Advanced system for risk assessment of the security expressed in the complex labor system and strategic objectives of national interest

GABRIEL – DRAGOŞ VASILESCU[1], TIBERIU – ATILA CSASZAR[2], STELA DINESCU[3], VALERIU PLEŞEA[4]
[1, 2,]INSEMEX, [3]Universitatea Petrosani, [4]ICPM SA Petroşani
[1, 2] G-ral Vasile Milea Street no.32-34, Petroşani
[3]Universitatii Street no.20, Petroşani,
[4]M. Viteazul Street no.3, 332006, Petroşani
ROMANIA

cercetator2006@yahoo.com, tiberiu.csaszar@insemex.ro, steladinescu@yahoo.com, vplesea@yahoo.com

Abstract: - In the present paper, a technical approach on establishing scientifically based tools for the quantification of threats and vulnerabilities or potential or apparent specific national security system, identified at a time, to substantiate of quantitative and qualitative risk and security establishment, wittingly, the detailed controls to eliminate or reduce hazardous situations arising from these factors disturbances. Results obtained from the investigation and diagnosis of national security, based on the methodology presented, leading to overall assessment of risk associated security status of specific environmental threats event and/or vulnerabilities identified in order substantiate and implementation of appropriate programs of action with maximum emergency/necessity or urgency/need to eliminate or reduce the dangerous situations that may affect national security.

Key-Words: - risk, negligible event, credibility, national security, probability, strategic objectives, vulnerabilities

1 Considerations related to the taken in risk studies

The specialized terminology in the theory of decision, the decision is a choice that involves a certain risk, based on several versions of possible actions.

Decision involving the application of Principle, relates to the interpretation of events″ ″practical certainty considered quasi-impossible, and states as follows: "If the probability of producing a certain event E is, in a given experience is sufficiently low, it can be considered that if the experience is made once, the event E can not occur [1,6].

This definition is adapted, in the same way, for the probabilities close to 1 that corresponds to almost surely certain events.

Failure by mathematical demonstration of this principle is obvious, but it is confirmed by everyday experience, which allows to formalize personal experience (subjective).

In fact, starting from such considerations most decisions are taken everyday, ignoring usually events with probabilities close to 0, a priori regarded as impossible a priori probabilities or adjacent to 1, ″and imposibilities″ ″such uncertitudines″ production of an event in the experience, be used with caution in security analysis. Indeed, "real time observation or practice" may be of several orders of magnitude smaller than that which would be needed to observe the undesired event taken into account by the security objective. It follows that such an event should not be a priori excluded from the analysis, if the only justification is that he has never been observed, given that temporal proximity of an event is not reflected by its probability of occurence.

Practical certainty principle stems from the law of large numbers, which reinforces the claim that "when a number of testing experience increased indefinitely, the frequency of observation of an event considered possible result, tends to a limit which is equal to the probability of occurence. In relation to the principle of practical certainty, this probability is adjacent to 0 or 1.

The large number of observations made on a given event is the determining factor that ensures the confidence in the resulting consequences of decisions.

Entropy maximization principle allows selection from series a set of observations related to the functioning of a system of all information used effectively to guide the decision.

Specifically, the existing legal regulations and procedures are designed to eliminate random factors in the design, implementation and operation of a system. In other words, compliance with regulations and rules for establishing links between actions and effects belonging to Zone of certainty, enabling the practical application of

the principle of certainty.

It becomes clear that a comprehensive system security - or at least its good operation - can be achieved only inside the certainty, an area whose boundaries were fixed only by taking into consideration the gain experience, ie the errors observed previously and subsequently" corrected.

Finally, to improve the basic concept of security systems, a very small probability and may be associated to the concept of "rare event" that G. Morlat defines it as follows: *"A rare event in the sense of security of systems, is an event that can cause serious consequences, and that, through decisions taken must be given a very low probability"* [3].

2 Setting the probability threshold in risk analysis

Events considered sometimes quasi-impossible, whose probability is extremely low production may occur in industrial practice.

