Bulgarian Academy of Sciences. Space Research and Technology Institute.
Aerospace Research in Bulgaria. 36, 2024, Sofia

DOI: https://doi.org/10.3897/arb.v36.e12

INTELLIGENT MONITORING AND PROTECTION SYSTEM OF CRITICAL INFRASTRUCTURE BASED ON MOBILE COMMUNICATION-INFORMATION SYSTEM WITH ELEMENTS OF ARTIFICIAL INTELLIGENCE

Evgeni Hubenov, Zoya Chiflidjanova

Space Research and Technology Institute – Bulgarian Academy of Sciences
e-mail: hubenov@space.bas.bg

Keywords: *Information and communication systems, Artificial Intelligence, Control, Communication architecture*

Abstract

The paper proposes innovative modern solutions for an integrated mobile monitoring system with elements of artificial intelligence in the Internet environment based on a mobile communication-information system for collecting, aggregating, processing, and presenting in real-time streams of information objects. It presents the management of communication networks to optimize the transport and processing of information objects based on discrete-event data flow representation and modeling with a hierarchical structure. Qualitative aspects are considered for networks designed for monitoring and notification of geophysical, climatic, and other natural phenomena as well as for anthropogenic systems. A comparison of centralized and decentralized management capabilities is made, as well as the state of the art of network technologies and the possibilities for practical implementation in different network architectures.

Introduction

Critical infrastructure (CI), considered a complex hierarchical system structured in elements, connections, and relationships between them, has a systemic goal (desired systemic property, result) of building and improving its management and protection [1]. The three main components of CI management are organization, communication and information support, and information. Management support encompasses all personnel, systems, and force resources that support the delivery, transport, and processing of information flows provided by specific system functions of the information system. The primary purpose of management support is to enhance the ability to make and implement decisions. Important elements of management support are the information systems, equipment, software, and infrastructure that enable the management of the system and the identified resources. These systems further help the manager monitor and influence his resources through the hierarchical chain. The CI protection and management system functions as a set of subsystems with unified management, providing specific objectives with their own information space (ISp). The ISp is a set of information resources and infrastructures for information access with structuring, navigation, and transport capabilities.

The critical infrastructure monitoring information system (CIMIS), which provides the information necessary to achieve the system goals, is an information space in which all the elements support the management processes functions. Its components have a certain structure and hierarchy, which provide a connection with one or more information subsystems for CI protection. An information system (IS) is a set of interconnected means, methods, and personnel that are used to store, process, and provide information, knowledge, and digital services [2] to achieve a set goal. In a narrow sense of the concept, IS is considered an information cluster, which is a set of information blocks with signs of a grouping of elements.

The management of the monitoring information system (MIS) must be carried out uniquely within the monitoring system structure, and the results must be presented in other subsystems with the necessary level of security to protect the information. If information from other sources outside the MIS (e.g., satellite information or open sources) is required for CI protection purposes, it should be in the form of an information service [3].

Access to reliable, accurate, and timely information at all levels of society is critical just before, during, and after a disaster. Without information, people and institutions are often forced to make critical decisions based on fragmented, contradictory messages or on the basis of "guesswork". Information on disaster risk and subsequent events should also be made available to the general public as one of the stakeholders in the disaster risk management process. Information and communication technologies (ICTs) have advantages in information dissemination and management that can and should be used to improve disaster and emergency risk management.

Communication-Information Monitoring System

The system-information approach focuses on the processes of receiving, transporting, processing, and presenting information in the system and its interaction with the external environment and critical infrastructure protection subsystems. This information interaction implies the construction of monitoring as a communication and information system (CIS) [4]. An organizational-structural approach defines a CIS as a set of technical (including communication means, border protection devices, cryptographic means, and signal distribution medium within the system boundaries) and programmatic means, methods, procedures, and personnel organized to perform one or several of the functions of creating, processing, using, storing, and exchanging (classified) information in electronic form. CIS is a complex distributed spatio-temporal discrete-event system that includes in its structure two interconnected subsystems (communication and information), which are created for the purpose of transporting and processing flows of information objects [5]. The information object streams are of different subjects and enter the CIS system from different sources in or related to the CI areas. The purpose of CIMIS is to detect, classify, identify, and monitor CI-related events in a timely manner and provide real-time situational awareness to support CI protection decision-making.

