Wiśniewski, Michał

Article

Concept of situational management of safety critical infrastructure of state

Foundations of Management

Provided in Cooperation with:
Faculty of Management, Warsaw University of Technology

Suggested Citation: Wiśniewski, Michał (2016) : Concept of situational management of safety critical infrastructure of state, Foundations of Management, ISSN 2300-5661, De Gruyter, Warsaw, Vol. 8, Iss. 1, pp. 297-310, https://doi.org/10.1515/fman-2016-0023

This Version is available at:
https://hdl.handle.net/10419/184610

Foundations of Management, Vol. 8 (2016), ISSN 2080-7279
DOI: 10.1515/fman-2016-0023

CONCEPT OF SITUATIONAL MANAGEMENT OF SAFETY CRITICAL INFRASTRUCTURE OF STATE

Michał WIŚNIEWSKI

Warsaw University of Technology, Faculty of Management, Warsaw, Poland
e-mail: Michal.Wisniewski@pw.edu.pl

Abstract: This article presents a synthesis of knowledge about safety management procedures for critical infrastructure (CI) in the context of risk management theory and the provisions of the Polish law on emergency management of 26 April 2007. In this paper, the inadequacy of the accepted procedures at present is highlighted, as well as their continuous improvement and adaptation to prevailing political, legal, social and economic conditions. It proposes using the concept of scenario approach and situational management approach and technique analysis of interconnected decision areas (AIDA) and case-based reasoning (CBR) to develop integral situational resource model CI. The considerations presented in this paper lead to a proposed a new method for predicting, preventing and responding to emerging crises within the CI.

Keywords: critical infrastructure, situational approach, analysis of interconnected decision areas, case based reasoning, crisis management, threat, risk assessment, scenario of events, a domino effect, flat and hierarchical decision problem.

1 Introduction

The development of civilization provides many solutions that lead to the effective functioning of the state and the comfortable life of society. The observed improvement applies to the entire space in which it operates modern man (technical solutions, the sphere of information, and services provided). The effect of constant changes felt by the public security level is defined as a condition in which people (society) are confident that they do not threaten them with no adverse events due to unpredictable events (natural) or non-random (intentional), which constitute an obstacle to sustainable development and normal existence" (Sobolewski, 2010, p.46). Simultaneously,constant progress of civilization leads to the reliance of the population of the wider infrastructure, that is,manufacturing plants, power system, the communication system of health care, water supply, and food.One of these entities is the so-called critical infrastructure (CI), which is defined in Act of 26 April 2007 on *crisis management* as systems and their constituent functionally interconnected objects, equipment, installations, and services essential for the security of the state and its citizens, which have to ensure the efficient functioning of public administration, institutions, and businesses (Dz. U. 2013, Item 1166, Article 3, § 1, as amended).

Suitablelevel of services (functionality) provided by CI systems is a necessary conditionfor the stability of economic development, national security, the functioning of the state administration and local government, and increasing the standard of living of the population. Unavailability of functionality CI or too low level gives rise to serious economic loss or a real threat to life and health of the population. For this reason, the objects considered as CI should be given particular protection across to ensure the appropriate level of functionality CI systems.

The correct level of functionality CI, understood as the certainty and reliability in operation, can be achieved through the application of adequate security model against identified threats, which are susceptible objects CI. Objects CI,because of the implemented the functions, are grouped into CI systems, also defined in the Act on Crisis Management (Dz. U. 2013, Item 1166, Article 3, § 2, as amended). Each CI system is characterized by some set of risks specific to projects through its objects functionality. It should also be noted that the CI systems are not isolated from each other and interact to form a network of relationships. Interdependence contributes

to the susceptibility of infrastructure to dangers present in other CI systems.

Differentiation of constituents of the systems CI prevents the use of a universal security model that ensures the required level of functional objects CI. Additionally, the interdependence of systems CI makes it difficult to recognize threats before, which should protect objects CI (Korzeniowska, pp.19-20). Process safety management CI complicated by the need to take into account the level of functionality (situation) objects CI, changing over time and as a result of the impact of threats. Regulations that are in use in Poland do not indicate standardized method of procedure for the management of safety CI, which complicates reporting and coordination between the administrative levels involved in the decision process models security against threats (Krupa, Wiśniewski, 2015b, pp.1027-1034).

Because of the close links between the CIs, there is a need to indicate the integrated system of concepts and methods of operation that will be suitable for any CI system. Allowing reflect the situation (level of functionality) CI objects and make decisions intended to ensure a predetermined level of security, taking into account the impact of these decisions on related systems CI.

With the introduction, three problems that emerge form the basis for the considerations contained in the article:

1) What kind of threats, including scenarios domino effect[1], is susceptible to analyzed piece of CI?
2) What security model is to be applied in relation to the identified hazards?
3) How to verify the effectiveness of the applied security model?

2 The current system of critical infrastructure management in Poland

State infrastructureis classified as CI based on the sectoral and sectional criteria (Dz. U. 2013, Item 1166, Article 6, § 1, as amended). Act on crisis management, hereinafter referred to as the Act, divides CI objects into 11 systems. In case of the European Union Civil Protection Mechanism, there is also a mark out additional system – Protection of National Heritage. This is interesting because it points out the need to build an open management methodology for CI.

The current model of the CI security management is based on Report a Threat to National Security (RTNS). According to the Act, the obligation to prepare RTNS have Ministries (18 reports), central offices (6 reports), and governors (16 reports) (RCB, 2013b, p.8). In this process, counties and municipalities can optionally participate. Discretionary, preparation of RTNS by the level of county and municipalities can cause difficulties in the collection of reliable data regarding hazards occurring at the various administrative levels and aggregation of data between these levels.

The Government Centre for Security is the coordinator of the RTNS developing process, which on the basis of the collected RTNS creates the so-called National Crisis Management Plan (NCMP). Subsequently, this document is submitted to the Council of Ministers, which shall accept it in the form of resolution. Conclusions from RTNS and NCMP are the base for the development of Emergency Management Plans (EMP)at all administrative levels (central, ministerial, provincial, county, municipal, CI operators). Under the existing CI security management procedures, National Critical Infrastructure Protection Program (NCIPP) defines the roles and responsibilities for the protection of CI (Krupa, Wiśniewski, 2015a, p.94).

