Chapter 19
Assessing Security of Soft Targets Using Complex Systems Analysis Methods

Bohus Leitner and Maria Luskova

Abstract The paper is dealing with issues of soft targets security represented by places with a high concentration of people and a low level of security against violent attacks. The aim of the paper is to assess the security of selected soft target object (with a large number of people) through appropriate methods for risk analysis, evaluation of results and proposal of indicators for implementing the methods into the practice. For solution of the issues analyses of complex systems methods – ETA and FMEA were used. Applying these methods resulted in a risk reduction at minimum required level. Based on the findings, the FMEA method was indicated to be the most effective due to flexible access to the object assessment. The results can be used as a basis for an assessment of soft targets security and also as an incentive in modelling of violent attacks.

Keywords Soft target · Complex systems · ETA · FMEA · Security assessment

19.1 Introduction

The security situation in the world is constantly worsening in term of terrorism and extremism and the incidence of violent attacks similar to (but not always ideologically motivated) terrorism on the most vulnerable targets – people is increasing, too. Organizers of such attacks are increasingly motivated to focus them on unprotected places with a high concentration of people regardless of whether they are politically or religiously symbolical by something. We talk about so-called soft targets.

The paper is dealing with assessment of security level and increasing the resilience of soft targets using selected methods of complex system analysis. Increased interest of terrorist groups in such objects also requires adaptation of the security system. In addition to the theoretical background of soft targets protection issues, the

B. Leitner (✉) · M. Luskova
University of Žilina, Žilina, Slovakia
e-mail: bohus.leitner@fbi.uniza.sk

L. Hofreiter et al. (eds.), *Soft Target Protection*, NATO Science for Peace and Security Series C: Environmental Security,
https://doi.org/10.1007/978-94-024-1755-5_19

results of the application of selected system analysis methods (ETA, FMEA) to the model object are presented in the paper.

Threat scenarios have been proposed, based on the hazard analysis and the results of the ETA and FMEA methods, measures to increase the security of the object have been proposed, and the verification of their effectiveness and impact on the resilience level of the object has been performed.

19.2 Soft Targets: Characteristics, Potential Targets and Ways of Attacks

A soft target is a term commonly used by the security community to designate places with a high concentration of people and a low level of security measures against the execution of a violent attack and its possible consequences. These are primarily tourist attractions or various social (especially sport, political, religious or cultural) events and traffic nodes (stations, airports) or means of transport. In the wider definition of soft targets, schools, hospitals, as well as swimming pools, sport fields and other objects are considered to be such objects.

According to [1], the soft targets are "objects, spaces or actions characterized by the high concentration of people, an absence or a low level of security measures against violent attacks and non-inclusion between critical infrastructure objects." Soft targets are "objects (buildings, premises, open spaces, etc.) in which a large number of people are grouped together at a certain place. These objects do not apply any or only slightly specific security measures to prevent a violent attack on the lives of persons in these objects, to ensure a rapid response to the attack, or to assist in managing a potential attack without losing people's lives. A violent attack on this target could cause death or injury to a person or more persons who are near the destination".

Based on the above mentioned, as well as [2], it is possible to include among the soft targets mainly:

- major traffic nodes train and bus stations, airport terminals,
- hospitals, clinics and other medical facilities,
- school facilities, dormitories, canteens, libraries, community centres,
- shopping centres, markets and business complexes,
- sport halls and stadiums,
- cinemas, theatres, concert halls, entertainment centres,
- public gatherings, processions, demonstrations, pilgrimages,
- cultural and religious monuments, museums, galleries,
- bars, clubs, discos, restaurants and hotels,
- cultural, sporting, religious and other events, . . .

For the state, the most important fact is that soft targets are large number. This significantly limits the practical possibilities of ensuring their security only by the

state/public administration and increases the necessity for the implementation of the security measures by the soft targets themselves. Most of them are able to secure their security much better (e.g. better knowledge of the environment, contact with surrounding entities, presence of staff on site but also funding to increase security, etc.) as the state itself. An analysis of terrorist attacks, according to data from the Global Terrorism Database [3], also reveals the priority ways of attacking. When analysing threats, defining scenarios and defining a security system for soft targets, considering the following ways of potential attacks is needed:

1. Explosive attack (except when using a vehicle).
2. Suicidal attack by an explosive.
3. Explosives in postal packets.
4. Explosive in a parked vehicle.
5. Arriving a vehicle with an explosive with a suicide attacker.
6. Incendiary attack.
7. Attack by shooting weapon (pistol, submachine gun, etc. – active shooter).
8. Taking up the hostage and barricade situation.
9. Cold weapon attack (knife).
10. Attack on soft target by crowd.
11. Attack by arriving vehicle.

