Foundations of Management, Vol. 7 (2015), ISSN 2080-7279
DOI: 10.1515/fman-2015-0028

SITUATIONAL MANAGEMENT OF CRITICAL INFRASTRUCTURE RESOURCES UNDER THREAT

Tadeusz KRUPA*, Michał WIŚNIEWSKI**

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

Abstract: This article presents a synthesis of knowledge about safety management procedures for critical infrastructure in the context of risk management theory and the provisions of the Polish law on emergency management launched on of April 26, 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. This paper proposes using the concept of situational management and knowledge management to develop a new method of predicting, preventing, and responding to emerging crises within critical infrastructure. The considerations presented in this paper lead to a proposed concept system supporting critical infrastructure safety management through the implementation of knowledge management methods.

Keywords: situational management, knowledge management, critical infrastructure, safety management, artificial intelligence, base of cases, domino effect, Case Based Reasoning.

1 Introduction

Critical Infrastructure (CI) [24] is the basis for the smooth functioning of the state and its population. Due to the importance of societal CI, it is naturally a priority in the process of ensuring public safety to maintain a predetermined level of service availability, which is dependent on the efficiency of CI objects and CI systems, and to also continuously improve crisis management procedures.

The achievement of this goal depends on comprehensive hazard identification, risk analysis, implementation of preventive actions against threats, and remedial actions against incidents, crises, and disasters. The appropriate response to an incident requires an estimation of the value of the risk and knowledge of the effectiveness of the activity undertaken to avert the crisis. This is related to the issue of gathering, organizing, and processing knowledge of past events in order to improve emergency response skills.

The process of documenting threats, as well as the crises that are the consequence of these threats, cannot be effectively implemented without support tools and the monitoring and analysis of the situation of CI objects. This article attempts to answer the question: how effectively is CI managed in emergencies?

The proposed approach is the result of work carried out within the framework of a development project, National Centre for Research and Development (NCR&D), or "Methodology of risk assessment for the purpose of crisis management systems in the Republic of Poland," agreement number DOBR/0077/R/ID3/2013/03, on the implementation of projects in the field of research and development for national defense and state security by a consortium of the University of National Defense, Scientific and Research Centre for Fire Protection, Warsaw University of Technology (Faculty of Management), Main School of Fire, and Medcore Ltd.

2 The current system of critical infrastructure management in Poland

Critical infrastructure in Poland is defined 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. The Crisis Management Act is divided into 11 CI systems, while the European Union Civil Protection Mechanism, to which Polish legislation must be adapted, is divided into 12 systems.

This is interesting, because it points out the need to build an open management methodology for CI. In the Polish regulations, CI objects are identified based on the following criteria [24]:

- systemic: characterized by the quantitative or subjective parameters (functions) of the object, device, system, or service, the fulfillment of this criterion would lead to it being designated a CI object,
- cross-cutting: describing the parameters relating to the consequences of the destruction or cessation of operation of the object equipment, installation, or service, including financial implications, the need to evacuate, recovery time, uniqueness, and casualties.

In accordance with the provisions of the National Critical Infrastructure Protection Program (NCIPP) along with the development of methods and tools for CI management, ultimately the only determinants of identifying elements of CI are those that fulfil the cross-cutting criterion [18]. This criterion can also be used as a target against which the activities under CI management should be carried out, for example, minimization of casualties or minimization of the cost of rebuilding the CI objects.

The current CI management model is based on the Report a Threat to National Security (RTNS) process. According to the Crisis Management Act, the task of drawing up such reports falls to ministries, central agencies, and provincial governors. This process may or may not include counties and municipalities. This fact makes it difficult to collect reliable data on the hazards present at the various administrative levels. The RTNS development coordinator is the Government Centre for Security (GCS), which, based on reports delivered, draws up a summary report, outlines the conclusions of this report and forms the National Crisis Management Plan (NCMP). These documents are then submitted to the Council of Ministers, which adopts them in the form of a resolution. The conclusions of the collective RTNS and NCMP are the basis for the Emergency Management Plans at the levels of province, district, and municipality. The preparation of plans is obligatory at all levels. Under the current CI management methods, the NCIPP is also created, defining the tasks and responsibilities for the protection of CI objects. NCIPP is reviewed and adopted every few years, and the current program is in force from 2013 until 2019. Figure 1 shows the current model of CI security management.

The main disadvantage of the current methods of CI management is that the documents produced define the tasks, deadlines, and persons/entities responsible for implementation, but do not indicate the methods that individual participants in the process should use. It leads to the formation of methodological and qualitative differences in the developed documents, which hinders their integration at an administrative level and then aggregation between the levels.

An example of the current mechanism of CI management can be seen in an incident in Krakow, which took place on May 19, 2015. The incident was attended by 20 vehicles and 15 people were injured, 10 of whom required hospitalization [27]. The person receiving notification of the incident decided to send an air ambulance, based on the number of victims and damaged vehicles and without waiting for information from the ground rescue team.

In this case, the decision to use the CI rescue system component resulted in saving the life of one of the victims. The person coordinating the action took a decision based on his or her own experience and knowledge of similar cases in the past. Quick access to such data may result in the acceleration of decision making in crisis situations and could be used to verify the proposed action. However, it must be part of a structured system, so that the effectiveness of decisions taken in times of danger or crisis is not only dependent on the knowledge, experience, and mastery of an individual.