Risk studies, may consider various stages of these events in order to:

a.- define the objectives for which the subjective probabilities associated explicitly to undesirable events**.**

b.- select scenarios likely to generate undesirable events. Most times, based on a qualitative analysis, the decision-maker considers the most credible scenarios of the identified or imagined by analysis.

c.- use in the post-evaluation of the probability of each scenario, when certain combinations of events may lead to negligible values.

These stages of analysis and assessment to meet the three stages of decision with a direct impact on the estimated risk level of system.

There is thus a major problem in all phases of risk studies, namely: "from what probability threshold can be neglected or improbable events or combinations of identified events, events to be ignored in the decisions process?"

2.1 Different methods of calculating the probability

Be there an undesirable event E in relation to the safe to work in a job, having a production probability p, the same each year. Thus, one can calculate the probability of the following events:

- ✓ the occurence of the event E in the year n
- ✓ the occurence of the event E at least once in n consecutive years
- ✓ the occurence of the event is between years m and n

a) The occurence of the event E in the year n

The probability p_n of the event E_n, during year n, in relation to the safe of the business can write:

$$p_n = \Pr\left(\bigcup_{i=1,n-1} \overline{E_i} \right) \cdot \Pr(E_n) = (1-p)^{n-1} \cdot p \quad (1)$$

b) The occurence of the event E at least once in n consecutive years

The probability P_n, in this situation can be directly evaluated starting from Poincaré's formula for independent events E_i.

$$P_n = \Pr\left(\bigcup_i E_i \right) = 1 - (1-p)^n \quad (2)$$

c) The occurence of the event is between years m and n

The probability of this event is obtained directly from the previous equation:

$$P_{n-m} = P_n - P_m = (1-p)^m - (1-p)^n \quad (3)$$

Approximating the value of equation P_n

For values p > 0,1 the basic equation can not be approximated and therefore for $n = \frac{1}{p}$ one should use of equation:

$$P_n = 1 - (1-p)^{\frac{1}{p}} \quad (4)$$

For values $p \le 0$, the first approximation of the basic equation is:

$$(1-p) \approx e^{-p} \text{ where: } P_n = 1 - e^{-np} \quad (5)$$

Therefore, for $n = \frac{1}{p}$ one can be calculate directly P_n

$$P_n = 1 - e^{-1} \approx 0{,}632 \quad (6)$$

The calculation using the exact equation gives a value of 0.6513 calculated for p = 0,1 şi n = 10.

For $p \le 0{,}1$ and $np \le 0{,}1$ the second approximation of the basic (exact) equation gives the following expression**:**

$$e^{-np} \approx 1 - np \text{ where } P_n \approx np$$

In this case, P_n can not be calculated for $n = \frac{1}{p}$ because this last approximation is valid for only for np <0.1, but not for np = 1.

Practical application:

1) If p = 0,5 , then $P_n = 1 - 0{,}5^n$
   - for n = 2, P_2 = 0,7500
   - for n = 4, P_4 = 0,9375
   - for n = 10, P_{10} = 0,9990
   - for n = 15, P_{15} = 0,999969
2) If p = 0,1, then $P_n = 1 - e^{-0{,}1n}$
   - for n = 2, P_2 = 0,183 (0,1900)
   - for n = 4, P_4 = 0,397 (0,3434)
   - for n = 10, P_{10} = 0,6321 (0,6513)
   - for n = 50, P_{50} = 0,9933 (0,9948)
   - for n = 100, P_{100} = 0,999955 (0,999973)

where the brackets are given the results calculated starting from the exact equation**.**

Approximation tends to underestimate the probabilities P_n.

3) If p = 0,01 and np < 0,1, then P_n = np

- for n = 2, $P_2 = 2.^{10\text{-}3}$ (0,0019)
- for n = 10, $P_{10} = 10^{-2}$ (0,0099)
- for n = 50, $P_{50} = 5.10^{-2}$ (0, 0488)
- for n = 100, P_{100} = 0,1(0,095)

For n<100, the approximation of the equation is not valid. Thus for n = 500, P_{500} = 0,5 (0,3936) is calculated directly. Approximation tends to over-estimated the probabilities P_n.

In conclusion, it is false to state that if an annual event whose probability is a priori equal to p, this will occur with a probability equal to 1 (certainty) after $n = \frac{1}{p}$ years.

