made of clay particles and organic matter. The long-term contamination of long-lived isotopes leads to their penetration into depth of the lower deposits and to the soil forming the bottom of the basin. Depth of penetration depends largely on water permeability of soil layers. Reverse entry into the water of radioactive substances retained by the bottom depends to a large extent on the alkaline-acid equilibrium. In an acidic environment, up to 50% of all radionuclides contained in the sludge are released into the water. It is easiest to leave the muddy radio station - up to 84-87% of the total radioactivity. Neutral salts also accelerate the release of radionuclides sorbed by the bottom.

It is obvious that the bottom plays the role of a depot for the radionuclides that have fallen into the basin and ensures their return to the water after the radioactive contamination has ceased. Therefore, the discharge into the open waters of heavy and other radioactive waste containing long-lived radionuclides should not be allowed under any circumstances. The presence of such should be strictly controlled and limited to free access.

The magnitude of concentration of radionuclides in plants and their products depends on many reasons. There is a direct link between the amount of radioactive pollutants in a given locality and the concentration of radionuclides in plants. With equal other conditions in mountain areas, grass and crops contain a higher concentration of radioisotopes than in the plains. It is assumed that in the areas situated at 1000 m above sea level the activity of the grass is 3-4 times higher than in the lowlands. The vegetation exposed to open winds has been shown to be more active than the one found in wind-protected areas. The activity of vegetation also depends on the amount of rainfall. The availability of radioactive deposits for vegetation depends on the water bivalence of their compounds in the biosphere. There are two main pathways to radioactive contamination of plants - through the roots and directly through the surface of their organs. The importance of the former is determined by the extent and nature of the radioactive contamination of the soil, its species, chemical composition, water content, etc. An important factor is the ability of the radionuclide to saturate from the soil. As much as this property is more pronounced, the smaller the amount of radioactive element penetrates the plants. Through the root system, radioisotopes are converted into ionic form or as salts (carbonates, sulphates). The penetration of the radioisotopes through the exposed parts of plants is as intense as their higher concentration in the air. The absorption of radioactive substances from the soil flora also depends on the properties of the chemical elements, the type of plants, the conditions of their cultivation, etc. It is currently assumed that the foliar pathway of radionuclide penetration in plants is paramount.
and root is secondary. Besides the initial deposition of the radioactive deposits on the leaves of the plants is also observed secondary - by the wind. A known part of the surface parts of the soil, together with the radionuclides in them, rise into the air in the form of ground dust and then are deposited and fixed on the plants.

Cesium-137, Barium-140 and Iod-131 are almost entirely absorbed through the leaves. The remaining radionuclides are sucked through the leaves considerably less. It is interesting to know that the radiosynthesis is sucked into plants through the leaves several hundred times more than strontium and is very mobile ie. quickly spreads throughout the plant. In iodine, it has been found that in gaseous form the radionuclide is incorporated by plants better than the aerosol form that remains on the surface of the plants. A large part of a radio station, falling on the leaves, stays at the site of the attack and migrates a little inside the plants. For this reason, this radioisotope is found in the leaves in larger quantities, compared to the rest of the plants.

Strontium-90 is rooted twice as much as cesium-137, despite the fact that the last radioisotope is in a higher concentration in the soil. Typical of other nuclear cerium products such as cerium, ruthenium, zirconium, yttrium, tellurium, plutonium, which are normally absent in plants, are poorly absorbed in the process of mineral soil metabolism. They are retained by soil particles and only small quantities of them pass through the root system.

Different types of agricultural plants to varying degrees absorb radionuclides. These differences can be observed even in the different plant species of one family. This is mainly related to the construction of leaves and roots. Leaves with more pronounced relief hold more radio aerosols. The age of the plant has a significant impact on the accumulation of radionuclides in it. Perennials always have more activity than annuals. In this regard, the lichen example is very prominent. They are perennial, grow slowly, are devoid of roots and receive mineral substances only from falling aerosols. For this reason, the strontium-90 concentration is 20 times higher than in the surrounding pastures.