The CI operators, who for the most part are private entrepreneurs (RCB, 2013, p.6), do not have a statutory obligation to prepare RTNS; however, the Act imposes an obligation to protect the CI systems through the preparation and implementation of the EMP (Dz. U. 2013, Item 1166, Article 6, § 5, as amended).

The disadvantage of the current CI security management system is the fact that arising within its framework documents,define the tasks, deadlines, and units responsible for their execution,however, there is neither unified system of concepts nor identi-

[1] Domino effect is the sequence of events to initiate the occurrence of the first one, in which each successive event will occur next. It is the direct cause of the spreading crisis events and the escalation of their effects (Kosieradzka, Zawiła-Niedźwiecki, 2016, p.361).

fied methods that the participants should use in this process. In combination with the different characteristics of11CI systems highlighted in the Polish legislation, it leads to discrepancies in the methodology and quality of EMP as well as hinders the identification of the correct security model. Also EMP do not include the functional level of the analyzed fragments of CI.

The above-mentioned problems have led to the development of the concept adopting that a unified conceptual system can be applied in the case of any CI system and a set of actions that allows to choose a proper security model for the identified threats. The proposed concept, with respect to the selection of the security model, also takes into account the level of functionality of the analyzed CI fragments and CI correlation systems. Hence, it is called the situational safety critical infrastructure management (SM-SCI).

3 Existing theoretical approaches used by SM-SCI

Risk management is a part of the diagnosis and control processes that aim to ensure stability and the conditions for the further development of the organization (Zawiła-Niedźwiecki, 2013). Current management concepts, derived mainly from the area of the organization of production at the companies, can be successfully applied in the areas such as banking, insurance, and trade. Using the analogy between the risk management process in enterprises and the CI safety management process, one can assume that they will also be suitable in this area. Concepts that seem to be particularly predisposed to support the CI safety management process are:

- scenario (Daszyńska-Żygadło, 2012) and situational (Wajda, 2003, pp.48-50) approach – in the context of recognition of the threat for analyzed CI fragment,
- analysis of interconnected decision areas (AIDA) method (Krupa, Ostrowska, 2012) – in the context of indication of the adequate model for the protection against threats,
- case-based reasoning (CBR) method (Yoon, et al., 2016) – in the context of the security model verification.

In the area of risk management, scenario approach is used as a way to prepare a plan of action in order to recover from external shocks and to get a balance after its occurrence (Worthington, et al., 2009, p.444). An external shock refers to the existence of the threat to which an analyzed CI object is exposed, that is, a terrorist attack, natural disaster, a crash in the CI system, and so on. On grounds of the list of hazards occurring in the scenario, a security model may be identified, in which the kinds of forces and a number of measures designed to prevent the identified risks should be specified, in order to reduce their impact or restore the functionality of the CI object. The need for scenarios development is indicated in CIPP (RCB, 2013). Currently, domino-effect scenarios are prepared by experts and are based on their experience.

Scenario approach enables the identification of the risks, on which CI objects are susceptible. Indication of these risks is the basis for determining the level of a risk. The impact on the risk index also has a functionality level implemented by the CI object. The reaction to the threat will look different in a high and a low availability of CI functionality. This relationship is determined by Equation (1) shownin the latter part of this article. Expanding the system of termsof scenario approach with situational elements, it is possible to take into account the functionality (situation) level of CI object in the decision-making process concerning the protection model against identified threats.

The main assumption in the situational approach is that the reality is too complex to apply universal methods of operation that are effective under different conditions (Wajda, 2003, p.48). This opinion is confirmed by Hamrol (1998, p.68), adding that the organizations are complex systems with unlimited collection of internal and external connections. There is no identical situation in which the standard solutions can be directly applied. Only after the analysis of the situation, the choice of adequate solutions can be made, what allows for the determination of their one-off effectiveness.

Formulation of a model solutions set for CI safety management process requires the knowledge in (Krupa, Wisniewski, 2015b, p.1028):

- resource open to risks,

- internal and external threats,
- links between threats,
- the effects of incidents,
- procedures and tools used for the reduction of not convenient situation and showing how to restore the status prior to its occurrence.

Particularly useful in the context of the CI safety management process, management of situational approach was presented by Klykow and Jurek (1988, p.71). He defines the situation as a set of nodes connected to each other, which map the relationships between nodes, forming the structure of the situation. The nodes represent the elements of the modeled reality and can represent other situation structures, what allows for the construction of hierarchical structures. The possibility of modeling hierarchical structures is desirable in the concept of the SM-SCI because of the fact that part of the decision concerning security models should be made at various levels of state and local administration and the CI operators themselves. Assumptions for the situational approach can be used to build the structure of the analyzed CI fragment, including the functionalities and CI facilities and threats that affect them. Determination of the structure of the analyzed CI fragment creates a possibility for pointing out a domino-effect scenario that might play a role in it.

Indication of a proper security model is a decision-making process thatmay be assisted by AIDA method and verified by CBR method. The use of AIDA method involves three steps. The decision problem model is created under which (Krupa, Ostrowska, 2012, p.26):

- decision-making areas and elementary decisions are assigned,
- a pair of elementary decisionsthat are in relationship full of contradictions are selected,
- the relative weight of significance Vi of the decision-making areas Diin a percentage scale and the weight of the relative significance vji (relative costs to the sum of 1 in every decision-making area Di) in elementary decision DJs on the scale (0..1) are assigned.

Then a set of permissible decisions free of pairs of elementary decisions being in a relationship full of contradictions is generated. The last step involves the assessment of the relative cost of all properly formed decisions and organizing them in a descending order of relative costs, analysis of obtained solutions, and the selection and implementation of decisions.

In the case of CI safety management process, the assumption that the risks occurring in the domino-effect scenario aredecision-making areas within which the decision-making problem and elementary decisions are interpreted as a possible protection against identified threats must be done. Thus, indication of the decision in the context of the analyzed problem is equal to the proposition of a security model before identification of threats in thescenario.