2.2 The credibility of the security objective

The security objective analyzed during the risk study can be defined by two issues [2,4,5]:

-Defining an unwanted event

-Frequency or credibility associated with undesirable event

The credibility of the security objective of a system is directly related to the security and demonstrated level that can be defined :

-by the ambition of the security objective

-confidence in the materialization of that goal with the help of a well identified and clearly described under a security plan set of tasks

Although in theory there can be defined and set very ambitious goals of security, however, achieving a certain level of security is not a certainty, it can only be estimated using probabilistic tools, starting from available data. Therefore, a level of security is based on the confidence gained during the studies and activities undertaken during the design, manufacture etc., on current or past programs. This fact highlights the real problem related to the credibility of demonstrated operations for security objectives that correspond mainly to effectiveness of ensuring security, validated by experimental verification of the level considered (activity, system, subsystem, etc.). Experimental verification may be-in terms of material either impossible or unacceptable, taking into account the damage that may result. This inability is given both by the considerable number of tests to be conducted in order to observe the undesired event defined by the security objective and by the fact that the event that can be found outside the test.

Available data for evaluation by probabilistic techniques, is obtained from the studies and activities undertaken during the design, implementation and operation of a system, a situation which determines the of the analysis credibility of the objectives of security.

Even if, in some cases, evaluating the security level of a system can be made with the laws of probability of extreme values, in most security studies scenarios for the production of accidents, are being modelled whose credibility is characterized by:

- representative models, particularly given the comprehensive nature defined by the number of parameters or internal and external variables of the system and by the laws that govern them;
- reliable data resulting from "natural" uncertainty (ignorance) on validation procedures and the findings and their interpretation.

This should not be compared with the uncertainty associated to the statement on, the a priori impossibility of defined of the undesirable event in the security objective.

If in the first case there can be investigated and proposeal suitable measures in the second case the statement *″such occur second shall maintain the real state of uncertainty, with potentially catastrophic* consequences which could be avoided.

2.3 Choice of possible scenarios in a risk study

Identifying scenarios that can lead to an undesirable event depends on experience and skills of experts with expertise in the preliminary analysis of risks for the system under consideration.

The scenarios in this phase can be classified into the following categories [1]**:**

C1: Scenarios already observed and interpreted as a realistic ones

C2: Scenarios already seen but regarded as unrealistic, given the measures taken

C3: Scenarios virtually unnoticed but considered the realistic ones

C4: Scenarios unnoticed and considered unrealistic one

Quality assessment between realistic and unrealistic scenarios depend on the amount of knowledge specific to the team of analysts and complemented by that of policy makers, the lower one it has a weighing considerably duet o his organizational role**.**

Decision-maker's dilemma, in most cases is as follows**:**

- eighter to reject the scenario considered less credible over the life of the system, accepting, more or less consciously, the possible consequences. A decision of this type does not change the system design, but it may result, additional operating costs, which can lead (in extreme cases) to cessation of work within the

system (first accident with media implications considered as unacceptable)

- or to accept to take into account a possible scenario, but a priori considered it as unlikely to occur during the life of the system. This decision may introduce additional technical, economic or operational constraints.

It is noted that, depending on the risk component considered (probability and severity), the decision-maker is forced to move from one extreme to another**:**

- ✓ taking into account only low probability, the scenario will not be accepted. It is a typical short-term decision
- ✓ if the seriousness of the consequences, is considered primarly the scenario will be considered regardless of the likelihood of occurence. This as a long term decision.

In the domain of uncertainty, a rule of decision on the consideration of scenarios is to give them a priori a level of plausibility startines from the objective associated to the considered undesirable event. This rule shall not be used without a prior evaluation. The field of ignorance is not covered in any of the presented cases, and there is no guarantee, irrespective of the effort made in terms of scenarios identified and considered.

3 Setting the calculated value related to the absolute thereshold negligible probability

A particularly important aspect during the evaluation of security systems is determined by setting the negligible event "e" whose probability p is to indicate the lower limit during probability calculations and assessments used in risk studies.

