Modelling of the Force Protection Process Automation in Military Engineering

Jaroslav Záleský(✉) and Tibor Palasiewicz(✉)

University of Defence, Brno, Czech Republic
{jaroslav.zalesky, tibor.palasiewicz}@unob.cz

Abstract. Article deals with a set of problems linked to a Engineer Force Protection Provision algorithm design and evaluation of input factors series. This algorithm is generally compatible with The NATO Force Protection Process Model adjusting it to a part of engineer forces' decision making process. The base of the algorithm is an application of repeated numerical matrix pattern and its word interpretation. The article provides a thought content being a possible key idea for the suitable software development.

Keywords: Force protection · Engineer support · Protective measures · Threat · Risk · Risk analyses · Risk management

1 Introduction

One of key success conditions of any military activity is own forces casualties reduction to such level that enable them keeping at disposal personal and material resources sufficiency therefore having preponderance over an adversary. Force protection presents a sectional field reflecting the demand mentioned above being multidisciplinary domain implicating all of military branches during a fulfilling of their tasks resulting from their predetermination. General abilities of forces necessary for successful force protection support are illustrated on Fig. 1. Force protection engineer measures are underlined on Fig. 2. The planning and execution force protection philosophy is based on the general force protection model (Fig. 3), presenting a force protection measures projection algorithm including an engineer provisions design. The algorithm is based on a thought model encompassing processes enabling to prevent potential incidents or to react to them by force protection measures adoption. Engineer measures act as possible means for a risk avoidance or it´s reduction. Their content and scope design followed by their planning and execution essentially belong to the risk management acting as a backbone activity of a planning and execution process of force protection measures.

Analyses procedures of processes leading to particular engineer force protection measure design had demonstrated that a specific engineer risk management algorithm based on above mentioned general force protection model has not been still exist. It has created an opportunity to develop such algorithm therefore to fill an "empty area" in the mentioned sphere.

J. Mazal (Ed.): MESAS 2018, LNCS 11472, pp. 599–613, 2019.
https://doi.org/10.1007/978-3-030-14984-0_45

2 Appropriate Engineer Force Protection Measures Design Process Based on Risk Assessment of Critical Resources Damage

Design process of engineer provisions acting as risk reduction means is illustrated in the chapter. The risk is based on an impact of a particular event reaching from a particular threat occurring and resulting to the loss of particular resource. There are suggested following steps being parts of the process:

- resources criticality assessment,
- resources vulnerability assessment,
- risk assessment,
- appropriate engineer measures design leading to a risk reduction.

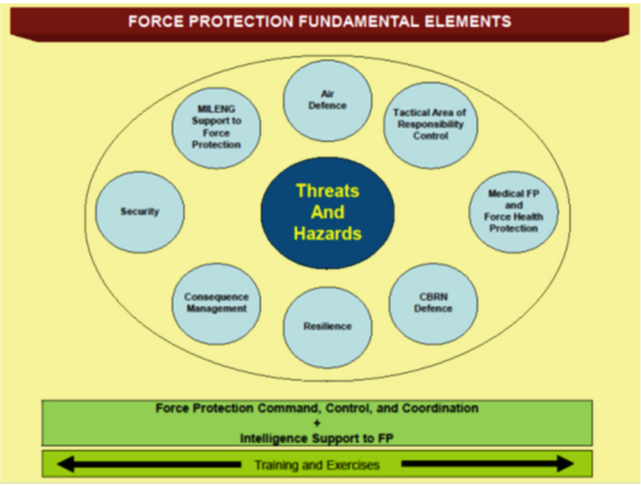

Fig. 1. General capabilities of forces required for a force protection support. (Source: STANAG 2528, p. 20)

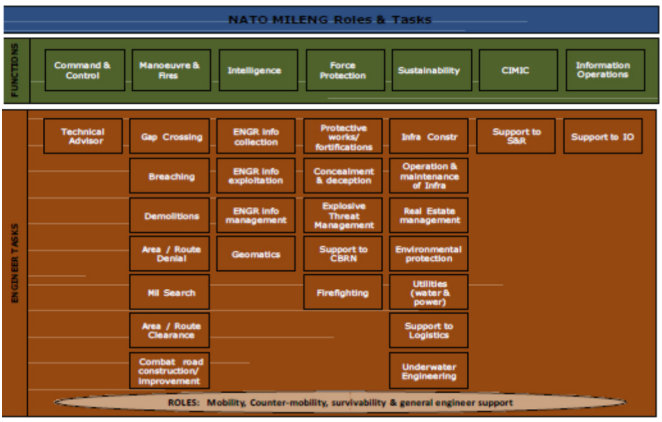

Fig. 2. System base of engineer roles and tasks. (Source: STANAG 2394, p. 18)