Verification of the effectiveness of the security model can be doneby the implementation of the CBR method. This method refers to the expert reasoning thatis seeking to solve the problem by using the experience from the past and creates his or her decision in respect to the decisions made in the past. CBR method determines the case as a pair of the problem and its solution (threat and protection model). Cases are independent, they are not rules, they are records of actual events initiated in specific situations that may be described with the appropriate data set (Yoon, et al., 2016). The essence of the CBR method shows that it is possible to solve the current problem by adapting the solutions used in the past.

Application of this method in the CI safety management process requires showing the criteria of similarityof the situation in which the analyzed CI fragment is. This gives the ability to compare a specific domino-effectscenario with cases taking place in the past. Therefore, it is possible to determine whether the adopted security model will bring the desired effect.

4 CI resource model

Domino-effect scenarios are accomplished in a system of interconnected objects. Taking as a starting point a country and share its components intothe elementary parts, it should be noted that the basis of any system are resources. Resources can be divided into two groups: actual (machines, facilities, tools, components, semi-finished products) and abstract (data, information, knowledge). Regardless

of the category, resources can be described as a set of functions and the risks to which it is vulnerable. The attribute describing the threat is, for example, a security model. This allows to propose a CI resource model (Fig. 1).

The implementation of the CI resource model enables mapping of any CI fragment, including its situation (functionality level) anda course of domino-effect scenario prediction. CI resourcemodelis characterized by openness. It means that without changing the terms and concepts used in the system, model can be supplemented with new elements and used to describe any CI system at any administrative level (CI operator, municipal, county, provincial, ministerial, and central).

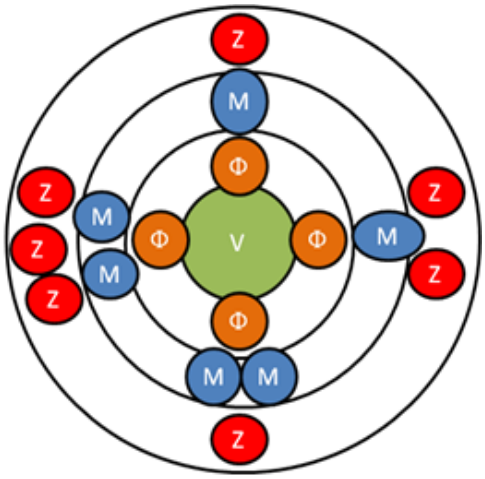

Figure 1. CI resource model
(*source:* own materials)

The resource functionalities are susceptible to the threats. Based on the analysis of the resource functionality, it is possible to identify a list of threats on which the resource is susceptible. Because the CI systems are composed of interrelated resources, the sum of the risks of system resources is also a list of threats for analyzed CI system. This approach will allow CI systems analysis in the terms of threats to the national security, which is required by the Act (Dz. U. 2013. Item. 1166, Article 5, as amended), and, at the same time, will be possible to conduct analyzes for other risks, for example, in the case of enlargement of the threats catalog to national security in the future.

There are connections between resources that can be defined as a virtual channel that connects two resources (Krupa, 2015b, p.7799). Knowledge of the organization process in which a resource is used in combination with the knowledge of the resource functionality, allow for the identification of links between resources. On this basis, the structure of the analyzed system is mapped, and by supplementing it with the current value of the resources functionalities, it is possible to determine the system situation. SM-SCI also allows the identification of relationships between threats based on analysis of historical domino effect scenarios.

5 Description of CI resources and acting on threats

The resource is interpreted as a piece of material reality (physical) or virtual (e.g., conceptual, informational, metalinguistic) with a nonempty set of functionality and a specific range of functionality. Resources to facilitate the analysis and the process of building the structure of CI system should be grouped in clusters. A cluster means a resource with the same set of functionality and the same range of permissible functionality values. It will allow for building clusters with a common security models. Basic attributes that make up the description of the resource are shown in Table 1.

Table 1. Basic attributes of the resource
(*source:* own materials)

Attributes	Symbol	Scale
Resource name V-type x index α	V^{x}_{α}	–
Threat Z of the index β y-type for the resource index α	$Z^{y}_{\alpha,\beta}$	–
FunctionalityΦindex γ resource x-type index α	$\Phi^{x}_{\alpha,\gamma}$	[0..100]%
Level of susceptibility the resource type U x index α the threat index β	$U^{x}_{\alpha,\beta}$	[0..1]

Threats are a component of the resource description. The term threat is defined as the expected impact on resources as a result of which their qualities – structural properties – may be degraded. Threat can also be classified into types. Threat type is a collection of threats with the same set of effects and the same range of permissible effects values. Basic attributes that make up the description of the threat are shown in Table 2.

Table 2. Basic attributes of the threat
(*source:* own materials)

Attributes	Symbol	Scale
Threat name Z y-type index β	Z^{y}_{β}	–
Effect C occurthreat y-type index β	C^{y}_{β}	[0..100]%
Probability P occur threat y-type index β	P^{y}_{β}	[0..1]
Protection model M index λ against the threat of the y-type index β	$M^{y}_{\beta,\lambda}$	[0..1]

There are two main types of threats: external – collection of threats (Z^{O}_{β})influencing on at least one of the system resources, not invoked by the resources of this system – and internal – a set of threats(Z^{T}_{β}) affecting the functionality of the system resources as a result of failure of another resource of this system. External and internal threats affect the resources byprocess structures in which the primary role is played by sequences of discrete events executing on virtual channels formed by pairs <susceptibility>:<result> determining the functional-structural condition of the resource V^{x}_{α} (Krupa, 2015b, p.7799).

6 Identification links between resources and threats

Taking advantage of the fact that resources are organized asa system, it is possible to determine the mutual influence of resources and recognize the threat, for example, constant drought reduces the availability of water needed to cool the power unit, whichleads to its overload and failure or even deliberate exclusion. Table 3 shows a relationship between the CI system resources. In column 1, all system resources (V_{α}) are presented. Starting with column 2 untill column N, dangers (Z^{T}_{β}), that are susceptible to system resources are shown. Subsequently, in the appropriate fields of the column 2, following information are included:

- resource $V_{\alpha'}$, on which resource V_{α}has an influence as a result of the threat Z^{T}_{β}, probability P of a danger Z^{T}_{β},
- susceptibility Uof the resource $V_{\alpha'}$ on the threat Z^{T}_{β}, lowered by the impact of protection instruments Mused for resource $V_{\alpha'}$,
- Q value representing the ratio of the probability of hazard occurrence Z^{T}_{B} and the susceptibility of resource$V_{\alpha'}$ on the threat Z^{T}_{β}, withthe assumption that the susceptibility of the expected impact of security M is lowered. Column N includes a checksum that shows whether the probability of the risks associated with resource V_{α}add up to 100%.

