Wiśniewski, Michał

Article

Methodology of situational management of critical infrastructure security

Foundations of Management

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

Suggested Citation: Wiśniewski, Michał (2020) : Methodology of situational management of critical infrastructure security, Foundations of Management, ISSN 2300-5661, De Gruyter, Warsaw, Vol. 12, Iss. 1, pp. 43-60, https://doi.org/10.2478/fman-2020-0004

This Version is available at:
https://hdl.handle.net/10419/237004

METHODOLOGY OF SITUATIONAL MANAGEMENT OF CRITICAL INFRASTRUCTURE SECURITY

Michał WIŚNIEWSKI

Warsaw University of Technology, Faculty of Management, Warsaw, POLAND
e-mail: michał.wisniewski@pw.edu.pl

Abstract: The article discusses the issues of the critical infrastructure security management from the perspective of entities responsible for its security and development of an integral model of critical infrastructure security, and shows the methodology of situational management of critical infrastructure safety. Proposed solutions are used for CI mapping, enabling the generation of adverse event scenarios, estimation of the risks dependent on the considered CI, and determination of decision problem, indicating a set of protection activities for elimination or reduction of the risk in the security threshold.

Keywords: crisis management, critical infrastructure, risk assessment, security threshold, adverse event scenario.

JEL Classification: H12.

1 Introduction

The development of civilization means that a single person cannot function in his own domain (as an individual or as a group) by undertaking supervision over his/her security, understood as an access to all goods – products and services that can guarantee basic human needs, for example, physiological or safety needs indicated in the Maslow's Pyramid. It leads to the explanation why the society is more and more dependent on the condition of infrastructure, particularly critical infrastructure (CI).

CI has been widely described in the literature. In Poland, it is referred to systems and their functionally interconnected objects, equipment, installations, and services essential for the security of the state and its citizens to ensure the efficient functioning of the public administration, institutions, and businesses (Dz.U. 2019, Item 209, Article 3).

The law of the European Union defines CI as an asset, system, or part located in a member state, which is essential for the maintenance of vital societal functions, health, safety, security, or economy. Any destruction or disruption may have a significant negative impact on the security and the well-being of citizens (Council Directive 2008/114/WE, Article 2b). The US (United States) law defines CI as those systems and assets, whether physical or virtual, which are so vital to the USA that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters (Presidential Policy Directive, 2013).

Regardless of the definition, CI entities are exposed to various types of threats related to human activities, natural disasters, and military, terrorist, or cyberspace attacks. Therefore, the ability to identify and predict threats toward CI entities and the capability to indicate how to proceed when they occur is nowadays a common subject of many research initiatives.

In the management of CI security, the following are currently observed:

- lack of a common conceptual system that allows to determine the characteristics of CI and the exchange of information between the entities responsible for CI security,
- lack of a dedicated methodology for the management of CI security that allows to take actions to eliminate or mitigate the effects of adverse events[1], and
- entities responsible for CI security do not include the risk of loss of CI functionality in protection activity planning process.

[1] Adverse event – an event resulting from the fulfillment of the threat, having negative effects on the organization, natural environment, or population.

Hence, the goal of my work was to develop an integral model of CI security[2] (IMCIS), which is vital to the methodology of situational management of CI security[3] (MSMCIS), which allows to determinate the characteristics of CI and make decisions regarding CI protection at the level of CI operators and local and central administration.

2 Conditions for managing the CI security in Poland and the European Union

Literature survey indicates a strong relationship between national security and the efficiency of CI, for which protective activities were planned as a part of the civil planning process (Fig. 1).

The civil planning process[4] is implemented as a part of the civil planning cycle, which involves six stages, at least once in every 2 years (Fig. 2).

The civil planning process is supplemented by the crisis management process when the adverse event or crisis situation[5] occurs.

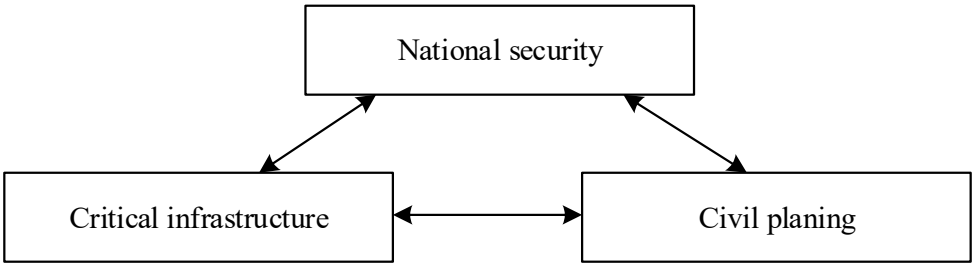

Figure 1. Dependence between national security, civil planning, and critical infrastructure (*Source:* Wiśniewski, 2019, p.14)

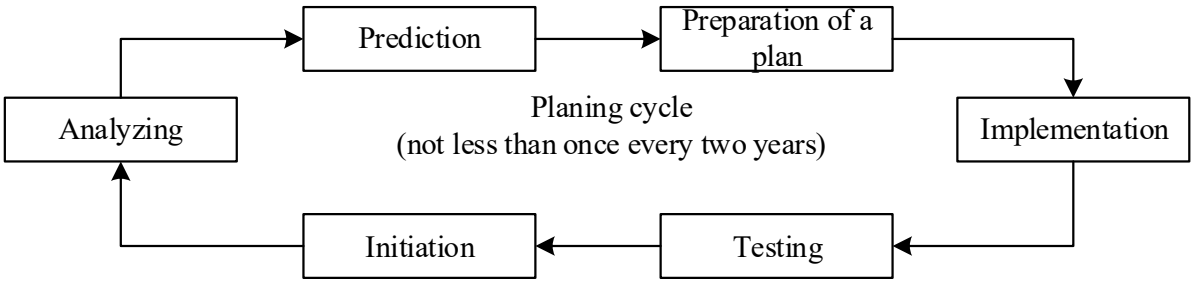

Figure 2. The civil planning cycle (*Source:* Dz.U., 2019, Item 209)

[2] Integral model of CI security (IMCIS)– a set of concepts enabling model mapping of the CI situation, such as CI entities, recognition of adverse events, estimation of risk resulting from threats to which CI is vulnerable, and determination of the decision problem regarding CI security against the identified threats.

[3] Methodology of situational management of CI safety (MSMCIS) – a set of stages allowing for specifying the CI situation, estimating the risk value depending on the CI situation, and determining a decision problem aimed at identifying safeguards that maintain the availability of functionality above the safety threshold, where the results obtained from the recent stage constitute input data for the next stage.

[4] Civil planning – activities aimed at preparing public administration for crisis management and planning to support the Armed Forces of the Republic of Poland in the event of their use, and planning the use of the Armed Forces of the Republic of Poland to implement tasks in the field of crisis management (Dz.U., 2019, Item 209).

[5] Crisis situation – a situation that has a negative effect on the level of people safety, property of significant size, or the environment, which causes significant limitation of the ability of the relevant public administration authorities to act due to inadequacy of the forces and measures in their possession (Dz.U., 2019, Item 1566, Article 3, Point 1).

The crisis management process consists of two periods and four phases:

- Period of stabilization – includes the prevention and preparation phases. The stabilization period refers to entirety of organizational activities undertaken at all levels of public administration, including the preparation and implementation of measures to prevent threats, as well as the development and implementation of operational procedures:
  - prevention phase – focuses on eliminating or limiting the risk by implementation of safeguards against identified threats,
  - preparation phase – includes activities to ensure protection against identified threats that cannot be avoided.
- Implementation period – includes the response and reconstruction phases. The implementation period covers all actions taken as a result of materialization of the threat that led to the emergence of a crisis situation and actions aimed at restoring the state from before materialization of the threat:
  - response phase – includes projects undertaken at the time of crisis,
  - reconstruction phase – conducting activities that regulate living conditions in terms of returning to the desired state of functioning of the object under consideration.

Therefore, CI operators as well as entities involved in both processes at various administrative levels, and the Government Centre for Security (GCS), coordinating all activities related to CI protection, constitute a set of entities responsible for CI security (Table 1).

