Article citation info:
VALIŠ D, VINTR Z, MALACH J. Selected aspects of physical structures vulnerability– state-of-the-art. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2012; 14 (3): 189-194.

David VALIŠ
Zdenek VINTR
Jindrich MALACH

SELECTED ASPECTS OF PHYSICAL STRUCTURES VULNERABILITY – STATE-OF-THE-ART

WYBRANE ZAGADNIENIA DOTYCZĄCE NARAŻENIA OBIEKTÓW FIZYCZNYCH NA ATAK – STAN WIEDZY

The paper is to deal with the selected aspects of structures vulnerability in terms of the physical protection. It is going to specify possible risks following from a terrorist attack, define a potential target and its characteristics, describe the resistance of an object to an attack, and determine the ways to reduce the probability of reaching a terrorist target, or increase object resilience. The results we are going to introduce reflect current knowledge in the area of physical protection.

Keywords: *Physical protection, target, vulnerability, risk.*

W artykule omówiono wybrane aspekty narażenia obiektów fizycznych na atak w kontekście ochrony fizycznej. Określono możliwe zagrożenia wynikające z ataku terrorystycznego, zdefiniowano potencjalne cele ataku i podano ich charakterystyki, opisano zjawisko wytrzymałości obiektu na atak, oraz ustalono sposoby zmniejszania prawdopodobieństwa dotarcia do celu ataku terrorystycznego lub zwiększania odporności obiektu. Przedstawione wyniki odzwierciedlają bieżący stan wiedzy w dziedzinie ochrony fizycznej.

Słowa kluczowe: *Ochrona fizyczna, cel ataku, narażenie na atak, zagrożenie.*

1. Introduction

Modern history is rich with examples of various terrorist attacks against structures, transportation systems, etc. worldwide. In the aftermath of the September 11th tragedies, the vulnerability of the all infrastructure to terrorist attack has gained national attention. In light of this vulnerability, various governmental agencies are looking into ways to improve the design of structures to better withstand extreme loadings. Tens of per cent of the homeland security outlays are devoted by countries to making potential targets less vulnerable to potential terrorist attacks. This is to protect what we usually call "Critical Infrastructure", "Key Asset" and/or "Key Resources". The concern of this paper is on the so called "passive defence" which is one part of several others like safe buildings, drinking water protection, Rapid Risk Assessment, etc. [14] We would like to discuss issues related to defining threat, describe vulnerability of possible targets and assess the possibilities of protection efficiency.

In terms of possible attack unpredictability is a key characteristics terrorist activity, for two main reasons [13]:

Terrorist have many more categories of legitimate targets, as well as worldwide scope, compared to traditional security concerns (which used to have the comparable luxury of protecting obvious military assets, or home territory).

Terrorist attack can have different objectives like to harm people, to damage infrastructure, to cause panic, etc.

Although such objectives may often overlap, these varying objectives lead to varying types or location targets. However, we have to keep in mind that detection and prevention must always remain the first line of defence [18].

Risk – definition and levels

We understand risk here as it is defined in [5]. The risk event is that the attack on a target with various outcomes. We have also to speak about the "acceptable risk level" based on the target selection and possible threat / consequences description. Taking into account work done by Stewart [19] there is after massive review decided to define following. The "global" consensus or generic quantitative safety goals obtained for involuntary fatality risk to an individual are thus:

- Annual fatality risk higher than 1×10^{-3} are deemed unacceptably high;
- Annual fatality risk in the range 1×10^{-3} to 1×10^{-6} are generally acceptable if the benefits outweigh the risk to provide an economic or social justification of the risk
- Annual fatality risk smaller than 1×10^{-6} are deemed as negligible and further regulation is not warranted.

The individual annual fatality risk can be therefore expressed:

$$\Pr(L) = \sum_{H}\sum_{DS}\sum_{L} \Pr(H)\Pr(DS|H)\Pr(L|DS) \quad (1)$$

where Pr(H) is the annual probability of hazard occurrence per item of infrastructure, Pr(DS | H) is the conditional probability of a damage state (e.g. safety hazard) given occurrence of the hazard and Pr(L | DS) is the conditional probability of a loss (e.g., damage costs, fatalities) given occurrence of the damage state.

