Taylor & Francis
Taylor & Francis Group

Sustainable and Resilient Infrastructure

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tsri20

Increasing the safety and security of strategic railway terminals through environmental and situational aspects

Tomas Lovecek, David Rehak, Martin Hromada, Jiri Pokorny, Ivo Haring & Radoslav Kuffa

To cite this article: Tomas Lovecek, David Rehak, Martin Hromada, Jiri Pokorny, Ivo Haring & Radoslav Kuffa (19 Sep 2024): Increasing the safety and security of strategic railway terminals through environmental and situational aspects, Sustainable and Resilient Infrastructure, DOI: 10.1080/23789689.2024.2403883

To link to this article: https://doi.org/10.1080/23789689.2024.2403883

Published online: 19 Sep 2024.

SUSTAINABLE AND RESILIENT INFRASTRUCTURE
https://doi.org/10.1080/23789689.2024.2403883

Taylor & Francis
Taylor & Francis Group

Increasing the safety and security of strategic railway terminals through environmental and situational aspects

Tomas Lovecek[a], David Rehak[b], Martin Hromada[c], Jiri Pokorny[b], Ivo Haring[d] and Radoslav Kuffa[a]

[a]Faculty of Security Engineering, University of Zilina, Zilina, Slovak Republic; [b]Faculty of Safety Engineering, VSB – Technical University of Ostrava, Ostrava, Czech Republic; [c]Faculty of Applied Informatics, Tomas Bata University in Zlin, Zlin, Czech Republic; [d]Department Safety and Resilience of Technical Systems, Fraunhofer Ernst-Mach-Institut, EMI, Freiburg, Germany

ABSTRACT
Rail transport is a vital sub-sector of critical infrastructure (CI) in public transportation, primarily through high-speed rail for national and international travel. Strategic railway terminals, designed for high-capacity entry/exit of people and cargo, are key elements of CI. However, they are also considered soft targets due to threats like terrorism and criminal activity. Current directives, standards, and procedures are inadequate for protecting these publicly accessible spaces, which are also critical infrastructure elements (CIE). There are no specific security standards for the technical protection of strategic railway or transport terminals. In response, a methodological procedure has been developed to enhance protection levels. This procedure is based on the CPTED (Crime Prevention Through Environmental Design) concept, incorporating international standards for crime and terrorism prevention. It focuses on assessing the environmental and situational security of railway terminals and recommending additional technical measures to address gaps in protection.

ARTICLE HISTORY
Received 25 March 2024
Accepted 9 September 2024

KEYWORDS
Critical infrastructure; railway terminals; technical protection; security measures; environmental aspect; situational aspect

1. Introduction

The growing interdependencies between sectoral infrastructures are the result of an increasingly large cross-border and interconnected network of service provision using a CI (Security Council 2017). All critical sectors in the European Union are currently defined by the European Parliament's Directive on the resilience of critical entities (Directive 2022/2557). In total, there are 11 strategic sectors, including the sub-sector of rail transport, which is determined by various elements of the railway infrastructure. According to Directive of the European Parliament and of the Council establishing a Single European Railway Area (Directive 2012/34), passenger stations are also part of the railway infrastructure.

Passenger railway stations can be characterized as transport structures with branched tracks, allowing trains to be overtaken and crossed. In these stations, contact with passengers, cargo handling of trucks (loading/unloading), transport equipment and others are ensured. Railway stations in major cities and airports, in order to fulfil the required function of multifunctional space, become rail transport terminals integrating different forms of transport (e.g., urban, suburban, international, road, rail, air), commercial activities as well as various entertainment services (CEN-TR 14,383-–7, 2009).

Some railway terminals have a significant impact on the implementation of the state social function, and thus on the quality of population life in terms of the protection of their life and health. This makes these facilities strategic and is designated as railway CIEs (Rehak, Slivkova, Pittner et al., 2020). However, strategic rail terminals are not standard CIEs, as in addition to the attributes of significance and attractiveness, they also exhibit the attributes of soft targets (Forest, 2006) and public crowded places (McIlhatton et al., 2020). Statistics show that they are not only the target of terrorist attacks (GTD, 2019), but also the object of common crime and other anti-social activities (RAILway POLice, 2022). Based on this fact, the current security requirements for the strategic railway terminals protection can be classified into three groups in the context of intentional physical threats.

The first group consists of measures related to the CI protection. These measures are not explicitly defined at the EU level, but the obligation to implement them at the national level arises from the already repealed

CONTACT Tomas Lovecek tomas.lovecek@uniza.sk

Council Directive (Directive 2008/114) and the currently valid Directive of the European Parliament and of the Council (Directive 2022/2557). The second group consists of measures related to the soft targets protection. Soft targets can currently be considered a territorially defined area with a relatively high concentration and number of people and an obvious absence of security measures, with an increased risk of terrorist attacks (Forest, 2006). In this context, current security measures are generally aimed at minimizing the risks of terrorist attacks using a booby-trap explosive system, firearm, or vehicle (2003; Berlin Police, 2021; 2003; 2012; 2007; JRC EC, 2022; Ministry of the Interior, 2016; Swedish Civil Contingencies Agency, 2020).

The third group consists of measures related to the public crowded places protection, sometimes also referred to as public places of mass gathering. This issue was first addressed by the CPTED concept (Jeffery, 1971). In contrast to the soft targets protection, the CPTED concept primarily addresses common forms of crime, such as property, violent or other crime (hooliganism, graffiti, spreading drug addiction, etc.). This group of measures is already specified for specific types of public crowded places, such as shops and offices (2006), petrol stations (2010), schools and educational institutions (2022), public transport facilities (2009), or healthcare facilities (2015).

It follows from the above-presented directives, standards, and procedures that they are not fully applicable to the publicly accessible space protection, which is also an CIE. This is mainly due to the nature of strategic railway terminals and the need to focus on a specific group of intentional physical threats, related vulnerabilities and the resulting security measures. These railway terminals are soft targets in the context of terrorism, but as a public space they are much more often the target of other physical nature threats, such as ordinary crime. For this reason, it can be stated that there are currently no security standards or other procedures aimed specifically at the technical protection of strategic railway (but also other transport) terminals.

This creates research space for the creation of a formalised procedure that would consider all specific aspects of strategic railway terminals. Based on these facts, the aim of the article is to define a methodological procedure for the implementation of security measures to increase the level of protection of strategic railway terminals. This methodological approach will consider both the requirements defined in international standards for the prevention of common crime and terrorism, e.g., 2009 or 2007, as well as current security methods and approaches, e.g., CPTED (Crowe, 2013; Jeffery, 1971).

2. Materials and methods

The content of this part of the article is the definition of the terms soft targets and public crowded places and clarification of the essence of their high vulnerability. In this context, strategic railway terminals are defined and described and attention is paid to their vulnerability. Based on these facts, current approaches to the protection of strategic railway terminals are identified, from the perspective of a CI, soft targets, and public crowded places.

2.1. Vulnerability of soft targets and public crowded places

Soft targets are defined as *'buildings in which large numbers of people gather, such as national monuments, hospitals, schools, sports grounds, hotels, cultural centres, theatres and cinemas, cafes and restaurants, places for work, nightclubs, shopping centres, and transport networks such as metro, trains, buses and others'* (Forest, 2006; Karlos, Larcher, & Solomos, 2018; Kelliher, 2018). Soft targets are also places in front of the actual entry into a hard target that is protected (e.g., airport arrival halls). According to Bennett (2007), a soft target is a person or thing that is relatively unprotected or vulnerable to a terrorist attack. In his work, McEntire (2018) defined soft targets as *'a potential network for terrorist attacks, due to its openness and accessibility to the public.'* According to Hesterman (2019), unlike attacks on hard targets, such as government institutions, military bases, or other symbolic sites for terrorist groups, attacking soft targets can cause fatal consequences on the national psyche and can discredit the government's ability to protect people. A high degree of their effect in the use of chemical or biological weapons is played by tourist, shopping, and recreation centres.

In contrast, public crowded places are generally all places of large number of people concentration (McIlhatton et al., 2020). These are physical places or environments characterized by a high density of people gathered close to each other, often exceeding the typical space capacity. These spaces can range from urban centres, public transportation hubs, stadiums, concert venues, shopping malls to crowded streets and markets.

Soft targets and public crowded places are inherently designed to be open and accessible, which increases their vulnerability. According to the Ministry of Homeland Security (Homeland Security, 2018), soft targets and public crowded places are places with a character allowing the entry and movement of large groups of people with a relatively low level of security and the potential occurrence of physical violence. Soft targets and public crowded places generally represent objects, events/actions and spaces in which a large number of people are concentrated, while they are not at all or only partially protected against terrorist attacks and other violent crimes. While soft targets and public crowded places might seem to express the same thing, it is important to realise that there is no security significance associated with public crowded places (Kubikova, 2017).

2.2. Strategic railway terminals and their vulnerabilities

Railway terminals are high-capacity stations used for the entry/exit of people and cargo to/from the transport process. Existing classifications rely heavily on the 'passenger frequency' indicator, which focuses on traffic-related issues and links performance to local assumptions (Zemp, Stauffacher., Lang et al., 2011). However, this method of classification is insufficient in the vulnerability context, as it does not consider other strategically important factors such as location, accessibility, significance or criticality (Rehak, Slivkova, Pittner et al., 2020). Based on these factors, it is possible to define railway terminals that are strategic for rail transport, which significantly increases their attractiveness in the context of terrorism or common crime. For this reason, such strategic railway terminals are more vulnerable than conventional railway stations.

Terrorism and crime threaten the fundamental principles of any public transport system, i.e., public trust and efficient operation, with significant economic and societal consequences. By its very nature, any aggressive or violent behaviour can have a negative impact on public trust in public transport. This trust can also be undermined by leaving the environment in a deteriorating state (e.g., dirt, poor lighting, graffiti). The international standard 2009 defines three groups of generic crime threats directed against persons and buildings of transport terminals, namely:

- attacks against persons (assault with/without physical violence, sexual assault and theft against persons);
- attacks against institutions, property and the environment (theft, robbery, shooting, graffiti, arson and other forms of vandalism);
- other offences and crimes (unauthorised passage of tracks and turnstiles, street sales, drug use, smoking in unauthorised areas, excessive consumption of alcoholic beverages, begging, etc.).

According to the Basics of Soft Targets Protection Guidelines (Ministry of the Interior, 2016), in the case of transport infrastructure, these are attacks on transport networks and means of transport that can not only affect a large number of people, but can also paralyse transport infrastructure, multiplying their impact on society. However, individual threats differ in the probability of occurrence, consequences, or efficiency, and effectiveness of various forms of security measures (Slivkova, Rehak, Michalcova et al., 2022). Primarily, it is necessary to deal with such attacks that can have fatal consequences on the lives or health of people and property (e.g., terrorist attacks, organized crime).

From 1971 to 2019, a total of more than 1100 attacks on transport infrastructures elements (air transport, road/bus transport, rail transport) were recorded in the world. Of these, a total of 431 attacks were recorded in Europe, representing a 40% share. Of the 431 attacks, 105 (24% share) targeted passenger stations or railway terminals. In 98 cases, it was a suicide attack with an explosive device or an booby-trap explosive system. In 6 cases, it was arson and in one case it was an attack with a cold weapon (e.g., a knife). However, firearm attacks or vehicle attacks, which have recently been often used for other types of soft targets, are not excluded either (GTD, 2022).

