THE USE OF EARLY WARNING SYSTEMS IN MANAGING CRITICAL INFRASTRUCTURE RESILIENT ARCHITECTURES - FROM OPTION TO NEED

Assoc.Prof. PhD. Dorel BADEA,
Research assistant PhD Gabriel MĂNESCU, Florin SABĂU

„Nicolae Bălcescu" Land Forces Academy, Sibiu

Abstract:
In the context of increasing the frequency of different types of disasters or natural disasters, the idea of operationalizing early warning systems, which ultimately reduces the consequences on society in general and especially on those areas regulated as critical to the functionality and continuity of essential services to the population. Some topical directions of investigation of the subject are highlighted in the article, the main research method being conceptual modeling.

***Keywords**:* resilience, system, early warning, conceptual model, IDEF0

1. Introduction

As early as 2009, when the „Cartography and Geoinformatics for Early Warning and Emergency Management" conference was held in Prague, with the topic „Towards better solutions", the importance of early warning and crisis management systems was emphasized against the background of increased natural, humanitarian, industrial and man-made (terrorism) disasters, most of the presentations highlighting the role of implementing advanced technologies in early warning systems. The concept should be discussed in conjunction with others, integrating the Civil Emergency Areas, set out below.

Critical Infrastructure Protection (CI) generally includes any activity aimed at ensuring the functionality, continuity and integrity of the CI in order to discourage, diminish and neutralize a threat, risk or vulnerability (risk assessment and analysis, ensuring protection of classified information, implementation of security plans of critical infrastructure operators, establishment of communications, as well as exercises, reports, re-evaluations and updates of prepared documents) [1]. Clarifications are also contained in the White Paper on Defense, approved by the Parliament's Decision no. 12/2016, which lists the national defense objectives established by the National Defense Strategy of the country and strengthening the security and protection of critical infrastructures - energy, transport and cybernetics. Resilience is considered as "the ability of a system, community or society which is exposed to a type of risk to cope, adapt and recover after a disaster by maintaining and rehabilitating its core structures and functions" [2]. Article 3, paragraph (2), letter (d) of the same legislative act stipulates as a strategic objective the substantial reduction of disaster damage and disturbances on critical infrastructure and basic services, such as health and education, through developing their resilience by 2030. Reference to the CI is also made at European level, underlining that the most significant actions needed to tackle hybrid threats are: identifying vulnerabilities that may affect national and pan-European structures and networks and common instruments, including indicators, capable of improving the protection and resilience of critical infrastructure [3]. Whether it's resistance to acts of terrorism, cyber-attacks, pandemics, or catastrophic natural disasters, according to the United States Department of Homeland Security, training to combat these challenges is the "joint responsibility of all levels of government, private or nonprofit, as well as individual citizens" [4]. Last but not least, at the level of the analysis of the current state of concern in the field, it is worth pointing out that at the European level, between 9-11 May 2017, the Conference on Critical Infrastructure Protection and Resilience [5] was held in Hague, based on the fact that more and more vital systems are managed electronically, and the interdependence between physical and cyber-based systems must be thoroughly disseminated to effectively deliver services to natural disasters, terrorist attacks and criminal activity. The plan approached at the conference focused on three key elements of economic security - transport, energy and telecommunications.

The purpose of presenting these content elements is to highlight the complexity of the underlying issues and the need for the approach. There is more and more talk of a stage of 4.0-type industries that embraces high tech elements. Extrapolated, it can be said that it is imperative to include advanced technical solutions for the management of critical infrastructure resilient architectures. We take into account the fact that CIs are interdependent and cascade-related, involving specific institutions, processes and technologies, both horizontally and vertically.

The current development of society almost imperatively imposes the *spatial reality* and the specific infrastructure that orbits above us in the adjacent area of the Earth as a technology that contributes to the integration of all the layers vertically, causing overwhelmingly the performance of the management of critical infrastructure resilient architectures. Even if we are sometimes unaware, the existence of space infrastructure is of overwhelming importance in our lives, and we all depend on it to a greater or lesser extent, both in the course of industrial, security and defense activities, and in the deployment of personal activities: managing intelligent military systems fire or guiding a ballistic missile; the use of a GPS while traveling with the vehicle, either for personal use or for road transport; weather prediction; oceanography and guidance of seagoing vessels; aircraft flights; mobile telephony and telecommunications; land monitoring and mapping; monitoring of floods, landslides, vegetation fires, crops, etc. [6].