Between the various parts of the plants radionuclides are distributed unevenly. Grains, seeds and fruits have been found to retain fewer radioisotopes than in leaves and stems of plants. In the shell their concentration is greater than the core. For this reason, no more than 15% of the radioactive strontium contained in the wheat grain is present in the flour.

All mentioned radioactive contamination features require specificity in the organization of radioactive contamination control.

4. Conclusions:

1. The formation of radioactive contamination and its behavior is of interest for both preventive measures and after a nuclear or nuclear accident at the NPP.
2. Radioactive contamination in a radiological or nuclear accident will be determined by a wide range of factors that determine the contamination of tropospheric air, soil, water, plants and the overall environment.
3. Optimized control of radioactive contamination following an accident contributes to the proper organization of evacuation rescue operations as well as to the decontamination of contaminated areas and food products.

4. Literature:

DETERMINATION OF CHANGE OF THE POINT OF THE FIRE SHOTS AT SHOOTING WITH FITTED CHAMBER TYPE SUPPRESSOR

Faculty of “Artillery, air defense and CIS” —National Military University “Vasil Levski”, Veliko Tarnovo, the Bulgarian Republic
vvganev@abv.bg

Abstract: Part of the global trends related with the development of armaments are currently focused on creating new samples of small arms and device which have increased combat effectiveness.

Two of the factors that have a significant impact on combat effectiveness are grouping and accuracy in shooting. Installation of the silencer on small arms leads to a change of these factors, especially when must be shoot at long distances.

The report scrutinizes an experimental investigation on the mathematical ratio of hit point on the target at shooting with small arms with fitted silencer of the chamber type with rubber chopper wheel.

Keywords: SMALL ARMS, SUPRESOR, MIDPOINT OF THE HITS.

1. Introduction

The use of special weapons in counter-terrorist operations with fitted suppressors and the necessity of reliable target damage even while using individual ballistic armor protection details initiates the need for combatant to consider for the changes of the weapons ballistic characteristics. The ballistic characteristics of the weapon are changed by the use special ammunition.

Suppressor fitting on the small arms causes a deviation from midpoint of hits and necessitates the determination of the dependencies between the horizontal and vertical deviations and the number of shots fired.

In the Republic of Bulgaria, main type of small arm is the automatic rifle AK-47. The suppressor designed for AK-47 is PBS-1, a chamber type suppressor with a rubber chopper wheel.

The science investigation presented in this report is a sequence of researches that include: examine the deviation of hits midpoint, the grouping, and the dimensions of target area limits.

2. Experimental investigation

2.1. Purpose: experimentally determine the dependence under which changes in the hit points are relative to the control point in a semi-automatic fire mode with small arms fitted with a chamber type suppressor with a rubber chopper wheel.

2.2. Tasks:

- to determine the mathematical expectation and the standard deviation of the impact points;
- to determine the dependence under which changes in the hit points are relative to the control point;

In order to achieve the purpose of this report, data obtained from the experimental investigation will be used, described in [1]. The automatic rifle fitted with the suppressor is installed in the "Samozhenkov" stand in order to exclude any errors that might unintentionally be done by the shooter. The distance to the target is 100 meters, the target dimensions are 1000x1000 mm, the rounds used are the 7.62x39 mm “MD” specially designed for shooting with the PBS-1. Shots are fired in 10 series of 20 shots each at a temperature of 21°C under normal atmospheric pressure and windless. Deviations of the hits from the control point in the horizontal and vertical plane are to be determined.

Deviations of the hits from the control point are shown horizontally in Table 1 and vertically in Table 2.

