Advances in Reliability, Safety and Security, Part 7 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-19-7 (printed), ISBN 978-83-68136-06-7 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Current Trends and Experience In Soft Targets Protection

Martin Hromada, Martin Bajer, Hemin Akram Muhammad

Tomas Bata University in Zlín, Faculty of Applied Informatics, Zlín, Czech Republic

Abstract

The issue of Soft Targets Protection is considered a strategic area of interest due to current trends in the security environment. The specific conditions and properties of this infrastructure system type increase the need for the creation of methodological tools for the objectification of risk assessment and the optimization of security measures. Due to the need for greater addressability, the article will be tied to the conditions in the Czech Republic in the context of the normative definition and classification of Soft Targets in a wider context. In the beginning of the article, the basic framework for understanding the issue in the environment of the Czech Republic will be presented, with a general definition of the basic philosophical framework of the security pillars. In view of the research activities of the author's collective workplace, selected methodological tools will be described. For the necessary level of detail, one selected methodological tool will be presented in detail.

Keywords: aoft targets, protection, resilience, risk, identification aspect, analytical aspect, application aspect

1. Introduction

As stated, the introductory part of the contribution will be devoted to the normative definition and classification of Soft Targets with regard to the conditions of the Czech Republic.

The basic strategic document that deals with the issues of the soft targets' protection of in the Czech Republic is the Conception of the Soft Targets Protection for the Years 2017–2020 (hereinafter referred to as the Conception), which was issued in 2017 (MoI CR, 2017) and (Apeltauer et al., 2019). The conception was approved by Government Resolution No. 711 of July 27, 2016. The aim was to establish the policy of the Czech Republic in the relatively new issue of soft targets protection and preparation of a well-functioning ST protection system establishment in the Czech Republic. At the outset, it is essential to realize that ST protection is based on protection of persons from terrorist and other serious violent attacks. Property protection is not the main interest of this area, or state policy, as is the case, for example, with the prevention of classic crime.

For the purposes of the Conception, the following definition is established: "***The term soft target refers to objects, spaces or events characterized by the frequent presence of a large number of people and at the same time the absence or low level of security against violent attacks.***" (MoI CR, 2017). It can be open spaces, but also closed spaces that are publicly accessible and where a large number of people are present. These places become targets for attackers because it is easy to cause great harm to the lives and health of persons. The large media impact that such an attack will cause is also an inescapable aspect. The number of attendees varies throughout the day, depending on opening hours and events in the space. It is important to collect this data in order to effectively target the security measures. A low level of security against violent attacks, or its complete absence, is important for target selection, as perpetrators generally follow the path of least resistance, where they want to achieve the greatest effect with the least effort. Many objects currently have physical security measures implemented, but most of them are measures for the guarding assets purpose, therefore, in such a mode of operation, it has only limited effectiveness in ST protection.

Examples of soft targets (MoI CR, 2017) and (Apeltauer et al., 2019):

- Bars, clubs, restaurants, hotels,
- Cinemas, theaters, concert halls and halls,
- Community centers,
- Cultural, sports events,

- Religious monuments and places of worship,
- Shops, shopping centers, markets,
- Hospitals,
- Parks, squares, streets, promenades,
- Demonstrations, parades, gatherings,
- Sports halls, stadiums,
- Schools, school facilities, dormitories, libraries,
- Tourist centers, monuments and attractions, museums, galleries,
- Government buildings and public institutions,
- Interchanges, train and bus stations, airport halls and terminals,
- Other symbolically significant places and events.

For soft target, a key feature is their attractiveness, which expresses how attractive the target is to the attacker. The attractiveness for an attacker can be influenced by the following criteria:

- Openness to the public,
- Presence and quality of security personnel,
- Number and concentration of people,
- Presence of the Police of the Czech Republic or municipal (city) police,
- Media presence,
- Symbolism of the goal.