Event-oriented CIS include hardware and software components that operate simultaneously in different domains of interconnected communication environments, with the use of events as the main object to organize the dynamic communication between components and adapt the structure to the data flow parameters. The dynamics of these systems are related to the occurrence of physical events at previously unknown, irregular moments of time. In general, an event is referred to as a change of state of the system in the discrete state space. Various information flows are formed in a CIS for monitoring and control purposes. For the users of the system, changes in monitoring parameters directly related to CI protection or events related to disasters, accidents, and catastrophes are of interest. For the purpose of maintaining the functional characteristics of the CIS and for the system operator, the information flows resulting from the interaction and interdependence of the CIS with other ISp elements and directly related to the management of the CIS are important. Only information flows related to CI monitoring will be the subject of this paper.

The architecture of data stream processing systems links the communication environment and network transport to information processing, including its aggregation for complex event processing in large systems. These systems are communication and information systems (CIS) insofar as the viewpoint and approach are from the network layer side of the communication model. From the perspective of the application layer of the network model (OSI, TCP/IP), the formation, movement, transformation, processing, and presentation of information objects give rise to the simultaneous use of the term information-communication system (ICS). Data flow can be viewed as information about events or things that have happened within an external system or domain. The same term is also used to refer to the object that represents what has happened in the ICS. Event-driven ICSs include hardware and software components that operate simultaneously across domains in interconnected communication environments, with the use of events as the primary object to organize dynamic communication between components and adapt the structure to the parameters of the data stream.

Cognitive (rational-mental segment) of the monitoring system

The need for diverse, timely, accurate, and adequate information on the state of CI and for making timely management decisions related to the prevention of the possible consequences of various contingencies leads to the need for the use of information systems (IS) that monitor the various possible states of CI, the various influences on it, as well as its behavior patterns. Moreover, the more different information-gathering systems there are, the greater the reliability of the information obtained.

Creating an IS for decision support based on emergency forecasting that combines problem solving for all types of natural and man-made emergencies [6] and allows for rapid response is an important and labor-intensive task. At the same time, the use of different monitoring systems necessitates the development of a conceptual approach to form a unified information space (UISp) of CI.

In this case, the UISp is a set of information tools and resources integrated into a single system, namely:

- its own information resources (document sets, databases and data banks, archives of all kinds, etc. containing information recorded on appropriate media);
- network and special software;
- telecommunications network (distributed corporate computer networks, telecommunications networks and systems for special and general use, data transmission networks and channels, means of switching and managing information flows).

Principally, IS is implemented on two levels:

- As an automated workplace (AWP) using a computer.
- In the form of a local computing network, connecting two to several computers (workstations) and peripherals within the CI to access common resources and exchange information.

In practice, it is possible to distinguish between natural, technogenic, and natural-technogenic emergencies. For all three classes of emergencies, it is first and foremost necessary to address the problems of early forecasting. When emergencies occur, it is necessary to make forecasts of their development and consequences. It is recommended that the whole IS structure be divided into three subsystems, each of which performs its functions:

The emergency prediction subsystem meets the following functional requirements:

- Provide analysis of monitoring and forecast information on the sources of accidents;
- Develop forecasts for the occurrence and development of emergencies;
- Provide for the creation and maintenance of a database of forecasts of the occurrence and development of emergencies and the data to substantiate them;

- Ensure monitoring and forecast data processing to identify new, more effective predictive relationships between emergency sources, their causes, conditions, and development parameters.

The subsystem for forecasting the consequences of man-made accidents meets the requirements:

- Provide predictive analysis of consequence assessment data and predictions;
- Develop forecasts of the consequences of man-made accidents;
- Ensure the establishment and maintenance of a database of forecasts of the consequences of man-made accidents and their degree of substantiation;
- Ensure the processing of monitoring and forecast data to establish new, more effective predictive relationships between the parameters and conditions for the occurrence, development, and progression of man-made accidents and their consequences.

The compliant decision support subsystem:

- Present forecasts of emergency occurrence and development in the form of forecast bulletins for management review and approval;
- Ensure the preparation of regulatory documentation for sites;
- Ensure the production of documents required by the rapid response services.