To sum up, the current system of crisis management of CI objects allows very wide-ranging discretion to apply methods to identify risks and develop plans to protect the CI objects. Because of the interdisciplinary nature of CI systems, developing CI safety management methods that are effective for each system is very difficult.

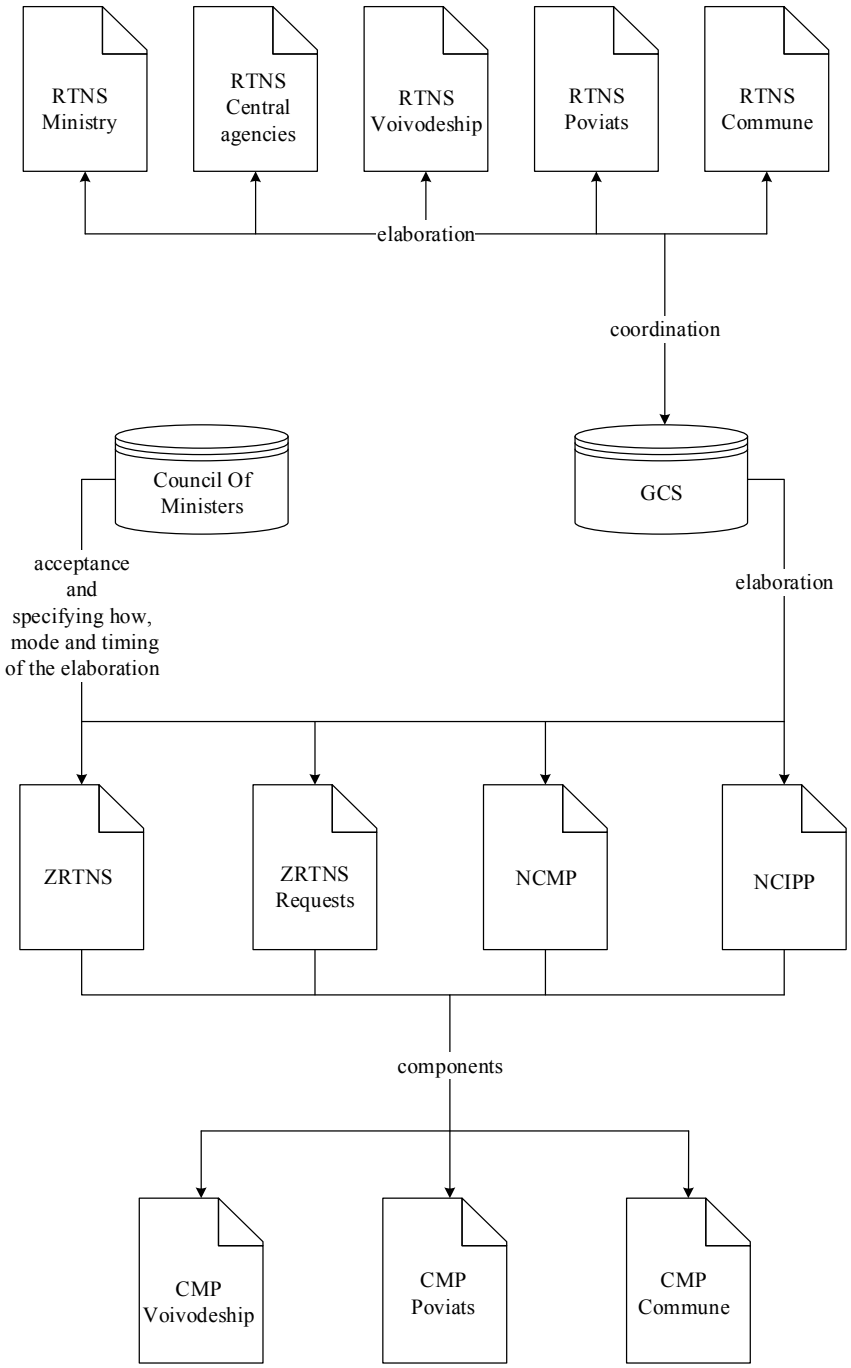

Figure 1. Diagram of the current model of safety management of CI objects
(Source: own analysis based on [24; 18])

Instead of one universal model of conduct within the framework of CI safety management, it is advisable to develop a set of model solutions for individual CI systems. Currently, the effectiveness of actions taken in CI safety management mainly depends on the knowledge, experience, and control of individual people. The aim should be a state in which the effectiveness of CI safety management results from accepted models of conduct and are not solely dependent on an individual. A theoretical basis for the construction of a new CI method of security management could be a situational management concept.

3 Critical infrastructure management systems and a situational approach

The preparation of answers to the question formulated in the paper's introduction, about CI effective management, used the analogy of a CI management safety process and a risk management process in an organization. In practice, a risk management process is concerned with the diagnosis and control of an object, and has the goals of providing international stability and creating conditions for continuing growth [5, 15, and 26].

