**Scientific Journals**
**Maritime University of Szczecin**

**Zeszyty Naukowe**
**Akademia Morska w Szczecinie**

**2012, 29(101) pp. 37–44**

**2012, 29(101) s. 37–44**

# Magneto-acoustic seaports security systems: state of the art

# Magnetyczno-akustyczne systemy zabezpieczania portów morskich: stan aktualny wiedzy

**Lucjan Gucma[1], Maciej Gucma[1], Larisa Dobryakova[2], Evgeny Ochin[1]**

[1] Maritime University of Szczecin, Faculty of Navigation
Akademia Morska w Szczecinie, Wydział Nawigacyjny
70-500 Szczecin, ul. Wały Chrobrego 1–2
e-mail: l.gucma@am.szczecin.pl, m.gucma@am.szczecin.pl, e.ochin@am.szczecin.pl
[2] West Pomeranian University of Technology, Faculty of Computer Science
Zachodniopomorski Uniwersytet Technologiczny, Wydział Informatyki
71-210 Szczecin, ul. Żołnierska 49, e-mail: ldobryakova@wi.zut.edu.pl

**Key words:** acoustic, hydro acoustic, vibration and magnetic systems, networks, telecommunications, WiMAX, port security

**Abstract**
The popularity of wireless technologies during the last decade has created a considerable expansion of wireless networks. Many researchers work now on the area of wireless resource planning and optimization. Optimization is considered as the main approach to designing and improving the performance of Wireless Local Area Networks Infrastructure of Seaports Security Systems. The presented models and algorithms enable flexible coverage planning and optimization of Wireless Network Infrastructure.

**Słowa kluczowe:** systemy akustyczne, hydroakustyczne, wibracyjne i magnetyczne, sieci komputerowe, telekomunikacje, WiMAX, zabezpieczanie portów

**Abstrakt**
Popularność technologii bezprzewodowych w ciągu ostatniego dziesięciolecia świadczy o znacznym rozwoju sieci bezprzewodowych. Dzięki rozwojowi technologicznemu wielu pracowników naukowych może zajmować się projektowaniem i optymalizacją sieci komputerowych i telekomunikacyjnych. Jednym z ważnych zastosowań technologii bezprzewodowych lokalnych sieci komputerowych może być budowa kompleksowych systemów zabezpieczania portów morskich, co przedstawiono w artykule.

## Introduction

In the aftermath of the terrorist attacks on September 11, 2001, the U.S. Senate began developing antiterrorism programs to help secure the United States (on September 14, 2001): S 1429 Airport and Seaport Terrorism Prevention Act. The multi-layered defense strategy includes the following programs and initiatives:

- Secure Border Initiative (SBI), a comprehensive multi-year plan to secure America's borders and reduce illegal migration.
- C-TPAT (Customs Trade Partnership Against Terrorism): CBP created a public-private and international partnership with nearly 5,800 businesses to improve baseline security standards for supply chain and container security.
- Screening and Inspection: U.S. Customs and Border Protection (CBP) screens 100% of all cargo before it arrives in the United States using intelligence and cutting edge technologies. CBP inspects all high-risk cargo.
- CSI (Container Security Initiative): enables CBP, in working with host government Customs Services, to examine high-risk maritime containerized cargo at foreign seaports, before they are loaded on board vessels destined for the United States.

- 24-Hour Rule: under this requirement, manifest information must be provided to CBP 24 hours prior to the sea container being loaded onto the vessel in the foreign port.
- Use of Cutting-Edge Technology: CBP is currently utilizing large-scale X-ray and gamma ray machines and radiation detection devices to screen cargo. CBP also uses biometrics to help verify the identities of most non-United States citizens arriving at United States ports of entry, as well as to identify non-United States citizens they encounter attempting to enter the country illegally.

The terrorist's ships can have ballistic and inspired bullets, airplanes with kamikaze and different striking means. For functioning of all systems from the side of the ocean, one should establish safeguards against threats 100% radar covering area on the sea from the shoreline and to oceanic 200-miles of the enterprise zone.

While much attention has been focused on threats to maritime security posed by cargo container ships, terrorists could also attempt to use oil tankers to stage an attack. If they were able to place an atomic bomb in a tanker and detonate it in a port, they would cause massive destruction and might halt crude oil shipments worldwide for some time. Detecting a bomb in a tanker would be difficult.