The Conception of soft target divides according to several factors. One is permanence or temporality:

- Permanent soft targets
    - Outdoor spaces
        - Stadiums,
        - Sports complexes
        - Marketplace,
        - Other,
    - Indoor spaces
        - Shopping centers,
        - Theaters,
        - Hospital,
        - Other,
- Temporary soft targets
    - Temporary paid events
        - Festivals,
        - Concerts,
        - Other,
    - Temporary events with free entry
        - Demonstration,
        - Christmas and Easter markets,
        - Marathons,
        - Next.

The basic classification and definition of individual soft targets types creates an idea of the changing conditions and properties. Understanding the different nature of individual soft targets types is an important aspect of correctly defining and establishing security approaches and measures.

2. Principles of soft target protection

As stated, the definition of specific measures for a specific type of soft targets must be based on the definition of the basic principles of protection. The following text therefore presents a philosophical level that is generally applicable to all soft targets types.

Four main principles of soft targets protection are established in the Conception

- Security is a matter for all concerned entities,
- Proactive attitude,
- Teamwork, cooperation.
- Setting communication processes and organization, and coordination of people's activities.

2.1. Soft target security as the responsibility of all concerned entities

At this point, the emphasis is on realizing that the subject should primarily take care of his own security and not leave everything to the state or the armed forces. This principle is based, among other things, on the reflection of the simple fact that violent attacks usually happen in a matter of seconds and minutes, and in most cases, it is not possible at all in terms of time for the state to effectively intervene at every soft target in the territory of the Czech Republic. It is also a reflection of the fact that there are a very large number of soft targets and no state is capable of covering the protection of all these targets at the same time. "*Then, if we talk about the fact that part of the responsibility for one's own security is necessarily borne by the soft targets itself, i.e. its founder, owner, operator and the like, it is also appropriate to emphasize the role of regions, cities and municipalities, which are the founders of many organizations in the field of culture, education, healthcare, social services and others. And then they are precisely in the position of the soft target founder, partly responsible for its security."* (MoI, 2017) and (Apeltauer et al., 2019)

2.2. Proactive attitude

A proactive approach is a necessary step to increase the security of a given soft target. It is necessary to anticipate, prevent emergencies and incidents and set up your system to respond quickly to a violent attack. This is partly because without this preparation there is practically no chance to respond effectively to such intense and fast incidents. Partly because proactive preparation multiplies the chance of reducing the consequences compared to just a simple reaction to the incident which is limited, for example, to efforts to reduce the consequences (e.g. measures only in the form of taking out insurance for a given type of event).

2.3. Teamwork, cooperation.

Cooperation must be between all interested parties – starting with the owner, through the security forces to municipalities, regions and ministries. Currently, the cooperation of soft target among themselves is also being developed. Groups are created on various communication platforms where information and good practice are shared.

2.4. Setting communication processes and organization, and coordination of people's activities.

A large number of soft targets face the finance problems. But for the soft target protection, it is necessary to focus primarily on security measures of a non-technical nature - setting up communication processes, coordinating the activities of people present at the given location, training, dividing tasks and powers, creating security analyzes and audits, etc. These security measures are often not associated with spending significant financial resources. When setting up processes, it is advisable to focus on all employees, whether they are professional or non-professional personnel.

From what has been presented, it is clear that the principles of protection established by the concept are only a basic definition of areas that can be considered fundamental in the subsequent process of formulating specific measures for specific soft targets types. The following text will therefore present methodological approaches that respect this basic framework and conditions. Subsequently, the selected methodology will be described and presented in detail.

3. Methodical procedures for the soft target protection

Methodological procedures solving selected aspects of the specific soft targets types security will be described in the following text. The subject methodologies were created as outputs of selected security research projects of the Security Research Program of the Ministry of the Interior of the Czech Republic and at the same time selected programs of the Technology Agency of the Czech Republic. The selected certification authority certified all presented methodologies. In chapter 3.1. the methodology that creates a basic and introductory approach to the creation of a complete and functional security system of this infrastructure system type will then be presented.

