A Computer System for CBRN Contamination Threats Analysis Support, Prediction Their Effects and Alarming the Population: Polish Case Study

Zbigniew Tarapata[1,a], Ryszard Antkiewicz[1], Mariusz Chmielewski[1], Michał Dyk[1], Rafał Kasprzyk[1], Wojciech Kulas[1], Andrzej Najgebauer[1], Dariusz Pierzchała[1], Jarosław Rulka[1]

[1] *Institute of Computer and Information Systems, Faculty of Cybernetics, Military University of Technology, Warsaw, Poland*

Abstract. The article outlines a concept for the system supporting analyses of threats related to contamination and alarming (WAZkA), for the purpose of the National System for Detection of Contamination and Alarming (Krajowy System Wykrywania Skażeń i Alarmowania, KSWSiA) in Poland. Additionally, the article presents the point of designing such system, its concept and components. The main objective of WAZkA is to support the following processes of the KSWSiA: information exchange between the system elements and coordination of the system operations, as well as to prepare assessment and expert analyses, needed by the decision-making bodies, with respect to risk emergency situations during natural disasters, technical failures or other events resulting in biological, chemical or radioactive contamination. The selected modules included in the WAZkA system: Event Tree Analyzer, visualization module (COP) and emulators of the threats monitoring systems, were described as well as the idea of using the system for the purpose of training, including the designed emulators of the risk monitoring systems together with the scenario editor. The Event Tree Anlyzer is a graphical representation of a chronological sequence of events, significant from the point of view of the functioning of the object, which occur after a given event that initiates such sequence. COP is the GIS tool, which allows to present an operating situation on the basis of background maps. The application offers a possibility of enriching the presented operating situation with the risk data provided in the form of NATO ADat-P3 (CBRN) reports. Emulators of the threats monitoring systems allow to generate, in an artificial and user-controlled manner, data on risks, which "pretend" to be real data obtained from the monitoring systems. The above approach significantly facilitates the organization of training and learning about rare situations or situations that have never occurred, but that are potentially dangerous.

1 Introduction and Motivation

Pursuant to appropriate provisions of law [11], the National System for Detection of Contamination and Alarming (Krajowy System Wykrywania Skażeń i Alarmowania, KSWSiA) was established in Poland. The main elements of KSWSiA are functional subsystems intended for detecting the CBRN (Chemical, Biological, Radiological, Nuclear) contamination and alarming about it organizational bodies and units, which analyze the contamination and evaluate the situation to later develop, announce and introduce intervention measures. The functional systems, which constitute the system core, are the following: The System of Contamination Detection of the Armed Forces of the Republic of Poland - supervised by the Minister of National Defense, networks and systems for the epidemiological surveillance and control of communicable diseases in the country as well as national contact points for the international surveillance system to identify threats to human health and life of large populations - supervised by the Minister of Health, systems of early detection of radioactive contamination and radioactive contamination centers, whose activities are coordinated by the President of the National Atomic Energy Agency, voivodeship early detection systems supervised by Voivodes [13], systems for epizootic and phytosanitary surveillance, supervision of safety of animal products and animal feeding stuffs, supervision of safety of agro-food products controlled by the competent Ministers of Agriculture and Agricultural Markets. The Central Contamination Analysis Center (COAS) in Warsaw acts as the KSWSiA coordinator.

The above-mentioned entities included in the composition of KSWSiA use various sources of contamination data and data processing systems. However, there is no system that would integrate all data from different sources (i.e. threat monitoring systems, TMS), allow information exchange between KSWSiA system elements and support the decision-making bodies in performing the following actions: (a) assessment and expert analyses concerning the contamination risks and (b) warning and alarming the population about such risks.

[a] Corresponding author: zbigniew.tarapata@wat.edu.pl

Therefore, the article presents a concept of the system supporting analyses of threats related to contamination and alarming (WAZkA). The presented concept falls within the scope of topics of the R&D project entitled: "Integration and support of the information management processes as well as optimization of decisions of the detection and alarming system" realized under the contest of the National R&D Center BiO 7/2015 by the scientific and industrial consortium composed of: Military University of Technology in Warsaw – leader, HTRC sp. z o.o., Central State Fire Service School in Częstochowa, Cardinal Stefan Wyszyński University in Warsaw.

The main objective of WAZkA [14] is to develop and construct a highly developed ICT tool, needed by the entities of KSWSiA, which shall support the following processes: information exchange between the system elements and coordination of the system operations, as well as to prepare assessment and expert analyses, needed by the decision-making bodies, with respect to risk emergency situations during natural disasters, technical failures or other events resulting in biological, chemical or radioactive contamination.

