DE GRUYTER OPEN
Foundations of Management, Vol. 7 (2015), ISSN 2080-7279
DOI: 10.1515/fman-2015-0032

DYNAMIC HAZARDS IN CRITICAL INFRASTRUCTURE OF STATE

Teresa OSTROWSKA*, Tadeusz KRUPA**, Michał WIŚNIEWSKI***

Warsaw University of Technology, Faculty of Management
*e-mail: t.ostrowska@wz.pw.edu.pl
**e-mail: t.krupa@wz.pw.edu.pl
***e-mail: m.wisniewski@wz.pw.edu.pl

Abstract: The authors are interested in some aspects of a development project entitled "*The methodology of risk assessment for the purposes of crisis management system RP (ID 193751)"*. The project funded by the National Research and Development Centre under the Competition 3/2012 (security and defense). As part of the project the following items were reviewed and analyzed: materials related to the Government Security Centre, already completed and available products of the project ID 193751, and literature relating to, among other things, crisis management, critical infrastructure, business continuity, security, and threats. The basic emphasis of the article is focused on the resource-critical infrastructure interpretation of the state, whereby the state is perceived as a complex administrative structure in which, on the basis of external and internal interactions of resources, the risk of threats measurement is done.

Keywords: critical infrastructure, resource, risk assessment, crisis management.

1 Introduction

The material analysis carried out during the work on the project[1] ID 193751, funded by The National Research Centre, showed that it is devoted mainly to pragmatic issues having to do with analyzing, evaluating and ensuring the security of the critical infrastructure (CI) of the state. There is no theoretical apparatus that would allow:

- uniform interpretation and modeling of CI,
- the carrying out of integral analysis related to the risk associated with crisis and crisis management at all levels and in all areas related to CI,
- a dynamic analysis of the structure and functioning of CI.

It seems that the solution might be to treat CI as an organizational and technical system, and to choose the appropriate methodological apparatus of systems theory to its modeling and analysis, as well as separating the functional aspects of the proposed system of its structural features – so that the operational modification of the functional aspects do not cause significant structural changes to the adopted solutions [1-4, 8].

Since we are considering in this paper the safety of CI, we use the resource approach based on the concept of resources, interpreted as a part of material reality (physical) or virtual (e.g. conceptual, information, metalinguistic), which is a non-empty set of features and their values [6].

2 The genesis of the subject of research and comparative analysis

Designing systems with organizational and technical characteristics specific for the resources can be implemented in many ways. The main difficulty lies in the proper selection of the methodological apparatus of systems theory. The key to a solution is the separation the functional aspects of the proposed system from its structural features that any modification of its structure does not cause "structural revolution" for the previously obtained solutions [1, 6, and 8].

The sine qua non of a satisfactory design and its implementation is the definition of the axioms' proper functioning (operation) of the future system. On the basis of the axioms' proper functioning one can construct theories and theorems, and prove

[1] The main objective of the project ID 193751 is to develop a methodology for estimating the risk of a crisis, including the destruction or disruption of the state's critical infrastructure, adapted to the requirements of planning documents and software developed for the purpose of a crisis management system.

the design's correctness (completeness and non-contradiction) as it pertains to the systems [10].

The determination of the variables and the aggregation of data are basic operations done in preparation of the Multi-dimensional Comparative Analysis (MDCA), by which it is possible to build logical and arithmetic models for structural and functional studies of real objects (resources and their complex interrelationships in the form of physical infrastructure, in particular CI) [13-16].

MDCA is used to detect patterns and similarities present in the investigated objects. The primary task is to seek MDCA methods to simplify complex data structures into separate categories, each of which represents a specific data type. An example is the concept of the universal category of the resource, its features, and the repertoires of these characteristics.

With respect to the main tasks of MDCA, one may include statistical analysis of the data and the optimization of the set of diagnostic variables. The main methods of MDCA can be carried out using four basic scales: nominal, ordinal, interval and quotient[2].

With respect to the description of the CI[3] of the resources, each of these scales can be used depending on the structural characteristics of these resources. This task becomes especially important when one is looking for an effective way of classifying and comparing resources in the accompanying decision-making processes – especially in emergency situations concerning their functionality.

The advanced analysis of resources leads, in terms of semiotic (semiotic signs), to its representation in the form of a continuum of semiotic signs [1, 6]. Using the model of the resource, in semiotic terms, we treat each resource as a triad: the reality, the identifier and the interpretation.

[2] data analysis – the procedure leading to the clustering effect data according to the adopted scale and the used criteria

[3] Critical Infrastructure (CI) – in accordance with the Act of 26 April 2007. Crisis Management Art. 3 pt. Critical Infrastructure as amended, includes the following resources and systems: energy supply, energy raw materials and fuels; communications, data communications networks; financial; food supplies; water supply; health care; transport; rescue; ensuring business continuity in public administration; production, stockpiling, storage and use of chemical and radioactive substances, including pipelines of hazardous substances; cultural resources and heritage.

The resource in its real form – this is the objectively existing physical or abstract element of the subject area. The resource as an identifier (Lat. denotat, denotates) is the distinguished (individual) name of the actual form of the resource. The resource in the sense of the interpretation is the resource as belonging to a particular class of resources, indicating its properties (among other things, which was awarded from other resources).

The semiotic characteristics of the resources enable to distinguish the names (denotates) from fragments of reality with these names, as well as the properties of these fragments (highlighted features) of the same fragments of reality.

This distinction is particularly important when the modeled subject area have become models (semiotic signs) of other realities. The phenomenon of this kind often happens, for example, when designing a hierarchical decision-making system [11, 12].

3 Resource interpretation of the Critical Infrastructure

The resource critical infrastructure interpretation is carried out from four different perspectives: in the form of a resource (unified) interpretation of a variety of CI resources; in the form of reactor technology realizing the uniform processing of data structures regardless of the specifics of the technological CI; in the acceptance of hyper graphs notation channels and objects that describe the resources and their internal and external impact; in recognition of the dynamics of resource states as a description of the interaction of functional and structural compounds and the memory resources phenomenon [17, 18].

3.1 Identification of CI systems

The interpretation of CI in terms of resources allows the use of a simple conceptual apparatus to describe the complex question concerning the identification and analysis of CI systems, which is the basis for specific actions related to national security.

The use of the resource approach allows to define a single CI as a system and its component functionally interrelated objects, such as: building structures, equipment, installations, services essential to the

security of the state and its citizens, and to ensure the efficient functioning of the public administration, as well as institutions and entrepreneurs.

As stated in the National Program for Critical Infrastructure Protection (NP-CIP)[4]: "Identification of facilities, equipment, installation or services for which the destruction or disruption of the functioning could cause a crisis is a key step in the process of protection CI" [19-21].

The resources are described and grouped by concepts of class resources arising as a result of the use of the method MDCA to the universe of CI[5] stocks, which is the subject of analysis and operations [23, 24].