In relation to a global event that shows a state event of a phenomenon that can serve as a reference to the principle of practical certainty, we shall consider the assumption that p is of the same order of magnitude as a function of the probability Pr (E).

For example, we can define the event E as survival (existence) of the universe after N years, knowing that he is n years. Event E, can be associated to probability q and a lifetime T, which in terms of formal link between the elements so defined, can be expressed as follows**:**

$\Pr(T \geq n, T \geq N) = \Pr(T \geq N)$ with $n < N = \Pr(T \geq n) \cdot \Pr(T \geq N / T \geq n)$

with $\Pr(T \geq N / T \geq n) = q$

which can be written**:**

$$\frac{\Pr(T \geq N)}{\Pr(T \geq n)} = q \qquad (7)$$

Therefore:

- assuming the equiprobability hypothesis of the annual disappearance p can be written:

$$\Pr(T \geq N) = (1-p)^N \qquad (8)$$

- if additionally, i fit is "admitted" that the Universe has been existing for n = 15. 10^9 years**;**

$\Pr(T \geq n) = 1$ (aspect observed currently).

- considering the hypothesis that: "*There is one chance in two that the Universe achieves and exceeds N = n+ 1 years, i.e. there is still a next year*".

Then, we can write**:**

$$(1-p)^N = 0{,}5 \qquad (9)$$

where $p = 4{,}6 \cdot 10^{-11} > 10^{-11}$ / year.

One can also make the following assumptions:

- ✓ eithes there to 2 to 1 chance in the universe to achieve and exceed $N = 2n = 30.10^{-9}$ years and then $p = 2{,}3.10^{-11} >> 10^{-11}$ /year.
- ✓ or there are 99 chances in 100 that the Universe exceeds $N = n + 1$, then $p = 10^{-12}$ /year.

It is noted that all these probabilities are of the same order of magnitude given the size of basic data.

Due to lack of another catastrophic event more serious than the disappearance of the Universe, the upper limit of negligible probability can be set between 10^{-11} and 10^{-12} per year, ie 10^{-15} 10^{-16} per hour.

3.1 Practical application (1)

In order to capitalize the research results obtained previously, we shall present the way to low foundations of the principles underlying the as sizing process risk assessment scale, with effect on determining the level of minimum risk [7].

It follows presentation the corresponding scales of health and safety parameters at work, namely P, G, R and S, the scale of attitudes in relation to risk and the risk matrix analyzer [8].

The scale parameter of gravity of the consequences, G

Classes of seriousness	Consequences	The seriousness of the consequences G
1	**Negligible**	Minor reversible consequences with predictible disability of up to 3 calendar days (healing without treatment)
2	**Small**	Reversible consequences with predictible disability between 3 - 45 days requiring medical treatment
3	**Average**	Consequences reversible with a disability expected 45 - 180 days requiring medical treatment and hospitalization
4	**High**	Irreversible consequences with a diminution of work capacity of at least 50%, the individual can perform to a professional activity (disability grade III)
5	**Serious**	Irreversible consequences with loss of 100% of working capability, but with the possibility of self, management and spatial orientation (disability grade II)
6	**Very serious**	Irreversible consequences with total loss of work capability, self management, the autoconducție or spatial orientation (degree invalidity)
7	**Maximum**	Death

The assessment scale of the risk level

Levels of risk, R / security, S	Risk assessment values, R	Level of professional risk assessment	Estimate the level occupational safety
1 / 7	1 ÷ 7	Minimal risk	Maximal security
2 / 6	8 ÷ 13	Risk very low	Very high security
3 / 5	14 ÷ 21	Risk low	High security
4 / 4	22 ÷ 29	Medium risk	Medium security
5 / 3	30 ÷ 35	High risk	Security low
6 / 2	36 ÷ 39	Very high risk	Security very low
7 / 1	40 ÷ 42	Maximal risk	Minimal security

Legend:

	Area of risk is unacceptable
	Area of risk is acceptable

CLASSES OF SERIOUSNESS "G"	CONSEQUENCES		CLASSES OF PROBABILITY "P"					
			1 ↓	2 ↓	3 ↓	4 ↓	5 ↓	6 ↓
			EXTREMELY RARE	VERY RARE	RARE	LESS COMMON	FREQUENT	VERY FREQUENT
			$10^{-12} \le P < 10^{-10}$	$10^{-10} \le P < 10^{-8}$	$10^{-8} \le P < 10^{-6}$	$10^{-6} \le P < 10^{-4}$	$10^{-4} \le P < 10^{-2}$	$10^{-2} \le P \le 10^{0}$
7 →	MAXIMAL	DEATH	21	29	35	39	41	42
6 →	VERY SERIOUS	DISABILITY GR. I	20	28	34	37	38	40
5 →	SERIOUS	DISABILITY GR. II	19	26	27	32	33	36
4 →	HIGH	DISABILITY GR. III	13	18	24	25	30	31
3 →	AVERAGE	ITM 45 – 180 DAYS	11	12	16	17	22	23
2 →	SMALL	ITM 3 – 45 DAYS	7	8	9	10	14	15
1 →	NEGLIJIBLE		1	2	3	4	5	6

Fig. 1 Matrix Risk Analyzer

Thus, we can say that the minimum risk level corresponds to the values 1, 2, 3, 4, 5, 6 and 7 of the risk analyzer, resulted from the combination between the classes of probability "P" 1, 2, 3, 4, 5 and 6 and the classes of seriousness "G" 1 and 2.

Also, the lower limit of the range of values $\{1,2,3,4,5,6\}$ related to the parameter probability i.e. the value of 1 corresponds to the value of neglijable probability set between $10^{-12} \div 10^{-11}$ per year and the to the value set 10^{-10} per year, and the maximum limit of 6 has a probability range between 10^{-2} and 10^{0} per year.

Similarly, we can set value limits associated to the probability parameter values corresponding to the following scale:

The scale parameter related to the probability of producing adverse events, P

Classes of probability	Events	Likelihood consequences P
1	Extrem rare/catastrophic	(extrem small) $10^{-12} \le P < 10^{-10}$
2	Very rare	(very small) $10^{-10} \le P < 10^{-8}$
3	Rare	(small) $10^{-8} \le P < 10^{-6}$
4	Less common	(medium) $10^{-6} \le P < 10^{-4}$
5	Frequent	(high) $10^{-4} \le P < 10^{-2}$
6	Very frequent/certain	(very high) $10^{-2} \le P \le 10^{0}$

Chart reduce risk

CLASE DE GRAVITATE "G"	CLASE DE PROBABILITATE "P"					
	1 ↓	2 ↓	3 ↓	4 ↓	5 ↓	6 ↓
7 →	21	29	35	39	41	42
6 →	20	28	34	37	38	40
5 →	← 19	← 26	27	32	33	36
4 →	↓ 13	18	24	25	30	31
3 →	11	12	16	17	22	23
2 →	7	8	9	10	14	15
1 →	1	2	3	4	5	6

3.2 Practical application (2)

In this section, a technical approach on establishing scientifically based tools for the quantification of threats and vulnerabilities or potential or apparent specific national security system, identified at a time, to substantiate of quantitative and qualitative risk and security establishment, wittingly, the detailed controls to eliminate or reduce hazardous situations arising from these factors disturbances [9].

3.2.1 Overview on security risk management

Risk Management Information security is composed of four distinct components of the process:

- Security Risk Analysis
- Assess security risk by assessing vulnerabilities / threats and control
- Analysis of cost / benefit
- Reduce risk of security

Security risk management is a process of total identification, control and minimize the impact of undesirable events and uncertain aims of the management of security risks arising from potential threats and vulnerabilities or obvious that you can identify at a time, to eliminate or reduction to an acceptable level.

- *Security risk analysis*

Any study of security on the strategic objectives of national interest, aims to establish the circumstances of identification of threats and / or vulnerabilities in these objectives, the methods of quantifying the possibility of the occurrence and manifestation of the security risk in relation to the seriousness of the impact associated and determination of security risks acceptable for the delimitation of areas unacceptable of these risks substantiate programs and actions to eliminate or reduce them.

In terms of specialty, national security is considered state of the national system in which the possibility of manifestation of threats and / or vulnerabilities in the production or destruction of human and material disaster.