The individual objectives are the following:

1. Development of the risk identification methodology, also with respect to international risks, including the risk assessment process in terms of risk occurrence and prioritization.
2. Development of rules for assessment of susceptibility of a given area to certain risks, including risk maps and threat maps.
3. Development of rules for collecting data from the risk monitoring systems.
4. Development of the module for collecting data by the ICT system and warnings saved by the monitoring systems.
5. Development of the module allowing to use the Regional Warning System and other systems for alarming regional population.
6. Design and implementation of a modern ICT system responsible for exchanging information on threats, preparing assessment and performing analyses of undesired events, coordinating actions, modeling scenarios, including identification of their risks, sending information to the people via available warning systems and carrying out preparatory exercises.
7. Development of the training schedule for public administration units, which use products that were created under the project, and development of the system of exercises.
8. Preparation of recommended legislative amendments to improve the functioning of the system for contamination detection and alarming.
9. Current dissemination of the project results.

The paper is organized as follows. In section 2 we present short review of threats monitoring systems, warning and alarm systems in Poland. Section 3 contains the concept of system WAZkA. In section 4 we describe a set of tools for threats analysis, visualization and training in WAZkA.

2 Threats monitoring, warning and alarm systems in Poland

The systems for the monitoring of radiological risks are supervised by the National Atomic Energy Agency. The above-mentioned systems include: PMS (Permanent Monitoring System) stations [8], ASS-500 stations [4], [8], stations of the Institute of Meteorology and Water Management, stations of the Automated Network of Radioactive Contamination Measurements (SAPOS), which belong to the military, and the System of Contamination Detection of the Armed Forces of the Republic of Poland. Furthermore, the following entities are responsible for the contamination monitoring: Provincial Sanitary-Epidemiological Stations, HACCP system, National Health Inspectorate, etc.

Regional Warning System (RSO) [16] is a service used to inform the citizens on upcoming dangers; it has been operational since 1 January 2015. The messages transmitted by the system mainly focused on meteorological warnings (e.g. strong winds, thunderstorms, icing), hydrological warnings (e.g. water levels), traffic information (e.g. traffic jams, construction works, detours), and other information relevant from a safety standpoint. Regional Warning System Messages can be seen in Polish Television programs in digital terrestrial multiplex MUX-3. The most important of them appear on a special news bar on the TV screen. All messages are also available on teletext pages in programs TVP1, TVP 2, TVP Kultura, TVP Historia and TVP Polonia from p. 190, while in the Regional TVP from p. 430. The same warnings will also appear on the websites of voivodeship (provincial) offices. Smartphone users can use a free application for mobile phones, available at shops with applications for the individual platforms (Google Play, Apple App Store, Windows Phone Store). The application may be searched for using key words “RSO” and “Regional Warning System”.

The digitexCZK/IP® system [17] has been created on the basis of on up-to-date technologies, according to a PLATAN construction team’s original design. This is the only one in Poland warning system which for data transmission uses not only analogue but also digital radio communication in the DMR (TDMA) and NXDN (FDMA) standards, as well as local area and wide area networks (LAN, WAN) and encoded IP. In the digitexCZK/IP® system, use of IP for data and voice transmission makes it possible to create and expand the system easily and it allows for integration with the existing analogue warning systems, i.e.: digitexCZK/ FSK, DSP-50, RSSS-2000/3000, MDSA-24.

These systems use different data formats: ATP-45(d) [2], NATO ADatP-3 (eg. CBRN report), CAP (Common Alerting Protocol), IRIX 1.0, EURDEP 2.1 (UE standard), others, including non-structural (simple e-mail, fax).

3 The concept of WAZkA system

The most important expected final result of the project implementation shall be the WAZkA system

demonstrator (the system supporting analyses of threats related to contamination and alarming). Figure 1 presents the WAZkA system concept. WAZkA means in polish language - the dragonfly. The dragonfly is considered a silent killer among insects - like a CBRN contamination.