Table 3. A conceptual notation of impact of threats on the CI system
(*source:* own materials)

Specification	**Internal threats (Z^T_β)**			**Checksum**
Column no. 1	Column no. 2		…	Column no. N
Resource (V_α)	Reosurce $V_{\alpha'}$	U – M	…	Sum P (100%)
	P	Q = P* (U – M)	…	

Using the principles of the description of the internal threats impact on CI resources, a description of the external threats impact on the analyzed CI system can be performed.

Collected data about the resources and threats allows for mapping the structure of the analyzed CI system and determination of the system situation. The situation is understood as a state of analyzed resource or the system as unity, determined by the values of functionality. Situation of the CI fragment is determined as a set of resources $V\{V^x_1, \ldots, V^x_n\}$ connected with each by threats $Z\ \{Z^y_1, \ldots, Z^y_n\}$. Those connections are numbered, and the numbers of connection correspond to the indices of threats B. An example of the CI structure system that takes into account the internal and external threats impact is shown in Fig. 2.

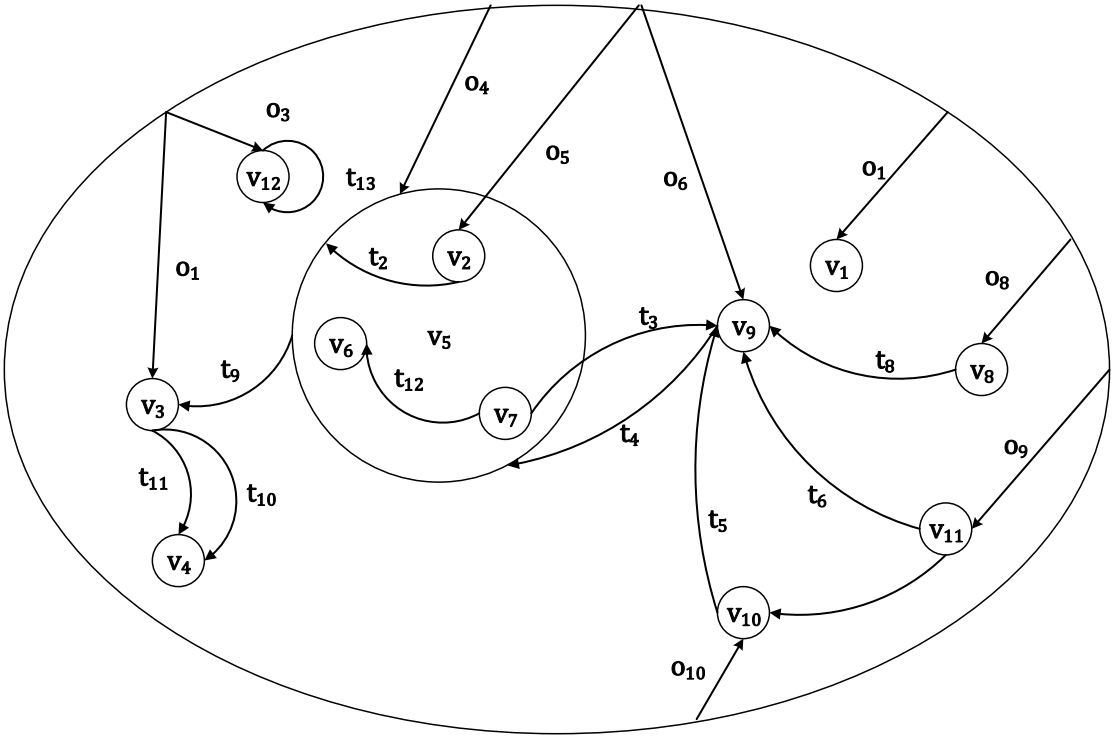

Figure 2. Graphical representation of the full structure of the situation CI system
(*source:* own materials)

Development of an external threats and internal structures of the CI system is a base for the determination the state of the analyzed system. By assigning individual resources V_α, values that describe the functionality of the resource, it is possible to determine the situation of the system and assess the risks faced by individual resources, parts of the system, or its entirety. Functionality values can be recorded via sensors, or in the case of a technical failing, they can be determined by experts.

The next step is to prepare the domino-effects scenarios that are possible to occur in the CI system. Especially useful tool to indicate the threats spreading scenarios are graphic diagrams illustrating potential dispersion of the negative events (Fig. 3).

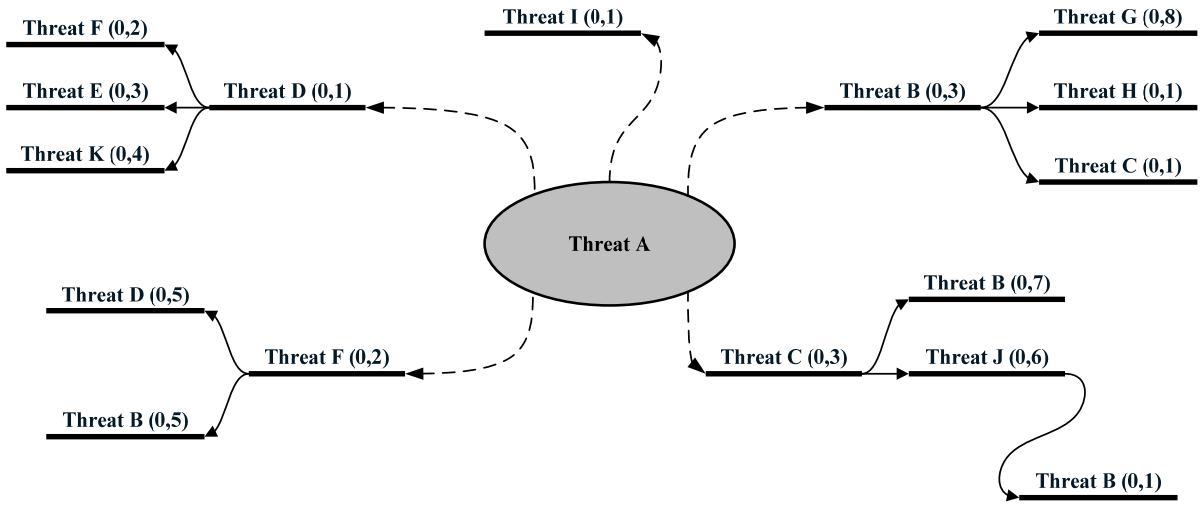

Figure 3. Graphic record of the possible consequences of the materialisation of the threat Z^T_1
(source: own materials*)*