Each class of resources has a specified (possible to refill) repertoire of features, which should include the following elements:

1) the characteristics of the resource;
2) the definition of the geographical allocation of resources;
3) the representation of the parameters relating to the consequences of the destruction or non-functioning a resource that matches the cross-sectional, as defined in the document NPCI (p. 11)[4], which includes: casualties, the financial implications, the need to evacuate, loss of services, recovery time, the effect of international and uniqueness;
4) the characteristics describing the state of the resource as falling within the limit values max-min, which would allow the introduction of hazard information;
5) an attribute indicating the significance (meaning) of the resource in the CI system;
6) the characteristics defining the resource susceptibility to destruction, disruption of the operation, reducing potential or effectiveness or improper use;
7) the characteristics useful for the purposes of risk analysis and to develop scenarios for the development of adverse events.

The repertoires of features should be harmonized for the entire CI, which will develop and apply the same tools for collecting operational data, reporting, aggregation of data, and conducting analytical and decision support.

The distinguishing characteristics of the respective class is always whenever we begin to describe the different resource groups; and also in this case when, with respect to the same set of characteristics, there are different repertoires of their value.

The dynamics of the changes in the characteristics of the resource should include only the features most important from the point of view of ensuring the continuity of the proper functioning (operation) of a particular class of resources. The failure to follow this rule (excessive number of features with a significant number of limit values) – due to the exponential increase in the complexity of state – will prevent an estimation of the effects of the interaction of resources.

For example, only with respect to 15 features of resource A, with five values of each feature, do we obtain about 30,5x109 states of that resource. If the resource A will have the same impact in terms of complexity as with respect to resource B, the number of possible such states the system will grow to 9,3x1019.

It is obvious that simplify the description of the interaction of normal and critical (and thus of risks) must be conducted and evaluated in a way that ensures their relevance to the objective function, which is to preserve the continuity of CI [5, 7, 9, 22-24, and 26].

From the above reasoning it follows that the analysis of the continuity of CI can be effectively conducted (with a chance of counteracting threats) only by using "highly simplified" modeling tools of logic and the potential impact of External Resources (ER) and through the impact of Internal Resources (IR), which are identifiable in structures of resources.

Modeling of logic is possible by means of hypergraph structures; modeling of the potential impacts – using additive operations on risk potentials, calculated taking into account the changes of the dynamics (speed and acceleration). The development of methodological examples of positioning risks detailed

[4] National Programme for Critical Infrastructure Protection 2013, p. 11.
http://rcb.gov.pl/wp-content/uploads/NPCIP-dokument-główny.pdf

[5] universe of resources - all distinguished collection of resources for research, analysis and operational activities

in the structures of resources should not be too difficult[6].

The resource can be subjected to three types of structural operations [6]:

- operations as a result of which class (set of features resources) is determined and the type of resource (due to the organization of the constituent stocks),
- operations as a result of which occurs class or type of resource change (for obvious reasons, not all variants of these changes are acceptable),
- operations as a result of which, in relation to the collective resource, one of the four measures is made:
  - the resource is introduced into population,
  - the resource is derived from the community,
  - the resource in the community is replaced by a resource from the outside,
  - checking whether the community contains a particular resource.

3.2 Technological reactors

The study of threats is being caused by the consequences of the interaction of human, material objects and physical phenomena. These consequences lead to an increased risk of adverse events, and in the case of severe intensity, also to the emergence of a crisis – and the resulting need for risk assessment.

A risk assessment is performed to determine the likelihood of an occurrence (as the relationship between the number of events that have occurred and that may be the cause of incidents, and the number of events that implement these risks) as well as the size of the loss (determined by: the new value, the replacement value or book value, and indirect losses). Risk should be expressed in the form of a model of risk assessment and a risk management model (including the transfer of risk).

The risk is a function (result) of two phenomena: threats and vulnerabilities. Estimating the risk in a specific area of activity, subject to observation and assessment, is the starting point to build a Crisis Management (CM)[7] system, the essence of which is to make decisions under time pressure in an emergency, maintaining key functions in the area. This statement implies the need to establish a working definition of a group of initial concepts, and then expand them in accordance with the needs of the CM plan. The basic concepts are the keywords: resource, event, process, decision, threat, risk and crisis situation [25, 27-29].

Each of these concepts is the starting point for defining and developing a system of concepts, deciding test methods with respect to hazards, risk assessments, and the process of crisis management. A well-designed ontology (a system of concepts) of the affected area of activity may have a significant impact on the architecture (spatial structure) and function (effectiveness) of the CM system.

The simplicity of the structure and effectiveness of the operation in this case are the key to the design of hierarchical (pyramidal) structure of the a CM system. The base of this pyramid are material objects or natural phenomena regarded as resources of reactors, and related organizations and companies that are operating in this environment. All these resources are management entities[8] responsible for the prevention, coordination and cope with emergencies by appropriately conducted management and technological processes.

The theoretical considerations should assume the existence of both negative impacts (risks) as well as positive impacts (benefits). These effects are cumulative and cancel each other as a result of synergies of the simultaneous operation of multiple resources. Modeling positive impacts can assist the processes of prevention and compensation and can overcome the effects of threats.

[6] Ostrowska T. - The determination and description of the criteria for passing an emergency situation in a crisis situation and threats to national security. The term methodical and the guidelines described. The final product stage PEVII.14 to be used in part to other products. Warsaw University of Technology, Faculty of Management, September 2014.

[7] Crisis Management (CM) - is an activity consisting of: (1) predicting and recognizing the signs of rising crisis; (2) inhibition and prevention of the formation and development of the crisis; (3) mastered, leveling and dealing with the consequences of crisis.

[8] The entity in charge is the person or entity acting as management at the level of the organizational structure of the state, responsible for the reliable operation of the critical infrastructure CI^x allocated to it.

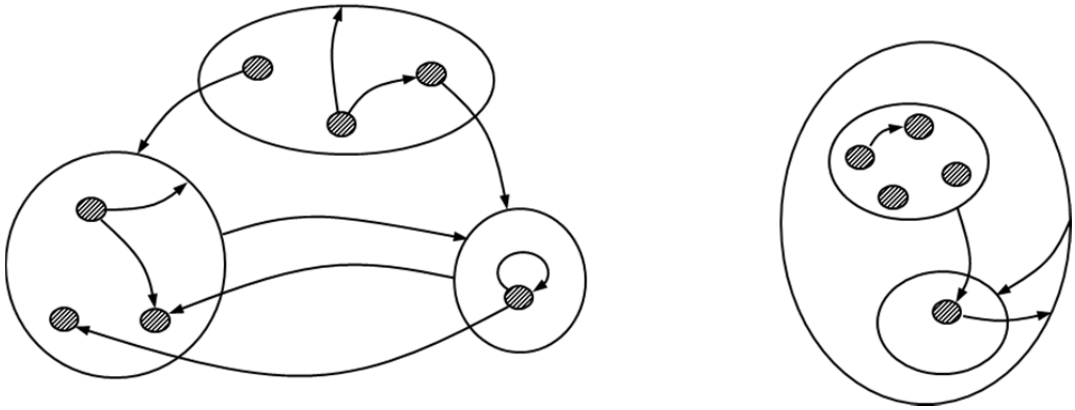

Figure 1. Examples of hypergraph models of threats clusters

3.3 External and internal resource impact

The external and internal resource impact of structures (see Fig. 1) are realized through the process structure, in which the primary role is played by sequences of discrete events, executing on virtual channels formed by the pair <susceptibility> : <threat>, which decide about the functional and structural condition of CIx resources.