The WAZkA system consists of the following modules [14]:

• Integration Module IM1 - responsible for the communication, transfer and initial processing of data from the current TMS. The data shall be obtained in an automated manner from the systems and entities having IT systems to process the risk-related information. For the purpose of other entities, an interface for semi-automatic and manual data supplementation shall be launched (e.g. serial mail dispatch);

• Integration Module IM2 - responsible for the integration with the existing detection and warning systems. The risk alerts from the WAZkA system are set through the above-mentioned module;

• Data Acquisition & Analysis Module DAAM - central module of the system responsible for the analysis of data obtained from the monitoring systems (via IM1). On the basis thereof, an assessment, arrangement in hierarchy and forecast of the risk development are made. In case of occurrence of such risks, an alert is sent to the detection and alarming systems (via IM2);

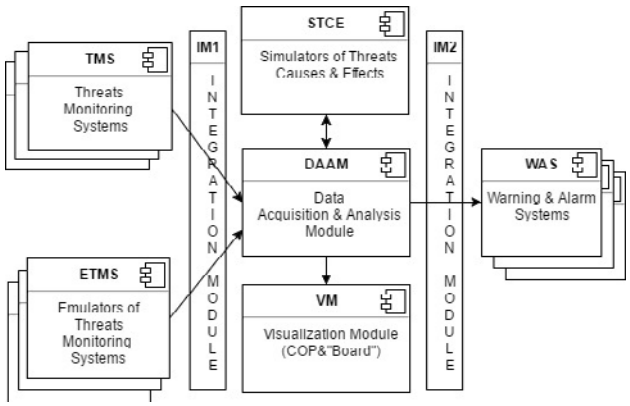

Figure 1. The idea of WAZkA system.

• Visualization Modules (VM) - responsible for the presentation of data and results of analyses (in particular - warnings about the risks), as needed by the KSWSiA entities. Two VMs are proposed:

o Board - a web portal, which facilitates quick access to the most recent information and the most serious risks. It shall be the central communication point between the KSWSiA entities. Access to the presented information shall be filtered depending on the privileges of the logged user.

o Common Operational Picture (COP) - similarly to the Board module, the COP shall be accessed via Internet. It shall present the information about the risks on a digital map.

• Simulators of Threats Causes and Effects STCE - the simulators shall support the DAAM module. They allow to simulate the processes of occurrence and development of risks, thanks to which it shall be possible to generate warning and prepare appropriate measures in advance. The simulators also allow to play different variants of the risk development scenarios, which shall contribute to faster and less risky decision-making process with respect to risk elimination. We also use existing simulators: Aloha [18] (the hazard modeling program, which is used widely to plan for and respond to chemical emergencies) and SI Promien [9].

• Emulators of the Threats Monitoring Systems (ETMS) allow to generate, in an artificial and user-controlled manner, data on risks, which "pretend" to be real data obtained from the monitoring systems. The above approach significantly facilitates the organization of training and learning about rare situations or situations that have never occurred, but that are potentially dangerous.

Practical use of the project results as regards national defense and security shall be in the form of the implementation of the WAZkA results at appropriate institutions responsible for contamination monitoring as well as warning and alarming of the population. Social benefits resulting therefrom may be compared to the implementation of, for example, the Regional Warning System, with which the WAZkA system shall naturally cooperate. The system built under this project shall allow collaboration with the military systems with similar functionalities, but shall be dedicated to civil services, in particular entities included in the National Firefighting and Rescue System under the responsibility of the State Fire Service. Therefore, the following entities may be included in the group of potential system recipients:

- Head of the National Civil Defense/Chief Commander Brigadier of the State Fire Service;
- entities subordinate to and supervised by the Minister of Interior (Emergency Management Department of the Ministry of Interior, National Police Headquarters, State Fire Service HQ, Border Guard HQ);
- voivodes (voivodeship emergency management center - especially, in terms of increasing the ability to inform civilians);
- other non-military components of KSWSiA (Radiological Incident Center "CEZAR" PAA, Central Meteorological Forecast Bureau - Institute of Meteorology and Water Management, Research Institute of the Ministry of Transport, Ministry of Agriculture and Rural Development, Ministry of Health, Ministry of Administration and Digitization, Chief Inspectorate for Veterinary and Heads of Maritime Offices).

4 A set of selected tools for threats analysis, visualization and training in WAZkA

4.1 Event Tree Analyser (ETA)

The Event Tree is a graphical representation of a chronological sequence of events, significant from the point of view of the functioning of the object, which occur after a given event that initiates such sequence (Figure 2, Figure 3, Figure 4). This is one of the forms of

the decision trees (e.g. stochastic PERT [1]). It can be used during e.g. planning of hazardous materials transport [12, sect. 3, sect. 6] for risk analysis.
Event tree [10] allows:

- Determination of probability of the occurrence of a given scenario of events;
- Assessment of the final event consequences;
- Calculation of frequency of the occurrence of particular event scenarios;
- Modification of the Event Tree characteristics in case of the occurrence of specific events.