Table 1. Entities responsible for CI security (*Source:* Wiśniewski, 2019, p.19)

<table>
<tr><td rowspan="8">Local government level</td><td rowspan="2">State</td><td colspan="2">The Council of Ministers</td><td rowspan="11">Government Security Center (State level)</td></tr>
<tr><td colspan="2">Governmental Crisis Management Team (GCMT)</td></tr>
<tr><td rowspan="2">Province</td><td colspan="2">Voivod</td></tr>
<tr><td>Provincial Crisis Management Team (PCMT)</td><td>Provincial Center for Crisis Management</td></tr>
<tr><td rowspan="2">District</td><td colspan="2">District officer</td></tr>
<tr><td>District Crisis Management Team (DCMT)</td><td>District Center for Crisis Management</td></tr>
<tr><td rowspan="2">Community</td><td colspan="2">Mayor / Mayor of the city</td></tr>
<tr><td>Commune Crisis Management Team (CCMT)</td><td>Commune Center for Crisis Management</td></tr>
<tr><td>The level of the CI operator</td><td>Systems of CI</td><td colspan="2">CI entities</td></tr>
</table>

In addition, GCS is a point of information exchange between the CI of Poland and the European CI[6]. These entities have to agree on CI protection plans including:

- differences in CI definitions,
- differences in the definition of CI protection,
- various lists of CI systems (Table 2), and
- lack of a dedicated methodology of CI security management.

The lack of this methodology, in the author's opinion, is due to the lack of a well-defined pattern of CI characteristic, which refers to the Model of CI Situation.

Table 2. List of CI systems in the EU and Poland
(*Source:* Dz.U.UE., 2008, No. 345, Item 75, Article 2b; Dz.U., 2019, Item 209, Article 3, Point 2)

European CI systems	Polish CI systems
• Electricity • Oil • Gas • Road transport • Rail transport • Air transport • Inland waterways transport • Ocean and short-sea shipping and ports	• Energy, fuel and energy supply systems • Communication systems • Tele-information network systems • Financial systems • Food supply systems • Water supply systems • Health protection systems • Transportation systems • Rescue systems • Systems ensuring the continuity of public administration activities • Systems of production, storing and use of chemical and radioactive substances, including pipelines for hazardous substances

In order to determine this pattern, the legal requirements of the civil planning and the crisis management processes were analyzed. It allowed indicating the canon of CI characterization (Fig. 3), which consists of data-describing resources, functionalities, threats, and security.

The CI characteristic canon is the major element of both IMCIS and MSMCIS. The analysis of national risk assessment methodologies for crisis management has been already implemented in Poland, German, Sweden, the Netherlands, Ireland, Canada, USA, and Australia.

Legal requirements of EUCPM (European Civil Protection Mechanism), the civilian planning, and crisis management processes allowed to indicate (Fig. 4):

- stages of the MSMCIS – rectangles,
- elements of the IMCIS, which are the vital utilities for the methodology – circles.

[6] European CI – constitutes those designated critical infrastructures which are of the highest importance for the community and which, if disrupted or destroyed, would affect two or more MS, or a single member state if the critical infrastructure is located in another member state (Dz.U., 2019, Item 209, Article 3).

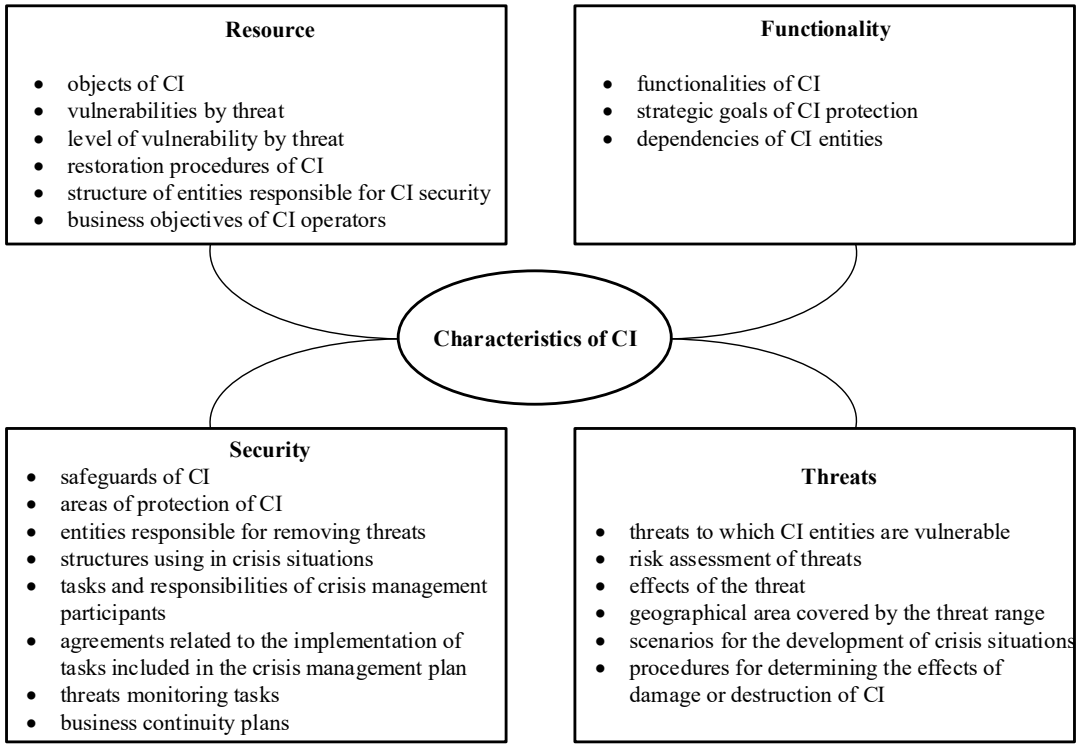

Figure 3. The canon of CI characterization (*Source:* Wiśniewski and Ostrowska, 2016, pp.118-119)

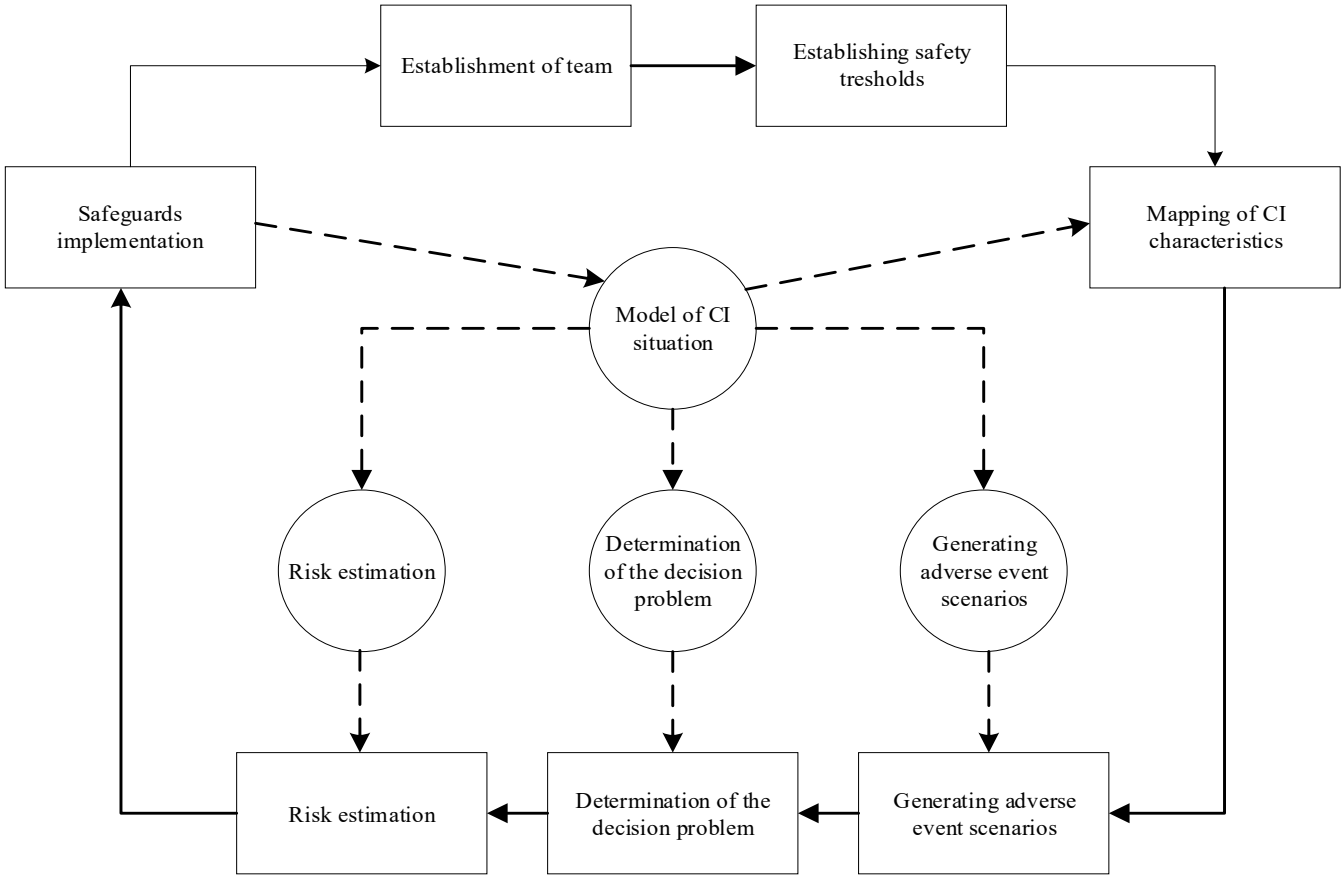

Figure 4. Dependence of the MSMCIS steps on IMCIS elements (*Source:* Wiśniewski, 2019, p.24)

3 The Integral Model of CI Safety

The IMCIS is divided into four parts: Model of CI Situation, Method of Adverse Events Scenario Generation, Method of Risk Estimation, and Method of Decision Problem Determination.