19.3 Principles of Soft Targets Protection

Soft targets are a large and very diverse group of subjects. They are characterized by security – relevant characteristics that differ them from other targets but also among themselves. Typical ways to commit terrorist attacks have been identified [4] and therefore it is possible to define the most of the relevant measures in advance. This makes it possible to target the protective and defensive elements more precisely, to formulate the principles of security and to recommend specific measures.

19.3.1 Establishment of an Appropriate Measure

To set up a functional soft target security system, it is needed to:

1. **Clarify protected interest**. At this stage, it is necessary to define what we value, what we do not want to lose, what could possibly damage us. Primarily it is about the health and life of people (violent attacks), property, information, social values, and also e.g. a good reputation.
2. **Define possible sources of danger (threat)** to protected interest. It is necessary to identify specific groups or categories of persons with potential motivation to attack. This is used to analyse previous similar attacks and to consider potential sources of threat. It is always necessary to take into account the specifics of a

particular object/action and usually specific threats (e. g. presence of VIP, risk date, pyrotechnics, media interest, resilience of buildings, effectiveness of current measures, etc.).

3. **Specify threatening ways of attack**. The basis of a high-quality soft-target security system is to define as precisely as possible the sources of threat. The security system must be the result of a thorough analysis of interests and potential threats. It is characterized by a systematic analysis of the threats to a specific target and then by setting up appropriate measures. This is a procedure based on relevant threats.
4. **Analyse specified threats by threat and risk analysis methods and identify priority threats**. The basic principle of relevant methods is to compare the likelihood of threat activation and impact rates (consequences) for individual threats. The threat rate overview is often expressed by a matrix which makes it possible to allocate resources to address priority threats more efficiently. Prioritization of threats makes it possible to determine their importance and to determine for which of them the resources will be allocated.
5. **Design and application of security measures**. Based on prioritization of threats and determination of appropriate measures, measures to increase the resilience of the object are applied. There are, for example, installed technical elements, elaborated specific security plans, determining not only preventive measures and routine procedures but also reaction if the crisis situation has not been prevented and its consequences have to be minimized.

19.3.2 Incident Timing

With all the planned incidents, it is necessary to work in three phases of time.

1. What can be done before the occurrence of the incident so that the likelihood of its occurrence and the extent of the consequences are reduced or the incident has diverged from the target.
2. What can be done when the incident is in progress.
3. What can be done to mitigate the impact when the incident has already taken place.

Before the incident: Prevention – deterrence:

- Preventive measures – reduce the likelihood of an attack, increase the speed and intensity of the response, and limit the extent of the consequences and reduce them more quickly.
- Deterrence tools – lead the attackers to decide not to choose the target.
- Crisis communication – leads to a calming situation and a mitigation of the conflict.

During the incident: Detection – immediate reaction:

- Immediate detection of unwanted activity or disturbance of protected zones – preferably before the attack itself.
- Immediate reaction of security personnel or other members of the security system – best according to a pre-planned Plan.

After Incident: Mitigation and adaptation:

- Follow-up to the prepared coordination plan for management and its defined priorities for each phase after the incident.
- Early renewal of the organization's activities and learned from a negative event.

The mentioned focus of security measures is the basis of a practically focused approach – DRRM (Deter – Reveal – Respond – Mitigate Impacts).

It is a methodological tool that verifies the effectiveness of security measures and reducing the level of threat the impact of which we want to reduce. The nature of the method: to list of possible incidents (which were rated relevant to the object and we want to minimize them), we will assign measures to deter, early detect, and respond as well as reducing impacts after an incident. The final form of the security system needs to be re-verified to determine whether it can reduce the threat rate before, during and after an incident. An immediate reaction that would stop an attacker (physical defence) is mostly only in the power of professional teams who are able tactically and technically eliminate the attackers while working with other people around. However, such teams are not usually available for soft targets.