Teams dealing with risk in companies use different methods of hazard identification and risk analysis, for example, as recommended by the ISO31000 norm: event trees, bow-ties and risk registers based on the experience of team members and their expertise. The use of the concept of knowledge management in the CI safety management process requires an answer to the question as to how to collect, process, and use information resources about threats to CI objects. Due to the diverse problems in this area, it is extremely difficult, or even impossible, to develop a universal mechanism for these processes.

An alternative is to assume that each type of CI object, which is in the system of CI reactors, is unique and requires unique situational management methods, appropriate to the situation. This view is confirmed by Hamrol [8, p. 68], and it should be said that organizations are complex systems with unlimited collections of internal and external feedback.

Therefore, there are no identical situations in which the known standard solutions can be directly applied. Only an examination of a specific situation gives us the possibility of selecting adequate models and allows us to specify their one-time effectiveness. The context of situational management concepts should be understood as a set of characteristics, an objective function, and a set of actions. A set of situational characteristics allows us to identify, classify, and compare with other observed situations. The objective function determines the direction of the aspirations and conditions of achievement, and the set of actions specifies the manner of its implementation.

Instead of universal management methods, in situational topics, it is assumed that [16; 10, pp. 24-25] a systems approach is the appropriate way to formulate general principles and that the situational approach is guided by the rule that every organization is unique and hence requires that, in managing processes, its resources also have situationally unique characteristics, which takes into account the relationship between situations, actions, and results [25, p. 48].

In any case, it is advisable to develop sets of model solutions at different levels and management in aspects of the organization. Model solutions are a set of possibilities, from which the best for the situation must be chosen. Developing a set of model solutions requires using knowledge-gathering mechanisms [21]:

- identification of vulnerable objects,
- hazard identification,
- identifying connections between threats (e.g., the domino effect),
- analysis of the causes of risk,
- vulnerability and the potential impact of the risk
- estimation of the impact of a crisis situation, individually and sequentially,
- data registration about the course of the crisis,
- data registration about the procedures and tools used to resolve the crisis and restore the state to before the occurrence of the crisis.

Thanks to the personal and/or institutional knowledge of resources, the people responsible for crisis management can recognize the symptoms that announce the occurrence of a crisis and take action that will allow them to avoid it or reduce its effects. This proves that the implementation of the principles of the situational approach requires the use of methods and tools for knowledge management.

Knowledge management is a complex notion described, inter alia, by Mikula [17], including different perspectives in the definition: functional, process, instrumental, and institutional. By synthesizing these definitions, it can be said that knowledge management is the process by which an organization generates value on the basis of its intellectual resources or the experiences of its organizational assets [4, pp. 41-42].

In the case of the CI process, safety management procedures and models, which show how effectively a goal is achieved, rely on proven concepts, good practice, and applicable legislation. In this context, it appears that, in the case of the specificity of CI safety management, the resource model is the most widely accepted [14, pp. 169–176; 19, p. 270], which treats knowledge as a resource that is needed and shared, but is also necessary to update during the collection of experiences and gaining access to methods and supporting tools.

One such method is the method of Case Based Reasoning (CBR), based on the observation of expert reasoning. The expert searching for a solution to a particular problem refers to experience (cases, situations) from the past and models it to the present action.

The CBR method treats the case as a pair: the problem and its solution. Both the problem and the solution have characteristics, which can be described as a set of data. The cases are independent, there are no rules, and there are registered actual events and specific situations, which may also be described in the relevant set of data. In essence, CBR boils down to saying that there is a possible solution to the current problem in adapting solutions used in the past for similar problems [23]. In the CBR method, the following steps are performed in a cycle [1]:

- retrieve: the database of cases is searched, for the case most similar to the current case,
- reuse: the way the previous case(s) were solved is a potential solution to the new problem,
- revise: the known solution is applied to the current problem, with the possibility of modifying the solution,
- retain: the problem with the applied solution is stored as a new case.

The CBR method is recommended for use in:

- regular phenomena, which are predictable, executed again doing the same thing, in the same or similar situations, leads to the same or similar results,
- repeats of similar phenomena: small changes in the present issues involve small changes in the way of solving the problem.

These conditions are also often observed in the CI safety management process.

4 Proposed changes to the system

The basis of the Polish CI safety management system is to prepare emergency management plans at all levels of state administration and local government. Plans are developed to respond to the identified safety risks to CI elements and must take into account the provisions of the applicable NCIPP.

A threat is understood as the expected impact on the object or between objects, as a result of which their functional and structural characteristics can degrade. Accordingly, the identification of hazards is the initiating act in activities related to a crisis management process, which should take into account two aspects. The first aspect is the identification of elementary threats that affect the objects and, as a result of this interaction, degrade the functional and structural characteristics of the object, but this interaction does not interfere with the functioning of other objects remaining in relationship with the analyzed object. The second aspect is the identification of complex risks that affect a minimum of two objects and, as a result of this interaction, degrade the functional and structural characteristics of both objects.

The purpose of hazard identification is to prepare actions that will quickly and efficiently eliminate or minimize the possibility of the threat and, in the case where the threat actually happens, eliminate the effects of this emergency. An emergency situation is defined as a range of variables and values of the characteristics that affects anything considered an element of the CI system, or the system as a whole, and prevents it from functioning at the required level.