The threat Z^T_1 symbolizes the drought, which may cause a threat Z^T_6 – a failure of a power unit that can lead to a danger Z^T_4 – closing the hospital. Another way of describing a materialization scenario of the threats is a text description. Its disadvantage is a lowerclearness in relation to the graphical scheme. However, it allows for the inclusion of more detail data describing the events. The best solution is to use the mixed method. Creation of a list of negative events scenarios for the CI system is a base for the preparationof a model of the decision-making process, which result with the protection model for the threats included in the scenario.

7 Estimation of Risk

Owing to the limited resources, it is necessary to definethe most important responses to the identified risks. This hierarchy can be determined using a risk indicator. Using the attributesthat describe the resources and the threats, it is possible to estimate the level of the risk (R) and the functionality of the individual components as well as the whole domino-effect scenario. Risk is defined as a numerical value that express the percentage of the expected loss of functionality on the channels of the highlighted resource or set of resources, which may arise as a result of threats. The value of the risk associated with a given scenario can be calculated according to Equation 1 (based on Krupa, 2014, p.31):

$$R = P * \Phi * (U - M) \quad (1)$$

where:

R – is the level of the risk on the scale [0..100]%,

P – is the probability of threats on the scale [0..1],

U – is the susceptibility of resource to the threat on the scale [0..1],

Φ – is thelevel of functionality of the resource [0..100]%,

M – is the impact of the security on the susceptibility of resource to the threat on the scale of [0..1].

It is recommended to introduce a five-point scale of risk (Krupa, 2014, p.31):

- acceptable level [0..20)%,
- warning level [20..40)%,
- conditionally acceptable level [40..60)%,
- unacceptable level [60..80)%,
- crisis level [80..100]%.

Acceptance of the above-mentioned scale of the risk ensures the consistency of the SM-SCI with the Methodology for risk assessment required by the crisis management RP (Skomra, et al., 2015).

Percent effects record of the channel $(U/\Phi)^{x}{}_{\alpha,\beta}$[2] is defined as a percentage loss of resource functionality as a result of the actual implementation of the event described in this threat.According to this clause, the sum of the functionality loss effects on all channels $(U/\Phi)^{x}{}_{\alpha,\beta}$ for considered CI resource in the model calculation and in the procedure method can exceed the value of 100%, even several times, although the actual loss of anticipated CI functionality resource does not exceed 100%, even as a result of physical liquidation of the resource (Krupa, 2015b, pp.7799–7800).

Functionality is a numerical value expressing the percentage of the availability degree of services provided by the resource or CI system. The level of service availability is determined by measurements or estimations of experts. It is proposed to adopt a four-level scale of functionality:

- acceptability level [100..75)%,
- warning state level [75..50)%,
- state of emergency I level [50..25)%,
- state of emergency level [25..0]%.

Using the formula for the risk, it is possible to determine the expected level of the resource functionality $V^{x}{}_{\alpha}$ in the next period. The value of the functionality in the period t_1 can be calculated using Equation 2.

$$\Phi_{t_i} = \Phi_{t_{i-1}} - R_{t_{i-1}} \tag{2}$$

where:

$\Phi_{t_{i-1}}$ – is the expected level of functionality in period t_{i-1},

Φ_{t_i} – is the measured /estimated level of functionality in the period t_i,

$R_{t_{i-1}}$ – is the level of the risk in the period t_{i-1}.

Level of the risk can be controlled by acting on the variables describing the threat (probability and consequence). However, CI system operator has a limited effect on these variables, thereby closing the way for effective reduction of the rick level by these methods.

Another way to reduce risk is to "strengthen the functionality" by applying protection models (e.g., alarm systems, emergency systems, increasing the number of physical resources) that increase the level of CI functionality and reduce the susceptibilityof resources to threats.

8 Construction of the protection model

A scenario of domino effect provides knowledge about risks against which we should be protected. Using the AIDA method, the decision-making D_j areas (Fig. 4) that correspond to the identified threats are defined. As a part of the decision-making areas, elementary decisions d_{ij} are marked symbolizing safeguards and tools useful for quick reaction on-threat. Next, a pair of security that cannot occur within one security model (elements connected with a solid line) should be defined.

The situation shown in Fig. 4 can be interpreted as a decision problem of the CI operator, who is supposed to indicate the security model for the specific functionality of the CI system, susceptible to the three identified domino-effect scenario threats (threat $Z^{T}{}_{1}$ symbolizes area D_1, the threat $Z^{T}{}_{6}$ symbolizes the area D_2, the threat $Z^{T}{}_{4}$ symbolizes area D_3). Decision problem can be represented as a matrix equation (Fig. 6), which solution lets to identify a set of securities that are in a good agreement with the accepted condition, for example,the smallest value of the relative cost assessment decision. For this purpose, decision-making areas (D_1, D_2, D_3) must be recorded in the form of vectors. The area decision D_1 will be defined as D_1 $\{d_{11},d_{21}, d_{31}, d_{41}\}$.

The same scheme should be implemented to the other decision-making areas. Having a vector record of decision-making areas, all tuples[3] that can be a solution for the problem should be indicated. Subsequently, from this set of tuples, those that contain contradictory pairs of security are removed.