Fig. 1 shows hypergraphs models of two clusters of threats caused by displacement relative to another resource – which has caused negative impacts in the resources of these clusters. Identified risks inherent in the resource are shown as shaded circles. The hypergraph's arches point to the direction of the negative impacts among resources; one of the arches illustrates the feedback risk of "self-destruction" the negative impacts among resources; one of the arches illustrates the feedback risk of "self-destruction".

The illustrated diversity of resources and links to related hazards indicates the need for a very flexible "channel" of treatment effects for the pair <susceptibility> : < threat > between resources and the environment in which they are sited.

The analysis of the process of workflow structures, as a product of processes carried out on the channels in the form of the interaction pair <susceptibility> : <threat> is decisive for determining.

- the effects of loss of functionality and opportunities for it to maintain or restore collectivities resources $\{CI^x\}$,
- halt and reverse transition from a situation of increasing threats to the crisis, as assessed on the base of chains of events and their probabilistic characteristics to measure the effects and risks of threats in relation to thresholds set by the gambling companies operating with precision to different channels $(U/Z)^x_{\alpha,\beta}$; the entire resource (all channels resource); all the resources of a given type of critical infrastructure CI^X and a set of subsets of all types of resources $\{CI^X\}$.

The impact of ER, and their impact on IR, determines the structure of different shelf lives. The resource structure is so long in terms of business continuity, as long as the operating entity, given the structure of the aggregated accept the risk of positive and negative interactions of its resources.

If the combined risk of the resource's structure[9] exceeds a safe threshold[10] then the carrier structure decomposes it by changing the balance of the potential risks by including new resources or disconnection of used one and change in the way the total potential of the risk[11] of the entire structure.

The effective positioning of the risks in the structures of the resources is significantly dependent on methods for monitoring the speed and direction of the change of the potential threats.

[9] Aggregated risk structure of the resources – the sum of risks on all virtual channels of the resource structure

[10] Safe threshold – in the deliberations adopted the following classification: acceptable, warning, and unacceptable I, unacceptable II, and crisis

[11] Risk potential – the difference between hazard and vulnerability; threat – is the expected impact on the object or between objects, as a result of which they can degrade their functional and structural characteristics; compliance (submission) – the opposite of resilience understood as a basic feature of infrastructure CI^x opposite danger (decrease or increase susceptibility is done with the resources available infrastructure CI^x)

Table 1. State transition matrix of the object
(*source:* own)

system status	00	01	10	11
00	0,06	0,14	0,24	0,56
01	0,08	0,12	0,32	0,48
10	0,18	0,42	0,12	0,28
11	0,24	0,36	0,16	0,24

3.4 Memory of resources

An inherent feature of any object as a model resource is its memory. The memory object is used to model the dynamics of the resource states[12]. The memory object should not be confused with the state of the resource, which is modeled, or the state of the object channels. The memory object is a list of statuses showing all the permissible combinations of pairs {<state input channel> : <state output channel>} and stochastic rule changes in statuses with parameters relevant to stochastic state changes the rules of the modeled resource.

The dynamics of the memory states of the object is a sequence of the states of an object, obtained as a Cartesian product of the input channel and output channel of this object – carrying the dynamic states of the input and output channels of the object[13].

The dynamics of the input channel status object is expressed by a sequence of the input channel status of this object, described as a sequence of input vector states of the sub channels of the object, which is the product of the state chart of the input channel of this object (describing the effect of internal influences on the considered channel of the object).

Similarly, the growth in the output channel states object is expressed by the sequence of states of the output channel object vectors, described as the sequence of states of the sub channels output of this object, which is the product of the state chart output channel of this object (describing the effect of impacts considered internal to the channel of the object).

An example of state changes at the input and output channels of the object is stored in the form of a state transition matrix (see Table 1) and its corresponding object to a graph object states (see Fig. 2) with 4 highlighted states, which are accompanied by symmetrical 16 events on the input and output channels of the object.

Using the transition matrix switch contained in the Table 1 one can efficiently calculate the probability of a particular state succession on the current state of the system at different trajectories of state changes. Thus, the probability of direct transition from state 00 to state 11 is 0.56; while the probability of transition from state 00 to state 11 via state 01 is only 0.0672.

Importantly, nearly a 10-fold reduction in the likelihood of the state 11 immediately after the state 00 may be the reduced risk value associated with the state 11, provided that the total risk of a intermediate state 01, then state 11 will not be larger.

Estimating the value of risk across the trajectory of the system state changes will be even more meaningful if we assign the system states the cost to restore them after the incident (realized risk) associated with the considered state of the system.

[12] Resource state – is a vector of the current values of attributes created with individual values for each of the resource features, describing the current state of the resource at a given moment or in a given interval of time

[13] Channel status object - corresponds clearly to the characteristics of the resource corresponding to the channel, which is the object model of the resource

