ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 2, 14-23 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Multiple Criteria Decision-making: Risk Analyses for the Soft Target

Dora Kotkova*, Lukas Kralik, Lukas Kotek, Jan Valouch

Department of Security Engineering, Tomas Bata University in Zlín, Zlín, 760 05, Czech Republic

ARTICLE INFO

Article history:
Received: 31 August, 2022
Accepted: 29 January, 2023
Online: 11 March, 2023

Keywords:
Soft targets
Risk analysis
TOPSIS

ABSTRACT

This article focuses on risk analysis using a multi-criteria decision-making method. Due to many performed risk analyses for soft targets, we are constantly trying to find new methods for objective risk assessment. Many risk analyses are subjective, which is a problem when planning security measures and comparing results (different events, objects, places, etc.). In this text, we present our case study, which deals with the use of fuzzy TOPSIS. As a reference object, we have chosen one of the specific categories of soft targets – cultural events. The goal was to find the location most at risk of violent attacks on a selected cultural event - a music concert. We then established cooperation with three experts. The completed data in the risk analysis was then compared with practice. The selected fuzzy TOPSIS method was chosen as presumably more objective. Our hypothesis was confirmed. The results were objective and consistent with practical experiences.

1. Introduction

The article aims to present our research, which we have worked on for several years [1-12]. The goal is to research the protection of soft targets and find new methods to strengthen security. In this article, we focus on one necessary step, risk analysis. The biggest problem is selecting the appropriate method and minimalizing subjective view. Currently, many risk analysis methods exist, but none are specifically designed for soft targets. Our effort is to explore these methods and choose one or develop a new one that will provide objective results.

This article extends the contribution from The IEEE International Carnahan Conference on Security Technology 2021, where we presented an essential and necessary introduction and case study with the applied Fuzzy TOPSIS method [1]. In this extended version, we provide additional information on why we selected Fuzzy TOPSIS and a more detailed risk analysis of the whole workflow. Also, the introduction offers more detailed information about previous research and project on soft targets protection [1-12].

Our research is mainly concerned with the area of soft target protection. *"The term "Soft Targets" can be referred to those objects (buildings), (open) spaces, or events characterized by the accumulation of many people, the absence or low level of security measures against violent assaults, and their omission among critical infrastructure and hard target objects"* [13].

The protection of soft targets is a relatively new phenomenon in the geopolitical space of Europe. This issue became relevant after the events in 2014 when the so-called Islamic State declared a caliphate and began carrying out terrorist attacks worldwide [13], [14]. As the first figure (Fig. 1) shows, the number of terrorist attacks almost doubled. The data is obtained from our database created for our research[7], [9], [11], where violent attacks against soft targets are recorded from Europe and parts of Russia and Turkey. The existence and updating of the database are crucial for our research because we need to register this information and add details such as the location of the attack, time, modus operandi (Fig. 2), type of soft target (Fig. 3), and other information about the attack [14], [15].

This paper describes a significant part of our research. It is focused on security measures and, above all, on risk analysis. Nowadays, there are many risk analysis methods but just a few of them suits soft targets. The central lack of those methods is objectiveness. Some complex methods, such as Failure Mode and Effects Analysis (FMEA), are claimed as objective methods. But the result of this method depends on one evaluator's opinion [16]. The section 3 specifies some methods that are mostly used in security issues. Following section 4 goes into more detail about methods verified and tested in our research.

We asked three security managers to participate in our case study by finding the most exposed and weakest point in protecting soft targets at cultural events. Our previous research has shown the utility of multi-criteria decision-making (MCDM) in identifying

*Corresponding Author: Dora Kotkova, kotkova@utb.cz

soft targets. This case study aimed to verify the hypothesis that some methods of MCDM should be used for risk analysis, especially risk assessment. One of the significant parts of risk analysis is proposing security measures and making a plan of necessary activities; however, we focused just on the part of risk assessment and compared the final risk ranking from MCDM and typical risk analysis.

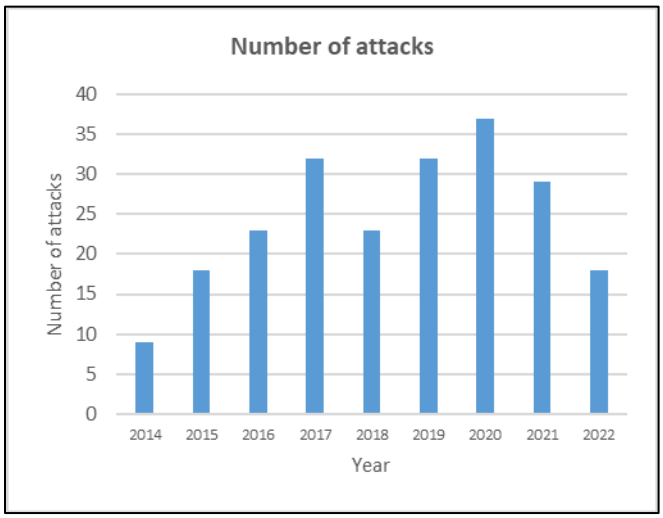

Figure 1: Number of terrorist attacks from 2014 to 2022 [15]

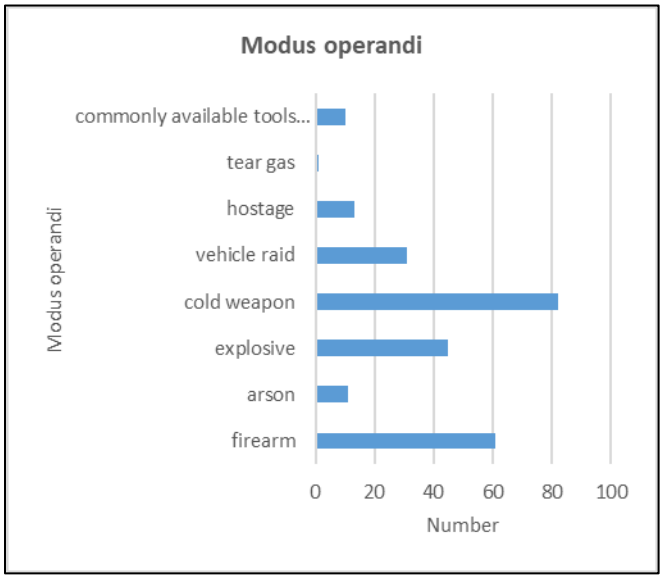

Figure 2: Modus operandi of terrorist attacks from 2014 to 2022 [15]

For this purpose, we selected some MCDM methods described deeply in section 4. Lately, we added the Fuzzy TOPSIS method to the list because this method perfectly fits our problem of objectives. Based on information from several publications [17 – 19], we decided to use the standard fuzzy TOPSIS version due to the existence of many hybrid approaches [20], [21], or updated methods [22], [23]. Some efforts are known to use Fuzzy TOPSIS for risk assessment [24], [25]. Classic fuzzy TOPSIS is only a segment of the developed methodology.