Railway terminals, as a public place, can be subject to other forms of crime. For example, from the data on the state of crime at railway stations in the Czech Republic, 2555 crimes were recorded in 2022 (Kubalova, 2023). Figure 1 shows an overview of registered offences and crimes. In 2022, the Czech Republic distinguishes 69 categories of registered acts, with only those that occurred most frequently presented in the figure, the others being included in the other category.

It follows from the above that the risk level is relevant both from the point of view of threats with high consequences and low probability of occurrence (e.g., attack by an explosive device or arson) and from the point of view of threats with low consequences and high probability and frequency of occurrence (e.g., vandalism or theft).

2.3. Current approaches applicable to the protection of strategic railway terminals

The security requirements for strategic railway terminals resulting from existing legislative requirements, technical standards requirements or requirements of other third parties can be divided into three groups according to the attributes of the research subject, i.e., high concentration of people, openness to the public,

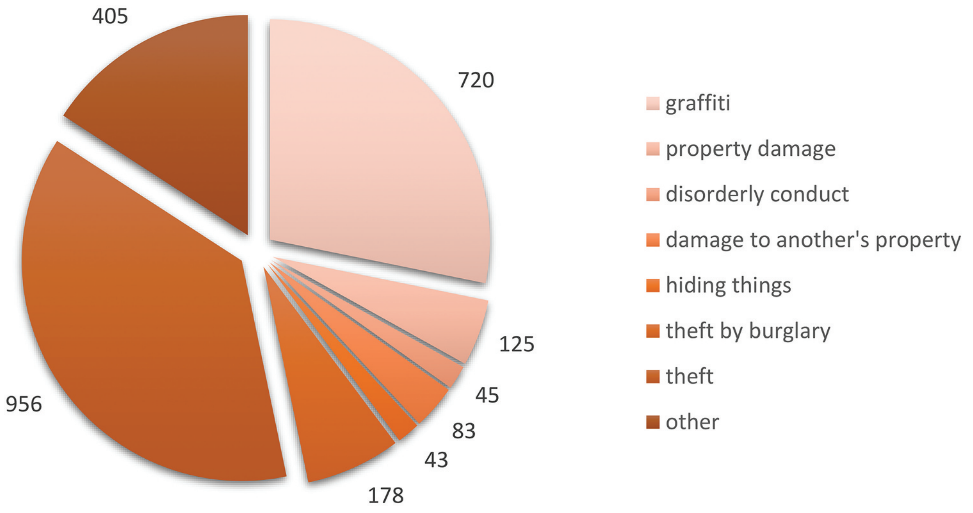


Figure 1. Overview of registered deeds at railway stations in the Czech Republic in 2022 (Kubalova, 2023).

low security level and public service. These three groups perceive strategic railway terminals as:

- critical infrastructure elements;
- soft targets;
- public crowded places.

The need to protect strategic railway terminals in the context of a CI first emerged in 2008 from the now-repealed Council Directive on the identification and designation of European critical infrastructures and on the assessment of the need to improve their protection (2008). However, this document only declared in general the need to improve prevention, protection, preparedness and response to the CI protection in the EU. Specific solutions remained the responsibility of the Member States and their national rules. For example, according to the document The Concept of Critical Infrastructure in the Slovak Republic and Ways of its Protection and Defence (GSK, 2008), the Slovak Republic considers such tools to be technical means of deterring, detecting, verifying, signalling and eliminating intruders (mechanical and electronic), as well as the activities of security services, including the intervention of security forces and armed forces. Similarly, in the Czech Republic, a technical standard focused on the CIEs physical protection has been issued (2013). For the time being, the last important document is the Directive (2022/2557), which, however, again contains only general rules regarding aspects of the resilience of critical entities. It follows from this Directive that '*critical entities should take technical, security and organisational measures that are appropriate and proportionate to the risks they face so as to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident*'.

On the basis of the above, it can be stated that all existing security requirements for the CI protection are rather of a formal nature, they do not specify in more detail the procedures for the CIEs protection and none of them is aimed at the transport terminals protection. The currently implemented security measures related to the CIEs protection fall more into the area of physical protection systems, i.e., mechanical barriers, alarm systems, security forces, and regime measures (Garcia, 2008; Kampova, Lovecek, & Rehak, 2020).

At the turn of the millennium, the Federal Emergency Management Agency (FEMA) began to issue a series of methodologies focused on risk management, which gradually focused on topics such as mitigation of the terrorist attacks consequences on buildings (2003; 2003), protecting the urban environment from terrorist attacks (2007) or protecting educational facilities from terrorist attacks (2012). Within Europe, it is obvious that issues of soft targets protection should be within the competence of the member states but built on the established legal and procedural basis of the EU. The starting point in this direction can be the Action Plan to support the protection of public spaces (European Commission, 2017). This document is considered a fundamental basis for the sharing of knowledge and experience at the national and transnational level. The next logical evolutionary step was the creation of Good Practices to Support the Protection of Public Spaces (European Commission, 2019). Best practices have been organised into four areas, namely assessment and planning, information and training, physical protection and cooperation. Protecting public spaces from terrorist attacks was an important objective of the EU Security Union Strategy (European Commission, 2020b). The focus was on providing stronger physical protection and adequate detection systems without compromising citizens' freedoms. As expected, the public spaces and soft targets protection is also an important priority of the EU Counter Terrorism Agenda (European Commission, 2020a). The Commission has stepped up efforts at EU level to promote security solutions and to integrate security into public spaces (i.e., buildings and infrastructure) from the very beginning of the design and urban planning process. In 2022, the European Commission issued a methodological guideline entitled Protection of public spaces from terrorist attacks (JRC EC, 2022). Despite the fact that the EU has created a framework for the soft targets protection, as in the case of the CI protection, there is no internationally recognized technical standard that would specify procedures for their protection. Admittedly, various framework methodologies for the soft targets protection are published within the Member States (e.g., Berlin Police, 2021; Ministry of the Interior, 2016; Swedish Civil Contingencies Agency, 2020), but none of them are aimed at protecting railway terminals as possible soft targets.

The issue of protecting public spaces from various forms of crime is dealt with in the theory focused on environmental design. The first publication to address this issue was the CPTED concept (Jeffery, 1971). The principle of the CPTED concept is based on the claim that the correct design and effective use of the built environment can lead to a reduction in fear and the crime incidence, to an improvement in the quality of life and increased profitability. Among the most cited contemporary authors is Paul Cozens, who argues that CPTED assumes that with an appropriate design process and effective use of the environment, a reduction in crime and related concerns can be achieved (Cozens & Love, 2015). Despite the fact that the concept of CPTED has been addressed in scientific circles since the 1970s, the first international technical standard dealing with this issue was not published until 2021 (ISO 22341, 2021). This standard provides guidance to organizations to establish essential elements, strategies, and processes for preventing and reducing crime and crime fear in a new or existing built environment. Since 2006, the European standardisation processes have developed technical standards aimed at preventing crime through urban planning and building design. Gradually, standards focused on commercial and administrative premises (CEN/TS 14383-4, 2006), petrol stations (CEN/TR 14383-5, 2010), schools and educational institutions (CEN/TS 14383-6, 2022) and public transport facilities (CEN/TR 14383-7, 2009) began to emerge. Another working group has also developed a standard for the healthcare facilities protection (CEN/TS 16850, 2015). From the service provided point of view, these standards for individual objects have their own specifics (e.g., legislative requirements, potential threats, vulnerabilities, consequences and impacts, cascade effects), so they cannot be directly applied to railway transport terminals.

3. Results

From the analysis presented above, it is clear that the existing security measures for the strategic railway terminals protection are fragmented into several areas. The lack of a coherent approach makes it impossible to take effective and efficient measures that consider all the specific aspects of strategic railway terminals. For this reason, the authors of the article defined a methodological procedure for the security measures implementation to increase the strategic railway terminals protection level (hereinafter referred to as the 'Methodology'). The essence of this methodology is to assess the environmental and situational security aspects of railway terminal and to recommend missing technical measures.

The novelty of the methodology lies primarily in the assessment of the soft targets technical protection level of the railway CI by determining the risk and security level. This is implemented with a direct link to the calculation of the technical protection level using a set of simple criteria to which it is possible to assign clear values. These criteria were developed in accordance with the CPTED concept (Crowe, 2013; Jeffery, 1971) and in accordance with international standards related to the soft targets protection (e.g., FEMA 430, 2007), the public crowded places protection (e.g., CEN/TR 14383-7, 2009) and physical protection systems (e.g., EN 50136-1, 2012). The proposed measures are incorporated into the overall design concept of the building, including in relation to the possible misuse of transport means.

3.1. Security measures catalogue to increase the strategic railway terminals technical protection

The Catalogue for the implementation of technical measures to increase the strategic railway terminals protection (hereinafter referred to as the Catalogue) is the starting point for objectifying the technical protection measures selection. As stated above, the created methodology and the resulting technical measures catalogue of are prepared in accordance with international standards related to the soft targets protection, the public crowded places protection, and physical protection systems. The measures defined in the Catalogue are incorporated into the overall design concept of the given building, including in relation to the possible misuse of transport means. These measures are based on a strategy of natural supervision, control, area maintenance management, and division of areas. The structure of the Catalogue is presented in Figure 2.

The essence of this Catalogue is to define technical measures that increase the strategic railway terminals environment security. These measures are classified into two groups according to their nature, namely technical measures of the environmental aspect of security and technical measures of the situational aspect of security. In both cases, these measures are further classified into internal and external.

In this context, the environmental aspect of security reflects the spatial, layout and design properties of the environment, which are environmental attributes in relation to the security bases of the CPTED concept (Lee, Park, & Jung, 2016). An overview of specific technical measures of the external environmental aspect of security with a focus on the spatial aspect is presented in Table 1.

On the other hand, the situational aspect of security reflects the surveillance, control and maintenance environment properties and is based on situational crime prevention. This claim has been supported by a number of publications (e.g., Mihinjac & Saville, 2019; Reynald & Mihinjac, 2019; Shariati & Guerette, 2017). An overview of specific technical measures of the internal situational aspect of security with a focus on the oversight aspect is presented in Table 2.

The technical measures of the internal situational aspect, with a focus on the surveillance aspect, primarily reflect the standards related to physical protection systems. Specifically, these are standards for Mechanical barriers (CEN/TR 14383-8, 2019), Video surveillance systems (EN 62676-1-1, 2013), Electronic access control systems (EN 60839-11-1, 2013), Alarm transmission systems (EN 50136-1, 2012), and Monitoring and alarm receiving centre (EN 50518, 2019). Technical measures for other environmental and situational aspects of security are defined in the final report of the grant project SECURAIL (Hromada, Lovecek, & Rehak, 2023).