Methodology for increasing the protection and resilience of selected soft target categories

The methodology was developed with the support of grant project VI20192022118 "Protection of soft targets in the security environment of the Czech Republic", supported by the Ministry of the Interior of the Czech Republic in the years 2019-2022.

The aim of the methodology is the development of basic requirements and approaches to the soft target objects protection with a specific link to increasing their resilience in a wider context. For these purposes, soft target objects are characterized as objects with a higher concentration of people and a relatively low level of security and protection. The ambition of this methodology was to develop the current state of knowledge, accepted methodological starting points approved by state administration bodies; experience based on so-called good practice and achieved project results. This chosen approach makes it possible to reflect and solve to a certain extent a general understanding of the issue of soft target protection. A set of preventive and mitigation tools for the needs of increasing the general soft target preparedness was presented here.

The benefit of this methodology is the creation of a concrete and objective tool for increasing the ST resilience level, also in relation to the needs to ensure a complex, multi-level system these infrastructure systems protections.

A new parameter that this methodology brings is the convergence of approaches to the assessment of internal and external aspects of vulnerability and, at the same time, internal and external aspects of security, considering organizational and regime aspects. This methodical approach therefore objectifies the process of assessing the level of vulnerability and security in a wider context and can be used to assess the resilience of both existing and future soft target objects. This methodology is a recommendatory and inspirational document, with no obligation to standardize its use. Locally specific adaptation of individual criteria can be expected (Hromada and Frohlich, 2021).

Methodology for the implementation of technical measures to increase the railway infrastructure soft target protection

The result was created as part of the solution to the project Increasing the resilience and security of the railway infrastructure and minimizing the impacts on other transport infrastructure sectors, reg. no. CK01000015. This project is co-financed with the state support of the Technology Agency of the Czech Republic as part of the Transport 2020+ Program.

The methodology approaches the implementation of technical measures to increase the railway infrastructure ST protection as an interrelated process, which will be implemented in four consecutive steps. First, the level of soft target risk and security is determined, and then the level of its technical protection is calculated, and absent technical measures will be recommended.

The methodology is focused on the application of the concept of the CPTED method (Crowe, 2013) to selected types of railway infrastructure objects. The methodology is developed in accordance with national and international standards intended for planning and designing the objects layout. The proposed measures are integrated into the overall concept of the design of the given object, including in relation to the possible misuse of transport means. The draft measures are based on a strategy of natural supervision, control, management of space maintenance and areas division.

The novelty of the methodology lies primarily in the method of railway infrastructure ST technical protection level through the determination of the risk and security level with a direct link to the calculation of the technical protection level using a set of simple criteria to which clear values can be assigned (Hromada et al., 2022).

Methodology for transport infrastructure objects identification and protection

The result was created within the framework of the project Development of identification and protection methods of transport infrastructure ST to increase their security and resilience against terrorist attack, reg. no. TH04010377. This project is co-financed with the state support of the Technology Agency of the Czech Republic within the EPSILON Program.

The aim of the methodology is to provide operators of vulnerable transport infrastructure buildings with a methodological framework through which they will be able to carry out a comprehensive risk analysis of these objects, with an emphasis primarily on anthropogenic threats. The methodology emphasizes the use of quantitative or semi-quantitative risk analysis methods with an emphasis on subsequent assessment of their impacts and prioritization of countermeasures.

The novelty of the methodology lies primarily in the method of determining the riskiness of a transport infrastructure object through the assessment of its identification, analytical and application aspect using a set of simple criteria to which clear values can be assigned. At the same time, the methodology connects the results of this analysis with a detailed analysis of the priority risk scenarios identified in this way and their impacts (Hromada et al., 2021).