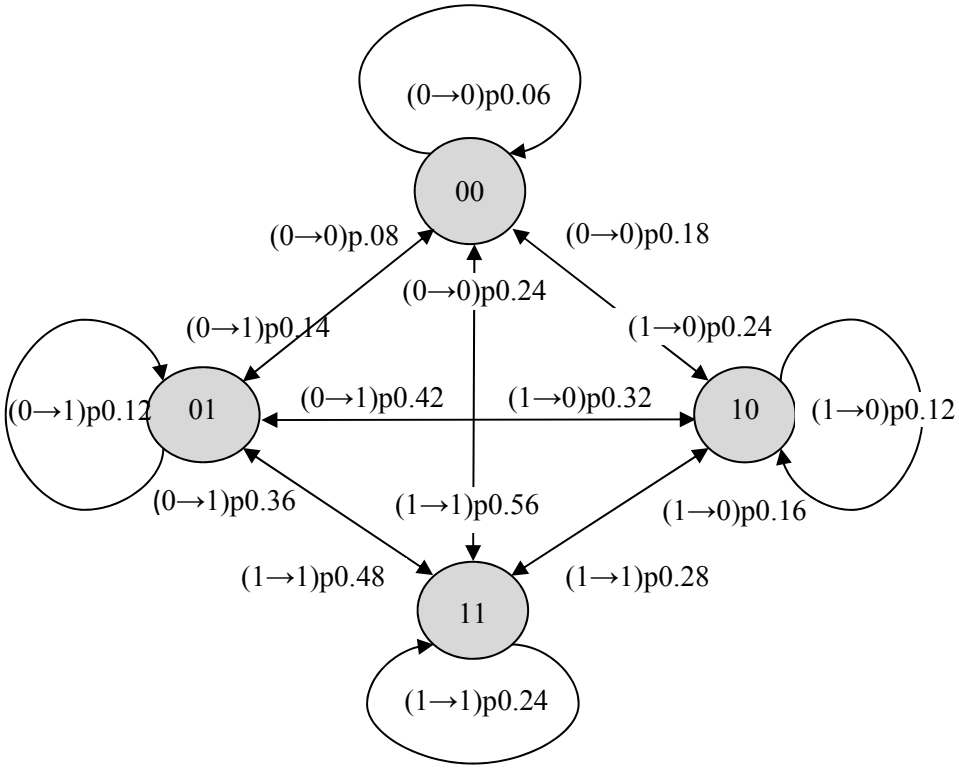

Figure 2. Graf states of stochastic system with four events on channels facility: 00, 01, 10, and 11 (*source:* own)

4 Risk measurement of risks and its essence in terms of calculation

The concept of risk is an abstract (numerical value) expressing the percentage of the expected loss of functionality on the channels of the portion of the resource, or set of resources – also called the level of risk[14].

The risk value R is expressed as the product of:

$$R = P \times U \times Z \quad (1)$$

where:

R – risk is the product of probability, vulnerability and threat, expressed as (0..1) x [0..1] x [20..100]%,

P – likely to be understood as a function of assigning values hazard within the closed numerical value [20..100]% in the range wiped away (0..1)[15],

U – susceptibility within closed borders [0..1] is understood as a basic feature of the infrastructure CI^x the opposite danger; control susceptibility (increase or decrease) is carried out with the available infrastructure CI^x,

Z – threat within the closed borders [20..100]% construed as the expected impact on the object or between objects, as a result of which they can degrade their functional and appropriate for their structural characteristics.

The percentage record of the effects of threats Z from the channel $(U/Z)^x_{\alpha,\beta}$ is not likely to occur, but their percentage of loss of functionality of the resource as a result of the actual implementation of the event describes this threat.

[14] The level of risk – for practical reasons adopts a 5-stage classification of risk levels: level acceptable [0..20), warning [20..40), unacceptable I [40..60), unacceptable II [60..80), and crisis [80..100)

[15] Closed borders [p..q] mean that a particular function for them can take the values ≤ q and ≥ p; open borders (p..q) mean that a particular function for them can take the values < q and > p

According to this clause, the sum of the effects of the loss of functionality on all channels $(U/Z)^{x}_{\alpha,\beta}$ of the affected resource infrastructure may in the calculation model and the method of proceeding exceed a value of 100%, even several times, although the actual loss of the intended functionality of the infrastructure resources, for obvious reasons, will not exceed 100%, even in the event of the physical liquidation of that resource.

With the threats and risks of their formation comes the danger of a crisis situation – i.e. a situation where the expected impact of the implementation of (the consequences) the threats have reached a critical level (threshold gambling H[16]): (1) for the given channel infrastructure CI^{x} within the municipality, county or state; (2) for the indicated resource CI^{x} infrastructure with respect to the territory of the municipality, county, state, or country; (3) for the indicated CI^{x} infrastructure on the territory of the municipality, county, state, or country; (4) or for a specified combination of channels, resources, and infrastructure CI^{x} within the municipality, county, state, or country.

5 Infrastructure

The classification of CI in terms of technology and of area depends on the type and the geographical and administrative allocation of this infrastructure. The classification process of CI should be carried out by the operators at the level of direct contact with the infrastructure objects and channels, in order to recognize and cope with the threats.

5.1 Geography deployment of CI resources

The infrastructure type CI^{x}[17] determines its susceptibility to the typical risks inherent to the technological specifics of this infrastructure.

The effectiveness of the diagnosis determines the behavior of the operators and the methodology used in the heuristic rule simplification. These rules should be subjected to systematic review with respect to the consistency of the reality of the threats.

Particular attention is required to recognize hazards from low intensity and diffuse areas of the country or region (e.g. poisonings, epidemics, flooding, road disasters), bringing together a domino effect that could lead to a crisis or even a threat to national security, if advanced (polynomial and correlated) analysis is not carried out of the dynamics of gambling diffuse threats.

5.2 Integral model of a crisis situation in CI

A fixed duty of government is a constant observation of the Critical Infrastructure CI^{X}. Continuously is providing the monitoring of increased growth rate of the degree of risk in relation to a group of identical CIx features (the Act of 26 April 2007 Crisis Management, Journal of Laws 2007 No. 89 item 590, as amended).

An an example of a group of identical CI^{x} shown in Figure 3, demonstratively illustrates the situation on 10 highlighted CI^{x}:

- infrastructure CI^{1} type: CI^{1}_{1}, CI^{1}_{2},
- infrastructure type CI^{2}: CI^{2}_{1}, CI^{2}_{2},
- infrastructure CI^{3} type: CI^{3}_{1}, CI^{3}_{2}, CI^{3}_{3},
- infrastructure CI^{4} type: CI^{4}_{1}, CI^{4}_{2},
- infrastructure type CI^{5}: CI^{5}_{1}.

The term "homogeneous CI^{x}_{i}, where x is the identifier of the type CI^{x}" means that there are contemplated within the $CI^{\chi}_{j} \subset CI^{x}_{i}$ other than the type CI^{x}, due to their optionality in relation to the risks. This limitation is illustrated by the example in Figure 4, which marked CI^{χ}_{j} infrastructure that was neglected in the modeling and exemplary implementation of infrastructures CI^{χ}_{1}, CI^{χ}_{2} and CI^{χ}_{3}.