However, instructed soft-target personnel (or other public present in the incident) may play a non-negligible role during the immediate reaction phase. In the case of a proper response, he may call for assistance, divert passers-by from the attack site, separate the attacker from by locking the area, warn others and also eliminate the attacker by his/her own strength within the necessary defence.

19.4 Security Diagnostics and Assessment of Soft Target Resilience

In order to select the appropriate security measures, each objective needs to be assessed individually, particularly with a view to clarifying the security relevant factors affecting two essential criteria:

1. attractiveness of the target from the perspective of the attacker,
2. real possibility of its security

19.4.1 Basic Diagnostic Factors for Selecting Security Measures

The basic factors in terms of the properties of soft targets:

1. **Openness to the public**. Especially if it is an outdoor action, a closed object or a public object. Such characteristic has an impact on the concept of security – whether measures can be taken at the entrances or in the open space.
2. **Own security personnel**. Using the own staff for security tasks significantly extends the security system's capabilities. The presence of security staff or organizational services reduces the attractiveness of the target.
3. **Amount and concentration of persons**. For a soft target, the amount and concentration of people at a certain point in certain time is primarily a factor influencing the focus of the security system and the preparation of security procedures.
4. **Presence of the police**. Police is a major deterrent; its presence decreases the attractiveness of the target. Usually, the police are present only short time, locally or only to maintain public order. If there is a permanent police in the building, it is not a soft object.
5. **Presence of the media**. For terrorists or otherwise motivated attackers, the media presence is very attractive. Especially, if it is an important event with TV transmission in real time.
6. **Target symbolism**. If the entity is a symbolic target for attackers, the threat of the subject increases significantly. For a soft target, this means taking into account in the security plan the ways in which the attacks of specific violent groups are carried out and adapting their security strategy to extreme threats.

Important factors in self-protection:

7. **Organizational structure**. It has a significant impact on the ability to formulate and implement a security policy, to develop a realistic security plan, and to manage the implementation of security measures for soft target. More entities in one vulnerable location (such as a business centres) create a need for coordination of individual entities. This is related to voluntary activity for common security interest and sharing possible costs.
8. **Resources and finances for security.** The budget for security and the appointment of a security manager, i.e. person in the organizational structure of the organization responsible for the security agenda and the definition of measures.
9. **Ability to identify risk situations**. It examines whether the subject is able to assess which activities and situations are at risk, what to focus on, what to consider as significant and to solve by their own choices.

Based on the above factors, every soft target can clarify what are its strengths and weaknesses and what are its opportunities or risks (e.g. using the SWOT analysis) it is possible to determine what should be the primary focus for the development of own security.

19.4.2 Improving the Resilience of Soft Targets

Soft targets protection requires a completely different, specific approach as defined e.g. for security of critical infrastructure objects [5, 6]. At the conceptual level, this requires the establishment of cooperation between the state, the self-government and the private entities. At the tactical level, this requires new training methods for the police, a new way of communicating with the public, identifying priority soft targets and their gradual resilience increasing. At the operational level, e.g. organization of the actions it is needed to involve the available personnel in the security management system, consult the police with security measures before each major action and progressively improve the management of the foreseen threat scenarios.

According to [1], soft targets can be protected in several ways:

- **Physical security** – plays a key role, e.g. staff checking people at the entrances to buildings, execution of walks or operator and security technology in the control room.
- **Electronic security equipment** – e.g. a camera system used to monitor the internal and external spaces and movement of persons, alarms and alarm systems, detectors of metals and explosives, as well as access and attendance systems that serve, in addition to registration purposes, also to "complicate" the entry of an unauthorized person or to restrict it movement around an object.
- **Mechanical security equipment** – e.g. security doors, in the case of external actions, concrete blocks [7–9], columns preventing the entrance of vehicles, or turnstiles that serve in the buildings to arrange and authorize the entry and exit of persons [10].

19.5 Case Study: Evaluation of the Asset from the Point of View of the Soft Target Protection

Selected object: Business and entertainment centre (BEC).