In reality, due to features of any national security, can not attain the status of absolute security risk type 0 or national security infinite.

In the case of national security can not be excluded that the threats and / or potential vulnerabilities, there is a residual risk associated with that depending on the size of the required corrective actions appropriate extreme / or emergency care / attention to be urgently implemented / immediately.

- *Security risk assessment by quantifying vulnerabilities / threats and control*

Security risk assessment is an important component of risk management to security, which is determined by the nature and type of threats identified to be specifically assessed in the determination of appropriate levels of risk. Prioritizing actions to prevent or combat the threats or vulnerabilities identified is carried out in accordance with the outcome of the risk assessment, under which are set out appropriate control measures to ensure and guarantee an acceptable level.

The risk assessment involves security through the following steps:

*P1:Defining evaluation:*The first step is the formation of the team for analysis and evaluation which will include specialists in the field and good knowledge of processes and strategic objectives of national interest subject to this analysis.

Before starting work, team members must know in detail the method of assessment instruments and procedures used for concrete work. Also, a minimum prior documentation of the objectives and processes of activity, to be analyzed and evaluated.

P2:Determining the probability of occurrence of threats and/or vulnerabilities: Once the list of identified threats that include both potential threats and that is, it is necessary to determine the likelihood of their occurrence. In this sense, the grid is presented for measuring the parameter of probability of occurrence of threats identified:

Class of the probability	Nuanced appreciation of the probability	Description of likelihood
1	Small	Threat unlikely occurrence in the coming year
2	Medium	Probable threat of emergence in the coming year
3	High	Very probable threat of emergence in the coming year

The rate of occurrence of threats and vulnerabilities

Result evaluation is closely related to how to quantify the identified threats or vulnerabilities. In this respect, a relationship used to estimate the security risk is the annual exposure that can become dangerous under certain conditions.

This establishes the link between the severity of threats and vulnerabilities identified and the likelihood of producing them.

Values ″Rate of occurrence of these risk factors ″are shown in the following table:

Rate of occurrence of these risk factors

Rate of occurence	Fraction equivalent	Multiplication factor
Never	0	0,0
Every 300 years	1/300	0,00333
Every 200 years	1/200	0,005
Every 100 years	1/100	0,01
Every 50 years	1/50	0,02
Every 25 years	1/25	0,04
Every 5 years	1/5	0,20
Every 2 years	1/2	0,50
Annually	1/1	1,0
Twice a year	1/0,5	2,0
Once a month	12/1	12,0
Once a week	52/1	52,0
Once daily	365/1	365,0

P3:Determining the level of risk: Figures following schedule is presented for quantifying the risk of security both in terms of actions and steps that should be undertaken to achieve a proper control of how to prevent and combat the phenomenon of depreciation of the national security strategic objectives, as a result of specific threats and vulnerabilities of these systems and in terms of appreciation and nuanced value assigned to this parameter.

Probability Matrix-Impact on the actions and steps to be taken to eliminate / reduce security risk are shown in the following table:

Probability Matrix-Impact

PROBABILITY	IMPACT		
	High	Medium	Small
High	A_1	A_2	B_2
Medium	A_2	B_1	C_1
Small	B_2	C_1	C_2

A_1,A_2-corrective actions of extreme urgency and emergency that must be implemented immediately
B_1,B_2-corrective actions for maximum attention and care that should be implemented
C_1-efforts aimed at the applicable requirements
C_2-approaches that do not require further action

Probability Matrix - Impact assessment on the levels risk associated with security are shown in the following table:

Probability Matrix - Impact assessment

PROBABILITY	IMPACT		
	High	Medium	Small
High	M (6)	M (5)	Me (4)
Medium	M (5)	Me (4)	Mi (3)
Small	Me (4)	Mi (3)	Mi (2)

M	security risk level high	Field of security unacceptable risk
Me	security risk-level (critical)	Field of security acceptable risk
Mi	security risk level low	

P4:Develop measures to eliminate or reduce the risk of security If assessed security risks of which are located in unacceptable risk to the procedure of analysis and reduce them by applying an appropriate corrective actions and preventive, to prevent and combat the causes of production of undesirable events arising from threats or vulnerabilities identified.

