MATRIX METHOD OF ASSESSING RISK CONFORMITY IN THE CONTEXT OF ENVIRONMENTAL SECURITY

M.Sc. Baev G. PhD.[1], Dimitrov M.[1], Dimitrov I. [1]
Vasil Levski National Military University, Veliko Tarnovo, Republic of Bulgaria [1]

gkbaev@nvu.bg, amirodimitrov@abv.bg, idimgb@gmail.com

Abstract: The research offers a simple matrix model of analysis for ranking risk levels in critical and emergency situations. The leading principles, which should be taken into consideration can be arranged in a group of steps, for example the qualification and grading of imminent danger and the level of endangerment of key assets, determining of the processes which can lead to harm and also the value of the structures susceptible to damage and the damage itself.

Keywords: MATRIX, NATIONAL SECURITY, ENVIRONMENT, DEFENSE

1. Introduction

The preliminary assessment of the threats aimed at the security of given process, event or a system is a mechanism creating a variety of tendencies connected with disaster management. The practice said above gives us the ability to engineer a strategy for system control.

Thanks to the processes of planning and forecasting there is an increased chance of reacting adequately and quickly if a disastrous event happens and its boost the future solving of the problem. An example for a decent tool in the field of disaster management is the remote examination of such happenings with the help of artificial satellites.

The usage of man-made objects orbiting our planet's orbit and the methods of their exploitation are crucial for the control of the environment security on the grounds of their precision and supreme scale of effectiveness. With their help a high volume of valuable intel showing the state of the environment is being able to be collected and furthermore the data gathered will aid the long and short-term danger scenarios. [1, 8,12,13,16,18]

2. Prerequisites and means for solving the problem

A supporting instrument in finding a solution to an environmental crisis are hypotheses. They tend to have a more general character in comparison with prognoses due to the fact that they mainly use guesses and ideas as a source that stemmed from risk analysis. [1,2,5,7]

The professional generation of a prognose for a single case is of utmost importance for the defining of the set of tasks given for achieving a stable level of environment security and its imminent support.

The main approach to overcome the dangers is the usage of prognosis techniques, used mainly for making conclusions and making a review of the needed resources for countermeasuring existing threats. [9,10]

The whole process of combating risks depends on vulnerability and danger measuring and analysis. Risk grading is important for determining the value of resources, their flaws and also the threats themselves, all of whom are able to be realized in the system and lead to ecological risks and compromising the environment. Risk grading exist when the danger is measured and the shortcomings of the resources are classified – a potential entry point for real troubles, and on the other hand the creation of adequate ways to reduce damage to the world's ecosystem. [11,14,15]

Measuring the risk and the risk factor are the first crucial step in threat analysis and management of environment security. Every asset in the security system must be evaluated in terms of its importance to the whole structure of danger control.

Assets should be categorized in different types with respect to their value and influence on the whole anti-risk concept. Of a great concern is the choice of criteria for classification of resources. If we dive deeper into the field of environment security we can see that it is nearly impossible to put a price on assets like the World Ocean for example. For an effective measurement we should grade the assets on a scale from 1 to 10 and for creating an easier measure method we can arrange resources concerning their quality from "very low" to "very high". The grading must be a responsibility of a team of experts or organization sorting the assets in their respective categories. [1,6,7,17]

3. Solution of the examined problem

Looking at the ISO accepted standard worldwide which regular risk assessment criteries we can come with acceptable terms for quality grading from the standards of informational security and the abovementioned used successfully in the field of environment security due to the lack of ISO algorithm in environment security.

The terms included should be as following: "lowest", "very low" "low", "medium", "high", "very high" and "of critical importance". The range of grading should be prepared by experts in the field and there must be no confusion in the usage of grading terms. The following terms are applicable – primary value, renewing value and exchange value.[1,11,12,13,]

Of a particular importance is the creation of a grading system. The higher the number of grading levels is, the better is the detail itself. In determining the threats we can utilize the recommended approach in Application C of the ISO/IEC 13335-3 standard where Application D contains the threats created by deliberate actions, A – random actions and E – natural threats.[1,17,18]

Table 1: *Ecological threats and their grading in accord with the international standard/ISO/IEC TR 13335-3:1998 Annex 1*

	THREAT	ВИД
1	Earthquake	E, A
2	Flood	E, A, D
3	Hurricane	E, A
4	Lightning strike	E, A
5	Radioactive contamination	A, D
6	Electromagnetic influences	A, D
7	Dust storms	E, A
8	Fire	E, A, D
9	Extreme values of temperature and humidity	E, A
10	Heavy snowfall	E, A
11	Drought	E, A
12	Volcanic activity	E, A
13	Tsunami	E, A
14	Other risks	

It is of great importance in evaluating the threats what question will be given when the asset is rated. For a more simple way of rating a sheet of questions should be created for every group of assets that are important for risk rating and with which risk can be evaluated and the level of vulnerability.