19.5.1 Characteristic of the Soft Target

The BEC has a total of 80 shops and services, 2 cinemas, 6 cash points, underground garages and technical facilities. The technical facility consists of the Security Operation Centre, the Centre of Administration and the Cleaning and Technical service.

The basement floor (Fig. 19.1) consists of underground parking and one operation (car wash). On the ground floor there are shops and services, a total of about 40 facilities. There are four entry points to the ground floor building, which serve

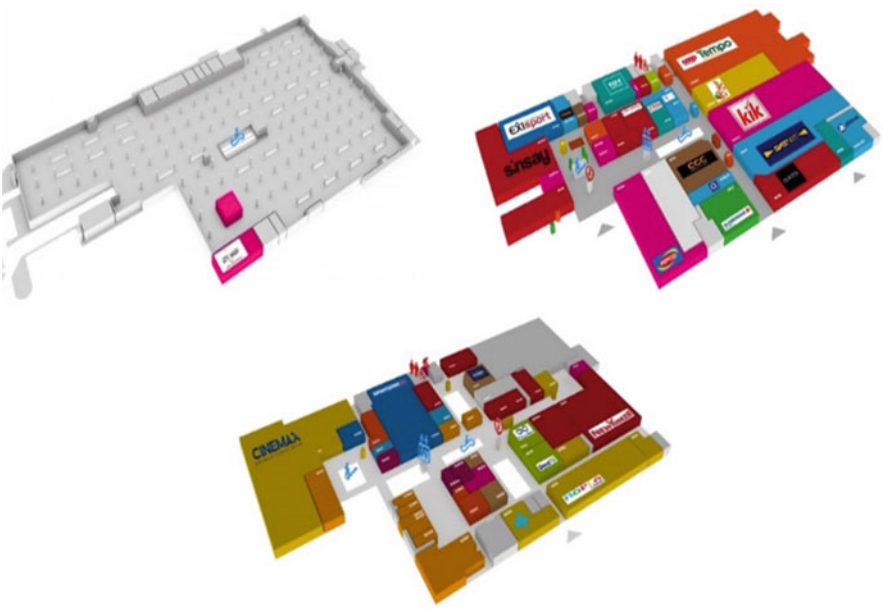

Fig. 19.1 Basement, ground floor and first floor of the BEC

also as an emergency exits in case of evacuation. The first floor serves for shopping and entertainment (40 shops, a cinema and a technical centre). From the first floor lead two emergency exits and a stairway. The BEC object has two emergency exits on each floor and an evacuation lift. On the ground floor there is possibility of exits through four access points, two of which are directly from shopping units. From the basement the exit is possible through two access points. The BEC object was analysed in detail from the standpoint of the external security environment (location of object, access roads, nearby surroundings and neighbouring objects, engineering networks, Integrated Recue System units arrival time, ...) and internal security environment (number of floors, arrangement of operations and support services, exits, number and character of entrance points in the building, permeability of emergency exits, security systems, entrance control, evacuation routes, technical infrastructure and key technology provision, location and building and technical solutions of parking lots and other factors).

The increased risk is due to the location of the centre along the main road, the large number of entrances to the building object, unsecured access to the technical section – no mechanical system. There is insufficient number of cameras and non-monitored entrances to the building from the view of electronic security. The critical issue is simple access to the ventilation system, the entry point is without any security. The high risk is also unsecured access to the terrace, the parking lot in the building as well as other identified security risks.

The time of arrival of all Integrated Recue System units in case of necessity is maximum 10 min. In case of a favourable traffic situation, it is possible to expect the arrival of Integrated Recue System units within 5–6 min.

19.5.2 Defining and Analysing Scenarios for Threats Related to Attacks on Soft Targets

Within the security analysis, four most likely scenarios, which could have a significant impact on the number of victims, were identified and there is a higher frequency of their occurrence, too. Selected scenarios:

- attack by firearm,
- vehicle attack,
- attack using an explosive stored in a bag or backpack,
- chemical attack.

