INFORMATION FLOWS AND INTELLIGENT PROCESSING IN CLUSTERS FOR CRITICAL INFRASTRUCTURE MANAGEMENT

Evgeni Hubenov, Zoya Chiflidzhanova, Georgi Sotirov

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

Keywords: *cluster, critical infrastructure, monitoring system, network-centric architecture, artificial intelligence*

Abstract: *We propose a methodology for transforming data into information objects that build a complete operational picture of a node with common interests within a cluster of a critical infrastructure monitoring system. The real-time processing and visualization of information object flows is based on network-centric architecture principles. The synthesized structure allows for the introduction of artificial intelligence and machine learning elements to generate predictive models for situational awareness and decision optimization.*

ИНФОРМАЦИОННИ ПОТОЦИ И ИНТЕЛИГЕНТНА ОБРАБОТКА В КЛЪСТЕРИ ЗА УПРАВЛЕНИЕ НА КРИТИЧНА ИНФРАСТРУКТУРА

Евгени Хубенов, Зоя Чифлиджанова, Георги Сотиров

Институт за космически изследвания и технологии – Българска академия на науките
e-mail: hubenov@space.bas.bg

Ключови думи: *клъстер, критична инфраструктура, система за мониторинг, мрежово-центрична архитектура, изкуствен интелект*

Резюме: *Предложена е методология за трансформиране на данни в информационни обекти, които изграждат пълна оперативна картина за възел с общи интереси в клъстер от система за мониторинг на критична инфраструктура. Обработката и визуализацията на потоците информационни обекти в реално време е базирана на принципите на мрежово-центричната архитектура. Синтезирана е структура с възможности за въвеждане на елементи на изкуствен интелект и машинно обучение за генериране прогнозни модели за ситуационна осведоменост и оптимизация на решенията.*

A Systems Approach to Critical Infrastructure Monitoring Information Systems

The information systems approach to critical infrastructure monitoring information systems (CIMIS) focuses on the processes of receiving, transporting, processing, and presenting information related to critical infrastructure (C**I**) protection processes. The information interface with other subsystems implies that CIMIS is designed as a communication and information system (CIS).

An organizational-structural approach defines a CIS as a set of technical means (including communication, security, and cryptographic devices; and a medium for signal propagation within system boundaries) and programmatic means (including methods, procedures, and personnel) organized to perform one or more functions of creating, processing, using, storing, and exchanging classified information in electronic form. A CIS is a distributed, spatio-temporal, discrete-event system that includes two interconnected subsystems (communication and information) in its structure, which are designed to transport and process flows of information objects (IOs).

An IO is a structured set of data, either single or composite, that is large and organized enough to be interpreted and processed. IOs can be divided into classes, subclasses, and entities. Each IO's structure also includes metadata, which describes the data's attributes and place of origin and time of creation. Streams of information objects cover different subjects and enter the CIS from

various sources within or related to CI domains. The purpose of CIMIS is to detect, classify, identify, and track CI-related events in a timely manner, providing real-time situational awareness to support CI protection decision-making [1].

Event-driven CISs include hardware and software components that operate simultaneously in different domains of interconnected communication environments. These systems use events as the main object to organize dynamic communication between components and adapt their structure to data flow parameters. The dynamics of these systems relate to the occurrence of physical events at irregular, previously unknown times. Generally, an event is defined as a change in the system's state in discrete state space. In a CIS, various information flows are formed for monitoring and control purposes. Users are interested in changes to monitoring parameters directly related to CIS protection, as well as events related to disasters, accidents, and catastrophes. To maintain the CIS's functional characteristics and support the system operator, it is important to understand the information flows resulting from the CIS's interaction and interdependence with other elements of the information space (IS).

The Network-centric nature of critical infrastructure monitoring information systems

The Network-Centric Environment (NCE) is an information interaction framework that provides full human and technical connectivity. This allows all users to share information as needed and in the required format to perform their functions. The NCE's principles, capabilities, and attributes are divided into two domains: the knowledge domain and the technical domain.