2. Creating a conceptual model to address the specific issue

An *Early Warning System* is defined as "a system by which a responsible authority announces the population or different administrative bodies where, in the near future, a negative event may occur; different communication means, such as sirens, SMS messages, radio ads are used" [7]. Some general features of such a system would be: easy to use, flexible, robust, extensible, user-friendly graphical interface and compatibility with other databases, cost-effective, regardless of the critical infrastructure sector where it will be used. The actuality of the subject is given, as it has already been mentioned, by the shortening of the reaction time, as a result of the possession of some preliminary information with a different degree of imminence, related to the possibility of an event with negative effects on the population (hurricane, tsunami, earthquake, collapse of a dam, landslide, unauthorized penetration into a strategic objective, etc.).

Very topical, along with SCADA-like systems, as a technological level at different levels of development, are those that use drones, providing timely information about the state of an infrastructure in our case by investigating some aspects of the state of the art or the existence of threats.

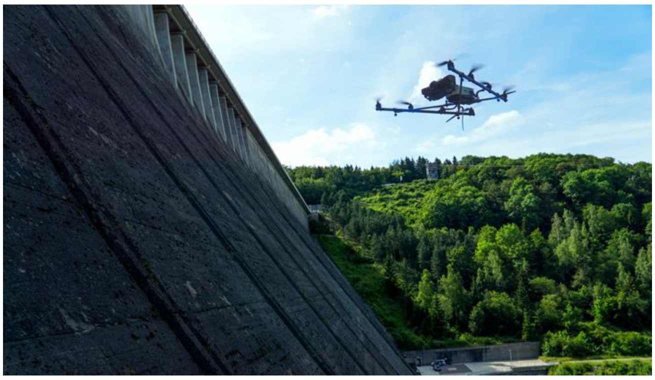


Fig.1 The use of a drone to inspect a dam [8]

The conceptual model for using such technology is presented in Figure 2.

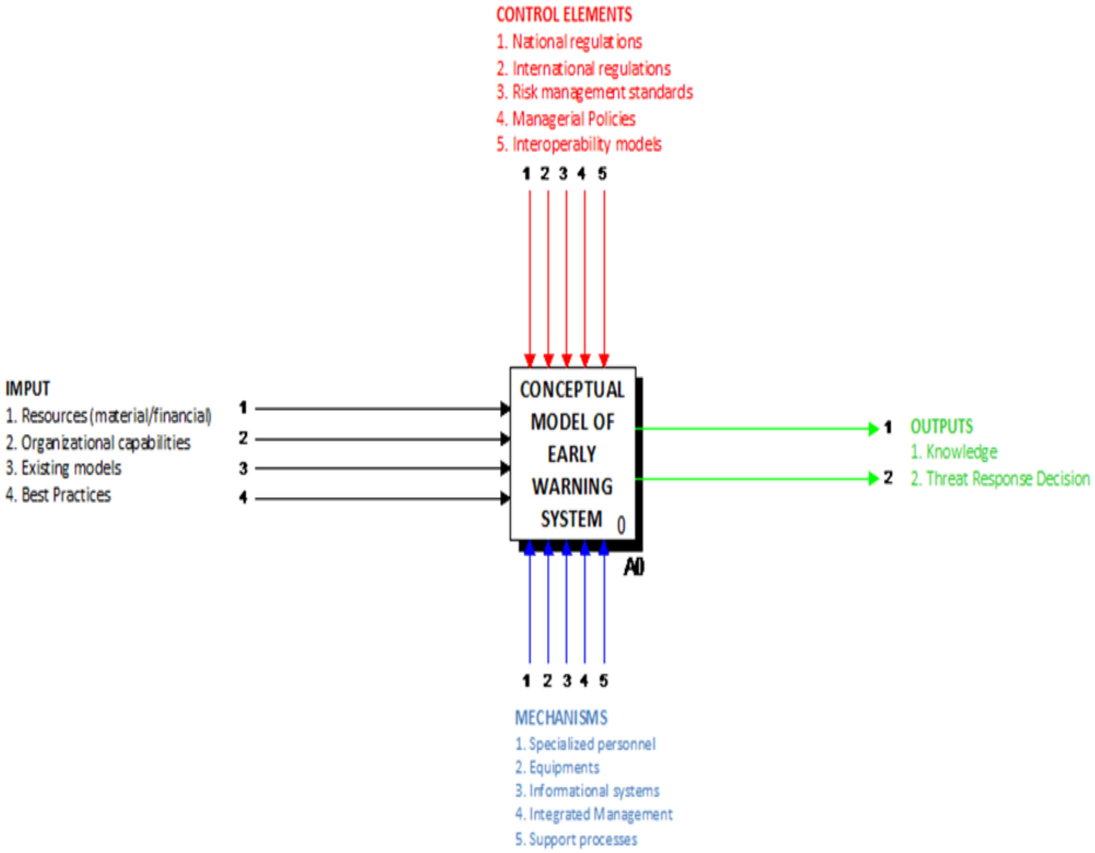
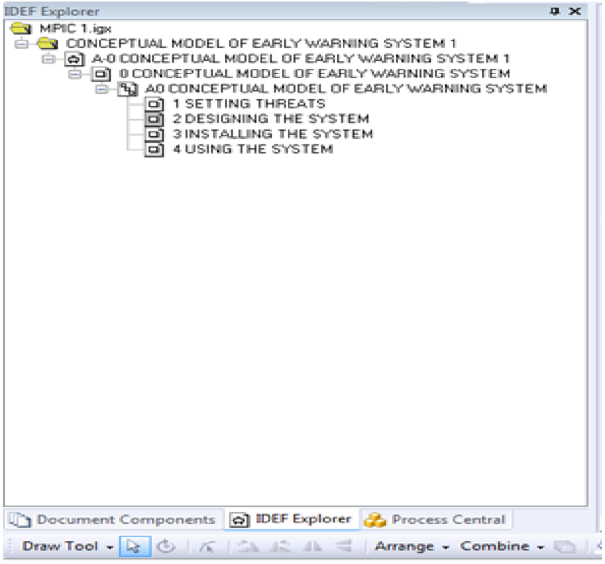