These scenarios were analysed using the ETA – Event Tree Analysis and FMEA -Analysis of possible failures and their consequences. Each analytical method has its strengths and weaknesses. However, it is important to select the right method for a particular purpose. E.g. according to [11], ETA is known for its clarity, while the FMEA stands out in simplicity but a prerequisite is the involvement of experienced professionals to objectively assess the degree of severity, probability and possible consequences of incidents.

ETA – Event Tree Analysis Four selected scenarios were considered in the analysis which appear to be the most serious in terms of the number of victims and the frequency of their occurrence. Since the analyses are rather extensive, only conditions and results for one scenario – **attack by a chemical dangerous substance released into the ventilation system are presented**. In the case of the BEC object being analysed, this is the most risk threat, since access to the ventilation system is possible because it is not secured enough, access is possible from the parking lot. There is also no rapid detection of hazardous chemicals. This type of attack actually threatens most of the people in the facility. The results of the probability analysis of the individual scenarios for the attack by the chemical dangerous substance are in Fig. 19.2

A key measure is the elimination of the access to the ventilation system, preferably through a mechanical interlocking system. In case of an attack through the ventilation system, it is also important to immediately identify the chemical attack (chemical detectors) for the possibility of early evacuation and minimization of losses. With the implemented measures, the most risk result was eliminated to half of the value (see Fig. 19.3).

FMEA – Analysis of Failures and Their Consequences The analysis of possible errors and their consequences on the BEC object contains defining 20 problems that

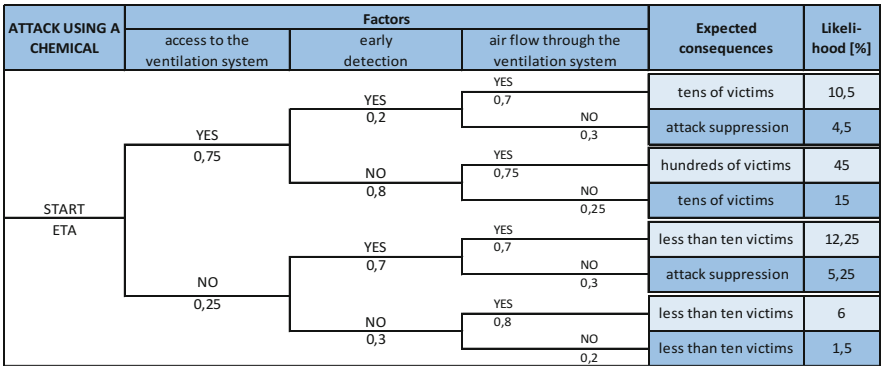

Fig. 19.2 ETA – chemical dangerous substance into the ventilation – current state

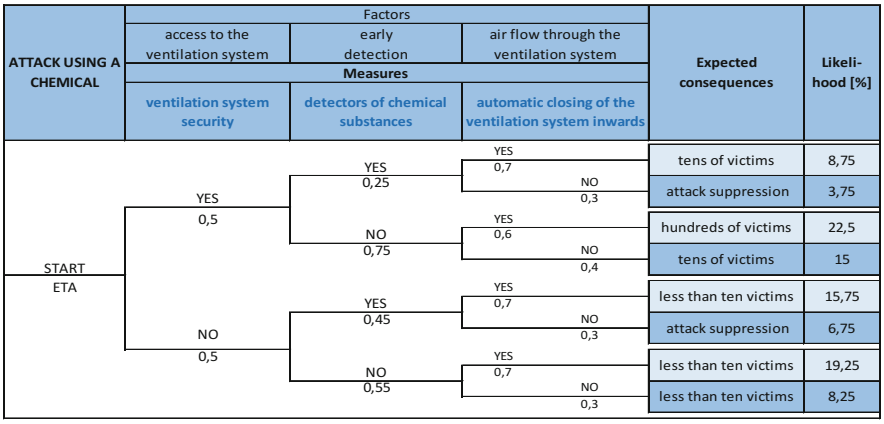

Fig. 19.3 ETA – chemical dangerous substance into the ventilation – after measures

may arise. The analysis consisted in assessing the severity (S), the probability (P) and the detectability of the problem (D) through the value of the parameter RPN – Risk Priority Number, representing conjunction of the 3 factors

$$\mathrm{RPN} = \mathrm{S} * \mathrm{P} * \mathrm{D} \tag{19.1}$$

If the value exceeded 100, appropriate permanent measures were defined based on the root cause and, once introduced, the RPN was determined again. To illustrate the progress of the analysis, only the severity of the adverse event in terms of possible health risk (Fig. 19.4) and the predicted frequency of occurrence are shown (Fig. 19.5).