The purpose of CIMIS is to provide information for situational awareness and real-time decision-making related to CI protection. Network-centric warfare is a military doctrine that seeks to transform an information advantage, in part provided by information technology, into a competitive advantage. This is achieved by using robust and effective network and information technologies to access a shared Unified Information Space (UIS). The UIS is defined as a system of information objects (IOs) aggregated into thematic clusters that are formed and modified by information exchange in a secure communication environment [2, 3].

The United States Department of Defense first introduced the doctrine in the 1990s. CIMIS is implemented during events such as disasters, accidents, and terrorist attacks when initial information or accurate predictions are lacking, as well as during wartime.

The network-centric systems approach defines the specific characteristics of the CIMIS information structure in the communication subsystem (i.e., the common transport network environment), the sensor area (i.e., sensors that convert physical parameters into data and sensor network access), and the control area of the technical means for collecting sensor data. A mandatory subsystem is dedicated to network and service management and monitoring. All subsystems must be accessible through the common transport environment.

Characteristics of a Critical Infrastructure Monitoring Information System

The network-centric system approach defines the specific characteristics of the information structure of CIMIS:

- CIMIS subsystems include the communication subsystem (common transport network environment), the sensor domain (which includes sensors that convert physical parameters into data and a sensor access network), and the control domain of technical means for acquiring sensor data. A mandatory subsystem manages and monitors CIMIS networks and services.
- The common transport environment must ensure the security of information and the protection of data and network transport. The monitoring system must provide remote access to information and management of system functionalities, including control.
- CIMIS services shall be defined and described by means of access and user rights, and they may be used at any point in the address space of the communication environment. The service registry shall specify the access method, service provider, processes that create the service, and information objects on which the service is based.

Information and Communication Cluster

Adopting Internet technologies, such as the TCP/IP architecture as the network model and protocol stack, is the basis for building a network-centric CIMIS. In a generalized form, its structure consists of functionally complete information and communication clusters (ICCs). The backbone network's communication architecture should ensure the operation of mobile and stationary information clusters and integration with other systems, such as the space segment and national networks related to CI protection. It should also be open to presenting results on the Internet. The

communication subsystem with mobile ICCs includes management of unmanned aerial vehicles (UAVs) and unmanned aerial systems (UASs). The network-centric requirements necessitate the use of a virtual private network (VPN) and transport technologies over the Internet. Mobile ICCs require Internet protocol transport over public mobile data networks (5G/4G). In areas without national mobile network coverage, satellite internet or internet protocol transport over a radio channel can be used. All ICs must be connected to the IP backbone. From an organizational and technical standpoint, ICCs are elements of the CI system that provide mobile groups for specific CI management and operational activities. For example, they are used in firefighting scenarios, search activities, and chemical pollution measurements.

Structure and Topology of a Network with Mobile ICCs for CI Monitoring

OpenVPN technology was selected as the virtual private network backbone. Its benefits and features are described in relation to a mobile ICC's specificity in the UAS composition and connectivity to a processing and presentation cluster. OpenVPN technology provides ICC integration in a common environment, as well as scalability, manageability, redundancy, facilitated migration, reliability, and backbone network evolution. Based on this, information object flows can be transported, and a functional CIMIS structure can be established.

The ICC structure, defined by the system's purpose, is hierarchical with a local degree of centralization (the UAV Control Center) and regional, with groups of UAVs connected to the global Internet network. Connecting to the Internet provides data transport, and the virtual private network provides a network-centric environment. By its nature, the network is an element of an open CIMIS, connected to the Internet and with the necessary level of data protection. A suitable logical network structure adequate for the project objectives is a star type with an OpenVPN server (control center) and a hierarchy of several ICCs. UASs can also be considered clusters or groups of clusters with a high degree of mobility. They provide flight control of multiple UAVs and deliver data from mobile or spatially distributed sensors, aggregating it into IOs [4].