Soft targets has many categories and each category has own specifications. Cultural events is a category that we selected for our research and case study. As Fig. 3 depicts, cultural events are not targeted mostly, however they are very diverse. The quality of security measures that are highly variable, is the main reason for our choise.

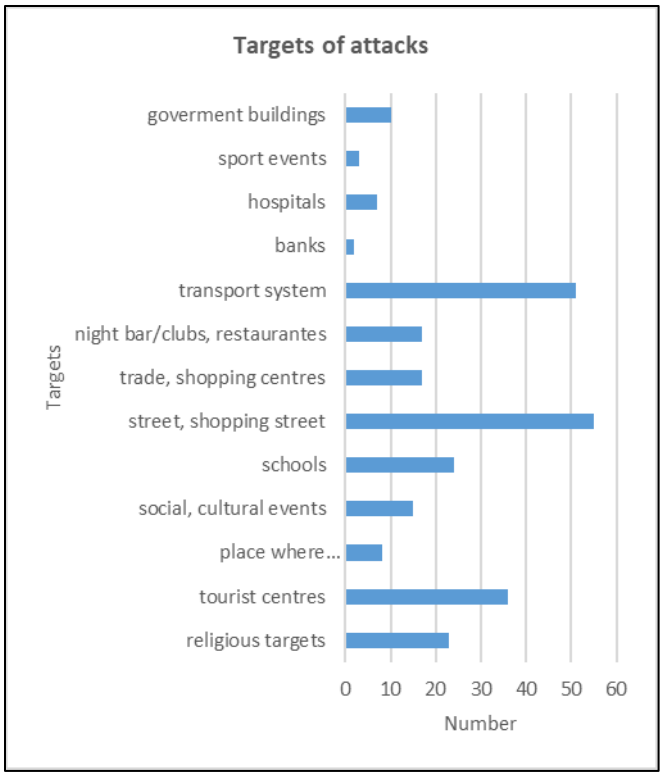

Figure 3: Targets of terrorist attacks from 2014 to 2022 [15]

2. Cultural events

Cultural events are one of the soft targets categories. *"Cultural events can be defined based on a combination of two words - culture and event or based on a combination of their defining concept. By combining these formulations, the following definition can be reached: cultural events are pre-planned events with a clearly defined place and time, the main goal of which is the presentation of spiritual and material values created by man."* [26]

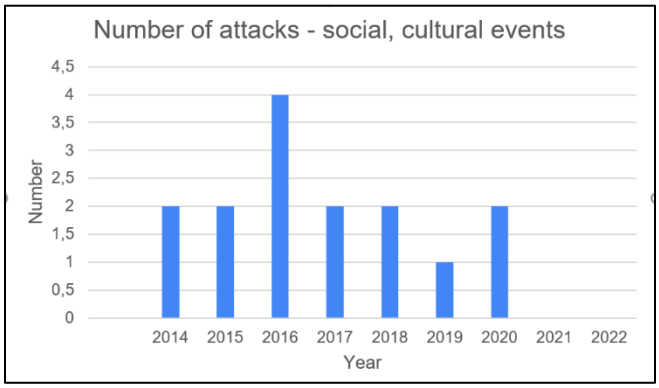

Figure 4: Number of terrorist attacks on social and cultural events from 2014 to 2022 [15]

Each mass event has its own specification, conditions and needs. Safety is a vital part of these mass events or gatherings. Differentiation of essential characteristics is absolutely necessary

to establish proper safety. Every successful terrorist attack on mass gathering may take many causalities. This is the reason why all mass gatherings must be well protected. The following figure (Fig. 4) shows that the average number of attacks is 2 and a half per year with a peak in 2016 [15].

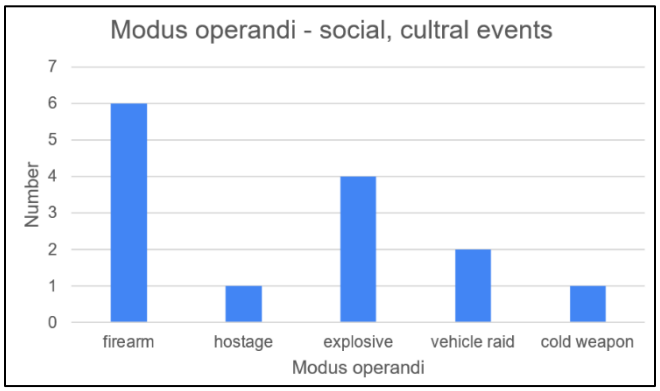

Figure 5: Modus operandi of terrorist attacks on social and cultural events from 2014 to 2022 [15]

3. Risk management

One of the integral parts of security planning is handling threats and their probability. We need to know what threats are in our facility. The objective of security planning is to take measures that lower the probability of emerging threats. The probability is also labeled as a risk.

Risk management (RM) is an endless process that subsists of three steps (fig. 6). Each step is described in more detail in the following sub-sections.