Studies conducted in the framework of the project "Methodology of risk assessment for the purpose of crisis management systems in the Republic of Poland" show that existing practices in the context of hazard identification of CI system components are as follows. Hazard identification and risk assessment are carried out using an expert method, which is based on expert experience, and/or by analyzing historical cases, if in existence. In public administra-

tion, often the expert is one of the office workers, to whom such duties have been assigned.

The study showed no clear criteria for identifying threats and drew attention to the wide-ranging literature available for classification of threats, which is still being developed and modified. It proves the lack of robust knowledge in this field. In particular, the identification of the connection between threats, which is very important in practice to predicting the development of potential crisis situations, is almost ignored in the methodologies examined. An analysis of crisis management methodologies in Canada, Denmark, Ireland, and Poland [3, 22, 2 and 15] showed no attempts to determine such connections. An analysis of operational risk management methodologies used in business did not indicate such practices, either [7, 6].

According to the observed circumstances, it can be pointed out that the main problem of CI safety management is the lack of a methodical approach to hazard identification and the lack of a development of response plans to implement effective crisis management. Effective management is understood here as taking action aimed at eliminating or reducing the possibility of threats happening, as well as the removal of the consequences and restoration of the state before an emergency situation arises, with the rational involvement of forces and means. This problem is reflected in practice due to the law-obliging public authorities to carry out regular CI hazard analysis.

The concept of CI situational management requires defining a basic conceptual area, which includes the definition of CI, situational management, and security.

The definition of CI has been adopted in accordance with the provisions of the law on crisis management already quoted in this article. Within the concept of situational management it is understood as the impact on a CI object, to maintain or achieve a target level of safety by maintaining or changing the values of the characteristics, describing the examined CI object in a range which allows its operation on the assumed level.. In contrast, CI safety is defined as maintaining a predetermined level of accessibility of public services, depending on the efficiency of the CI objects.

The proposed method of situational management of CI in emergencies consists of three stages: identifying the situation, identifying possible actions, and making decisions.

The implementation of the identifying situations stage of CI objects can be based on the elements of the resource approach. Breaking CI down to its basic components shows that its basis is the resource on which the CI object's processes are carried out. The objects from certain categories are grouped into CI systems. In contrast, the 11 systems specified in the Act on Crisis Management comprise the Polish CI object.

The resource, as part of a material reality (physical) or virtual reality (e.g., conceptual, information, metalinguistic), which has a non-empty set of values and characteristics, has a structure that can be described by a set of variables. By registering the values of the individual characteristics, the particular state of the resource may be indicated, according to the situation in which it is located.

An example of a resource can be a cistern for the transportation of chemicals, which has three characteristics (pump, tank, and hoses). The characteristics of the resource are described by four variables (pump capacity, hoses capacity, integrity of the tank, transported substance). Each variable can take values of specific ranges with the defined limits of the possible states of a given variable. Using this fact, a function can be written that defines all the possible situations in which the resource can be found:

$$S\{(C_1Z_1); (C_2Z_2); (C_3Z_3); (C_3Z_4)\} \quad (1)$$

where:

- S – the resource situation,
- C – the characteristics of the resource,
- Z – the variables describing a particular feature of the resource.

Resources are also vulnerable to risks associated with the characteristics that describe them. Based on the analysis of the characteristics of the resource, it is possible to identify a list of potential threats to the resource. Such an action will make the estimation of the risks that are associated with the CI object easier.