3.2. *Methodological procedure for increasing the strategic railway terminals technical protection level*

In connection with the created Catalogue, it is possible to define a procedure to increase the strategic railway terminals technical protection level. The essence of this methodological procedure is to determine the risk level,

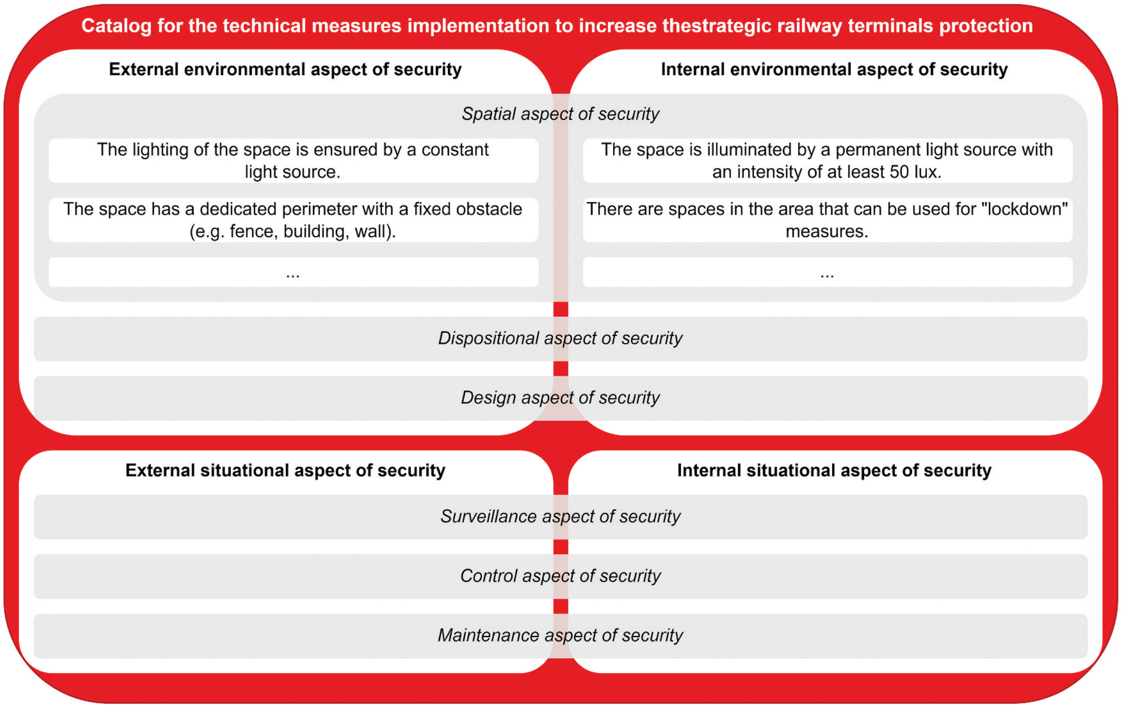

Catalog for the technical measures implementation to increase thestrategic railway terminals protection
External environmental aspect of security
Internal environmental aspect of security
Spatial aspect of security
The lighting of the space is ensured by a constant light source.
The space is illuminated by a permanent light source with an intensity of at least 50 lux.
The space has a dedicated perimeter with a fixed obstacle (e.g. fence, building, wall).
There are spaces in the area that can be used for "lockdown" measures.
...
...
Dispositional aspect of security
Design aspect of security
External situational aspect of security
Internal situational aspect of security
Surveillance aspect of security
Control aspect of security
Maintenance aspect of security

Figure 2. Structure of the catalogue for the implementation of technical measures to increase the strategic railway terminals protection.

Table 1. Technical measures of the external environmental aspect with a focus on the spatial aspect.

Aspect	Technical measures
Spatial aspect of external environmental Aspect	The lighting of the space is provided by a constant light source. The constant light source is in the colour temperature range of 3000 to 4000 K, representing cold white light. The light source is placed at the maximum possible height that the space allows. The space is illuminated by a constant light source with an intensity of at least 50 lux. The area is secured by specially designed protective measures means (fixed, movable or recessed bollards; tyre penetrators; folding barriers; fixed or movable girders or poles allowing entry or passage only to authorised vehicles depending on their dimensions; reinforced concrete blocks; chain or rope barriers; fixed or folding, gates, etc.) preventing the parking of a passenger vehicle at a distance of more than 300 metres. The area is secured by specially designed protective measures means (fixed, movable or recessed bollards; tyre penetrators; folding barriers; fixed or movable girders or poles allowing entry or passage only to authorised vehicles depending on their dimensions; reinforced concrete blocks; chain or rope barriers; fixed or folding, gates, etc.) preventing the parking of a van or light truck at a distance of more than 600 metres. The space is secured by natural protective measures means (meeting a minimum height of 50 cm), designed for the purpose of multi-purpose function (containers with plants, multi-stage curbs, street lighting poles, hydrants, crash barriers, benches, sculptures, fountains, etc.), preventing the parking of a passenger vehicle at a distance of more than 300 meters. The space is secured by natural protective measures means (meeting a minimum height of 50 cm), designed for the purpose of multi-purpose (containers with plants, multi-stage curbs, street lighting poles, hydrants, crash barriers, benches, sculptures, fountains, etc.), preventing the parking of a van or light truck at a distance of more than 600 meters. The space has a dedicated perimeter with a solid obstacle (e.g., fence, building, wall). The space fulfils the basic principle of natural surveillance, which is based on the principle of "see and be seen".

Table 2. Technical measures for the internal situational aspect with a focus on the supervisory aspect.

Aspect	Technical measures
Supervisory aspect of the internal situational aspect	The procedure for managing security incidents (e.g., reaction to criminal and other anti-social activities, finding suspicious luggage) is formalized and practiced with employees. It is a formalized procedure for recording security incidents that have occurred, how they are resolved. The procedure for reporting security incidents by the persons present (via SMS, own applications, leaflets, posters, etc.) is formalized. The procedure for informing the persons present about the security incident (via SMS, own applications, radio, etc.) is formalized. Physical security has formalized regime measures (license, certificate, guidelines for the performance of security, recording of incidents, etc.). Cooperation with selected units of the Integrated Rescue System is formalized. The space is secured by a surveillance (camera) video system with at least level 1 security according to EN 62,676-1-1 (2014). The surveillance (camera) video system has an intelligent video analysis function (motion detection, detection of non-standard behaviour, tracing of people, etc.). The surveillance (camera) video system has AWR (Automatic Weekly Recording), day/night, or IR (Infra Rot) illumination. The area is permanently supervised by its own employee (informant, ticket office employee, dispatcher, technical staff, etc.). Permanent 7/24 surveillance is carried out in the given area by means of physical security (self-protection, private security service, municipal, city or state police, etc.).

to determine the security level, to calculate and evaluate the technical protection level and to define measures to increase the technical protection level. The interconnectedness of the individual phases of this procedure is presented in Figure 3.

In the following part of the article, a detailed description of the individual phases of the methodological procedure is made, including the mathematical apparatus that is necessary for the calculation of environmental and situational aspects and the technical protection level.

3.2.1. Determining the risk level

At the beginning of the procedure, it is necessary to determine the risk level (Phase 1). The essence of this phase is to assess the riskiness of the external and internal environment of the evaluated railway terminal in the context of the layout or division of the space (i.e., the environmental aspect of risk) and in the context of material and procedural deficiencies in the area of supervision, control and maintenance (i.e., the situational aspect of risk).

3.2.1.1. Determination of the environmental aspect of risk. The determination of the environmental aspect of the risk consists in the assessment of the riskiness of the layout or division of the railway terminal area. This assessment is carried out for the exterior and interior areas of the terminal. In both cases, the assessment is

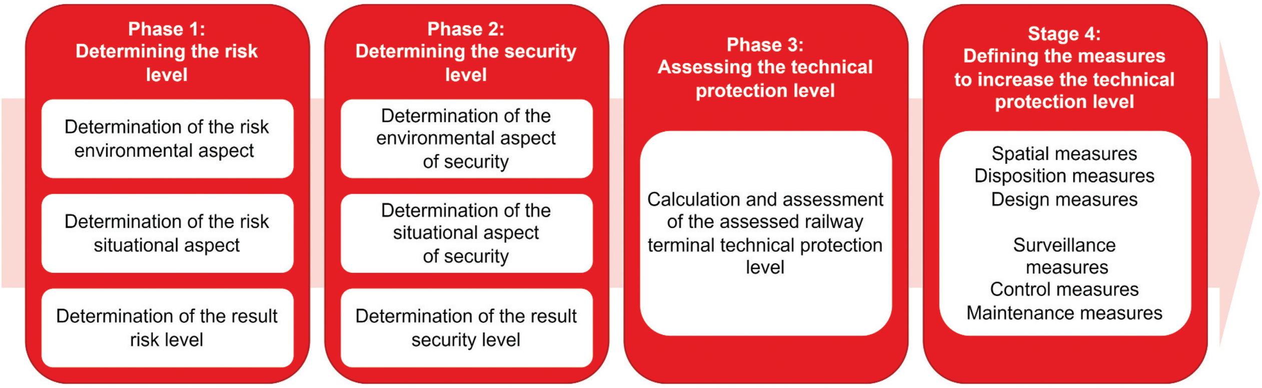

Phase 1:
Determining the risk level
Determination of the risk environmental aspect
Determination of the risk situational aspect
Determination of the result risk level
Phase 2:
Determining the security level
Determination of the environmental aspect of security
Determination of the situational aspect of security
Determination of the result security level
Phase 3:
Assessing the technical protection level
Calculation and assessment of the assessed railway terminal technical protection level
Stage 4:
Defining the measures to increase the technical protection level
Spatial measures
Disposition measures
Design measures
Surveillance measures
Control measures
Maintenance measures

Figure 3. Procedure for establishing, objectifying and enhancing the strategic railway terminals technical protection level.

carried out through several sets of criteria, which are focused on the assessment of the spatial aspect of risk, the dispositional aspect of risk, and the design aspect of risk. These criteria are evaluated by means of individual evaluation sheets. An example of an evaluation sheet for the assessment of the Dispositional aspect of the risk of the external space is presented in Table 3.

Barriers higher than 1.2 meters, which do not allow a natural view of the perimeter of the station space, play a significant role in assessing the Dispositional aspect of the risk of the external space. These are, for example, fences, walls, columns, sheds, storage facilities or advertising banners. An example of good practice of ensuring natural supervision is presented in Figure 4.

Another important factor in assessing the Dispositional aspect of the risk of the external space is the greenery creating a natural barrier. In the case of trees, the lower part of the crown should not be lower than 2 meters above the ground, and the height of scrub should not be higher than 0.7 meters. An example of good practice in green care in accordance with the CPTED concept is presented in Figure 5.

In the context of assessing the Dispositional aspect of the risk of the external space, it is also appropriate to mention the importance of the space organization from the point of view of the visitor planned activity, e.g., by creating a naturally controlled entrance to the object, the so-called ‘funnel’. An example of the difference between an uncontrolled and a naturally controlled entrance to an object is presented in Figure 6.

Table 3. Assessment sheet for the assessment of the dispositional aspect of the risk of the external space.