The following methods may be used to assess the consequences of emergencies:

- Assessment of the consequences of accidents in fire- and explosion-hazardous facilities;
- Prediction and assessment of the medical consequences of accidents in explosive and fire-hazardous installations;
- Prediction of the magnitude of contamination with highly toxic substances in accidents (destruction) of chemically hazardous facilities and transport;
- Prediction of possible accidents, catastrophes, and natural disasters;
- Damage assessment of emergencies of technogenic, natural, and terrorist nature, as well as classification and reporting of emergencies.

Figure 1 shows a typical functional diagram of a decision support system based on emergency monitoring and forecasting, which includes developed base software.

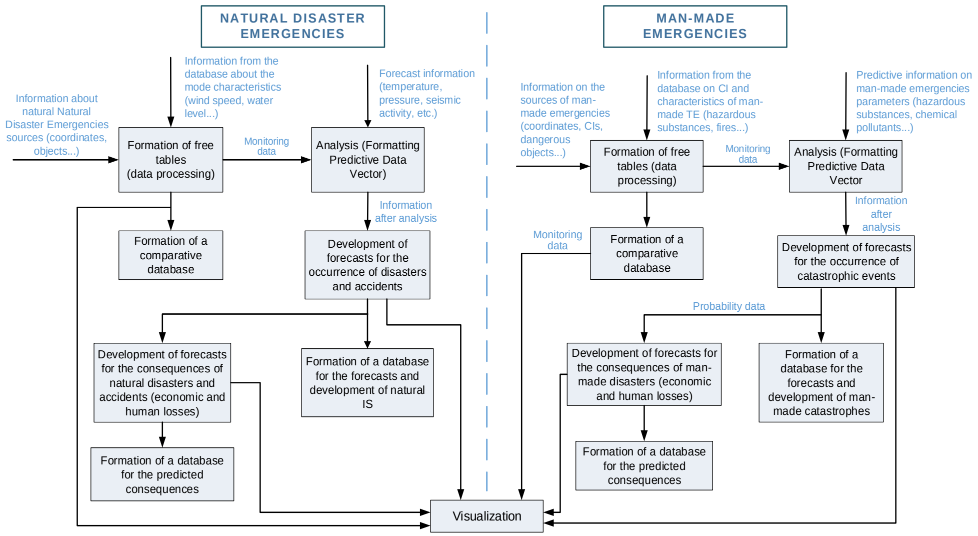

Fig. 1. Functional diagram of a decision support system information

The state must have a disaster information strategy to provide information that can be used for pre-disaster preparation, emergency response during a disaster, and damage and loss assessment, recovery, and reconstruction after a disaster [7]. Such baseline information can be gathered through careful mapping of risk areas and assessment of regions prone to major disasters.

Data are measurements or observations with variable magnitude (e.g., population size), classes (e.g., ethnic groups), or images (e.g., photographs). After analysis, the original data are converted into information that, through useful information extraction operations, is used for decision-making and action.

Information is translated into disaster risk knowledge through a learning process, and the timely and correct application of knowledge is translated into practical activities on the ground. Practice, in turn, produces new data that can be collected and analyzed. Thus, the entire information management cycle is not a linear process; rather, it is the information management cycle that continuously moves in a circle.

The development of intelligent management systems is one of the most important tasks nowadays, when computerization and intellectualization of vast areas of our lives are the basis for solving modern management problems. Modern automated control systems are essentially intelligent systems. In these systems, decision-making is a central process at all levels of human information processing. Problems are associated with the choice of decisions under conditions of incomplete information, arising when modeling the work of the human operator who perceives signals from the screens of indicators.

Intelligent technologies and AI systems to support decision-making

An intelligent decision support system (IDSS) is a decision support system that makes extensive use of artificial intelligence (AI) techniques. In general, intelligence is the ability to think, understand, and make decisions instead of doing something instinctively or automatically. The main ideas for creating artificial intelligence relate to the study of human thought processes, the representation and duplication of these processes using machines (computers, robots, etc.), and the study of behavior using a machine but performed by a human. The creation and development of artificial intelligence aim to make computers do things that humans now do to replicate some of the intelligent behaviors in a computer system.