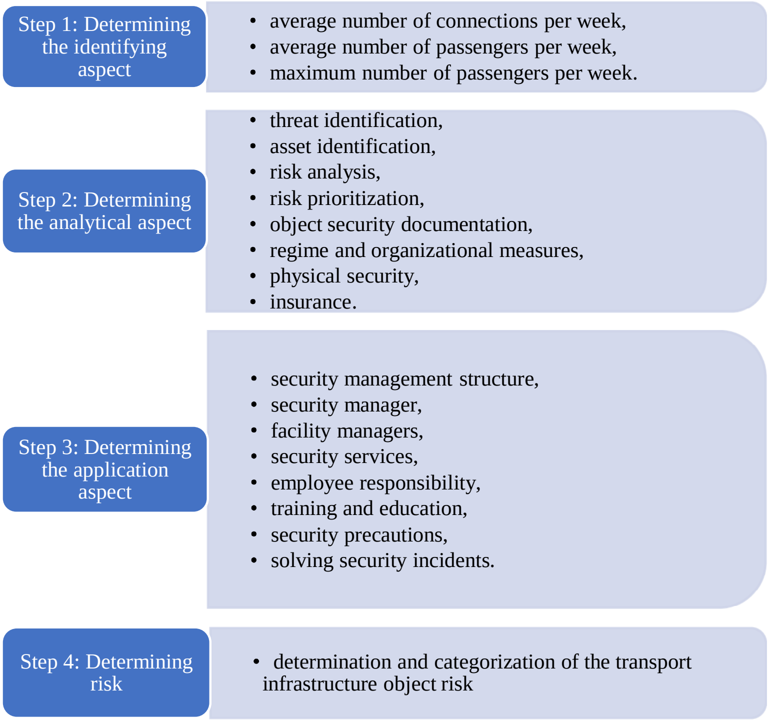
3.1. Methodology for transport infrastructure objects identification and protection

When creating this methodology, the research team had to take into account the fact that transport infrastructure operators often do not have even the basic framework of a security system in place. It was therefore necessary to create an assessment system that would, on the one hand, enable risk assessment and, on the other hand, formulate areas that can be considered as basic attributes of a functional security system.

The methodology approaches risk analysis as an interrelated process, which will be implemented in three consecutive steps: firstly, the identification, analytical and application aspects of the object will be assessed, followed by threat analysis with an emphasis on quantitative methods, and in the last step, the implementation of the results of this analysis to assess individual scenarios and their impacts. At the same time, the methodology provides simple worksheets for the analysis individual steps as a whole.

The methodology is intended for urban, rail and bus mass transport and transfer terminals of this transport operators, which is in national, supra-regional and regional mode. The methodology can be applied to stations, railway stations and subway, train and bus transfer terminals, while in the case of these objects the application is limited to those parts of the objects where passengers move (thus excluding e.g. technical facilities).

The basic publication of the preceding methodology is the work of Pacinda - Network analysis and the KARS method. (Pacinda S., 2010) For the first time, this work introduces the method of quantitative risk analysis using risk correlation (hereafter referred to as KARS). Another key starting point is the work of Saaty T.L (Saaty, 2018). Decision making with the analytical hierarchy process, which defines a method of pairwise comparison of variants supporting evaluation of criteria hierarchies. The methodology develops and practically implements these theoretically defined procedures in a specific area.



Step 1: Determining the identifying aspect

- average number of connections per week,
- average number of passengers per week,
- maximum number of passengers per week.

Step 2: Determining the analytical aspect

- threat identification,
- asset identification,
- risk analysis,
- risk prioritization,
- object security documentation,
- regime and organizational measures,
- physical security,
- insurance.

Step 3: Determining the application aspect

- security management structure,
- security manager,
- facility managers,
- security services,
- employee responsibility,
- training and education,
- security precautions,
- solving security incidents.

Step 4: Determining risk

- determination and categorization of the transport infrastructure object risk

Fig. 1. Transport infrastructure object risk assessment process (Hromada et al., 2021).

Due to the nature of transport infrastructure objects as an important infrastructure system, the identification aspect will to some extent reflect the logic of object identification and marking; transport infrastructure, from the point of view of the proposed criteria cross-cutting nature. In this context, the following categories of criteria are identified:

- Average number of connections per week,
- Average number of passengers per week,

- Symbolism,
- Significance,
- Territorial transport links.

