

Application of a systematic methodology to terrorism risk management

M. M. Bardazza², P. Vestrucci¹, G. Zappellini¹, P. Adinolfi²,
M. Buldrini¹, S. La Rovere¹ & C. Vercilli¹

¹*NIER Ingegneria S.p.A., Italy*

²*ESSETI, Italy*

Abstract

Due to the complexity and the heterogeneity of the evaluations involved, terrorism risk management requires a systematic and organized methodology to enable a thorough analysis of the possible attack modes and vulnerabilities that the structure being analyzed presents. This study defines an overall methodological approach for assessing the terrorism risk and provides a practical application to a localized but duly characterized infrastructure. Many standards of American and Anglo-Saxon origin, featuring different levels of detail and fields of application, define the essential characteristics of the analysis process and terrorism risk management. The proposed approach has been developed on the basis of said criterion and of the methodologies currently used in the assessment of natural and industrial risks. The essential risk management tool, which must be updated during the analysis, is known as the Hazard Log. It is by means of an index model that a quantitative assessment of the structure's vulnerabilities is performed. The application of this methodology to a real building ("Pirelli" skyscraper, federal building in Milan) aims at evaluating its effectiveness in terms of analytical detail and ability to provide concrete guidelines as to the need for further technical and procedural countermeasures and/or detail analysis.

Keywords: terrorism, building, risk prevention, risk protection, vulnerability assessment, risk assessment.

1 Introduction

The application of a systematic methodology is particularly necessary during a preliminary risk assessment, aimed mainly at defining the subsequent closer



examination on the basis of the peculiarities of the structure in reference. For this purpose, the guidelines fixed in many standards of American and Anglo-Saxon origin are taken as a reference for defining an overall analysis methodology and, in particular, a structured approach aimed at the “initial screening” of a localized infrastructure (building, church, stadium, event, etc.). The standards taken as reference are essentially publications of the Federal Emergency Management Agency (FEMA) and National Institute of Standard and Technology (NIST). FEMA [1, 2] recently launched a new series of publications directed at providing design guidance for mitigating terrorist risks, reducing physical damage to structural and nonstructural components of buildings and related infrastructure. NIST [3] suggests the use of the analysis methodologies proposed by FEMA and integrates them with methods and models for subsequent cost/benefit analyses, performed to choose the technical and/or procedural countermeasures to implement in order to reduce the residual risk to a level deemed acceptable.

According to a commonly adopted division, the terrorism risk analysis process develops in three distinct phases: Threat Assessment (TA), Vulnerability Assessment (VA) and Risk Assessment (RA). The purpose of the TA is to identify and study the hazardous conditions in terms of potential aggressor (Threat) and attack mode (Hazard). In the proposed analysis method Threat Assessment is performed in two distinct stages: a Hazard Identification phase, which precedes the Vulnerability Assessment of the structure and defines the attack modes to analyze, and a subsequent Hazard Analysis in which potential consequences are assessed on the basis of the results obtained. The list of attack modes taken as a reference is defined by FEMA [1, 2]. The consequences linked to a terrorist attack are assessed with reference to the following elements considered significant: loss of human life, material damage, business interruption and untouchable consequences (in terms of “image” and impact on the public opinion). The purpose of the VA phase is to assess the “weaknesses” of the structure, such as the specific characteristics or the deficiencies of the existing security system. The analysis is performed by applying Check Lists defined by FEMA [1, 2]. The purpose of the RA phase is to summarize, both analytically and numerically, the results obtained from the analysis of each attack mode in terms of structure vulnerability and possible consequences.

The level of analysis detail can be established on the basis of the aims proposed (e.g. census of “sensitive” infrastructures, detail analysis of a “sensitive” infrastructure), while not altering the described methodological approach.

2 Methodological approach

2.1 Hazard identification

The Hazard Identification phase aims at identifying and characterizing the attack modes to take into account in the terrorism risk analysis of the structure in reference. The identification and characterization of the terrorist subject consists of a continual and complex activity that simultaneously includes the



governmental spheres and each public or private subject involved. The definition over time of the terrorist subjects (Threats) and their characterization in terms of “existence”, “capacities”, “history”, “intention” and “probability of performing a hostile act”, is an activity that cannot be assigned to appointed governmental spheres.