The decision-making process today is complex, supported by computerized systems, and involves the following steps:

1. Problem definition. This is the basic stage. It provides decision-makers with a basis on which they can make assumptions, collect and analyze data, and evaluate alternatives. Problem definition begins with the recognition that a problem exists. A problem exists when

- There is a gap between what is expected and what is delivered;
- There is a deviation from the usual;
- The action taken is not justified;

The IDSS defines the problem and the complexities associated with the matched results.

2. Identification of the decision-maker. Depending on the nature of the problem, it is sent to the right person. A poorly structured problem will go to upper management, a difficult problem will go to managers, and repetitive problems will be sent to an employee at a lower hierarchical level.

3. Collection of information. Once the problem has been sent to the right person, the affected person can begin to collect data and identify the factors influencing the situation. Without DSS, data collection and analysis will take too long. DSS processes the data in a matter of seconds.

4. Evaluation of alternatives and decisions. This stage involves analyzing all possible courses of action and determining the most appropriate one by evaluating the pros and cons of each alternative. IDSS helps justify a particular choice.

5. Implementation and control. Once a decision has been made, it is necessary to move forward. Implementation requires planning. Monitoring is also important to determine the usefulness of a decision in achieving goals. This may require some adjustments or lead to a new problem. In the latter case, the entire process may need to be repeated.

The increased use of computer-based decision support systems is perceived as shifting the emphasis of decision-making to programs. The example in Fig. 2 of such a system [8] consists of the following components: data management, model management, user interface management, and decision support system architecture.

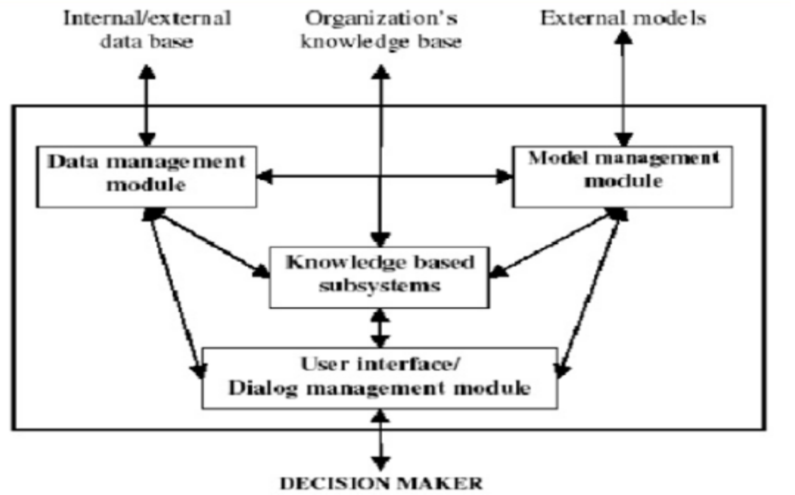

Fig. 2. Decision support system

The intellectual capabilities and behaviors integrated with the computer system create an intelligent machine. The machine must act as an assistant in decision-making, information search, the management of complex objects, and, finally, in understanding the meaning of words. To develop an intelligent computer system, it is necessary to gather, organize, and utilize human expertise and knowledge in various fields to improve the computing power of the system's brain with sophisticated algorithms using sensory processing, world modeling, behavior generation, value estimation, and global communication.

Mobile wireless networks have undergone a significant transformation in recent decades. At the same time, the generation of mobile wireless networks is usually determined based on such metrics as speed, technology, frequency, data volume, delay, user density, etc. Each generation has some features, standards, different capabilities, new methods, and new characteristics that make it different from the previous generation.

Wireless mobile technologies have evolved and improved significantly over the years as a result of intensive research and innovation. Now is the time when we can connect different wireless technologies, networks, and applications simultaneously through the latest technology, 5G (5th generation mobile communication technology). The new revolution in the mobile communication market is changing the use of mobile phones with very high bandwidth. This has transformed the network planning process from designing only for mobile devices to designing systems that connect different devices at high speeds [9].

