An approach to information exchange management in multimodule multi-position security systems

Nikolay Litchkov Gueorguiev[1], Konstantin Nikolov Nesterov[2], Stanimir Minchev Minev[2]
Institute of Robotics "St. Ap. and Gospeller Matthew" - Bulgarian Academy of Science, Sofia, Bulgaria[1]
Institute of Metal Science, equipment and technologies with Center for Hydro- and Aerodynamics "Acad. A. Balevski" - Bulgarian Academy of Science, Sofia, Bulgaria[2]
niki0611@abv.bg, k.nesterov66@gmail.bg, tp-stc@technopol.bg

Abstract: *The material presents a standard scheme of a multimodule multi-position security system and offers an approach for managing the information exchange in it, taking into account the specific location and condition of the individual modules and the functional relationships between them.*
Keywords*: INFORMATION EXCHANGE MANAGEMENT, PROTECTION SYSTEM, ADAPTIVE APPROACH*

1. Introduction

Modern security systems usually consist of many interconnected modules located at different points in space. Most often, these modules perform functions of intelligence, management, lethal (destructive) and non-lethal (non-destructive) impact on different types of targets, etc. [1,2,3,4]. The functioning of the system as such is determined by the possibility of information exchange between its various components so as to ensure maximum efficiency in its use. In most cases, the individual modules do not work simultaneously, but are in different states - active, ready for quick activation, ready to activate after a certain longer period of time. The transition of the modules from one state to another is done by controlling them from the respective command center and / or according to a certain algorithm.

2. Results and discussion

The main components of the Protection System are sensor modules (intelligence modules), impact modules and communication and control modules (Figure 1).

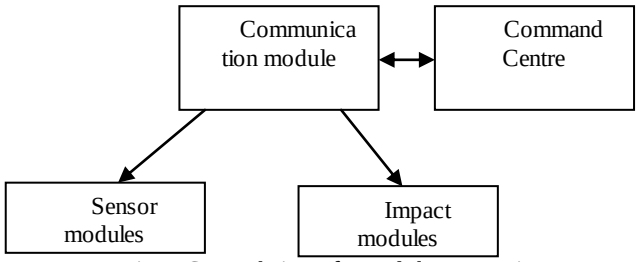

Fig. 1 General view of a modular protection system

The standard approach for information exchange within the System is the so-called continuous centralized exchange, in which the high-frequency communication modules check the status of the other elements of the system over time and, if necessary, issue an execution command to the impact modules. The disadvantage of such an approach is the high occupancy of communication modules, especially with a centralized management architecture and a large number of other modules to which they provide information, which leads to delays in information exchange due to waiting for a communication channel to be released. In addition, if the communication modules use their own battery power supply, such an approach leads to a large high energy consumption and a significant reduction in the time for their autonomous operation.

The second approach offers a step-by-step option for the operation of the individual modules. This approach is based on the logic of using the specific protection system and its location on the ground. Conditionally, these logics can be divided into tactical and technical.

Tactical logic takes into account the fact that in general the deployed modules cover a certain area to be protected and which has peripheral and internal sections. The operation of the respective modules in the inner part of the protected area is generally carried out after the respective intruder enters it, ie. it is logical to initially expect the activation of the modules located on the periphery of the protected area. Therefore, it is appropriate to introduce priority exchange of information with the individual modules, as the degree of priority decreases as they move away from the periphery of the deployed multimodule multi-position system.

In addition, if a module has registered an intruder and it has not ceased its activities, it is logical to expect its subsequent registration in modules that are adjacent to the original. The logic described in this way presupposes the consideration of the tactical location of the individual modules of the multi-position protection systems when organizing the management of the information exchange in them. This could be done by increasing the priority of exchanging information with neighboring modules when data on intruder appears in a module.

