Annals of the Academy of Romanian Scientists
Series on Engineering Sciences
ISSN 2066-8570 Volume **2**, Number **2**/**2010**

SECURITY SYSTEMS FOR MARITIME HARBOUR

Georgică SLĂMNOIU[1], Iuliana-Lidia CALANCEA[2]

Rezumat: *Obiectivele protecției infrastructurii sunt pe ordinea de zi a celor responsabili cu acestea în Uniunea Europeană. În prezent, România este una din țările situate pe frontiera de est a Uniunii şi acest lucru are implicatii deosebite în ceea ce priveşte măsurile de securitate necesare petru a fi implementate. Navele maritime şi porturile sunt importante în stadiul actual al conflictului. Un sistem integrat de protecție trebuie pregătit dinainte pentru a furniza informații în mod continuu, ceea ce va duce la creşterea performanțelor forțelor de intervenție.*

Abstract: *Infrastructure protection objectives are at the top of the agenda of those responsible in the European Union. Currently Romania is one of the countries on its eastern border of the Union and this has special implications in terms of security measures that are required to be implemented. Ships and harbours are important current conflict stage. An integrated system of protection of harbours must be prepared in advance in order to continuously provide information that will increase the overall performance of the intervention forces*.

Keywords: infrastructure, security, harbours, threats

1. Introduction

The following paper establishes a set of mandatory actions both for ships and harbour's authorities or administrations, meant to lead to enhancement of the security level for the ships operating in the harbours as well as for harbour's facilities.

Basically, an Integrated Security System for harbour area has to ensure the following servitudes:

- enhanced monitoring of the trespassing within harbour perimeter;
- early warning;
- monitoring of the security incidents and after incident analysis;
- surveillance of the risks factors;
- information dissemination among harbour authorities and security institution involved in coping with security incidents.

Within the International Maritime Organization, which deals with formulating and enforcement of the legislative frame regarding maritime navigation within international waters, operates the Maritime Security Committee, which focuses on the ships security issues and, until present, elaborated and issued for endorsement many international conventions for protection of human lives on the sea.

[1]Commander lecturer Ph.D., Scientific Research Center for Navy, Constanta
[2]Researcher gr. III engineer , Scientific Research Center for Navy, Constanta

Following the 9/11/2001 events, the International Maritime Organization has taken into account the risks due to the terrorist attack aiming the ships and harbour facilities and revealed the necessity of an elaborate analyze based on general experience of the communities involved in maritime transportation, aiming to develop and endorse urgently a international legislative tool. Therefore an working group was established to draft the International Code for Ship and Harbour Facilities Security, which was endorsed during 2002.

2. Types of threats facing harbour facilities

- Pilfering from the ships and harbour facilities;
- Terrorism: IED attacks, and hostages;
- High level of Illegal emigration from the war zones around Black Sea;
- Smuggling of illegal substances;
- Sabotages: deliberate destruction of harbour facilities, of the communication and data transmission networks, of a part of a ship, ship's equipments or cargo, vandalism;
- Illegal trafficking of human beings;
- Pirates attack/rubbery: acts of violence, rubbery or capture/threatening of persons;
- Attacks: from the land, from the sea, and from the air;
- Threats upon environment: accidental or deliberate spilling or drainage of pollutant substances;
- Smuggling;
- Accidents: collisions, explosions, fire, flooding, stranding;
- Proliferation and development of terrorist organizations, transnational organized crime; illegal trafficking of human beings, narcotics, weapons and ammunitions, radioactive and controlled substances;
- Illegal emigration and refugees;
- Provocation to extremism, intolerance, separatism, or xenophobia which may affect the Romanian stat and promotion of the democratic values;
- Limiting of the access of Romanian stat to certain resources and regional opportunities to fulfil its national interests.

In that context in which is observed a enhancement of the complexity level and unpredictability of the international terrorism phenomenon is required that the internal actions for crisis management to be better coordinated due to the requirement of the operative and efficient involvement of our country in the international efforts for cupping with this threat.