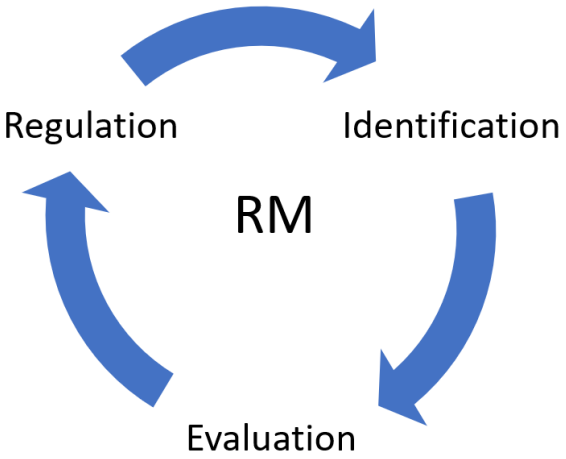

Figure 6: Risk Management steps [15]

3.1. Risk identification

Risk identification is ensured through risk analysis. The risk identification step usually includes the following activities:

1) Identification of sources of risk – this part includes:
   a) Determination of initial data – data on the analyzed entity, description of operation, location, etc.
   b) Identification of assets - definition and determination of the value of the assets owned by the subject;
2) Identification of threats – identification of events and actions that can negatively affect the value of assets;
3) Identification of vulnerabilities – every asset has its vulnerability or weakness to an identified threat. The level of this vulnerability affects the impact when a threat affects a protected asset;
4) Determining and assessment of impact.
5) Determination of risk - determination of the probability of the occurrence of threats and the degree of vulnerability of the subject [27]

There are three basic groups of risk analysis. The first one contains qualitative methods such as tree analysis – Event Tree Analysis (ETA), or Fault Tree Analysis (FTA). One of the most used and elemental methods is Safety/Security review. The group of quantitative methods stands on the other side, Failure Mode and Effect Analysis. (FMEA) is one of the well-known methods in this category. The last category is the combination of the two previous. It is a group of semi-quantitative methods that combine experience and numerical expression of risk [15].

3.2. Risk evaluation

Risk evaluation is an activity determined to enumerate risks and assign them to the correct category. The risks scale from the lowest negligible to the highest critical (Fig. 7). When planning security measures, we start with the necessary risk and need to spend the most funds in this category.

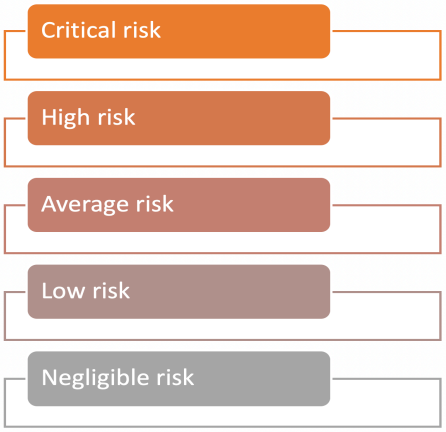

Figure 7: Risk scale

3.3. Risk regulation

The last step in risk management is risk regulation. This step includes six different approaches. Each approach has its own positives and negatives. It is very complicated to say which one is the best. It depends on the point of view. The possible approaches are:

- Ignoring the risk – conscious or unconscious
- Acceptance of the risk – this approach covers also issues with residual risk.
- Reduction of the risk – this is the most logical approach that implements corresponding security measures or reduces the severity of the impact.

- Risk avoidance
- Transfer of risk – transferring risk to another entity (e.g., outsourcing)
- Risk monitoring – the risk is not static, but it is variable and might change over time.

4. Methods

MCDM is a very complex field and provides many different methods and procedures. The most well-known methods such as the Analytic Hierarchy Process (AHP) [28], Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) [29], [30] or Višekriterijumsko Kompromisno Rangiranje (VIKOR) [30] has been selected for our research.

4.1. AHP

Tasks, the number of elements (variants and criteria), and the complexity in more complicated decision-making increase exceptionally. Due to this, the decision-maker has a problem getting his bearings in the task. Therefore, in the 1970s, Professor Thomas L. Saaty created the AHP method, which he and his colleagues developed into a practical tool for solving these complicated tasks. [28]

AHP can be described as a method of breaking down a complex unstructured situation into simpler parts – the establishment of a hierarchical system (Fig. 8). The following part uses the subjective assessment of pairwise comparisons, which assigns numerical values to individual components that express their relative importance. The subsequent synthesis of these evaluations determines the element with the highest priority.

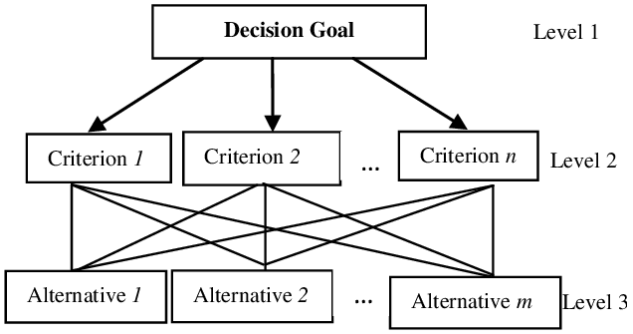

Figure 8: Structure (hierarchy) of AHP [31]

4.2. TOPSIS

The TOPSIS method, according to R.R. Venkata [32], was developed by Hwang and Yoon and is characterized by the fact that it requires only a minimum number of inputs from the user and also that the outputs are very understandable. The only subjective parameters are the weights of the criteria. The TOPSIS method is based on the idea that the optimal solution is the one that has the shortest distance from the ideal solution and is also the furthest from the solution that is negative [29], [30].

The method is based on five computational steps:

1. obtaining performance evaluation of alternatives on various criteria,
2. normalization of assessment,
3. normalized scores are assessed,
4. the distance between the ideal and negative solutions is calculated
5. the ideal solution selected based on ratios of calculated distances [29], [30]

4.3. VIKOR

The VIKOR method is another method that searches for the best solution on a set of alternatives according to the distance from the ideal solution [33]. This method was developed for multi-criteria optimization in complex systems and focused on evaluation and selection in the presence of conflicting criteria. Each alternative is evaluated according to the multi-criteria function, and the resulting compromise solution is obtained based on the proximity to the ideal alternative. The evaluation is obtained using five steps [30], [34].