For the assessment of the identification aspect of the transport infrastructure object risk, Assessment sheet 1 is used, differentiating objects according to the nature of transport:

Assessment sheet 1: Assessment of the identification aspect

Table 1. Assessment sheet 1: Assessment of the identification aspect (Hromada et al., 2021).

ID	Controlled area	State Yes/No
1.	**Coefficient expressing the average number of connections per week (P_{st})**	
1.1	Is the average number of transport connections per week greater than 350 (an average of 50 connections per day) within the transport infrastructure object?	
2.	**Coefficient expressing the average number of passengers per week (P_{lp})**	
2.1	Does the average weekly number of passengers exceed 14,000/week (an average of 2,000 people per day)?	
3.	**Coefficient expressing symbolism**[1] **(P_{sm})**	
3.1	Can the object of transport infrastructure be perceived from the point of view of religious, political or social symbolism?	
4.	**Coefficient expressing the object significance (P_{vo})**	
4.1	Is the selected object of transport infrastructure of regional importance?	
5.	**Coefficient expressing territorial transport ties (P_{dv})**	
5.1	Does the selected object of transport infrastructure have a territorial connection to another type of transport?	

If the criterion is met and the answer is Yes, the given variable is assigned the value 1, if the answer is No, the value 0.

The calculation of the identification aspect of the transport infrastructure object risk is a weighted average of the defined variables according to relation (1):

$$A_{id} = P_{st} \cdot v_{st} + P_{lp} \cdot v_{lp} + P_{sm} \cdot v_{sm} + P_{vo} \cdot v_{vo} + P_{dv} \cdot v_{dv} \qquad (1)$$

where the weights of the individual defined variables are determined by the following table.

Table 2. Weights of the identification aspect individual defined variables (Hromada et al., 2021).

	P_{st}	P_{lp}	P_{sm}	P_{vo}	P_{dv}	$\sum$
v_j	0,15	0,20	0,25	0,15	0,25	1,0

The determination of the weighting coefficients and their subsequent normalization was carried out on the basis of an expert assessment of the expected future users of the method (i.e. subjects of selected territorial entities using the Analytic Hierarchy Process method, which is based on a pairwise comparison of variants supporting the assessment of the hierarchy of criteria.

Assessment of the identification aspect of the transport infrastructure object risk:

$$\langle 1; 0.5 \rangle \ = \text{high identification aspect}$$
$$\langle 0.499; 0.250 \rangle \ = \text{moderate identification aspect}$$
$$\langle 0.249; 0 \rangle \ = \text{low identification aspect}$$

[1] It expresses the increased danger of the object due to the motivation of the potential attacker

Assessment sheet 2 is used to assess the analytical aspect of the transport infrastructure object risk

Assessment sheet 2: Assessment of the analytical aspect

Table 3. Assessment sheet 2: Assessment of the analytical aspect (Hromada et al., 2021).

ID	Controlled area	State Yes/No
1.	**Threat identification coefficient (K_{ih})**	
1.1	Does the operator carry out the identification and categorization of threats?	
2.	**Asset identification coefficient (K_{ia})**	
2.1	Does the operator carry out identification and categorization of assets?	
3.	**Risk analysis coefficient (K_{ar})**	
3.1	Is the risk analysis method and process described and implemented?	
4.	**Risk prioritization coefficient (K_{pr})**	
4.1	Are the risks, as an output of the risk analysis, prioritized?	
5.	**Object security documentation coefficient (K_{dz})**	
5.1	Does the operator have a description (documentation) of the facility's security technical protection systems?	
6.	**Coefficient of regime and organizational measures (K_{ro})**	
6.1	Are regime and organizational measures established by the operator?	
7.	**Coefficient of physical security (K_{fo})**	
7.1	Is physical security formalized within the operator and part of the physical protection system?	
8.	**Insurance coefficient (K_{po})**	
8.1	Does the operator have insurance covering insurance risks specific to transport infrastructure objects?	