Evaluated space	Evaluation criterion	Status of compliance with the criterion (Yes/No)
Railway terminal building	Barriers higher than 1.2 meters (shelters, fences, walls, etc.) forming the perimeter of the station area are opaque and do not allow natural surveillance.	
	The greenery forming the natural barrier has a minimum crown height of less than 2 metres, or the height of the shrub stand is higher than 0.7 metres.	
	The space is disorganized from the point of view of the visitor’s planned activity, e.g., by creating a “funnel”.	
	The layout of the space does not allow for a reduction in the speed parameter of an approaching vehicle.	
	The layout of the space does not allow it to prevent a frontal collision with a vehicle.	
Parking spaces	Barriers in the space higher than 1.2 meters (walls, columns, advertising banners, etc.) creating the layout of the space are opaque and do not allow natural supervision.	
	The greenery forming the natural barrier has a minimum crown height of less than 2 metres, or the height of the shrub stand is higher than 0.7 metres.	
	The space is disorganized from the point of view of the visitor’s planned activity, e.g., by creating a “funnel”.	
	The layout of the space does not allow for a reduction in the speed parameter of an approaching vehicle.	
	The layout of the space does not allow it to prevent a frontal collision with a vehicle.	
Underpasses/ Overpasses/ Corridors	Barriers in the space higher than 1.2 meters (walls, columns, stalls, storage objects, advertising banners, etc.) creating the layout of the space are opaque and do not allow natural supervision.	
	The greenery forming the natural barrier has a minimum crown height of less than 2 metres, or the height of the shrub stand is higher than 0.7 metres.	
	The layout of the space does not allow for a reduction in the speed parameter of an approaching vehicle.	
	The layout of the space does not allow it to prevent a frontal collision with a vehicle.	

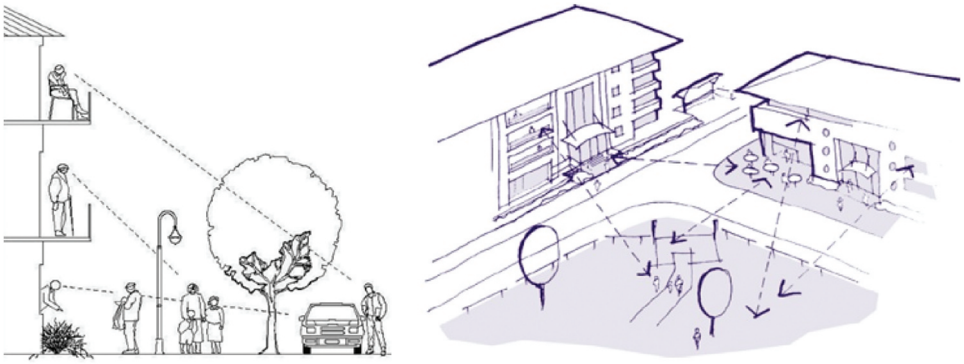


Figure 4. Example of good practice in ensuring natural supervision (Livingstone Shire Council, 2018).

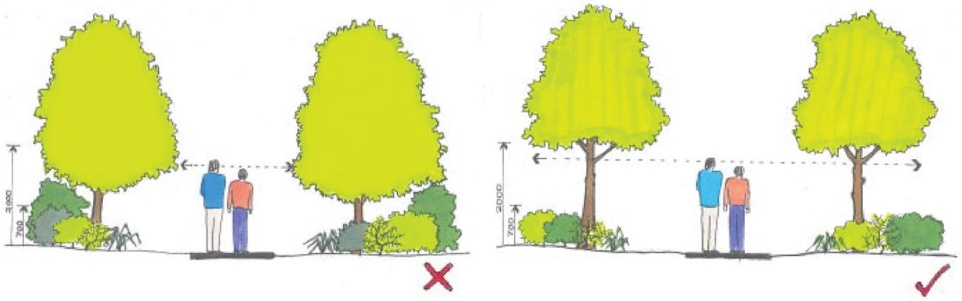


Figure 5. Example of good practice in green management in accordance with the CPTED concept (Canterbury Safety Working Party, 2004).

When assessing the Dispositional aspect of the risk of the external space through the Evaluation sheet (see Table 3), it is necessary to proceed as follows. If the criterion is met, i.e., the answer is YES, the value is assigned to 0, if the answer is NO, the value is 1. Due to the fact that the evaluated objects may differ in practice, the evaluator selects only the relevant ones from the criteria catalogue. The value of a given variable is then determined by the sum of all NO answers, which is divided by the number of all criteria used. Comprehensive assessment sheets for the assessment of all environmental aspects of risk are available in the final report of the grant project SECURAIL (Hromada, Lovecek, & Rehak, 2023).

Subsequently, the environmental aspect of risk is determined separately for the external and internal environment of the railway terminal. The calculation of the external environmental aspect of risk is given by the Formula (1):

$$ER_{ex} = \sum_{i=1}^{n} EARex_i \, w(ex)_i \tag{1}$$

where ER_{ex} = external environmental aspect of risk [0–1]; $EARex_i$ = i-th partial external environmental aspect of risk [0–1]; $w(ex)_i$ = i-th normalized weight of the i-th partial external environmental aspect of risk [0–1]; n = number of partial external environmental aspects of risk.

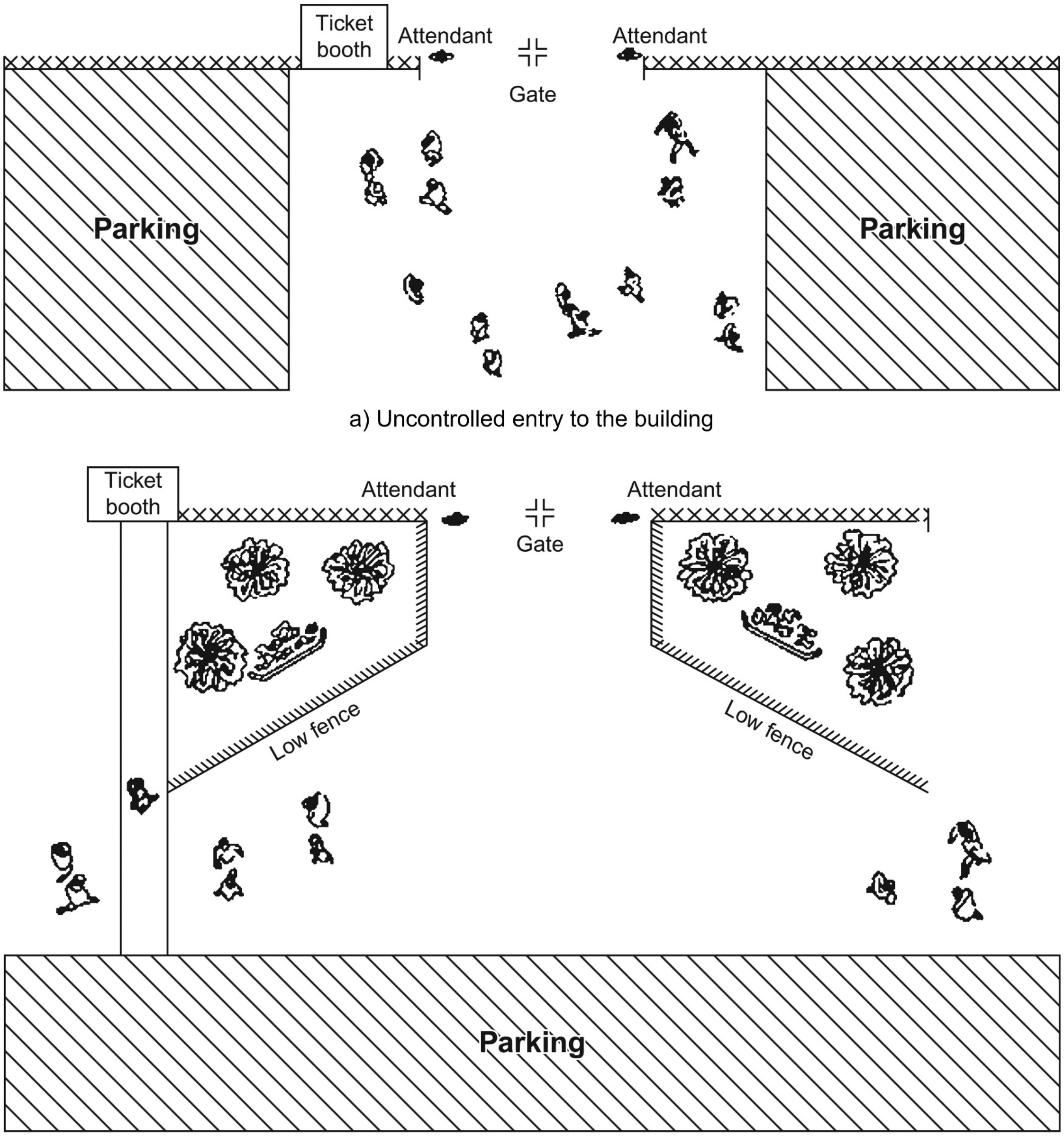
Specific partial external environmental aspects of risk are the Spatial aspect of risk, the Dispositional aspect of risk, and the Design aspect of risk.

The calculation of the internal environmental aspect of risk is given by the Formula (2):

$$ER_{in} = \sum_{i=1}^{n} EARin_i \, w(in)_i \tag{2}$$

where ER_{in} = internal environmental aspect of risk [0–1]; $EARin_i$ = i-th partial internal environmental aspect of risk [0–1]; $w(in)_i$ = i-th normalized weight of the i-th partial internal environmental aspect of risk [0–1]; n = number of partial internal environmental aspects of risk. Specific partial internal environmental aspects of riskiness are, similarly to the external environment, the Spatial aspect of risk, the Dispositional aspect of risk, and the Design aspect of risk.

The determination of weighted coefficients and their subsequent normalization were carried out on the basis of expert evaluation of expected future users using the Analytic Hierarchy Process (Saaty, 2008), which is based on a pairwise comparison of variants supporting the



a) Uncontrolled entry to the building

b) Naturally controlled entry to the building

Figure 6. Example of good practice of uncontrolled and naturally controlled building entry (Crowe, 2013).

evaluation of criteria hierarchy. Specific values of standardized scales for partial environmental aspects of the risk of the external and internal environment of railway terminals are presented in Table 4.

The results of the normalization of the weights show that in the environmental context, the most important evaluation criteria are found in spatial and dispositional aspects. Their significance reaches the same level, both in the external and internal environment. On the other hand, the design aspect in both cases reaches a slightly lower significance level, which is mainly due to the composition of the evaluation criteria, which in most cases require technically demanding construction modifications.

Table 4. Values of standardised weights for partial environmental aspects of risk.

	Spatial Aspect of Risk	Dispositional Aspect of Risk	Design Aspect of Risk	Σ
$w(ex)_i$	0.35	0.35	0.30	1.00
$w(in)_i$	0.35	0.35	0.30	1.00

3.2.1.2. Determination of the situational aspect of risk. The determination of the situational aspect of risk consists of a material and procedural deficiencies assessment in the area of supervision, control and maintenance. This assessment, similarly to the environmental aspect, is carried out for the exterior and interior areas of the terminal, but in this case with an emphasis on the supervisory aspect of risk, assessment the control aspect of riskiness and the maintenance aspect of risk. In this case, too, the criteria are evaluated through individual evaluation sheets, which focus on the external and internal situational aspects assessment. These aspects are assessed specifically for the following spaces:

- the railway terminal building (i.e., entrance hall, waiting rooms, staircases, elevators, commercial areas, non-public areas);
- platforms;
- parking spaces;
- related underpasses, overpasses and corridors.