1. The alternatives are labeled as $x1$, $x2$, … , xm; where m is number of alternatives.
2. Determination of the maximum and minimum values of all criterion functions.
3. Calculation of the utility and regret measure of the respective alternative.
4. Calculation of performance evaluation of alternatives.
5. Sorting of alternatives according to performance evaluation. A lower rating value represents a better alternative [30]

4.4. Comparison and selection

The results of the above methods were compared against results from semi-quantitive risk analysis PIE. We carefully selected security issues for risk analysis and compared only cases with exactly ten threats (criteria). We asked highly renewed experts for security and safety. Each of them made a PIE analysis, and then we made a threat list ranked according to the mean value of obtained results. This list served as a "standard" for comparing our selected methods. The method with the lowest ranking difference against our PIE "standard" was selected for further research. As shown in tab. I. Fuzzy TOPSIS (FTOPSIS) presents the best results. FTOPSIS was added in the progress of research because it allows the processing of opinion of more evaluators.

Table 1: Rank Comparison

	Threat 1	**Threat 2**	**Threat 3**	**Threat 4**	**Threat 5**
TOPSIS	0.20	0.11	0.20	0.19	0.18
AHP	0.28	0.15	0.19	0.23	0.27
VIKOR	0.18	0.12	0.19	0.18	0.23
FTOPSIS	0.08	0.14	0.10	0.12	0.15
	Threat 6	**Threat 7**	**Threat 8**	**Threat 9**	**Threat 10**
TOPSIS	0.11	0.14	0.19	0.12	0.15
AHP	0.28	0.18	0.21	0.30	0.26
VIKOR	0.11	0.15	0.10	0.15	0.12
FTOPSIS	0.10	0.13	0.11	0.14	0.13

Every change of rank by one position is reflected in comparison by value 0.1. The average value for comparison of all cases is in the above table (Tab. I.)

The most significant similarity with PIE (Tab. II.) shows FTOPSIS had similar threats rank for six threats. Similar methods, TOPSIS and VIKOR, has almost identical results. (Tab. I. and Tab. II.)

Table 2: Overal Similarity

	Similarity
TOPSIS	2/10
AHP	0/10
VIKOR	2/10
Fuzzy TOPSIS	6/10

5. Fuzzy TOPSIS

FTOPSIS is a modified standard TOPSIS, which belongs to the most used techniques for MCDM. It consists of adding fuzzy logic that allows the reflection opinion of all decision-makers. This technique utilizes two ideal solutions. Those solutions are called Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS) [29]. The aim is to find a distance from both of these ideal solutions. The longest distance from FNIS and the shortest distance from the FPIS is the best result. It is calculated as a geometric distance from these solutions [16].

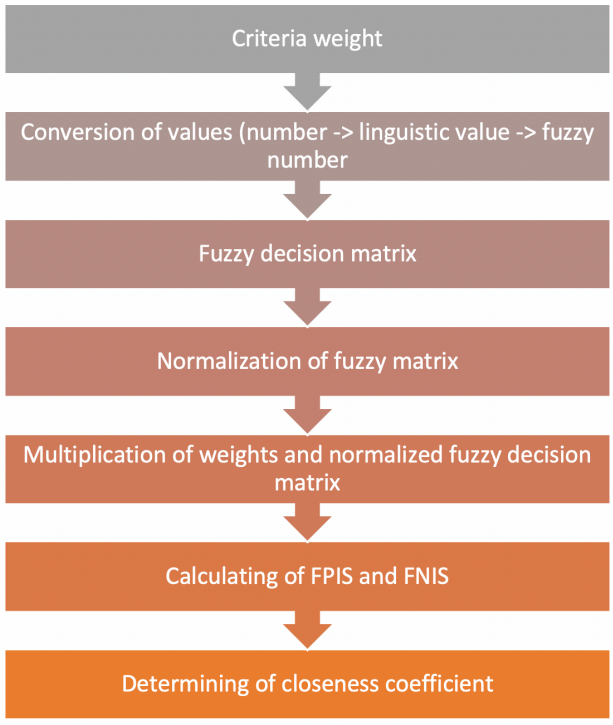

Figure 9:Seven steps of FTOPSIS [1]

Complete calculation and ordering of alternatives according to distance have seven steps (Fig. 9) [1], [16-18].

Table 3: Conversion table [1]

Numerical value	Linguistic value	Fuzzy number
1	Very low	{1, 1, 3}
2	Low	{1, 3, 5}
3	Average	{3, 5, 7}
4	High	{5, 7, 9}
5	Very high	{7, 7, 9}

Usage of linguistic values showed as a not appropriate. Each linguistic value was represented by numerical value which made it easier for our decision-makers. Consequently, we converted it into fuzzy numbers to obtain correct weights for further calculation. (Tab. III.).

Converted fuzzy numbers are used to build a corresponding fuzzy matrix for each decision-maker (three matrices, in our case). Those matrices are merged to the united fuzzy matrix. Every triangular fuzzy numbers is represented by three values ($F=\{a;b;c\}$). Calculation of these values are based on following formulas (1):

$$a_{ij} = min_k\{a_{ij}^k\};\ b_{ij} = \frac{1}{K}\sum_{k=1}^{K} b_{ij}^k; c_{ij} = max_k\{c_{ij}^k\} \quad (1)$$

The uniform matrix is built from a combination of decision matrices and the above formulas. Next step is the normalization of the uniform matrix. Normalization is one of the essential activities for almost all MCDMs. The TOPSIS and also its fuzzy modification work with two types of criteria. The first group brings benefits (eg. increasing efficiency). The second group has a negative influence on the decision maker and this group is called as a cost criteria (eg. salary). Each group has slightly different formula for normalization. Benefits criteria (2) looks for maximal value and cost criteria (3) for minimal value :

$$\tilde{r_{ij}} = \left(\frac{a_{ij}}{c_j^+}, \frac{b_{ij}}{c_j^+}, \frac{c_{ij}}{c_j^+}\right); . c_j^+ = max_i\{c_{ij}\} \quad (2)$$

$$\tilde{r_{ij}} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right);\ a_j^- = min_i\{a_{ij}\} \quad (3)$$

The normalized matrix must be supplemented by criteria weight. Normalized values are simply multiplicated by reciprocal weight values of criterion (4).

$$\tilde{A_1} \otimes \tilde{A_2} = (a_1, b_1, c_1) \otimes (a_2, b_2, c_2) = (a_1 * a_2, b_1 * b_2, c_1 * c_2) \quad (4)$$