Figure 2 presents an example of the event tree created in the Event Tree Analyser application. The tree consists of the initial element (black circle), events (rectangles with the names recorded inside), final elements, i.e. the effects (white circles) and curves joining the tree elements. Two curves described by the probability are always derived from every event. One of them determines consequences of the fact that the event occurred, whereas the other one - that the event did not occur.
The presented example describes development and consequences of the loss of integrity of a ammonia container. At the beginning, it is considered whether the bottom of the container lost integrity. If so (probability 0.99), the ammonia pool will be created, otherwise (probability 0.01) - the pool will not be created. Then, a possibility of immediate explosion or delayed ignition is considered. The above may happen on two paths of the risk development, but with high probability thereof. On the basis of the probability of occurrence and non-occurrence of certain events, the probability of occurrence of particular effects of the lost integrity is determined. In the analyzed case, three types of effects are possible, i.e. immediate explosion, explosion and chemical contamination. Together with the risk development, certain events may become more probable and some - completely improbable. In such case, the probability of occurrence of specific risk effects is also changing.
The Event Tree Analyser application allows to determine which of the events has actually occurred and to automatically calculate the probabilities. Figure 3 presents an example of such situation. The event "no pool formed" was checked, which means that the bottom of the container did not lose its integrity, thus, the events on an alternative paths become improbable, whereas the probability of occurrence of the events on the checked path significantly increases. For example, the probability of delayed ignition increased from 0.09 to 0.90. The increase was substantial - i.e. by two orders of magnitude. The probability of occurrence of every risk effect also increased, since the bottom part of the container was not damaged and no pool was formed. Figure 4 shows recalculated Event Tree from Figure 2 with situation after “Delayed ignition” event done.
The presented application constitutes an alternative to the solutions similar to the tree event analysis, e.g. Logan [15]. However, a significant difference is that the Event Tree Analyser application does not require the necessity to build complementary event in every case, even though it provides for such a possibility.

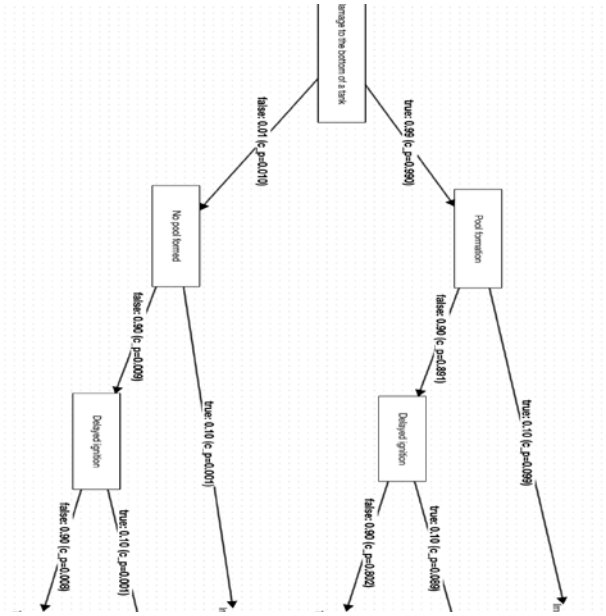

Figure 2. Event Tree with some initial situations.

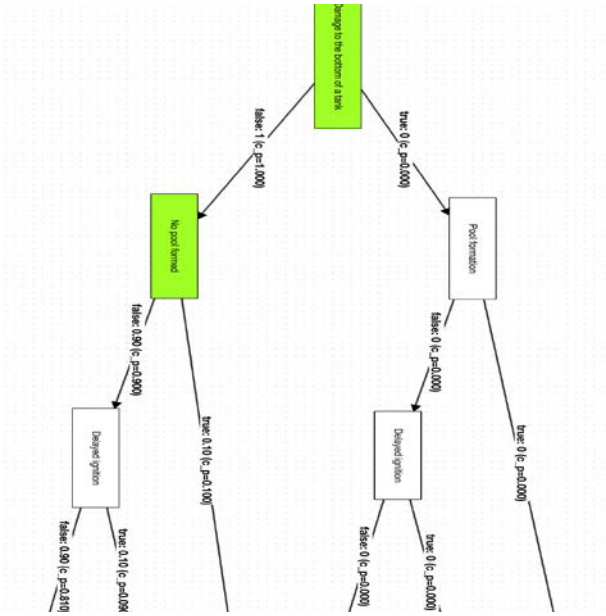

Figure 3. Recalculated Event Tree from Figure 2 with situation after “No pool formed” event done.