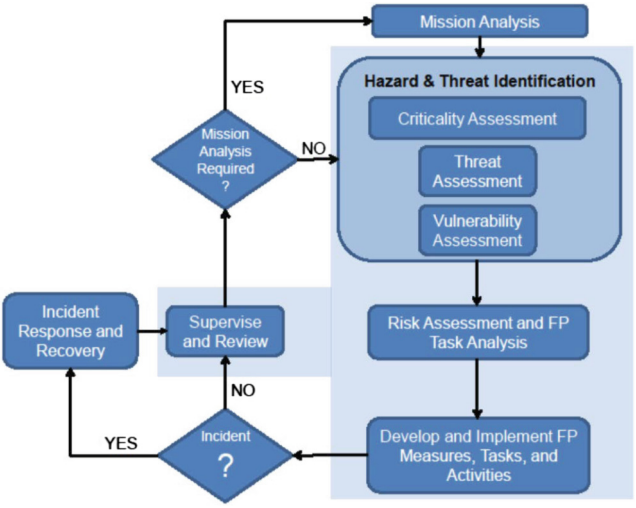

Fig. 3. Force protection model (Source: STANAG 2528, p. 35)

2.1 Resources Criticality Assessment

Critical assessment can be based on two main attributes necessary for a source to be critical. Its significance for particular task accomplishment can be considered as the first attribute while its restorability in case of a loss presents the second one. Assessment scales of source´s significance and restorability have been formulated in Tables 1 and 2. Each degree has been determined as based on possible consequences' alternatives of resources' loss and their restoration possibilities.

Value of criticality H_k can be evaluated using a formula

$$Hk = STv * STo, \tag{1}$$

where H_k = criticality value of particular source, ST_v = significance degree of source and ST_o = recovery degree of source.

Possible criticality values determined using the formula mentioned above while taking into account different combinations of significance and recovery degrees have been expressed in Table 3. Each sources' evaluation using scale of criticality values can be formulated as:

- extremely critical source (criticality value 20 to 15),
- highly critical source (criticality value 12 to 9),
- moderately critical source (criticality value 8 to 5),
- low critical source (criticality value 4 to 1).

The evaluation enables assessors to prioritize sources and suggest which ones would require adequate engineer force protection measures adoption.

2.2 Resources Vulnerability Assessment

Each resource (without additional protective provision) can be characterized by vulnerability from the point of view of force protection. The character describes its ability to be eliminated or damaged by particular threat. Vulnerability levels can be determined by analogy with recovery and significance levels definitions (see Tables 1 and 2). An example of such expression for combat vehicle BVP-2 has been illustrated in Table 4 and Diagram 1. Based on similar vulnerability evaluations of each asset it is possible to develop and maintain resources´ vulnerability records. For numerical expression and definitions of vulnerability levels see Table 5. For vulnerability assessment of each resource from the point of view of all threats causing its potential loss the following procedure can be used:

- specific vulnerability level for each resource from each particular threat identified can be assigned,
- all vulnerability levels can be expressed with a table,
- the table will be then transformed to a diagram,
- based on an interpretation of data from a diagram it is possible to state resource´s level of vulnerability from each threat to consider which potential risk will be significant enough to evaluate its level.