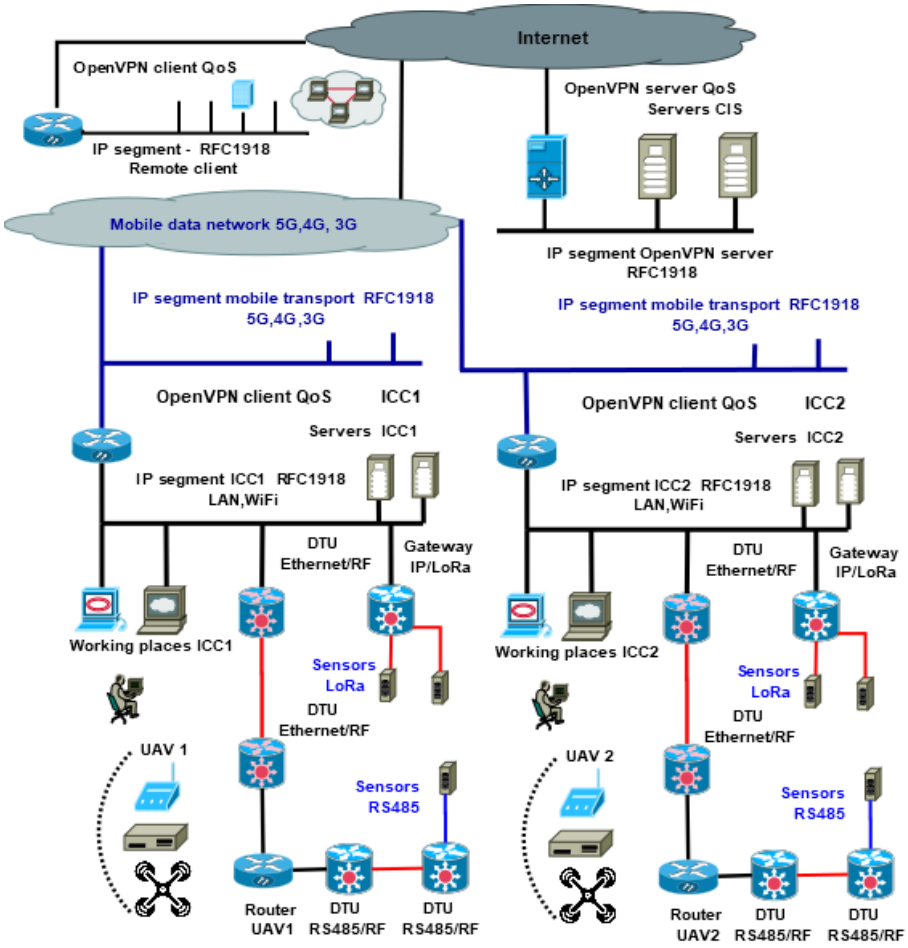

Fig. 1. Network topology of information and communication clusters

The IP segment is "unicast," and the OpenVPN server configures its routing. This ensures the formation of specific ICC groups and the management of communication and information exchange between them. Radio channels are used for IP transport for remote points within the ICC that need to use addresses from the internal IP segment. This provides IP control to the UAV for flying sensors and to IP gateways for the sensor network.

Fig. 1 shows the topology of the ICC network. Two ICCs are shown to illustrate how the number of mobile teams and sensor fields can be increased through horizontal scaling, or by adding more ICCs. Increasing the number of supported ICCs is achieved through vertical scaling of the OpenVPN servers and the servers supporting the CIMIS services (i.e., communication and computing resources). The two ICCs differ in their networking and internet access due to their different certificates, access keys, and private internal IP network segments. Management of connectivity and data exchange between the two ICCs is done via a centralized routing configuration in the OpenVPN server.

In a network-centric environment, it is necessary to isolate a compromised ICC from the virtual network in the event of a UAV or router loss, for example. For the selected network technology, this is accomplished by disabling the corresponding certificate and excluding the OpenVPN client network segment routing tables from the OpenVPN server configuration. Fig. 1 illustrates two types of IP gateways to the sensor network (in this case, the topology is LoRa). One gateway is connected directly to the Ethernet segment at the ECC control point, and the other is connected via the radio channel used to control the UAV and access the IP/RS485 gateway carried by the UAV as a payload.

Community of Interest (COI) and COI Node

The system architecture adheres to the principles of Network-Centric Architecture (NCA), as defined in the United States Department of Defense (DoD) and NATO doctrines, and adapts them to the needs of civil crisis management. In this model, each information cluster represents a community of interest (COI) or COI node.