Artificial intelligence and algorithms simplify the decision-making process. Using data processing systems has several undeniable advantages:

- Speed of decision-making: artificial intelligence can find optimal solutions in the enterprise much faster than a human;
- Minimizing errors and human influence: algorithms are not influenced by emotions and impulses when making decisions;
- Increasing the scope of the data analyzed: e.g., cross-analyses of geopolitical, economic, technical, etc. data;
- Expanding the possibilities and perspectives in problem-solving: applying new solutions and looking for different options.

In contemporary publications, various aspects of the intellectual activity of the human operator (HO) are considered, in particular expediency, the ability to acquire, complete, reproduce, and use knowledge, the ability to pose and solve problems, the ability to anticipate the unknown, the ability to generalize and make associations, etc. The intellectual activity of a person is associated with the search for solutions (actions and regularities) in new, non-standard situations when the solution is a priori unknown. In this case, the solution to the problem is understood as any activity (human or machine) related to the creation of plans and actions necessary to reach a certain goal, as well as the corresponding new conclusions and regularities.

Knowledge is the useful information accumulated by an individual, and intelligence is his ability to use this accumulated information in some useful and purposeful form. The intellectual (cognitive) functions of the living intellect are perception, intuition, creativity, association, induction (generalization), syllogism, prediction, planning, deduction, classification, and also search and selection, comparison, identification, and calculation. At present, the following functions have been analyzed and formalized in detail: search, choice, calculation, comparison, and deduction. Attempts to implement higher-level intellectual abilities on the computer have so far yielded no practical result. Thus, the full realization of intellectual capabilities related to decision-making, planning, forecasting, and effective management, as well as intellectual decision support systems, should be based on the use of the latest AI-based technologies and expert systems.

Nature and composition of the critical infrastructure monitoring system

By its nature, an CIMIS from a system-information perspective should be an event-driven CIS (ICS) with the provision of a continuous flow of sensor data processed and presented with AI technologies and tools as the CI that performs real-time information assurance and decision-making for users.

In organizational and technical terms, the CIMIS should be a network-centric system that includes a communication subsystem (a common transport network environment), a sensor area (sensors for conversion of physical parameters into data and a sensor network for access), and a technical management area including other management subsystems (Unmanned Aircraft Systems (UAS), network, and application management). The users of the network-centric system should be provided with a common communication environment with a high degree of intelligence and interactivity and with capabilities to access, update, and reuse the CI from other information subsystems [10, 11].

The CIMIS must be integrated and provide and present both information from its sensor networks so that, in the application layer, it is open and can include and integrate data from other segments and subsystems (e.g., space, specialized IS of government and public organizations).

Integrated mobile monitoring systems in Internet environment

Modern integrated mobile monitoring systems (IMMS) are CIS-inherently distributed computing resource systems that secure important sectors of the national economy, security, ecology, and people's business activities. The convergence of information objects and network structure in information-centric networks allows for increasing the speed of real-time information exchange in the composition of their information structure, including in their geographical boundaries and hard-to-reach areas. In addition to communication services with guaranteed availability and quality, the IMMC provides access to dynamic information in real-time with information object formation, data analysis, and presentation appropriate for the system, which gives grounds for its analysis as a CIS.

Mobility nodes for forming, collecting, and aggregating information from fixed or mobile sensors deployed on unmanned aerial vehicles (UAVs) are aggregated into CI with information integrated from other information systems, including satellite systems. The latter, from a cybernetic point of view, are large (complex) systems and, in contrast to UAVs, are characterized by specific properties such as globality of use, multi-purpose, and multi-functionality. Aerospace technology is an important modern preventive factor ensuring timely detection, identification, and scoping of various crisis processes. Space- and air-based technologies overcome a significant portion of the shortcomings and limitations of traditional ground-based technologies, mainly related to monitoring, navigation, and communication.

Modern IMMS for monitoring have an information and communication resource, providing a wide class of tasks for events, the solution of which exceeds the capacity of the system to serve the usual activities, ensuring business activity and protecting society. The observation and monitoring based on such technical solutions are necessary when it is necessary to supply and analyze data from urgently installed sensors in connection with a specific situation, such as fires and their containment in remote areas; chemical pollution with high dynamics and danger to people's lives and health; in the event of an urgent inspection and expert assessment of damage in hard-to-reach objects; finding and rescuing people; monitoring for telemedicine purposes; and many others. Integration into the monitoring system of satellite information and data from other information systems provides additional opportunities for forecasting and analysis of the monitoring data obtained as a result and their processing to achieve the system's goals. In addition, the space monitoring system is a complex system with a space and ground segment, collecting, processing, archiving, and providing users with information about objects, phenomena, and processes on the earth's surface.