The identification of attack modes (Hazard) is closely correlated to the result of the previous activity; however, in the absence of precise guidelines, identification of the attack modes (Hazard) can be performed in parallel. In the example contained in §3, the list of attack modes is inferred from the publications of FEMA [1, 2]. The hazards analyzed, duly characterized in terms of Application Mode and Hazard Duration, are as follows: Conventional Bomb (Stationary vehicle, Moving vehicle, Mail, Supply, Thrown, Placed, Personnel), Biological Agents ((1) Anthrax, Plague, Viral hemorrhagic fever; (2) Smallpox, Botulism, Brucellosis, Tularemia, Toxins), Chemical Agents ((1) Blister, Blood, Choking/lung/pulmonary; (2) Nerve; (3) Riot control/tear gas, Vomiting, Incapacitating), Armed (Ballistics, Stand-off weapons), Arson/Incendiary Attack, Nuclear Device, Radiological Agents, Hazardous Material Release (fixed facility or transportation).

On the basis of this list the Hazard Log is initialized.

In this paper is deliberately neglected the assessment of the probability of occurrence of each attack mode that involves the evaluation of parameters based on political and historical considerations: the risk of a terrorist attack is strictly associated to the vulnerability that characterizes the analyzed infrastructure.

2.2 Vulnerability assessment

The Vulnerability Assessment phase aims at identifying the “vulnerabilities”, meaning the specific aspects or physical part of the structure which, with reference to one or more attack modes, can involve scenarios of considerable damage. A preliminary phase of familiarization with the structure to analyze is aimed at gathering the technical and management information that can be important in subsequent assessments.

In the example used in §3, Check Lists defined by FEMA [1, 2] have been used, each referred to a specific Vulnerability Feature. On the basis of the proposed objectives, it is possible to adjust the analysis detail level by integrating or simplifying the Check List in reference. FEMA Check Lists underlines a significant superimposition of the information linked to different aspects of vulnerability. In order to identify a reduced number of vulnerability aspects, that are uniform in terms of detail of the associated information and distinct from each other, the following main features are defined: Site, Architectural - Structural System, Utility System, Equipment Operations and Maintenance, Security Systems. A Check list is developed for each Vulnerability feature.

In general, the check list is made by analyzing the structure plan and management records and through on-the-spot technical inspections. In the example contained in §3, only information accessible by the public has been used; this approach enables to perform an implicit “accessibility” analysis of the



information (identification of the information deemed “vital” as it is necessary for identifying an aspect as being vulnerable).

Using the previously initialized Hazard Log as a basic tool, the analysis is performed systematically by individually assessing the identified attack modes as well as, for each of them, the vulnerability aspects. In general, each structure vulnerability aspect affects the risk associated with a certain attack mode as it can influence the possibility of occurrence of a damage event and its gravity. As regards the vulnerability aspects which, for the attack mode in reference, affect the structure Accessibility, a related Accessibility Index is assigned, from 0 (Vulnerability Feature not regarding Structure Accessibility) to 3 (Major Structure Accessibility). It enables a quantitative evaluation of the possibility of occurrence of a damage event due to an identified attack mode. An overall structure Accessibility Index is evaluated as the average of the Accessibility Indexes assigned for the pertinent vulnerability aspects.

2.3 Hazard analysis

Hazard Analysis is aimed at assessing the potential consequences of each attack mode. In the preliminary analysis phase it assigns an overall Damage Index to each attack mode, with reference to the heaviest damage scenario among those which can be hypothesized. The overall Damage Index - from 0 (No Damage) to 3 (Major Damage) - enables a quantitative evaluation of the damage impact of the attack mode in reference. It includes different aspects (Damage Feature) considered important for the overall assessment of the consequences of the attack: Loss of Human Life, Material Damage, Unavailability / Business Interruption and Untouchable Consequence (image and public opinion). As a characterization of the considered infrastructure, is defined a weight for each of the above mentioned aspects representing its relative importance in the overall assessment of the consequences of each attack method. The weights characterizing the analyzed structure in the example contained in §3 are shown in Table 1. For each attack mode, an overall Damage Index is evaluated as the average of the Damage Indexes assigned to each Damage Feature, weighed on the (normalized) coefficients characterizing the structure.