In this sense, is used risk Analyzer , which was built on the (whose matrix is shown in scales provided by the classes of values corresponding to the two parameters: the probability of producing an undesirable event, P and gravity consequences, G.

- *Risk Analyzer*

The next figures are present the corresponding scale parameter associated security risk, and R scale and the attitude towards risk and risk matrix analyzer, which are used to estimate the risk assessment and security, to eliminate / reduce impact.

The scale of assessment of security risk

Level of security risk	Values of security risk assessment	Assessing the security risk
1	2÷3	Security risk level low
2	4	Security risk-level (critical)
3	5÷6	Security risk level high

5÷6	security risk level high	Field of security unacceptable risk
4	security risk-level (critical)	Field of security acceptable risk
2÷3	security risk level low	

Scale of attitudes towards the risk of security

The risk of security	Assess the level of security risk depending on the parameters P and G	Attitude toward the risk of security
1	Small-Small (1+1=2)	Approaches that do not require further action
	Small-Medium (1+2=3)	Efforts aimed at the applicable requirements
	Medium-Small (2+1=3)	Efforts aimed at the applicable requirements
2	Medium-Medium(2+2=4)	The corrective actions that should be carefully implemented
	Small-High (1+3=4)	The corrective actions that should be carefully implemented
	High-Small (3+1=4)	Corrective actions of extreme caution that should be implemented
3	Medium-High (2+3=5)	Emergency corrective actions to be implemented immediately
	High-Medium (3+2=5)	Emergency corrective actions to be implemented immediately
	High-High (3+3=6)	Corrective actions of extreme urgency to be implemented immediately

Matrix Risk Analyzer

PROBABILITY	IMPACT		
	High 3↓	Medium 2↓	Small 1↓
High (3) →	**6**	**5**	**4**
Medium (2) →	**5**	**4**	**3**
Small (1) →	**4**	**3**	**2**

P5:Reporting the results of security risk assessment: In the next table, the form is submitted for analysis and risk assessment of security, where the categories are provided to identified threats, depending on their applicability, will be quantified and used in calculating the security risk:

Results of security risk assessment

Threats	Applicable YES/ NO	Probability 1=Small 2=Medium 3=High	Impact 1=Small 2=Medium 3=High	Security risk assessed (2+3)-Small (4)-Medium (5+6)-High	Actions to eliminate / reduce the risk of security	Residual security risk (2+3)-Small (4)-Medium (5+6)-High
Natural Threats						
Electrical storm						
Ice storm						
Snowstorm/Blizzard						
Major landslide						
Mudslide						
Tsunami						
Tornado						
Hurricane / typhoon						
High winds (>70km/h)						
Tropical storm						
Tidal flooding						
Seasonal flooding						
Local flooding						
Upstream dam/reservoir failure						
Sandstorm						
Volcanic activity						
Earthquake (2+4 Richter Scale)						
Earthquake (>5 Richter Scale)						
Epidemic						
Human - Accidental						
Fire:Internal-minor						
Fire:Internal - major						
Fire:Internal - catastrophic						
Fire:External						
Accidental explosion – on site						
Accidental explosion – off site						
Aircraft crash						
Train crash						
Derailment						
Auto/truck cras hat site						
Human error - maintenance						
Humann error -programming						
Human error - users						

Toxic contamination						
Medical emergency						
Loss of key staff						
Human - Deliberate						
Sabotage/terrorism:external - physical						
Sabotage/terrorism:internal - physical						
Terrorism: biological						
Terrorism: chemical						
Bombing						
Bombing threat						
Arson						
Hostage taking						
Vandalism						
Labor dispute/strike						
Riot/civil disorder						
Toxic contamination						
Environmental						
Power flux						
Power outage - internal						
Power outage - external						
Wter leak/plumbing failure						
Temperature inadequacy						
Telecomunications failure						
Toxic contamination						

- *Reduce risk of security*

If the security risk assessment, risk resulting in the unacceptable risk area, it will highlight the risk index records (shown below), after which it will fill in the form of analysis and risk reduction, presented in the continuation index.