Trends in the formation of a global information infrastructure in modern societies and the development of the needs of citizens, businesses, and society imply the simultaneous use of monitoring systems, modern mobile data transmission technologies (4G/5G), and export opportunities of information on the Internet with appropriate formatting and presentation.

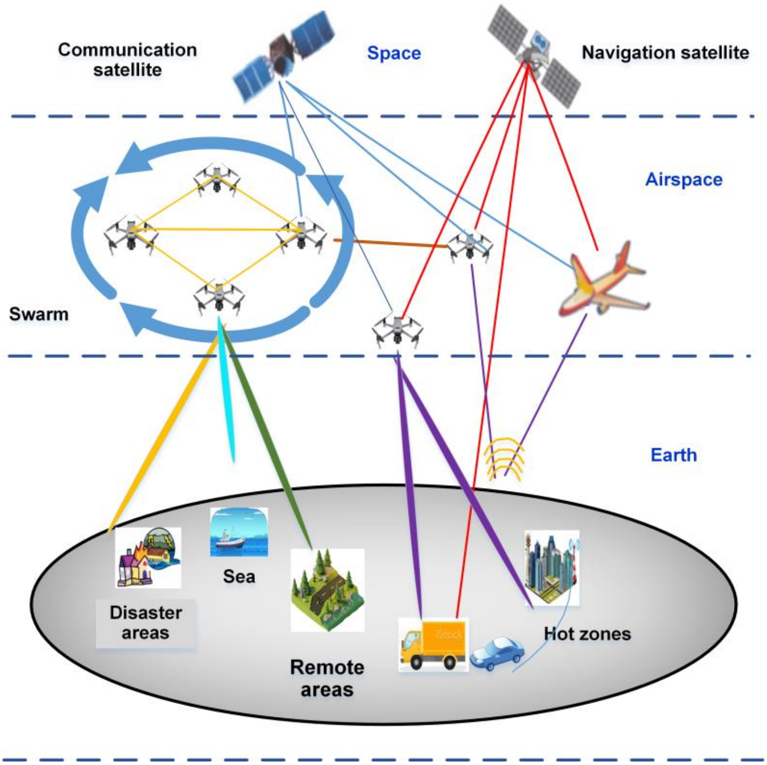

Fig. 3. Integrated monitoring system

The adoption of Internet technologies (the TCP/IP architecture as a network model and protocol stack) was justified as the basis for building a network-centric CIMIS. Its structure in generalized form consisted of functionally complete information-communication clusters (ICCs). The communication architecture of the backbone network should ensure the operation of mobile and stationary information clusters, integration with other ISs (space segment, national networks related to CI protection), and the presentation of results on the Internet. The requirements to be network-centric require the use of virtual private network technologies and transport over the Internet. For mobile ICS, transport must be over Internet protocol over public mobile data networks (5G, 4G, 3G, and 2G). In geographic areas where there is no coverage by national mobile operators, satellite Internet can be used, or Internet protocol transport can be built over a radio channel. A necessary requirement for all ICs is that they are connected to the IP backbone and operate in a network-centric environment.