Table 1: Damage weight.

Damage Feature	Human Life	Material Damage	Mission Unavailability / Business Interruption	Untouchable Consequence: Image	Untouchable Consequence: Public Opinion
Damage Weight	0.4	0.1	0.2	0.1	0.2

The above-mentioned weights are assigned on the basis of the following qualitative considerations: the loss of human lives represents the most critical aspect to consider when assessing the damage produced by the terrorist event, especially in a federal building; in case of unavailability of the structure, the interruption of the service provided by the (public) subject who manages/uses the structure is considered more critical than the associated material (hence economic) damage; as they are intangible consequences, the impact of the public

opinion of the event in itself is considered more critical than the “damage to the image” suffered by the (public) subject managing/using the structure.

The approach described can be considered exhaustive if the study is aimed at taking a census of the critical structures. When performing a detail analysis, which generally refers to a limited number of attack modes, the HA should: identify and formalize the possible damage scenarios linked to each attack mode, analyzing the possible evolutions and assigning an overall Damage Index to each one; keep in mind possible diversionary attacks (against different infrastructures) and emergency situations caused by external events, even if not intentional; systematically identify the scenarios consequent to the failure of each prearranged technical measure; analyze the measures established to manage the emergency by integrating the index model in order to take into account their effectiveness and timeliness (for this purpose the models defined by the Federal Energy Regulatory Commission (FERC [5]) are recommended).

2.4 Risk assessment

For each attack mode an overall Risk Index is evaluated on the basis of the vulnerability of the structure (Accessibility Index) and its “heaviest” consequences (Damage Index). Following is the expression used: $\text{Risk Index} = \text{Accessibility Index} + \text{Damage Index} - 1$.

This expression makes it possible to approximate the expression $\text{Risk} = \text{probability of occurrence} * \text{Damage}$ (where in the analysis of terrorism risk the probability of occurrence is replaced by the vulnerability of the structure), thus reducing the number of “Classes of Risk”.

The defined Risk Assessment model makes it possible to assess the relative criticality of each vulnerable aspect, for each hypothesized attack method and the relative criticality of each attack mode, on the basis of the characteristics of the structure. For this purpose, simple graphic representations of the results obtained by applying the defined index model are particularly effective.

3 Application

3.1 Subject of the study

The analysis methodology described in §2 is applied to a real case: the “Pirelli” skyscraper, Milan. Figure 1 shows a view extracted from the 3D model developed to analyze in detail the site in reference.

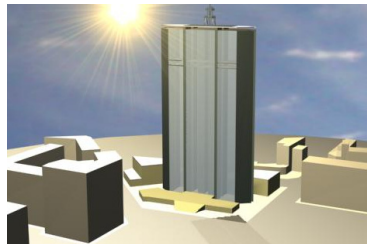


Figure 1: “Pirelli” skyscraper, Milan.

For reasons of synthesis, the Check Lists developed for each structure Vulnerability Feature are not included. In what follows, a part of the Hazard Log card developed for a specific attack mode is provided.

3.2 Hazard log

The following tables contain the parts constituting a single Hazard Log card, regarding a specific attack mode: Conventional Bomb by a Moving Vehicle. Table 2 contains the information regarding the identification of the Hazard in reference, in terms of Application Mode and Hazard Duration.

Table 2: Hazard log, hazard identification.

Hazard	Application Mode	Hazard Duration
Conventional Bomb by Moving vehicle	Detonation of explosive device on or near target	Instantaneous

Table 3 contains the results obtained from the Vulnerability Assessment, regarding the attack mode in reference: for each Vulnerability Feature, its Damage impact and the corresponding Accessibility Index is evaluated on the basis of the results obtained by applying the relative Check List.

Table 3: Hazard log, vulnerability assessment.