It allows to avoid certain artificial aspects in the constructed trees. Additionally, apart from determining the probability of occurrence of the effects, the probability of occurrence of each of the indirect events is also measured provided that predecessor of such events occurred. The following examples show the value in brackets, recorded on curves between the events.
Event Tree Analyser is the application built in the client-server architecture, which does not need any additional software to be installed by the user outside a web browser.

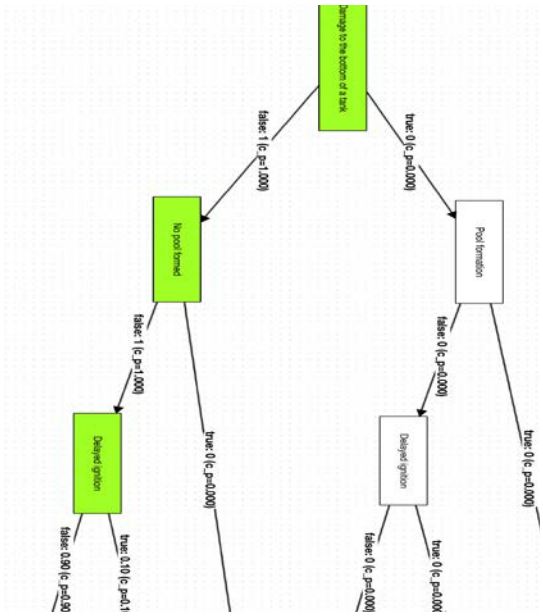

Figure 4. Recalculated Event Tree from Figure 2 with situation after "Delayed ignition" event done.

4.2 Common Operational Picture (COP)

It is the GIS tool, which allows to present an operating situation on the basis of background maps. The application offers a possibility of enriching the presented operating situation with the risk data provided in the form of NATO ADat-P3 (CBRN) reports. The map module allows to perform map measurements of the indicated routes and areas as well as provides special functions supporting the decision-making process by defining flood zones and terrain profiles (Figure 6). The map module allows to present the objects within geographical space, in accordance with the symbols of NATO APP-6A and Ministry of the Interior and Administration. When applying this property, it is possible to reflect the operating situations of military units and supporting forces (fire service, police, border guards, etc.) with respect to the emergency infrastructure elements.

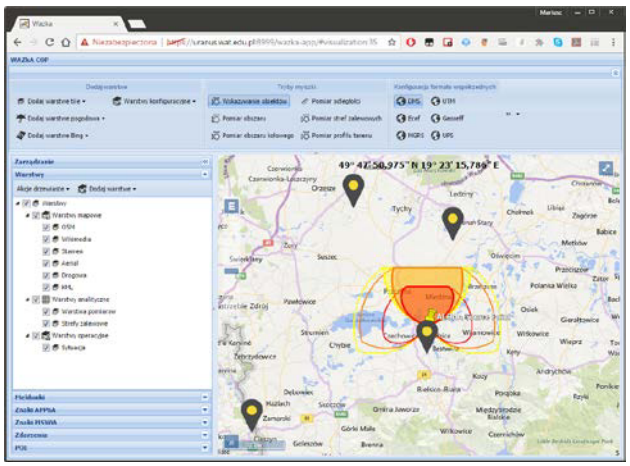

Figure 5. COP visualization for simulated CBRN threat (Chemical).

An important function for building an image of the executed operation (reaction to risk) is to manage the information about such risk. The risk data may be entered with the use of the dedicated data format system - WAZkA - or CBRN standard ADatP3 reports (Figure 5). The use of the map mechanisms of the OpenLayers component allowed to integrate many sources of the provided mapping data.

The COP visualization is provided in the form of a state application (communicating asynchronously with the data feeding services), created in Sencha GXT technology, supported by the Spring framework from services perspective. COP is delivered as 2 services: the first one is responsible for creating and feeding with data of the analyzed risk scenario, while the second one is responsible for generating visualization of a given scenario on the map, with the set geographic projection parameters.

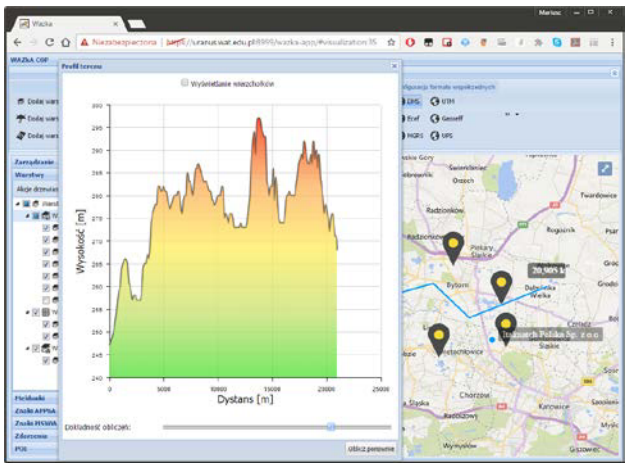

Figure 6. Terrain profile for the path defined in COP.