We can also estimate expected cost spent on risk reduction per life saved. Protective measures will reduce fatality risks, with a reduction in expected fatalities of p_{attack} Pr(L | H)RN/100 where N is the number of people exposed to the hazard. It follows that the expected cost spent on risk reduction per statistical life saved (E_{LS}) is:

$$E_{LS} = \frac{100C_R}{p_{atteck}\Pr(L|H)RN} \quad (2)$$

where p_{attack} Pr(L | H) is the baseline individual annual fatality risk assuming no protective measures, C_R is the annual cost spent on protective measures for the item of infrastructure and R is the percentage risk reduction as a result of protective measures. We do not fully agree with this formula since risk reduction R plays role also in the Pr(L | H) as well as in the p_{attack}. Therefore the value R shall not be explicitly mentioned in the equation (2). On the other hand the percentage risk reduction modifies significantly the cost spent.

For illustration Figure 1 shows that a 95% reduction in risks results in annual fatality risks at least an order of magnitude lower than the quantitative safety goal [19].

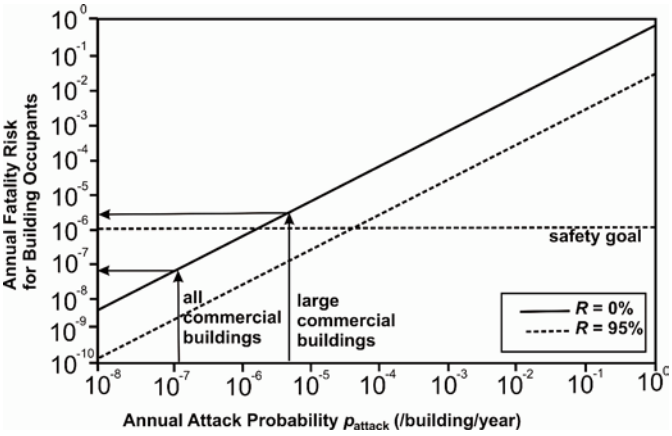

Figure 1. Individual annual fatality for building occupants risk showing quantitative safety goal of 1×10^{-6} fatalities/year

Since Pr(L) = 0.5p_{attack}, equation (3) can then be re-expressed as:

$$E_{LS} = \frac{100C_R}{0.5p_{atteck}RN} \quad (3)$$

2. Discussing threat

Before developing a plan to enhance building security, a risk manager shall first gain an understanding of potential threats acting against a structure/building as well as understanding of terrorists' goals and tactics. There are numerous combinations of explosive devices, cutting devices, impact vehicles and specific attack location to consider. It is impossible to design and protect all structures/buildings to resist all possible combinations of terrorist attacks that may occur. Simply said there are too many possible combinations. Therefore, a process is proposed to determine the most likely tactics from the terrorists' perspective and reduce number of possible combinations of attack that need to be considered for the purpose of design [20]. Various threat characteristics (against which a physical protection is prepared) are defined by a state authority. This characteristic in in Czech Republic called as "Design Basis Threat". Such characteristic includes numbers, equipment, knowledge and skills, intentions, strategy, etc.

Terrorist goal will vary depending upon the specific interest of different domestic or international organisation. However, goals which are most often encountered include making a high visibility statement through media coverage, obtaining publicity for their cause, destroying landmark or critical assets, exerting political pressure, advancing religious imperative, seeking vengeance, creating public fear and panic, maximizing casualties, disrupting the economy, and interrupting main or emergency transportation routes. Based on statement in [13] it is highly improbable that near-optimal stations were targeted by chance.

Due primarily to the amount of preparation time required, terrorists are not typically/likely to use conventional civilian or military structure demolition tactics. These techniques require specialized skills and considerably more time on target in order to achieve the precision demolition effects. Terrorist generally seek simple, rapid, and flexible plans; therefore, the tactics that they are most likely to use include making bomb threats to disrupt the structures, transportation systems; employing hand-placed explosives or cutting devices in critical hidden areas of a building – if possible. Than using fragments to target vehicles during times of high traffic density; targeting multiple structures to disrupt the infrastructure systems and reduce emergency responder effectiveness; cutting critical utilities running on bridges; using collapsed span as an obstacle to block a critical waterway or destroy a nearby facility; making use of trucks, ships, trains, or planes as impact or explosive vehicles.