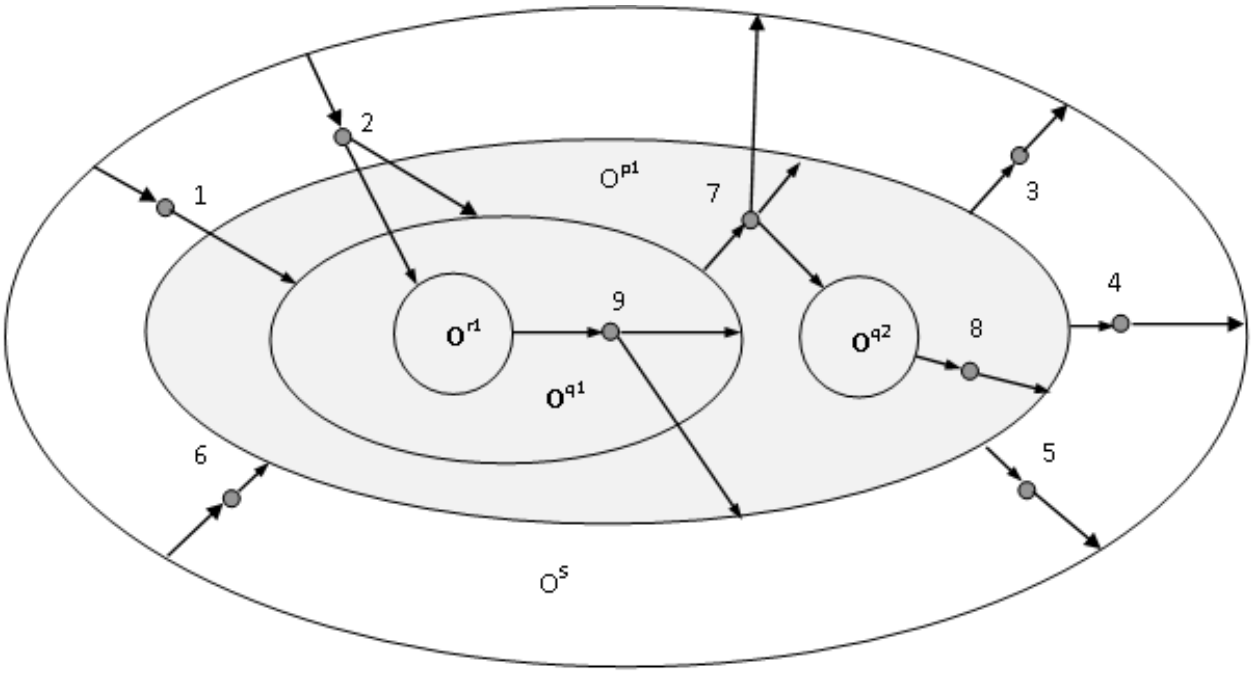

Figure 2. The hypergraphs structure of objects and their connecting channels
(source: [12])

There are connections between resources, which can be defined as a connecting channel between the two resources [13]. The knowledge of the process organization in which the resource is used and combining this with the knowledge about the characteristics of the resources allow the specification of the relationships between them. On this basis, the state of any CI object can be specified, and the entire system of the country, and threats identified at each of its levels.

In turn, the knowledge of the value of the variable characteristics of the resource can determine the susceptibility of the resource to the identified threat. This is illustrated by the example of a hospital dependent on electricity provided by the municipal grid. This institution is vulnerable to the threat of a power failure. Buying a power generator reduces this susceptibility.

Using two criteria, the correct functioning and knowledge about the reaction to a threat, it is possible to divide circumstances into a designated set, in which this resource may be found. The possible situations will then be divided into four categories:

1) Acceptable state: the considered resource is functioning correctly; defined sets of actions for the individual hazards that are associated with it are in place.
2) Emergency state: the considered resource is not functioning correctly; sets of activities designed to restore the desired state of the resource are known.
3) Warning state: the considered resource is functioning correctly; there are no developed plans to respond to identified threats.
4) Crisis state: the considered resource is not functioning correctly; there are no developed plans to respond to identified threats.

Similarly, a discussion can then start to determine the significance of identified risks, which arises from the characteristics of the analyzed resource. Using knowledge of the probability of a particular hazard and its effects (financial, number of victims, time needed to restore the resource, etc.), the classification of types of risk can be made: low risk, medium risk, high risk. It is also possible to determine a level of negligible risk, a risk that the organization is aware of but takes no preventive action due to the lack of economic justification.

Describing CI resources by key features, it is possible to develop a situation matrix, in which the resource can be found. Part of the matrix can be isolated clusters of similar situations in terms of, for example, the consequences of a malfunction, or sets of actions that can be taken to restore the desired state of the resource. Situation sets of activities can be assigned to individual groups and the amount estimated of forces and means that have worked in the past and helped to maintain the target level of CI safety [11, 18].

The application of correct functioning criteria and knowledge of the reactions to identified threats allows us to identify acceptable, emergency, warning, and crisis states. Collecting data on the variables value of the characteristics of the resource means that the situation in which the resource is current can be identified and monitored. Following the variability of the situation in time, it is possible to predict an undesirable state and take appropriate action in advance.

The implementation of this mechanism requires the collection of data on incidents of malfunctioning CI resources, the effectiveness and costs of actions taken to ensure CI safety, and the development of criteria for identifying similar situations. Data on incidents and responses to them may come both from observations and experiences of other CI objects.

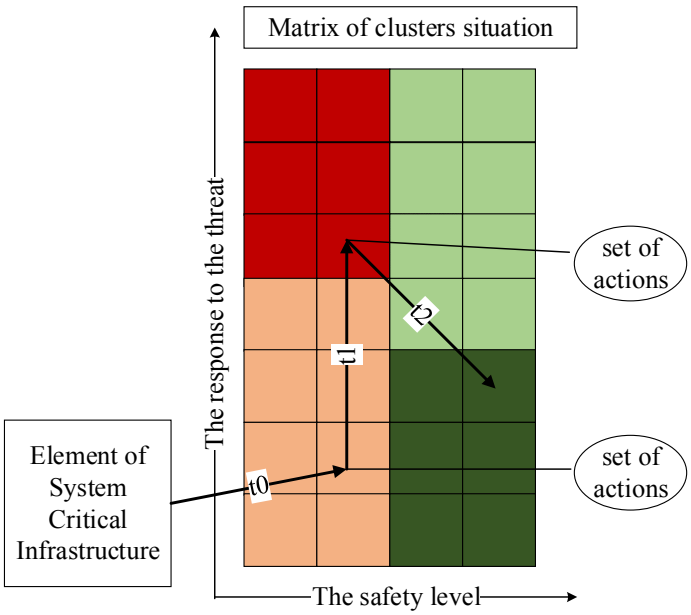

Figure 3. Schematic diagram of the process of CI safety monitoring
(*source:* own materials)

The second stage task of the proposed method is to identify a set of actions to maintain or achieve a desired state in the analyzed CI resource. The theoretical basis of this stage is the CBR knowledge management method. In this method, it is assumed that the case comprises a pair: the identified problem and its solution. By adopting this approach for the needs of CI situational management, it is proposed that the case is defined as a:

- registered situation: due to the value describing the variable characteristics and parameters of the CI resource,
- objective function: the goal that should be pursued,
- operation: the best performing objective function, selected from a set of effective actions taken in the past.