Comprehensive assessment sheets for the assessment of all situational aspects of risk are available in the final report of the grant project SECURAIL (Hromada, Lovecek, & Rehak, 2023). The principle of evaluation of these sheets is the same as in the case of environmental aspects of risk. If the criterion is met, i.e., the answer is YES, the value is assigned to 0, if the answer is NO, the value is 1. The value of a given variable is then determined by the sum of all NO answers, which is divided by the number of all criteria used.

The situational aspect of risk is then determined separately for the external and internal environment of the railway terminal. The calculation of the external situational aspect of risk is given by the Formula (3):

$$SR_{ex} = \sum_{i=1}^{n} SARex_i \, x(ex)_i \tag{3}$$

where SR_{ex} = external situational aspect of risk [0–1]; $SARex_i$ = i-th partial external situational aspect of risk [0–1]; $x(ex)_i$ = i-th normalized weight of the i-th partial external situational aspect of risk [0–1]; n = number of partial external situational aspects of risk. Specific partial external situational aspects of risk are the Surveillance aspect of risk, the Control aspect of risk, and the Maintenance aspect of risk.

The calculation of the internal situational aspect of the risk is given by the Formula (4):

$$SR_{in} = \sum_{i=1}^{n} SARin_i \, x(in)_i \tag{4}$$

where SR_{in} = internal situational aspect of risk [0–1]; [0–1]; $SARin_i$ = i-th partial internal situational aspect of risk [0–1]; $x(in)_i$ = i-th normalized weight of the i-th partial internal situational aspect of risk [0–1]; n = number of partial internal situational aspects of risk. As in the case of the external environment, the specific partial internal situational aspects of risk are the Surveillance aspect of risk, the Control aspect of risk, and the Maintenance aspect of risk.

The determination of weighted coefficients and their subsequent normalization were again carried out on the basis of expert evaluation of expected future users using the Analytic Hierarchy Process (Saaty, 2008). Specific values of standardized weights for partial situational aspects of the risk of the external and internal environment of railway terminals are presented in Table 5.

The results of the normalization of the weights show that in the situational context, the most important evaluation criteria are found in the supervisory and maintenance aspects. Their significance reaches the same level, both in the external and internal environment. On the other hand, the control aspect reaches half the significance level in both cases, which is mainly due to the composition of the evaluation criteria, which in most cases are uncontrollable.

3.2.1.3. Determination of the resulting risk level.

At the end of the first phase of the procedure, it is necessary to determine the railway terminal resulting risk level. This level is the result of an assessment of the sub-levels of environmental and situational aspects of risk. This resulting risk level is calculated according to the Formula (5):

$$R = \frac{1}{n} \sum_{i=1}^{n} DR_i \tag{5}$$

where R = risk level of the railway terminal [0–1]; DR_i = i-th determinant of risk level [0–1]; n = number of determinants assessed. The determinants in this case are the External environmental aspect of risk (ER_{ex}), the Internal environmental aspect of risk (ER_{in}), the External situational aspect of risk (SR_{ex}) and the Internal situational aspect of risk (SR_{in}). The resulting risk level of the railway terminal (R) will then be used to assess the technical protection level (see Phase 3).

3.2.2. Determining the security level

In the second stage of the procedure, it is necessary to determine the security level (Phase 2). The essence of this phase is the assessment of positive external and internal aspects of environmental and situational security. Specifically, these are technical measures increasing the security of the environment, such as a suitable layout

Table 5. Values of standardised weights for partial situational aspects of risk.

	Supervisory Aspect of Risk	Control Aspect of Risk	Maintenance Aspect of Risk	Σ
$x(ex)_i$	0.4	0.2	0.4	1.00
$x(in)_i$	0.4	0.2	0.4	1.00

of selected elements of the environment, appropriate design aspects of the environment or the use of external and internal surveillance and control systems.

3.2.2.1. Determination of the environmental aspect of security.

The determination of the environmental aspect of security is carried out in an analogous way as in the case of the environmental aspect of risk. Attention is again paid to the external and internal layout or division of the railway terminal area, but this time with regard to the security of these areas. This assessment is also carried out through evaluation sheets (Hromada, Lovecek, & Rehak, 2023), which focus on assessing the spatial aspect of security, the dispositional aspect of security, and the design aspect of security.

In this context, however, it is necessary to draw attention to the fact that the evaluation of the security level criteria is the opposite of that used in the case of risk. If the criterion is met, i.e., the answer is YES, the value 1 is assigned to the criterion, if the answer is NO, the value is 0. Due to the fact that the evaluated objects may differ in practice, the evaluator selects only the relevant ones from the catalogue of criteria. The value of a given variable is then determined by the sum of all YES answers, which is divided by the number of all criteria used.

Subsequently, the environmental aspect of security is determined separately for the external and internal environment of the railway terminal. The calculation of the external environmental aspect of security is given by the Formula (6):

$$ES_{ex} = \sum_{i=1}^{n} EASex_i y(ex)_i \qquad (6)$$

where ES_{ex} = external environmental aspect of security [0–1]; $EASex_i$ = i-th partial external environmental aspect of security [0–1]; $y(ex)_i$ = i-th normalized weight of the i-th partial external environmental aspect of security [0–1]; n = number of partial external environmental aspects of security. Specific partial external environmental aspects of security are the Spatial aspect of security, the Dispositional aspect of security, and the Design aspect of security.

The calculation of the internal environmental aspect of security is given by the Formula (7):

$$ES_{in} = \sum_{i=1}^{n} EASin_i\, y(in)_i \qquad (7)$$

where ES_{in} = internal environmental aspect of security [0–1]; $EASin_i$ = i-th partial internal environmental aspect of security [0–1]; $y(in)_i$ = i-th normalized weight of the i-th partial internal environmental aspect of security [0–1]; n = number of partial internal environmental aspects of security. Specific partial internal environmental aspects of security are, similarly to the external environment, the Spatial aspect of security, the Dispositional aspect of security, and the Design aspect of security.

The determination of weighted coefficients and their subsequent normalization were again carried out on the basis of expert evaluation of expected future users using the Analytic Hierarchy Process (Saaty, 2008). Specific values of standardized scales for partial environmental aspects of external and internal environmental security of railway terminals are presented in Table 6.

3.2.2.2. Determination of the situational aspect of security.

In this case, the determination of the situational aspect of security is carried out in an analogous way as in the case of the situational aspect of risk. Again, attention is paid to the areas of supervision, inspection and maintenance, but this time from the security point of view. Even in this case, the criteria are evaluated through individual evaluation sheets (Hromada, Lovecek, & Rehak, 2023), which focus on the assessment of the external and internal situational aspects. The calculation of the external situational aspect of security is given by the Formula (8):

$$SS_{ex} = \sum_{i=1}^{n} SASex_i z(ex)_i \qquad (8)$$

where SS_{ex} = external situational aspect of security [0–1]; $SASex_i$ = i-th partial external situational aspect of security [0–1]; $z(ex)_i$= i-th normalized weight of the i-th partial external situational aspect of security [0–1]; n = number of partial external situational aspects of security. Specific partial external situational aspects of security are the Surveillance aspect of security, the Control aspect of security, and the Maintenance aspect of security.

The calculation of the internal situational aspect of security is given by the Formula (9):

$$SS_{in} = \sum_{i=1}^{n} SASin_i z(in)_i \qquad (9)$$

where SS_{in} = internal situational aspect of security [0–1]; $SASin_i$ = i-th partial internal situational aspect of security [0–1]; $z(in)_i$= i-th normalized weight of the i-th partial internal situational aspect of security [0–1];

Table 6. Values of standard weights for partial environmental aspects of security.

	Spatial Aspect of Risk	Dispositional Aspect of Risk	Design Aspect of Risk	Σ
$y(ex)_i$	0.35	0.35	0.30	1.00
$y(in)_i$	0.35	0.35	0.30	1.00

n = number of partial internal situational aspects of security. Specific partial internal situational aspects of security are, similarly to the external environment, the Surveillance aspect of security, the Control aspect of security, and the Maintenance aspect of security.

The determination of weighted coefficients and their subsequent normalization were again carried out on the basis of expert evaluation of expected future users using the Analytic Hierarchy Process (Saaty, 2008). Specific values of standardized scales for partial situational aspects of security of the external and internal environment of railway terminals are presented in Table 7.

3.2.2.3. Determination of the resulting security level.

At the end of the second phase of the procedure, it is necessary to determine the railway terminal final security level. This level is the result of an assessment of the sub-levels of environmental and situational aspects of security. This resulting security level is calculated according to the Formula (10):

$$S = \frac{1}{n}\sum_{i=1}^{n} DS_i \tag{10}$$

where S = security level of the railway terminal [0–1]; DS_i = i-th determinant of security level [0–1]; n = number of determinants assessed. The determinants in this case are the External environmental aspect of security (ES_{ex}), the Internal environmental aspect of security (ES_{in}), the External situational aspect of security (SS_{ex}) and the Internal situational aspect of security (SS_{in}). The resulting security level of the railway terminal (S) will then be used to assess the technical protection level (see Phase 3).

Table 7. Values of standardised weights for partial situational aspects of security.

	Supervisory Aspect of Risk	Control Aspect of Risk	Maintenance Aspect of Risk	Σ
$z(ex)_i$	0.4	0.2	0.4	1.00
$z(in)_i$	0.4	0.2	0.4	1.00

3.2.3. Assessing the technical protection level

The essence of the third phase of the procedure is the calculation and evaluation of the railway terminal technical protection level (Phase 3). The technical protection level is the result of a comprehensive assessment of the environmental and situational aspects of risk and security. This level is calculated according to the Formula (11):

$$TP = \frac{1}{n}\sum_{i=1}^{n} DTP_i \tag{11}$$

where TP = railway terminal technical protection level [0–1]; DTP_i = i-th determinant of technical protection level [0–1]; n = number of determinants assessed. In this case, the determinants are the Risk level of the railway terminal (R) and the Security level of the railway terminal (S). The resulting railway terminal technical protection level (TP) must then be categorized according to the scale shown in Figure 7.