Table 1: Deviations of hits from control point horizontally

<table>
<thead>
<tr>
<th>Series №</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-83</td>
<td>-189</td>
<td>-197</td>
<td>-95</td>
<td>-164</td>
<td>22</td>
<td>-12</td>
<td>-70</td>
<td>-273</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-70</td>
<td>-84</td>
<td>-206</td>
<td>-206</td>
<td>-172</td>
<td>-182</td>
<td>22</td>
<td>-15</td>
<td>-83</td>
<td>-284</td>
</tr>
<tr>
<td>3</td>
<td>-74</td>
<td>-313</td>
<td>-250</td>
<td>-206</td>
<td>-198</td>
<td>64</td>
<td>-35</td>
<td>-100</td>
<td>-312</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>-106</td>
<td>-102</td>
<td>-220</td>
<td>-258</td>
<td>-209</td>
<td>-200</td>
<td>75</td>
<td>-38</td>
<td>-113</td>
<td>-327</td>
</tr>
<tr>
<td>5</td>
<td>-102</td>
<td>-110</td>
<td>-237</td>
<td>-265</td>
<td>-224</td>
<td>-205</td>
<td>10</td>
<td>-10</td>
<td>-128</td>
<td>-358</td>
</tr>
<tr>
<td>6</td>
<td>-125</td>
<td>-120</td>
<td>-249</td>
<td>-266</td>
<td>-225</td>
<td>-228</td>
<td>-11</td>
<td>-83</td>
<td>-128</td>
<td>-358</td>
</tr>
<tr>
<td>10</td>
<td>-152</td>
<td>-180</td>
<td>-268</td>
<td>-278</td>
<td>-241</td>
<td>-240</td>
<td>-11</td>
<td>-120</td>
<td>-140</td>
<td>-370</td>
</tr>
<tr>
<td>14</td>
<td>-188</td>
<td>-211</td>
<td>-279</td>
<td>-256</td>
<td>-286</td>
<td>-264</td>
<td>-10</td>
<td>-158</td>
<td>-174</td>
<td>-406</td>
</tr>
<tr>
<td>16</td>
<td>-194</td>
<td>-240</td>
<td>-319</td>
<td>-294</td>
<td>-285</td>
<td>-236</td>
<td>-8</td>
<td>-26</td>
<td>-180</td>
<td>-412</td>
</tr>
<tr>
<td>18</td>
<td>-223</td>
<td>-253</td>
<td>-299</td>
<td>-342</td>
<td>-318</td>
<td>-100</td>
<td>-9</td>
<td>-224</td>
<td>-195</td>
<td>-432</td>
</tr>
<tr>
<td>20</td>
<td>-283</td>
<td>-310</td>
<td>-343</td>
<td>-414</td>
<td>-358</td>
<td>-386</td>
<td>-9</td>
<td>-197</td>
<td>-236</td>
<td>-485</td>
</tr>
</tbody>
</table>