[16] Threshold gambling H is the situation on the designated channel resource, infrastructure or a combination thereof, which has reached a point of discontinuity risk, expressed symbolically by $H = P \times U \times Z \geq 50\%$ (value of H = 50% is determined a priori assuming that: P = 0.8, U = 0.8 and Z = 80%, the next level of P = 0.9, U = 0.9 and Z = 90% would result in approximately 50% increase in the value H, i.e. H = 73, 9%)

[17] Type CI^{x} – one of the highlighted infrastructures CI^{1}, CI^{2}, CI^{3}, ... CI^{12}

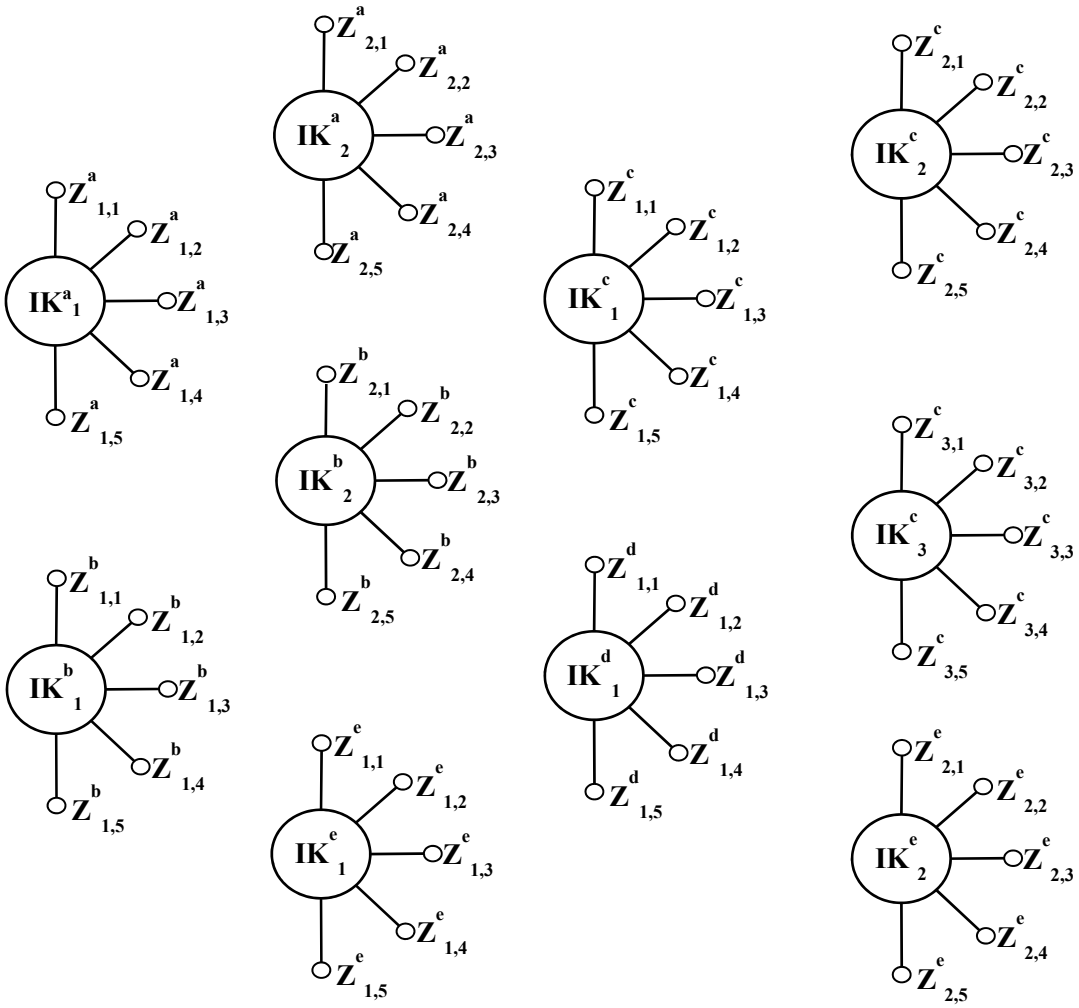

Figure 3. Groups of identical CI, for which monitoring of the recorded increase the risk above tolerable, where:
CI^x_i i-type infrastructure x,
Z^x_j - a threat kinds j for CI^x,
j – hazard identification of infrastructure CI^x

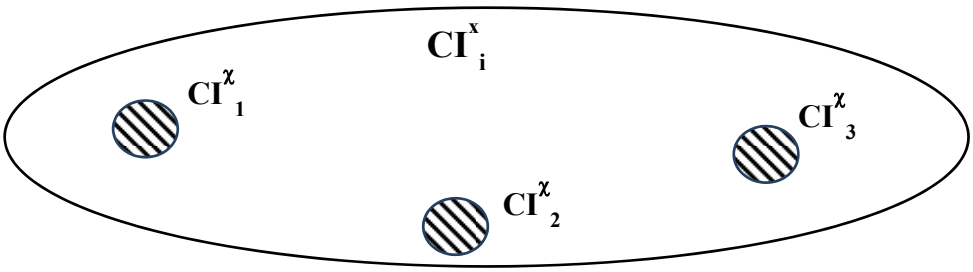

Figure 4. Example of three neglected infrastructure CI_i type χ

Table 2. Infrastructure and their hypothetical threats list

IK^a	<name of infrastructure>	
	threats:	authentic descriptions from official sources*
Z^a_1	<the essence of threat threat>	
Z^a_2	<the essence of threat threat>	
. . .		
IK^b	<name of infrastructure>	
	threats:	authentic descriptions from official sources*
Z^b_1	<the essence of threat threat>	
Z^b_2	<the essence of threat threat>	
. . .		
*) comment: some sources list of threats are treated as "confidential"		

Table 3. Infrastructure model and their symbolic threat

CI^a	critical infrastructure CI^a
	threats:
Z^a_1	- threat Z^a_1
Z^a_2	- threat Z^a_2
. . .	. . .
Z^a_5	- threat Z^b_5
CI^b	critical infrastructure CI^b
	threats:
Z^b_1	- threat Z^b_1
Z^b_2	- threat Z^b_2
. . .	. . .
Z^b_5	- threat Z^b_5
. . .	
CI^x	critical infrastructure CI^x
	threats:
Z^x_1	- threat Z^x_1
Z^x_2	- threat Z^x_2
. . .	. . .
Z^x_5	- threat Z^x_5