The Model of CI Situation (Fig. 5), based on Kłykov's Model of Situation (Kłykow and Jurek, 1988, pp.71-73), was implemented into the canon of CI characterization (Fig. 3) and made up for CI set and threat dependencies (Eq. 1):

$$<V, \Phi, Z, H, M, G, T> \quad (1)$$

where:

V – is considered CI,

Φ – is a set of CI functionalities,

Z – a set of threats,

H – a set of excitation of threats,

M – a set of security,

G – a set of CI dependencies between CI entities, and

T – is the moment of determining CI characteristic.

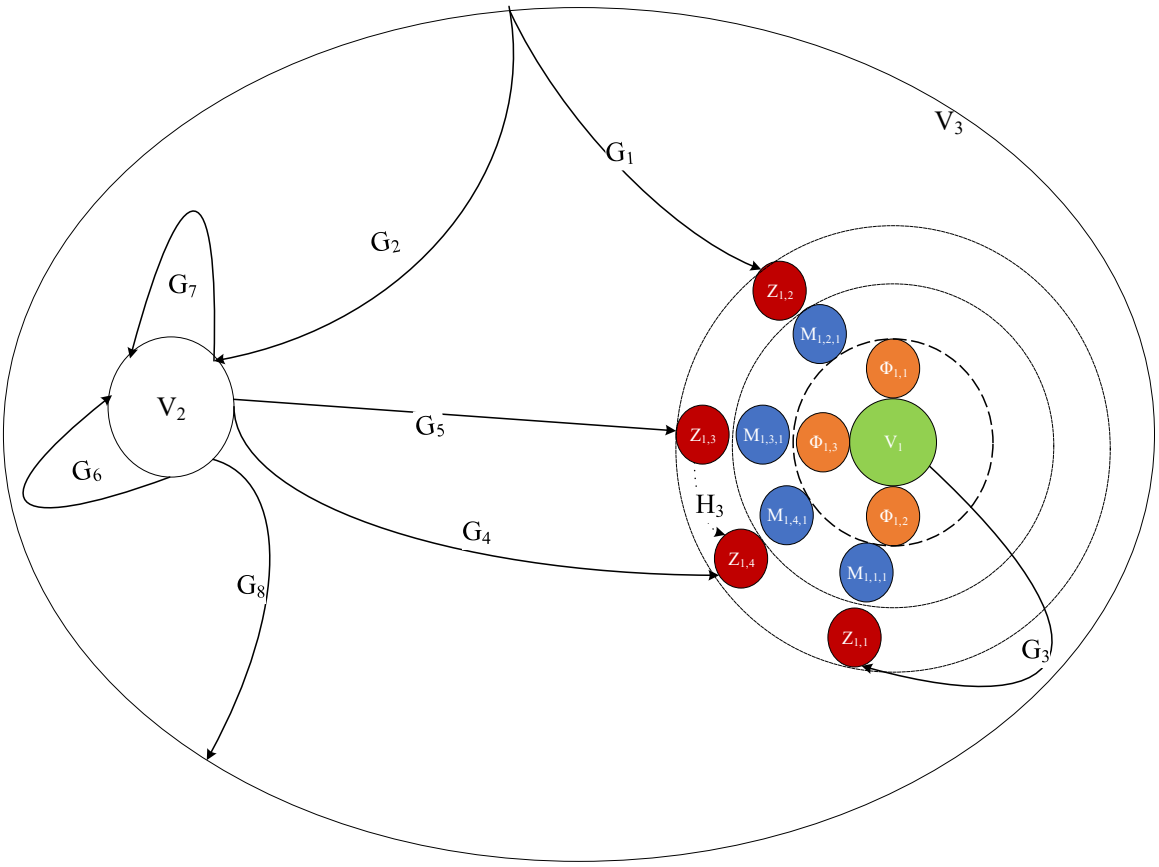

Figure 5. An example of a graphic illustration of the dependence of CI entities
(*Source:* Wiśniewski, 2019, p.52)

All elements included in this model are connected to each other, as depicted in a relational database (Fig. 6). Each element has been written up with a set of attributes that are required to perform the model's methods. Moreover, elements of the CI situation model can be described with additional attributes required by applicable national or international law.

The Model of CI Situation provides data, which allows determining the level of the risk resulting from threats. The Method of Risk Estimation, which has been developed (Eq. 2), is based on the classic risk pattern, which was implemented to the canon of CI characteristics.

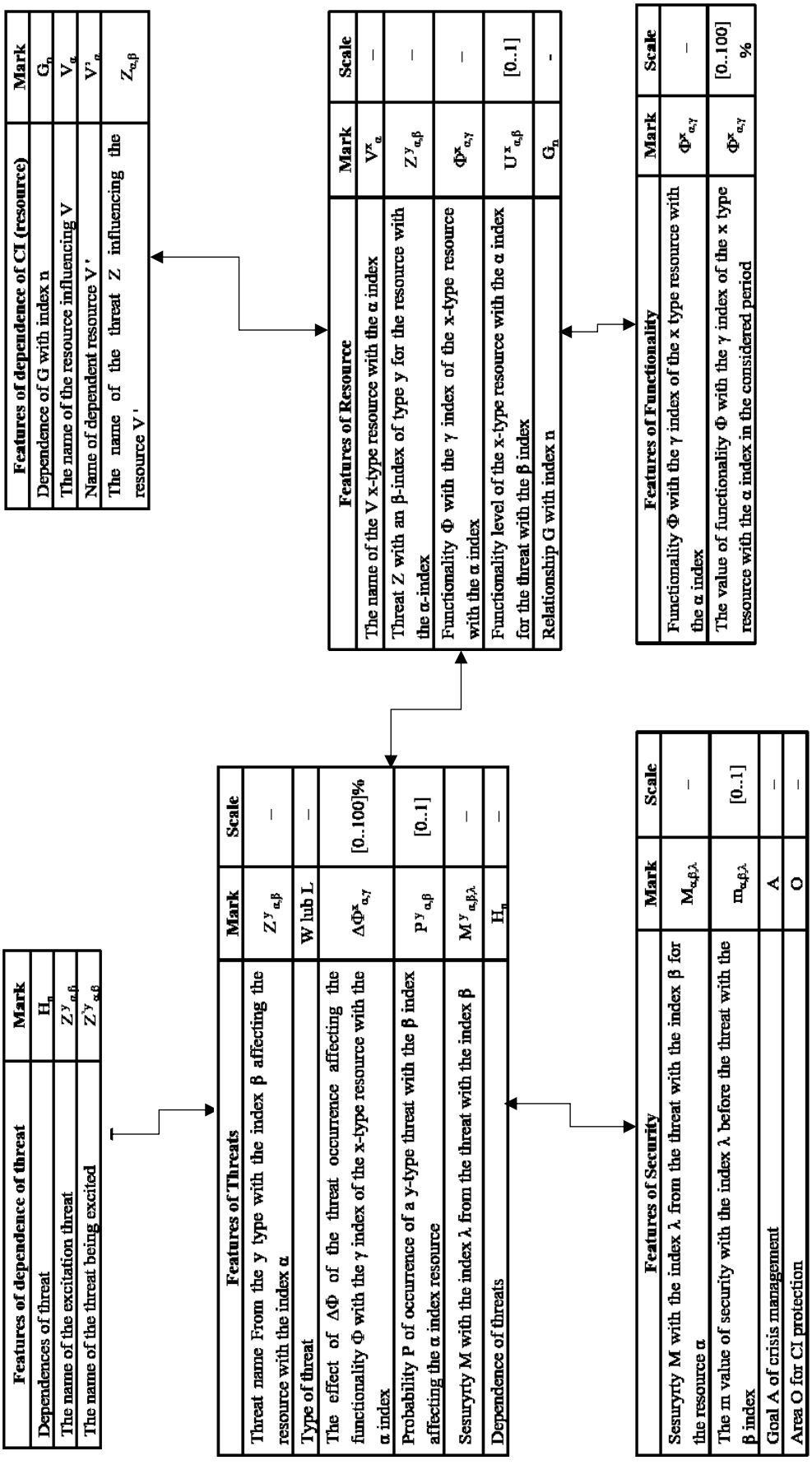

Figure 6. Dependencies of elements of the CI situation model
(S*ource:* Wiśniewski, 2019, pp.53-55)

$$R_{\alpha,\beta} = P_{\alpha,\beta} * \left|\Delta\Phi_{\alpha,\gamma}\right| * \left(U_{\alpha,\beta} - M_{\alpha,\beta}\right) \quad (2)$$

where:

α – is the CI index,

β – the index of threat,

γ – the index of functionality of the considered CI,

$R_{\alpha,\beta}$ – the level of risk [0..100]%,

$P_{\alpha,\beta}$ – the probability of β threat on the scale [0..1],

$U_{\alpha,\beta}$ – the CI vulnerability to β threat on the scale [0..1],

$\Delta\Phi_{\alpha,\gamma}$ – the effect of β threat occurrence [0..100]%, and

$M_{\alpha,\beta}$ – is the impact of security on vulnerability of CI to β threat on a scale [0..1].

This allows us to describe the risk of losing functionality depending on:

- the probability of a threat occurring;
- losing functionality, which is caused by threat occurrence;
- CI vulnerability; and

the impact of applied securities for CI resistance.

Computing the risk of losing functionality allows determining the future level of functionality after threat occurrence. This can be done by subtraction of the risk of losing functionality from the current level of functionality value (Eq. 3):

$$\Phi_{\alpha,\gamma}(t_{n+1}) = \Phi_{\alpha,\gamma}(t_n) - R_{\Phi_{\alpha,\gamma}}(t_n) \quad (3)$$

where:

$\Phi_{\alpha,\gamma}(t_{n+1})$ – is the expected level of functionality at the moment t_{n+1},

$\Phi_{\alpha,\gamma}(t_n)$ – the measured/estimated functional level at the moment t_n resulting from the Model of CI Situation, and

$R_{\Phi_{\alpha,\gamma}}(t_n)$ – is the level of risk of losing functionality at the considered moment t_n.

In consequence, it is possible to determinate the threshold of CI security (Eq. 4). The security threshold has to be greater than the level of functionality, which assumes threat occurrence.

$$\Phi^{PB} \leq \Phi_{\alpha,\gamma}(t_n) - R_{\Phi_{\alpha,\gamma}}(t_n) \quad (4)$$

If the threshold of CI security is not achieved, the CI operator is required to formulate a decision problem, whose solution will allow identification of the safeguards limiting the risk value to an acceptable level.

The Method of Adverse Event Scenario Generation allows to create a model of dependence between CIs and the considered threats (Fig. 7).

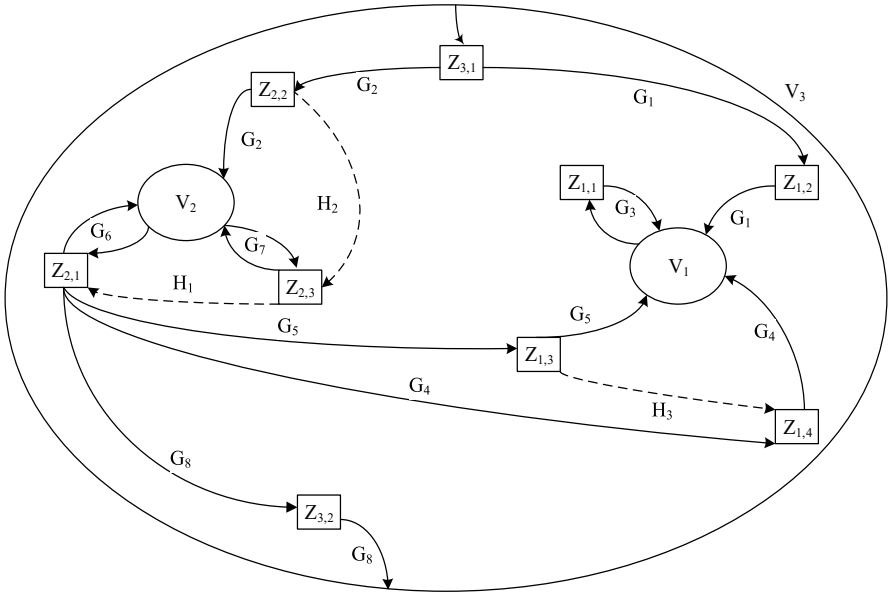

Figure 7. Example of identification of CI dependencies in the considered model
Note: Ellipses are Cis (V_α), rectangles are threats ($Z_{\alpha,\beta}$), full arrows mean the dependencies of the considered CI (G_n), and dashed arrows mean threats' excitation (H_n)?
(*Source:* Wiśniewski, 2019, p.63)

It enables:

- to examine whether the Model of CI Situation contains all threats to which the CI is exposed, and
- to generate adverse event scenario which may occur in the considered CI.

Determination of The method of Problem Decision is the last method of the IMCIS. It allows to determine decision areas resulting from threats to which CI is exposed. Then, it is possible to establish the relation between contradictions and elementary decisions. Those elements connected to the edge (Fig. 8) cannot be together in one solution to the decision problem.

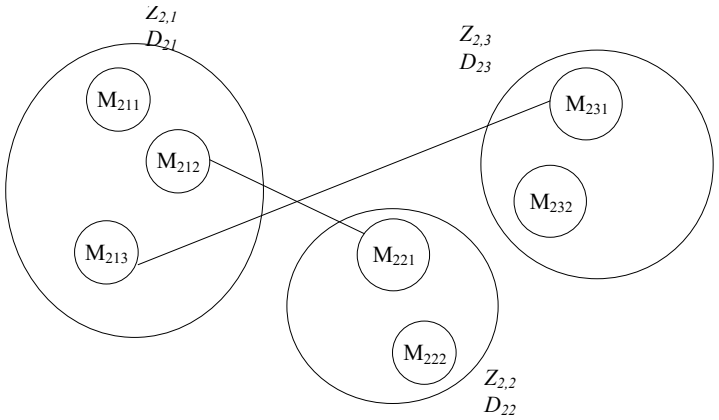

Figure 8. An example of decision problem (*Source:* Own elaboration)

The decision problem can be solved by indicating all combinations of elementary decisions, one from each decision area (Eq. 5) (Wiśniewski, 2019, p.75).

$$\begin{array}{llllll} Z_{\alpha,\beta} & \{M_{\alpha,\beta,1}, & M_{\alpha,\beta,\lambda+1}, & \ldots, & M_{\alpha,\beta,I} & \} \\ Z_{\alpha,\beta+1} & \{M_{\alpha,\beta+1,1}, & M_{\alpha,\beta+1,\lambda+1}, & \ldots, & M_{\alpha,\beta+1,i} & \} \\ \ldots & \{\ldots, & \ldots, & \ldots, & \ldots & \} \\ Z_{\alpha,j} & \{M_{\alpha,j,1}, & M_{\alpha,j,\lambda+1}, & \ldots, & M_{\alpha,j,i} & \} \end{array} \quad (5)$$

where:

α – is the CI index,

β – the index of threat,

i – the number of all available security, and

j – is the number of threats to which the CI is vulnerable.

Subsequently, the cost assessment of all combinations can be estimated, and it makes a base for determining which decision is desired by the CI operator (Fig. 9).