Terrorist plans include at least following characteristics:
- Realistic;
- Coordinated;
- Cohesive;
- Simple;
- Creative;
- Flexible; and
- Secretive.

In deciding which strategy to use, terrorists will probably use comparison criteria such as:
- Having a high probability of success;
- Being realistic with easily obtainable materials;
- Occurring quickly to minimise placement and priming time;
- Utilising secrecy and surprise to minimise chances of being detected;
- Being simple and easy to coordinate;
- Providing flexibility to change the plan;
- Having a large impact and magnitude to maximize damage, casualties, and public panic, etc.

Course of action involving vehicles generally perform well when considering all these criteria, and therefore tend to be the "most likely" courses used. Scenarios involving hand-placed explosives limit the charge weight that can be used, and thus reduce the overall impact and chances of success unless they can achieve sufficient time on target. Most of the cases where smaller charges would be very effective involve locations that can often be difficult to access, thereby reducing their speed, simplicity, and flexibility. Additionally, the threat of hand-placed precision demolitions can be readily countered with physical security and detection measures on a structure/building.

Threat therefore modifies intended levels of physical protection as well as risk profile in terms of possible attack. This all might be described by common mathematical characteristics.

Threat levels

Protective measures could be divided into threat levels for implementation as the appropriate level is reached, as demonstrated in table 1. Each country has its own "Common threat levels" e.g. according to the legislative for the critical infrastructure protection. Countermeasures are therefore modified by such possible threat levels. In Table 1 there is modified scale in accordance with [20].

Table 1. Scale levels of threat levels and measures

Threat level to a structure/ building	Additional security measures
Severe	Restricted access with guards, barriers, and vehicle searches. All other measures listed bellow.
High	Increased frequency of patrols and checks. Conduct unscheduled exercise of emergency response plans. Postpone nonessential maintenance. Coordinate with national security corps or law enforcement for possible closure and vehicle searches once severe level is reached. All other measures listed bellow.
Elevated	Implement regularly scheduled police patrols. All other measures listed bellow.
Guarded	Review and update emergency response procedures. Increase frequency of periodic checks of cameras, fences, etc. All other measures listed bellow.
Low	Monitor security systems in place (including periodic checks). Disseminate threat information to personnel. Regular refinement and exercising of emergency operations plan. Emergency responder training. Continually updating threat and vulnerability assessment.

Each of the security measures stated above is worth respective amount of money.

3. Defining vulnerability

Department of Homeland Security (DHS) in the USA defines vulnerability as "physical feature or operational attribute that renders an entity, asset, system, network, or geographical area to exploitation or susceptible to a given hazard" (2010) [3]. The key of assessing vulnerability properly is in the last phrase of that definition. Although vulnerability assessments can be standalone documents, vulnerability is best understood within a risk context, specifically the interaction between the threat and the consequence. This interaction is the reason that vulnerability V is sometimes defined as the probability of success (of an attack) P_S given an attack A or probability of the consequence occurring given an event. Mathematical expression is than:

$$V = P_S(\mathrm{A}) \tag{4}$$

In either case vulnerability is the collective influence of physical features or operations that reduce the effectiveness (alternatively success) of the adversary's attack or that make the target better able to sustain the attack. Analysis is highly dependent, therefore, on the method of attack and strength of the attack expected. A building's vulnerability to an improvised explosive device (IED) will differ from the vulnerability to a vehicle-born IED (VBIED), for example, depending on the assumption in the definition of those attacks, such as amount or type of explosives, entry points, and stand-off distance. Even within the category of VBIED, vulnerability will differ based on terrorist tactics, such as leaving the vehicle on the street adjacent to the building or ramming the vehicle into a building or its defensive perimeter. The more specific the context, the more accurate the vulnerability assessment for particular target can be.