For every answered question in the quiz points will be allocated to the database and the whole asset will be compared with ranks thus giving the threat level (See matrix in 2) [1,17,18]

Table 2: *Scale for determination of threat and vulnerability*

Asset Value	Threat Level								
	Low			Medium			High		
	Level of vulnerability			*Level of vulnerability *			*Level of vulnerability*		
	L	M	H	L	M	H	L	M	H
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

4. Results and discussion

The amount of value of the assets and the threat level and vulnerability, according to every type of influence are inserted in the matrix to determine every combination of the supposed risk level on the scale with a random equation – in cases 1-8. The same are shown in Table 2.

For every asset the vulnerable points and their threats are evaluated. If there are vulnerabilities, but there are no threats or there are threats but no vulnerabilities it is assumed that there is no risk present.

In those cases there is a careful measurement of a possible change in the status quo so unexpected risks are successfully evaded. Afterwards the queue in the matrix is calculated based on the value of the asset and the column adjusted to the value – by the threat and vulnerability level. [1,7,9,15,16,17,18]

The size of the matrix from the point of view of the categories characterising the level of threat and vulnerability of the asset are chosen depending on the specification of the needs of the mentioned case. The value of this method is concluded in the ability to sort threats and dangers alike.

5. Conclusion

For determining the dependence between factors and influence and the possibility for a threat to happen (with considering the character of vulnerability) a matrix can be proposed.

After defining, in the final phase of grading a summary grading of the risk must be done. The risk shows itself as a stat of the vulnerability of the system and his value is influenced by the resources, threats, the realisations of possibilities of the dangers in vulnerable points and the existing measures for deterrence and defence, thus lowering vulnerability and threat to the ecosystem.

The goal of the analysis is consisting of the determination and grading of the risks that are influencing the system and its resources with the goal of choosing the adequate countermeasures.

6. References:

1.Млеченков М., Учебно пособие. Методика за разработване на система за информационна сигурност, ИМК фак. "А, ПВО и КИС", Шумен 2010 г.

2. Bründl, M., Romang, H. E., Bischof, N., and Rheinberger, C. M.: The risk concept and its application in natural hazard risk management in Switzerland, Nat. Hazards Earth Syst. Sci., 9, 801–813

3. Eiser, J. R., Bostrom, A., Burton, I., Johnston, D. M., Mc-Clure, J., Paton, D., and van der White, M. P.: Risk interpretation and action: a conceptual framework for responses to natural hazards, Int. J. Disaster Risk Reduc., 1, 5–16

4. Erden, T. and Co¸skun, M. Z.: Multi-criteria site selection for fire services: the interaction with analytic hierarchy process and geographic information systems, Nat. Hazards Earth Syst. Sci., 10, 2127–2134

5. Glade, T. and Nadim, F.: Early warning systems for natural hazards and risks, Nat. Hazards, 70, 1669–1671, 2014

6. Intrieri, E., Gigli, G., Casagli, N., and Nadim, F.: Brief communication “Landslide Early Warning System: toolbox and general concepts”, Nat. Hazards Earth Syst. Sci., 13, 85–90

7. Lindell, M. K. and Hwang, S. N.: Household’s perceived personal risk and responses in a multihazard environment, Risk Anal., 28, 539–556

8. Rogers, D. and Tsirkunov, V.: Implementing Hazard Early Warning Systems, Global Facility for Disaster Reduction and Recovery, WCIDS Report 11-03, 2011

9. Slovic, P., Finucane, M. L., Peters, E., and MacGregor, D. G.: Risk as analysis and risk as feelings: some thoughts about affect, reason, risk, and rationality, Risk Anal., 24, 311–322

10. Wachinger G., Renn O., Begg C., and Kuhlicke C.: The Risk Perception Paradox – Implications for Governance and Communication of Natural Hazards. Risk Anal., 33, 1049–1065

11. ISO 140001:2015

12. ISO 270001:2013

13. ISO 31000:2009

14. ISO 31010:2009

15. ISO/IEC 27000:2009

16. ISO/IEC 27005:2009

17. ISO/IEC Guide 73

18. ISO/IEC TR 13335-3:1998