Vulnerability feature	Damage Impact	Accessibility index
Site	x	2
Architectural - Structural System	x	2
Utility Systems	x	0
Equipment Operations and Maintenance		3
Security Systems	x	2
All Vulnerability features		1.80

Table 4 contains the results obtained from analyzing the attack mode in reference: for each Damage Feature the corresponding Damage Index has been evaluated on the basis of the heaviest damage scenario among those which can be hypothesized. The overall Damage Index is calculated as the average of the Damage Indexes assigned to each Damage Feature, weighed on the coefficients characterizing the structure, contained in Table 1.

Table 4: Hazard log, hazard analysis.

Loss of Human Life	Material damage	Unavailability / business interruption	Untouchable consequence: image	Untouchable consequence: public opinion	Damage index
3	3	3	2	2	2.7

As main results of the Risk Assessment, a related Risk Index is evaluated for each Hazard on the basis of the values assessed for the Accessibility Index

(whether overall or related to each feature) and for the overall Damage Indexes. With respect to the attack mode in reference, it results a Risk Index equal to 3.5.

The analysis is completed by identifying the possible countermeasures to adopt to reduce the risk associated with each attack mode. With reference to a specific Hazard, each single Vulnerability aspect is analyzed and the possible measures in terms of prevention and structure protection are identified. The preventive measures aim at reducing structure accessibility; the protective measures, which usually include all the emergency management aspects, are aimed at reducing the damage consequent to the occurrence of the terrorist event.

Table 5 contains several additional preventive and structure protection measures, as well as the detail assessments to perform, with reference to the Hazard in reference and the main Vulnerability features.

Table 5: Risk assessment – possible countermeasures.

Vulnerability Feature	Preventive Measures	Protective Measures	Detail Assessments
Site	No parking on the block where the building is located. Use of reinforced devices (built into urban furnishing components). Creation of guided and low speed lanes for all vehicles entering the parking area. Inspection of vehicles entering from the perimeter.	Separate paths for pedestrians and vehicles.	Calculation of the vehicle maximum approach speed.
Utility Systems	<u>Mechanical Systems</u> Drafting of a specific protection plan for the ventilation system.	<u>Mechanical Systems</u> : Fume evacuation system. Creation of a (at least partially) redundant system. <u>Plumbing and Gas System</u> : Partial redundancy of the plumbing system. Electricity distribution redundancy in critically important areas. Backup fuel storage outside the building. <u>Fire Alarm System</u> : Use of weight- and pressure-resistant components. Facilities integrated with building safety and management systems. <u>Communications and IT Systems</u> : Redundancy of the server and data storage. Room climate control system. Implementation of a satellite communication network.	Analysis of the availability of auxiliary systems, even as regards preliminary sabotage events.

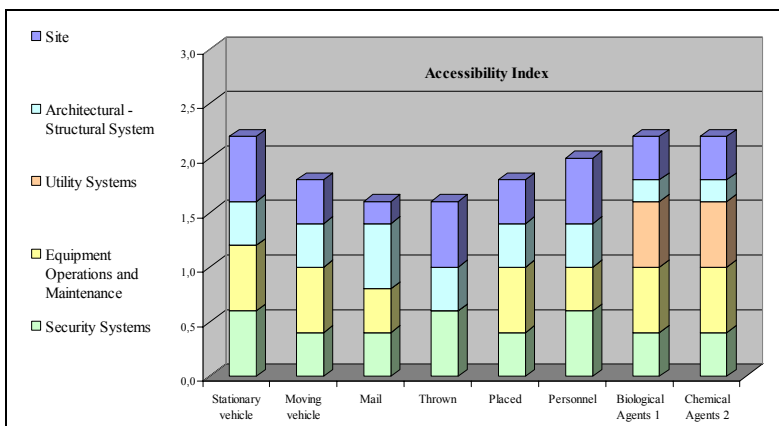


Figure 2: Structure accessibility index.

3.3 Summary of the results

For the main attack modes (Hazard), Figure 2 provides the overall Accessibility Index and the contributions regarding each vulnerability aspects.

