SYNTHESIS OF A UNIFIED INFORMATION SPACE FOR CRITICAL INFRASTRUCTURE MONITORING

Zoya Chiflidzhanova, Evgeni Hubenov, Georgi Sotirov

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

Keywords: *information space, communication-information system, service-oriented architecture*

Abstract: *An approach for synthesizing a unified information space to support critical infrastructure management in a network-centric environment is presented. Information from a sensor network structured into information objects is provided within a communication-information system. The system is structured in mobile information-communication clusters. Aggregation of information in clusters and centralized processing of information objects flows is provided by a service-oriented architecture.*

СИНТЕЗ НА ЕДИННО ИНФОРМАЦИОННО ПРОСТРАНСТВО ЗА МОНИТОРИНГ НА КРИТИЧНА ИНФРАСТРУКТУРА

Зоя Чифлиджанова, Евгени Хубенов, Георги Сотиров

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

Ключови думи: *информационно пространство, комуникационно-информационна система, ориентирана към услуги архитектура*

Резюме: *Представен е подход за синтез на единно информационно пространство за подпомагане на управлението на критична инфраструктура в мрежово-центрична среда. Информацията от сензорна мрежа, структуриране в информационни обекти се осигурява в рамките на комуникационно-информационна система. Системата е структурирана в мобилни информационни-комуникационни клъстери. Агрегирането на информацията в клъстерите и централизираната обработка на потоци от информационни обекти е в ориентирана към услуги архитектура.*

Introduction

Critical Infrastructure (CI), considered as a complex hierarchical system structured in elements, connections and relationships between them, has a system goal (desired system 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. The main objective of CI management information support is to improve the ability to make and implement informed decisions. The CI protection and management system operates as multiple subsystems with unified management, providing specific objectives with their own unified information space (UIS) [2]. The UIS is a collection of information resources and information access systems with structuring, navigation, and transport capabilities. For the purpose of the analysis, we assume a definition of the UIS as a communication environment in the form of a system with complex links between information sources, in which aggregated (clustered) sets of similar subject matter are formed and transformed as a result of information messages between them. If we accept the hypothesis of defining CI as a system or the effectiveness of protection as a result of the actions of multiple stakeholders united in a system of systems [1], then monitoring should be included in them in a common infrastructure (framework) [3,4]. The objectives of monitoring in the Critical Infrastructure Monitoring Information System (CIMIS) do not imply the management of processes related to CI protection, but only information for decision support and situational awareness.

Requirements for operation in a network-centric environment

The Net-Centric Environment (NCE) [5,6] is a framework for full human and technical connectivity and interoperability that enables real-time information assurance for all users of the CIMIS. The existing networks and systems that form the NCE provide a wide range of information services and functional capabilities within each of the Information and Communication Clusters (ICCs) for CI management and protection operations. The system architecture uses common services and architectures that have the following characteristics:

- The use of a common set of standards and rules is supported to provide a common, shared and secure infrastructure;
- Information services with the required level of protection can be used in any area of activity to provide situational awareness, regardless of which partner provided the information;
- Management of access to information resources is centralized and provides the ability to efficiently reuse information.

The NCE systems approach defines specific information structure characteristics of the CIMIS [7]. They should provide UIS and information awareness to all teams and structures that are involved in CI and emergency management:

- It is a system of systems in and of itself and as a subsystem within the overall CI protection tasks. The subsystems within the CIMIS are the communication subsystem (common transport network environment), the sensor area (sensors for converting of physical parameters into data and sensor access network), the control area of the technical means for sensor data collection including unmanned aerial vehicles (UAVs) and unmanned aerial systems (UAS). A subsystem for managing and monitoring of CIMIS networks and services is mandatory. All subsystems shall be accessible through the common transport environment. The monitoring system shall provide services for remote access to information and management of system functionalities, including system management.
- The services of the CIMIS are defined and described with the access method and user rights and can be used at any point in the address space of a communication environment. For each service, the service registry must specify the access method, the service provider, the processes that create the service and the information objects (IOs) on which it is based. An Information Object (IO) is a structure of single or composite data, positioned at different locations in the information space, in a volume and organization sufficient for their interpretation and processing. IOs can be divided by classes, subclasses, and subjects. Metadata or data about the data can serve to discover and identify information resources, to describe the structure, other attributes - origin, time of creation. IO is a data and metadata structure that does not require additional information for its processing and use.
- The information structures used by service providers must be built according to common rules and standards and allow reuse in other information systems or processes as "building blocks" [5], Fig. 1.
- Users of the system should be able to use services from the registry and developers of the services should have access to the IO.
- An information security system must be defined and operational in the system [4].