The categorization of technical protection levels is philosophically based on the Failure Mode and Effects Analysis method (2006) in relation to the determination of the Risk Priority Number (ISO 31,010, 2019). The essence is to define alternative solutions for meeting the criteria of the risk aspect and the security aspect:

- when all aspects of risk are minimised and all aspects of security are maximised, the technical protection level reaches 100%;
- where all aspects of risk are minimised and no aspect of security is maximised or no aspect of risk is minimised and all aspects of security are maximised, the technical protection level shall be 50%;
- where at least half of the aspects of risk are minimised and no aspect of security is maximised or no aspect of risk is minimised and at least half of the aspects of security are maximised, the technical protection level shall be 25%;

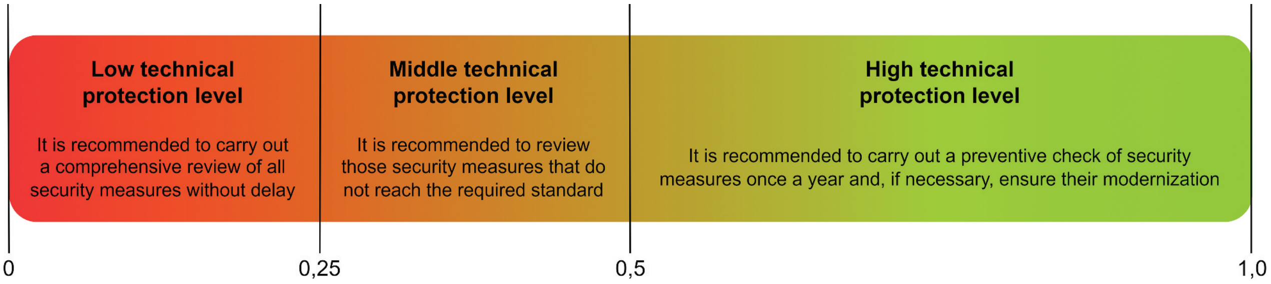

Low technical protection level
It is recommended to carry out a comprehensive review of all security measures without delay
Middle technical protection level
It is recommended to review those security measures that do not reach the required standard
High technical protection level
It is recommended to carry out a preventive check of security measures once a year and, if necessary, ensure their modernization
0
0,25
0,5
1,0

Figure 7. Categorization of the railway terminal technical protection levels.

- in the case that no aspect of risk is minimised or any aspect of security is maximised, the technical protection level of is 0%.

Subsequently, the values set in this way were consulted and approved by the application guarantor, i.e., Ministry of Transport of the Czech Republic, and tested in practice at selected strategic railway terminals.

3.2.4. Defining the measures to increase the technical protection level

The last stage of the procedure is the definition of measures to increase the technical protection level (Phase 4). The initial step of this phase of the procedure is the railway terminal technical protection categorization to the appropriate level. This is because measures are implemented to a different extent for each level.

3.2.4.1. High technical protection level. If a railway terminal achieves a technical protection high level, no specific measures need to be implemented. In this case, it is recommended to carry out a preventive check of the existing security measures once a year and, if necessary, to ensure that they are modernised. Preventive control should be carried out through the procedure described above to increase the strategic railway terminals technical protection level.

3.2.4.2. Middle technical protection level. If a railway terminal achieves a middle technical protection level, it is recommended to revise those security measures that do not meet the required standard. The essence of this revision is to identify weaknesses in the spatial, layout and design arrangement of the railway terminal (i.e., environmental aspects) and in the area of supervision, control and maintenance (i.e., situational aspects). This identification should be carried out in both risk and security areas:

- in the area of risk, all aspects for which the YES criterion has been registered should be identified;
- in the area of security, all aspects for which the NO criterion has been registered should be identified.

On the basis of the deficiencies identified in this way, it is possible to define measures to increase the technical protection level. These measures should be defined using the Catalogue for the technical measures implementation to increase the strategic railway terminals protection (see Figure 2).

3.2.4.3. Low technical protection level. If a railway terminal achieves a low technical protection level, it is recommended to carry out a comprehensive review of all existing security measures without delay. Again, attention should be paid to both environmental and situational aspects, both in terms of risk and security. A reassessment of the technical protection level should be carried out once the revision of the security measures has been completed.

4. Results of the application of the methodological procedure in practice

The created methodological procedure has already been successfully applied at several railway terminals in the Czech Republic and Slovakia. The results achieved from the assessment of the technical protection level were subsequently consulted with the relevant critical entities and with the relevant Ministries of Transport. The following is a presentation of the results of one of these assessments. However, as this is sensitive information, the name and location of the selected railway terminal are anonymized.

To present the results of the practical application of the methodological procedure, a medium-sized railway terminal was chosen, which, however, is considered strategic due to its location within the railway network. Within this terminal, the following buildings/areas were assessed: Railway station building, Entrance hall, Outdoor parking areas, Commercially used areas, Non-public areas of the station, Platforms, Underpasses, Waiting rooms, and elevators. The assessment itself was carried out using eight assessment sheets, which assessed the environmental and situational aspects of the risk and security of these buildings/premises.

4.1. Phase 1: determining the risk level

The determination of the level of risk of the external and internal environment of the assessed railway terminal was carried out using the following assessment sheets:

- Assessment sheet 1: Determination of the external environmental aspect of risk;
- Assessment sheet 2: Determination of the internal environmental aspect of risk;
- Assessment sheet 3: Determination of the external situational aspect of risk;

- Assessment sheet 4: Determination of the internal situational aspect of risk.

Within these sheets, the individual relevant criteria were assessed (see, for example, Table 3), the results of which are presented in Tables 8–11.

Based on the results of the individual criteria assessment, it is possible to calculate the external environmental aspect of risk (see Formula 1), the internal environmental aspect of risk (see Formula 2), the external situational aspect of risk (see Formula 3) and the internal situational aspect of risk (see Formula 4). The results of the calculations are presented in Tables 12–15.

The last step of the first phase is to determine the resulting risk level (see Formula 5). The result of the calculations is presented in Table 16.

Table 8. Results of the selected railway terminal external environmental risk criteria assessment.

Aspects assessed	Number of criteria with NO answer	Number of all evaluated criteria	$EARex_i$
Spatial aspect of risk	8	19	0.42
Dispositional aspect of risk	10	12	0.83
Design Aspect of Risk	0	6	0

The value of a given aspect is determined by the number of all criteria with a NO answer, which is divided by the number of all criteria assessed.

Table 9. Results of the selected railway terminal internal environmental criteria of the risk assessment.

Aspects assessed	Number of criteria with NO answer	Number of all evaluated criteria	$EARin_i$
Spatial aspect of risk	18	20	0.90
Dispositional aspect of risk	8	9	0.89
Design Aspect of Risk	2	15	0.13

The value of a given aspect is determined by the number of all criteria with a NO answer, which is divided by the number of all criteria assessed.

Table 10. Results of the selected railway terminal external situational aspect criteria of the risk assessment.

Aspects assessed	Number of criteria with NO answer	Number of all evaluated criteria	$SARex_i$
Supervisory aspect of risk	4	4	1
Control aspect of risk	5	15	0.33
Maintenance aspect of risk	12	12	1

The value of a given aspect is determined by the number of all criteria with a NO answer, which is divided by the number of all criteria assessed.

Table 11. Results of the selected railway terminal internal situational aspect criteria of the risk assessment.

Aspects assessed	Number of criteria with NO answer	Number of all evaluated criteria	$SARin_i$
Supervisory aspect of risk	7	8	0.88
Control aspect of risk	8	22	0.36
Maintenance aspect of risk	18	18	1

The value of a given aspect is determined by the number of all criteria with a NO answer, which is divided by the number of all criteria assessed.

Table 12. Calculation of the selected railway terminal external environmental aspect of the risk.

Aspects assessed	$EARex_i$	$w(ex)_i$	ER_{ex}
Spatial aspect of risk	0.42	0.35	0.44
Dispositional aspect of risk	0.83	0.35	
Design Aspect of Risk	0	0.3	

Table 13. Calculation of the selected railway terminal internal environmental aspect of the risk.

Aspects assessed	$EARin_i$	$w(in)_i$	ER_{in}
Spatial aspect of risk	0.90	0.35	0.67
Dispositional aspect of risk	0.89	0.35	
Design Aspect of Risk	0.13	0.3	

Table 14. Calculation of the selected railway terminal external situational aspect of the risk.

Aspects assessed	$SARex_i$	$x(ex)_i$	SR_{ex}
Supervisory aspect of risk	1	0.4	0.87
Control aspect of risk	0.33	0.2	
Maintenance aspect of risk	1	0.4	

Table 15. Calculation of the selected railway terminal internal situational aspect of the risk.

Aspects assessed	$SARin_i$	$x(in)_i$	SR_{in}
Supervisory aspect of risk	0.88	0.4	0.82
Control aspect of risk	0.36	0.2	
Maintenance aspect of risk	1	0.4	

Table 16. Determination of the selected railway terminal resulting risk level.

ER_{ex}	ER_{in}	SR_{ex}	SR_{in}	R
0.44	0.67	0.87	0.82	0.7

The resulting Rail Terminal R risk level will then be used to assess the technical protection level (see Phase 3).

4.2. Phase 2: determining the security level

The determination of the security level of the external and internal environment of the assessed railway terminal was carried out using the following assessment sheets:

- Assessment Sheet 5: Determination of the external environmental aspect of security;
- Assessment Sheet 6: Determination of the internal environmental aspect of security;
- Assessment Sheet 7: Determining the external situational aspect of security;
- Assessment Sheet 8: Determination of the internal situational aspect of security.

Within these sheets, the individual relevant criteria were gradually assessed, the results of which are presented in Tables 17–20.

Based on the results of each criterion assessment, it is possible to calculate the external environmental aspect of security (see Formula 6), the internal environmental aspect of security (see Formula 7), the external situational aspect of security (see Formula 8) and the internal situational aspect of security (see Formula 9). The results of the calculations are presented in Tables 21–24.

The last step of the first stage is to determine the resulting security level (see Formula 10). The result of the calculations is presented in Table 25.

Table 17. Results of the selected railway terminal external environmental aspect criteria of the security assessment.

Aspects assessed	Number of criteria answered YES	Number of all evaluated criteria	$EASex_i$
Spatial aspect of risk	15	20	0.75
Dispositional aspect of risk	6	14	0.43
Design Aspect of Risk	0	4	0

The value of a given aspect is determined by the number of all criteria with the answer YES, which is divided by the number of all assessed criteria.

Table 18. Results of the selected railway terminal internal environmental aspects criteria of the security assessment.

Aspects assessed	Number of criteria answered YES	Number of all evaluated criteria	$EASin_i$
Spatial aspect of risk	36	37	0.97
Dispositional aspect of risk	18	26	0.69
Design Aspect of Risk	0	2	0

The value of a given aspect is determined by the number of all criteria with the answer YES, which is divided by the number of all assessed criteria.

Table 19. Results of the selected railway terminal external situational aspect criteria of the security assessment.

Aspects assessed	Number of criteria answered YES	Number of all evaluated criteria	$SASex_i$
Supervisory aspect of risk	6	21	0.29
Control aspect of risk	1	8	0.13
Maintenance aspect of risk	12	12	1

The value of a given aspect is determined by the number of all criteria with the answer YES, which is divided by the number of all assessed criteria.

Table 20. Results of the selected railway terminal internal situational aspect criteria of the security assessment.

Aspects assessed	Number of criteria answered YES	Number of all evaluated criteria	$SASin_i$
Supervisory aspect of risk	15	54	0.28
Control aspect of risk	6	23	0.26
Maintenance aspect of risk	15	15	1

The value of a given aspect is determined by the number of all criteria with the answer YES, which is divided by the number of all assessed criteria.

Table 21. Calculation of the selected railway terminal external environmental aspect of the security.

Aspects assessed	$EASex_i$	$y(ex)_i$	ES_{ex}
Spatial aspect of risk	0.75	0.35	0.41
Dispositional aspect of risk	0.43	0.35	
Design Aspect of Risk	0	0.3	

Table 22. Calculation of the selected railway terminal internal environmental aspect of the security.