The progress of the CBR is achieved in the cycle illustrated in Fig. 4.

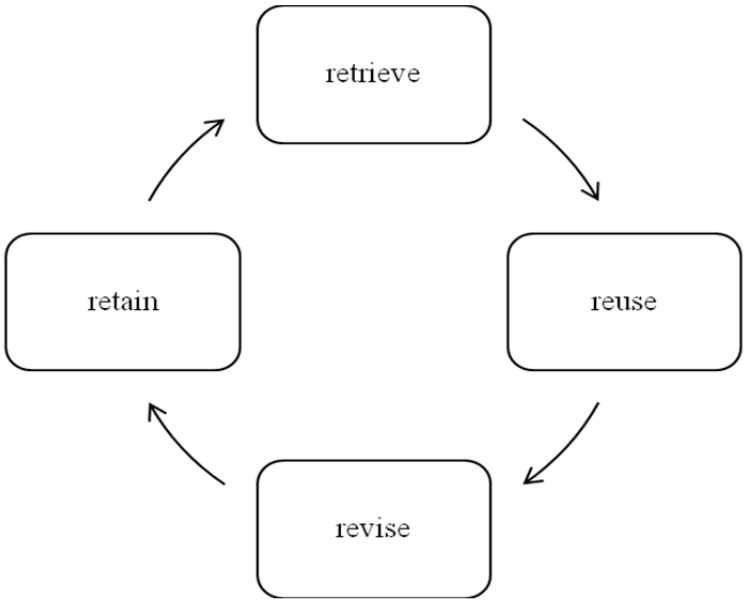

Figure 4. Cycle of proceedings in the CBR method
(*source:* [1])

Taking the situation of the CI resource identified in the first stage of CI situational management as a starting point and using the criteria for determining the similarity of the situation, a similar situation to the observed situation can be retrieved from the database of cases. It can then be checked whether the effective actions taken in the past can be used to achieve the intended purpose of the current task. If the verification of the effectiveness of the actions is positive, the economic usefulness of action should be assessed. Otherwise, the manual development of a plan to achieve the objective, understood as a specific security level of the CI object, should be carried out.

The advantages of this process are the low costs of acquiring knowledge, the high user acceptance of the methods, and learning through memorization. A disadvantage is the need for a database of cases covering clusters of similar situations, as indicated in the first step of the method.

The implementation of the third stage of the CI situational management is associated with the assessment of the suitability of actions implemented in the second stage. After determining whether the actions taken in the past in a similar situation to the current one will achieve the expected goal, it should be decided whether these actions are economically justified. Assessing suitability can be based on the principle that the cost of measures taken is less than or equal to the risks associated with the observed situation. This demand is consistent with the provisions of the applicable NCIPP. The value of the risk situation can be determined using the formula:

$$R = P * U * S \quad (2)$$

where:

- R – value of risks,
- P – probability of crisis situation [0–100%],
- U – susceptibility of the resource to the threat [0–100%],
- S – effect (point scale or the size of the losses incurred as a result of the materialization of risks).

An example illustrating this principle is the problem of maintaining an airport runway in good condition during the winter. The threat is the potential heavy snowfall (P = 60%). An airport's susceptibility to this threat, after the analysis of available forces and means, has been assessed at the level of U = 40%. The potential effect of the materialization of risks of having a paralyzed airport for one day would be loss of 150 000 Polish Zloty (PLN).

A possible solution is to hire additional resources (people and equipment) to clear the runway, which would cost K = 60 000 PLN per day. With these assumptions, undertaking additional activities to prevent possible losses is economically unprofitable.

The value of risk in this case would be R_1 = 36 000 PLN. However, if the probability rises, for example, by 10%, and the susceptibility of airport to the threat increases by 20% due to, for example the absence of some staff, it turns out that the proposed actions are economically justified, because the risk value is R_2 = 63 000 PLN.

The principle works well in situations where the effects of the materialization of the risk can be expressed as financial costs. Unfortunately, financial losses are not the only consequences of security incidents. In cases of exposure to threat to life and human health or the loss of valuable cultural assets, it is necessary to adopt other criteria to assess the usefulness of a response to identified threats.

In summary, the proposed method of CI situational management consists of three stages: identifying the situation, identifying possible actions, and taking decisions. As part of the identification of the situation stage, identifying the critical resources for individual CI objects is necessary. Next, it is important to describe it by its characteristics and assign variables that will allow us to take measurements. The registered values will be used to indicate a situation in which the CI object exists. Subsequently it is determined in which category the observed situation should be (acceptable, emergency, warning, crisis). If the situation requires it, the second and the third steps of method are implemented: finding a similar situation in the case database and checking whether the action taken in the past can be applied to the current situation. If so, the suitability of the actions identified is assessed in economic terms. An evaluation is carried out according to established criteria and requires hazard identification based on the characteristics of critical resources. Then the reciprocal influence of resources is identified, the susceptibility of resources to identified threats assessed, and the probability of their materialization is also assessed. With the above data it is possible to determine the value of the risk and, by comparing it with the costs of a potential reaction to identified threats, to assess their usefulness. Fig. 5 shows a schematic diagram of the realization of the CI situational management method.