[2] $(U/\Phi)^{x}{}_{\alpha,\beta}$is a contractual dependence of susceptibility to and result (an attribute describing threat), expressed in percentage [100]%, defining an actual degree of functionality of resource $V^{x}{}_{\alpha,\beta}$, where alpha α is the index of CI resource, x the type, β the index if threat (according to a principle that one of resource is connected to one or a few types of threat, the result of threat is changed proportional to the product of multiplication of the susceptibility to scale [0..1] and result to scale [0…100]%) (based on Krupa, 2014, pp 6,8).

[3] Tuple is a solution of decision problem that consists of number of elementary decisions D_{ij}, which is equal to number of m decision areas D_i with one elementary decision from every decision area D_i.

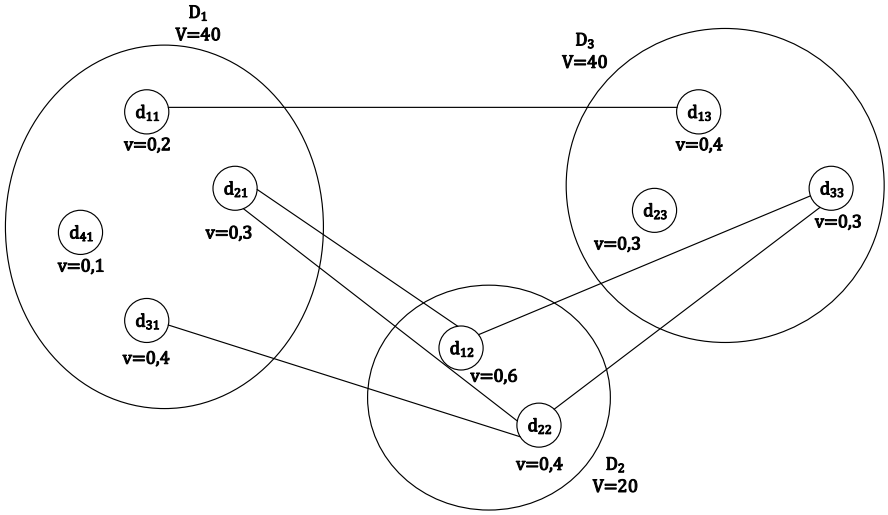

Figure 4. Example model of decision-making performed in the AIDA technique (*source*: own materials)

Conflicts of security can be a result of many different reasons, for example, in case of fire, if the electrical equipment is not disconnect from the current, fire cannot be extinguished with water. In another example, a contradiction may be due to the administrative decisions. After eliminating conflicting pairs, a list of possible security models ready to use is formed (Fig. 5).

d_{11}	d_{12}	d_{23}
d_{11}	d_{22}	d_{23}
d_{31}	d_{12}	d_{13}
d_{31}	d_{12}	d_{23}
d_{41}	d_{12}	d_{13}
d_{41}	d_{12}	d_{23}
d_{41}	d_{22}	d_{13}
d_{41}	d_{22}	d_{23}

Figure 5. Matrix of possible solutions to the problem of decision-making (*source:* own materials)

Putting numerical values in place of the elementary decision, a matrix of possible application models protection against threats is created. Multiplying this matrix by a matrix of individual decision-making areas V_j, a list of values for the different security models is obtained (Fig. 6).

0.2	0.6	0.3		40		32
0.2	0.4	0.3		20		28
0.4	0.6	0.4		40		44
0.4	0.6	0.3	*		=	40
0.1	0.6	0.4				32
0.1	0.6	0.3				28
0.1	0.4	0.4				28
0.1	**0.4**	**0.3**				**24**

Figure 6. List of the relative value of cost solutions to the problem of decision-making (*source:* own materials)