For the main attack modes (Hazard), Figure 3 provides the overall Damage Index and the contribution regarding each Damage Feature (evaluated on the basis of the Damage Indexes assigned during the HA and of weights defined in Table 1).

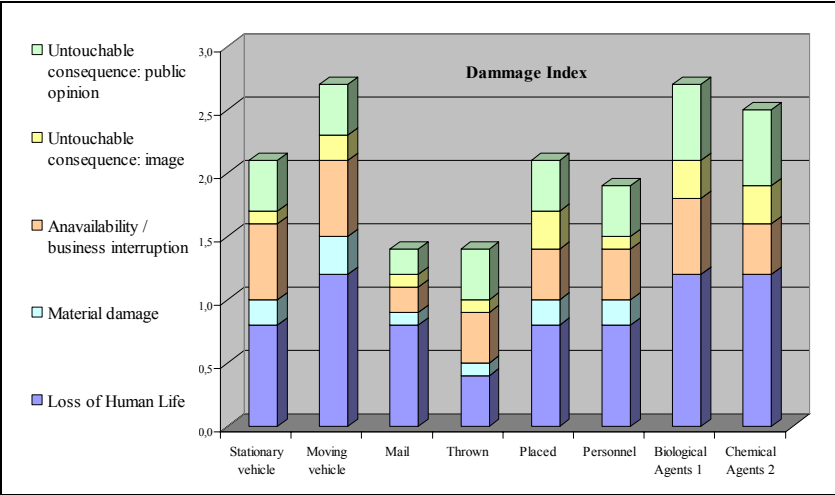


Figure 3: Structure damage index.

The following graphs contain two equivalent representations of the Risk Assessment model. Figure 4 provides the Risk Index (Accessibility Index + Damage Index – 1) resulting from the main Hazard.

Figure 5 provides the same results by means of a “Risk Matrix”.

This last representation is suitable for defining the different classes of risk on the basis of which an Acceptability Criteria is established. As regards the aims proposed for this (preliminary) analysis, a possible acceptability criteria is to consider: “acceptable” the risk associated with an attack mode of the “low risk” area; “tolerable” the risk associated with the attack mode in the intermediate area; “intolerable” the risk associated with the attack mode in the “high risk” area. It is considered strictly necessary to adopt technical and operational measures for the prevention and structure protection from attack modes whose risk is “intolerable”. Detail analyses are deemed necessary for attack modes whose risk is “tolerable”.

The defined model can be used to assess the effectiveness of each measure, whether technical or operational, selected among the possible countermeasures identified in the analysis. Assuming the implementation of one or more preventive measures, the VA is updated by assessing their impact on each (Vulnerability) feature. Assuming the implementation of one or more protective



measures, including special emergency management measures, the HA is updated by assessing their impact in terms of damage mitigation, for each (Damage) feature. In both cases, the consequent reduction of risk and the level of residual are assessed, with reference to the defined acceptability criteria.

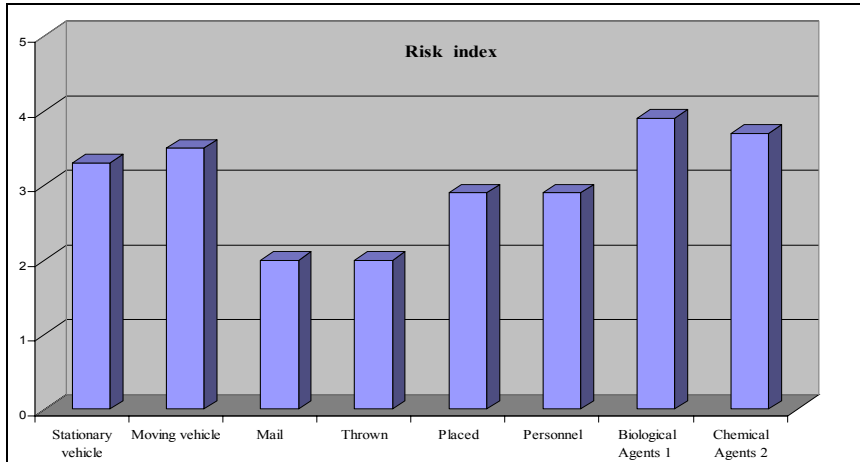


Figure 4: Structure risk index.