Additional classification tables have been introduced in the implementation of the FMEA method focusing on other important factors such as the possibility of detecting an undesirable event, possible consequences of an asset nature, etc.

Problem severity	Possible health damage	Rating
Very high	death	10
	serious injury - 2 or more people hospitalization	9
	serious injury – 1 person hospitalization	8
High	injuries with the incapacity for work – 2 or more persons	7
	injuries with the incapacity for work – 1 person	6
Medium	injuries requiring treatment - 2 or more persons	5
	injuries requiring treatment – 1 person	4
Low	minor injury 2 or more people - no treatment required	3
	minor injury 1 person - no treatment required	2
Negligible	no damage to health	1

Fig. 19.4 FMEA – classification for event severity: possible injury to health

Problem: likelihood	The frequency of problem occurrence	Rating
Very high	Once a day	10
	Once a week	9
	Once 2 weeks	8
High	Once a month	7
	Once 3 months	6
Medium	Once 6 months	5
	Once a year	4
Low	Once 5 years	3
	Ones 10 years	2
Negligible	Once 50 years	1

Fig. 19.5 FMEA – classification for event severity: frequency of occurrence of the problem

Out of the total of 20 identified threats, 7 risk scenarios were identified for the BEC object (Fig. 19.6). These were threats relevant to the soft targets: a cold weapon attack, attack by shooting weapon, a chemical attack through the ventilation system, and an attack by a vehicle driven into persons at a bus stop, a suicide bomber, an attack by an explosive stored in abandoned luggage and an acid spray.

The Attack of Chemical Released into the Ventilation System After introduction of all measures within the anti-chemical threat, it is possible to reduce the probability of a successful attack by 51.4% but still to a relatively high value of 28% (see Fig. 19.7)

The Attack of Chemical Released into the Ventilation System After introduction of all measures within the anti-chemical threat, it is possible to reduce the probability of a successful attack by 51.4% but still to a relatively high value of 28% (see Fig. 19.7)

For chemicals, it is a major problem that even after detection, it is not usually possible to prevent the spread of the substance. After the introduction of the measures, it is possible to expect a significant improvement in the number of

Problem	Risk category	Before the measures				Immediate measures	Root cause	Permanent measures	After the measures			
		S	P	D	RPN				S	P	D	RPN
a cold weapon attack	attacker	9	5	7	**315**	action by the security service, detention of the offender, handing over of police	**insufficient controls, identification and monitoring of suspects**	installation of smart video system	8	4	3	**96**
attack by shooting weapon	attacker	9	3	7	**189**	action by the security service, detention of the offender, handing over of police	**insufficient controls, identification and monitoring of suspects**	installation of smart video system	9	3	3	**81**
a chemical attack through the ventilation system	attacker	10	3	6	**180**	evacuation of persons, suction through the ventilation for maximum performance	**insufficient security and monitoring of access to the ventilation system**	mechanical barriers to access to the ventilation system	10	1	5	**50**
an attack by a vehicle driven into persons at a bus stop	attacker	8	3	7	**168**	evacuation in case of explosion	**insufficient barrier systems**	building a defense system	10	1	7	**70**
a suicide bomber	attacker	10	3	6	**180**	detention of the offender, evacuation of person	**insufficient control of suspects**	random checks of person	10	1	6	**60**
an attack by an explosive stored in abandoned luggage	attacker	9	3	7	**189**	evacuation of persons	**capturing an explosive into an object**	random baggage checks	10	2	3	**60**
an acid spray	attacker	6	3	6	**108**	rescue call, first aid	**a ban on bringing bottles into the building**	control of visible bottles	7	1	8	**56**

S– severity P – probability D – detectability RPN – Risk Priority Number (RPN = S * P * D)

Fig. 19.6 FMEA analysis – results (before and after the implementation of measures)