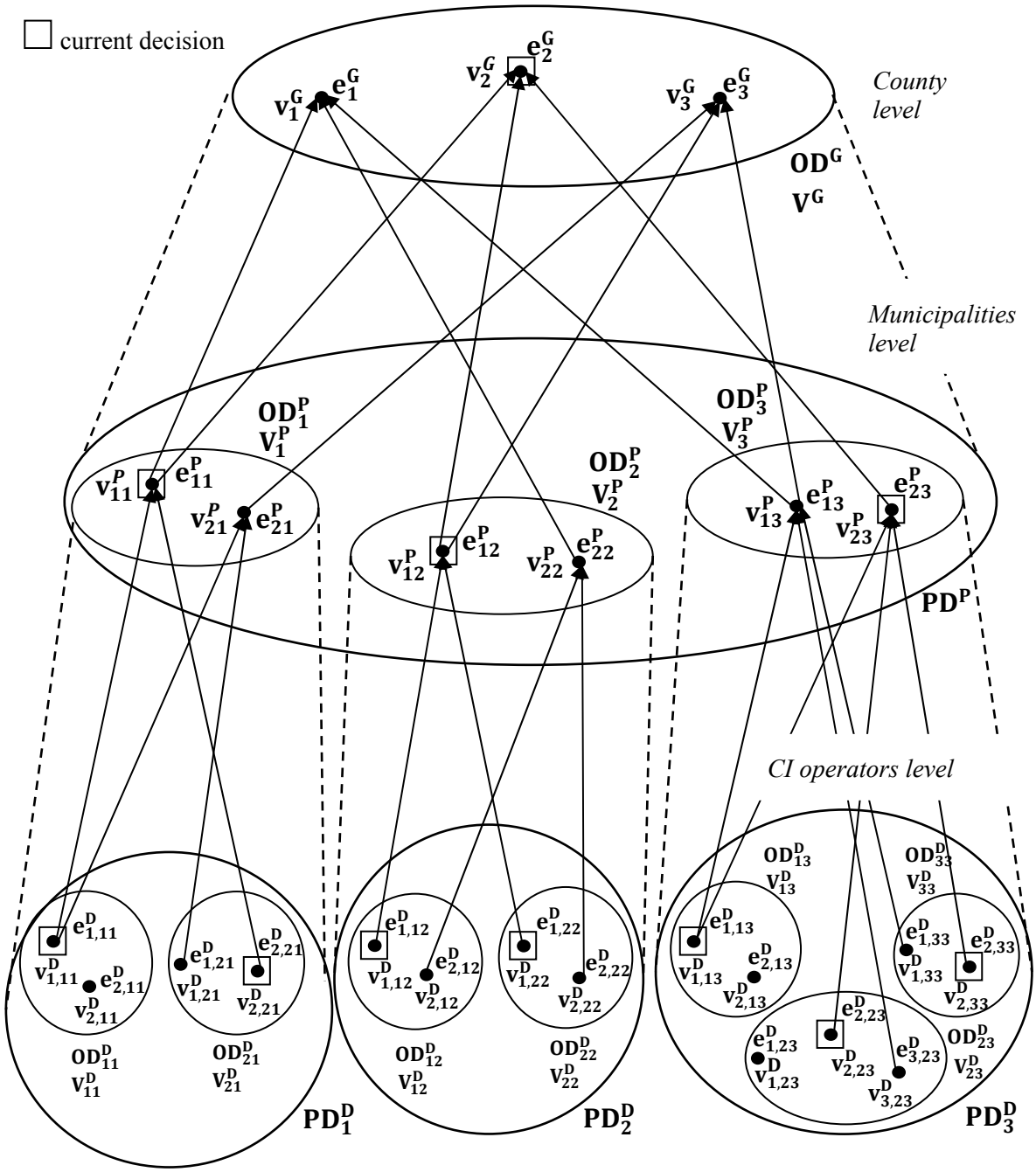

Figure 7. Example of a hierarchical decision-making problem
(*source:* Krupa, Ostrowska, 2012; Krupa, Ostrowska, 2016)

In the analyzed case, protection model against threats Z^T_1, Z^T_6, and Z^T_4 looks as follows. The reaction to the threat Z^T_1 is the elementary decision d_{41}, which symbolizes the construction of the storage reservoir. The reaction to the threat Z^T_6 is the elementary decision d_{22}, which symbolizes the purchase of electricity from other power plant in order to relieve its own devices. The reaction to the threat Z^T_4 is the elementary decision d_{23}, which symbolizes the hospital supply with an autonomous power generator.

Implementing the above-mentioned assumptions, flat and hierarchical decision-making problems can be solved. Flat decision-making problem in the case of the CI security issues occurs when the decision to use the security model can be identified and implemented on a single administrative level, for example, on the competence level of the CI operator.

Another type of decision problems in the case of CI is the situations in which the risk is on the same decision-making level, for example, the CI operator level and the response to the threat requires the involvement of forces that are governed by a local government administration. Then we have to deal with the hierarchical decision-making problem (Fig. 7).

Computational complexity of flat decision-making problems depends on the number of decision-making areas and elementary decisions and is expressed as the product of these two values. In the case of hierarchical decision-making problems, the complexity level increases as a result of the need of an iterative calculations, caused by the influence of the elementary decisions from higher levels on the solutions from lower levels and vice-versa.

As in the case of flat decision-making problems, the solution for hierarchical decision-making problem is the system of equations in which the values of the elementary level of the higher lever are determined by the sum of the products of the values of the elementary level of lower level and weights of the decision-making area of origin. This is illustrated in the following set of equations, which shows the relationship between the elementary decisions ofthe county level and the elementary decisions of themunicipalities' level. The whole hierarchical decision-making problem is illustrated by the system of equations shown in Fig. 9.

$$v_1^G = (V_1^P * v_{11}^P) + (V_2^P * v_{22}^P) + (V_3^P * v_{13}^P)$$
$$v_2^G = (V_1^P * v_{11}^P) + (V_2^P * v_{12}^P) + (V_3^P * v_{23}^P)$$
$$v_1^G = (V_1^P * v_{21}^P) + (V_2^P * v_{12}^P) + (V_3^P * v_{13}^P)$$

Presented system of equations can be written in the form of a matrix, which will facilitate the use of iterative calculations required in the case of hierarchical decision-making problems (Fig. 8).

v_{11}^P	v_{22}^P	v_{13}^P		V_1^P		v_1^G
v_{11}^P	v_{12}^P	v_{23}^P	*	V_2^P	=	v_2^G
v_{21}^P	v_{12}^P	v_{13}^P		V_3^P		v_3^G

Figure 8.The matrix record of ratio of values of elementary decisions of county level and values of elementary decisions of municipalities' level
(*source:* own materials)

Depending on the county level – the level of municipalities
Decision problem OD^G

v_{11}^P	v_{22}^P	v_{13}^P		V_1^P		v_1^G
v_{11}^P	v_{12}^P	v_{23}^P	*	V_2^P	=	v_2^G
v_{21}^P	v_{12}^P	v_{13}^P		V_3^P		v_3^G

Depending on the level of municipalities—level of CI operators
Decision problem $OD^P{}_1$

v_{111}^D	v_{221}^D		V_{11}^D		v_{11}^P
v_{111}^D	v_{121}^D	*	V_{21}^D	=	v_{21}^P

Decision problem $OD^P{}_2$

v_{112}^D	v_{122}^D		V_{12}^D		v_{12}^P
v_{212}^D	v_{222}^D	*	V_{22}^D	=	v_{22}^P

Decision problem $OD^P{}_3$

v_{113}^D	v_{323}^D	v_{133}^D		V_{13}^D		v_1^P
v_{113}^D	v_{223}^D	v_{233}^D	*	V_{23}^D	=	v_2^P
				V_{33}^D		

Figure 9. Example for matrix record of hierarchical decision-making problem
(*source:* own materials)

Applying this principle to all decision-making levels of the hierarchical decision-making problem, a matrix equation is obtained (Fig. 9). The equation, which starts from the equation mapping the lowest level, comes to the values of elementary decisions of the highest level. In other words it solves a hierarchical problem of decision.

The solution depends on the assumed objective function (maximum value, minimum, value in a range of the relative cost-decision assessment).

9 Verification of protection model

Using the assumptions of SM-SCI model, it is possible to find similar cases in the database and verify if the selected protection model allows to maintain an appropriate level of CI functionality system. Criteria of situation similarity may relate to:

- resources,
- internal and external threats,
- protection models,
- levels of system functionality or,
- be any combi
- nation of the above mentioned elements.