For security risk, vulnerability is also influenced by the terrorist adversary. Terrorist groups have different levels of competence and expertise. This can affect not only target selection but also their knowledge of countermeasures and their determination to overcome those countermeasures through technology or effort. These aspects of the threat can influence judgements of degree of accessibility or strength of countermeasures (this states actually one of very hardly measured characteristics physical protection system which is the deterrence. But for well-equipped and trained terrorist discourage is very low however). Opportunity to attack, in other words, reflects the interaction of threat and vulnerability; the characteristics of potential attackers help provide further context for high-quality vulnerability assessments. With all of these variables, it is easy to see why some argue that vulnerability is not a static characteristic but very dynamic state and, in the extreme, a combination of the various states of all the aspects of the asset, facility, or system, which is in constant flux. There always still need for simple way to generate a repeatable and comparable vulnerability level that is useful for the user (government for instance) in the infrastructure protection.

For this reason we have to accept kind of conceptual approach to vulnerability assessment of structures as mention for instance in [3]:

1. Characteristics of the asset itself;
2. The protective measures that prevent access for attack;
3. Access allowed to outsiders and insiders;
4. The functional dependencies on internal and external entries;
5. Generating scenarios
6. Attack methods filtering
7. Event/fault tree analysis (recognisability, countermeasures effectiveness, robustness/resistance)
8. Combining the components

If we speak about vulnerability we cannot forget also to emphasise the structural robustness. It might be expressed by "Protection categories" as said in [21], "Robustness Index" as mentioned in [4] and has several degrees on scale – usually 1-10. Some retrofit recommendations for increasing the structure robustness are for instance listed in [2]. Considering the further statements in [4] there are three most important structural properties which increase a structure's/ building's ability to survive catastrophic overload or damage:

- Structural redundancy (A structure that will perform well in catastrophic situation will permit gravity loads that must be supported during the event to be carried to the foundations using multiple load paths).
- Fireproofing toughness (A structure's ability to resist fire is an important contribution to its robustness, since fire is often a part of catastrophic event).
- Connection robustness (Structural connections are very important and are critical in holding a building together during the large movements that occur in a fire or other catastrophic event).

There are several ways for assessing the severity of possible terrorist attack. Many of them are based on conventional standards like [5, 7, 8, 9, 10, 11, 12]. In [16] there are also mentioned some possible tools for risk assessment either software-based (e.g. RAMPART – Risk Assessment Method-Property Analysis and Ranking Tool; CONTAMW – software for vulnerability assessment; HVAC – software for heating, ventilation, and air condition in buildings assessment) or classical (standards and books). One interesting procedure is mentioned in [1] and is based on risk approach. In defining the problem and deciding an appropriate scope given the time frame and resources there are four critical targets identified for the risk based methodology.

1. Identifying potential targets of attack, methods of attack, and courses of actions.
2. Deciding which possibilities merit deeper scrutiny.
3. Identifying a mathematical way to represent intelligence data in the model.
1. Integrating the first three tasks into a framework that yields output useful in fulfilling the objectives.

The methodology proposed – called "Risk Filtering and Ranking Method (RFRM) addresses what can go wrong, what can be done and deciding which possibilities merit deeper scrutiny. The methodology uses RFRM to identify the most critical contributors to the risk associated with a potential terrorist event to focus the rest of the analysis on. RFRM considers both quantitative factors, such as severity as measured by number of deaths or injuries, and qualitative factors, such type of attack. Since the number of components under consideration often can be large, RFRM is very useful in filtering and prioritizing scenarios.

3.1. Vulnerability characteristics

If we are to talk about building's vulnerability, we have to bear in mind the following facts [17].