For cupping with the threats against harbour security, the following actions are to be taken:

- Focusing the intelligence, threats assessment and analyzes aiming to identify, delay and annihilate the possible or probable actions;
- Planning the security actions in the perspective of implementing of the management system and the development of the Security Plan for Harbour Facilities;
- Setting security actions and procedures aiming to control, security check and supervise the flow of persons, luggage, supplies and merchandise;
- Operational security elements: intelligent security systems, and ward, protection and intervention personal;
- Crisis management in perspective of establishing responsibilities and understanding them, setting the methods to be applied, defining the performance standards and the requirements to be accomplished;
- Training the personal through specific to maritime security training sessions.

3. Vulnerability analysis

Any location of harbour category assume the existence of a very large area, difficult to manage and protect, has a diversified economic activity, an administrative and control structure and a complex property boundary, all of them making from it a difficult to manage and protect from the threats on which is contently facing.

The diversity of activities involves a high flow of merchandise, persons, and transportation assets which has to be monitored to assure the security and safety of the facilities.

Taking into account all of the above, the requirement for implementation of a management system for harbour security, complementary to and correlated with the systems implemented by harbour's facilities emerges as a requirement based on international and national regulations and orientations.

4. Security mechanism

The security mechanism is the pragmatic element of the security strategy which, depending on its complexity, is taking one of the following forms:

- set of actions which comprises partial technical and organizational solutions from years 80;
- security mechanism (integrated), assembling actions, equipments and task forces professionally organized;
- security system with characteristics specific with theory of systems and having functions of forecasting (prevision) and adaptability.

Depending on specific characteristics of the objective, the structure of the security mechanism may be developed based on the model in the following figure:

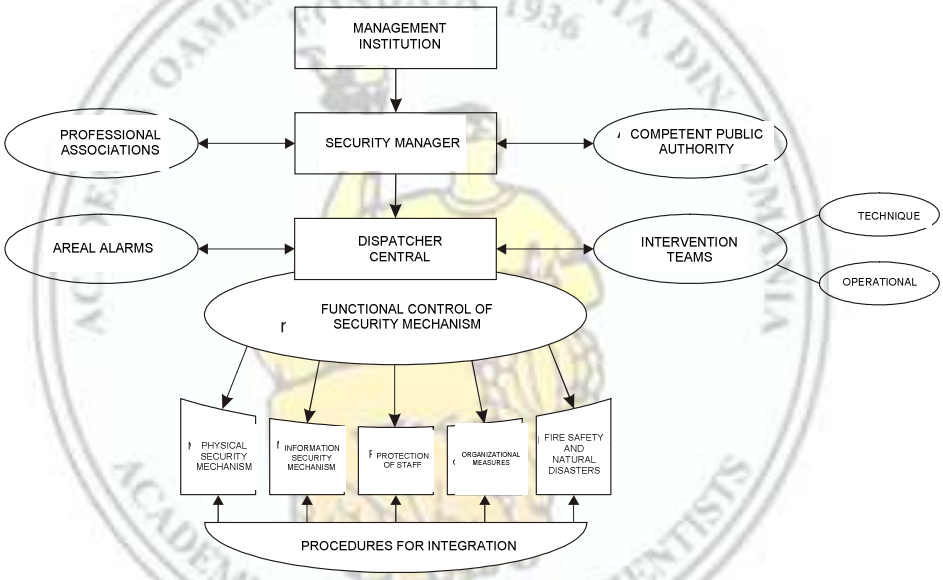

Fig. 1. The (basic) structure of a security mechanism

The physical security mechanism, as a component element of the security mechanism of an institution, has the main goal the detection, delay and annihilation of any hostile action or dangerous situation. It consist of mechanisms with role as physical barrier, intrusion and fire detection, access control, and TV surveillance as well as mechanisms for alarming, intervention and fire extinguishing.