Multiplication results are used to find the ideal solution. There are two possible solutions: a positive solution with the "best" values and a negative solution with the worst values. Because this is fuzzy modification than solutions are called as fuzzy positive/negative solutions (FPIS (5)/ FNIS (6)), Calculation of these solution is given by:

$$A^+ = (\tilde{v_1^+}, \tilde{v_2^+}, \ldots \tilde{v_n^+});\ \tilde{v_j^+} = max_i\{v_{ij3}\} \quad (5)$$

$$A^- = (\tilde{v_1^-}, \tilde{v_2^-}, \ldots \tilde{v_n^-});\ \tilde{v_j^-} = min_i\{v_{ij1}\} \quad (6)$$

However, it is the best or the worst situation that probably never occurs. Each involved alternative has its own solution and the distance, which is between FPIS, FNIS and this solution, (7) describes the quality of the involved alternative. The distance is given as:

$$the\ d(\tilde{x}, \tilde{y}) = \sqrt{\frac{1}{3}[(a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2]} \quad (7)$$

The closeness coefficient (8) is the final step to ordering all involved alternatives.

$$CC_i = \frac{d_i^-}{d_i^- + d_i^+} \quad (8)$$

6. Case study

We have focused on applying the TOPSIS method to one cultural event in the case study. The basic information about the event:

- Specialization: music metal concert - group Arakain
- Where: Masters of Rock Café in Zlín, Czech Republic
- Frequency: once a year (various dates)
- Number of visitors: 400 - 500 people

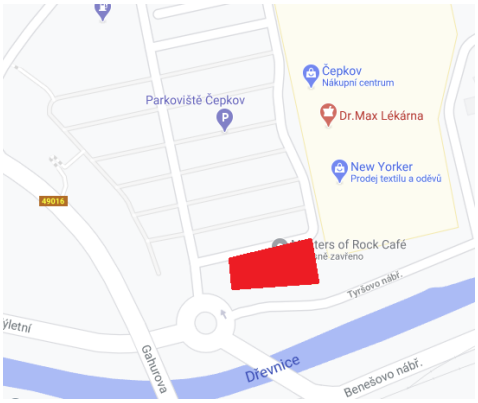

Figure 9: Localization of the Master of Rock Café. [35]

Figure 10: The main entrance of the Mater of Rock Café. [35]

6.1. Risk management

Assets are determined based on a security inspection of the given location, where we analyzed what is crucial for the owner of the building, whether from the point of view of finances, operations, or maintaining continuity. There are assets within the selected object:

- People
- Property of the club, visitors, performers
- Building
- Continuity
- Money
- Etc. [15].

The next step is to identify the threats. Several ways could do this. One possible way is again an on-site security inspection where a security professional has enough experience in the required field and can identify the most problems that may arise. The second way is to start from the threat catalog. A threat catalog is a document or, more accurately, a list of generic and most common threats. This catalog is made by some security experts to provide a tool that may help identify threats and save time.

In our case study, we combined more methods. The threat catalog was thoroughly studied, and some threats were selected as relevant. Check-list had been made from these threats, and this check-list we used for security inspection. Threats identified for our case study:

- **Assault, injury**
- Property theft, damage (vandalism), or destruction
- Pickpocketing
- Fire or flood
- Power failure, delay in the arrival of performers, cancellation of the concert
- Entrance with an invalid ticket [15].

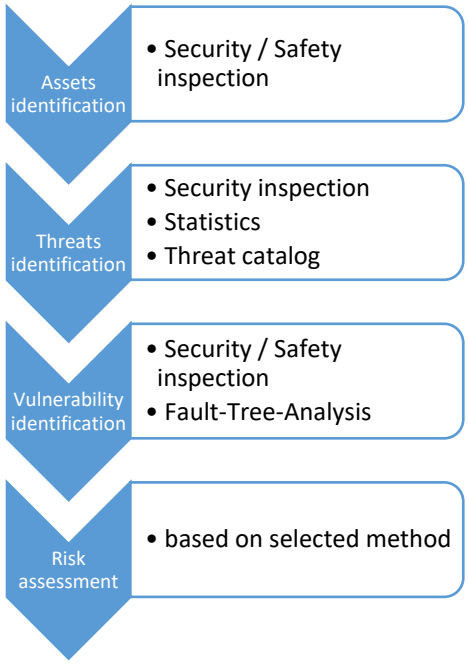

Figure 11: Risk assessment workflow

Vulnerability is always determined at a given location when existing security measures, accessibility to the facility, employee reactions, etc., are checked based on the inspection. Vulnerability identification for our case study:

- Obsolete security systems
- Absence of mechanical restraint systems
- Lack of the Visitor Regulations
- Number of glazed surfaces
- Proximity to the river

- Etc.

The whole process is outlined in the following steps (sub-processes) (fig. 11).

The final risk assessment is made with the help of the TOPSIS method. Inputs are based on the opinion of three "common" security managers. "Common" means that they are not specialized in advanced risk analysis and especially in the field of soft targets protection.

The main objective was to find the most exposed location with the highest probability of attack that may have fatal consequences. Based on experience, the location of attacks is determined by on-site inspection, security assessment, and determining which areas are attractive for the attack. This can be assessed from the point of view of their vulnerability, lack of security, or the number of people we expect at a given location. Thanks to the localization of the attack, when planning security measures, we can directly target security at a given location and thereby strengthen it.

Analyzed localizations are:

- Main entrance
- Audience space
- Stage
- Refreshments space
- Parking lot [15].

Initially, we must define the criteria for TOPSIS, which increase or decrease the risk. The criteria were determined on a similar basis to the location of the attack. Thanks to our many years of experience in planning the security of cultural events, as well as from the methodologies, books, and works of experts that have been published on this topic. Initially, it is always important to say what we want to analyze. For soft targets, one of the most critical locations are those with accumulated large numbers of people. Subsequently, we focus on how easy it is to get into the object, if someone stops the attacker, etc. When I already have security measures, I have to ask if they are effective and if they can detect and respond to an attack.