The COI node is fully functional and provides a group of users united by a common mission or geographical area with all the necessary information support. For the sake of specificity, we will assume that the COI users are two groups of firefighters working in neighboring geographical areas. Mobile ICCs provide information services with a mobile sensor network and UAVs for visual surveillance and aggregating sensor data. This forms a collaboration environment (or federation), which allows for the exchange of information and coordination between different COI nodes. Fig. 2 shows the formation of information flows within the COI.

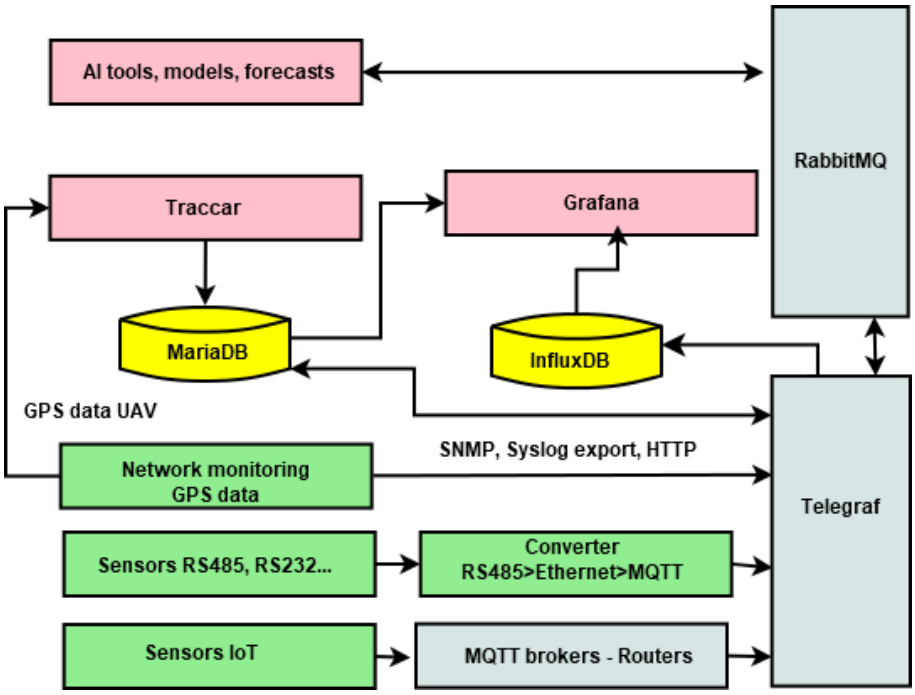

Fig. 2. Iinformation flows within the COI

Various edge-to-core data pipelines have been defined to formalize the flow of information from sensor networks on the periphery to central visualization systems. Visualization for COI information services manages specific processes, such as firefighting. The UAV payload operator evaluates data from the sensor field and video surveillance.

CIMIS's goal within the COI Node is to create a Common Operational Picture (COP) and a Shared Information Space within the federation of geographically adjacent COIs. Intelligent decision support is achieved by introducing elements of artificial intelligence (AI) and machine learning to analyze information and generate predictive models. These models form the basis of the Decision Support System (DSS), which is designed to help teams forecast incident development and optimize resources. This is a step towards achieving predictive awareness and self-synchronization.

The composition and structure of the COI node

The COI sensor network field consists of different types of sensors, and remote access is implemented via a radio channel. For sensors with telecommunication interfaces that provide a point-to-multipoint topology (RS485), Data Transfer Units (DTUs) are used. These DTUs are "transparent" to the protocol. The DTUs are UAV-based, and the router has an RS485 bus. The router also acts as an RS485 hub with IP access. Multiple sensors in the COI Node's geographical area can be connected to a single converter via an RS485 hub, reducing the number of wireless modules required. DTU RS232/RF or Ethernet/RF are used for sensors with telecommunication and network interfaces, and they are terminated on the UAV-based router. This method can be used to collect data from large geographic areas when the geographic coordinates of the sensors are known.

Message Queuing Telemetry Transport (MQTT) is an Internet of Things (IoT) standard messaging protocol. Designed for event-driven systems, it uses publish-subscribe technology. The MQTT broker is central to event-based communication. The broker receives data from protocol gateways, and each message is published in a specific "topic" or channel. MQTT clients, such as user applications, visualization systems, and databases, subscribe to these channels and receive real-time data without the need for constant polling.