From the structural point of view, the security mechanism has the following structure:

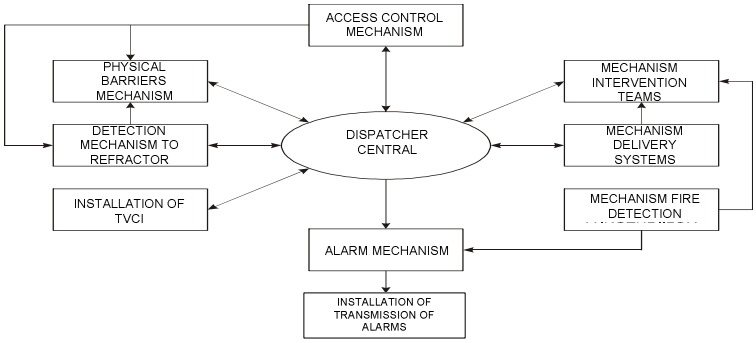

Fig. 2. Hierarchy and functional structure of the security mechanism

Constructively, the physical barrier has to be displaced circular, concentric to assure an efficient separation of the inner vital area from the external

environment. The number of circular protection barrier is designed to obtain the calculated delay.

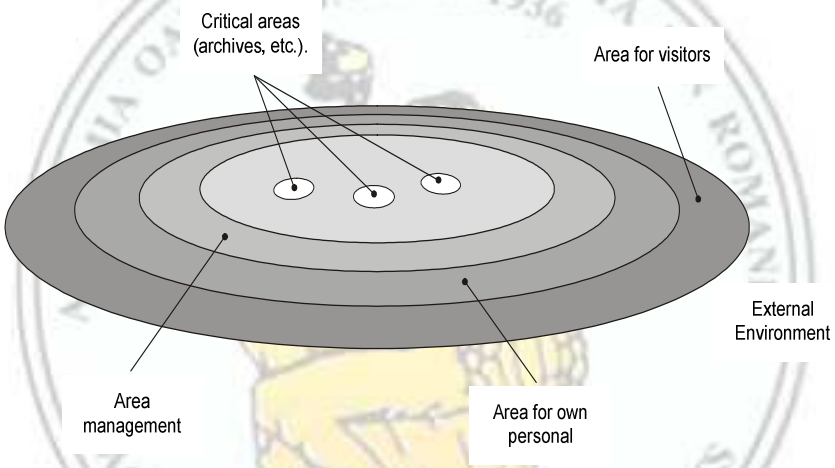

Fig. 3. Display fundamental of physical barriers

The total reaction time of the security system depends on the number of the barriers on the approaching route, the detection time of the system and the reaction time of the intervention task force.

Particularization of the security concept in case of harbours aiming the implementation of the system in accordance with the mentioned requirements, as well as evaluation, design and implementation of the security integrated mechanisms comprising:

- Constructive elements;
- Management and procedural actions;
- Human resources actions.

5. Possibilities for implementation of security mechanisms

Any harbour area is physically characterized by:

- perimeter boundary;
- access points to inner area;
- infrastructures (transportation, communications, utilities, command & control of maritime flow, s.o.);
- laugh port (the area in the vicinity of the coast (costal area), with natural or artificial protection allowing protection of ships against winds, waves and currents);
- berth (operational and technical) to ensure the interface ship-harbour;
- breakwaters for the protection of the berth and wharfs against the waves;

- port's operators which provides services (piloting, tugging, tying-untying ships, supply the ships, operating;
- Facilities for storing merchandise.

Aiming to provide the safety and security of all the above which are assumed by the establishment of each harbour, one of the basic functions of the system is the ***control of the incoming flow***, which implies prevention of (trespassing) unauthorized access through the access points.

To prevent unauthorized access through the access points are taken specific masseurs of ***access control system*** implementation which has to allow only the authorized flow of personnel, transportation assets and merchandise.

Taking into account the diversity and more and more atypical manifestation of the terrorist attack and of the means used by this, as well as the rising of illegal substances trafficking, emerges as an imperative request the accomplishment of security control using adequate technical devices able to perform detection in this heavy traffic.

To accomplish this are used supplemental technical means for detection of weapons, CBRN agents, narcotics, and so on.