Table 2: Deviations of hits from control point vertically

<table>
<thead>
<tr>
<th>Series №</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>135</td>
<td>330</td>
<td>188</td>
<td>83</td>
<td>44</td>
<td>-52</td>
<td>8</td>
<td>156</td>
<td>58</td>
<td>346</td>
</tr>
<tr>
<td>2</td>
<td>68</td>
<td>321</td>
<td>95</td>
<td>15</td>
<td>66</td>
<td>-45</td>
<td>-70</td>
<td>31</td>
<td>64</td>
<td>293</td>
</tr>
<tr>
<td>3</td>
<td>180</td>
<td>319</td>
<td>101</td>
<td>110</td>
<td>53</td>
<td>-34</td>
<td>-24</td>
<td>129</td>
<td>58</td>
<td>398</td>
</tr>
<tr>
<td>4</td>
<td>159</td>
<td>344</td>
<td>65</td>
<td>113</td>
<td>25</td>
<td>-24</td>
<td>-25</td>
<td>8</td>
<td>119</td>
<td>51</td>
</tr>
<tr>
<td>5</td>
<td>220</td>
<td>297</td>
<td>128</td>
<td>130</td>
<td>63</td>
<td>-42</td>
<td>-5</td>
<td>83</td>
<td>33</td>
<td>264</td>
</tr>
<tr>
<td>6</td>
<td>118</td>
<td>315</td>
<td>444</td>
<td>34</td>
<td>-22</td>
<td>-20</td>
<td>-17</td>
<td>178</td>
<td>18</td>
<td>268</td>
</tr>
<tr>
<td>7</td>
<td>138</td>
<td>274</td>
<td>140</td>
<td>32</td>
<td>-37</td>
<td>-45</td>
<td>-45</td>
<td>144</td>
<td>17</td>
<td>268</td>
</tr>
<tr>
<td>8</td>
<td>229</td>
<td>268</td>
<td>151</td>
<td>107</td>
<td>19</td>
<td>-68</td>
<td>8</td>
<td>135</td>
<td>26</td>
<td>314</td>
</tr>
<tr>
<td>9</td>
<td>142</td>
<td>369</td>
<td>38</td>
<td>76</td>
<td>-22</td>
<td>-21</td>
<td>-135</td>
<td>56</td>
<td>188</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>278</td>
<td>328</td>
<td>140</td>
<td>8</td>
<td>42</td>
<td>-37</td>
<td>-83</td>
<td>198</td>
<td>147</td>
<td>282</td>
</tr>
<tr>
<td>11</td>
<td>155</td>
<td>286</td>
<td>145</td>
<td>8</td>
<td>42</td>
<td>-37</td>
<td>-83</td>
<td>198</td>
<td>147</td>
<td>282</td>
</tr>
<tr>
<td>12</td>
<td>135</td>
<td>306</td>
<td>187</td>
<td>16</td>
<td>-64</td>
<td>-6</td>
<td>-17</td>
<td>56</td>
<td>338</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>141</td>
<td>266</td>
<td>103</td>
<td>60</td>
<td>63</td>
<td>-64</td>
<td>-6</td>
<td>-17</td>
<td>56</td>
<td>338</td>
</tr>
<tr>
<td>14</td>
<td>171</td>
<td>322</td>
<td>210</td>
<td>108</td>
<td>168</td>
<td>-50</td>
<td>-122</td>
<td>20</td>
<td>-62</td>
<td>344</td>
</tr>
<tr>
<td>15</td>
<td>188</td>
<td>179</td>
<td>135</td>
<td>121</td>
<td>65</td>
<td>-22</td>
<td>-42</td>
<td>96</td>
<td>-23</td>
<td>243</td>
</tr>
<tr>
<td>16</td>
<td>170</td>
<td>306</td>
<td>170</td>
<td>123</td>
<td>98</td>
<td>-50</td>
<td>-2</td>
<td>24</td>
<td>44</td>
<td>298</td>
</tr>
<tr>
<td>17</td>
<td>155</td>
<td>326</td>
<td>177</td>
<td>91</td>
<td>114</td>
<td>-92</td>
<td>-4</td>
<td>18</td>
<td>-9</td>
<td>345</td>
</tr>
<tr>
<td>18</td>
<td>161</td>
<td>262</td>
<td>218</td>
<td>72</td>
<td>134</td>
<td>-83</td>
<td>8</td>
<td>77</td>
<td>4</td>
<td>173</td>
</tr>
<tr>
<td>19</td>
<td>254</td>
<td>246</td>
<td>160</td>
<td>125</td>
<td>92</td>
<td>-32</td>
<td>5</td>
<td>-14</td>
<td>45</td>
<td>244</td>
</tr>
<tr>
<td>20</td>
<td>171</td>
<td>57</td>
<td>55</td>
<td>102</td>
<td>78</td>
<td>-76</td>
<td>-4</td>
<td>-43</td>
<td>36</td>
<td>192</td>
</tr>
</tbody>
</table>
The results are recorded in the following matrix:

\[
m = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & & \vdots \\
 a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}
\]

The quantities are defined as:

\[n = 10 \text{ – number of series;}
\]
\[m = 20 \text{ – number of shots per series.}
\]

To define the mathematical expectation and the standard deviation of the hits by using mathematical software Matlab, following equations would be used:

- for the mathematical expectation
  \[\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i,\]

- for the standard deviation
  \[\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})^2}\]

In these equations, the quantities are defined as:

\[n\] - number of series on the basis of which the arithmetic mean value is determined;
\[x_i\] - value of \(i^{th}\) \((i=1..n)\) examined deviation.