Fig. 2 Conceptual model of an early warning system

This conceptual model is made using the IDEF methodology (Integration DEFinition), a family of modeling languages in systems and software engineering. They cover a wide range of uses, from functional modeling, to data, simulation, object-oriented analysis/design, and acquisition of knowledge [9]. IDEF methods are used to model activities and processes to support the process of integrating information. IDEF methods are a set of independent methods that prove to be very useful when used on a large scale. IDEF0 (Functional Modeling Method) was designed to allow an efficient description of the system’s functions through the function decomposition process and the classification of relations between functions (in the form of inputs, outputs, control and mechanisms) [10].

In order to develop the conceptual model, iGrafx 2013 v.15.0 software was used, the menu of the application, with the main stages represented sequentially being presented in Figure 3.



IDEF Explorer

MPIC 1.igx
- CONCEPTUAL MODEL OF EARLY WARNING SYSTEM 1
  - A-0 CONCEPTUAL MODEL OF EARLY WARNING SYSTEM 1
    - 0 CONCEPTUAL MODEL OF EARLY WARNING SYSTEM
      - A0 CONCEPTUAL MODEL OF EARLY WARNING SYSTEM
        - 1 SETTING THREATS
        - 2 DESIGNING THE SYSTEM
        - 3 INSTALLING THE SYSTEM
        - 4 USING THE SYSTEM

Fig. 3 Decomposition of the model steps into the iGrafx main window

One of most important attributes of this methodology is that it allows the processes to be detached between a minimum of 3 and a maximum of 6 stages and the decomposition of each up to 3 levels. Figure 2 shows the generalized model, level 0, with all the elements that contribute to the model’s generation. For a better understanding of how the conceptual model is realized, it was decomposed into specific stages within the first decomposition level (Figure 4).