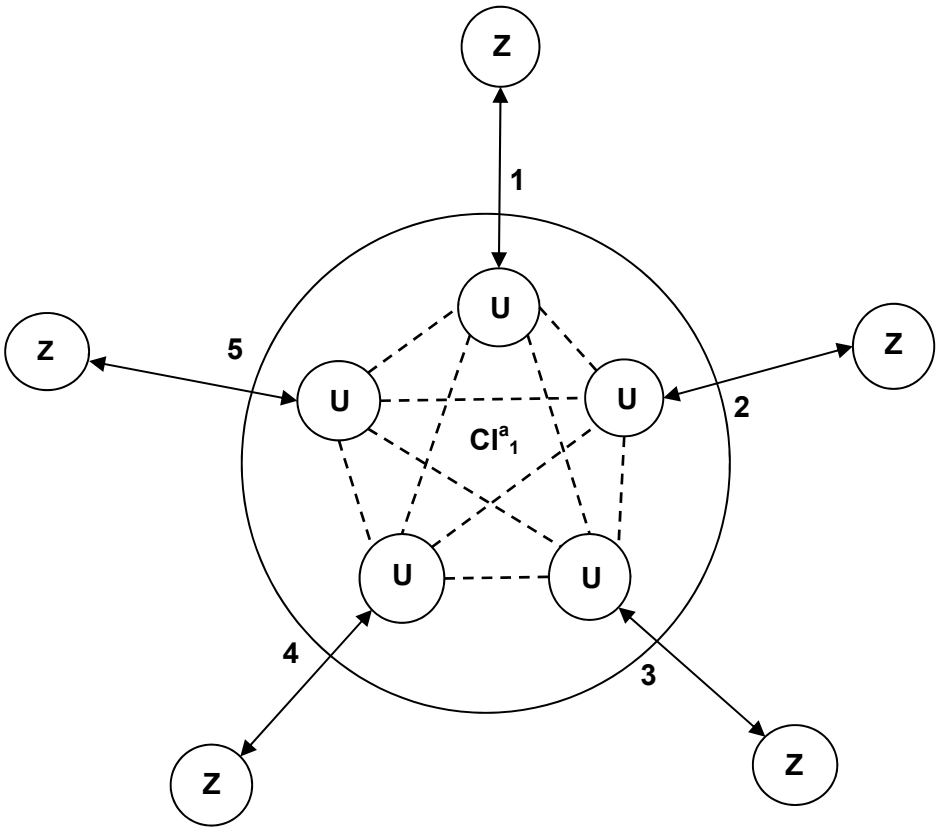

Figure 5. Infrastructure model CI^a_1 in terms of object, in which communication channels "vulnerability - a threat" are highlighted
(a dotted line is used to indicate relationship of mutual substitution of vulnerability protection resources in an emergency)

5.3 Procedures to be followed in assessing and addressing the crisis situation

For each type of the Critical Infrastructure CI^x presented in the Act on Crisis Management of 26 April 2007 have been described a corresponding groups of hazards and the resulting risks.

The hypothetical list of possible CI^x types and risks are presented in Table 2.

List of threats are presented in Table 3 symbolically (simplified for purposes of modeling and construction of methodology).

The list of threats in Table 3 are fixed in relation to the model shown in Fig. 3. In any case, the model has the list of threats limited to five. For each hazard from Table 3, a uniform percentage scale was adopted to meet its current level (in the evaluation of monitoring).

Fig. 5 shows the object model of infrastructure CI^a_1 (see. Fig. 3), on which channels $(U/Z)^1_{a,1\text{-}5}$ are shown to illustrate the phenomenon of compensation of threats $Z^a_{1,1\text{-}5}$ by the vulnerability $U^a_{1,1\text{-}5}$ of the infrastructure CI^a_1.

Table 4 shows the percentage scale of the threat, uniform for the entire model.

All the assumptions made in Table 2, Table 3 and Table 4 are contractual and used to build models of vector vulnerabilities (U), threats (Z), consequences (S), and risks (R).

Table 4. The percentage scale of the degree fulfillment of threats

extent of the risks	a symbolic designation	term verbal threats
1% ÷ 20%	20%	minimum
21% ÷ 40%	40%	little
41% ÷ 60%	60%	medium
61% ÷ 80%	80%	big
81% ÷ 100%	100%	extreme

Table 5. Vectors susceptibility (U) and threats (Z) for infrastructure CI^a_1 and the effects (S)

IK^a_1	t_0 – phase 1			t_1 – phase 2			t_2 – phase 3		
channel U/Z	susceptibility [0..1]	threat [%]	effect [0..1] x [20..100]%	susceptibility [0..1]	threat [%]	effect [0..1] x [20..100]%	susceptibility [0..1]	threat [%]	effect [0..1] x [20..100]%
$U/Z^a_{1,1}$	1	20	20	0,5	40	20	0,7	40	28
$U/Z^a_{1,2}$	1	20	20	0,5	20	10	0,3	20	6
$U/Z^a_{1,3}$	1	20	20	0,5	20	10	0,1	20	2
$U/Z^a_{1,4}$	1	20	20	0,5	40	20	0,4	40	16
$U/Z^a_{1,5}$	1	20	20	0,5	60	30	0,9	60	54

5.4 Estimating the state of emergency on simulated areas

Fig. 3 is an illustration of the experiment computing, which consists of assigning infrastructures CI^X:

- varying in time the threats expressed in % loss of functionality for infrastructure,
- continuing vulnerability $U_i(\tau)$ for different moments of time t_0, t_1, t_2, t_3 succession of threats,
- and the moments of time τ, in which occurred extortion by threats or decrease of susceptibility change caused by the operator CI^X.

The values entered for threats were selected from Table 4. The initial value of the threats was adopted at 20%, which corresponds to the verbal definition of "minimal".

In the prepared phase of the experiment shown in Table 5 provides an analysis of the functioning of infrastructure such as CI^a_1 at three points in time:

1) from time t_0, for the purpose of simulations it was found that the vulnerability is 1 on the scale [0..1], for each type of threat and the maximum value of the risk for each type of hazard is 20% of the total CI^a_1; this means that the effect of the implementation of the risks is the loss of ability to function 1/5 of that infrastructure (see Tables 5 and 6);
2) from the time t_1 for the simulation it was found that the susceptibility is reduced for each channel risks for 0,5 of the current value of risk because, for example, the high cost of maintaining a low susceptibility – a risk, however, increased 2-fold at the 1st and 4th of the channel U/Z and 3 times on the 6th channel;
3) at the time t_2 drawn new vector susceptibility while maintaining the same risks.

The basis for estimating the risks is Table 4, whereby as a result of monitoring determined to be the possible (probable) current effect of threats and vulnerabilities in all CI^x_α, wherein:

x - the type of infrastructure,

α - an index of 1, 2, … infrastructures x.

Table 5 is used in situations where the probability of occurrences are known risks $Z^x_{\alpha,\beta}$ for CI^x_α on the channel "vulnerability/threat" $(U/Z)^x_{\alpha,\beta}$, where:
α - index infrastructures CI^x_α (in the example shown in Fig. 5 type x: a, b, c, d, e,

β - the index of the hazard (in this example: from 1 to 5).

In the presented example, a percentage of the consequence channels $(U/Z)^x_{\alpha,\beta}$ is the percentage of the loss of functionality of the resource as a result of the threat. According to this principle the sum of the effects of the loss of functionality on all channels $(U/Z)^x_{\alpha,\beta}$ of the infrastructure resource could theoretically exceed 100%.

Table 6. Vectors of risk (R) for infrastructure CI^a_1

channel U/Z	probability [0..1]	effect [%]	risk [%]	probability [0..1]	effect [%]	risk [%]	probability [0..1]	effect [%]	risk [%]
$U/Z^a_{1,1}$	0,10	20	2	0,10	20	2,0	0,15	28	4,2
$U/Z^a_{1,2}$	0,10	20	2	0,15	10	1,5	0,20	6	1,2
$U/Z^a_{1,3}$	0,10	20	2	0,20	10	2,0	0,25	2	0,5
$U/Z^a_{1,4}$	0,10	20	2	0,10	20	2,2	0,15	16	2,4
$U/Z^a_{1,5}$	0,10	20	2	0,15	30	4,5	0,20	54	10,8

5.5 Signals crisis

In the first stage of the experiment, it was assumed, as a signal of rising crisis, that at least on a one channel of the CI possible threat exceeded 50% loss of functionality conveyed through this channel (see. Tables 5 and 6, channel $U/Z^1_{1,5}$) – for example, the temporary loss of access to 50% of the drinking water caused the failure of filters.