In many cases, security measures are only passive. It means that security measures serve as a monitoring tool for the occurred security situation but cannot respond. This is entirely unacceptable in the case of an attack on people. Therefore, the effort is to plan measures that will actively detect the attack and trigger some reaction (alarm). Our chosen criteria are defined in the basic document for soft target protection [13]. Those criteria are:

- A number of people – it is labeled as a benefit criterion because more people increase the risk.
- Accessibility – benefit criterion; higher accessibility = lower security -> less effective security measures such as security guards or surveillance system.
- Detectability – because this criterion decreases the risk, it is labeled as a cost criterion. Security guards are able to detect the attack in the early stage.
- Reactivity – another cost criterion. This criterion expresses the time between the start of attack and the first reaction of guards or policemen.

7. Results

There is evaluation from three professionals and security specialists in the following tables (Tab. IV, V, and VI).

Table 4: Decision maker 1 [15]

	Number of people	Accessibility	Detectability	Reactivity
Weight (numerical)	5	3	3	1
Main entrance	{5, 7, 9}	{7, 9, 9}	{1, 3, 5}	{5, 7, 9}
Audience space	{7, 9, 9}	{3, 5, 7}	{3, 5, 7}	{3, 5, 7}
Stage	{1, 3, 5}	{1, 1, 3}	{5, 7, 9}	{5, 7, 9}
Refreshments space	{5, 7, 9}	{3, 5, 7}	{3, 5, 7}	{3, 5, 7}
Parking lot	{1, 3, 5}	{7, 9, 9}	{1, 1, 3}	{1, 3, 5}

Table 5: Decision maker 2 [15]

	Number of people	Accessibility	Detectability	Reactivity
Weight (numerical)	4	4	5	4
Main entrance	{5, 7, 9}	{7, 9, 9}	{5, 7, 9}	{5, 7, 9}
Audience space	{7, 9, 9}	{3, 5, 7}	{1, 3, 5}	{1, 3, 5}
Stage	{1, 3, 5}	{1, 1, 3}	{7, 9, 9}	{5, 7, 9}
Refreshments space	{3, 5, 7}	{3, 5, 7}	{1, 3, 5}	{1, 3, 5}
Parking lot	{1, 3, 5}	{7, 9, 9}	{1, 1, 3}	{1, 1, 3}

Table 6: Decision maker 3 [15]

	Number of people	Accessibility	Detectability	Reactivity
Weight	5	3	4	3
Main entrance	{5, 7, 9}	{7, 9, 9}	{1, 3, 5}	{3, 5, 7}
Audience space	{7, 9, 9}	{3, 5, 7}	{1, 3, 5}	{1, 1, 3}
Stage	{1, 1, 3}	{1, 1, 3}	{7, 9, 9}	{7, 9, 9}
Refreshments space	{3, 5, 7}	{1, 3, 5}	{3, 5, 7}	{3, 5, 7}
Parking lot	{1, 3, 5}	{7, 9, 9}	{3, 5, 7}	{1, 3, 5}

When we have the results from decision makers, we combined the decision fuzzy matrix (1) (Tab. VII).

Table 7: Combined decision fuzzy matrix[15]

		Number of people	Accessibility	Detectability	Reactivity
weight	numerical	5	3	4	3
	linguistic	Very high	Average	High	Average
Main entrance		{5, 7, 9}	{7, 9, 9}	{1, 4.333, 9}	{3, 6.333, 9}
Audience space		{7, 9, 9}	{3, 5, 7}	{1, 3.667, 9}	{1, 3, 7}
Stage		{1, 2.333, 5}	{1, 1, 3}	{5, 8.333, 9}	{5, 7.667, 9}
Refreshments space		{3, 5.667, 9}	{1, 4.333, 7}	{1, 4.333, 7}	{1, 4.333, 7}
Parking lot		{1, 3, 5}	{7, 9, 9}	{1, 2.333, 7}	1, 2.333, 5}

Then we normalized the fuzzy matrix according to (2) and (3) (Tab. VIII).

Table 8: Normalized fuzzy matrix [15]

	Number of people	Accessibility	Detectability	Reactivity
weight	{7, 9, 9}	{3, 5, 7}	{5, 7, 9}	{3, 5, 7}
Main entrance	{0.556, 0.778, 1}	{0.778, 1, 1}	{0.111, 0.231, 1}	{0.111, 0.158, 0.333}
Audience space	{0.778, 1, 1}	{0.333, 0.556, 0.778}	{0.143, 0.273, 1}	{0.143, 0.333, 1}
Stage	{0.111, 0.259, 0.556}	{0.111, 0.111, 0.333}	{0.111, 0.120, 0}	{0.111, 0.130, 0}
Refreshments space	{0.333, 0.630, 1}	{0.111, 0.481, 0.778}	{0.143, 0, 1}	{0.143, 0.032, 1}
Parking lot	{0.111, 0.333, 0.556}	{0.778, 1, 1}	{0.143, 0, 1}	{0.200, 0, 1}

Then we created a weighted normalized fuzzy matrix according to (4) (Tab. IX). The A^+ and A- are according to (5) and (6).

Table 9: Weighted normalized fuzzy matrix [15]

	Number of people	Accessibility	Detectability	Reactivity
Main entrance	{3.889, 7, 9}	{2.333, 5, 7}	{0.556, 1.615, 9}	{0.333, 0789, 2.333}
Audience space	{5.444, 9, 9}	1, 2.778, 5.444}	{0.714, 1.909, 9}	{0.429, 1.667, 7}
Stage	{0.778, 2.333, 5}	{0.333, 0.556, 2.333}	{0.556, 0.840, 1.800}	{0.333, 0.652, 1.400}
Refreshments space	{2.333, 5.667, 9}	{0.333, 2.407, 5.444}	{0.714, 1,615, 9}	{0.429, 0.161, 7}
Parking lot	{0.778, 3, 5}	{2.333, 5, 7}	{0.714, 3, 9}	{0.600, 2.143, 7}
A+	**{5.444, 9, 9}**	**{2.333, 5, 7}**	**{0.714, 3, 9}**	**{0.600, 2.143, 7}**
A-	**0.778, 2.333, 5}**	**{0.333, 0.556, 2.333}**	**{0.556, 0.840, 1.800}**	**{0.333, 0.652, 1.400}**

Then we calculated distance FPIS and FNIS according to (7) (Tab. X).