COP uses a possibility of visualizing any WMS (Web Map Service), allowing to enrich the operation area with satellite data, analytical maps, terrain elevation models and other analytical data related to, for example, weather information. Additional application mechanisms provide map calculation tools, which determine the lengths of the user-defined routes, fields of marked areas, terrain elevation profiles and flood zones (Figure 7). The functions supporting the decision-making process in the form of additional configurable GIS layers may be applied to the analyzed risk data, which significantly facilitates the analysis of an examined emergency situation.

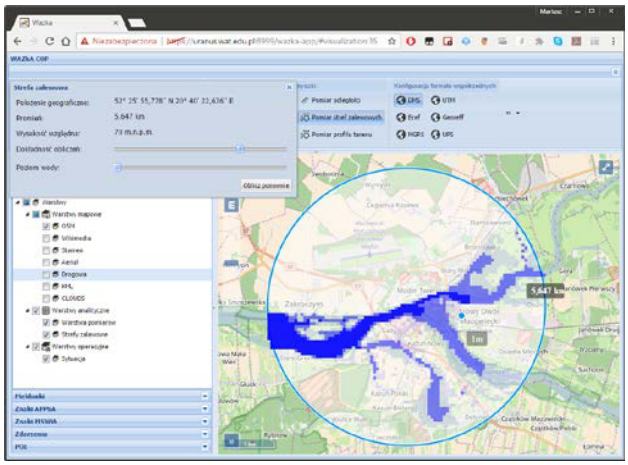

Figure 7. Flood area in defined region merged with detailed OpenStreetMap data layer fused in COP.

The COP tool provides services in the form of RESTful API and handles data serialization, in both XML and JSON formats. The tool has been equipped with additional applications supporting the manual configuration of requests to establish the scenario data and map application configuration, which additionally allows to use COP as a component of other web pages as well as automatic functional application.

4.3 Emulators of Threats Monitoring Systems (ETMS)

One of the goals of the designed WAZkA system is to use it for the purpose of training. To accomplish this goal, it is necessary to develop an artificial working environment of the system. It is aimed at providing the most exact recreation of the environment, preferably at such level of fidelity so that the trainees get the impression that they work in an actual environment. To reflect the data provider systems (in this case, the Threats Monitoring Systems), it was suggested to use the emulators (ETMS in Figure 1), i.e. the tools launched in environment other than the actual systems, aimed at providing data in the same way as real environments do.

The emulators were proposed as purely IT tool, launched in the same or identical hardware environment as the designed WAZkA system. The constructive simulation method, reduced to a simple determine data provider, in accordance with the predefined scenario, was selected as the emulation method.

Originally, the emulators should have been integrated with the whole system in the same manner as the actual systems. Thanks to that, they were supposed to be "transparent" for other system modules. Therefore, the emulators constitute an independent subsystem using the typical interfaced of the designed WAZkA system.

The above assumptions and general concept of the solution is presented in Figure 8. The requirements for the subsystem of emulators result from the requirements for the whole system. They were developed in the form of use cases.

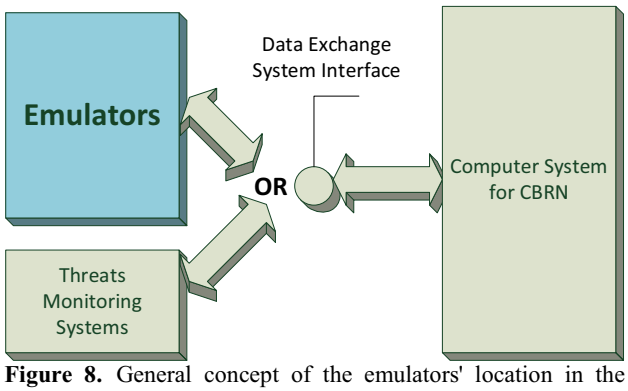

Figure 8. General concept of the emulators' location in the system *WAZkA*, *Source: own elaboration*

Emulation of the monitoring systems should be a function available to all users in the capacity of the *Emulator Operators*. Such users may influence the emulation process by controlling the simulation process for the purpose of emulation and by developing specific emulation scenarios (in this case - simulation scenarios). The process of emulation uses a typical function of the system known as the *Information Exchange*, which is aimed at integrating the whole system with the actual environment. On the other hand, the *Emulation of the Monitoring Systems* is an element of the use case - *Training*, which constitutes the function of the entire system.