Table 1. Significance degree of a resource (Source: Záleský J, p. 77)

Significance degree of a resource ST_v	Numerical quantification	Definition
Indispensable resource	**5**	Resource which loss or damage makes a task accomplishment impossible
Highly significant resource	**4**	Resource which loss or damage will require significant change of a task accomplishment course of action
Moderate significant resource	**3**	Resource which loss or damage will cause acceptable delay of task accomplishment or immediate resource restoration necessity
Low significant resource	**2**	Resource which loss or damage will cause task accomplishment constraint without affecting a final success
Insignificant resource	**1**	Resource which loss or damage will not affect task accomplishment

Table 2. Recovery degree of a resource (Source: Záleský J, p. 78)

Recovery degree of a resource STo	Numerical quantification	Definition
Unrecoverable resource	**4**	Source which availability for task accomplishment is significantly limited and it is impossible to share it with other forces. Restoration or recovery of such resource requires conduct such activities which are impracticable under particular conditions or the time required for its conduction exceeds the time of task accomplishment
Hardly recoverable resource	**3**	Source which availability for task accomplishment is limited but it is possible to share it with other forces however the accomplishment itself has to be modified under such conditions. Resource recovery or restoration will require course of action change or required accomplishment time reevaluation
Resource recoverable with difficulties	**2**	Source which availability for task accomplishment is limited but it is possible to share it with other forces until it is recovered or restored
Easy recoverable resource	**1**	Source which availability for task accomplishment is unlimited or which recovery or restoration will not affect course of action

Table 3. Resource criticality value (Source: Záleský J, p. 78)

Recovery degree of a resource ST_o		Significance degree of a resource ST_v				
		Indispensable resource	Highly significant resource	Moderate significant resource	Low significant resource	Insignificant resource
		5	4	3	2	1
Unrecoverable resource	4	20	16	12	8	4
Hardly recoverable resource	3	15	12	9	6	3
Resource recoverable with difficulties	2	10	8	6	4	2
Easy recoverable resource	1	5	4	3	2	1

Table 4. Vulnerability level assignment from point of view of particular threats (Source: Záleský J, p. 80)

Threat	Vulnerability level
Anti-tank mine	**4**
100 kg explosive VB - IED	**4**
Machine gun direct fire	**1**
RPG	**5**
Molotov cocktail	**1**
Artillery shell 155 mm	**3**

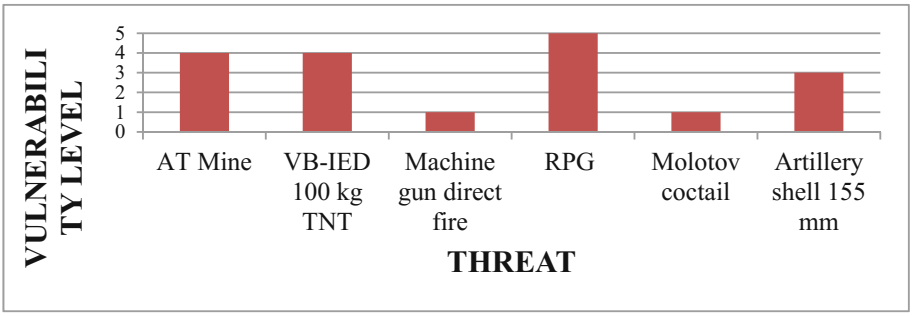

Diagram 1. Vulnerability level assignment to particular threats (Source: Záleský J, p. 82)

2.3 Risk Assessment

A purpose of a risk assessment is an incident occurrence probability estimation and expected impact forecast [4, 5]. Based on results of such sub assessments it is possible to access specific level of risk of task accomplishing hamper or limitation. Risk assessment process consists of following steps:

- likehood assessment of incident occurrence,
- assessment of incident´s expected impact on a task accomplishing,
- level of risk assessment based on sub assessments of incident´s impact and probability,
- risk prioritization. [4, 5].

Likehood Assessment of Incident Occurrence

Occurrence likehood of particular incident has to be estimated in case of each threat. To express it by quantitative way the Table 6 can be used.

Each incident occurrence likehood category can be expressed by percent using rectangular probability distribution as the most useful mathematic tool. Then a numerical expression can be used. Particular incident likehood can be estimated based on its occurrence in a particular operation during directly determined period of time. The time range will depend on particular conditions.

Severity Assessment of Particular Threat Impact on Particular Resource and Its Effect on Particular Task Accomplishment

Particular threat impact of particular resource assessment can be expressed by a level degree describing consequences of such impact on fighting power, combat task accomplishments or for combat readiness.

Following scale of potential consequences can be used for each threat impact severity assessment:

- catastrophic impact,
- critical impact,
- marginal impact,
- negligible impact.