If the criterion is met and the answer is Yes, the given variable is assigned the value 0, if the answer is No, the value 1.

The calculation of the analytical aspect of the transport infrastructure object risk of the is a weighted average of the defined variables according to relation (2):

$$A_{an} = K_{ih} \cdot v_{ih} + K_{ia} \cdot v_{ia} + K_{ar} \cdot v_{ar} + K_{pr} \cdot v_{pr} + K_{dz} \cdot v_{dz} + K_{ro} \cdot v_{ro} + K_{fo} \cdot v_{fo} + K_{po} \cdot v_{po} \qquad (2)$$

where the weights of the individual defined variables are determined by the following table

Table 4. Weights of the analytical aspect individual defined variables (Hromada et al., 2021).

	K_{ih}	K_{ia}	K_{ar}	K_{pr}	K_{dz}	K_{ro}	K_{fo}	K_{po}	Σ
v_j	0,10	0,10	0,15	0,10	0,10	0,20	0,15	0,10	1,0

Determination of the weight coefficients and their subsequent normalization was carried out using the same method as in the case of the calculation of the identification aspect of the riskiness of the transport infrastructure object.

Assessment of the analytical aspect of the transport infrastructure object risk:

$$\langle 1; 0.5\rangle \ = \text{low analytical aspect}$$
$$\langle 0.499; 0.250\rangle \ = \text{moderate analytical aspect}$$
$$\langle 0.249; 0\rangle \ = \text{high analytical aspect}$$

Assessment sheet 3 is used to assess the application aspect of the transport infrastructure object risk:

Assessment sheet 3: Assessment of the application aspect

Table 5. Assessment sheet 3: Assessment of the application aspect (Hromada et al., 2021).

ID	Controlled area	State Yes/No
1.	**Security management structure coefficient (K_{sb})**	
1.1	Does the operator have a defined internal security management structure?	
2.	**Security management structure coefficient (K_{bm})**	
2.1	Is the function of a security manager related to the protection of transport infrastructure objects established within the operator?	
3.	**Coefficient of facility management (K_{so})**	
3.1	Are facility managers specified within the operator?	
4.	**Coefficient of security services outsourcing (K_{bs})**	
4.1	Are the operator's security services handled by outsourcing?	
5.	**Coefficient of employee responsibility (K_{oz})**	
5.1	Does the operator determine the responsibilities and tasks of the employees in custody for the protection of the transport infrastructure objects?	
6.	**Coefficient of training and education (K_{sv})**	
6.1	Does the operator carry out training and education of employees in connection with the protection of transport infrastructure objects?	
7.	**Coefficient of security measures control (K_{kb})**	
7.1	Is a security measures control process created and implemented within the operator?	
8.	**Coefficient of solving security events/incidents (K_{rb})**	
8.1	Has the operator set up a process for solving/reporting security events/incidents?	

If the criterion is met and the answer is Yes, the given variable is assigned the value 0, if the answer is No, the value 1).

The calculation of the application aspect of the transport infrastructure object risk is a weighted average of the defined variables according to relation (3):

$$A_{ap} = K_{sb} \cdot v_{sb} + K_{bm} \cdot v_{bm} + K_{so} \cdot v_{so} + K_{bs} \cdot v_{bs} + K_{oz} \cdot v_{oz} + K_{sv} \cdot v_{sv} + K_{kb} \cdot v_{kb} + K_{rb} \cdot v_{rb} \qquad (3)$$

where the weights of the individual defined variables are determined by the following table

Table 6. Weights of the application aspect individual defined variables (Hromada et al., 2021).

	K_{sb}	K_{bm}	K_{so}	K_{bs}	K_{oz}	K_{sv}	K_{kb}	K_{rb}	$\sum$
v_j	0,10	0,15	0,05	0,15	0,10	0,15	0,10	0,20	1,0

The determination of the weighting coefficients and their subsequent normalization was carried out using the same method as in the case of the calculation of the identification aspect of the transport infrastructure object risk.