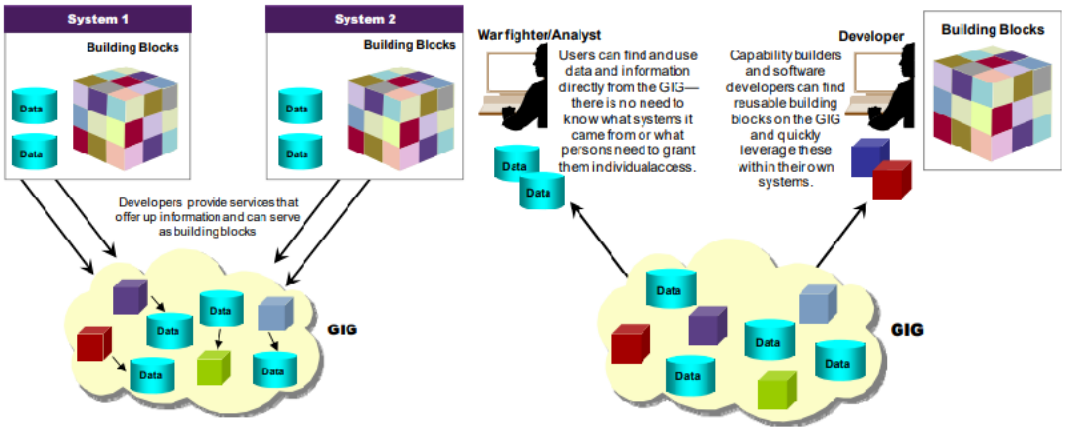

Fig. 1. Information objects in the terminology of network-centric architecture [4]

Structure and topology of a communication-information system

A communication-information system (CIS) is defined as a collection of technical (including communication facilities, security devices, cryptographic facilities and signal distribution media) and software facilities, methods, procedures and personnel. The elements of a CIS are organized to perform one or more of the functions of creating, processing, using, storing and exchanging (classified) information in electronic form [1]. A CIS is a complex distributed spatio-temporal discrete-event system that includes in its structure two interconnected subsystems (communication and information) that are designed for the purpose of transporting and processing flows of IOs [7].

The communication environment is based on a Virtual Private Network (VPN). OpenVPN technology provides encryption of traffic with a high level of protection and OpenVPN clients' access to it based on generated certificates. The OpenVPN client certificate can be considered as a group single-factor authentication and authorization for the users whose work is provided by the router (e.g., operators and personnel in a mobile UAV control workstation). The structure allows for a centralized management based on the ICCs, which are OpenVPN clients in the network plan structure.

The communication architecture of VPN ensures the operation of mobile and stationary information clusters, integration with other information systems (space segment, national networks related to CI protection), and provides an ability to present the results on the Internet. The requirements for NCE require the use of virtual private network technologies and transport through the Internet. For mobile ICC, transport is via Internet protocols over public mobile data networks (5G/4G/3G/2G). In geographic areas where there is no national mobile coverage from national mobile operators, satellite Internet can be used or Internet Protocol (IP) transport can be built on a radio channel. It is a prerequisite that all ICCs are connected to the IP backbone and operate in a network-centric environment.

Unified Information Space of the Monitoring System

The IOs streams have different topics and arrive at the CIS from different sources within or related to the CI domains. The purpose of CI monitoring is to detect, classify, identify, and monitor events in a timely manner and provide real-time situational awareness to support CI protection decision making. An event is defined as a change of system state in the discrete state space.

Monitoring and CIMIS processes are associated with a class of applications that continuously and indefinitely process CI from one or more sources. The sequence of data generated by the sources is called a data stream, which after transformation and processing is converted into a stream of information objects. An IO is a structure which contains data (from sensors), information (data) about the structure, context data (sensor, geographic coordinates and time of the notification), data about the data (metadata) - e.g. about variations of physical quantities, representation format.