Severity assessment of an incident caused by threat exploiting a vulnerability of particular resource can be based on following two key factors:

- particular resource vulnerability to a particular threat – expressed with vulnerability level STzr,
- particular resource criticality for particular task accomplishment – expressed with criticality value Hk.

Based on those factors severity level can be expressed using following equation:

$$Dz = STzr * Hk, \tag{2}$$

where D_z = severity level, ST_{zr} = vulnerability level of particular resource and H_k = criticality value of particular resource.

Equation mentioned above is analogical to critical value (H_k) assessment mathematical formula. If particular numerical values expressed in Tables 3 and 5 are put down to the equation the level of severity will assume values expressed in the Table 7.

Apart from numerical expression severity value can be described using definitions (see Table 8).

Specific Risk Level Assessment

Value of particular risk level of particular task nonfulfillment caused by particular incident impact resulting to a particular resource loss due to particular threat application can be expressed with following equation:

$$Ru = Dz * Pv, \tag{3}$$

where R_u = incident appearance risk level, D_z = severity level and P_v = likehood category.

Putting down numerical values of likehood category (see Table 6) and severity level (see Table 7) to the equation shown above the value of appearance risk level assumes values expressed in the Table 9. Levels of risk can be classified into five categories (see Table 10). Based on such classification and prioritization force protection measures can be designed and implemented to reduce risk level assessed above.

Table 5. Vulnerability levels of personnel, equipment, material and structures (Source: Záleský J, p. 81)

Vulnerability level ST_{zr}	Definition			
	Personnel	Equipment	Material	Structure
5	Threat causes fatal injuries to personnel	Threat causes total destruction of equipment or damages requiring more 1000 man-hours to be repaired	Threat causes permanent loss of 60% available material or more	Total damage of structure. Building has been unable to fulfill its purpose
4	Threat causes major to fatal injuries to personnel	Threat causes damages requiring 400 to1000 man-hours to be repaired	Threat causes permanent loss of more than 30% of available material and damage of more than 30% of available material limits its function	Strong damage. Structure lost its essential characteristics and it has been already disabled to fulfil its purpose
3	Threat causes minor to major injuries to personnel	Threat causes damages requiring 100 to 400 man-hours to be repaired	Threat causes damage of more than 30% of available material limiting its function	Middle damage. Structure has still fulfilled its purpose however loosing significant part of its essential characteristics it requires conduction of extensive repairs to be fully useful. During the time of repairs the structure will be untuneful for its purpose
2	Threat causes no injury to major injuries to personnel	Threat causes damages requiring 60 to100 man-hours to be repaired	Threat causes damage of less than 30% of available material limiting its function	Small damages. It will be necessary to conduct repairs. Structure will be useful during a time of repairs
1	Threat causes no injury to personnel	Threat causes no damages or damages requiring 40 to 60 man-hours to be repaired	Threat causes no or small damage of a material	Minor damages. No or small repairs will be conducted. Structure will be fully useful

Table 6. Incident likehood categories (Source: Záleský J, p. 83)

Likehood category P_v	Numerical expression	Probability scope (%)
Frequent	**5**	81–100
Likely	**4**	61–80
Occasional	**3**	41–60
Seldom	**2**	21–40
Unlikely	**1**	0–20

Table 7. Severity level values (Source: Záleský J, p. 84)

Resource vulnerability level ST_{zr}	Resource criticality value H_k												
	20	16	15	12	10	9	8	6	5	4	3	2	1
5	100	80	75	60	50	45	40	30	25	20	15	10	5
4	80	64	60	48	40	36	32	24	20	16	12	8	4
3	60	48	45	36	30	27	24	18	15	12	9	6	3
2	40	32	30	24	20	18	16	12	10	8	6	4	2
1	20	16	15	12	10	9	8	6	5	4	3	2	1

2.4 Appropriate Engineer Force Protection Measure Determination as a Mean to Reduce Value of Risk

Particular engineer force protection measure (set of measures) draft suitable for a particular resource in a logical sequence of risk level evaluated before seems to be a key issue. The measure has to be designed in detail in logical sequence of draft mentioned above.

Measure effectivity presumption has to be based on the fact that the vulnerability level of particular resource achieved after the measure adoption will be lower than the former one existing before the measure adoption. The proper measure design requires applying the resource destruction or damaging risk reduction rate. The rate may be based on the comparison of resource vulnerability before and after the adoption of a particular measure.

