JCSS Joint Committee on Structural Safety
Associations supporting the JCSS:
CEB, CIB, ECCS, FIP, IABSE, IASS, RILEM

ASSESSMENT OF RISK REDUCTION STRATEGIES FOR TERRORIST ATTACKS ON STRUCTURES

Annex to Risk Assessment in Engineering - Principles, System Representation & Risk Criteria (2008)

Sebastian Thöns, Technical University of Denmark, BAM Federal Institute for Materials Research and Testing, Berlin, Germany

Mark G. Stewart, The University of Newcastle, Australia

AUGUST 2019

PREFACE

This JCSS document states principles of terrorism risk assessment and decision support for the identification of efficient and performing risk reduction strategies. It aims at establishing a basis for a consistent risk assessment in conjunction with the general principles in the JCSS document on Risk Assessment in Engineering - Principles, System Representation & Risk Criteria (Faber (2008)) and the identification and ranking of risk reduction strategies accounting for cost-efficiency, life safety in conjunction with societal preferences and capabilities and the risk reduction performance quantification.

Table of Contents

1 PRINCIPLES FOR TERRORISM RISK ASSESSMENT

Terrorist attacks may be characterised as intentional man-made high consequence events. This may include acts of terrorism, insurgency, sabotage, or other malevolent events that aim to cause damage and failure of structural systems such as buildings, bridges, offshore platforms, process plants, communication towers, pipelines, dams, and others. Terrorist attack hazards may include blast loading from explosives or other energetic materials; ballistic impact from munitions and weapons; vehicle, aircraft or ship impact on structures or protective devices such as bollards; uncontrolled discharge from dams; train derailment or other hazards that affect the integrity, stability or functionality of constituents and structural systems.

The risk assessment necessitates the identification, formulation and modelling of all relevant hazard, damage and failure scenarios which lead to consequences affecting the integrity, stability or functionality of constituents and systems. The spatial and temporal boundaries have to be specified.

The formulation for the risk assessment follows the JCSS document on Risk Assessment in Engineering - Principles, System Representation & Risk Criteria (Faber (2008)). The risks are quantified as the sum of the direct and the indirect risks R_D and R_{ID} associated to direct and indirect consequences. The risks are calculated by aggregating the product of n_{EXP} exposure and direct consequence probabilities ($p\left(EX_k\right)$ and $p\left(\mathbf{C}_l \mid EX_k\right)$, respectively, associated to n_{CSTA} constituent damage states $\mathbf{C}_l$) with the direct consequences $C_D\left(\mathbf{C}_l\right)$ and of probabilities of n_{SSTA} system failure states S_m, $p\left(S_m \mid \mathbf{C}_l, EX_k\right)$, with the indirect consequences $C_{ID}\left(S_m, C_D\left(\mathbf{C}_l\right)\right)$, i.e.:

$$\begin{aligned} R &= R_D + R_{ID} \\ &= \sum_{k=1}^{n_{EXP}} \sum_{l=1}^{n_{CSTA}} \sum_{m=1}^{n_{SSTA}} \left(C_{ID}\left(S_m, C_D\left(\mathbf{C}_l\right)\right) \cdot p\left(S_m \mid \mathbf{C}_l, EX_k\right) + C_D\left(\mathbf{C}_l\right)\right) \cdot p\left(\mathbf{C}_l \mid EX_k\right) \cdot p\left(EX_k\right) \end{aligned} \tag{1}$$

1.1 THREAT AND HAZARD ASSESSMENT

The exposure probability is calculated with the probability of a threat $\Pr\left(T_k\right)$ and the probability of a hazard given a threat $\Pr\left(H_k \mid T_k\right)$.

$$p\left(EX_k\right) = \Pr\left(H_k \mid T_k\right) \cdot \Pr\left(T_k\right) \tag{2}$$

The threat constitutes the intent to attack or damage a system involving structures. A threat assessment should allow for the modelling of the k relevant threat scenarios covering the time period of the risk analysis. Threat scenarios should include e.g. planned attacks with Vehicle-Borne Improvised Explosive Devices (VBIEDs), person-borne IEDs, vehicle impact, etc.. Government agencies and standards also provide guidance on threats and hazards to consider (e.g., FEMA 2003, US DoD 2003). The analysis of events with e.g. the Global Terrorism Database (GTD 2018) may provide useful information and statistics for the past development of threats. The GTD constitutes comprehensive and publicly accessible database of 170,000 terror attacks around the world from 1970. A threat assessment and prediction should be performed with a well-defined interface to a threat assessment provider in conjunction with police and security services information.