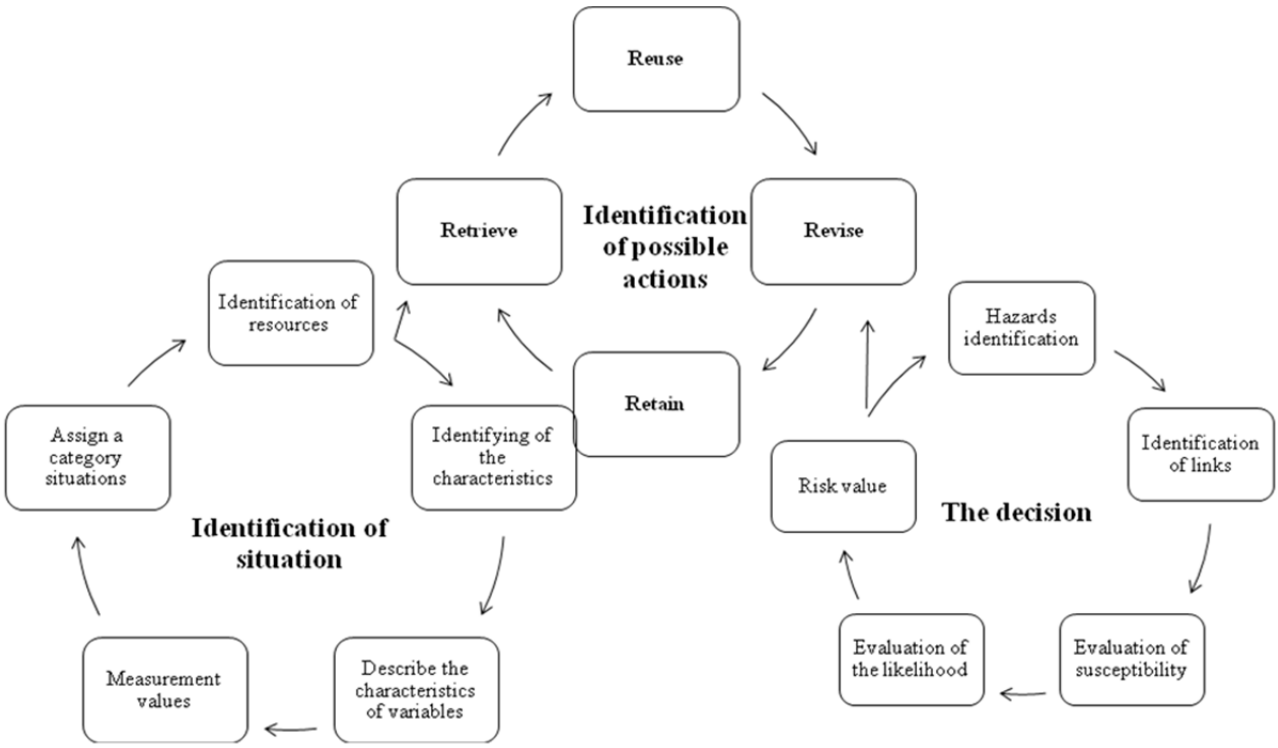

Figure 5. Schematic diagram of the situational management method of CI (*source:* own materials)

The concept of the situational management method of CI is the proposal of a methodical procedure in the area of identifying situations, finding a situation similar to the one being observed, and assessing the suitability of the actions taken in the past in response to the identified danger.

This method can also be used to develop information systems, where the task is to support the identified actions. Potential recipients of this method are units of central and local government, that is, GCS, Crisis Management Centers, Crisis Management Teams and all operators of CI objects, who regularly face the problem of providing secure and stable operation of the country's CI elements. Developed within the CI framework, the situational management model of conduct is designed to:

- accumulate knowledge about the state of the CI,
- identify development scenarios of crisis situations,
- plan activities within the framework of CI safety assurance,
- monitor the situation of CI objects and systems, and
- respond to identified situations.

5 Summary

Ensuring an adequate level of security of CI objects, which is necessary for the functioning of state and society, is the duty of public authorities. The studies conducted in the framework of the project "Methodology of risk assessment for the purpose of crisis management systems in the Republic of Poland" have demonstrated the need for continuous improvement of the procedures adopted that are related to the safety of CI objects. This need is determined by constant changes in the internal and external environment of CI objects and common technological developments. These studies have shown an insufficient application of knowledge about emergency situations in the past. The experience of these events are inefficiently used in the estimation of the necessary forces to reduce risks, minimize the possibility of interference, and mitigate the effects of crisis events in the future.

Using knowledge of the past can greatly improve procedures to respond to identified threats, which can allow a faster deployment of more efficient and effective preventive measures, minimize the possibility of the appearance of interference, and, if necessary, remove the effects of an emergency.