Table 10: Final FPIS and FNIS distances [15]

	FPIS				FNIS			
Main entrance	1.463	0.000	0.805	3.808	3.977	3.896	4.181	0.650
Audience space	0.000	1.745	0.630	2.217	5.235	2.241	4.203	3.348
Stage	5.235	3.896	4.341	4.253	0.000	0.000	0.000	0.283
Refreshments space	2.632	2.093	0.799	3.002	3.137	2.090	4.182	3.234
Parking lot	4.959	0.000	0.000	1.929	0.385	3.896	4.341	3.433

As the results show, the riskiest area is the audience space. Many people in a small area have a crucial effect on early detection and mainly on possible reactions. A mass of people complicates and prevents the moving of security guards. The second risky area is the main entrance. It reflects practical experience from previous terrorist attacks. Many people standing in the queue are very attractive to attack by vehicles. The parking lot stands in third place. Protection of this area is a little bit complicated because people move in unpredictable directions, and installing anti-collision barriers is almost impossible. The results were calculated by using the formula (8) (Tab. XI).

Table 11: Results [15]

CC_i	**Localizations**	**rank**
0,676	Main entrance	2
0,766	Audience space	1
0,016	Stage	5
0,597	Refreshments space	4
0,636	Parking lot	3

8. Discussion

There are many different methods that should be tested in the risk management of soft targets; however, FTOPSIS shows very promising results (Tab. XI). It can easily involve "standard" security managers and specialists and reflect the opinion of all of them. Also, the results were discussed and consulted with experts for soft targets protection. Their professional view confirmed our results. The exact value of risk is not important. Important is the rank in the case of social or cultural events. It is necessary to test this method and approach for other types of soft targets and validate results with others risk analysis methods.

Used method (FTOPSIS) has provided results that are consistent and comparable with practice. Even if this case study was limited by cooperation with only three experts, the results are representative enough. This case study also validates and confirms the utilization of FTOPSIS as a risk analysis. Many other risk analyses have a problem subjective approach of an evaluator. This could be a serious problem when we have different results from different evaluators. This may bring an underestimation of risk, which means, in general, higher risk. FTOPSIS brings a certain amount of objectivity and it should be used without prominent experience in soft target protection.

This article aimed to examine one of the risk analysis methods and test it with other selected methods. As already mentioned, the intention is to find a method that will be simple for experts, quick to use, and above all, objective. But the work of a security expert does not end there. We now know what and where we are in danger and to what extent. Subsequently, it is necessary to start the process of reducing the risk, where we look for various measures to reduce the resulting value of the threat. There are several ways - security measures, insurance, avoiding a given risk, monitoring, etc. The most commonly used are technical and non-technical security measures, by which we understand various security systems, camera systems, and fire protection, but also the setting of processes for how to behave in the event of a security incident, crisis communication, detection of suspicious behavior, training of security and emergency personnel, etc.

9. Conclusion

Risk analysis is about finding and ordering risks. This process is very similar to other decision-making processes and thus, MCDM should be effectively applied to this field. The biggest challenge, as for every decision-making, is correctly defined criteria. A properly set template may save a lot of time, and usage of FTOPSIS could be faster and more time effective than other risk analysis methods based on subjective opinion. On the other hand, FTOPSIS presumes some elementary knowledge of mathematics.

Next research step is case studies and validation on upcoming events. We would like to use MCDM not only for risk analysis but also for prioritization of proposed security measures and evaluation of incidents.

Acknowledgment

This work was supported by the research project VI20192021163 "Built-up and operation development of security systems at mass events", supported by the Ministry of the Interior of the Czech Republic in the years 2019-2021.

References

[1] D. Kotkova, L. Kralik, L. Kotek, "Multiple Criteria Decision-making: Risk Analyses for Cultural Events as one of the Soft Target Categories," in 2021 IEEE International Carnahan Conference on Security Technology (ICCST) 1-6, 2021, doi: 10.1109/ICCST49569.2021.9717382.

[2] D. Lapkova, L. Kotek, J. Nevrkla, K. Jenckova, "Decision support - Tool for customization of security measures for cultural events," in 2020 11th Iberian Conference on Information Systems and Technologies (CISTI), 1-6, doi: 10.23919/CISTI49556.2020.9140917.

[3] D. Kotkova, M. Hromada, T. Sternova, K. Ljubymenko, "Methodology of identification and protection of soft targets of transport infrastructure – initial study," in 2020 Transport Means - International Conference, 1107-1112. 2020.

[4] L. Kotek, M. Hromada, D. Lapkova, "Protection of Soft Targets from Terrorism," in 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), 71-78. 2019, doi: 10.1109/ACDT47198.2019.9072743.

[5] D. Lapkova, L. Kotek, D. Rozek, "Terrorism Situation and Identification of Soft Target's Attractiveness," in 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), 65-70, 2019, doi: 10.1109/ACDT47198.2019.9072875.

[6] D. Lapkova, L. Kotek, D. Rozek, "Counter-terrorism Measures - Determining of Soft Target's Vulnerability," in 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), 79-84, 2019, doi: 10.1109/ACDT47198.2019.9072861.

[7] L. Kotek, M. Hromada, D. Kotkova, "Educational platform for personal and community protection situations from the perspective of soft targets," in 2020 Iberian Conference on Information Systems and Technologies (CISTI), 1-4, 2020, doi: 10.1109/ICCST52959.2022.9896561.

[8] D. Kotkova, K. Jenckova, "DETERMINING OF SOFT TARGET'S VULNERABILITY," in 2019 DAAAM International Scientific Book, 205-214, 2019, doi: 10.2507/daaam.scibook.2019.16.

[9] D. Kotkova, K. Jenckova, "COMPARISON OF MODUS OPERANDI OF TERRORIST'S ATTACKS - VEHICLE RAMMING ATTACK AND FIREARM ATTACK," DAAAM International Scientific Book 2019. Vienna : DAAAM International Vienna, **2019**, s. 191-198. ISBN 978-3-902734-24-2, doi: 10.2507/daaam.scibook.2019.14.

[10] D. Kotkova, T. Sternova, Z. Kalvach, L. Kotek, "The Process to Plan Security Measures for Cultural Events," in 2021 IEEE International Carnahan Conference on Security Technology (ICCST), 1-6, 2021 doi: 10.1109/ICCST49569.2021.9717380.