The evaluation crisis in the prescribed area of the territory is carried out by means of the ongoing monitoring of the expected impact of the implementation of (the consequences of) threats.

For this, a specified range of functionality and the corresponding channels defined the threshold value of the expected effects of the implementation risks:

- the highlighted channel of infrastructure within the municipality, county, state or country (see instance channel to channel in the infrastructure index 5 in an unspecified threat municipality),
- the highlighted resource of the infrastructure CI^x for the sum of the expected impact of the implementation of risks on all channels within the municipality, county, state or country,
- highlighted the infrastructure CI^x for the sum of the expected impact of the implementation of risks on all channels within the municipality, county, state or country,
- highlighted the combination of resources and infrastructure CI^x for the sum of the expected impact of the implementation of risks on all channels within the municipality, county, state or country.

The crisis rating is conducted at five levels, as shown in Fig. 6.

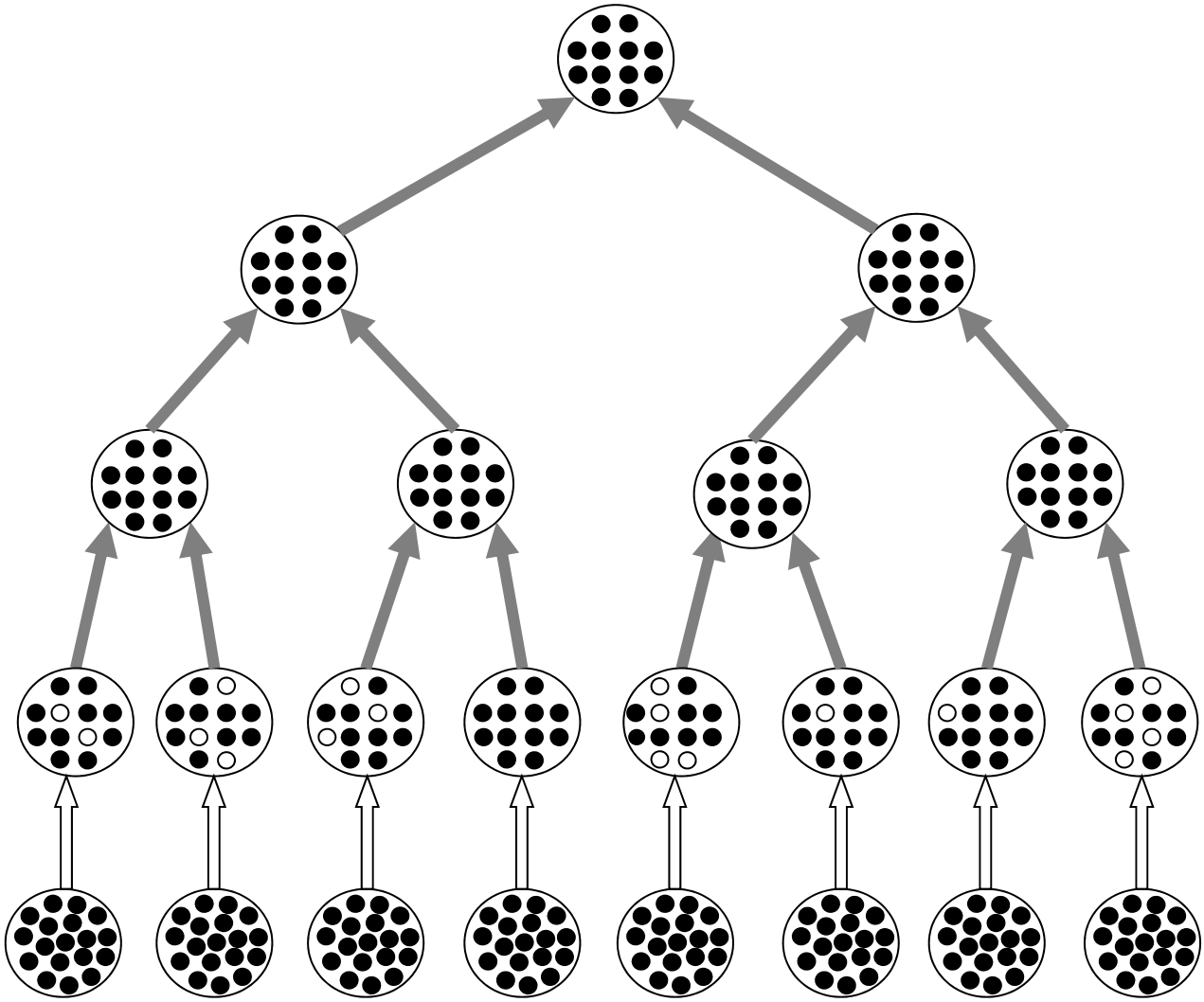

Figure 6. 5-leveling the assessment of the crisis in the levels of meta infrastructures of state, provinces, districts and communes at the infrastructure level

The data monitoring was limited to all the distinguished physical channels (U/Z) of the resources CI^X (operating resources of municipalities) to the following activities:

- estimating the probability P succession of threats functionality on the scale [0..1],
- estimating susceptibility U to threats functionality Z,
- assessing threats Z to the highlighted features on a percentage scale [20..100]%,
- assessing the effects of loss S of functionality as a result of threats on open a percentage scale [0 ...]% as the product of vulnerability (U) and threats (Z) in the form of a formula [0..1] x [20..100]%,
- assessing the risks R of loss of functionality as a result of threats on open a percentage scale [0 ...]% as the product of the probability (P), vulnerability (U) and threats (Z) in the form of formula (0..1) x [0 ..1] x [20..100]%.

6 Conclusions

The main aim of this study was to determine the mechanisms to measure the risks to which they may find themselves useful for diagnostic processes in management of critical situations in the Critical Infrastructure of the resources. Our intentions, in some cases significantly exceeded the scope of work that could be performed by the authors.

Our intentions, in some cases, far exceeded the scope of work that had been possible to perform by the author.

In conclusion we can say that in this article we approached to the nature of the problem of dynamic assessment of the crisis situations - in the Critical Infrastructures of resources - with many promising perspectives to which we included following theoretical and practical issues: (1) resource interpretation of the Critical Infrastructure concept; (2) the concept of technology reactor modeling the impact of internal and external resources; (3) the internal memory of resources; (4) the risk measurement in terms of the calculation; (5) the integral model of a crisis in the Critical Infrastructure environment; (6) the point of gambling as a start of the risk management, connected with the geographical and administrative deployment of the Critical Infrastructure.