According to the directive of the European Parliament and advice of 2005/65/EB, all without exception ports of the European Union must to have elaborated systems of the protection of ports and port devices.

## Classification of Seaports Security Systems

Each of environments has the features of the signals distribution. However, the majority of kinds SSS can be divided into following classes:

- acoustic,
- hydroacoustic,
- vibration,
- magnetic,
- radar,
- video,
- thermal Video.

Within the limits of given article, we will consider only first four classes – acoustic, hydroacoustic, vibration and magnetic sss. Other three classes – video, thermal video and radar sss will be considered in following article.

## Acoustic Seaports Security Systems

The acoustic seaports security system is a passive electronic intrusion detector system. The system is ideal for outdoor protection and can be easily installed on fences, roofs and solid walls, or for indoor use to protect vaults, strong rooms etc. Acoustical sss is based on an audio frequency miniature sensor cable featuring digital signal processing.

The acoustic sss offers a solution for intrusion detection by the analysis of typical noise patterns made by a forced entry attempt. The system can recognize motion caused by an attempt to pass through the fence and disregard signals caused by weather conditions, preventing nuisance alarms. This is an easy-to-install and easy to adjust system, it will provide the end user an economic and highly secure perimeter protection system, with a very high probability of intruder detection and relatively low rate of false alarms.

### The acoustic seaports security system MICALERT-303

The acoustic sss MICALERT-303 from firm RBtec [1] is realized in the form of Multi-Zone-Configuration, i.e. the quantity of connected zones, each of which in length to 305 m, can be a little. So, for example, on figure 1 it is represented Dual Zone Configuration. This configuration will secure a total perimeter length of up to 610 m using one LPU-303 Dual Analyzer unit. The detection zones must be continuous with no gaps between the individual zones. The Micalert-303 Dual Zone kit contains two carton roll dispensers of sensor cable, 305 m each, a Dual Zone LPU-303 Analyzer (with two dry

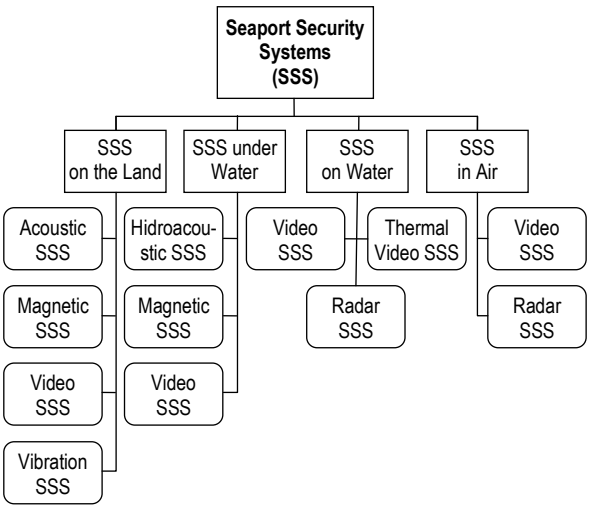


Fig. 1. The classification of seaports security systems
Rys. 1. Klasyfikacja systemów zabezpieczenia portów

contact outputs), two MCT units that are built-in the sensor cable ends and 2 packages of cable ties.

The signal processor receives and analyzes the signals generated by the Microphonic cable and detects minute vibrations in the fence. The sensor has independent adjustments and thresholds for each type of intrusion and the processor identifies, by type whether a cut intrusion, or climb intrusion has occurred.

The MICALERT-303 system includes several main components:

- Microphonic Sensor Line Cable;

The Microphonic Sensor Line Cable is attached to the desired-to-protect structure (fence / wall), converting the whole structure into a gigantic microphone of high fidelity, which will detect any kind of intrusion. The electric output of this cable is a highly accurate reproduction of all sounds, generated by the fence / wall.

The Microphonic Sensor Line Cable has a life expectancy of 10 years, is easy to install and non obstructive to the eye. This cable is attached directly to the fence with cable ties. If additional mechanical protection is required, it can be installed inside a plastic or metallic ledge / pipe. The sensor is totally passive and has different ranges of sensitivity that will allow adapting it to any specific application. The zone starts at the electronic processor (Analyzer) and ends at the MCT- End Line protection module.