For easy mathematical expression of facts mentioned above the vulnerability mitigation coefficient Ksz can be established using an equation

$$Ksz = \frac{STzrpre}{STzrpos}, \tag{4}$$

where K_{zs} = vulnerability mitigation coefficient, ST_{zrpre} = resource vulnerability level before force protection measure design and ST_{zrpos} = resource vulnerability level after force protection measure design.

If the numerical value of the coefficient is 1 or more the resource vulnerability level will be the same or higher after measure adoption. If it is lower than 1 the level will be lower too and the measure will be effective.

Reduced risk level of incident causing the loss of particular resource therefore the task completion failure or limitation can be evaluated using an equation:

$$R\,\mathrm{mod} \;=\; Ksz * Ru, \tag{5}$$

where R_{mod} = reduced value of incident risk, K_{sz} = vulnerability mitigation coefficient and R_u = initial value of incident risk before the measure was designed.

The risk can be also reduced by decreasing of a likehood and engineer camouflage and deception measures can be usefull means to reach it but the rate of likehood reduction measure assignment requires more difficult method using mathematical probability models. Therefore, it may be the topic of individual article.

Table 8. Severity level values definitions (Source: Záleský J, p. 85)

Severity level	Numerical expression	Consequences
Catastrophic	**100 − 50**	Full mission failure or the loss of ability to accomplish it, death or permanent personnel disability to accomplish the task, loss of main systems equipment or material critical for mission success, significant equipment material or stallations damage
Critical	**49 − 25**	Significantly limited ability to fulfill the task or unit readiness, permanent partial disability or temporary (more than three months) full disability of personnel to fulfil a task, extensive significant damage of systems, equipment and installations
Marginal	**24 − 15**	Limited ability to fulfill the task or unit readiness, small systems 'equipment's and installations 'damages, several days' waste of time caused by personnel wounds or diseases (healing less than three mounts)
Negligible	**12 − 1**	Small or no loss of ability to fulfill the task first aid or small rate medical care necessary, bare damages of equipment, systems or installations (remain fully operational or useful)

Characteristics of Particular Engineer Measures Supporting Force Protection

Following measures illustrated on Fig. 2 represent the real and tangible part of force protection engineer measures design. If adopted, the elimination risk of personnel, equipment, material, installation, or breakdown of activity critical for mission accomplishment will be eliminated or limited.

Their combination creates the synergic effect increasing the efficiency of force protection more than, if they would have adopted sequentially:

- **protective works and field fortifications** (chicanes or route access control points, fences, screens, or bunkers surrounding a facility or vehicle, equipment or troop concentration, preparation of sites for tactical air and aviation units, advice/assistance with the construction of protective barriers, perimeter protection

Table 9. Potential values of incident risk (Source: Záleský J, p. 86)

Severity level Dz		Likehood category Pv				
		Frequent	Likely	Occasional	Seldom	Unlikely
		5	4	3	2	1
Catastrophic	**100**	500	400	300	200	100
	80	400	320	240	160	80
	75	375	300	225	150	75
	64	320	256	192	128	64
	60	300	240	180	120	60
	50	250	200	150	100	50
Critical	**48**	240	192	144	96	48
	45	225	180	135	90	45
	40	200	160	120	80	40
	36	180	144	108	72	36
	32	160	128	96	64	32
	30	150	120	90	60	30
	27	135	108	81	54	27
	25	125	100	75	50	25
Marginal	**24**	120	96	72	48	24
	20	100	80	60	40	20
	18	90	72	54	36	18
	16	80	64	48	32	16
	15	75	60	45	30	15
Negligible	**12**	60	48	36	24	12
	10	50	40	30	20	10
	9	45	36	27	18	9
	8	40	32	24	16	8
	6	30	24	18	12	6
	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

systems, support to CBRN collective protection, advice on the construction of field fortifications, construction of command posts, construction of artillery gun positions, tank scrapes and weapon pits, preparation of alternate positions, preparation of sites for tactical air and aviation units, strengthening field fortifications and building reinforcement),

- **concealment and deception** (terrain camouflage capacity exploitation assessment, assistance with natural camouflage measures design, assistance with artificial camouflage measures implementation, dummy objects building, decoy installation,

anti-radar camouflage measures, thermal camouflage measures, explosives usage for the purpose of deception),

- **explosive threat management** (planning, command, control and training of activities connected in with explosive hazards, EOD activities, engineer part of C-IED),
- **support to CBRN** (field fortifications building and collective protection means installation, mobility support within contaminated areas and around them, assistance with decontamination points building, assistance with industrial disasters consequences disposal),
- **Firefighting** (fire protection means installation, assistance with fire extinguishing and localization, fire-fighting equipment building) [2].