Technical logic takes into account the fact that in general deployed modules are activated in a certain sequence - most often first activate a certain type of sensor means, then activate sensors to confirm and further identify the threat and only then activate the impact modules. In this case, it is logical to first organize the information exchange with the activated sensors, after their activation - with the sensors for additional identification of violators and only then or in parallel - with the impact modules. The described so-called technical logic presupposes the consideration of the specific functional-technological interactions between the components of the individual components of the modules, as well as the technological interaction between the individual modules of the multi-position protection systems in organizing the management of information exchange..

Naturally, in practice it is necessary to define a sufficiently clear and workable approach to the management of information exchange in multi-position security systems, taking into account both their tactical and technical features. Such an approach could be reduced to a formalized description of the state, tactical and technical logic through dynamic matrices, the content of which is adapted to the changing situation. In it it is expedient to enter the data for the currently active modules and their priority. Possibilities for such a formalized description are, for example, the designation of system modules by three symbols - their indexes, conditional (or sequential) numbers, indicating whether the module is currently active (for example, symbol A - active and symbol P - passive) and the priority of the module (it is expedient to formalize 3 to 4 levels of priority, with 1 denoting the highest and 3 or 4 the lowest priority). At the same time, it is necessary to introduce the technological logical connection between the state and priorities of the individual modules of the system, and it is appropriate to do so through indices 1 (for direct connection between the actions of the two modules) and 0 (for lack of connection between both modules). Naturally, the matrix must be dynamic, and any change in the situation is associated with automatic updating of the data in it.

To clarify the proposed approach, we can consider a relatively simple multimodular multi-position system with lethal action to protect against land intruders such as humans, not armored and lightly armored means, developed in IMSETHC-BAS and designated by the conditional name STR [5,6].

The STR system includes a command center with a radio for exchanging information with the other components of the system, each of which consists of the following modules - seismic sensor (SS), radar (RC) or, at the customer's choice, infrared sensor and warhead) with fragmentation action (Figure 2).

***Fig. 2** Components of STR*

Components can operate autonomously (command center control is reduced to initial and sporadic change of their state via two-way radio), centralized (each activity of each component module is controlled by the command center) and semi-centralized (component modules have automatic interaction - ie the seismic sensor automatically activates the radar / infrared sensor, which automatically activates the warhead. Due to the fact that the requirements for information exchange are the most complex in centralized management, only this case will be considered in the present study.

In the case of centrally managed, the technical logic of operation of the individual component is as follows:

- is switched on in active state or deactivated by the Command Center, by radio commands;
- transmits data on its status upon request from the Command Center;
- in case of alarm situations (reduction of the power supply, probing, attempt for unauthorized access, etc.) transmits data for this to the Command Center;
- initially in active mode is the seismic sensor, which processes data on seismic signals by detecting and classifying them using specialized software;
- when detecting a target, the seismic sensor informs the Command Center, which decides to turn on the radar / infrared sensor;

When a target is detected, the Radar / Infrared Sensor informs the Command Center, which decides to include the combat unit, which hits the target with fragments (Figure 3).

***Fig. 3.** Result of the impact of STR*

Let's assume that in order to ensure sustainable protection of a certain area, the STR system is deployed in three concentric circles. Figure 4 shows a section of the deployed components of the system, and Tables 1 and 2 show the dynamic matrix of the initial state in full of the seismic sensors, and in short - the other components. In Figure 4 and in the matrices, the seismic modules are indicated by index C, the radar / infrared sensors by the R index, and the warheads by the W index. Their serial numbers are denoted by x, x + 1 and x + 2 - for the outer circle, by y, y + 1 and y + 2 - for the middle circle and by z, z + 1 and z + 2 - for the inner circle. On the diagonals of the dynamic matrix the symbols A and P indicate whether they are active or passive (A - active, P - passive) and the number from 1 to 4 shows their priority. The other fields of the dynamic matrix show their mutual logical connection (by indices 1 - direct connection and by 0 - absence of direct connection).