- LPU-303;

An electronic processor that continuously monitors the cable signal output and detects any attempt to penetrate the perimeter. The analyzer is designed to ignore signals generated by rain, wind or birds. It utilizes highly advanced microprocessor technology in a microprocessor and is installed inside an IP65 rated weatherproof box. The analyzer scans the integrity of the sensor line, thus monitoring the terminal that has been integrated to the cable. If the cable is cut, damaged or interfered in any way, the analyzer will immediately detect it, and activate a warning signal. The LPU-303 is design to control up to two zones of 305 m (1000Ft). The analyzer is equipped with build in communication and relay output for fully integration and meteorological outputs for Weather Compensation Unit.

- End of Line Resistor;

The End of Line Resistor (MCT) is connected at the end of the zone to complete the circuit. It can also be used as an extension unit when the zone extends more than 305 m. For single and dual zone kits, MCT modules are built-in at the sensor cable ends.

- Multi-Zone Configuration;

The Micalert-303 system, with its onboard communication outputs, easily affords all of the possible means of relaying alarm messages back to the control center without the need for third party communication devices. In the multi-zone configuration (Fig. 2), the Micalert-303 have built the modularity of the system to be simple and straight forward. Each zone requiring the same components throughout the system.

It is necessary to underline especially, that alarm transmission it is realized with the help of protocols Ethernet and TCP/IP.

Fig. 2. The multi-zone configuration of the Micalert-303
Rys. 2. Micalert-303 – przykładowa konfiguracja wielostrefowa

#### Electronic signals underwater sound SygAk 07

SygAk 07 (ESUS – Electronic Signals Underwater Sound) [2] is designed to pass acoustic signals to submarine when acoustic contact between the submerged submarine and surface platform (helicopter) is lost. In addition, the SygAk 07 device can be used to indicate the beginning / completion of episodes executed during joint exercises of submarines and ASW assets. Signals emitted by SygAk 07 device conform to the requirements listed in NATO Standardization Agency Publication "Allied submarine and antisubmarine exercise manual" [AXP1 (D)(Navy)(Air)]. The standard of engineering realization of SygAk 07 ensures deploying the device from ships and helicopters.

Sweep is designed for fighting the sea mines utilizing influence fuses set off by acoustic and magnetic fields.

#### Monostatic Acoustic Barrier (MAB)

The Monostatic Acoustic Barrier (MAB) [2] is multisensory hydroacoustic system (Fig. 3) designed for maritime critical infrastructure protection such as:

– port entrance,
– harbour basin,

– ships moored at harbours,
– fairways to harbours,
– anchorages,
– drilling platforms,
– handling terminals.

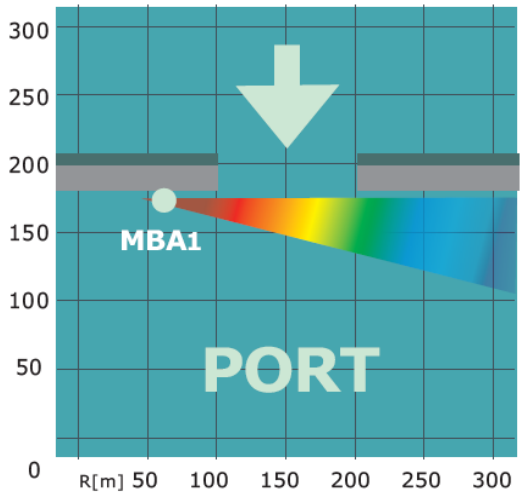


Fig. 3. The Monostatic Acoustic Barrier
Rys. 3. Pojedyncza bariera akustyczna statyczna

The MAB system is designed for detection of small underwater and floating objects. It can be used as an autonomic system or as part of bistatic barriers, or more extended harbour protection systems. The MAB system does not constitute any threats to the natural environment because the best available technologies were used during its design and production. Figure 4 illustrates one of ways of port gate protection.