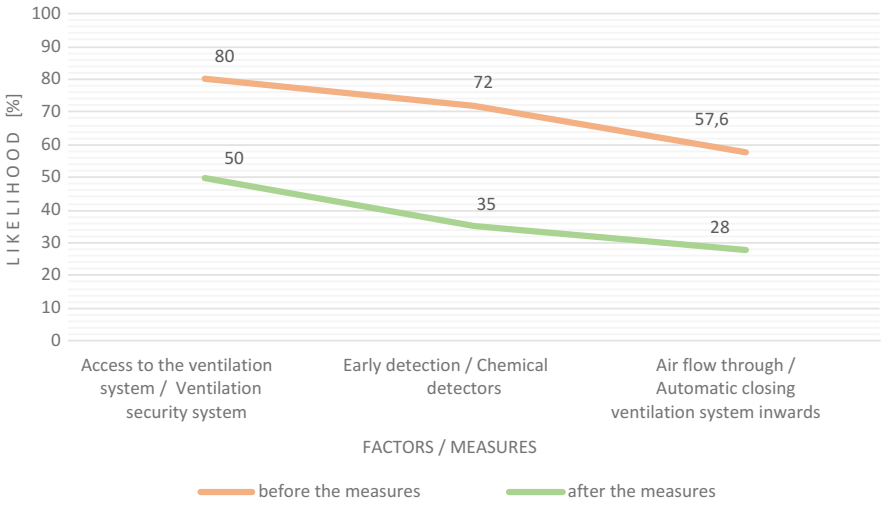

Fig. 19.7 FMEA – comparison of the likelihood of an incident (before and after the measures)

predicted casualties from tens to individuals (see Fig. 19.8). An increase in the likelihood of an attack disposal in 250% is significant but the absolute value is still low at 12%.

The results of the FMEA analyses revealed that the first three threats can be significantly eliminated by introducing appropriate measures (Fig. 19.9). In the first scenario – a cold weapon attack, the threat decreased in 70%. In the case of a

Fig. 19.8 FMEA – comparison of the consequences of the attack (before and after the measures)

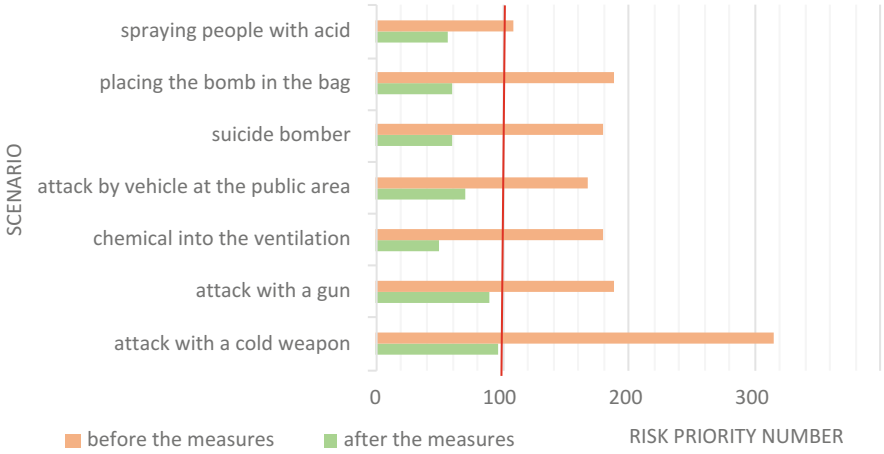

Fig. 19.9 FMEA – results (before and after the measures implementation)

short firearm, the threat was reduced by 57.1% and in the case of attack by the chemical released into the ventilation, an improvement of up to 76.2% was achieved. See Fig. 19.6.

For RPN coefficients with value above 100, immediate countermeasures were set and a root cause was determined (Fig. 19.6). Consequently, permanent measures have been introduced to reduce the frequency of occurrence and consequences of the undesirable event. Efforts were to find such measures that would reduce the RPN value below 100 points. The attack by the vehicle driven into persons at the bus stop

in front of the BEC, the attack by suicide bombers, the attack by placing the explosive in abandoned luggage and attack by acid scourging – the threat level was reduced by 50%. The most significant positive change was the implementation of mechanical protection system of the access to the ventilation system.