	$d_{2,1,\lambda}$	$d_{2,2,\lambda}$	$d_{2,3,\lambda}$		$D_{2,\beta}$		Cost assessment
Decision 1	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,1}$		$D_{2,1}$		$(M_{2,1,1*} D_{2,1})+ (M_{2,2,1*} D_{2,2})+ (M_{2,3,1*} D_{2,3})$
Decision 2	$M_{2,1,1}$	$M_{2,2,1}$	$M_{2,3,2}$		$D_{2,2}$		$(M_{2,1,1*} D_{2,1})+ (M_{2,2,1*} D_{2,2})+ (M_{2,3,2*} D_{2,3})$
Decision 3	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,1}$		$D_{2,3}$		$(M_{2,1,1*} D_{2,1})+ (M_{2,2,2*} D_{2,2})+ (M_{2,3,1*} D_{2,3})$
Decision 4	$M_{2,1,1}$	$M_{2,2,2}$	$M_{2,3,2}$	*		=	$(M_{2,1,1*} D_{2,1})+ (M_{2,2,2*} D_{2,2})+ (M_{2,3,2*} D_{2,3})$
Decision 5	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,1}$				$(M_{2,1,2*} D_{2,1})+ (M_{2,2,2*} D_{2,2})+ (M_{2,3,1*} D_{2,3})$
Decision 6	$M_{2,1,2}$	$M_{2,2,2}$	$M_{2,3,2}$				$(M_{2,1,2*} D_{2,1})+ (M_{2,2,2*} D_{2,2})+ (M_{2,3,2*} D_{2,3})$
Decision 7	$M_{2,1,3}$	$M_{2,2,1}$	$M_{2,3,2}$				$(M_{2,1,3*} D_{2,1})+ (M_{2,2,1*} D_{2,2})+ (M_{2,3,2*} D_{2,3})$
Decision 8	$M_{2,1,3}$	$M_{2,2,2}$	$M_{2,3,2}$				$(M_{2,1,3*} D_{2,1})+ (M_{2,2,2*} D_{2,2})+ (M_{2,3,2*} D_{2,3})$

Figure 9. An example of calculating the value of solution cost for a decision problem (*Source*: Own elaboration)

Making a decision allows to calculate the risk of losing functionality which is included into account new security. Consequently, the new level of functionality can be estimated. It shows whether the required safety threshold has been reached.

4 The Methodology of Situational Management of CI Security

Development of the integral CI security model allowed to specify the stages of the Methodology of Situational Management of CI Security (Fig. 4).

Each of the seven stages is described in Table 3, which contains:

- goal of the stage,
- utilities supporting execution of the stage,
- input data for the stage,
- output data for the stage, and
- procedure of stage execution.

MSMCIS was supplemented by two procedures of its execution, for the case of flat and hierarchical decision problems (Fig. 10).

Table 3. An example of synthetic characteristics of the stage of MSMCIS (*Source:* Wiśniewski, 2019, p.86)

The name of the stage	Establishment of a team		
The goal of the stage	Used utilities	Input data	Output data
Establishment of the list of members in the analytical team responsible for CI security	Model of CI situation Matrix of competence	Characteristics of CI List of CI stakeholders	List of analytical team members
Procedure	• analysis of stakeholders considered IK and selection of team members • evaluation of matrix of analytical team competence		

A flat decision problem assumes that the choice of using additional security is made only on one decision level, for example, by the CI operator. The hierarchical decision problem assumes that the decision on additional security involves at least two decision levels, for example, the CI operator has to consult his decision with the commune authorities.

The case of a hierarchical decision problem requires executive iteration computing, which is illustrated in Fig. 10 by grey.

The MSMCIS has been evaluated on the basis of two computational experiments. The first experiment was built on a flat decision problem and the second one using a hierarchical decision problem.

The object taken under investigation in this study was the Refinery PKN ORLEN Inc. in Płock. Data were obtained from the Crisis Management Plan of Płock (Plan Zarządzania Kryzysowego Powiatu Płockiego, 2015) district and the ORLEN Group Integrated Report (Raport Zintegrowany Grupy ORLEN, 2106). A list of CI entities, their functionality, threats, and safeguards was established by the Crisis Management Plan. The ORLEN Group Integrated Report allowed to determine the level of functionality performed by the analyzed object. Based on the available data, the author was able to evaluate the following:

- stage of CI characteristics determination,
- stage of risk estimation,
- stage of adverse event scenario generation, and
- stage of decision problem determination.

It is also worth to clarify that as a refinery in Płock, we understand actually three different entities:

- Refinery Orglan Inc.,
- Basell Orlen Poliolefins Ltd, and
- Production Facility Orlen Oil Ltd.

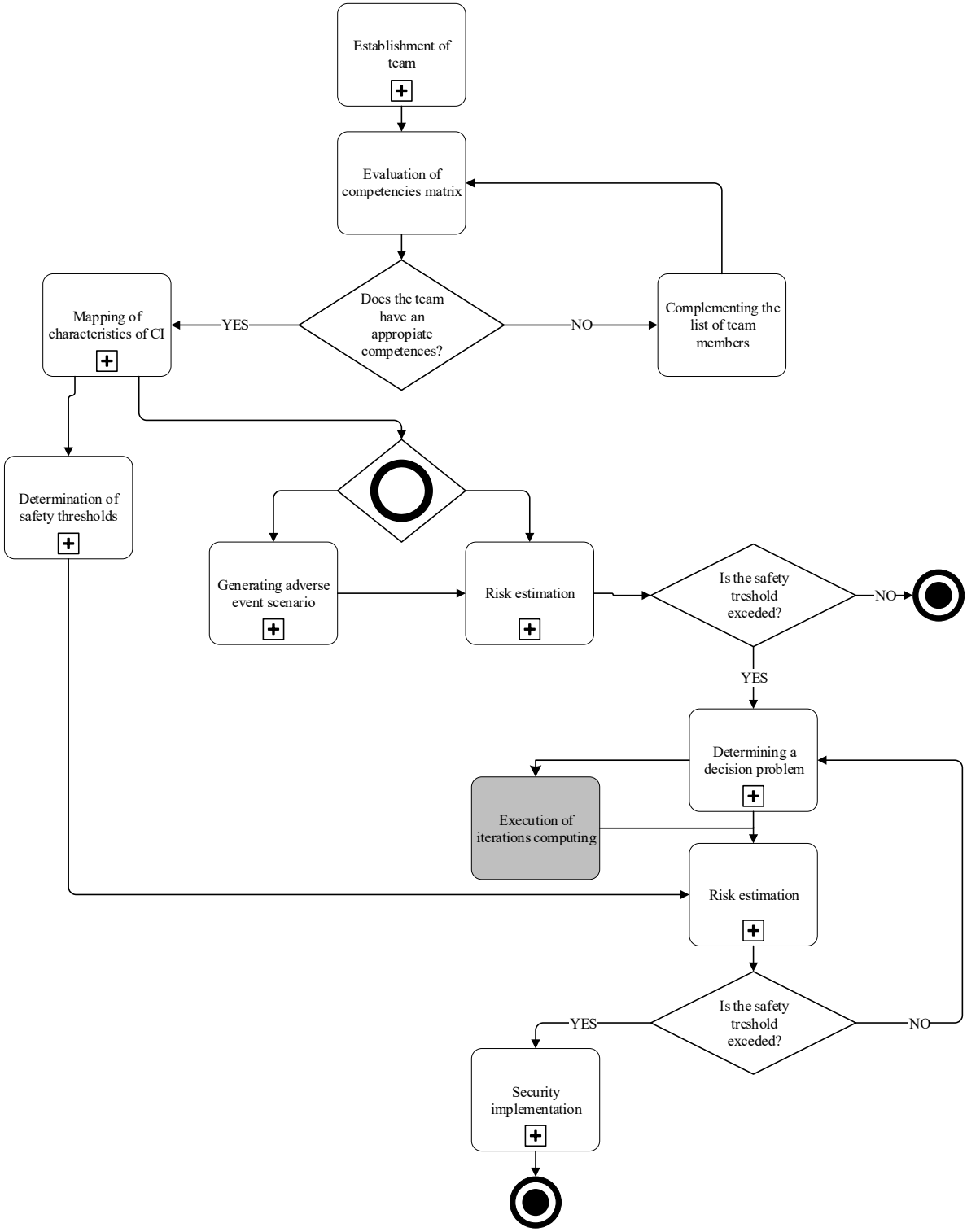

Figure 10. Procedures for implementing the MSMCIS
(*Source:* Wiśniewski, 2019, p.92 and p.94)

These enterprises are managed by three CI operators, and their characteristic according to the Model of CI Situation is presented in Table 4.

Based on the situation of the entities of CI under consideration, the risk of losing functionality was computed (Table 5) for all functionalities of the entities.