Evaluation of the application aspect of the transport infrastructure object risk:

$$\langle 1; 0.5 \rangle \ = \text{low application aspect}$$
$$\langle 0.499; 0.250 \rangle \ = \text{moderate application aspect}$$
$$\langle 0.249; 0 \rangle \ = \text{high application aspect}$$

The calculation and assessment of the transport infrastructure soft target risk is implemented as an arithmetic average of the values of the above steps, according to relation (4):

$$R = \frac{1}{n}\sum_{i=1}^{n} D_i = \frac{A_{id}+A_{an}+A_{ap}}{3} \qquad (4)$$

$R$where R = the transport infrastructure soft target risk; D_i = i-th determinant R; n = number of determinants; A_{id} = identification aspect; A_{an}= identification aspect; A_{ap}= application aspect.

Categorization of the transport infrastructure soft target risk

$$\langle 1; 0{,}5\rangle = \text{high risk}$$
$$\langle 0{,}499; 0{,}250\rangle = \text{moderate risk}$$
$$\langle 0{,}249; 0\rangle = \text{low risk}$$

As stated at the beginning of this subchapter, the goal of the methodology was to create an evaluation system that, on the one hand, would enable risk assessment and, on the other hand, formulate areas that can be considered basic attributes of a functional security system. The resulting risk value in this context serves as information about the quality and sufficiency of the security system of a specific object with regard to the requirements of the founder. It then enables the operator to determine areas that can positively influence the value of the risk.

4. Conclusion

Protection of soft targets is a complex issue. The dynamically changing conditions of the security environment increase the demands for the creation of functional security systems. Therefore, current security management and engineering approaches must be applied in this context. In the article, the facts defining and classifying soft targets as one of the important infrastructure systems were presented in the introduction. Subsequently, basic philosophical areas and pillars of security were presented, which were subsequently transformed into certified methodologies by the author's collective workplace. In the conclusion, the methodology was described in detail, which, as it was stated, creates a risk assessment process in the context of the assumed structure of a functional security system. The presented methodology is currently used by the Ministry of Transport of the Czech Republic to assess the risk level in the transferred meaning of the quality and sufficiency of the transport infrastructure soft targets operators security system.

References

Ministry of the Interior of the Czech Republic. (2017). Conception for the soft targets protection for 2017-2020. Prague. Retrieved from https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilu-pro-2017-2020-pdf.aspx

Apeltauer, T., Dufek, Z., Vangeli, B., Rosenkranz, J., Hromada, M., Mrázková, L., Lapková, D., Kotek, L., Ljubymenko, K.(2019) Soft Targets Protection. Prague: Leges, 171 p.

Hromada, M., Frohlich, T.(2021). Methodology for increasing the protection and resilience of selected soft target categories. Zlín: Tomas Bata University in Zlín, 52 p.

Crowe, T. 2013. Crime prevention through environmental design. Elsevier, Butterworth-Heinemann. ISBN 978-0-12-411635-1. https://doi.org/10.1016/C2012-0-03280-2

Hromada, M., Loveček, T., Řehák, D., (2022). Methodology for the implementation of technical measures to increase the railway infrastructure soft target protection, VSB – Technical University of Ostrava, Faculty of Safety Engineering, 52 p.

Hromada, M. Apeltauer, T., Kotkova, D., (2021). Methodology for transport infrastructure objects identification and protection. Brno University of Technology, Faculty of Civil Engineering. 27 p.

Saaty, T.L. (2008). Decision making with the analytic hierarchy proces. International Journal of Services Sciences, Vol. 1, No. 1, pp. 83-98. https://doi.org/10.1504/IJSSCI.2008.017590

Pacinda, (2010) "Network Analysis and the KARS Method," The Science for Population, Protection [online]. 2010 (1), pp. 1-22.