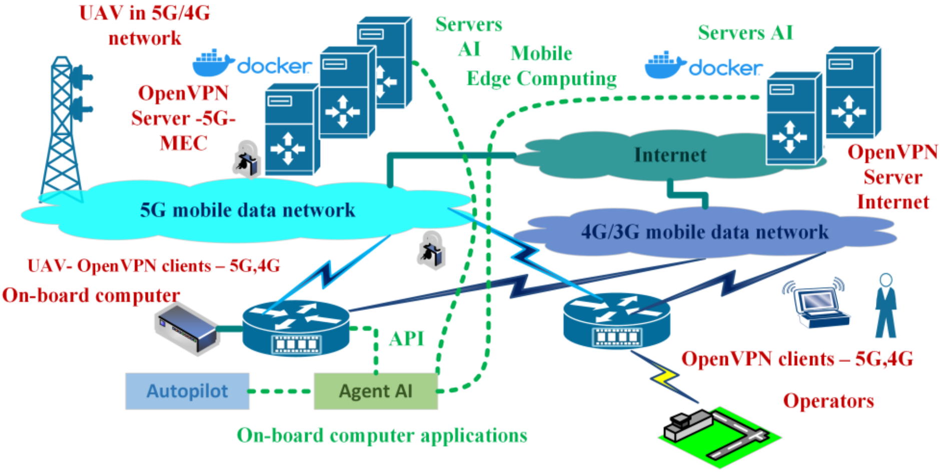

Fig. 4. Clusters of CIMIS in a virtual private network [5]

The server part of the IC (the application layer in the network model) can also be viewed as an ICC or a group of clusters that are located in the network address space [5].

OpenVPN technology is chosen as the backbone of the virtual private network. The advantages and features provided by the technology will be described in detail for a mobile ICC of UAS and connectivity to a processing and presentation cluster. The application of OpenVPN technology provides the integration of the ICC into a common environment, scalability, manageability, redundancy, migration, reliability, and evolution of the backbone network. On this basis, flows of information objects (IO) can be transported and a functional ICC structure can be built.

The network-centric environment performs its protection and monitoring functions in four main logical network architectures: centralized, on-demand (ad hoc), swarm, and combined.

Centralized network-centric architecture

In the centralized architecture, a single OpenVPN server is used to provide network access to all clusters through routers running as OpenVPN clients. The availability and survivability of the configuration are related to having a single vulnerable point in the structure at all levels of the network model. The advantages of the centralized architecture are in terms of synergy effects in terms of management and coordination of the entities and sites in the CIMIS. It provides coordination of the work with the different ICCs and efficiency greater than the efficiency of the clusters individually. A significant disadvantage is the complexity of maintaining, administering, and coordinating a large number of nodes in the network, for example, from the CI control center level down to the UAV or gateway level in a sensor radio network. The information flows in the CIMIS have to be pre-formed as IO-type flows, and their direction is not always directly to the logical center of the network, which is fixed in a centralized architecture. For CIMIS, a centralized network-centric architecture can be provided by OpenVPN technology, but it is only applicable to relatively small systems.

Swarm architecture

The chosen technology for building a virtual private network, OpenVPN, enables the most complex and most promising architecture in a network-centric environment: swarm architecture. A swarm is a combination of homogeneous elements with limited and fixed resources of their own that must exchange information with each other for the purposes of self-synchronization, self-organization, efficiency gains, and achieving multiplicative effects. A swarm can be considered a group of UAVs, one of which has the role of an information hub, an ICC of mobile monitoring and control stations, united and linked to one of them, which has a satellite Internet connection and provides the network access of the others and the coordination between them. There are different types of network-centric swarm architectures: managed, hierarchical, distributed, and mixed.

The chosen virtual private network technology, OpenVPN, with centralized routing management for full connectivity (everyone to everyone), independence from a fixed port, and the possibility of simultaneous participation of a network node as a server or client, allows the implementation of an arbitrary logical structure in a network-centric environment.

Conclusions

Modern integrated mobile monitoring systems are inherently communication and information systems (CIS) with distributed computing resources, which provide important branches of the national economy, security, ecology, and business activity of people. The convergence of information objects and network structure in information-centered networks allows for increased speed of real-time information exchange in the composition of their information structure, including in their geographical boundaries and hard-to-reach areas. In addition to communication services with guaranteed availability and quality, the monitoring system provides access to dynamic information in real-time with the formation of information objects, data analysis, and presentation appropriate for the purposes of the system, which gives grounds for its analysis as an information and communication system.

The integrated system incorporates both real-time geographic data from sensors in hard-to-reach areas and mobile asset-based sensors (UAS), as well as data for forecasting or overcoming disasters and critical situations obtained through electro-optical, infrared, and radar sensors on surveillance satellites. Solving problems related to the integration of data from different systems, management of information flows, presentation on the Internet, export to other systems, and provision of information security is relevant and significant in modern monitoring systems. The combination of local and cloud technologies, tailored to the capabilities of mobile data networks (4G/5G), and the optimization with regard to the required speed performance are contemporary issues in the context of the development of modern automated systems for the transport of people and goods.