The built-in publication-subscription structure of the COI Node application supports the MQTT protocol through the use of Telegraf as an MQTT client. The application converts information from MQTT channels into time series metrics, which it then records in databases such as InfluxDB and MariaDB. Telegraf also creates time series from data structures received from various sensors via an MQTT broker. These structures are essentially information objects that can be reused in a network-centric environment. Telegraf's functionalities are provided by specialized plugins.

SNMP (Simple Network Management Protocol) plug-ins are used to monitor the IP network and maintain quality of service (QoS). The routers in the COI's ICC use various technologies to export information for managing, monitoring, and controlling the network in a mobile environment. This process can be summarized as syslog export from different network devices, categorizing by facility and severity, and processing time series data.

The Traccar application is used to provide information about the geographical coordinates of the UAV and the sensors, as well as additional information related to the tasks in the COI, such as the fire front, hot spots, and direction of spread. An HTTP-format API (application programming interface) is available for automated requests from sensors, network devices, and the UAV payload operator.

The UAV payload operator's workspace uses Grafana. This application provides the video monitoring operator with real-time integration capabilities on their desktop. These capabilities include access to cameras located on the UAV, the Traccar screen, UAV movement data, and physical values from sensors. All of this information is simultaneously recorded in databases.

Telegraf collects data from sensors and network devices, as well as observations and data from the payload operator's activities. This data is visualized on the Traccar desktop and stored in InfluxDB and MariaDB databases. A specialized plugin establishes a connection between Telegraf and RabbitMQ. Acting as an information broker, the application processes, stores, and handles streams of information objects formed for COI purposes. There is also the possibility of flexible routing to neighboring COIs or forming a Service Oriented Architecture of CIMIS [5, 6].

Data from RabbitMQ is stored in databases to create machine learning models or to feed into trained models for real-time predictions to achieve COINode objectives. Processing time series data from the COI Node provides real-time predictions for Predictive Awareness, such as fire spread rate, direction, and risk levels. Integrating RabbitMQ into the structure of information flows in COI facilitates the integration of various AI development tools. RabbitMQ analyzes time series from sensor data and information objects, then routes them to AI tools for creating and using machine learning models.

Conclusions

This paper proposes a structure and methods for transforming data into streams of information objects. These methods build a complete operational picture for nodes with common interests in clusters of critical infrastructure monitoring systems. Real-time processing and visualization of information object streams provide self-synchronization for operation in a network-centric environment. This synthesized structure can introduce elements of artificial intelligence and generate predictive models to improve situational awareness and decision-making.

Acknowledgments:

This article was prepared within the framework of project p.1.1.6 and 3.1.7 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. Hubenov E, Z. Chiflidjanova, Intelligent Monitoring and Protection System of Critical Infrastructure Based on Mobile Communication-Information System with Elements of Artificial Intelligence, Aerospace Research in Bulgaria. 36, 2024, Sofia; DOI: https://doi.org/10.3897/arb.v36.e12
2. Department of Defense Net-Centric Services Strategy Strategy for a Net-Centric, Service Oriented DoD Enterprise March 2007 Prepared by the DoD CIO
3. Net-Centric Environment Joint Functional Concept Department of Defence USA, version 1.0 2005
4. Сотиров Г., Е. Хубенов, З. Чифлиджанова, Агрегиране на услуги, базирани на изкуствен интелект, в интегрирани мобилни системи за мониторинг в интернет среда, SES`2022, Sofia, PROCEEDINGS SES 2022, стр. 127–134
5. Chiflidzhanova Z., E. Hubenov, G. Sotirov, Synthesis of a Unified Information Space for Critical Infrastructure Monitoring, SES`2024, Sofia, PROCEEDINGS SES 2024, p. 133–140
6. Хубенов Е., Г. Сотиров, К. Алексиев, З. Хубенова, Системи за мониторинг на критичната инфраструктура с елементи на изкуствен интелект, и-во на БАН „Проф. М. Дринов", София, 2024.