Effective use of knowledge derived from the experience of the past requires tools to identify and compare the registered situations. This mechanism is described in the theoretical part of the concepts of situational management and requires the implementation of knowledge management methods. Theoretical assumptions of the situational approach and knowledge management are concentrated in the CBR method, which involves registering the situation observed as the basis case in the database and, on the basis of experience, providing decision-makers with options for action that have worked in the past.

6 References

[1] Aamodt A., Plaza E. - *Case-Based Reasoning: Foundational Issues, Methodological Variation and System Approaches* [in] Artificial Intelligence Communications, 7(1), 1994.

[2] *A National Risk Assessment for Ireland* [in] An Oifig um Pleanáil Éigeandála Office of Emergency Planning, December 2012,

[3] www.emergencyplanning.ie/media/docs/A%20National%20Risk%20Assessment%20for%20Ireland%20Published.pdf, (access: 22.07.2015).

[4] *All Hazards Risk Assessment* [in] Methodology Guidelines 2012–2013, Canada 2012, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/index-eng.aspx, (access: 22.07. 2015).

[5] Bukowitz W.R., Williams R.L. - *The Knowledge Management Fieldbook* [in] Financial Times – Prentice Hall, Pearson Education Limited, Harlow – London 1999.

[6] Conrow E.H. - *Effective Risk Management. Some Keys to Success*, AIAA Inc., 2000.

[7] *Departament Audytu Sektora Finansów Publicznych Ministerstwa Finansów*, www.archbip.mf.gov.pl/bip/_files_/audyt_wewn_i_kontrola_zarz/kontrola_zarzadcza_w_sektorze_publicznym

/metodyka_i_dobre_praktyki/metodyka/zarzadzanie_ryzykiem.pdf, (access: 22.07.2015).

[8] *Federation of European Risk Management Associations – FERMA*, www.ferma.eu (access: 20.07.2015).

[9] Hamrol A. - *Zarządzanie jakością. Teoria i praktyka*, PWN, Warszawa 1998.

[10] PN-ISO 31000:2012 - *Zarządzanie ryzykiem – Zasady i wytyczne*, http://sklep.pkn.pl/pn-iso-31000-2012p.html, (access: 20.07.2015).

[11] Kaczmarek B., Sikorski C. - *Podstawy zarządzania – zachowania organizacyjne*, 1996.

[12] Krupa T., Maj K. - *The management method preventing a Crisis Situation* [in] Foundations of Management - International Journal. Faculty of Management WUT, No 2, Vol. 2, 2010.

[13] Krupa T. - *Semiotyka kluczowych pojęć tezaurusa ciągłości działania w infrastrukturze krytycznej*, Logistyka nr 5/2014.

[14] Krupa T. - *V.A. Gorbatov Theory of Characterization – Solutions and Examples* [in] Foundations of Management - International Journal. Faculty of Management WUT, No 3, Vol. 5, 2013.

[15] Krupski R., Niemczyk J., Stańczyk-Hugiet E. - *Koncepcje strategii organizacji*, PWE, Warszawa 2009.

[16] Loader D. - *Operations risk managing a key component of operational risk*, 2006.

[17] Maracz T. - *Ujęcie sytuacyjne* [in] Współczesne teorie organizacji, (red.) Koźmiński A., Warszawa 1983.

[18] Mikuła B. - *Zadania organizacji w zakresie zarządzania wiedzą*, E-mentor nr 5 (17) / 2006, www.e-mentor.edu.pl/artykul/index/numer/17/id/368 (access: 13.05.2015).

[19] *National Critical Infrastructure Protection Programme,* Polska 2013, http://GCS.test.safehost.pl/ ?p=3173, (access: 23.07.2015).

[20] Probst G., Raub S., Romhardt K. - *Zarządzanie wiedzą w organizacji*, Oficyna Ekonomiczna, Kraków 2002.

[21] Rostek K., Wiśniewski M. - *Metoda wspomagania organizacji logistyki w scenariuszach reagowania na sytuacje kryzysowe w ratownictwie*, Logistyka nr 4/2014.

[22] Rostek K., Wiśniewski M. - *Zarządzanie wiedzą w doskonaleniu i rozwoju systemu bezpieczeństwa*, Logistyka nr 5/2014.

[23] *RVA model Introduction and User Guide DEMA's Model for Risk and Vulnerability Analysis*, Danish Emergency Management Agency, 2006, http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx, (access: 19.07.2015).

[24] Riesbeck C., Schank R. - *Inside Case-Based Reasoning*, Lawrence Erlbaum 1989.

[25] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, www.gcs.gov.pl/wp-content/uploads/ ustawa-o-zarz%C4%85dzaniu-kryzysowym.pdf, (access: 23.07.2015).

[26] Wajda A. - *Podstawy nauki o zarządzaniu organizacjami*, Warszawa 2003.

[27] Zawiła-Niedźwiecki J. - *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, Wydawnictwo edu-Libri, Kraków 2013.

[28] www.tvp.info/20117254/karambol-w-krakowie-tir-staranowal-19-samochodow-10-osob-trafilo-do-szpitala, (access: 15.07.2015).