For data in CIMIS, we take information from sensors that convert physical quantities - temperature, gas concentration, or radiation intensity. The context is information about how we can use this data - what quantities it reflects, what its source is. The data is transformed within the context and used as information.

The system objective of the CIMIS is to support critical CI event management decisions by providing information in an appropriate format and to different classes of users. For some of the users operating in the ICC area, the information is directly related to the performance of their functions and implies information interaction - the generation and use of real-time IO (sensor information) or objects entered into the information space by an operator. An exemplary scenario is the operation on CI elements in fire conditions and the generation of objects related to the extent and locations of the fire areas by both a UAV operator and sensors in real time. The computing resources in the ICC domain must provide information and network connectivity to users in the area locally without the need for an Internet connection. Decision support should also be available within a defined scope defined by user functions and artificial intelligence elements should also be available and accessible. This requirement follows directly from the NCE approach adopted for the construction of building ICCs.

The development of SOA in CIMIS as a network-centric environment defines how information and functionality will be shared. Shared services means that information sources and service providers make them available in the IO in a format suitable for reuse.

In SOA architectures, the integration between different applications evolves from point-to-point and applications connected to their own specific database in the pre-SOA architecture to a distinct integration and service layer. As a result of the transition to SOA, redundant functions and data are consistently reduced because all services are involved and all systems use the same data sources. The integration platform serves as an intermediate layer that provides data transformation and interaction between services from different subsystems within the UIS.

The integration platform uses an Enterprise Service Bus (ESB), which is a software framework for centralized and unified event-driven exchange of information objects between information subsystems. In a general sense, the ESB is also an element of the SOA architecture and as such is a distributed subsystem.