The pace and direction of modern scientific and technical progress require new state-of-the-art ideas on the methodology of building integrated systems for forecasting, containment, and eradication of environmental incidents, search for people, and rescue of human life. They must also be compatible with new generations of information and communication systems designed to ensure user mobility and innovation in the use of modern technologies. This is one of the main objectives of this project.

Acknowledgments: This article was prepared within the framework of project t.1.1.6 of the National Science Program “Security and Defense” (adopted with № 731 of 21.10.2021) and according to Agreement № 01-74/ 19.05.2022 between the Ministry of Education and Science and Defense Institute “Professor Tsvetan Lazarov”

References

1. Димитров, Н., Системен подход към критичната инфраструктура, ВВМУ "Н. Й. Вапцаров", Варна, 2019.
2. Додонов, А., Д. Ландэ, Живучесть информационных систем. К.: Наук. думка, 2011.
3. Сотиров, Г., Е. Хубенов, З. Чифлиджанова, Агрегиране на услуги, базирани на изкуствен интелект, в интегрирани мобилни системи за мониторинг в интернет среда, Eighteenth International Scientific Conference, SES2022, PROCEEDINGS SES`22, pp. 127–133, Sofia. http://space.bas.bg/SES/archive/SES%202022_DOKLADI/2_Aerospace%20Tec hnologies/7_Sotirov.pdf
4. The Future Internet, Editor: Domingue J., Galis A., and ect., 2011, Publisher: Springer Berlin Heidelberg, Lecture Notes in Computer Science, DOI:10.1007/978-3-642-20898 -0 , https://www.researchgate.net/publication/230634079_The_Future_Internet
5. Хубенов, Е., Г. Сотиров, З. Хубенова, Безпилотни авиационни системи с елементи на изкуствен интелект в интернет среда, SES`2021, Seventeenth International Scientific Conference „Space, Ecology, Safety", PROCEEDINGS SES`21, pp. 121–127, Sofia. http://space.bas.bg/SES/archive/SES%202021_DOKLADI/PROCEEDINGS%20SES%202021.pd
6. Мардиросян, Г., Природни бедствия и екологични катастрофи АИ "Проф. Марин Дринов", 2009 г.
7. ДИРЕКТИВА 2008/114/ЕО НА СЪВЕТА, относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита, https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32008L0114&from=HR
8. Scott Morton M. S. Management Decision Systems: Computer-based Support for Decision Making.—Boston: Harvard University, 1971.
9. Munir Md. S., S. F. Abedin, C. S. Hong, Artificial Intelligence-based Service Aggregation for Mobile-Agent in Edge Computing, Conference: The 20th Asia-Pacific Network Operations and Management Symposium, Japan, 2019.
10. Department of Defense Net-Centric Services Strategy Strategy for a Net-Centric, Service Oriented DoD Enterprise March 2007 Prepared by the DoD CIO
11. Net-Centric Environment Joint Functional Concept Department of Defence USA, version 1.0

ИНТЕЛИГЕНТНА СИСТЕМА ЗА МОНИТОРИНГ И ЗАЩИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА НА БАЗА МОБИЛНА КОМУНИКАЦИОННА-ИНФОРМАЦИОННА СИСТЕМА С ЕЛЕМЕНТИ НА ИЗКУСТВЕН ИНТЕЛЕКТ

Е. Хубенов, З. Чифлиджанова

Резюме

В статията се предлагат съвременни иновационни решения за интегрирана мобилна система за мониторинг с елементи на изкуствен интелект в Интернет среда на база мобилна комуникационна-информационна система за събиране, агрегиране, обработка и презентиране в реално време на потоци от информационни обекти. Представено е управлението на комуникационни мрежи с цел оптимизация на транспорта и обработката на информационни обекти на основа на дискретно-събитийно представяне на потока от данни и моделиране с йерархична структура. Разгледани са качествени аспекти както за мрежи, предназначени за мониторинг и известяване на геофизически, климатични и други природни феномени, така и за антропогенни системи. Направено е сравнение на възможностите на централизираното и децентрализирано управление, както и състоянието на съвременните мрежови технологии и възможностите за практическа реализация в различни мрежови архитектури.