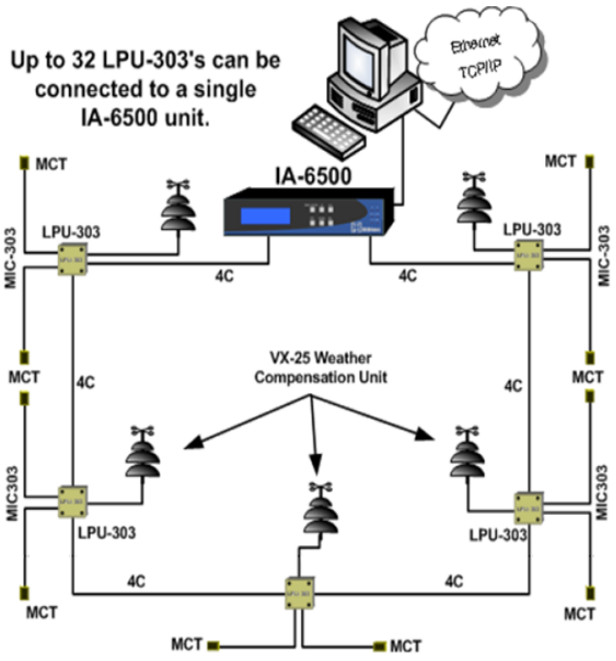


Fig. 4. The seaport gate protection
Rys. 4. Przykładowe zabezpiecznie portu

## Vibration Seaports Security Systems

The vibration sss is a passive electronic intrusion detector system. The system is applied for outdoor protection and can be easily installed on fences, on a concertina razor coil on a roofs and solid walls or for indoor use to protect vaults, strong rooms etc. The vibration sss is based on vibration of miniature sensor cable featuring digital signal processing.

The vibration sss offers a solution for intrusion detection by the analysis of typical vibration patterns made by a forced entry attempt. The system must recognize motion caused by an attempt to pass through the fence and disregard signals caused by weather conditions, preventing nuisance alarms.

### Vibration sss Ironclad Sensor Line Cable

The vibration sss Ironclad Sensor Line Cable [1] receives and analyzes the signals generated by the ironclad sensor cable and detects minute vibrations in the fence. The sensor has independent adjustments and thresholds for each type of intrusion and the processor identifies by type whether a cut intrusion or climb intrusion has occurred.

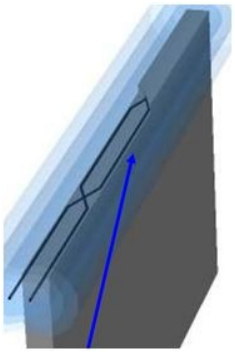

Fig. 5. The Ironclad Sensor Line Cable
Rys. 5. Czujnik linowy w osłonie stalowej

The Ironclad Sensor Line Cable system includes several main components:

- Ironclad Sensor Line Cable;

The Ironclad Sensor Cable is attached to the desired-to-protect structure (fence / wall), converting the whole structure into a gigantic vibration of high fidelity, which will detect any kind of intrusion. The electric output of this cable is a highly accurate reproduction of all sounds, generated by the fence / wall. The Ironclad Sensor Line Cable has a life expectancy of 10 years, is easy to install and non obstructive to the eye. This cable is attached directly to the fence with cable ties. The sensor is totally passive and has different ranges of sensitivity that will allow adapting it to any specific application. The zone starts at the electronic processor

(Analyzer) and ends at the MCT – End Line protection module.

- LPU-303;

An electronic processor that continuously monitors the cable signal output and detects any attempt to penetrate the perimeter. The analyzer is designed to ignore signals generated by rain, wind or birds. It utilizes highly advanced microprocessor technology in a microprocessor and is installed inside an IP65 rated weatherproof box. The analyzer scans the integrity of the sensor line, thus monitoring the terminal that has been integrated to the cable. If the cable is cut, damaged or interfered in anyway, the analyzer will immediately detect it, and activate a warning signal. The LPU-303 is design to control up to two zones of 305 m. The analyzer is equipped with build in communication and relay output for fully integration and meteorological outputs for Weather Compensation Unit.

- End of Line Resistor;

The End of Line Resistor is connected at the end of the zone to complete the circuit. It can also be used as an extension unit when the zone extends more than 305 m. For single and dual zone kits, the End of Line Resistors are built-in at the sensor cable ends.

- Multi Zone Configuration;

If Dual Zone Configuration will secure a total perimeter length of up to 610 m using one LPU-303 Dual Analyzer unit and the detection zones must be continuous with no gaps between the individual zones then Multi Zone Configuration can control remotely up to 32 LPU-303, or up to 64 zones of 305 meach, a total of 19.52 km. The structure of Ironclad Multi Zone Configuration is equivalent to the structure of MICALERT-303 Multi Zone Configuration (Fig. 2). The system was designed for several types of configuration:

- To work with multi drope configuration, using RS-485 communication.
- To connect the contact output from each LPU-303 card to other communication interface.
- To connect via LAN, using TCP/IP communication protocol (Lantronix: Micro100 Ethernet Connection). Each LPU-303 has its address ID which allow remote half duplex communication and receive alarm and change remotely parameter such as ARM / DISARM or sensibility change.