Aspects assessed	$EASin_i$	$y(in)_i$	ES_{in}
Spatial aspect of risk	0.97	0.35	0.58
Dispositional aspect of risk	0.69	0.35	
Design Aspect of Risk	0	0.3	

Table 23. Calculation of the selected railway terminal external situational aspect of the security.

Aspects assessed	$SASex_i$	$z(ex)_i$	SS_{ex}
Supervisory aspect of risk	0.29	0.4	0.54
Control aspect of risk	0.13	0.2	
Maintenance aspect of risk	1	0.4	

Table 24. Calculation of the selected railway terminal internal situational aspect of the security.

Aspects assessed	$SASin_i$	$z(in)_i$	SS_{in}
Supervisory aspect of risk	0.28	0.4	0.56
Control aspect of risk	0.26	0.2	
Maintenance aspect of risk	1	0.4	

Table 25. Determination of the selected railway terminal resulting security level.

ES_{ex}	ES_{in}	SS_{ex}	SS_{in}	S
0.41	0.58	0.54	0.56	0.52

Table 26. Assessment of the selected railway terminal technical protection level.

R	S	TP
0.7	0.52	0.61

The resulting Terminal S security level will then be used to assess the technical protection level (see Phase 3).

4.3. Phase 3: assessing the technical protection level

The assessment of the railway terminal technical protection level was carried out by calculation according to the Formula (11). The result of the calculations is presented in Table 26.

The resulting technical protection level must then be categorized according to the scale shown in Figure 7. In this case, it is clear that the selected railway terminal technical protection reaches a high level. In such a case, it is recommended to carry out a preventive check of the security measures once a year and, if necessary, to ensure that they are modernized.

4.4. Phase 4: defining the measures to increase the technical protection level

The essence of defining measures to increase the level of technical protection of a railway terminal is:

- identification of risk aspects that should be minimised;
- identification of aspects of security that should be maximised (strengthened).

ZIn this case, 13 environmental aspects of risk, 7 situational aspects of risk, 10 environmental aspects of security and 18 situational aspects of security were identified. For a clearer understanding, the recommended measures to strengthen the environmental aspects of security are presented below:

(1) The external area of the railway station building should be secured by specially designed protective measures (fixed bollards, movable or recessed; tyre penetrators; folding barriers; fixed or movable girders or poles allowing entry or passage only to authorised vehicles, depending on their dimensions; reinforced concrete blocks; chain or rope barriers; fixed or folding, gates, etc.) to prevent the parking of a passenger vehicle at a distance of more than 300 metres and a light goods vehicle at a distance of more than 600 metres.

(2) The external area of the railway station building should be secured by natural protective measures means (meeting a minimum height of 50 cm) designed for the purpose of a multipurpose function (containers with plants, multistage curbs, street light poles, hydrants, crash barriers, benches, sculptures, fountains, etc.), to prevent the parking of a passenger vehicle at a distance of more than 300 metres and a light lorry at a distance of more than 600 metres.

(3) The external area of the railway station building should be implemented by special landscaping means (embankments, ditches, water areas, etc.) preventing the parking of a passenger vehicle at a distance of more than 300 metres and a light freight vehicle at a distance of more than 600 metres.

(4) Parking spaces should have a dedicated perimeter with a solid barrier (e.g., fence, building, wall).

(5) The building structure of the railway station building and entrance hall should be modified with new explosion protection materials (aluminium foam, durable coatings, carbon plate, fiber-reinforced polymers, polymer sandwich composite, etc.).

(6) The openings of the railway station building and the entrance hall should have increased passive resistance according to 2021 (minimum security class RC2) or 1999 (minimum security class P5A).

(7) All elements intended for resting in the outdoor and indoor environment should be structurally designed in such a way that they do not allow for permanent dwelling (e.g., sleeping).

(8) The interior of the railway station building and the entrance hall, as well as underpasses and overpasses, should have mirrors installed to allow persons to see beyond blind corners and sharp bends.

(9) Passenger information boards with transport routes, times and basic navigation should be clearly displayed in all areas of the railway terminal.

(10) Parking areas should be equipped with information boards with traffic routes, times, and basic navigation visible even in the evening.

5. Conclusion

The analysis of the current situation shows that the current directives, standards, and procedures are not fully applicable or sufficient to protect the publicly accessible space protection, which is also a CIE. For this reason, there is currently a lack of security standards or other procedures aimed specifically at the technical protection of strategic railway (but also other transport) terminals. On the basis of these facts, a methodological procedure for the security measures implementation to increase the strategic railway terminals protection level has been created.

This methodological procedure is based on the application of the CPTED concept and considers both the requirements defined in international standards for the prevention of common crime and terrorism and current security methods and approaches that can be used to protect CIEs. The essence of the suggested methodological procedure is the assessment of the environmental and situational aspects of the security of railway terminals and the identification of weak points in the area of the spatial, layout and design arrangement of the railway terminal and in the area of supervision, control and maintenance. On the basis of the deficiencies identified in this way, it is possible to define adequate measures to increase the technical protection level. The methodological procedure is primarily intended for security managers of strategic railway terminals, but after partial modification it can also be used for security managers of bus terminals, air transport terminals and multifunctional transport terminals.

The application of the methodological procedure contributes to increasing the strategic railway terminals technical protection level of, as well as of persons and cargo located in its external and internal areas. The application of recommended security measures reduces the risk and increases the security not only of railway terminals, but also of related CIEs, which are dependent on the functionality of the terminals. The methodological procedure has already been successfully tested at selected railway terminals in the Czech Republic and Slovakia. It is clear from the results of the testing that the follow-up research should be focused mainly on the expansion of the assessed aspects of risk and security in the context of other current threats of an anthropogenic nature, such as personnel or cyber threats.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Technology Agency of the Czech Republic under Grant number CK01000015 and by the Slovak Research and Development Agency under Grant number [APVV-20-0457].

Notes on contributors

Tomas Lovecek is a full professor and vice-dean for science and research at the University of Žilina, Faculty of Security Engineering in Slovakia. In his research activities he deals with issues of designing and evaluation of the object protection systems and issues of information security management. He was project coordinator of the project Competency Based e-portal of Security and Safety Engineering (502092-LLP-1-2009-1-SK-ERASMUS-EMHE 2010-261814) and partner coordinator of two projects funded by EC/DG Home Affairs (HOME/2010/CIPS/AG/044 PACITA: Methodology for physical protection assessment of critical infrastructure elements against terrorist and other types of attacks and HOME/2013/CIPS/AG/4000005073 CI-PAC: Critical Infrastructure Protection Against Chemical Attack. He has experience of dealing with projects of FP7 (e.g. FP7-ERAChairs-PilotCall-2013 621386 Enhancing Research and innovation dimension of the University of Zilina in intelligent transport systems, 7. FP 313308 The Community Based Comprehensive Recovery). He is author of scientific monographs “Design and Evaluation of the Object Protection Systems” and “Object Protection of Critical Transport Infrastructure”. He is a member of editorial boards for scientific journals: European Journal of Security and Safety, Communications, Journal of Criminal Justice and Security and Crisis Management.

David Rehak is a full professor at the VSB – Technical University of Ostrava, Faculty of Safety Engineering. At this faculty, he also holds the position of guarantor of the doctoral study program “Fire Protection and Safety”. In the years 2012-2015, he held the position of vice dean for science and research. Currently, he is e.g. member of the International Association of Critical Infrastructure Protection Professionals (IACIPP), member of the World Road Association (PIARC), member of the Czech Technology Platform Energy Security (TPEB), Editor-in-Chief of the Transactions of the VSB-Technical University of Ostrava, Safety Engineering Series (TSES), and Associate Editor of the International Journal of Critical Infrastructure Protection (IJCIP). His scientific and research work is aimed on critical infrastructure resilience & protection, risk management, civil protection, energy security, environmental protection, and disaster risk reduction.

Jiri Pokorny graduated in 1992 at the Faculty of Mining and Geology of the VSB – Technical University of Ostrava, specialization Fire Protection. In 2002, he finished the doctoral program Fire protection and Industrial Safety. In 2013 he graduated from CEVRO Institute in Prague, specialization Master of Public Administration. From 2017 he finished habilitation. In 1993, began working in the Fire Prevention Department of the Fire Brigade in Opava. In 2001, he became a head of the Fire Prevention Department and a Deputy Director of the Fire Rescue Brigade Moravian-Silesian region, territorial department Opava. Between 2005 and 2010 he worked as a Director of the Fire Prevention Department of the Fire Rescue Brigade Moravian-Silesian region, regional headquarters in Ostrava. From 2011 to 2015 he was a Deputy Director for prevention and civil emergency preparedness of the Fire Rescue Brigade Moravian-Silesian region. Since September 2015 has worked as an academic employee at the VSB – Technical University of Ostrava, Faculty of Safety Engineering.

Ivo Haring gained his doctorate at Max-Planck-Institute for the Physics of Complex Systems (MPIPKS) and TU Dresden. Since 2004 he works at Fraunhofer Ernst-Mach-Institute (EMI), currently as Senior Scientist in the Department Safety and Resilience of Technical Systems. He lectures for the master courses Risk Engineering at Furtwangen University of Applied Science (HFU) and for Sustainable Systems Engineering (SSE) at the corresponding department INATECH of the Faculty of Engineering of the University of Freiburg. Research projects (set up) and corresponding publication record covered in 2023 25 million Euro research funding. Domains of interest include the analysis of event probabilities and susceptibility, of hazards, damage and vulnerability, risks and resilience of socio-technical systems, in particular of critical infrastructures and assets. Furthermore, concepts of engineering-inspired risk and resilience analysis processes and management, and related simulation and (semi-) quantification options as well as analytical approaches based on system performance functions. Another topic of interest is functional safety and reliability analysis and related methods, in particular when applied to new domains, e.g. autonomous driving. Projects cover localization and communication for more sustainable systems, e.g. for inspection of rotor blades. He (co-) authored 2 books, 25 articles, 70 conference papers and 7 book chapters.

Martin Hromada graduated in 2008 at the Tomas Bata University in Zlín in study field Security technologies, systems and management. He defended the dissertation thesis “Technological Aspects of Critical Infrastructure Protection of the SR” in 2011. He worked as a consultant of Deloitte Advisory, s.r.o. and currently works as a lecturer at the Department of Security Engineering, Faculty of Applied Informatics, Tomas Bata University in Zlín. In 2017 he defended his habilitation work at the Faculty of Safety Engineering, VŠB – TU in Ostrava and received an academic title of Associate Professor in the Department of Security Engineering. Safety and fire protection. Within the framework of research activities, he actively focuses on the protection and resilience of critical (information) infrastructure and the evaluation of functionality of physical protection systems.

Radoslav Kuffa graduated in 2004 in the field of IT technologies at the Armed Forces Academy in Liptovsky Mikulas. In 2017, he also graduated in Law at the Pan-European University in Bratislava. His work was focused on IT technologies and computer networks. Since 2009, he has been working as a technical director at DIS company. Currently, he is studying for a PhD at the Faculty of Security Engineering, University of Žilina.