- The number of potential terrorist targets is essentially infinite (Terrorists seek to kill people and/or destroy property in pursuit of political goal).
- The number of terrorists appears to be exceedingly small and their efforts and competence rather limited (In 2002 an intelligence report were asserting that the number of trained al-Qaeda operatives in USA was between 2.000 and 5.000).
- In many cases the target selection is effectively a random process (This process, together with other internal motivating mechanisms stressing group cohesion and camaraderie more than grand planning, effectively make terrorist target selection something like random process. Efforts to determine terrorist "intent" in advance become, then, highly problematic.
- The probability that any specific target will be attacked is extremely small in almost all cases (Despite the attention in garners, terrorism is rather rare occurrence comprised of incidental, isolated acts of mayhem perpetrated by individuals or small groups, violence that generally does a comparatively limited amount of damage. Even under quite dire scenarios, in country like the USA, the chance an individual target will be hit is vanishingly small).
- If one potential target happens to enjoy a degree of protection, the agile terrorist generally can readily move on to another one (There is also something that might be called "the displacement effect" Terrorists can choose and change their targets depending on local circumstances. There have been instances in Israel in which the suicide bombers, seeing their primary targets, shopping malls, rather well protected, blew themselves up instead on the street).
- To the degree protection measures make one target safer, they make other ones less safe (For example, there is a program to protect bridges in the USA, and a list of something like 200 of the most important bridges had been drawn up. There seems to be no evidence terrorists have any particular desire to blow up a bridge, due in part, perhaps, to the fact that it is an exceedingly difficult task under the best of circumstances, and the number of casualties is likely to be much lower than for many other targets.
- Most targets are "vulnerable" in that it is not very difficult to damage them, but invulnerable in that they can be rebuilt in fairly short order and at tolerable expenses (on the one hand, most, probably almost all, potential terrorist targets are "vulnerable" in the sense that they can be damaged, in many cases badly, even by a simple explosion).
- It is essentially impossible adequately to protect a very wide variety of potential terrorist targets except by completely closing them down (As it happened, the bombs did no damage because they were poorly constructed and did not actually explode, but this fortunate result, of course, stems entirely from terrorist incompetence, not from the protective measures).

As stated in [17] for example, the applications leading to resistance increase are appropriate in case they take a required effect. These are:

- Nuclear and chemical plants and material (there are not large number of nuclear plants, and an adept terrorist attack on them could potentially have devastating consequences. Consequently, they seem to be prime candidates for protection).
- Key infrastructure nodes (unfortunately it is not at all clear that any such nodes exist although they are some in the EU legislative and some also in respective countries legislation.
- Major ports.
- Symbolic structures – potential targets (religious, historical, etc.).
- Others.

Based on the principles presented in [15] we can understand nine criteria or variables selected for constructions vulnerability assessment like:

- Visibility level of the site ("0" – invisible up to "5" – very high visibility).
- Criticality of the site to its jurisdiction (e.g., city or town "0" no usefulness up to "5" – critical).
- Impact of the site outside of the jurisdiction ("0" – none up to "5" – very high).
- Accessibility of the site to the public ("0" – restricted up to "5" – unlimited).
- Possible hazard located on the site (like Weapons of Mass Destruction – WMD or CBRNE. "0" – none up to "5" – very high).
- Height of the structure ("0" – underground up to "5" – sky scraper).
- Type of the structure ("0" – underground up to "5" – wood structure)
- Population capacity on the site ("0" – no population up to "5" – more than 50.000 people).
- Potential for collateral mass casualties ("0" – 0-100 people up to "5" – more than 5.000 people).

The total number of points formed by the above nine scale should be got by addition between 0 and 45. Vulnerability categories are broken down into five groups as follows:

- Negligible vulnerability – total ranking score 0-9 points.
- Low vulnerability – total ranking score 10-18 points.
- Medium vulnerability – total ranking score 19-27 points.
- High vulnerability – total ranking score 28-36 points.
- Critical vulnerability – total ranking score 37-45 points.

3.2. Approaches for solving vulnerability

There are more options for solving the vulnerability of structures. One is based on the Israeli experience with thousands of armed attacks and the proposed structure of SEPHRA (SEcurity Protection and Hardening Risk Analysis) which was successfully used worldwide in the last 20 years in numerous projects. Scheme of principles is on the figure 2 bellow.

We would also like to present several proposals for vulnerability minimisation of possible targets [17]:

1. Planning
   a) Updating the emergency operation plans/crisis management plan to include response and recovery to a terrorist threat involving important structures.

b) Communication and coordination with local and state law enforcement agencies to obtain intelligence, training, and technical support.

c) Regular drills, table-top exercises, and full scale simulations to test response procedures, communication, and coordination.

d) Planning additional redundancy in transportation system through alternate routes, traffic management, modified lane usage, etc.

e) Planning for prompt debris removal and repairs to ensure rapid restoration of services and restore public confidence in the structure.

f) Developing a training plan for maintenance personnel to be observant of surroundings and capable of dealing with suspicious objects.