In order to determine the minimum required number of shots that provide confidence interval of 99.9%, the following equation is used:

\[n = \frac{S^2 u^2}{\varepsilon^2} = \frac{5.71^2 \times 3.37^2}{4.57^2} = 17.7\]

This equation, the quantities are defined as:

\[u^2\] - is a quantile of the normal distribution that provide confidence level of 99.9%
\[S\] - standard deviation calculated using the formulas:

\[S = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2};\]

\[\varepsilon\] - accuracy of the estimation of mathematical expectation calculated by the formulas \[\varepsilon = t_{\frac{\alpha}{2}} \frac{S}{\sqrt{n}}\] - \(t_{\frac{\alpha}{2}}\) a quantile of the Student’s normal distribution.

Twenty shots in series were fired during the investigation, satisfying the requirement of the minimum required number of shots - 18.

In table 3 the mathematical expectation and the standard deviation of the hits in horizontal and vertical plane are presented.

**Table 3:** Mathematical expectation and standard deviation of series hits

<table>
<thead>
<tr>
<th>Series No</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>X horizontally in millimetres</td>
<td>153.2</td>
<td>-178.6</td>
<td>-265.2</td>
<td>-290.0</td>
<td>-255.8</td>
<td>-252.1</td>
<td>-41.3</td>
<td>-127.7</td>
<td>-150.3</td>
<td>-379.8</td>
</tr>
<tr>
<td>Y vertically in millimetres</td>
<td>168.2</td>
<td>283.1</td>
<td>152.7</td>
<td>66.0</td>
<td>51.7</td>
<td>-51.1</td>
<td>10.9</td>
<td>76.0</td>
<td>11.3</td>
<td>263.1</td>
</tr>
<tr>
<td>(\sigma) horizontally in millimetres</td>
<td>64.8</td>
<td>64.3</td>
<td>37.9</td>
<td>49.1</td>
<td>58.5</td>
<td>50.7</td>
<td>63.4</td>
<td>73.5</td>
<td>41.8</td>
<td>52.0</td>
</tr>
<tr>
<td>(\sigma) vertically in millimetres</td>
<td>47.3</td>
<td>63.8</td>
<td>48.2</td>
<td>47.1</td>
<td>71.8</td>
<td>22.4</td>
<td>43.4</td>
<td>83.4</td>
<td>32.6</td>
<td>90.6</td>
</tr>
</tbody>
</table>

Using the mathematical expectation, Matlab’s Curve Fitting application has proposed the following dependencies for changing the hit point:

- in the horizontal direction:
  - Linear Fitting:
    \[y = a\sin(x - \pi) + b(x - 10)^2 + c\]
    \[a = -10.86\]
    \[b = -0.05873\]
    \[c = -20.8\]

- Polynomial:
  \[y = p_1 x^8 + p_2 x^7 + p_3 x^6 + p_4 x^5 + p_5 x^4 + p_6 x^3 + p_7 x^2 + p_8 x + p_9\]
  \[p_1 = -0.0659\]
  \[p_2 = -2.474\]
  \[p_3 = -53.4\]
  \[p_4 = -457.2\]
  \[p_5 = -3148\]
  \[p_6 = -9525\]
  \[p_7 = -2.246 e^4\]
  \[p_8 = -2.029 e^4\]
  \[p_9 = -9503\]

- Rational:
  \[y = \frac{p_1 x^4 + p_2 x^3 + p_3 x^2 + p_4 x + p_5}{x + q_1}\]
  \[p_1 = -1.051\]
  \[p_2 = 19.08\]
  \[p_3 = -106.7\]
  \[p_4 = 176.1\]

![Graph of deviation of the hit point from the control point calculated using Linear Fitting.](image1)

![Graph of deviation of the hit point from the control point calculated using Polynomial.](image2)
Fig. 3 Graph of deviation of the hit point from the control point calculated using Rational.