ORCID

Tomas Lovecek http://orcid.org/0000-0002-3869-7099
David Rehak http://orcid.org/0000-0002-4617-0553
Martin Hromada http://orcid.org/0000-0003-0347-7528
Jiri Pokorny http://orcid.org/0000-0002-1829-8437
Ivo Haring http://orcid.org/0000-0002-0318-6133
Radoslav Kuffa http://orcid.org/0009-0004-3561-8756

Data availability statement

The authors confirm that the data supporting the findings of this study are available within the article. Any other required information are available from the corresponding author upon reasonable request.

References

Bennett, B. T. (2007). *Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel*. Wiley-Interscience.

Berlin Police. (2021). European recommendations for the protection of public spaces against terrorist attacks. Retrieved October 31, 2023, from https://www.berlin.de/polizei/_assets/aufgaben/praevention/english_safeci_handbook_shortversion.pdf

Canterbury Safety Working Party. (2004). Safer Canterbury: Creating safer communities. *Canterbury safety working party, canterbury*. Retrieved October 26, 2023, from https://www.ccc.govt.nz/assets/Documents/Culture-Community/Community-Safety/CPTEDFull-docs.pdf

CEN/TR 14383-5. (2010). *Prevention of crime - urban planning and building design - part 5: Petrol stations*. European Committee for Standardization.

CEN/TR 14383-7. (2009). *Prevention of crime - urban planning and building design - part 7: Design and management of public transport facilities*. European Committee for Standardization.

CEN/TR 14383-8. (2019). *Prevention of crime - urban planning and building design - part 8: Protection of buildings and sites against criminal attacks with vehicles*. European Committee for Electrotechnical Standardization.

CEN/TS 14383-4. (2006). *Prevention of crime - urban planning and building design - part 4: Shops and offices*. European Committee for Standardization.

CEN/TS 14383-6. (2022). *Prevention of crime - urban planning and building design - part 6: Schools and educational institutions*. European Committee for Standardization.

CEN/TS 16850. (2015). *Societal and citizen security - guidance for managing security in healthcare facilities*. European Committee for Standardization.

Cozens, P., & Love, T. (2015). A review and current status of crime prevention through environmental design (CPTED). *Journal of Planning Literature*, *30*(4), 393–412. https://doi.org/10.1177/0885412215595440

Crowe, T. (2013). *Crime prevention through environmental design*. Elsevier, Butterworth-Heinemann. https://doi.org/10.1016/C2012-0-03280-2

Directive 2012/34/EU of the European parliament and of the council of 21 November 2012 establishing a single European railway area

Directive (EU) 2022/2557 of the European parliament and of the council of 14 December 2022 on the resilience of critical entities and repealing council directive 2008/114/EC

EN 1627. (2021). *Pedestrian doorsets, windows, curtain walling, grilles and shutters - burglar resistance - requirements and classification*. European Committee for Standardization.

EN 356. (1999). *Glass in building - security glazing - testing and classification of resistance against manual attack*. European Committee for Standardization.

EN 50136-1. (2012). *Alarm systems - alarm transmission systems and equipment - part 1: General requirements for alarm transmission systems*. European Committee for Electrotechnical Standardization.

EN 50518. (2019). *Monitoring and alarm receiving centre*. European Committee for Electrotechnical Standardization.

EN 60839-11-1. (2013). *Alarm and electronic security systems - part 11-1: Electronic access control systems - system and components requirements*. European Committee for Electrotechnical Standardization.

EN 62676-1-1. (2013). *Video surveillance systems for use in security applications - part 1-1: System requirements – General*. European Committee for Electrotechnical Standardization.

European Commission. (2017). *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions: Action plan to support the protection of public spaces (COM/2017/0612 final)*.

European Commission. (2019). *Commission staff working document: Good practices to support the protection of public spaces (COM(2019) 145 final)*.

European Commission. (2020a). *A counter-terrorism agenda for the EU: Anticipate, prevent, protect, respond (COM (2020) 795 final)*.

European Commission. (2020b). *The EU security union strategy (COM(2020) 605 final)*.

FEMA 426. (2003). Risk management series. Reference manual to mitigate potential terrorist attacks against buildings. Retrieved October 31, 2023, from, https://www.fema.gov/sites/default/files/2020-08/fema426_0.pdf

FEMA 427. (2003). Risk management series. Primer for design of commercial buildings to mitigate terrorist attacks. Retrieved october 31, 2023, from https://www.wbdg.org/FFC/DHS/fema427.pdf

FEMA 428. (2012). Buildings and infrastructure protection series. Primer to design safe school projects in case of terrorist attacks and school shootings. Retrieved October 31, 2023, from http://files.eric.ed.gov/fulltext/ED541448.pdf

FEMA 430. (2007). Risk management series. Site and urban design for security guidance against potential terrorist attacks. Retrieved October 31, 2023, from, https://www.fema.gov/sites/default/files/2020-08/fema430.pdf

Forest, J. (2006). *Homeland security: Protecting American´s targets*. Praeger.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Elsevier. https://doi.org/10.1016/C2009-0-25612-1

GSK. (2008). *The concept of critical infrastructure in the Slovak Republic and ways of its protection and defence*. Government of the Slovak Republic.

GTD. (2022). Global terrorism database. University of Maryland. Retrieved October 13, 2023, from https://www.start.umd.edu/gtd/

Hesterman, J. (2019). *Soft target hardening protecting people from attack* (2nd ed.). Routledge.

Homeland Security. (2018). *Soft targets and crowded places: Security plan overview*. U.S. Department of Homeland Security. Retrieved October 07, 2023, from https://www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf

Hromada, M., Lovecek, T., & Rehak, D. (2023). *Increasing resilience, security of railway infrastructure and minimizing negative impacts on other sectors of transport infrastructure. Final report of the grant project SECURAIL*. VSB – Technical University of Ostrava.

IEC 60812. (2006). *Analysis techniques for system reliability – procedure for failure mode and effects analysis (FMEA)*. International Electrotechnical Commission.

ISO 22341. (2021). *Security and resilience – protective security – guidelines for crime prevention through environmental design*. International Organization for Standardization.

Jeffery, C. R. (1971). Crime prevention through environmental design. *The American Behavioral Scientist*, *14*(4), 598–598. https://doi.org/10.1177/000276427101400409

JRC EC. (2022). Security by design: Protection of public spaces from terrorist attacks. European Commission, Joint Research Centre. Retrieved October 31, 2023, from https://home-affairs.ec.europa.eu/news/security-design-protection-public-spaces-terrorist-attacks-2022-12-14_en

Kampova, K., Lovecek, T., & Rehak, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak Republic. *International Journal of Critical Infrastructure Protection*, *30*, 100376. https://doi.org/10.1016/j.ijcip.2020.100376

Karlos, V., Larcher, M., & Solomos, G. (2018). *Review on soft Target/Public space protection guidance* (2nd ed.). Publications Office of the European Union. https://doi.org/10.2760/553545

Kelliher, M. (2018). Protecting public spaces and soft targets. Bureau of Counterterrorism. Retrieved September 23, 2023, from https://2017-2021.state.gov/protecting-public-spaces-and-soft-targets/index.html

Kubalova, K. (2023). *Protection of railway infrastructure soft targets* [Dissertation Thesis]. University of Žilina,

Kubikova, Z. (2017, October 11–13). Identification and evaluation of soft targets in the local environment. Conference: In *International workshop Security in the Local Environment*, Zuberec, Slovak Republic (pp. 82–96). (in Slovak).

Lee, J. S., Park, S., & Jung, S. (2016). Effect of crime prevention through environmental design (CPTED) measures on active living and fear of crime. *Sustainability*, *8*(9), 872. https://doi.org/10.3390/su8090872

Livingstone Shire Council. (2018). Community safety and design principles. Retrieved October 23, 2023, from https://www.livingstone.qld.gov.au/doing-business/building-and-development/town-planning/planning-scheme-information/planning-scheme-user-guide

McEntire, D. A. (2018). *Introduction to homeland security: Understanding terrorism prevention and emergency management* (2nd ed.). Wiley.

McIlhatton, D., Berry, J., Chapman, D., Christensen, P., Cuddihy, J., Monaghan, R., & Range, D. (2020). Protecting crowded places from terrorism: An analysis of the current considerations and barriers inhibiting the adoption of counter terrorism protective security measures. *Studies in Conflict & Terrorism*, *43*(9), 753–774. https://doi.org/10.1080/1057610X.2018.1507311

Mihinjac, M., & Saville, G. (2019). Third-generation crime prevention through environmental design (CPTED). *Social Sciences*, *8*(6), 182. https://doi.org/10.3390/socsci8060182

Ministry of the Interior. (2016). Basics of soft targets protection – Guidelines. 2nd version. Soft targets protection institute, Prague. Retrieved October31, 2023, from https://www.mvcr.cz/cthh/clanek/terorismus-web-dokumenty-dokumenty.aspx (in Czech).

P 73 4450-1. (2013). *Physical protection of the object of critical infrastructure – part 1: General requirements*. Czech Agency for Standardization.

RAILway POLice. (2022). Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Annual review*. Retrieved October 31, 2023, from https://www.railpol.eu/site/documents

Rehak, D., Slivkova, S., Pittner, R., & Dvorak, Z. (2020). Integral approach to assessing the criticality of railway infrastructure elements. *International Journal of Critical Infrastructures*, *16*(2), 107–129. https://doi.org/10.1504/IJCIS.2020.107256

Reynald, D. M., & Mihinjac, M. (2019). Using guardianship and situational crime prevention (SCP) to strengthen crime prevention through environmental design (CPTED). In R. Armitage & P. Ekblom (Eds.), *Rebuilding crime prevention through environmental design: Strengthening the links with crime science* (pp. 58–74). Routledge. https://doi.org/10.4324/9781315687773

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, *1* (1), 83–98. https://doi.org/10.1504/IJSSCI.2008.017590

Security Council resolution 2341. (2017). *On protection of critical infrastructure against terrorist acts*. United Nations Security Council.

Shariati, A., & Guerette, R. T. (2017). Situational crime prevention. In B. Teasdale & M. Bradley (Eds.), *Preventing crime and violence. Advances in prevention science* (pp. 261–268). Springer. https://doi.org/10.1007/978-3-319-44124-5_22

Slivkova, S., Rehak, D., Michalcova, L., Pittner, R., & Yatskiv (Jackiva), I. (2022). Threat assessment of the railway infrastructure soft targets. In O. Prentkovskis, P. Skačkauskas, R. Junevičius, & P. Maruschak (Eds.), *TRANSBALTICA XII: Transportation science and technology. TRANSBALTICA 2021. Lecture notes in intelligent transportation and infrastructure* (pp. 429–438). Springer. https://doi.org/10.1007/978-3-030-94774-3_42

Swedish Civil Contingencies Agency. (2020). Guideline on protection of public spaces – protection against terrorism in crowded places. *Swedish civil contingencies agency*. Retrieved October 31, 2023, from https://rib.msb.se/filer/pdf/29010.pdf

Zemp, S., Stauffacher, M., Lang, D. J., & Scholz, R. W. (2011). Classifying railway stations for strategic transport and land use planning: Context matters! *Journal of Transport Geography*, *19*(4), 670–679. https://doi.org/10.1016/j.jtrangeo.2010.08.008