The hazard is the expected loading or demand given the threat like e.g. the structural force resulting from a vehicle impact. The hazard probability should be calculated accounting for the process of realising the threat which is e.g. for an IED the manufacturing, the placement and technical reliability of the detonation mechanism. The hazard probability can be modelled discretely, distributed or as a hazard curve. For example, the likelihood that a terrorist bomb or IED will successfully detonate and reach its full energetic potential is less than $\Pr\left(H_k \mid T_k\right) = 20\%$ for attacks in Western countries (Grant and Stewart Mark (2015)). Figure 1 provides a hazard curve for a threat scenario constituting the detonation of a small van-sized VBIED comprising 116 kg of homemade Ammonia Nitrate Fuel Oil (ANFO). Here, the uncertainties relating to the charge mass, its manufacture, and blast loading model errors are accounted for. Figure 1 shows the resulting peak pressure hazard curve on a structure located 50 m from the detonation (see e.g. Stewart and Netherton (2015)).

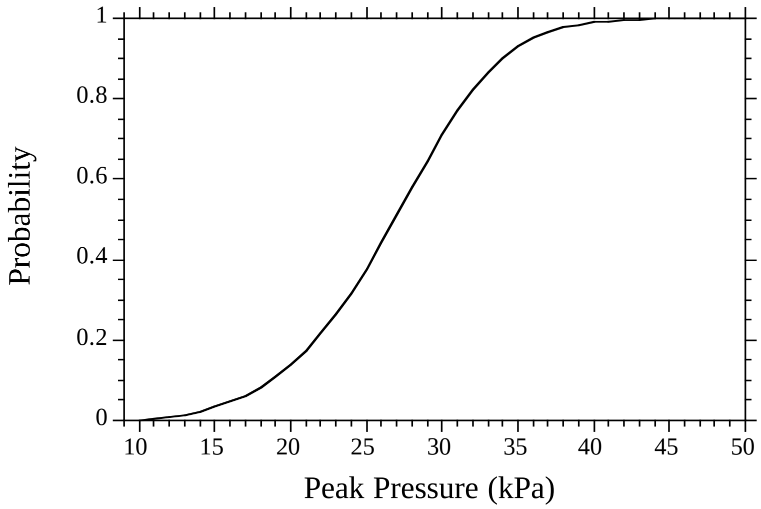

Figure 1: Blast loading hazard curve for a VBIED comprising 116 kg of homemade explosives.

1.2 DAMAGE AND FAILURE ASSESSMENT

The probabilities of the system and constituents damage and failure states should be quantified in conjunction with the relevance of the consequences. The probabilities of system damage state given exposure and constituents damage states $p\left(S_m \mid \mathbf{C}_l, EX_k\right)$ and the probability of a damage given exposure $p\left(\mathbf{C}_l \mid EX_k\right)$should be available depending on the explosives, impact or other hazard exposure scenarios and varying parameters. Such curves can be assessed by using standard probabilistic methods and/or statistics.

1.3 CONSEQUENCE ASSESSMENT

The consequences of a terrorist attack may encompass (i) direct consequences $C_D\left(\mathbf{C}_l\right)$due to constituent and system damage and (ii) indirect consequences

$C_{ID}\left(S_m, C_D\left(\mathbf{C}_l\right)\right)$ such as (a) loss of life, (b) business losses, loss of tourism, reduction in GDP, etc. and (c) social losses as the effect of the level of fear and anxiety within society (and perhaps on civil liberties). The consequences are interconnected, for example, a fearful public may be reluctant to travel and contributing to business and tourism losses, or may be reluctant to invest. The indirect consequences may be significantly affected by the fear they generate leading to large indirect and social losses (Mueller and Stewart (2011)).

A unique feature of terrorism and malevolent events is the desire to terrorise or psychologically affect their target, whether it be individuals, society or government. These consequences may be difficult if not impossible to quantify appropriately. However, caution is need so as not to magnify these consequences which are often self-inflicted after such an attack. Individual and societal resilience will reduce the indirect and follow-on consequences of such attacks (e.g. Mueller and Stewart (2011)).

All relevant consequences should be quantified and discounted with an appropriate discount rate applicable to decision scenario, system boundaries and time horizon.

1.4 RISK ACCEPTANCE, DOCUMENTATION AND COMMUNICATION

The risk acceptance in the context of terrorist attacks is largely related to life safety. The standards and regulations applicable to the temporal and spatial scope of the risk assessment must be fulfilled. Present standards and regulations often specify occupational or working risks to individuals and/or risks to society.

For societal risks, target probabilities can be derived by utilising the Life Quality Index and the marginal live saving principles (see Faber (2008) and ISO 2394 (2015)). This facilities that the societal preferences and capabilities can be accounted for. This might include a level of risk aversion often associated with terrorism. The target probabilities can then be compared with the quantified constituent and system failure probabilities.

As mentioned before, a unique feature of terrorism and malevolent events is the desire to terrorise or psychologically affect their target. It is thus suggested to differentiate between tangible risks expressible in monetary terms and intangible risks, which cannot easily expressed in monetary terms.

The risk documentation should encompass a detailed documentation of the considered scenarios, specifications on the calibration of the probabilistic models and the level of model sophistication and contain how the analysis depends on the threat probabilities. Both, tangible and intangible risks should be documented.