- in the vertical direction:
  - Linear Fitting:
    
    \[ y = a \sin(x - \pi) + b(x - 10)^2 + c \]
    
    \[
    \begin{align*}
    a &= -1,11 \\
    b &= 0,1683 \\
    c &= 5,163
    \end{align*}
    \]

Fig. 4 Graph of deviation of the hit point from the control point calculated using Linear Fitting.

- Polynomial:
  
  \[ y = p_1 x^8 + p_2 x^7 + p_3 x^6 + p_4 x^5 + p_5 x^4 + p_6 x^3 + p_7 x^2 + p_8 x + p_9 \]

  \[
  \begin{align*}
  p_1 &= 0,0004949 \\
  p_2 &= -0,01196 \\
  p_3 &= 0,02677 \\
  p_4 &= 1,804 \\
  p_5 &= -2,375 \\
  p_6 &= 1,338 \\
  p_7 &= -3,831 \\
  p_8 &= 5,244 \\
  p_9 &= -2,364
  \end{align*}
  \]

Fig. 5 Graph of deviation of the hit point from the control point calculated using Polynomial.

- Rational:
  
  \[ y = \frac{p_1 x^5 + p_2 x^4 + p_3 x^3 + p_4 x^2 + p_5 x + p_6}{x + q_1} \]

  \[
  \begin{align*}
  p_1 &= 1590 \\
  p_2 &= -4,497e^4 \\
  p_3 &= 4,771e^5 \\
  p_4 &= -2,29e^6 \\
  p_5 &= 4,559e^6 \\
  p_6 &= -2,035e^6 \\
  q_1 &= 3,983e^4
  \end{align*}
  \]

Fig. 6 Graph of deviation of the hit point from the control point calculated using Rational.

3. Conclusions

The deviation of the hit point can be described with dependencies of the Linear Fitting, Polynomial and Rational types. If it is necessary to calculate the alteration of the hit point in the horizontal and vertical directions, it is advisable to use Polynomial equations, due to the most exact match with the experimental data.

The alteration of the hit point in horizontal direction - to the left and in vertical direction - in the upward direction

Graphs analysis shows that the value of the deviation in both directions increases steadily up to 200 shots permissible for the rubber chopper wheel, and then the deviation value become much higher.

Due to the specific characteristics of these alterations of the hit point in continuous shooting with a chamber type suppressor with a rubber chopper wheel requires additional training of the shooters.
REFERENCES


5. Потемкин В. Г., Система инженерных и научных расчетов MATLAB, Том 1 и 2, М., 1999.


11. Цонев Ц. Г., Богданов А. И., Проверка боя и привеждане на стрелковото оръжие към нормален бой, Шумен 2006.
Abstract: Field tests of fiber-reinforced concrete (FRC) and reinforced concrete specimens were performed by research team from Faculty of Civil Engineering, Czech Technical University in Prague, Czech Republic in cooperation with University and the Czech Army corps in the military training area Boletice. The test were performed using real scale reinforced concrete precast slabs (6 x 1.5 x 0.3 m) with varying fiber type, fiber strength, fiber content and concrete strength class. TNT charges of 25kg placed at distance from the slab for better simulation of real in-situ conditions. The paper presents conclusions from sets of tests from 2016 and three previous in 2010, 2011 and 2013. Eleven specimens were tested in total. Two specimens were without fibres and had different concrete strength. Polypropylene fibres (PP) with length 50mm and strength of 600MPa and steel fibers (FE) with low ductility 25mm long and strength 400MPa were added in different content (0.5% and 1%) to the other nine specimens.

KEYWORDS: BLAST LOAD, RC STRUCTURES, STEEL FIBRES, POLYPROPYLEN FIBRES, EXPLOSION, BLAST WAVE

1. Introduction

The rising threat from terrorist attacks using different explosive materials is a significant threat to the modern society. The biggest damages are caused by the blast load on objects from critical infrastructure. The report presents the results from experiments of a method of monitoring the shock wave propagation and spall formation using a high speed framing camera. The use of a high speed camera for full scale concrete blast loading experiments is frequently mentioned in the literature, but small number of articles provides useful results of such kind recordings.