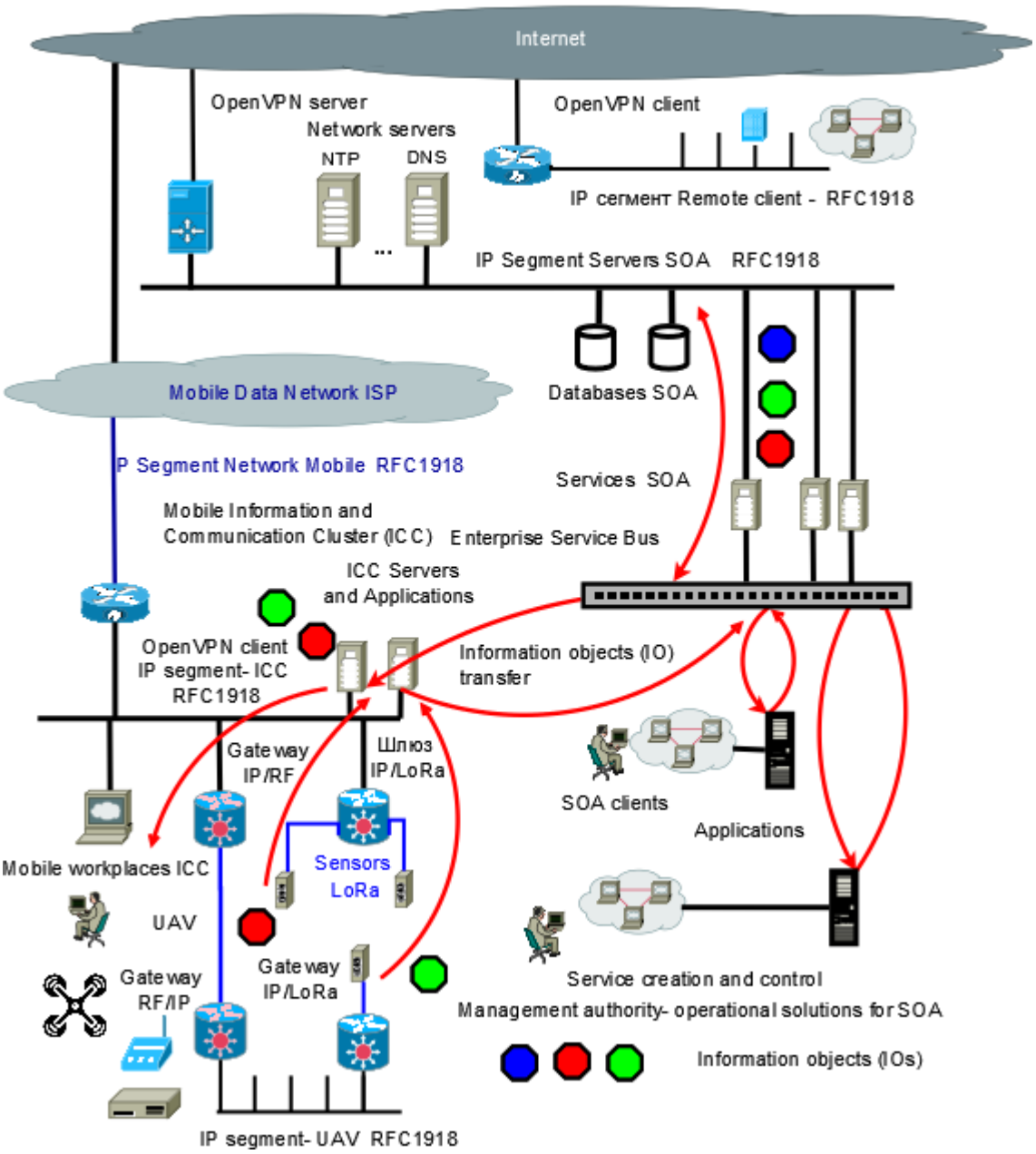

Fig. 2. Structure of CIMIS with mobile ICC and SOA for processing and representing IO flows

The Enterprise Service Bus (ESB) provides collaborative and interoperable capabilities with the following features:

- Multiprotocol. This is a solution to the problem of data exchange when different services need to exchange information using different protocols, making it easier to integrate different services into the system;
- Data transformations. Different data formats are possible within a protocol and must be transformed by the ESB for service interaction;
- Routing. This is a core part of the ESB. When something needs to be sent from one service to another, the bus provides the routing to the correct recipient;
- Routing logic, or conditional routing policy. Ensures that the routing of the message changes based on its content;
- Multiplexing. Sending the message to a list of recipients.

The UIS in the CIMIS structure provides situational awareness to decision makers in the handling and protection of CI. Based on the monitoring, IOs are created, processed and presented to create mental models for easy perception and interpretation of the results obtained in real time in the ICC. The aggregation and processing of information in SOA enables aggregated assessment with event correlation and prediction of CI protection processes. SOA's ability to create new IOs facilitates the integration of other information systems and provides the ability to develop new applications based on existing sites.

Conclusions

The structure of a mobile information system for critical infrastructure monitoring that provides a unified information space for real-time monitoring is discussed. The functions of the system include monitoring, detecting, classifying, recognizing, and tracking events related to critical infrastructure, forming and processing streams of information objects.

The communication environment is a virtual private network with IP address space and is protected by traffic encryption and certificate access. The system is implemented as a communication-information in mobile information-communication clusters and servers in the composition of a service-oriented architecture for centralized information processing.

The presence of processing and presentation information objects in the composition of each cluster provides situational awareness for field teams. The aggregation and service-oriented information processing architecture provides models for prediction and analysis. The structure provides a network-centric environment and a unified information space with reuse of information objects and procedures, and the ability to develop new applications.

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. Димитров, Н., ВВМУ “Н. Й. Вапцаров“ Системен подход към критичната инфраструктура, Варна, 2019
2. Додонов, А. Г., Д. В. Ландэ. Живучесть информационных систем. К.: Наук. думка, 2011. — 256 с.
3. Department of Defense Standard Department of Defense Trusted Computer System Evaluation Criteria December, l985 DoD 5200.28-STD Supersedes CSC-STD-00l-83, dtd l5 Aug 83 Library No. S225,7ll
4. Evaluation criteria for IT security, ISO/IEC 15408, Third edition 2009-12-15, Corrected version 2014-01-15
5. Department of Defense Net-Centric Services Strategy Strategy for a Net-Centric, Service Oriented DoD Enterprise March, 2007, Prepared by the DoD CIO
6. Net-Centric Environment Joint Functional Concept Department of Defence USA, version 1.0 2005
7. 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. Vol. 36, 2024, Sofia, pp. 131–146.