7 Bibliography

[1] Domański J., Kotarba W., Krupa T. - *W pryzmatach zarządzania* (In the prisms of management) [in] Klasyczne i współczesne koncepcje zarządzania. Aspekty teoretyczne i praktyczne. Wyd. Uniwersytetu Ekonomicznego, Poznań 2014.

[2] Korzeniowski L.F. - *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem* (Basics teachings about security. Security management). Difin, Warszawa 2012.

[3] Kosieradzka A., Kąkol U. - *Propozycja modelu kompleksowej oceny ryzyka w zarządzaniu kryzysowym* (Proposal model of comprehensive risk assessment and crisis management) [in] Logistyka, nr 5/2014.

[4] Kosieradzka A., Uklańska A. - *Wykorzystanie współczesnych koncepcji i metod zarządzania organizacjami w zarządzaniu kryzysowym* (Use of modern concepts and methods of managing organizations in crisis management) [in] Logistyka nr 5/2014.

[5] Krupa T. - *Model systemu wspomagania rozmytych procesów decyzyjnych* (Model support system of fuzzy decision-making processes) [in] Komputerowo zintegrowane zarządzanie (red. R. Knosala). WNT, Warszawa 1998, pp. 203-212.

[6] Krupa T. - *Elementy organizacji. Zasoby i zadania* (Elements of the organization. Resources and tasks). WNT, Warszawa 2006, pp. 240.

[7] Krupa T. - *Events and Events Processes* [in] Foundations of Management - International Journal, Vol. 1, No. 2, 2009, pp. 143-158.

[8] Krupa T. – *Modelowanie procesów dyskretnych w aksjomatyce teorii charakteryzacji Gorbatov'a* (Modeling discrete processes using Gorbatov axiomatic theory of characterization) [in] Wybrane zagadnienia informatyki gospodarczej (red. T. Krupa). Oficyna PTZP, Warszawa 2009.

[9] Krupa T. - *Operacje na sieciach zdarzeń* (Operations on events networks) [in] Logistyka, nr 5/2014.

[10] Krupa T. - *V.A. Gorbatov Theory of Characterization – Principles and Examples* [in] Foundations of Management, Vol. 5, No. 3, 2014.

[11] Krupa T., Ostrowska T. - *Multilayer Decision Support Model for Value and Cost Analysis of IT Solutions – Hierarchical Approach* [in] Managing Worldwide Operations and Communications with Information Technology. IGI Publishing, Vancouver Canada, 2007, pp. 86-90.

[12] Krupa T., Ostrowska T. - *Decision-making in flat and hierarchical decision problems* [in] Foundations of Management, Vol. 4, No. 5, 2012.

[13] Krupski R. - *Rozwój szkoły zasobów zarządzania strategicznego* (The development of strategic management resource school) [in] Przegląd Organizacji nr 4/2012.

[14] Kunikowski G. - *Funkcjonowanie zasobów infrastruktury krytycznej w kategoriach Pareto-optymalnych i w równowadze Nasha* (The functioning of critical infrastructure resources in terms of Pareto-optimal, and a Nash equilibrium) [in] Logistyka, nr 5/2014.

[15] Łuniewska M., Tarczyński W. - *Metody wielowymiarowej analizy porównawczej na rynku kapitałowym* (Methods of multidimensional comparative analysis on the capital market). Wydawnictwo Naukowe PWN, Warszawa 2012.

[16] Marczewski M., Staniszewski M. - *Identyfikacja i analiza danych niezbędnych do oceny ryzyka – klucz do skutecznego zarządzania kryzysowego* (Identification and analysis of data required for risk assessment - the key to effective crisis management) [in] Logistyka, nr 5/2014.

[17] Ostrowska T. - *The Resource Hazards Model for the Critical Infrastructure of the State Emergency Management Process* [in] Foundations of Management - International Journal, Vol. 5, No. 3, 2013, pp. 49-60.

[18] Ostrowska T., Krupa T. - *Przetwarzanie zasobów w sieciach technologicznych* (Processing of resources in technology networks) [in] Logistyka 5/2014.

[19] Prońko J., Wiśniewski B., Wojtuszek T. - *Kryzys i zarządzanie* (Crisis and management). Wyższa Szkoła Administracji w Bielsku-Białej, Bielsko-Biała 2006.

[20] Pyznar M. - *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa* (The National Programme for Critical Infrastructure Protection in the protection of this infrastructure - a vision of the Government Security Centre) [in] Ochrona infrastruktury krytycznej, red. A. Tyburska, Szczytno 2010.

[21] Wiśniewski B. - *Reguły ochrony obiektów infrastruktury krytycznej w warunkach zagrożenia dywersją* (Rules to protect critical infrastructure in potentially sabotage) [in] Ochrona infrastruktury krytycznej, red. A. Tyburska, Szczytno 2010.

[22] Zawiła-Niedźwiecki J. - *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji* (Operational risk management in ensuring the continuity of the organization). Wyd. edu-Libri, Kraków 2013.

[23] Zawiła-Niedźwiecki J. - *Analiza ryzyka operacyjnego z perspektywy teorii organizacji* (Analysis of operational risk from the perspective of organization theory). Uniwersytet Szczeciński, Zeszyty Naukowe Wydziału Nauk Ekonomicznych i Zarządzania, seria: Finanse, Rynki Finansowe, Ubezpieczenia, nr 51 (2014).

[24] Zawiła-Niedźwiecki J. - *Dualne naukowo postrzeganie zarządzania kryzysowego* (Dual scientific perception of crisis management) [in] Logistyka 6/2014.

[25] Zawiła-Niedźwiecki J. - *Analogie zarządzania kryzysowego z zarządzaniem ryzykiem operacyjnym przedsiębiorstwa* (Analogies crisis management with the business operational risk management) [in] Logistyka, nr 5/2014.

[26] Zawiła-Niedźwiecki J. - *Ciągłość Działania Organizacji* (The continuity of the organization). Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.

[27] Zawiła-Niedźwiecki J. - *Metodyka analizy ryzyka w ochronie infrastruktury krytycznej państwa* (Methodology of risk analysis, protection of critical infrastructure in the state). Uniwersytet Szczeciński, Zeszyty Naukowe Wydziału Nauk Ekonomicznych i Zarządzania, seria: Finanse, Rynki Finansowe, Ubezpieczenia, nr 65 (2014).

[28] Zawiła-Niedźwiecki J. - *Operational risk as a problematic triad: risk – resource security – business continuity*. edu-Libri, Kraków 2014.

[29] Zawiła-Niedźwiecki J. - *Zapewnianie bezpieczeństwa transportu, jako systemu infrastruktury krytycznej państwa, w konwencji triady ryzyka operacyjnego* (Ensuring the security of transportation, as a state system of critical infrastructure in conventions of an operational risk triad). Logistyka, nr 3/2014.