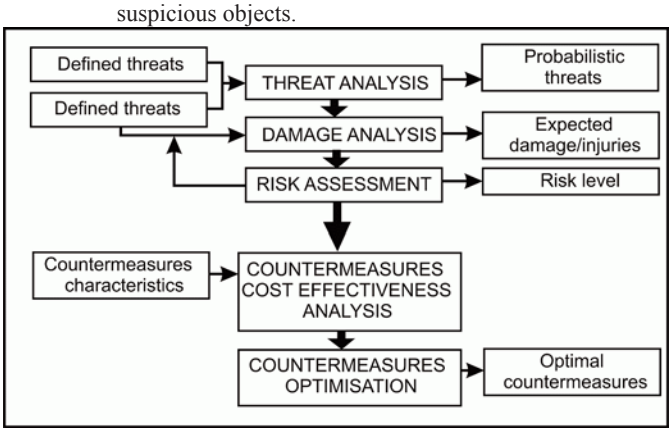

Figure 2. The SEPHRA diagram

2. Information control:
   a) Establish "need-to-know basis" procedures for the release of vulnerabilities, security measures, emergency response plans, or structural details for specific structure.
   b) Review and sanitize websites for potential information which may be beneficial for terrorists.
3. Site layout measures:
   a) Improved lighting with emergency backup, combined with the elimination of hiding spaces which could be used to prepare explosive charges.
   b) Clearing overgrown vegetation to improve lines of sight to critical areas.
   c) Using creative landscaping with regular maintenance to increase vehicular standoff distance to important structural components.
   d) Elimination of access to critical areas such as beneath the deck, maintenance rooms, etc.
   e) Elimination of parking spaces inside or around/beneath the structure.
   f) Providing pass-through gates in concrete median barriers to enable rerouting of traffic and access to emergency vehicles.
   g) Planning redundancy in individual future structures/buildings.
   h) Avoiding architectural features that may magnify blast effects.
4. Access control:
   a) Police patrols, surveillance, and guards.
   b) Keyed or keyless entry systems on access panels, tower entrances, and maintenance areas.
   c) Exterior and interior intrusion detection systems (boundary penetration sensors, volumetric motion sensors, and point sensors, etc.).
   d) Closed circuit television placed where in cannot be easily damaged or avoided, while providing coverage of critical areas to monitor activity, detect suspicious actions, and identify suspects.
   e) Incorporate a higher level of identification procedures and verification of credentials for maintenance personnel.
   f) Deny/limit access to critical structural elements (i.e. providing fencing around important building parts, restricting access to some places of structures, etc.).
   g) Physical barriers to protect gates, towers, piers, etc.
   h) Physical barriers to control access to the structures during credible threat (use conjunction with random vehicle search).
   i) Rapid removal of abandoned vehicles.
   j) No-fly zones around and above critical structures.
   k) Emergency telephones to report incidents or suspicious activity.
   l) Use of an advanced warning system, including warning signs, horns, and popup barricades to restrict access after span failure.
5. Deception measures:
   a) Installing dummy CCTV cameras to augment active cameras when resources are limited.
   b) Parking an abandoned police vehicle nearby.
   c) Posting intrusion detection signs and warnings.
   d) Effectiveness assessment of physical protection systems.

4. Conclusion

This paper is to analyse the present state of the selected aspects of physical protection. It is quite obvious that terrorist attacks can occur at any time and any place. We are not going to tackle the motives for a terrorist act, or different types of attacks which might be performed by an individual (a recent event in Norway) whose motives are quite personal, or by a group (controlled by an organization) the motives of which are religious or political.

The article is focused on two basic aspects related to physical safety. It is a potential target of an attack, the selection of a target versus the target vulnerability. The paper is to assess both possible risks as a consequence of the attack and objects vulnerability. All the current and commonly used approaches listed above are recommended for possible modification.

It is assumed that this work is by no means the end and later it will focus more on assessing the efficiency of physical protection systems and more precise determination of risks resulting from a potential attack. Therefore the authors will concentrate on specifying in a qualitative and quantitative manner the probability of a successful attack, or the probability of an object to resist.