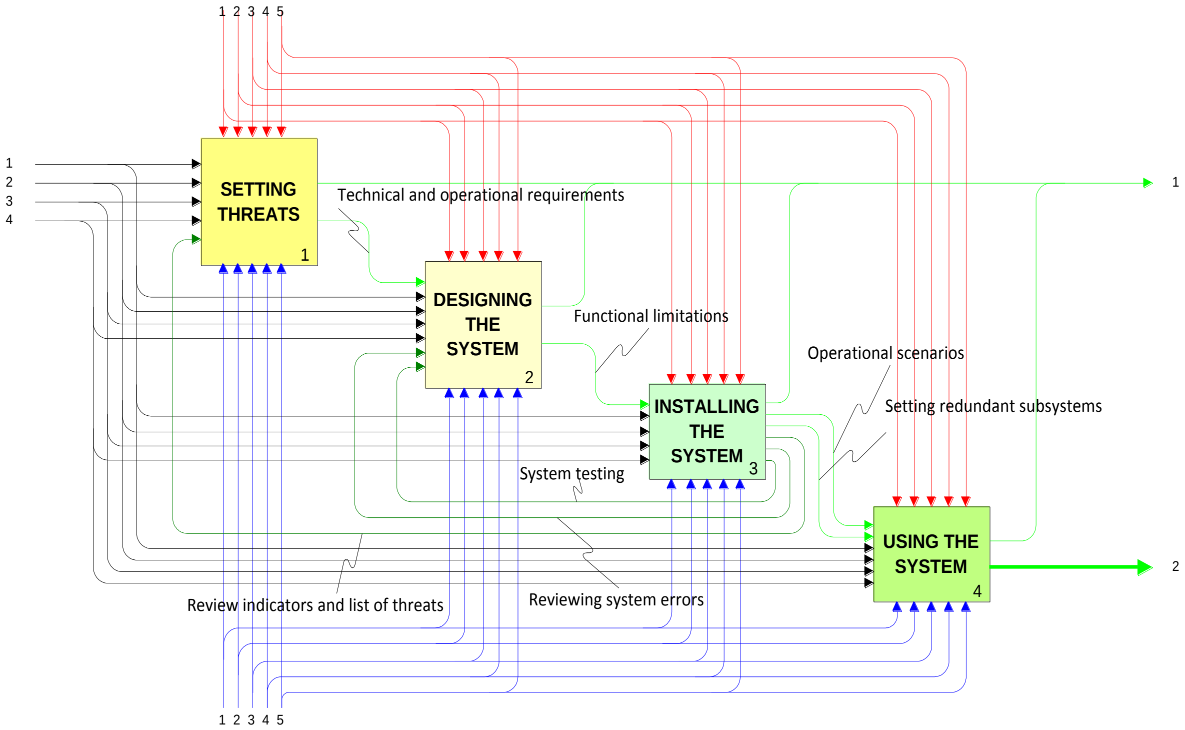


Fig. 4 The conceptual model decomposed by stages.

As it can be noticed, at this level, all stages specific to the conceptual model of the Early Warning System are presented in detail, starting from input data and generating the response to the threat under the circumstances imposed by the constraints and the mechanisms at its disposal. One very important thing is that this model allows the visualization of relationships that are established between different stages / activities and the fact that it can intervene at any time to correct or ameliorate processes or activities in order to make the best decision.

If a detailed analysis of each step/activity is necessary or desirable, these may be detailed on the following levels of decomposition but for what we have proposed in this paper we consider that it is sufficient to present the model on this first level of decomposition.

3. Conclusions

We believe that the conceptual model presented may be a starting point for defining the attributes specific to an early warning system, and that such an approach can be deepened and / or developed by undertaking the following actions:

- interdisciplinary analysis of security dimensions to highlight potential risk under current conditions;
- multidimensional (national-international, civil-military) exploratory research on addressing early warning for risk situations;
- systemic, technical and operational study of the possibilities to ensure flexibility (update and upgrade) of a complex early warning methodology;
- creating an initial database with reconfigurable multi-attribute characteristics for different areas of national security;
- establishing a set of indicators for comprehensive vulnerability analysis on a territory of interest and primary verification as a tool for assessing the level of intervention urgency in a relevant case study;
- analyzing the possibilities of implementing advanced technologies in the early warning systems architecture - demonstrating the necessity and relevance of drone-based systems;
- developing a conceptual integrating model (e.g., UML) for early warning, for national and regional use, testing and validation;
- the materialization of a course support *Early warning for risk situations* usable for different academic disciplines specific to the curricula at the level of the institutions in the field of defense, security, public order and national security, but also for the awareness of the civil population.

References:

[1] The Government of Romania. *Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructure,* Art. 3, point c), Official Gazette of Romania no. 757/12.11. 2010.

[2] The Government of Romania. *GD no. 768/2016 on the organization and functioning of the National Disaster Risk Reduction Platform*, Official Gazette of Romania no. 852/26.10.2016.

[3] Chamber of Deputies. *Decision no. 85/2016 on the adoption of the opinion on the Joint Communication to the European Parliament and the Council - Common Framework for*

Combating Hybrid Threats - A response by the European Union JOIN (2016) 18, Official Gazette of Romania no.771/27.09.2016.

[4] Homeland Security. *Resilience*, available at: https://www.dhs.gov/topic/resilience

[5] United Nations Office for Disaster Risk Reduction, *Critical Infrastructure Protection and Resilience Europe 2017*, available at: https://www.unisdr.org/we/inform/events/52040

[6] Coman, M., *Vulnerabilități și riscuri ale spațiului - infrastructură critică în era globalizării,* in Boşcoianu, M., Badea, D., (coord), *Managementul situaţiilor de risc în contextul crizelor de securitate,* Editura Academiei Forţelor Terestre „Nicolae Bălcescu", Sibiu, 2017. pp. 226-248.

[7] N-WatchWiki. *Sistem de avertizare timpurie*, available at: http://nwatchwiki.aii.pub.ro/tiki-index.php?page=Sistem+avertizare+timpurie

[8] Ascending Technologies. *UAV inspection & survey of Germany's highest dam*, available at: http://www.asctec.de/en/uav-inspection-survey-of-germanys-highest-dam/

[9] Air Force Wright Aeronautical Laboratories, Materials Laboratory, ICAM Architecture, Part II-Volume IV - Function Modeling Manual (IDEF0), *AFWAL-TR-81-4023,* Air Force Systems Command, Wright-Patterson Air Force Base, Ohio, 1981.

[10]. Mănescu, G. *Cercetări privind realizarea unui model colaborativ al cercetării ştiinţifice în instituţiile din domeniul apărării,* 2015, Teză de doctorat, Universitatea „Lucian Blaga" din Sibiu.