## Magnetic Seaports Security Systems

The magnetic sss is based on the "Magnetic Anomaly Detection" principle. As to Faraday's Law, a local change in the magnetic flux of earth will cause current to flow in a closed loop of electric conductor and build magnetic field around the sensor cable. The system is designed to detect the local change in magnetic flux caused by movement of ferromagnetic materials and ignore local changes in magnetic flux caused by other sources. The magnetic sss is a concealed and passive perimeter intrusion detection sensor system that is signed to detect and locate intruders moving over an unseen boundary and perimeter line. The movement of ferromagnetic materials (iron or steel) is one source that causes local changes to the magnetic flux of the earth.

In principle, the magnetic sss is a moving iron or steel detector. Its high probability of detection is based on the proven assumption that intruders carry weapons, military equipment, cameras, wire-cutters, keys, cellular telephones, or other such tools of their trade.

### Magnetic seaports security system MBS-404

The protected perimeter of MBS-404 is divided into zones, each of which can be as short as 10 m or as longer as 500 m. Each zone is connected to an LPU (local processing unit), and corresponding alarm circuitry. The sensor cable is concealed while the LPU's and control cables are stabilized to the wall. Should the protected perimeter be crossed, an audio-visual alarm is instantly set off at the control center. An elongated loop of sensor cable (Fig. 6) consisting of a continuous length of cable is buried underground. Movement of ferromagnetic materials above or beneath the sensor changes the currents flow of earth flux and detected by the sensor cable. The sensor detects the low level intrusion signals for amplification and processing by an Amplifier. Sensor cable length – up to 500 m, sensor width –

Fig. 6. The magnetic seaports security system MBS-404
Rys. 6. Magnetyczne czujniki systemu MBS-404

0.12 m, zone length – 140 m. The sensitivity of MBS-404 is 0.5 m (Fig. 7).

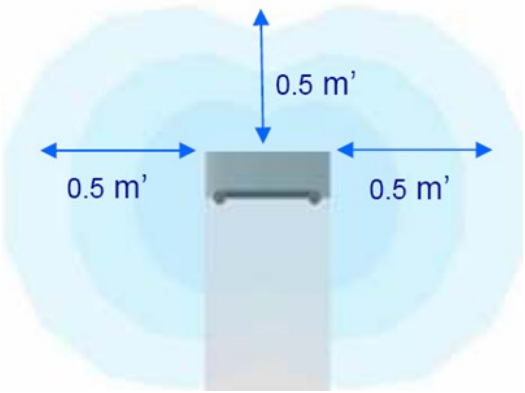


Fig. 7. The sensitivity of MBS-404
Rys. 7. Czułość czujnika MBS-404

- LPU – LOCAL PROCESSING UNIT;

A self-contained, waterproof and corrosion resistant unit especially designed to amplify, filter and process low level signals. Amplifier input signal is derived from respective sensor and its output is connected to:

- Separator – in those cases where grounding isolation of Amplifiers is essential.
- Control cable – otherwise, (normally in small systems).

A special amplifier (Inhibitor) connected to an inhibition sensor enables the system to ignore atmospheric and geomagnetic phenomena and man-made electrical and magnetic interferences (power lines, RF transmission, etc.), thus preventing false alarms due to these sources.

- SPU – Signal Processing Unit;

The signal processing unit (SPU) receives and analyzes signals from the system's field sensors, and then transfers the processed data to the central control interface unit (IA-6500). This weather proof double layer, high impact plastic enclosure contains transponder card (SPU-2004), and a lightning protection card (LP-05).

One transponder card (SPU-2004) can cover up to 8 zones and is installed at a convenient location along the fence. Up to 16 smart processing units (SPU-2004) may be connected to one control interface unit enabling coverage of up to 128 zones by a single controlled interface (IA-6500).

#### Magnetic seaports security system MBS-405

The magnetic sss MBS-405 [1] is a concealed, passive, buried perimeter intrusion detection sensor system that is designed to detect and locate intruders moving over unseen boundary lines and perimeters (Fig. 8).