To prevent the unauthorized access by trespassing the peripheral fence is required the implementation of a ***perimeter security system***.

Such a system represents a combination of actions: human, technical and procedural, meant to accomplish the deterrence, *DELAY, DETECTION, EVALUATION AND INTERVENTION* in case of unauthorized access attempt in harbour perimeter, as well as harbour facilities used by economic agents.

6. Achievement possibilities

6.1. Establishing the criteria and the attributes

A Port Security Integrated System is essentially a typical command and control system (or even a so called **C^4I** = Command, Control, Communications, Computers & Intelligence) whose main functions are:

- information gathering through various means, including technical ones;
- to transmit and process that information;
- decision assistance;
- to provide the means to response.

The system is **distributed throughout the port area** and is composed of operational centres that process the information provided by a network of complementary sensors and control equipment, for decision elaboration and reaction organizing.

The composing subsystems are integrated through a common computers and communications infrastructure which allows on-line processing, analysis and dissemination, thus providing decision support for the units involved in assuring port security.

6.2. System concept

The system includes human resources and equipments based on modern monitoring technologies in a concept of real-time operational coordination of intervention factors.

The concept employs the depth protection method which is based on establishing of **concentrically monitoring areas (detection, identification and response)** whose detection systems of potential intruders are placed as close to the outline as to attain a minimal time for identification and local response.

The security systems algorithms infer that **the detection systems have sensed the event, the information has been passed on for assessment, a solution for handling the situation has been chosen and the response forces have intervened for threat annihilation**.

The process of implementing the system is based on a computers and communications system that allows fast information processing and transmission and a proper coordination of response forces in the security area, forces which in a hierarchic structure overlap every echelon involved in the act of decision in the case of a special event.

Within system concept there has been taken into account the use of previous tested, high performance monitoring equipment, so to make the most out of the latest technological capabilities while providing a high probability of detection and a minimal rate of false alarms.

For all equipment that is to be installed outdoor it shall be selected that option adjusted to the marine environment.

At the same time the projection solutions of data analysis and transmission software applications constantly consider the restraints imposed by the system's response time in each case.

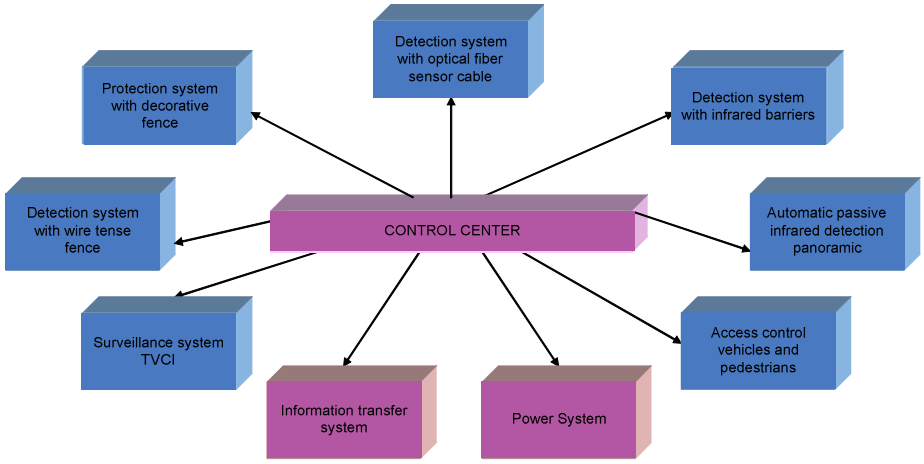

Fig. 4. Integrated port security

7. The perimeter detection system

In the purpose of reducing the false alarms and taking into consideration the rough climatic conditions representative for port location, the analysis of a marginal system is achieved through a combination of two subsystems which employ different detection principles:

- detection with sensitive fibber optic;
- wires tense technologies.

Thus the land perimeter has the advantage of an improved physical obstacle besides the combined detection of intrusion attempts, because the tense wire subsystem provides a tense line mesh through its constituents.