During the analysis of the emulation requirements, six functional areas have been distinguished:

- Authorization;
- Emulation startup;
- Read of emulation parameters;
- Change of emulation parameters;
- Stopping emulation;
- Building of the scenario.

Each of the above areas has been specified by describing a dialog of the environment with the subsystem of emulators. Sample requirements for the manner of initiating the emulation process are presented in Table 1.

Table 1. Description of the project requirement with respect to the manner of initiating the emulation process, *Source: own elaboration.*

Emulator Operator	Emulation of the Monitoring Systems	Information Exchange
indication of the system for emulation	change of emulation parameters	
indication of the emulation scenario (sequence of events)	verification of emulation parameters (positive)	
instructions on initiating emulation at a given moment from the time of an indicated event	provision of data for emulation (correct data)	access to the system monitoring channel
	initiation of emulation at a given moment from the time of an	receipt and processing of data from

Emulator Operator	Emulation of the Monitoring Systems	Information Exchange
	indicated event; calling the interpretation service of the set type event and set parameters; sending messages to the system monitoring channel,	emulator;
	access to data of the emulation status	

The specification of functionalities, whose fragment was presented above, was developed on the basis of desired characteristics of the designed system, within the scope of the training requirements. The description in the form of interaction between the environment and emulation subsystem allowed to build a dynamic software model and hence generate the prototype template. The outline of the dynamic software mode, performed on the basis of the above table, is presented in Figure 9.

The software model developed in such a manner, executed for all functional areas and interaction variants, allowed to created the software static model, which in turn constituted grounds for generating the prototype template. After supplementing the implementation, the emulation subsystem prototype was created. The prototype form to use the above-mentioned functionality is presented in Figure 10.

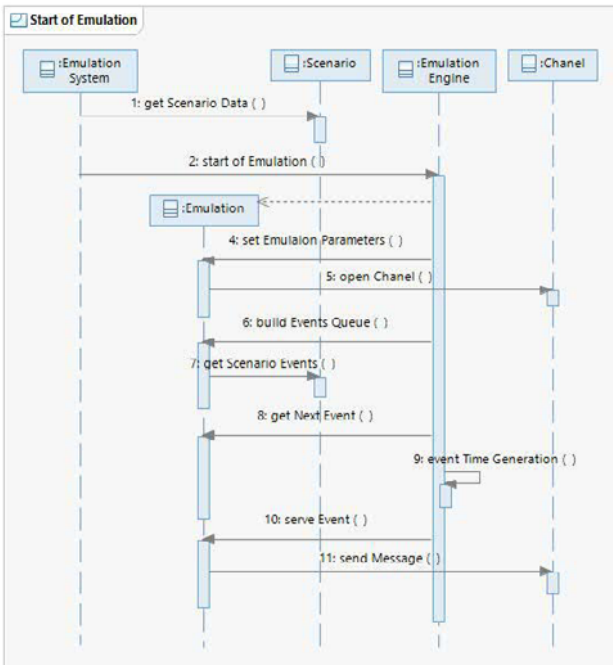

Figure 9. Diagram of the functional area sequence *Initiation of the emulation process, Source: own elaboration*

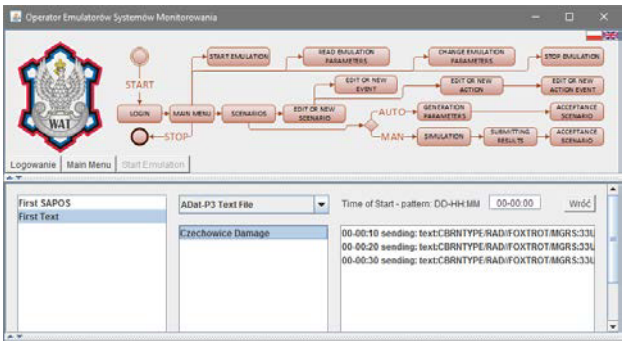

Figure 10. Activation screen for the emulation subsystem prototype, *Source: own elaboration*

5 Conclusions

The article outlined the concept of the system supporting analyses of threats related to contamination and alarming (WAZkA) for the purpose of the National System for Detection of Contamination and Alarming in Poland. Some of the selected software tools created for the WAZkA system were described.