Acknowledgement: *We gratefully acknowledge the Czech Ministry of the Interior supporting us under project "Security Research – Target Identification VG 20112015040 and with the support of the "Project for institutional development of K-202", University of Defence, Brno.+9971988*

References

1. Blais R A, Henry M D, Lilley S R, Pan J A, Grimes M, Haimes Y Y. Risk-based methodology for assessing and managing the severity of terrorist attack. IEEE Systems and Information Engineering Design Symposium, SIEDS '09 , art. no. 5166175, 171-176.
2. Eytan R. Cost effective retrofit of structures against the effect of terrorist attack – the Israeli experience. Proceedings of the Structures Congress and Exposition 2005, 2161-2172.
3. French G S, Gootzit D. Defining and assessing vulnerability of infrastructure to terrorist attack. Vulnerability, Uncertainty, and Risk: Analysis, Modelling, and Management - Proceedings of the ICVRAM 2011 and ISUMA 2011 Conferences, 782-789.
4. Iding R H. A methodology to evaluate robustness in steel buildings – Surviving extreme fires or terrorist attack using a robustness index. Proceedings of the Structure Congress and Exposition 2005, 511-515.
5. ISO/IEC Guide 73:2009 Ed 2.0 Risk management – Vocabulary – Guidelines for use in standards.
6. ISO 31 000:2009 Ed 1.0 Risk management – Principles and guidelines on implementation.
7. ISO 31 010:2009 Ed 1.0 Risk management – Risk Assessment Techniques.
8. ISO 13 824:2009 Ed 1.0 General Principles on Risk Assessment of systems involving structures.
9. ISO 61 508-(1-7):2008 Ed 2.0 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.
10. JCSS (Joint Committee on Structural Safety) – Principles, System Representation × Risk Criteria.
11. ECSS (European Cooperation for Space Standardisation) – Q-ST-40-02C Space Product Assurance – Hazard Analysis.
12. MIL-STD 882B Standard Practice for System Safety.
13. Jordán F. Predicting target selection by terrorists: A network analysis of the 2005 London underground attacks. International Journal of Critical Infrastructures 2008; 4 (1-2): 206-214.
14. Kelly T J, Hofacre K C, Derringer T L, Riggs K B, Koglin E N. Testing of safe building detection technologies and other homeland security technologies in EPA´s Environmental Technology Verification (ETV) program. Proceedings of the Air and Waste Management Association's Annual Meeting and Exhibition 2004, 3449-3457.
15. Kemp R L. Assessing the vulnerability of buildings. Journal of Applied Fire Science, 2007; 14 (1): 53-61.
16. Marshall H E, Chapman R E, Leng C J. Risk mitigation plan for optimizing protection of constructed facilities. Cost Engineering 2004; 46 (8): 26-33.
17. Mueller J. Assessing Measures Designed to Protect the Homeland. Policy Studies Journal 2010; 38(1): 1-21.
18. Stewart M G. Cost effectiveness of risk mitigation strategies for protection of buildings against terrorist attack. Journal of Performance of Constructed Facilities 2008; 22(2): 115-120.
19. Stewart M G. Life-Safety risks and optimisation of protective measures against terrorist threats to infrastructure. Structure and Infrastructure Engineering 2011; 7(6):431-440.
20. Williamson E B, Winget D G. Risk management and design of critical bridges for terrorist attacks. Journal of Bridge Engineering 2005; 10(1): 96-106.
21. Zehrt Jr. W H, Acosta P F. Analysis and design of structures to withstand terrorist attack. Proceedings of the Structures Congress and Exposition 2003, 585-592.

Assoc. Prof. David VALIŠ, Ph.D.
Department of Combat and Special Vehicles
Faculty of Military Technologies
University of Defence
Kounicova 65, 662 10 Brno, Czech Republic
E-mail: david.valis@unob.cz

Prof. Zdenek VINTR, Ph.D.
Department of Combat and Special Vehicles
Faculty of Military Technologies
University of Defence
Kounicova 65, 662 10 Brno, Czech Republic
E-mail: zdenek.vintr@unob.cz

Jindrich MALACH, Ph.D.
EBIS, Ltd.
Krizikova 2962/70a, 612 00 Brno, Czech Republic
E-mail: jmalach@ebis.cz