Table 10. Risk level categories (Source: Záleský J, p. 88)

Category	Numerical expression	Definition
Extremely high risk	**500 − 180**	The loss of ability to accomplish the mission, if threats occur during its accomplishment. Frequent catastrophic casualties or their high likehood level, frequent critical casualties. It means that the risk of incident can cause serious consequences related to mission accomplishment. Decision of mission accomplishment continuation has to be properly evaluated in consideration of potential benefit achieved if task is fulfilled by the way suggested before risk was assessed
High risk	**160 − 75**	Serious loss of ability to accomplish the mission it scheduled time, disability to fulfill partial tasks or disability to fulfill the task in compliance with requirements if threat occurs during the task accomplishment. Occasional or seldom occurrence of catastrophic casualties. Likely to occasional occurrence of critical casualties. Frequent marginal casualties. It implies if the dangerous incident occurs, it will cause significant consequences. Decision of mission accomplishment continuation will have to be properly evaluated in consideration of potential benefit achieved if task is fulfilled by the way suggested before risk was assessed
Moderate risk	**72 − 30**	If the threat occurs during the mission accomplishment, the deterioration of ability to fulfill a task in accordance with requirements may be expected. The final impairment of task result quality would be a consequence. Unlikely catastrophic casualties. Seldom-critical casualties. Frequent to likely marginal casualties. Frequent negligible casualties
Low risk	**27 − 1**	Expected casualties cause marginal or negligible consequences to task accomplishment. Unlikely critical casualties, the probability of marginal casualties can be classified as seldom or unlikely. Negligible casualties seldom or unlikely. Severity of expected casualties cause no or limited consequences to the task accomplishing. Wounds, diseases or damages are not expected, or their impact on mission accomplishment will be not significant or long lasting

The Development Procedure of Engineer Force Protection Measures as Means to Reduce Risk

Rules of suitable engineer force protection measures design mentioned above can be formulated as a procedure that is a result of their applicability research. The procedure consists of following steps:

1. Significance degree quantification of particular resource based on particular task analyses (see Table 1),
2. Recovery degree quantification of the resource based on its availability and capabilities to distribute it to particular unit or troop (see Table 2),
3. Criticality value calculation via Eq. 1,
4. Arrangement of all resources necessary for particular mission accomplishment in compliance with criticality value,
5. Assignment of all identified threats to each resource that can be threaten by such hazards,
6. Vulnerability level assignment of each resource from each threat relevant for it (see Table 5),
7. Severity level calculation for each relationship threat-resource via Eq. 2,
8. Likehood evaluation of each threat occuring for each resource (see Table 6),
9. The risk calculation of event capable to limit or harm the usage of particular resource critical for particular mission accomplishment due to particular threat exploring particular vulnerability. Using of Eq. 3,
10. Acceptability evaluation of each risk calculated,
11. Prioritization of all risks in compliance with their value,
12. Particular engineer measures adoption and their impact evaluation on risk reduction. The evaluation is based on equation vulnerability levels before and after the adoption comparison (see step 6) with usage of Table 5,
13. Vulnerability mitigation coefficient calculation using the Eq. 4
14. Reevaluation of risk level after the particular measure adoption for each relationship threat-resource. Using Eq. 5,
15. Repeated arrangement of all risks in compliance with their value and their acceptance decision or next possible measure adoption.

The process illustrated above even though it seems to be difficult, can be routinely repeated. If some resource is then recognized as low critical and generally available in terms of a price and a quantity it will not be necessary to continue the risk assessment process to protect it. Likewise, if the threat although generally perceived does not affect the resource in particular situation or if the resource is invulnerable by the hazard, it will be void to access the potential risk.