Table 4. Synthetic record of the situation of the Refinery ORLEN inc., the Basell Orlen Polyolefins ltd. and the Production Facility Orlen Oil ltd (*Source:* Wiśniewski, 2019, p.104)

CI	Functionalities		Threats							Vulnerability
	Mark	Value of functionality	Mark	Type	Excited threat	Probability	Effect	Safeguards: Mark	Safeguards: Degree of reduction of vulnerability	
V_1	$\Phi_{1,1}$	93%	$Z_{1,1}$	IN	explosion, environmental contamination	0.7	-47% ($\Phi_{1,1}$)	$M_{1,1,1}$	0.46	0.88
							-37% ($\Phi_{1,2}$)			
							-13% ($\Phi_{1,3}$)	$M_{1,1,2}$	0.31	
	$\Phi_{1,2}$	93%	$Z_{1,2}$	IN	fire	0.56	-42% ($\Phi_{1,1}$)	$M_{1,2,1}$	0.16	0.81
							-39% ($\Phi_{1,2}$)			
							-46% ($\Phi_{1,3}$)			
	$\Phi_{1,3}$	93%	$Z_{1,3}$	IN	-	0.81	-9% ($\Phi_{1,1}$)	$M_{1,3,1}$	0.16	0.31
							-9% ($\Phi_{1,3}$)			
V_2	$\Phi_{2,1}$	93%	$Z_{2,1}$	IN	explosion, environmental contamination	0.42	-94% ($\Phi_{2,1}$)	$M_{2,1,1}$	0.27	0.56
								$M_{2,1,2}$	0.18	
			$Z_{2,2}$	IN	fire	0.35	-48% ($\Phi_{2,1}$)	$M_{2,2,1}$	0.17	0.91
			$Z_{2,3}$	IN	-	0.61	-5% ($\Phi_{2,1}$)	$M_{2,3,1}$	0.52	0.82
V_3	$\Phi_{3,1}$	93%	$Z_{3,1}$	IN	explosion, environmental contamination	0.58	-55% ($\Phi_{3,1}$)	$M_{3,1,1}$	0.05	0.92
							-34% ($\Phi_{3,2}$)			
							-65% ($\Phi_{3,3}$)	$M_{3,1,2}$	0.75	
	$\Phi_{3,2}$	93%	$Z_{3,2}$	IN	fire	0.52	-41% ($\Phi_{3,1}$)	$M_{3,2,1}$	0.14	0.83
							-27% ($\Phi_{3,2}$)			
							-38% ($\Phi_{3,3}$)			
	$\Phi_{3,3}$	93%	$Z_{3,3}$	IN	-	0.49	-18% ($\Phi_{3,1}$)	$M_{3,3,1}$	0.26	0.36
							-19% ($\Phi_{3,2}$)			
							-15% ($\Phi_{3,3}$)			

Table 5. Synthetic record of the risk of functionality loss for considered CI entities (*Source:* Wiśniewski, 2019, p.105)

CI	Threat	Probability	Effect		Vulnerability	Safeguard	Inherent risk	Residual risk
V_α	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	R^i	R^r
V_1	$Z_{1,1}$	0.7	$\Phi_{1,1}$	47%	0.88	0.77	28.95%	3.62%
			$\Phi_{1,2}$	37%			22.79%	2.85%
			$\Phi_{1,3}$	13%			8.01%	1.00%
	$Z_{1,2}$	0.56	$\Phi_{1,1}$	42%	0.81	0.16	19.05%	15.29%
			$\Phi_{1,2}$	39%			17.69%	14.20%
			$\Phi_{1,3}$	46%			20.87%	16.74%
	$Z_{1,3}$	0.81	$\Phi_{1,1}$	9%	0.31	0.16	2.26%	1.09%
			$\Phi_{1,3}$	9%			2.26%	1.09%
Sum of risk for						$\Phi_{1,1}$	50.26%	20.00%
						$\Phi_{1,2}$	40.48%	17.05%
						$\Phi_{1,3}$	31.13%	18.84%

Table 5. Synthetic record of the risk of functionality loss for considered CI entities (cont.)
(*Source:* Wiśniewski, 2019, p.105)

CI	Threat	Probability	Effect		Vulnerability	Safeguard	Inherent risk	Residual risk
V_α	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$M_{\alpha,\beta}$	R^i	R^r
V_2	$Z_{2,1}$	0.42	$\Phi_{2,1}$	94%	0.56	0.45	22.11%	4.34%
	$Z_{2,2}$	0.35	$\Phi_{2,1}$	48%	0.91	0.17	15.29%	12.43%
	$Z_{2,3}$	0.61	$\Phi_{2,1}$	5%	0.82	0.52	2.50%	0.92%
Sum of risk for						$\Phi_{2,2}$	39.90%	17.69%
V_3	$Z_{3,1}$	0.58	$\Phi_{3,1}$	55%	0.92	0.8	29.35%	3.83%
			$\Phi_{3,2}$	34%			18.14%	2.37%
			$\Phi_{3,3}$	65%			34.68%	4.52%
	$Z_{3,2}$	0.52	$\Phi_{3,1}$	41%	0.83	0.14	17.70%	14.71%
			$\Phi_{3,2}$	27%			11.65%	9.69%
			$\Phi_{3,3}$	38%			16.40%	13.63%
	$Z_{3,3}$	0.49	$\Phi_{3,1}$	18%	0.36	0.26	3.18%	0.88%
			$\Phi_{3,2}$	19%			3.35%	0.93%
			$\Phi_{3,3}$	15%			2.65%	0.74%
Sum of risk for						$\Phi_{3,1}$	50.22%	19.42%
						$\Phi_{3,2}$	33.15%	12.99%
						$\Phi_{3,3}$	53.73%	18.89%

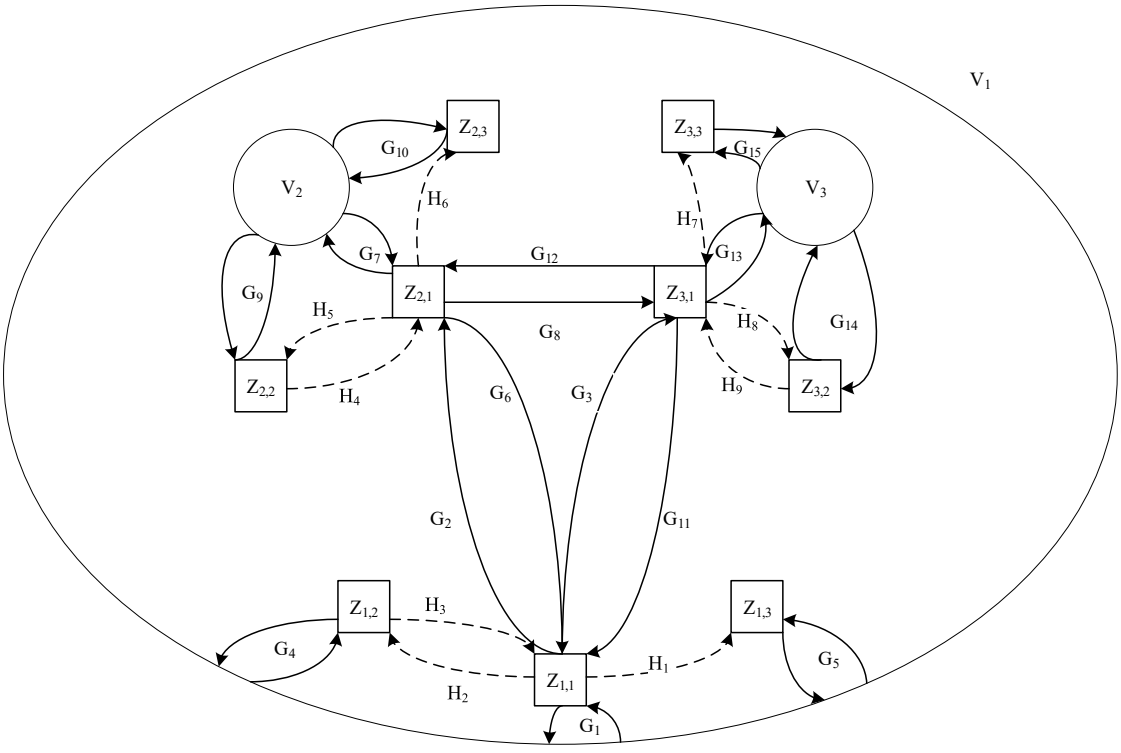

Figure 11. The model of dependencies of the Refinery ORLEN Inc., the Basell Orlen Polyolefins Ltd, and the Production Facility Orlen Oil Ltd (*Source:* Wiśniewski, 2019, p.106)

Next, a model of CI entities' dependence was developed (Fig. 11) and calculations for a 1000 random cases of threats excitation were performed.

Based on available data, 93 adverse event scenarios were obtained, of which 61 scenarios had a negative impact on at least one CI under consideration and

32 scenarios did not have a negative impact on CI entities. To conclude, in terms of the analyzed cases, the security used has been sufficient.

A flat decision problem was indicated for a 20% risk of losing oil-processing functionality (Table 5). The functionality was exposed to three threats: fire, explosion, and environmental contamination. Hence, the decision problem includes three decision areas (Fig. 12). Additional security for these threats comes from the Lotos refinery where they are used (Informacja dotycząca sposobu ostrzegania i postępowania społeczeństwa w przypadku wystapienia poważnnej awarii przemysłowej dla grupy Lotos S.A., access 04.04.2018).