Harbour access can be supervised by means thermal cameras having the capability of identification of fire on board ships, deliberate collisions or groundings.

The fairways must be kept under surveillance for signalling the passage of people and ships, including the small ones in/out of the port, by using an automatic panoramic detection system with passive infrared which allows scanning over a selectable area, thus offering an image of target's IR signature, as well as its evolution from the entrance to the exit of supervised area.

7.1. The wires tense detection subsystem

The wires tense detection subsystem is a marginal protection system which is used as a first line defence for the protection of high or average risk objectives (seaports, airports, military objectives, oil refinery, large deposits, prisons, etc.).

This serves both as a **physical hedge** and as a **real time alarm system**, because it instantly detects any unauthorized attempt to break in by clipping it, jumping over or any other means of forcing the fence. The unauthorized attempt's exact location and the time of the event are displayed and signalled in the command and control unit laid out in the objective dispatching and recorded for subsequent analysis and storage.

The system may be installed as a self-contained peripheral hedge or it can be incorporated in a pre-existent fence or wall and integrated with intrusion detection sensors based on different functioning principles, such as: vibration sensors (cables), infrared barrier, microwaves barrier, etc.

The system's composing elements are:

- sensors;
- barbed wire;
- sensor poles;
- external processing unit;
- signal transmission cables;
- fibber optic interface;
- central computer with the objective map.

The sensor-fitted poles are attached to the fence posts made of built-up or wire mesh and placed along the perimeter. The horizontal wires pass through every sensor, forming a vertical barrier parallel outwards the wire mesh fence. Any attempt to cut the wires, to jump over by making use of them, stretching them to go through or transcending the fence any other way, provided that the wires are touched, is mechanical transmitted at once to the sensors that sense it and communicate it to the external processing unit microprocessor. The sensor to which the wire is connected senses the strength, direction and frequency of wire movement, reports these values to its microprocessor who, after determining the existence of an unauthorized attempt, signals an alarm condition that is passed from the external processing unit over to central dispatch computer.

The system calibrates itself and it is modular, allowing further extensions if necessary.

The sensitivity of each area can be controlled and adjusted by the display and control unit located in the Dispatch.

The advantages of this system are the following:

- physical barrier and electronic detection combined in one system;
- extremely low false alarms rate;
- extremely high efficiency – every stretched wire's movement is detected by an individual sensor;
- computerized central control for a practically unlimited number of areas;

- the system is not influenced by radio radiations nor electrical fields;
- immediate detection of unauthorized attempts of system intrusion;
- continuous operating in rough weather and difficult terrain conditions, virtually unaffected by weather conditions;
- easy integration with other types of sensors and alarm systems.

7.2. The fibber optic detection subsystem

The fibber optic detection subsystem shall be used as a second detection subsystem for perimeter monitoring of a harbour area.

To achieve this function a system developed and patented on **detection by means of fibber optic tracking sensitivity** is employed for high security applications.

The project infers the installing of a "fibber optic detection and tracking system" which **provides for real time detection and tracking** of any intrusion attempt.

The system is fitted with the "locator" function that **tracks and reports the position of an intrusion attempt**.

The recommended subsystem provides for real time detection, warning and reporting the exact location of intrusion attempt. The system has outputs that help subsystem integration, supplying with information of intrusion location.

The **buried cable** detection technology is designed for borders and perimeter security. This type of technology **does not require the presence of electronics or electric power on field**, except the optic cable sensor acting along the perimeter. The cable sensor is routed directly to the control/equipment room where the Sensitivity Controller is installed.

This solution assures an incorruptible security system for the detection of intrusion attempts in the secure areas from people who walk, crawl, run or drive a monitored vehicle. The controller sends to the **Central Monitoring System** data that holds out user friendly charts and displays, alarms and event reports for the security personnel.

The controller also provides for **the sensitivity optimization** for filtering background noise **by programming of preset events and for the positive identification** for differentiation from the unauthorized events. This selective filtering of noise rejects false alarms.

The sensitivity controller underlies the system and offers the possibility of calibration and adjustment **for filtering the noise made by wind, storm, birds, animals, aircraft, motor vehicles, etc**.