Index records security risk

No. doc	Description of threats and/or vulnerabilities (concrete form of manifestation)	Strategic objective of national interest

FORM AND ANALYSIS OF SECURITY RISK REDUCTION

Economic operator: ……..
Place of origin: ……
Strategic objective of national interest: .....

Paper nr. ……..	**Risk of security**: ……	**Level**: …….

Security risk located in the area caused unacceptable	**P**	**G**	Estimate / safety risk assessment **R**	
	….	….	….	.....

Name of the threat or identified vulnerability: .....

Description of threat or vulnerability identified (concrete form of expression)**:** ……..

Causes:
- ……

Dysfunctions
- ……

Possible measures**:** Corrective actions -	**References:** .....
Implementation measures: -	**References:** ……..

Identification residual security risk	**P**	**G**	Estimate / safety risk assessment **R**	
	…… …	…… ..	…… ..	Small
Residual security risk: ……..	Assessment of the action to reduce security risk, according to the chart in Figure **6:** …… ……			

Chart reduce risk of security

PROBABILITY \ IMPACT	High 3	Medium 2	Small 1
High (3)	6↓→	5↓→	4↓
Medium (2)	5↓→	4↓→	3↓
Small (1)	4→	3→	2

4 Conclusions

Any study of risk intends mainly to establish and quantisize the security objectives for identifying the factors determining dangerous situations, the ways to quantify the possibilitie of occurrence and manifestation of risk of injury and occupational disease in relation to impact severity associated, and and determination of acceptable risk, in establishing the areas of their unacceptability and grounding prevention programs, and insurance protection, for eliminating or reducing them.

In this regard, the paper show different methods for calculating the probability of occurence of undesirable events in relation to a safe opersation within a work system.

It was also shown the possibility of establishing by calculation the probability associated with negligible event whose value is the lower limit to be taken in consideration the calculations and probabilistic assessments of the security studies. This aspect allows highlighting the importance of time scale used and the plausibility of the event examined, elements which the analyst should always consider.

Therefore it can be considered as unrealistic or even absurd to preserve and to handle probabilities at or below this threshold in safety studies.

At present, the security risk assessment are two major imperatives resulting from the implementation of a reasonable and prudent control at the same time, and preparing and organizing the steps necessary documentation management of national security ever.

In this respect, in the paper has been considered the possibility of establishing a methodology for assessing security risk, and how the procedure for application in a given situation.

Results obtained from the investigation and diagnosis of national security, based on the methodology presented, leading to overall assessment of risk associated security status of specific environmental threats event and/or vulnerabilities identified in order substantiate and implementation of appropriate programs of action with maximum emergency/necessity or urgency/need to eliminate or reduce the dangerous situations that may affect national security.

All these methodological approaches and procedures, ensuring the purpose of ensuring and maintaining acceptable levels of national security strategic objectives, in line with the level of resources allocated to achieve this goal.

References:

[1]Desroches, A., *Concepts et methodes probabilistes de base de la securite,* Lavoisier-TEC&DOC, 1995, Paris.

[2]Bureau de Normalisation de l′Aeronautique et de l′space (BNAE) *Guide d´elaboration des objectifs de securite d´un systeme missile ou spatial,* RG AERO 701 12, 1987.

[3]G., Morlat *Sur la theorie de la decision appliquee aux evenements rares,* OECD NEA, 1978.

[4]C., Lievens *Securite des systems,* CEPADUES, 1976.

[5]Rasmussen & Co *Reactor Safety Study-An assessment of accident risks in US commercial nuclear power plants,* NASH 1400-US nuclear regulatory commission, 1975

[6]H., Ventsel *Theorie des probabilities,* MIR, 1973.

[7]M.,Tribus *Decisions rationnelles dans l´încertain,* MASSON, 1972.

[8]Darabont A., Pece Şt., Dăscălescu A.- *Managementul securităţii şi sănătăţii în muncă. Volumul 1, 2,* Editura AGIR.

[9]Thomas R., Peltier.-*Information Security Risk Analysis, Second Edition, 2005,* ISBN 0-8493-3346-4.