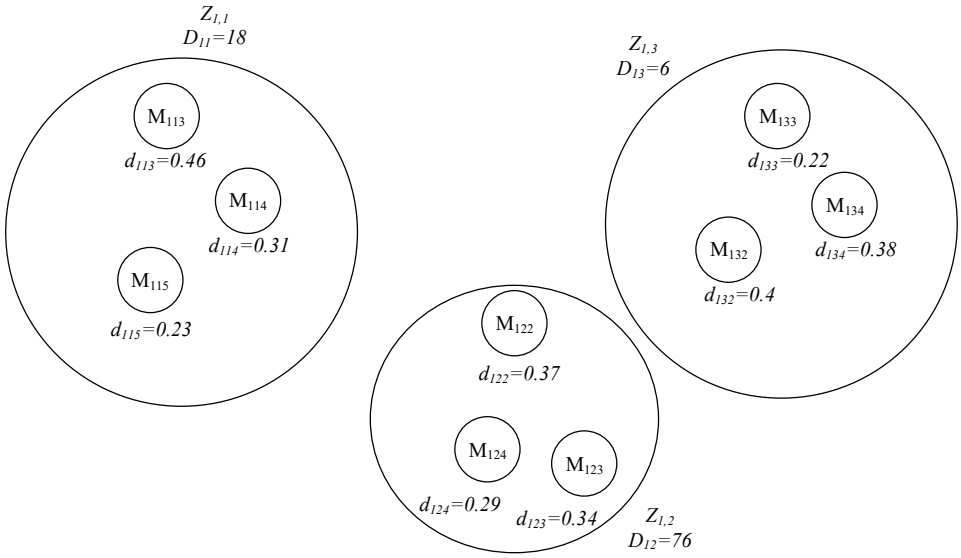

Figure 12. Illustration of the considered flat decision problem (*Source:* Wiśniewski, 2019, p.113)

The solution of the decision problem allowed indicating a set of three additional securities, which were used for achieving the assumed security threshold.

Indicated safeguards reduce the level of the risk for the considered functionality from 20% to slightly over 2%. Furthermore, the indicated security has also reduced the risk of losing other functionalities of the considered CI (Table 6). Implementation of additional securities determines the new situation of the Orlen refinery.

Table 6. Synthetic record of the risk of functionality loss for considered CI entities after adding new safeguards (*Source:* Own elaboration)

CI	Threat	Probability	Effect		Vulnerability	Safeguard	Inherent risk	Residual risk
$V\alpha$	$Z_{\alpha,\beta}$	P	$\Phi_{\alpha,\gamma}$	$\Delta\Phi_{\alpha,\gamma}$	$U_{\alpha,\beta}$	$\sum M_{\alpha,\beta,\lambda}$	R^i	R^r_2
V_1	$Z_{1,1}$	0.7	$\Phi_{1,1}$	47%	0.88	0.88	28.95%	0.00%
			$\Phi_{1,2}$	37%			22.79%	0.00%
			$\Phi_{1,3}$	13%			8.01%	0.00%
	$Z_{1,2}$	0.56	$\Phi_{1,1}$	42%	0.81	0.72	19.05%	2.12%
			$\Phi_{1,2}$	39%			17.69%	1.97%
			$\Phi_{1,3}$	46%			20.87%	2.32%
	$Z_{1,3}$	0.81	$\Phi_{1,1}$	9%	0.31	0.29	2.26%	0.15%
			$\Phi_{1,3}$	9%			2.26%	0.15%
Sum of risk for						$\Phi_{1,1}$	50.26%	2.26%
						$\Phi_{1,2}$	40.48%	1.97%
						$\Phi_{1,3}$	31.13%	2.46%

For the following case, a hierarchical decision problem, the decision problem was followed by one of the adverse event scenarios, which may occur at the ORLEN refinery. The scenario assumes that the Refinery ORLEN Inc. and the Production Facility Orlen Oil Ltd are affected by fire, environmental contamination, and explosion.

Additionally, an assumption was made – the authorities of Płock city will co-finance a set of security, what can minimize the risk of losing functionality of the considered CI entities.

CI operators may use three alternative securities for each threat. Therefore, the operator of the Production Facility Orlen Oil Ltd has three alternative securities to choose and the ORLEN refinery operator has nine alternative scenarios. The authorities of Płock City have 27 opportunities to choose (Fig. 13).

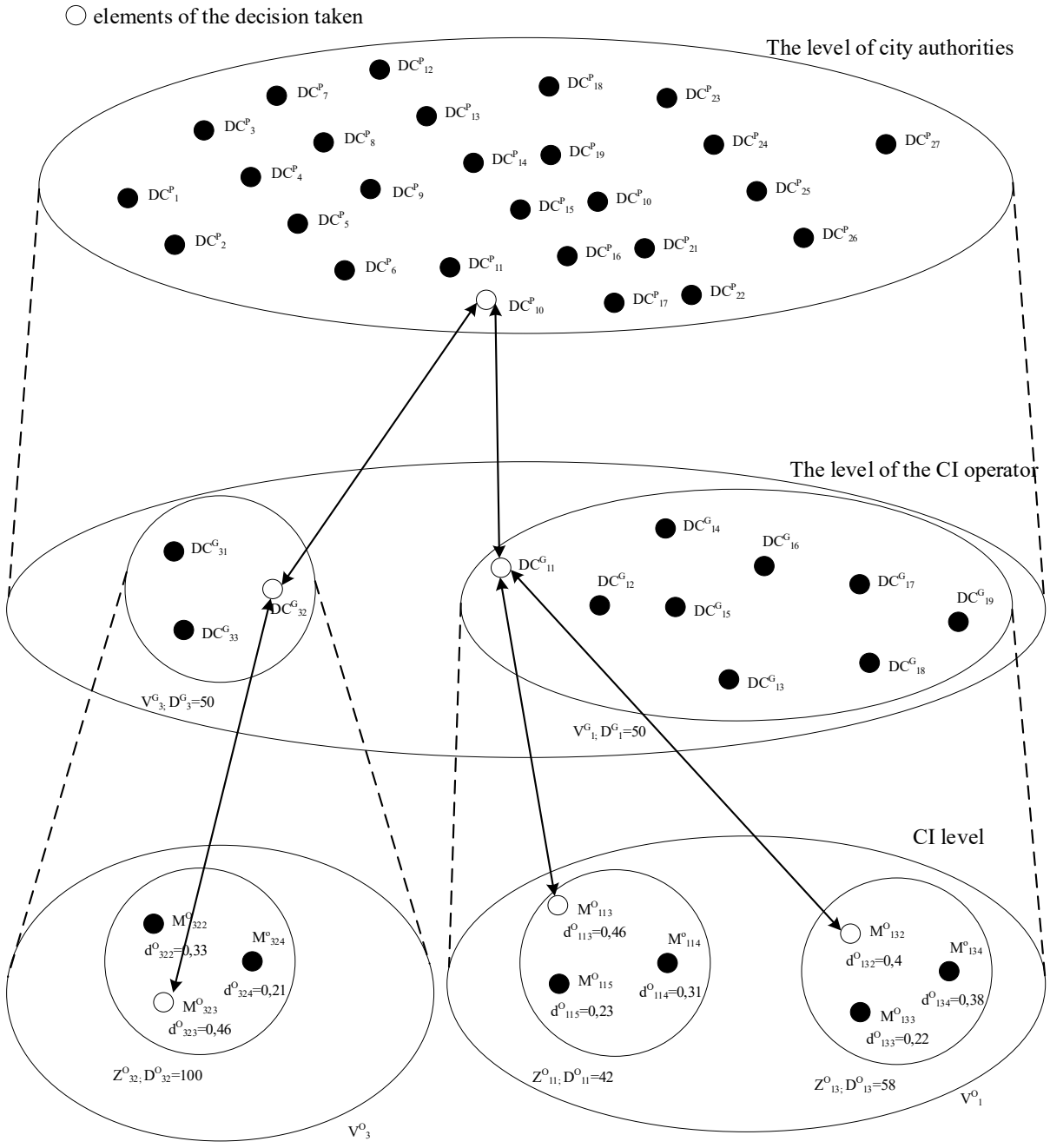

Figure 13. Illustration of the considered hierarchical decision problem
(*Source:* Wiśniewski, 2019, p.124)