1.5 MODELLING REQUIREMENTS

The risk reduction strategy models have to account for the information and action type, their probabilistic properties and their costs and consequences. Risk reduction strategies have to be modelled with the distinction of (I) actions such as e.g. protection measures and (II) information from (a) physical measurement devices such as e.g. surveillance systems and (b) analysis information provided by e.g. enhanced models and scientific assessments.

The probabilistic system state models should be calibrated and/or substantiated with sound and high quality engineering models appropriate for the system behaviour according to the considered scenarios, system and time range.

A threat assessment and prediction should be performed with a well-defined interface to a threat assessment provider in conjunction with police and security services information. This interface should account for (1) the reference period of the threat, (2) the time period and temporal decision horizon of risk and/or decision analysis and (3) for the properties of the considered random process such as stationarity and/or ergodicity.

2 ASSESSMENT AND RANKING OF RISK REDUCTION STRATEGIES

The assessment and ranking of risk reduction strategies requires a specification of a decision scenario with an objective function based on a risk assessment, decision variables associated to the risk reduction strategies and a decision maker. The decision point in time and temporal period of the risk and decision analyses should be clearly specified for transparency and for the choice of the proper decision analysis type.

Risk reduction strategies have to be assessed in terms of their cost-efficiency and performance fulfilling the life safety and risk acceptance requirements (see above). All dependencies to the risk assessment model (Equ. (1)) need to be explicitly modelled.

A risk reduction strategy s_i is described with the information acquirement strategy $i_{i,j}$ its probabilistic outcomes $Z_{i,g}$, the probabilistic action models $a_{i,h}$ and the strategy costs and consequences C_{s_i}. The indices j, h and g refer to information or action associated decision variables.

The cost-efficiency of the strategy s_i is to be assessed by using the Bayesian decision analysis, i.e. minimising the risks and expected total costs in conjunction with the risk assessment (Section 0 and Equ. (1)) in dependency of the information and action associated decision variables and their influence on the constituent and system damage and failure states $\mathbf{C}_l$ and $\mathbf{S}$, i.e.:

$$E\left[R_i\left(i^*_{i,j}, a_{i,h}{}^*\right)\right] = \min_{i_{i,j}} E_{Z_{i,g}}\left[\min_{a_{i,h}} E''_{S_m}\left[R_i\left(i_{i,j}, Z_{i,g}, a_{i,h}, C_{s_i}, \mathbf{C}_l, \mathbf{S}\right)\right]\right] \quad (3)$$

$$\text{s.t. } E\left[R_i\left(i^*_{i,j}, a_{i,h}{}^*\right)\right] \leq R_{acc} \quad (4)$$

The optimal risk reduction strategy must comply with life safety requirements according to marginal live saving principle based on the Life Quality Index (see Faber (2008) and ISO 2394 (2015)) and fulfil the acceptability boundary R_{acc}.

Further measures to describe the performance of the risk reduction strategies may be the significance, i.e. the relative value of the strategy in relation to the risks without risk reduction, and the effectiveness. The effectiveness, as the probability of cost-efficiency of risk reduction strategies, is quantified with the distribution of the risks with and without risk reduction measures, i.e. $P\left(R_i\left(i_{i,j}, Z_{i,k}, a_{i,h}, C_{s_i}, \mathbf{C}_l, \mathbf{S}\right) > R\right)$.

The ranking of the risk reduction strategies and their combination has to be performed on the basis of the cost-efficiency in compliance with life safety requirements. A positive effect on structural vulnerability, robustness and on resilience according to the scope of the assessment should be demonstrated. Risk reduction and expected strategy costs can be documented separately to allow for an assessment with different decision maker utilities.

REFERENCES

Faber, M. H., Ed. (2008). Risk Assessment in Engineering - Principles, System Representation & Risk Criteria, JCSS Joint Committee on Structural Safety.

Grant, M. and G. Stewart Mark (2015). Probabilistic Risk Assessment for Improvised Explosive Device Attacks That Cause Significant Building Damage. Journal of Performance of Constructed Facilities 29(5): B4014009. DOI: 10.1061/(ASCE)CF.1943-5509.0000694.

ISO 2394 (2015). General Principles on Reliability for Structures ISO 2394.

Mueller, J. and M. G. Stewart (2011). Terror, Security and Money: Balancing the Risks, Benefits, and Costs of Homeland Security, Oxford University Press, USA.

Stewart, M. G. and M. D. Netherton (2015). Reliability-Based Design Load Factors for Explosive Blast Loading. Journal of Performance of Constructed Facilities 29(5): B4014010. DOI: 10.1061/(ASCE)CF.1943-5509.0000709.

US DoD (2003), DoD Minimum Antiterrorism Standoff Distances for Buildings, United Facilities Criteria UFC 4-010-02, Department of Defense, Washington, DC, 8 October 2003.