The approximate initial state of this section of the deployed STR system shows that all modules in the innermost circle are in a passive state and have the lowest priority for data exchange (priority 4), and of the modules in the middle and outer circle only seismic are active, with those in the outer circle having priority 2 and those in the middle circle having priority 3. Radar modules and warheads in the outer circle have priority 3, and those in the middle circle have priority 4.

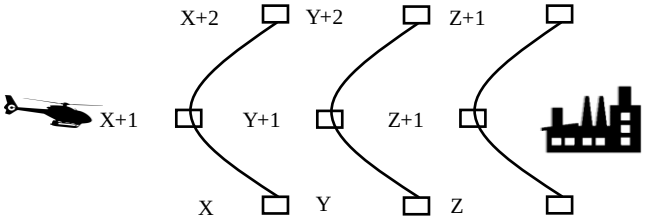

***Fig. 4** A section of located system components*

The approximate initial state of this section of the deployed STR system shows that all modules in the innermost circle are in a passive state and have the lowest priority for data exchange (priority 4), and of the modules in the middle and outer circle only seismic are active, with those in the outer circle having priority 2 and those in the middle circle having priority 3. Radar modules and warheads in the outer circle have priority 3 and those in the middle circle have priority 4. It should be noted that the direct connection between the adjacent seismic sensors, between the seismic sensors and the radar sensors with the same numbers and between the radar sensors and the warhead with the same numbers is 1, and between the other modules is 0.

***Table 1** Initial state of seismic sensors*

	Cx	C x+1	C x+2	Cy	C y+1	C y+2	Cz	C z+1	C z+2
Cx	A2	1	0	1	1	0	0	0	0
Cx+1	1	A2	1	1	1	1	0	0	0
Cx+2	0	1	A2	0	1	1	0	0	0
Cy	1	1	0	A3	1	0	1	1	0
Cy+1	1	1	1	1	A3	1	1	1	1
Cy+2	0	1	1	0	1	A3	0	1	1
Cz	0	0	0	1	1	0	P4	1	0
Cz+1	0	0	0	1	1	1	1	P4	1
Cz+2	0	0	0	0	1	1	0	1	P4

***Table 2** Initial state of radar, infrared sensors and warheads*

	x	x+1	x+2	y	y+1		y+2	z	z+1	z+2
R	P3	P3	P3	P4	P4		P4	P4	P4	P4
W	P3	P3	P3	P4	P4		P4	P4	P4	P4

Of course, depending on the specific tactical and operational situation, another way is possible to determine the priorities of the individual modules, but as far as the aim of the study is to

demonstrate the approach to dynamic matrix change, we will limit ourselves to the proposed description.

Let's assume that at some point in time the seismic sensor with the number x + 1 registers an intruder. In this case, the logic of information process control is appropriate to increase its priority, as well as that of the radar / infrared sensor and the warhead with the number x + 1 to 1. Due to the possibility of the intruder to move to the areas of neighboring modules is it is appropriate to increase the priorities of information exchange between the Command Center and the seismic centers with numbers x, x + 2, y, y + 1 and y + 2 (which have a tactical connection 1 with module Cx + 1) to 1, and for the same the radar numbers should be activated on them and on the combat units the priority should be increased to 2. It is also expedient to activate all seismic modules of the innermost circle and to increase the priority of data exchange with them to 2 and the combat parts in the middle circle change their priority to 3. The results of this dynamic change led to a change in the matrices for the seismic sensors in the manner shown in Tables 3 and 4.

Table 3 *Modified status of seismic sensors*

	Cx	C x+1	C x+2	Cy	C y+1	C y+2	Cz	C z+1	C z+2
Cx	A1	1	0	1	1	0	0	0	0
Cx+1	1	A1	1	1	1	1	0	0	0
Cx+2	0	1	A1	0	1	1	0	0	0
Cy	1	1	0	A1	1	0	1	1	0
Cy+1	1	1	1	1	A1	1	1	1	1
Cy+2	0	1	1	0	1	A1	0	1	1
Cz	0	0	0	1	1	0	A2	1	0
Cz+1	0	0	0	1	1	1	1	A2	1
Cz+2	0	0	0	0	1	1	0	1	A2