19.6 Conclusions

In general, it can be said that soft targets are not protected in any country sufficiently. Soft targets cannot be protected by police or other unit from the outside from capacity reasons. They always require the active cooperation of all entities located in a vulnerable place. Objects categorized as soft targets are always different because each object has its own specifics that are reflected in different changing values.

For all soft targets, however, the same principles for enhancing their resilience are valid which can be characterized as follows:

- Know own security features and character – analyse what or who is to be protected and against whom, to define strengths and weaknesses.
- Methodologically set up security development – identify threats, define scenarios, assess the probability of occurrence and possible impact of threats, define security measures, determine competencies and responsibility for measures and practice the relevant scenarios regularly.
- Define measures to prevent and mitigate impacts – early detection of a threatening attack and defining measures for subsequent mitigation of impacts on protected interest.
- Involve unskilled staff – co-operation and involvement of local staff, e.g. assistance with adherence to preventive measures and reporting suspicious activity.
- Standardize security procedures – the exactness and system of the actions taken in every situation and for everyone (mainly evacuation, designation of a secure temporary hide place, . . .).
- Elaborate Management Coordination Plan – allow to limit stress-related mistakes in respective situation, division of tasks among more persons and so eliminating dependence on one person, a clearly formulated way of communication, appointment of a coordinator with his/her representatives.
- Increase security awareness – through regular training, familiarizing staff with likely scenarios, practicing procedures.
- Collaborate with the Integrated Rescue System (IRS) units – allow to inspect the object, involve appropriate units in the preparation of security actions, inform about suspected and security incidents.
- Implement rigorous authorization and entry control – enable detecting intentions of violent activity, detection of suspicious behaviour, physical control to detect the weapon, preventive security interview and others.

- Analyse surroundings and work with other soft targets – create communication channels with surrounding entities, share information and etc. [3].

References

1. Ministry of the Interior of the Czech Republic (2016) Security policy [online]. Praha. http://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx. Last accessed 22 Aug 2018
2. Kalvach Z (2016): Soft targets protection elements: methodology [online]. Ministry of Interior of the Czech Republic, Praha
3. Global Terrorism Database (GTD), University of Maryland. https://www.start.umd.edu/gtd/. Last accessed 31 July 2018
4. Potential Terrorist Attack Methods (2008) Joint special assessment [online]. Federal Bureau of Investigation, Washington, DC. https://nsarchive2.gwu.edu/nukevault/ebb388/docs/EBB015.pdf. Last accessed 12 Sept 2018
5. Rehak D, Hromada M Novotny P (2016) European critical infrastructure risk and safety management: directive implementation in practice. In: 15th international symposium on loss prevention and safety promotion, Freiburg, Germany, June 05–08, 2016. Chemical engineering transactions. vol 48, pp 943–948
6. Rehak D, Markuci J, Hromada M et al (2016) Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. Int J Crit Infrastruct Prot 14:3–17
7. Stoller J, Zezulova E (2015) The field testing of high performance fiber reinforced concrete slabs under the TNT load explosion together with the analytical solution and the numerical modelling of those tests results. In: International conference on military technologies – ICMT 2015, Brno, May 19–21, 2015. OPROX, Inc., pp 211–218
8. Stoller J, Dvorak P (2016) experimental ballistic loading of steel fiber reinforced concrete slabs and unreinforced concrete slabs by plastic explosives. In: International conference on durability of critical infrastructure, monitoring and testing (ICDCF), 2016. Lecture notes in mechanical engineering, pp 110–119
9. Figuli L, Bedon Ch, Zvakova Z et al (2017) Dynamic analysis of a blast loaded steel structure. In: 10th international conference on structural dynamics (EURODYN), Sapienza Rome, Italy, 2017. Procedia engineering, vol 199, pp 2463–2469
10. Lovecek T, Ristvej J, Sventekova E et al (2016) Currently required competencies of crisis and security managers and new tool for their acquirement. In: 3rd international conference on management innovation and business innovation (ICMIBI 2016). Lecture notes in management science, vol 58, pp 3–8
11. Sventekova E, Dvorak Z (2011) Human activity as a risk in railway transport. In: 15th international conference "transport means", University of Technology, Kaunas, 2011. Transport means, pp 524–529