A laser beam is transmitted over the fibber optic cable which is buried in the scope of providing for an invisible detection solution, the echo is automatically analyzed and monitored for any noise, movement and vibration of the cable or nearby. **The signal is cleverly processed for minimizing the false alarms** caused by the environment, whilst detecting and responding to the faintest real intrusion events.

This system's advantages are:

- the sensor is a standard communication cable;
- real time detection, monitoring and warning;
- intelligent signal processing for noise filtering and real events detection optimization;
- precise and repeated reporting of intrusion location;
- no electronics or feeding lines on the field;
- no seasonal changes in terms of accuracy or sensitivity;
- robust technology with no maintenance need in normal operation.

The detection principle – interferometer – applied to the fibber optic cable detection any motion, vibration or noise induced on the cable or in its surroundings.

The sensitive cable is buried to a depth of **100-150 mm below ground level** in a detection area **2 meters wide along the perimeter**. The detection area is filled with a gravel layer beneath and above the cable thus rendering a high sensitivity in various soil and climate changes.

The Operation Station allows outputs to be remotely monitored, displays the entire perimeter outlined as a bitmap image in an automatic zoom window, warning and reporting any detected intrusion. By means of a password events can be controlled and noted by any operator, including alarm awareness, resetting or other actions.

8. Infrared barriers

8.1. Describing the solution

The marginal detection ring is achieved by Taut wire and fibber optic detection subsystems and cut off the vehicle and railway access gates.

For closing the perimeter, the vehicle and railway access points must be equipped with IR barrier type detection elements. They are designed to detect any attempt to penetrate these areas. The infrared barriers are connected with the access control panels placed at every gate. This way alarms generated by unauthorized intrusion through the IR barriers shall be immediately transmitted

through the fibber optic network over to the integrated security application on the main control centre computers.

Infrared barriers consist of a transmitter that radiates an infrared light beam, invisible to the naked eye, and a receiver that collects and analyses the received infrared energy. The emitter is installed on one side of the protected area, while the receiver is installed at the opposite.

Inside the emitter the infrared energy of a LED is radiated and focused through an optical system. The infrared spotlight is modulated at the pulse generator rate so to be protected from natural light external sources or the ones generated with the purpose of sabotaging its operation.

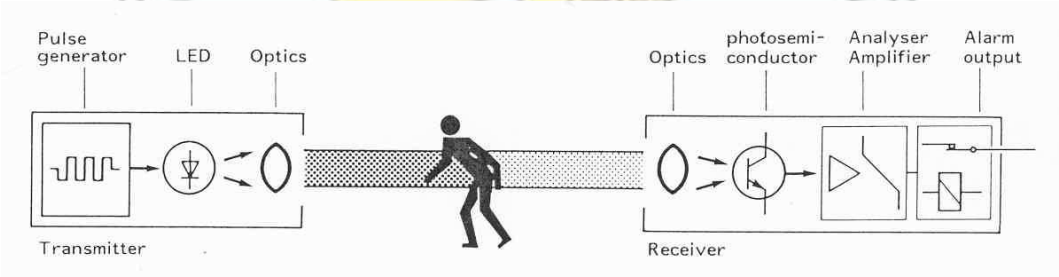

Fig. 5. Working principle of a barrier IR

The infrared energy arrived to the receiver is passed on through the optical system to a phototransistor which turns it into an electrical signal. The signal is amplified and analyzed in an electronic circuit for the alarm situation assessment triggered if the signal decreases under a preset value for a certain period.

The IR barriers are perimeter detection systems of high performance. They consist of two columns, one for transmission and another for reception, equipped with eight infrared beams installed one against the other at the maximum technically assured range, thus forming an immaterial and invisible detection area.