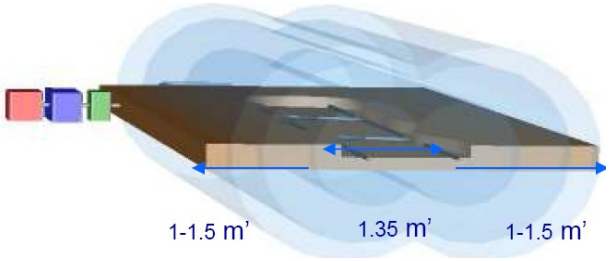


Fig. 8. The detection zone of the magnetic seaports security system MBS-405
Rys. 8. Strefa detekcji czujnika magnetycznego MBS-405

- MBS-405 Sensor Cable;

An elongated loop of sensor cable consisting of a continuous length of cable, buried underground. Movement of ferromagnetic materials above or beneath the sensor changes the currents flow of earth flux and detected by the sensor cable. The sensor detects the low level intrusion signals for amplification and processing by an Amplifier. Sensor cable length – up to 500 m, sensor width – 1.35 m, installation depth: minimum 40 cm.

- The Local Processing Unit and the Signal Processing Unit are the same as LPU and SPU of MBS-404.

### The Magneto-Acoustic Seaports Security Systems

The magneto-acoustic seaports security systems is two types:

- the passive magneto-acoustic sss,
- the active magneto-acoustic sss.

#### The passive magneto-acoustic seaports security system

The passive magneto-acoustic seaports security system is a passive electronic intrusion detector system. The system is ideal for outdoor protection and can be easily installed on fences, roofs and solid walls or for indoor use to protect vaults, strong rooms etc. The passive magneto-acoustic sss is based on an audio frequencyminiature sensor cable featuring digital signal processing.

The passive magneto-acoustic sss offers a solution for intrusion detection by the analysis of typical noise patterns made by a forced entry attempt and also based on the „Magnetic Anomaly Detection" principle. The system can recognize motion caused by an attempt to pass through the fence and disregard signals caused by weather conditions, preventing nuisance alarms and is designed to detect the local change in magnetic flux caused by movement of ferromagnetic materials and ignore local changes in magnetic flux caused by other sources.

In principle, the passive magneto-acoustic sss is a noisy object or/and a moving iron or steel detector. Its high probability of detection is based on the proven assumption that intruders carry weapons, military equipment, cameras, wire-cutters, keys, cellular telephones, or other such tools of their trade.

#### The active magneto-acoustic seaports security system

The active acoustic-magnetic seaports security system is an active electronic intrusion system. The system is ideal for outdoor protection and can be on water. In principle, the active acoustic--magnetic sss is a precise simulator of ships' acoustic-magnetic fields. For example, Influents Magneto-Acoustic Sweep [2] is designed for fighting the sea mines utilizing influence fuses set off by acoustic and magnetic fields.

## The System Integration of the diverse Seaports Security Systems

The system integration of the diverse sss is based on the next information technologies:

- Ethernet,
- TCP / IP,
- WiMAX – Worldwide Interoperability for Microwave Access.

It is possible to explain the principle of system integration by means of the following scheme (Fig. 9). In port territory one central aerial WiMAX and set of peripheral aerials WiMAX is established. Subsystems sss are connected to peripheral aerials WiMAX by means of Ethernet Protocol: acoustic, hydroacoustic, vibration, magnetic, video, thermal video and radar sss.

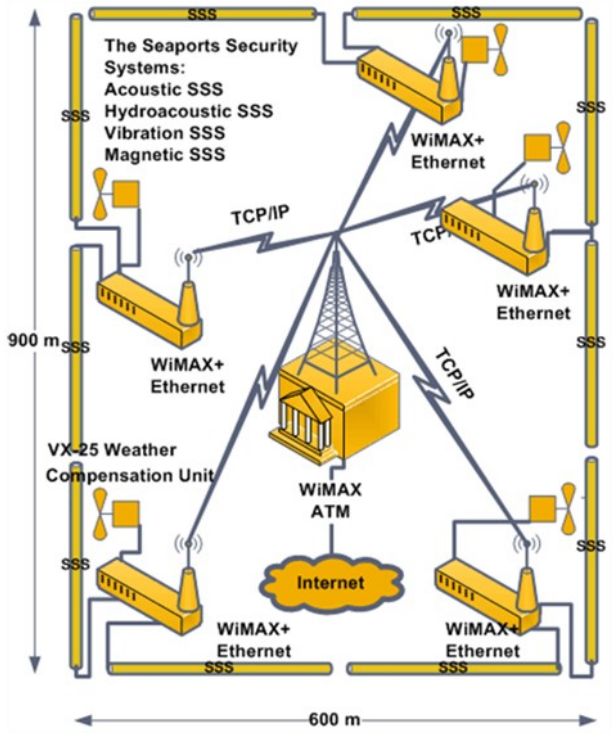


Fig. 9. The principle of system integration
Rys. 9. Zasada integracji systemów zabezpieczenia portów