Table 4 *Initial state of radar, infrared sensors and warheads*

	x	x+1	x+2	y	y+1	y+2	z	z+1	z+2
R	A2	A1	A2	A2	A2	A2	A2	A2	A2
W	P2	P2	P2	P2	P2	P2	P3	P3	P3

The proposed approach for managing the flow of information in a complex system is implemented in the System for Combating Low-Flight Objects developed at IMSETHC-BAS, designed to counter large groups of low-flying targets such as helicopters or unmanned aerial vehicles. This system in its standard configuration includes one stationary command center (CC) with a central stationary communication module, one mobile CC with a mobile communication module that duplicates the stationary CC if necessary, as well as external modules each with external built-in communication modules as follows - one repeater, one passive radar, one active radar, up to 160 antidrone mines (controlled by group fuse with 4 outputs), up to 160 anti-helicopter mines (controlled by group fuse with 4 outputs), up to 4 pieces portable and up to 10 mobile systems for electronic interference of the means of navigation and control of the aerial vehicles [5].

In the standard approach, the data exchange between the CC and the modules is performed at a distance of up to 10 km. on simplex radio channels with an operating frequency of about 170 MHz. GFSK modulation with constant exchange rate of 38400 bps, digital modulation with 25 kHz band, 15 W power radio modems and non-directional antennas with 4 dBi gain is used. In this case, in the established mode of operation, the CC exchanges two types of data with the modules. The first type is a short question to all modules about whether there is a change in their state and receives an answer from them. As this short request is sent to all modules at the same time, the time for its reception and processing is important only for the first module, and for the others it can be ignored. Each module answers this query after a wait, which is equal to its sequence number multiplied by the time to broadcast the shortest response, in this case - 50 ms. The short answer contains only data on whether the module is in the same state or there is a change in its state (which means that there is a need to transmit additional data to the CC - for example to detect targets of a sensor, for an alarm event such as reduced power supply, unauthorized access, damage, etc.). In this case, in the next cycle of queries, which starts with a delay of 10 ms after receiving the response from the last module by number, CC asks the module for data on the changed state and then the module forms a response, its broadcast time is 80 ms . Therefore, if a module needs to transmit any information about the occurrence of a target or an alarm event, it will take time to:

- transmission of the first, short message, for the emergence of this need (50 ms.);
- - requesting all other modules and receiving a new request to the same module (50 IDmax + 10, where IDmax is the number of modules managed by the CC);
- transmission of the second, information message, about the occurrence of a target or an alarm event (80 ms.).

Therefore, the delay time of data exchange with a module (Tmax) can be calculated by the formula:

$$Tmax = (50\ IDmax\ ) + 10 + 80\ , [ms]$$

For the considered system for control of low-flying objects IDmax = 97, ie Tmax = 4940 ms., Which indicates that sending the next command or request to a module can be done after about 5 seconds. At a flight speed of drones or helicopters of the order of 200 km / h (ie 55.56 m / sec) for the time of delay, they will fly about 280 meters. This significantly complicates the operational management of the system and the ability to quickly activate various modules, their inclusion in combat mode, the possible authorization of lethal and non-lethal effects (with fragments and disturbances), termination of a type of action (eg interference) and etc. For example, the algorithm for firing antidrone and anti-helicopter mines requires the sequential implementation of 4 processes - detecting the target from the radar, switching to active mode of mines in whose areas of action is expected to pass the target, detecting the target from mines' own sensors . In this case, the target will fly over a kilometer, which in most cases will take her to the area where she will be able to perform its tasks.

In the second approach, in which the priority of the modules is variable, it can be assumed that the system is deployed in three circles. In the inner circle are the passive and active radars, 4 portable systems for electronic suppression and 36 antidrones and anti-helicopter mines (controlled by group fuse with 4 outputs). In the middle circle are deployed repeater, 4 mobile systems for electronic suppression and 56 pieces of antidrone and anti-helicopter mines (controlled by group fuse with 4 outputs), and in the outer circle are deployed 6 mobile systems for electronic suppression and 68 antidrone and anti-helicopter mines (controlled by group fuse with 4 outputs).