[11] D. Kotkova, M. Hromada, M. Malanikova, S. Kovar, "The concept of a software tool with an interactive map for identification and determination of soft targets of transport infrastructure," in 2021 IEEE International Carnahan Conference on Security Technology (ICCST), 1-5, 2021 doi: 10.1109/ICCST49569.2021.9717375.

[12] K. Ljubymenko D. Kotkova, T. Sternova, "Use of detection of suspicious behavior in ensuring the security of persons in transport," in 2021 IEEE International Carnahan Conference on Security Technology (ICCST), 1-4, 2021, doi:10.1109/ICCST49569.2021.9717399.

[13] Z. Kalvach, "Definition of Soft Targets," Prague, 2017

[14] T. Sternova, "Vývoj teroristických útoků v období 2014 - 2017. Rozbor vybraných útoků v roce 2017 (Development of terrorist attacks in 2014-2017. Analysis of selected attacks in 2017.)," in The Conference of Security Technologies, Systems and Management, 2017.

[15] Application for database management of terrorist attacks, *DoVA* [online], Prague, 2019.

[16] L. Hofreiter, V. Berezutskyi, L. Figuli, Z. Zvakova, "Soft Target Protection-NATO Science for Peace and Security Series C: Environmental Security," Springer, ISBN: 978-94-024-1754-8.

[17] S. Nădăban, S. Dzitac, I. Dzitac, "Fuzzy TOPSIS: A General View," Procedia Computer Science, **91**, 823-831, 2016, doi: https://doi.org/10.1016/j.procs.2016.07.088.

[18] I. Mahdavi, A. Heidarzade, B. Sadeghpour-Gildeh, "A general fuzzy TOPSIS model in multiple criteria decision making," Int J Adv Manuf Technol **45**, 406 – 420, 2009. https://doi.org/10.1007/s00170-009-1971-5

[19] N. B. Kore, K. Ravi, S. B. Patil, "A simplified description of fuzzy TOPSIS method for multi criteria decision making," International Research Journal of Engineering and Technology (IRJET), **4**(5), 2047-2050, 2017, e-ISSN: 2395 -0056.

[20] G. Kannan, S. Pokharel, P. S. Kumar, "A hybrid approach using ISM and fuzzy TOPSIS for the selection of reverse logistics provider," Resources, Conservation and Recycling, **54**(1), 28-36, 2009 doi: https://doi.org/10.1016/j.resconrec.2009.06.004.

[21] E. Afful-Dadzie, "Hybridized integrated methods in fuzzy multicriteria decision making (with case studies)," PhD Thesis, Thomas Bata University in Zlin, 2013.
[22] B. Vahdani, S. M. Mousavi, R. Tavakkoli-Moghaddam, "Group decision making based on novel fuzzy modified TOPSIS method," Applied Mathematical Modelling, **35**(9), 4257-4269, 2011, doi: https://doi.org/10.1016/j.apm.2011.02.040.
[23] P. Rani, A. R. Mishra, A. Mardani, F. Cavallaro, M. Alrasheedi, A. Alrashidi, "A novel approach to extended fuzzy TOPSIS based on new divergence measures for renewable energy sources selection," Journal of Cleaner Production, **257**(1), 120352, 2020, doi:10.1016/j.jclepro.2020.120352.
[24] G. K. Koulinas, O. Demesouka, P. Marhavilas, A. P. Vavatsikos, D. Koulouriotis, "Risk assessment using fuzzy TOPSIS and PRAT for sustainable engineering projects," Sustainability, **11**, 615, 2019, doi: 10.3390/su11030615.
[25] M. Nazam, J. Xu, Z. Tao, J. Ahmad, M. Hashim, "A Fuzzy AHP-TOPSIS Framework for the Risk Assessment of Green Supply Chain Implementation in the Textile Industry," International Journal of Supply and Operations Management, **2**(1), 548-568, 2015, doi: 10.22034/2015.1.02
[26] K. Jenckova, "Zajišťování bezpečnosti kulturních akcí za účasti většího množství osob v České republice (Ensuring the safety of cultural events with the participation of a larger number of people in the Czech Republic)," diploma thesis, Police Academy of Czech Republic in Prague, 2019.
[27] D. Kotkova, L. Kralik, "Change Of Soft Target's Resilience In Time – Case Study," in 2019 DAAAM International Scientific Book, 199-204, 2019, doi: 10.2507/daaam.scibook.2019.15.
[28] R. F.S.M. Russo, R. Camanho, "Criteria in AHP: A Systematic Review of Literature, Procedia Computer Science," **55**, 2015, 1123-1132, https://doi.org/10.1016/j.procs.2015.07.081.
[29] M. Behzadian, S. K. Otaghsara, M. Yazdani, J. Ignatius, "A state-of the-art survey of TOPSIS applications, Expert Systems with Applications," Volume **39**(17), 2012, Pages 13051-13069, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2012.05.056.
[30] T. Licek, "Vícekriteriální rozhodování agentů v ekonomických prostředích," University of Hradec Kralove, 2015, Czechia.
[31] A. Daniel, F. E. Onuodu, "A Fuzzy AHP Model for Selection of University Academic Staff," International Journal of Computer Applications **141** (2016), 19-26, 2016, doi: 10.5120/ijca2016908969.
[32] R. R. Venkata, "Decision making in manufacturing environment using graph theory and fuzzy multiple attribute decision making methods," Springer, 2013, doi: https://doi.org/10.1007/978-1-4471-4375-8.
[33] K. Mela, T.Tianen and M. Heinisuo, "Comparative study of multiple criteria decision making methods for building design," Advanced Engineering Informatics, **26**(4), 716-726, 2012, doi: https://doi.org/10.1016/j.aei.2012.03.001.
[34] A. Mardani, E. K. Zavadskas, K. Govindan, A. Amat Senin, A. Jusoh, "VIKOR Technique: A Systematic Review of the State of the Art Literature on Methodologies and Applications," Sustainability. **8**(1), 37, 2016, https://doi.org/10.3390/su8010037
[35] Google Maps Available from: https://www.google.com/maps/place/Zl%C3%ADn/@49.2284554,17.6597917,17z/data=!4m5!3m4!1s0x47130cad4c888e0d:0x418d4c16a8ac214f!8m2!3d49.2244365!4d17.6627635