## The safety of data transmission

The data transmission safety problem is based on Wireless Virtual Private Network [3] and Encryption IT (for example PGPEncryption Platform [4]). A Virtual Private Network is a network of virtual circuits for carrying private traffic. A virtual circuit is a connection set up on a network between a sender and a receiver in which both the route for the session and bandwidth is allocated dynamically. VPNs can be established between two or more Local Area Networks (LANs), or between remote users and a LAN. A Wireless VPN in addition uses a number of the protocols developed for increase of safety level.

The PGP Encryption Platform reduces the complexities of protecting data by enabling organizations to deploy and manage multiple encryption applications cost effectively from a single management console. When the organization needs additional encryption applications, the PGP Encryption Platform makes installing another, separate infrastructure unnecessary, because the infrastructure was deployed with the first PGP encryption application.

The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user and key management, policy, and provisioning that is automated across multiple, integrated encryption applications. Integrated PGP Corporation and third-party encryption applications enable organizations to deploy automated encryption as needed, with the data security functions required to solve the business requirement. This data-centric approach protects data in motion and in transit anywhere, anytime.

## Embedded Systems in Seaports Security Systems

Every activity in technical security systems is related to large amount of data computing and interfacing this data into other subsystems. Currently, these mechanisms are performed by embedded systems, i.e. such computer that performs one or more dedicated functions and is "embedded" as part of a complete system including hardware and mechanical parts. In a contrary, a general purpose computer, like a personal computer, is designed to

be very flexible and to meet a wide range of end-user needs. Embedded computers are controlled by main processing core that is usually a microcontroller (of type ARM or AVR, RISC type processor), or a digital signaling processor – DSP.

Large competition on microprocessors market has lead to setting some standards in. Whilst before 2000 Motorola microcontrollers (like 68H family) were in charge, now ARM type core is dominant in embedded systems. It's due to possibility of scaling, low power consumption and many interfaces enhancements. Price of single electronic devices is also very important factor. DSP cores are less frequents in typical applications, but in case of signal processing DSP cores are indispensible. Although total core speed is not outstanding, main advantage is in parallel threading and floating point operation speed and in details advantages are:

- Single-cycle MAC (multiply accumulate), DSPs today can even do two MACs in a single cycle.
- Repeat single instruction and repeat block of instructions.
- Addressing Modes: Capability to do hardware circular addressing and other post-increments / decrements in the same cycle as the instruction.
- Multiple memory accesses. Often there are multiple buses available.

In embedded systems it can be observed that unix based systems for microcontrollers are most popular such as real-time operating system (RTOS) such as MicroC / OS-II or Linux 2.6. Languages for programming of such system are in most cases C type languages.

Seaports security systems are very complex systems and embedded computers must be widely used. Every single network controller or segment integrator uses embedded computing. Very important factor is interfacing of system to each other, as well as safe and redundant protocols in such systems. Looking into computation power of such system, "embeddednes" might be confusing – main server of data collection and transformation is far more powerful than single web hosting server, and additionally all sub-systems might be faster than any commercial workstation. As such embedded system, here will be treated as a very specific task system.

## Conclusions

The designing problem of seaports security systems represents a challenge of intuitive (heuristic) synthesis of architecture sss and applications of multifactorial optimization sss procedure which is formalized enough now. However, in the course of optimization one more procedure of intuitive synthesis of global criterion of the optimization, based on operating experience sss is used. In many countries, the point of view on set of the requirement to sss has started to be formed after tragedy 11.08.2001 and now process of understanding of a problem is far from end. In such situation engineers should rely on already available set of practical achievements in the research-and--production companies of all world which, as is known, reluctantly share the knowledge. Differently, it is possible to assert, that **the scientific concept of Computer Aided Design of seaports security systems is absent now.** In following article, authors plan to consider state of the art "Video Seaports Security Systems".

## References (www)

1. Rbtec Electronic Security Systems <http://rbtec.com>
2. Centrum Techniki Morskiej <http://www.ctm.gdynia.pl>
3. VPN Consortium <http://www.vpnc.org>
4. PGP Corporation <http://www.pgp.com>