Due to improved ductility, fiber-reinforced concrete (FRC) shows better performance under blast and impact loading compared to conventionally reinforced concrete, as mentioned in many sources. The experiments from year 2016 determine blast performance of FRC with low strength and low ductility steel fibers (strength 400 MPa).

2. Setup of the experiments

Dimensions of the specimens were designed in real scale of a small span bridge as concrete slabs, 6m long, 1.5m wide and 0.3m thick.

The slabs were placed on timber posts and the soil under the slabs was removed; a channel 10m in length and 2.3m in depth (except 1.5m in test 1) was excavated under the slabs in order to allow observation of the soffit.

The 25kg TNT charges were built up using standard military 200g TNT charges. The charges were placed on steel holders in the middle of the slabs. The holders provided a 450mm stand-off distance from the slab for better simulation of real in-situ conditions. This value was chosen as the most usual height of a car trunk. The setup of the experiment is shown in fig. 1.

3. Instrumentation

The early stages of spall formation were observed on the soffit using angled mirrors which were placed under the concrete specimens. Another mirror was placed in front of the cameras in order to allow indirect observation without the risk of camera damage by fragments.

The experiments were captured using a NAC Memrecam GX3 high speed movie camera and IVV UHSi 12/24 ultra-high speed framing camera, the former being intended for expected spall formation while the latter for crack growth observations.

Sigma 70–300mm f/4–5.6, Samyang 800mm f/8, and Samyang 85mm f/1.4 lenses were mounted on the cameras. The aperture and gain were set to maximum values. The frame rates, single frame exposure times, and lens types are shown in Table 1. The view of the cameras can be seen in fig. 2.

<table>
<thead>
<tr>
<th>Test No</th>
<th>Lens¹</th>
<th>Exposure time [μs]</th>
<th>Frame rate [s⁻¹]</th>
<th>Lens¹</th>
<th>Exposure time [μs]</th>
<th>Frame rate [s⁻¹]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C</td>
<td>64</td>
<td>15000</td>
<td>A</td>
<td>2</td>
<td>50000</td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td>50</td>
<td>15000</td>
<td>A</td>
<td>2</td>
<td>10000</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
<td>50</td>
<td>15000</td>
<td>B</td>
<td>5</td>
<td>10000</td>
</tr>
<tr>
<td>4</td>
<td>A</td>
<td>20</td>
<td>20000</td>
<td>C</td>
<td>5</td>
<td>10000</td>
</tr>
<tr>
<td>5</td>
<td>A</td>
<td>50</td>
<td>15000</td>
<td>C</td>
<td>5</td>
<td>10000</td>
</tr>
</tbody>
</table>

Fig. 1 Layout of the experiment.

Fig. 2 Camera view.
4. Results and discussions

The process of blast loading of concrete has the following time schedule. The detonation of the main charge generates an expanding cloud of gases led by a strong shock wave which approaches the concrete specimen. The shock wave partially reflects back from the specimen surface. The compressive stress at the top surface of the specimen can cause local crushing of concrete or a shear failure of the specimen (puncture by shear-punching behavior). The other part of the shock wave passes through to the bottom side of the specimen, where it reflects again, interfering with the release part itself. In this time, cracks develop on the soffit and the spall begins to form. Part of the shockwave again passes through the interface, creating an air shock wave under the specimen. This air shock wave is combined with a shock wave which overflows the test specimen from the side. The air shock wave is later followed by flying spall debris.

Results of monitoring the blast wave propagation, which were obtained from the Memrecam records, can be seen in Table 2 and fig. 3–6. The first cracks are visible on the soffit at about 0.3 ms after the main charge detonation according to test 4, but they probably formed earlier. The average spall debris velocity was 120m.s⁻¹. In test 1, the air shock wave velocity under the specimen as determined from the movie reached 1150m.s⁻¹ while it was only 480m.s⁻¹ and 600m.s⁻¹ in tests 2 and 5, respectively.