Passive radar and repeater have priority 1, active radar and all modules located in the outer circle have priority 2, those located in the middle circle (without repeater) have priority 3, and modules in the inner circle (without radar) have priority 4

In this configuration with priority 1 are 2 modules, with priority 2 are a total of 41 pieces, with priority 3 are a total of 32 pieces. and with priority 4 are 22 pcs. modules.

Different algorithms for data exchange management are possible depending on the priorities of the respective modules. An algorithm was chosen for the considered System in which the data exchange of priority 1 modules is at maximum speed, with priority 2 modules is every 10 minutes, with priority 3 modules is every 60 minutes, and with priority 4 modules is 4 hours. The researches in IMSETHC-BAS, confirmed by simulation in virtual environment and by conducted field experiments [7,8] showed that in this case the delay time of the data exchange with a given module is of the order of 0.35 seconds. Naturally, when aerial target appears and the priorities of the modules increase, this time increases as well, but in general it does not exceed one second (ie about 5 times less than the delay time in the standard approach).

3. Conclusion

An approach for data management, implemented in a prototype of Protection Systems developed by a team of IMSETHC-BAS, is presented. The approach is based on the introduction of a dynamic matrix describing the state of the modules of the system and the introduction of the possibility for a formalized description of the technical and tactical features and connections between them. The approach is demonstrated for one type of system for protection of a land object, and data on the effect of its use in a complex system for combating low-flying objects are presented.

The proposed approach is able to significantly improve the information exchange in complex multi-position modular security systems, which is confirmed by the results of a number of experiments with real systems or their functional models.

Acknowledgment

The research is aimed at the implementation of Work Package 2 "Intelligent Security Systems" of project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum Communication, Intelligent Security Systems and Risk Management (Quasar) ", which received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

4. References

1. Kiril Stoichev**,** Dimitar Dimitrov**,** Valeri Panevski, Critical infrasturture integrated security and protection. IMSETHAC-BAS, 2018, ISBN:978-619-90310-8-7, 258
2. Panevski V.S.. Systemic approach to the development of security systems for critical infrastructure protection as a research methodology applied at the Center of competence QUASAR. International Scientific Journal "SECURITY & FUTURE", 4/2019, Scientific Technical Union of Mechanical Engineering "Industry 4.0", 2019, ISSN:2535-0668, 144-147
3. Ivanov I**,** Nikolova V**,** Yaneva S**.**. Investigation of the possibilities for planning the protection of the sites from the critical infrastructure and adequate response in the event of incidents near them. International Scientific Journal “Security & Future”, 4, 3, Scientific Technical Union of Mechanical Engineering – Bulgaria, 2020, ISSN:(PRINT) 2603-2945
4. Тумбарска А**.**. Високотехнологични несмъртоносни оръжия с военно предназначение. Сборник доклади от Годишна университетска научна конференция, НВУ "В. Левски", 2021, ISSN:2367-7481, 1186-1196
5. Хай-Тех Ай Ем Ес ЕООД – BDIA (bdia-bg.com)
6. Крумов, Ангел**,** Симеонова, Антоанета. Изследване на възможностите за създаване на нови модули за въздействие от разстояние. НВУ "Васил Левски", 2019, ISSN:2367-7481, 1741-1747
7. Varbanov Vladimir. Modelling uncertainty in multisensory systems at conflict measurements with dempstershafer combinatorial rule. International Scientific Journal “Mathematical Modelling”, 5, 3, STUME, 2021, ISSN:2603-2929, 104-105
8. Венцислав Пехливански. Изпитвания в процеса на проектиране на системи за защита. ИМСТЦХА-БАН, 2020, ISBN:978-619-188-359-2, 169