Their main functional features are:

- they have incorporated alignment means (optical viewfinder, LEDs, signal measuring points, acoustic and visual indication of signal reception, optional portable terminal), allowing one-person enhancements start-up and adjustment thanks to the transfer of alignment quality and alarm status to the transmission and reception columns;
- real time storing, indicating the date and time of the last 100 events (non-volatile memory);
- feasible voice communication through terminal or computer for column configuration and consulting, as well as for the memory of events;

- adjustable fog detector with the inhibition of intrusion alarms, signalling any drop in the intensity of the received signal due to fog, rain or snowing;
- manual removal (by configuration) or automatic removal (by disqualification or obstruction) of non-operational beams;
- internal technical alarms (lack of network power, of 12 V voltage, etc.);
- highly proofed against weather disturbances and unexpected alarms due to double transmission beams, synchronized pulse operation and to an adjustable detection time delay that allows it to readjust to the characteristics of the protected objective.

8.2. Working principle

Each barrier's transmission column, under the control of the reception column against it, radiates infrared light pulses on each beam. The reception column analyzes the infrared pulses received by its cells and generates the following types of alarms:

- **prompt intrusion alarm** - at the break off of a preset number of adjacent beams (typical reaction time 40 milliseconds);
- **delayed intrusion alarm** – at the break off of a single beam (typical reaction time 500 ms);
- **instant or delayed intrusion alarm** – at the break off of the low beam (typical reaction time 1,5 s);
- **delayed incapacity alarm** – at low decrease of the infrared signal received on a preset number or beams;
- **masking alarm** – at the break off for a long time of at least one beam;
- **prompt auxiliary alarm** – at circuit discontinuity of an auxiliary alarm input on a transmission or reception column;
- **technical alarm** – at network voltage interruption or absence of 12 V voltage.

All events (alarms, configurations, etc.) are submitted to central integration equipment and then saved and orodated (indicating date and time) in real time in a non-volatile memory. An auxiliary input allows remote alarm memory validation to avoid storing the events intercurrent during deactivation periods.

Conclusion

Two axioms are generally accepted in field analysis:

- it is practically impossible to ensure 100% protection of a critical infrastructure;
- there is no universal solution for solving this problem.

The security system's proper functioning and efficiency are assessed through analysis of response time for each phase of the operational cycle. These times depend on design solution and sensor system performance (detection time and warning transmission time) as well as on the performance of identification algorithms and methods (cause identification time), but also on the human and procedural factor (decision making time and reaction forces intervention time).

REFERENCES

[1] Alfred Thayer Mahan, *Influența puterii maritime în istorie (1660-1783)*, 1890

[2] Asofiei Virgil, comandor dr., *Apărarea comunicațiilor maritime*, Editura Militară, Bucureşti, Romania, 2004;

[3] Aymeric Chauprade, Francois Thual, *Dicționar de geopolitică*, Grupul editorial Corint, Bucureşti, Romania, 2003;

[4] Minchev Ognyan; Lesenski, Marin şi Plamen Ralchev, *Strategia transatlantică pentru stabilizarea şi integrarea zonei Mării Negre (Strategia SIMN*), Editura IRSI, Bucureşti, 2004;

[5] Popa Vasile, Dinu Mihai-Ștefan, *România şi procesul de stabilizare regională*, Editura UNAp, Bucureşti, Romania, 2004;

[6] Sarcinschi Alesandra, Băhnăreanu Cristian, *Redimensionări şi configurări ale mediului de securitate regional (Zona Mării Negre şi Balcani)*, Editura UNAp, Bucureşti, Romania, 2005;

[7] Slămnoiu Georgică, Ovidiu Radu, *Riscuri şi amenințări la adresa securității şi siguranței platformelor marine de foraj şi extracție româneşti*, Editura UNAP, Bucureşti, Romania, 2009;

[8] Văduva Gheorghe, *Geostrategii euroasiatice*, Editura Academiei Naționale de Informații, Bucuresti, Romania, 2004;

[9] *International Monetary Fund*, World Economic Outlook Database, September 2005 [http://www.imf.org/external/pubs/ft/weo/2005/02/data/dbcoutm];

[10] *Buletinul Universității Naționale de Apărare nr. 4*, Bucuresti, Romania, 2003.