Therefore, a condition of effectiveness (Equation 3) of the security model for the management process of the CI situational safety can be created.

$$\begin{cases} K \leq R \\ \Phi_{t_i} \geq \Phi_{min} \end{cases} \quad (3)$$

where:

K – is the cost of the security model,

R – is thepredicted value of the risk scenario (interpreted as the potential costs of materialization of threats),

Φ_{t_i} – is the expected level of functionality in the period t_i,

Φ_{min} – is the minimum level of functionality or system resource considered to be acceptable.

10 Summary

The aim of the article is to present the concept of the situational management of the CI safety based on the model of the CI resource, which allows to map the composition of the analyzed system, including objects and threats associated with them, possible to use in any CI system and at every administrative level (CI operator, municipal, county, districts and central). Development of the structure of the analyzed CI fragment allows for the proper choice of domino-effect scenario and the threats to which CI is prone to. This is the basis for the selection of the protection model that allows CI to function at a given level.

The novelty in presented SM-SCI conceptis a reference to the threats collectivescoming from the domino-effect scenario and linking a model of protection against the threat with registered functionality level of the affected CI fragment (Equation 3). The SM-SCI concept allows indicating the decisions for using a protection model in the case of flat and hierarchical decision-making problems. The proposed approach involvesthe current principlesapplicable to protect the CI in Poland and the European Union, at the same time, remaining open to the changes that will take place in the future, that is, extension of the list of threats to national security, amend the list of CI systems.

The need of development of the SM-SCI concept has been demonstrated as a results ofresearch carried out in the framework of the development project NCBiR – "Highly specialized platform supporting civil emergency planning and rescue services in polish public administration and organizationalThe National System of Rescue and Fire Protection units" Agreement No. DOB - Bio7/11/02/2015 forthe execution of projects in the fields of research and development projects for national defense and security, carried out by the consortium: Warsaw University of Technology (Faculty of Management), Medcore sp. z oo. Studies have shown that the use of the CI resource model will increase the efficiency of use of the data about negative events occurring in the past and systematize the CI safety management process. In addition, it will be a useful tool for experts for verification and elimination of methodical discrepancies for the development of plans to protect the CI because of differences in the CI systems.

11 Bibliography

[1] Daszyńska-Żygadło, K., 2012. *Podejście scenariuszowe w zarządzaniu ryzykiem (Scenario approach in risk management*). In: Annales Unicersitatis Mariae Curie-Skłodowska, Vol. 46(4).

[2] Hamrol, A., 1998. *Zarządzanie jakością. Teoria i praktyka (Quality management. Theory and practice)*.Warsaw: PWN.

[3] Klykow, J., Jurek, J., 1988. *Dialogowe semiotyczne systemy podejmowania decyzji (Dialog semiotic decision-making systems)*. Warszawa: PWN.

[4] Korzeniowska, S., *Cyberbezpieczeństwo infrastruktury Krytycznej (Cybersecurity for Critical Infrastructure)*, LSW – Leśnodorski Ślusarek andPartner, [online] Available at: www.lsw.com.pl [Accessed 29 August 2016].

[5] Kosieradzka, A., Zawiła-Niedźwiecki, J. (ed.), 2016. *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym (Advanced methods of risk assessment in the public crisis management*). Cracow: edu-Libri.

[6] Krupa, T., 2014. *Model zależności ryzyka bezpieczeństwa narodowego od zmian poziomu bezpieczeństwa IK (Depending on the model of national security risks from changes in the level of securityCI)*. Product design Methodology of risk assessment for the purposes of crisis management system RP.

[7] Krupa, T., 2015. Semiotyka kluczowych pojęć tezaurusa ciągłości działania w infrastrukturze krytycznej (Semiotics of the key concepts of critical infrastructure business continuity processes). *Logistyka* (*Logistics*), No 4, pp.7793-7802.

[8] Krupa, T., Ostrowska T., 2012. Decision-making in flat and hierarchical decision problems. *Foundations of Management*, Vol. 4, No 2, pp.23-36.

[9] Krupa, T., Ostrowska, T., 2016. Hierarchical Decision-Making Problems – Modeling and Solutions. *Foundations of Management*, Vol. 8, pp.311-324).

[10] Krupa, T., Wiśniewski, M., 2015a. Situational management of critical infrastructure resources under threat. *Foundations of Management*, Vol. 07, pp.93-104.

[11] Krupa, T., Wiśniewski, M., 2015b. Wykorzystanie wiedzy w zarządzaniu sytuacyjnym bezpieczeństwem infrastruktury krytycznej Polski (The use of knowledge in security of the Polish critical infrastructure of the situational management). *Logistyka* (*Logistics)*, No 5, pp.1027-1034.

[12] Rządowe Centrum Bezpieczeństwa (Government Center for Security), 2013a. Narodowy Program Ochrony Infrastruktury Krytycznej *(National Critical Infrastructure Protection Programme)*.Warsaw.

[13] Rządowe Centrum Bezpieczeństwa (Government Center for Security), 2013b.*Ocena ryzyka napotrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego (The risk assessment for crisis management. The report on threats of national security).*Warsaw.

[14] Skomra, W. (ed.), 2015. *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP (Methodology of risk assessment for the purposes of crisis management system RP).* Warsaw.

[15] Sobolewski, G., 2010. Zarządzanie kryzysowe wobec współczesnych wyzwań i zagrożeń (Crisis management to contemporary challenges and threats). In: Sobczak, E. (ed.), et al. *Nowe wyzwania i wykorzystanie współczesnej nauki w zarządzaniu kryzysowym (New challenges and the use of modern science in crisis management)*. Warsaw.

[16] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Act of 26 April 2007 on crisis management). Dz. U. 2013, Item 1166.

[17] Wajda, A., 2003. *Podstawy nauki o zarządzaniu organizacjami (Basics of management science organizations)*. Warsaw: Difin SA.

[18] Worthington, W., Collins, J., Hitt, M., 2009. Beyond risk mitigation: Enhancing corporate innovation with scenario planning. *Business Horizons*, No 52(5), pp.441-450.

[19] Yoon,Y., Jung, J., Changtaek Hyun, C., 2016. Decision-making Support Systems Using Case-based Reasoning for Construction Project Delivery Method Selection: Focused on the Road Construction Projects in Korea. *The Open Civil Engineering Journal*, Vol 10, pp.500-512.

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