Table 2: Monitoring of blast wave propagation.

<table>
<thead>
<tr>
<th>Test No</th>
<th>Test No1</th>
<th>Test No2</th>
<th>Test No3</th>
<th>Test No4</th>
<th>Test No5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>frame</td>
<td>time [ms]</td>
<td>frame</td>
<td>time [ms]</td>
<td>frame</td>
</tr>
<tr>
<td>Detonation of the auxiliary charge</td>
<td>0</td>
<td>1.93</td>
<td>0</td>
<td>2.13</td>
<td>0</td>
</tr>
<tr>
<td>Detonation of the main charge</td>
<td>29</td>
<td>0</td>
<td>32</td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>Crack development on the soffit</td>
<td>42</td>
<td>0.85</td>
<td>44</td>
<td>0.80</td>
<td>34</td>
</tr>
<tr>
<td>Shock wave arrive to the ground</td>
<td>59</td>
<td>2.00</td>
<td>86</td>
<td>3.60</td>
<td>94</td>
</tr>
<tr>
<td>Spall debris arrive to the mirror upper edge</td>
<td>---</td>
<td>---</td>
<td>183</td>
<td>10.07</td>
<td>---</td>
</tr>
<tr>
<td>Shock wave arrive to the second mirror</td>
<td>---</td>
<td>---</td>
<td>1101</td>
<td>71.27</td>
<td>---</td>
</tr>
</tbody>
</table>

Fig. 3 Spalling just started on the soffit (test 5, t = 0.67 ms).

Fig. 4 Air shock wave passes along the mirror (highlighted by the white line, test 5; t = 2.8 ms).

Fig. 5 Extended damage of the soffit (test 4; t = 2.85 ms).

Fig. 6 The flying spall debris reach the upper edge of the mirror (test 2; t = 10 ms).

5. Numerical modelling of the specimen response

LS-DYNA solver was used for computing the response of the specimen to the adjacent blast. The setup of the numerical model was adapted from previous experiments.

A numerical model was successfully calibrated to describe the behavior of concrete slabs subjected to blast loading and the corresponding damage.

The camera instrumentation confirmed some numerical model expectations. The overpressure wave arrived at the top surface of the specimen at t=0.2ms in the numerical model. After the rebound of the overpressure wave from the soffit of the specimen, the first elements started to erode (t=0.4ms). Fig. 7 shows the contours of normal stress in time t=0.3 ms.

Fig. 7 Normal stress – t=0.3ms
The extend crack development is an indicator of the extent of damage of the concrete. Material model MAT159_CSCM used in LS-DYNA solver for concrete elements have another indicator for damage; the plastic strain value. If the plastic strain indicator overpasses the setting value, concrete elements erode.

Differentiating between numerical simulation and real behavior of concrete is in the eroding elements in the model and inertia of concrete in real conditions. The concrete element has its own static inertia and does not erode in the same time in real behavior and numerical simulation. The shape and the size of a plastic strain pattern is the decisive parameter for the modeling and experiments’ agreement consideration.

For detailed concrete loss of weight research, the 3D models of concrete slabs were created. The crack, puncture and spalling patterns were made in every concrete layer in accordance to a known depth. The connection of separated layer patterns brought the 3D model of the concrete slab (fig 9).

6. Conclusions

The observation of real scale blast loading experiments using high speed cameras was performed according to the experiment request.

The spall formation process on the soffit and blast waves under the specimen were captured using a Memrecam movie camera, allowing the air shock wave and spall debris velocities to be estimated. The attempt to catch the foremost crack growth on the soffit using the UHSI camera was not successful due to insufficient illumination of the target. The model of spall formation was created using LS-DYNA solver.

For the next experiments, concrete shielding panels for more efficient fireball elimination and also an improved triggering system are being designed. LS-DYNA solver was used for computing the response of the specimen to the adjacent blast.

7. Literature