Dependence between CI operator and city authorities levels

$d_{31}^{G} = 33$	$d_{11}^{G} = 42.52$		$D_{1}^{G} = 50$	$dc_{1}^{P} = 3776$
$d_{31}^{G} = 33$	$d_{12}^{G} = 32.08$		$D_{3}^{G} = 50$	$dc_{2}^{P} = 3254$
$d_{31}^{G} = 33$	$d_{13}^{G} = 41.36$			$dc_{3}^{P} = 3718$
$d_{31}^{G} = 33$	$d_{14}^{G} = 36.22$			$dc_{4}^{P} = 3461$
$d_{31}^{G} = 33$	$d_{15}^{G} = 25.78$			$dc_{5}^{P} = 2939$
$d_{31}^{G} = 33$	$d_{16}^{G} = 35.06$			$dc_{6}^{P} = 3403$
$d_{31}^{G} = 33$	$d_{17}^{G} = 32.86$			$dc_{7}^{P} = 3293$
$d_{31}^{G} = 33$	$d_{18}^{G} = 22.42$			$dc_{8}^{P} = 2771$
$d_{31}^{G} = 33$	$d_{19}^{G} = 31.7$			$dc_{9}^{P} = 3235$
$d_{32}^{G} = 46$	$d_{11}^{G} = 42.52$			$dc_{10}^{P} = 4426$
$d_{32}^{G} = 46$	$d_{12}^{G} = 32.08$			$dc_{11}^{P} = 3904$
$d_{32}^{G} = 46$	$d_{13}^{G} = 41.36$			$dc_{12}^{P} = 4368$
$d_{32}^{G} = 46$	$d_{14}^{G} = 36.22$			$dc_{13}^{P} = 4111$
$d_{32}^{G} = 46$	$d_{15}^{G} = 25.78$	*		= $dc_{14}^{P} = 3589$
$d_{32}^{G} = 46$	$d_{16}^{G} = 35.06$			$dc_{15}^{P} = 4053$
$d_{32}^{G} = 46$	$d_{17}^{G} = 32.86$			$dc_{16}^{P} = 3943$
$d_{32}^{G} = 46$	$d_{18}^{G} = 22.42$			$dc_{17}^{P} = 3421$
$d_{32}^{G} = 46$	$d_{19}^{G} = 31.7$			$dc_{18}^{P} = 3885$
$d_{33}^{G} = 21$	$d_{11}^{G} = 42.52$			$dc_{19}^{P} = 3176$
$d_{33}^{G} = 21$	$d_{12}^{G} = 32.08$			$dc_{20}^{P} = 2654$
$d_{33}^{G} = 21$	$d_{13}^{G} = 41.36$			$dc_{21}^{P} = 3118$
$d_{33}^{G} = 21$	$d_{14}^{G} = 36.22$			$dc_{22}^{P} = 2861$
$d_{33}^{G} = 21$	$d_{15}^{G} = 25.78$			$dc_{23}^{P} = 2339$
$d_{33}^{G} = 21$	$d_{16}^{G} = 35.06$			$dc_{24}^{P} = 2803$
$d_{33}^{G} = 21$	$d_{17}^{G} = 32.86$			$dc_{25}^{P} = 2693$
$d_{33}^{G} = 21$	$d_{18}^{G} = 22.42$			$dc_{26}^{P} = 2171$
$d_{33}^{G} = 21$	$d_{19}^{G} = 31.7$			$dc_{27}^{P} = 2635$

Dependence between CI operators – CI operators level

Decision problem $V^{O}{}_{1}$

$d_{113}^{O} = 0.46$	$d_{132}^{O} = 0.4$		$D_{11}^{O} = 42$	$d_{11}^{G} = 42.52$
$d_{113}^{O} = 0.46$	$d_{133}^{O} = 0.22$		$D_{13}^{O} = 58$	$d_{12}^{G} = 32.08$
$d_{113}^{O} = 0.46$	$d_{134}^{O} = 0.38$			$d_{13}^{G} = 41.36$
$d_{114}^{O} = 0.31$	$d_{132}^{O} = 0.4$			$d_{14}^{G} = 36.22$
$d_{114}^{O} = 0.31$	$d_{133}^{O} = 0.22$	*		= $d_{15}^{G} = 25.78$
$d_{114}^{O} = 0.31$	$d_{134}^{O} = 0.38$			$d_{16}^{G} = 35.06$
$d_{115}^{O} = 0.23$	$d_{132}^{O} = 0.4$			$d_{17}^{G} = 32.86$
$d_{115}^{O} = 0.23$	$d_{133}^{O} = 0.22$			$d_{18}^{G} = 22.42$
$d_{115}^{O} = 0.23$	$d_{134}^{O} = 0.38$			$d_{19}^{G} = 31.7$

Decision problem $V^{O}{}_{3}$

$d_{322}^{O} = 0.33$			$D_{32}^{O} = 100$	$d_{31}^{G} = 33$
$d_{323}^{O} = 0.46$		*		= $d_{32}^{G} = 46$
$d_{324}^{O} = 0.21$				$d_{33}^{G} = 21$

Figure 14. Matrix record of the considered hierarchical decision problem
(*Source:* Wiśniewski, 2019, p.125)

Decision problem's solution at successive decision levels, starting from the CI level, allowed for computing of the cost assessment at the level of city authorities (Fig. 14).

DC_{10} decision has the highest assessment cost, and therefore is desirable for implementation by all the city authorities. Decision at the level of city authorities indicates elementary decisions at the level of the CI operator and CI level – elements of the decision taken Fig. 13.

5 Conclusions

Results of presented experiments were used to confirm the utility of the methodology of the situational management CI security for the entities responsible for CI security in the areas of:

- determination of the CI characteristics,
- risk estimation,
- adverse event scenario generation, and
- decision problem determination.

It was proved that the MSMCIS should be used for civil planning and crisis management processes in Poland.

The most important theoretical conclusions of the study are:

- indication of the CI characteristic canon, which is based on a risk assessment method for the crisis management (utilized in Poland, USA, Canada, Australia, and selected EU countries),
- development of the CI Situation Model (based on the CI canon), which allows determining the CI characteristics, and
- development of methods based on data collected in the CI Situation Model: Method of Adverse Events Scenario Generation, Method of Risk Estimation, and Method of Decision Problem Determination.

The most important practical conclusions are:

- development and evaluation of the MSMCIS, which may be used in civil planning process and crisis management in Poland, and
- development of two procedures of this methodology for the cases of flat and hierarchical decision problems.

6 References

[1] Cuncil Directive 2008/114/EC, 2008. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Official Journal of the European Union*, L345/75.

[2] Kłykow, J., Jurek, J., 1988. *Dialogically Semiotic Decision Making Systems*. Warsaw: PWN.

[3] Informacja dotycząca sposobu ostrzegania i postępowania społeczeństwa w przypadku wystąpienia poważnnej awarii przemysłowej dla grupy Lotos S.A., 2019 (Information on the Manner of Warning and Behaviour of the Public in Case of a Serious Industrial Accident for Grupa Lotos Inc.) [online] Available at: m.odpowiedzialny.lotos.pl/repository/39634/ [Access 04.01.2020].

[4] Plan zarządzania kryzysowego powiatu płockiego (Crisis Management Plan for the District of Płock), 2015. [online] Available at: powiatplock.pl/attachments/article/44/powiatowy_plan_zk_sp_plock.pdf, [Access 28.12.2017].

[5] Presidential Policy Directive, 2013. Presidential Policy Directive - Critical Infrastructure Security and Resilience. [online] Available at: obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, [Access 12.01. 2019].

[6] Raport Zintegrowany Grupy ORLEN, 2106 (*ORLEN Group Integrated Report, 2016*) [online] Available at: www.orlen.pl/PL/OFirmie/StrukturaGrupyORLEN/Strony/default.aspx?pl [data odczytu 13.02.2018 r.].

[7] Dz.U., 2010. *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej* (*Regulation of the Council of Ministers of 30 April 2010 on Plans for the Protection of Critical Infrastructure*) (Dz.U. 2010, No. 83, Item 542).

[8] Dz.U., 2019. *Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Act of 26 April 2007 on Crisis Management)* (Dz.U. 2019, poz. 1398).

[9] Wiśniewski, M., Ostrowska, T., 2016. Challenges and good practices in critical infrastructure security management. In: M. Ćwiklicki, M. Jabłoński, S. Mazur, eds. *Contemporary concepts of public management. Modernization challenges in the public sector*, Krakow: Foundation GAP, pp.111-125.

[10] Wiśniewski, M., 2019. *Situational Management of Critical Infrastructure Security of State*. Warsaw: Warsaw University of Technology, Faculty of Management.Wiśniewski, M., 2019. *Situational Management of Critical Infrastructure Security of State*. Warsaw: Warsaw University of Technology, Faculty of Management.