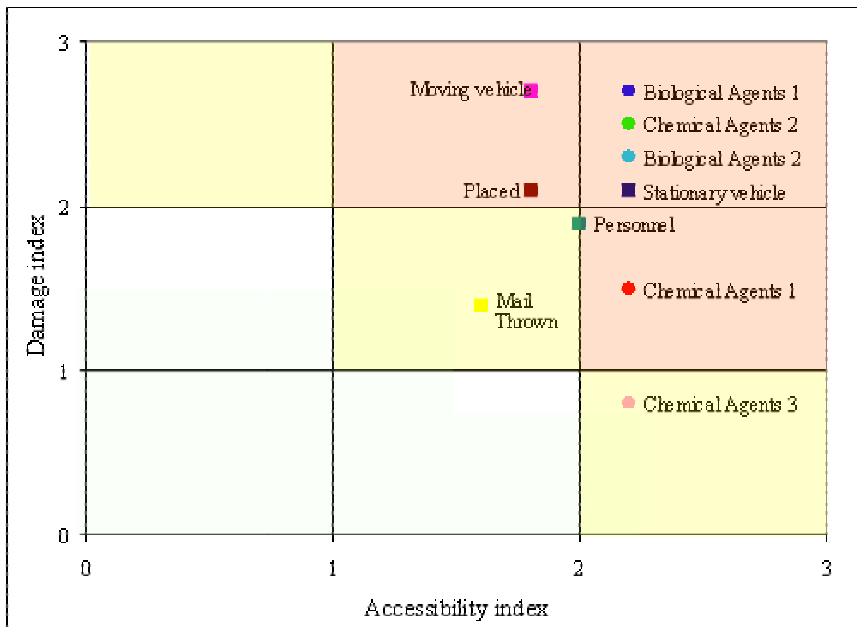


Figure 5: Risk matrix.

4 Conclusion

The application of the guidelines defined in literature for the assessment of terrorism risk, and their development on the basis of methods and models normally used when assessing natural and industrial risks, have led to the definition of a synthetic methodological approach. Said approach makes it possible to integrate innovative aspects currently not covered.

The structure's vulnerabilities (Site, Architectural - Structural System, Utility System, Equipment Operations and Maintenance, Security Systems) are defined with reference to a uniform level of detail and on the basis of specific information. The concept of "Vulnerability" is analyzed in its twofold impact on structure accessibility (possibility of occurrence of a damaging event) and on the gravity of the consequences of the terrorist event. The gravity of the event is evaluated by assessing the aspects deemed significant (Loss of Human Life, Material Damage, Unavailability/ Business Interruption and Untouchable Consequence), with respect to the characteristics of the structure and of the subject that manages it. The possible countermeasures are identified in term of preventive and protective measures which, in different ways, can reduce the residual risk.

In conclusion, it is felt that the application of a systematic approach for assessing the terrorism risk can be effectively performed according to the described methodological approach. It is suitable for analyses featuring different levels of detail; further, it can be integrated in a cost/benefit analysis context, thus enabling the assessment of residual risk following the implementation of countermeasures in addition to the existing ones

References

- [1] Federal Emergency Management Agency (FEMA) 426, Risk Management Series – Reference Manual to Mitigate Potential Terrorist attacks against Buildings, December 2003.
- [2] Federal Emergency Management Agency (FEMA) 429, Risk Management Series – Insurance, Finance and Regulation Primer for Terrorism Risk Management in Buildings, December 2003.
- [3] Robert E. Chapman and Chi J. Leng, National Institute of Standards and Technology (NIST). NISTIR 7073, Cost-Effective Responses to Terrorist Risks in Constructed Facilities, March 2004.
- [4] Department of Defense (DoD), Unified Facilities Criteria (UFC), Minimum Antiterrorism Standards for Buildings, July 2002.
- [5] Federal Energy Regulatory Commission (FERC), RAM-D – Risk Assessment Methodology for Dams.