One of the key elements for the project success is identification of the processes implemented under the National System for Detection of Contamination and Alarming, which require support by the IT services (program applications). One of the way to do it is using some approaches e.g. described in [5], [6], [7]. The main assumption is integration of KSWSiA with the existing systems (risk monitoring, warning and alarming). Furthermore, some of the KSWSiA entities are convinced that the designed system shall support the operations of KSWSiA and not replace the well-functioning areas. Therefore, numerous consultations are underway with the KSWSiA entities, in particular with the Central Contamination Analysis Center, which is at the same time the Administrative Center of KSWSiA, and State Fire Service Headquarters - the project owner.

A serious and difficult problem is to obtain access to the sources of data from the existing risk monitoring systems, managed by various institutions (IMGW, GIS, GIOŚ, RCB, PAA, etc). Additionally, the quality of the collected data shall determine the usability of the IT system and adequacy of the developed analyses and decisions. It is also worth noticing that due to the implementation of the project, new legislative and organizational solutions shall be indicated, which allow to reduce the time - from the moment of obtaining the information on an event to the time of undertaking appropriate actions by the KSWSiA entities (including, above all, the actions related to alarming and warning population), which may be an innovative solution within the European Union.

Acknowledgments

This work was partially supported by grant N^{oo} DOB-BIO7/12/01/2015 of Polish National Center for Research and Development (NCBiR) titled „Integration and support of information management processes and decision optimization in warning and alarm system”.

References

1. R. Antkiewicz, A. Gąsecki, A. Najgebauer, D. Pierzchała, Z. Tarapata, Stochastic PERT and CAST Logic Approach for Computer Support of Complex Operation Planning, *ASMTA'2010,* Lecture Notes in Computer Science, **6148**, Springer-Verlag Berlin Heidelberg, 159-173 (2010)
2. *ATP-45(d): Warning and reporting and hazard prediction of chemical, biological, radiological and nuclear incidents (operators manual)*, NATO unclassified (2010)
3. T. Binek, J. Czepiel, The National System of Contamination Detection and Alarm, Currently Operating in Poland, BiTP Vol. **36** Issue **4**, pp. 15-24 (2014)
4. D. Grabowski, W. Kurowski, W. Muszynski, B. Rubel, G. Smagala, J. Swietochowska, Radiation monitoring network in Poland, Nukleonika, **46(4)**: pp.147–149, (2001)
5. M. Kiedrowicz, J. Stanik, Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity, (in:) *Information Management in Practice*, (eds) B.F. Kubiak and J. Maślankowski, pp. 231-249, (2015)
6. M. Kiedrowicz, Location with the use of the RFID and GPS technologies - opportunities and threats, *Proceedings of the Geographic Information Systems Conference and Exhibition, GIS ODYSSEY 2016*, pp.122-128 (2016)
7. M. Kiedrowicz, Objects identification in the informations models used by information systems, *Proceedings of the Geographic Information Systems Conference and Exhibition, GIS ODYSSEY 2016*, pp. 129-136, (2016)
8. P. Lipiński, P. , K. Isajenko, M. Biernacka, A. Żak, Integration of Polish Monitoring Networks (ASS-500 and PMS systems), Nukleonica, vol. **46(4)**: pp. 143–146 (2001)
9. M. Mlynarczyk, P. Maciejewski, M. Szerszen, CBRN Analysis and SI Promień – Comparison of the Functionality of the Software for the Assessment of Contamination, BiTP Vol. **40** Issue **4**, pp. 133-138 (2015)
10. M.E. Pate-Cornell, Fault Trees vs. Event Trees in Reliability Analysis, Risk Analysis, Vol. **4**, Issue **3**, pp. 177–186 (1984)
11. *Regulation of the Council of Minister of October 16, 2006 on the contamination detection systems and level of competence of appropriate bodies* (Journal of Laws [DzU] of 2006 No. 191, item 1415), (2006)
12. Z. Tarapata, *Models and algorithms for knowledge-based decision support and simulation in defense and transport applications*, ISBN 978-83-62954-15-5, Military University of Technology in Warsaw (2011)
13. *Act of April 26, 2007 Journal of Laws [DzU], No. 89, item 590, as amended, and Regulation of the Council of Ministers of June 25 on the detailed scope of activities of the Head of the National Civil Defense, heads of civil defense of voivodeships, poviats and communes*, Journal of Laws [DzU] No. 96, item 850, (2007)
14. http://wazka.wat.edu.pl (2017)
15. http://loganfta.com (2017)
16. https://www.premier.gov.pl/en/news/news/a-promise-from-expose-kept-regional-warning-system-rso-is-fully-operational.html
17. https://www.publicalerting.com/products/public-warning-system/advantages-of-digitexczkip/
18. https://www.epa.gov/cameo/aloha-software