Tables 3, 7, and 9 containing data calculated with an application of particular equations after data from Tables 1, 2, 5, and 6 had been inserted can be used for calculation advance.

Data ranges in Tables 8 and 10 specifying severity and risk levels reach from singular numerical values reaching from insertion of numerical expression of vulnerability levels, significance and recovery degrees to particular equations. The generally accepted axiom has been taken in account, that catastrophical and critical severity

levels of risks represent the highest necessity of force protection measures adoption including engineer ones. Therefore, it is the reason why the scale of these severity levels has been developer so wide (Fig. 4).

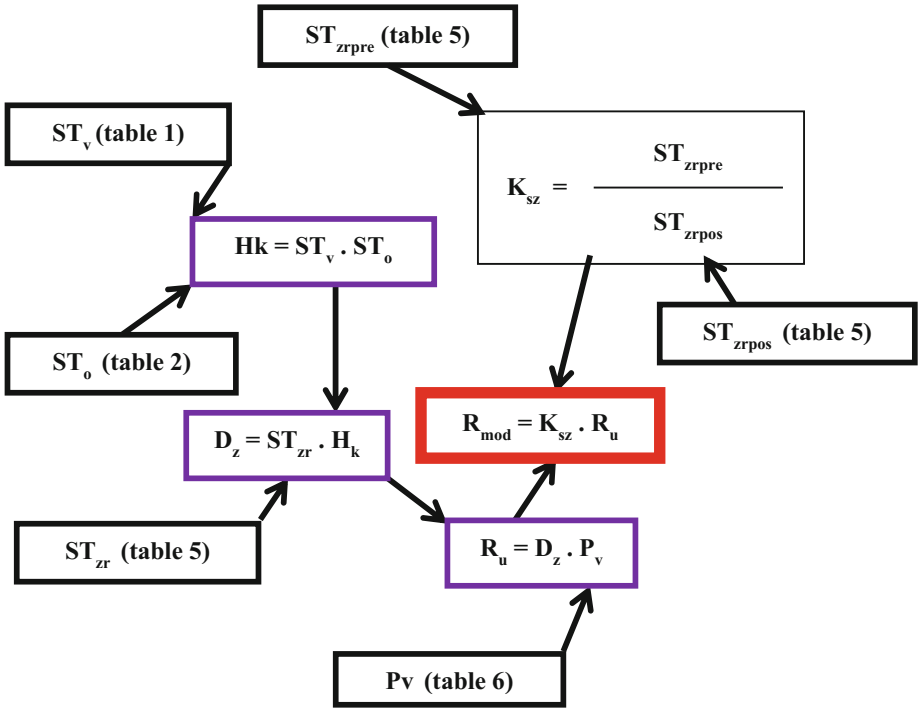

Fig. 4. Design process of engineer force protection measures as means for risk reduction (Source: Author)

3 Conclusion

Process suggested in the article would be useful for each engineer measure development and assessment based on risk level of incident occurring that can cause the particular resource loss or damage originating its usability thwarting for particular mission accomplishment. The process ca be applied also for more measures designed together to accomplish their synergic effect. The area for additional research has been opened therefore. Each step of the process can be used separately too as a mean for decision making process. The potentials to develop software based on mathematic equations and data tables expressed in the article can be taken in account as well together with the usage of existing software having mathematical functions. The example of such software can be MS Office Excel, MS Office Project or MATLAB.

References

1. Allied Joint Doctrine for Force Protection. STANAG 2528. NATO Standardization Office, Bruxels, pp. 20, 35. AJP-3.14 (2015)
2. Allied Tactical Doctrine for Military Engineering. STANAG 2394. NATO Standardization Office, Bruxels, pp. 18, 49–50. ATP-3.12.1 (2016)
3. Záleský J.: Ženijní opatření ochrany vojsk v operacích mimo území České republiky. Doctoral thesis. Univerzita obrany v Brně, Fakulta ekonomiky a management, Brno, pp. 77–86, 88 (2012)
4. Composite Risk Management: Headquarters department of the army, Washington, DC, pp. 7–8, 9. FM 5–19 (2006)
5. Comparative study: Australian defence risk management framework: DSTO systems sciences laboratory, Adelaide, pp. 10–11. DSTO-GD-0427 (2005)